FORTINET
Network Security Expert 7

Advanced Threat Protection Study Guide

for FortiSandbox 3.0

FORTINET
NSE
NSE Certification Program

Fortinet Training

http://www.fortinet.com/training

Fortinet Document Library

http://docs.fortinet.com

Fortinet Knowledge Base

http://kb.fortinet.com

Fortinet Forums

https://forum.fortinet.com

Fortinet Support

https://support.fortinet.com

FortiGuard Labs

http://www.fortiguard.com

Fortinet Network Security Expert Program (NSE)

https://www.fortinet.com/support-and-training/training/network-security-expert-program.html

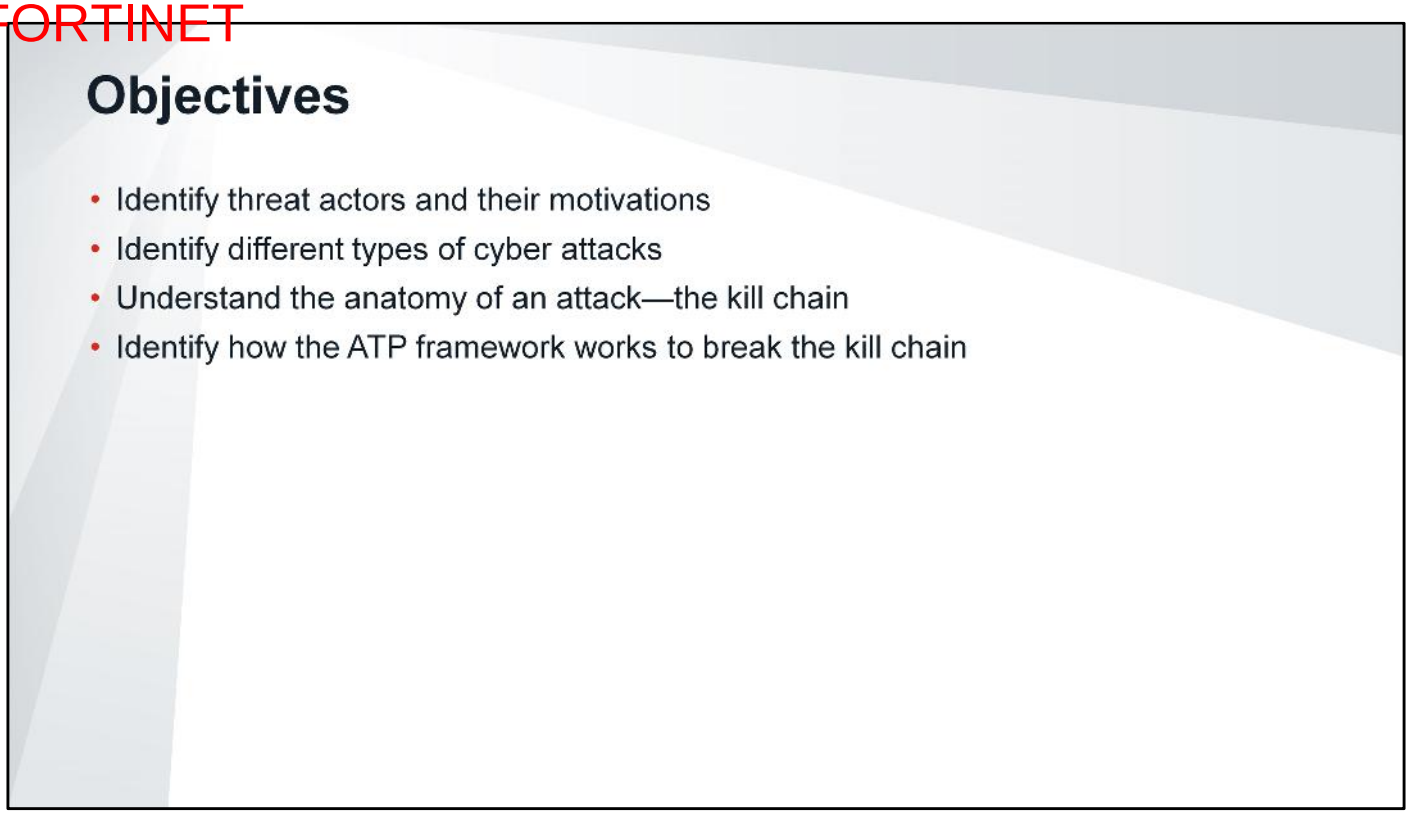
Feedback

Email: courseware@fortinet.com

7/2/2019

TABLE OF CONTENTS

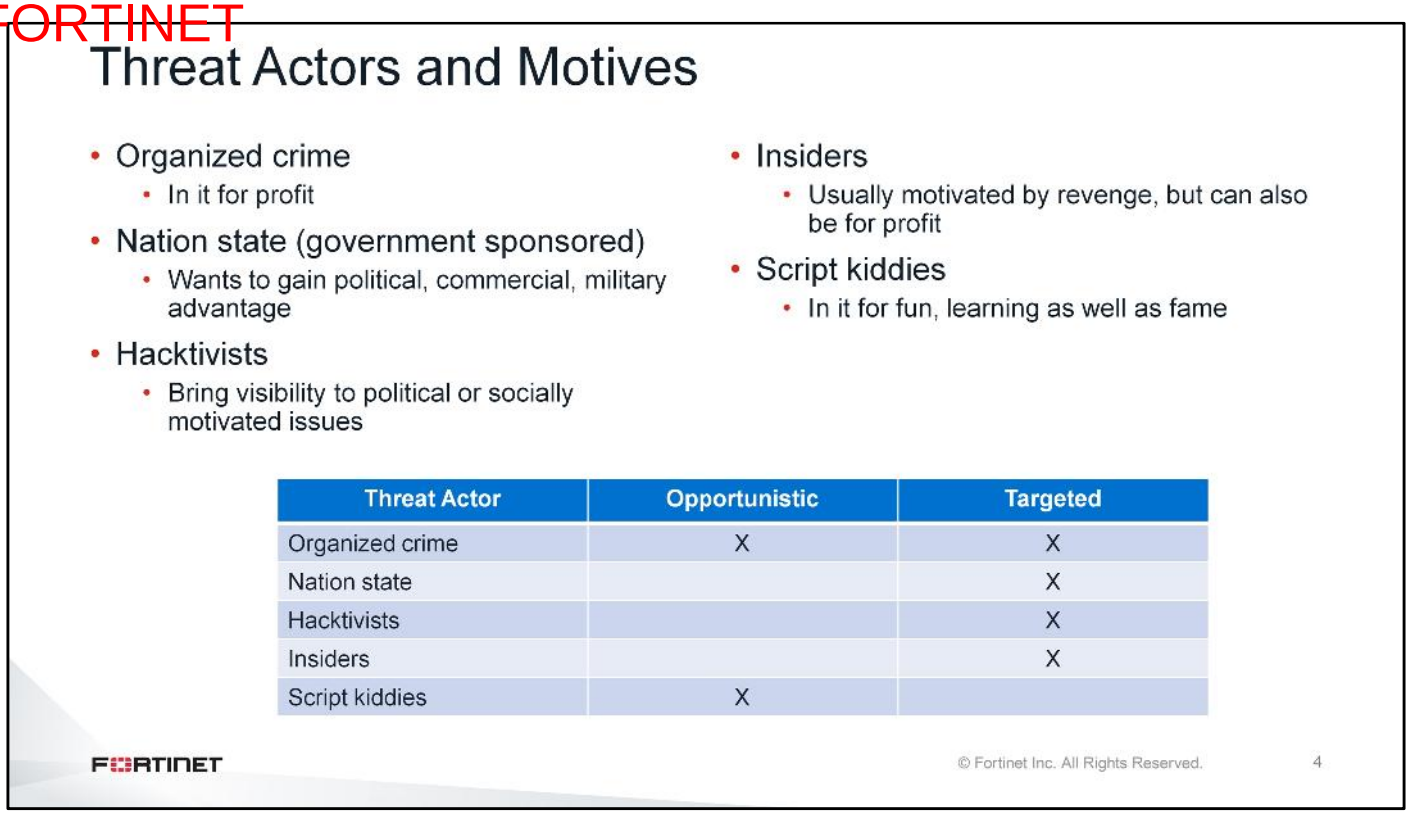
In this lesson, you will learn about threat actors and their motivations. You will also learn about the anatomy of an attack, which is also known as the kill chain, and how the advanced threat protection (ATP) framework is works to break the kill chain and stop advanced threats.



After completing this lesson, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in attack methodologies and the ATP framework, you will be able to design your ATP solution to protect your network from advanced threats.

In this section, you will learn about threat actors, what motivates them, and different types of attacks.

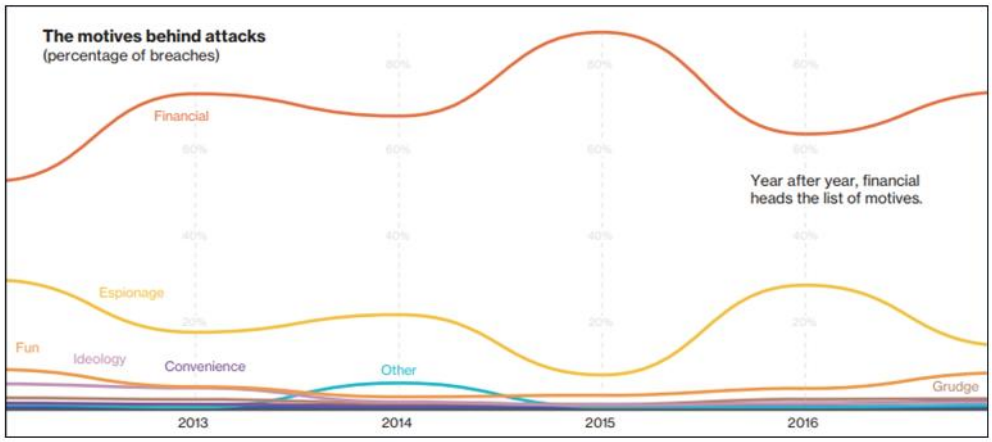


A threat actor is typically a person, or an organization, that acts with malicious intent with the purpose of compromising an organization's security or data. Threat actors are typically categorized into the groups shown on this slide.

Criminal organizations can be motivated by profit. There are government-sanctioned attacks that are looking to gain political, commercial, or military advantage. Hacktivists spearhead attacks to bring visibility to political or socially motivated issues. Insiders, such as ex-employees, can be out to get revenge or make a profit. Then, there are script kiddies who are in it for fun or fame.

Threat Actor Risk Levels

- Financial motives accounted for 76% of the breaches according to the 2018 Verizon Data Breach and Incident Report
- 39% of malware cases where ransomware



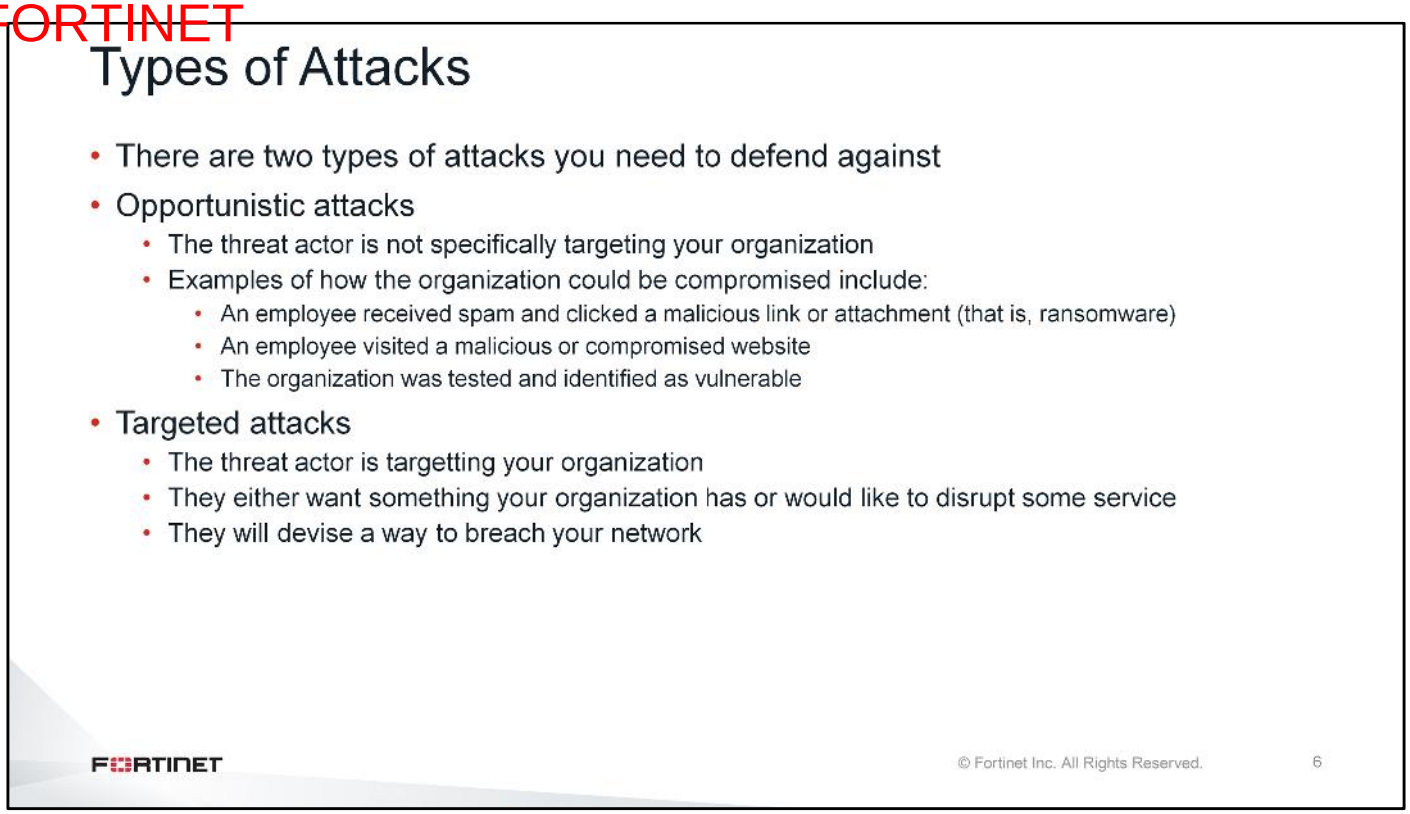
Source: https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf

FORTINET

5

According to the 2018 Verizon Data Breach and Incident Report, 76% of data breaches were financially motivated. Year after year, financial gain is the main motive for data breaches.

Ransomware is the top variety of malicious software and it is found in 39% of the cases were malware was identified.

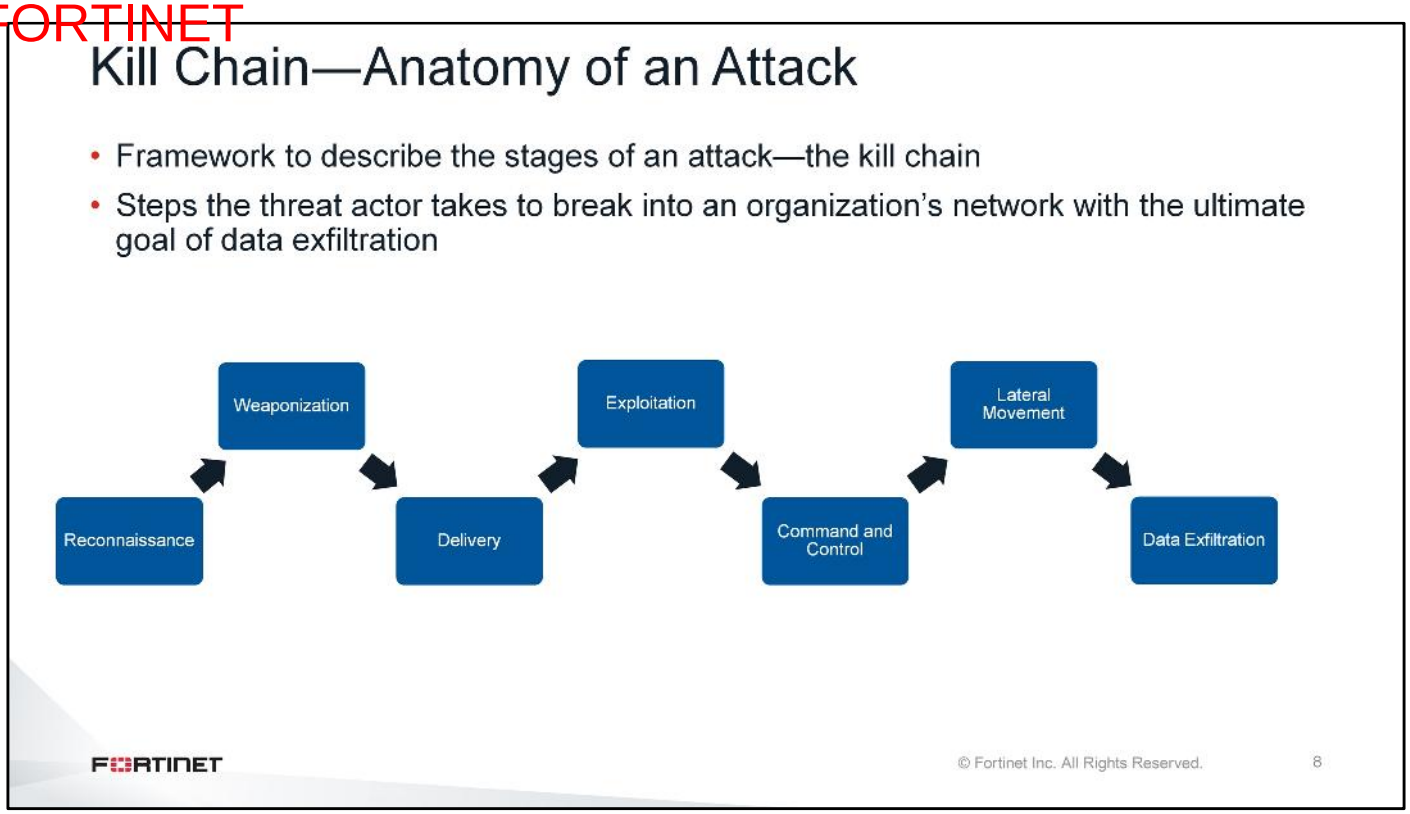


There are two categories of attacks that organizations are faced with: opportunistic attacks and targeted attacks.

In opportunistic attacks, the threat actors are *not* specifically targeting the organization in question; however, the organization can be compromised if an employee clicks on a malicious URL or attachment that was received in a spam email, or visits a malicious or compromised website. The threat actor may also use an Internet scan, or Google search to identify that the organization is potentially vulnerable to a known exploit.

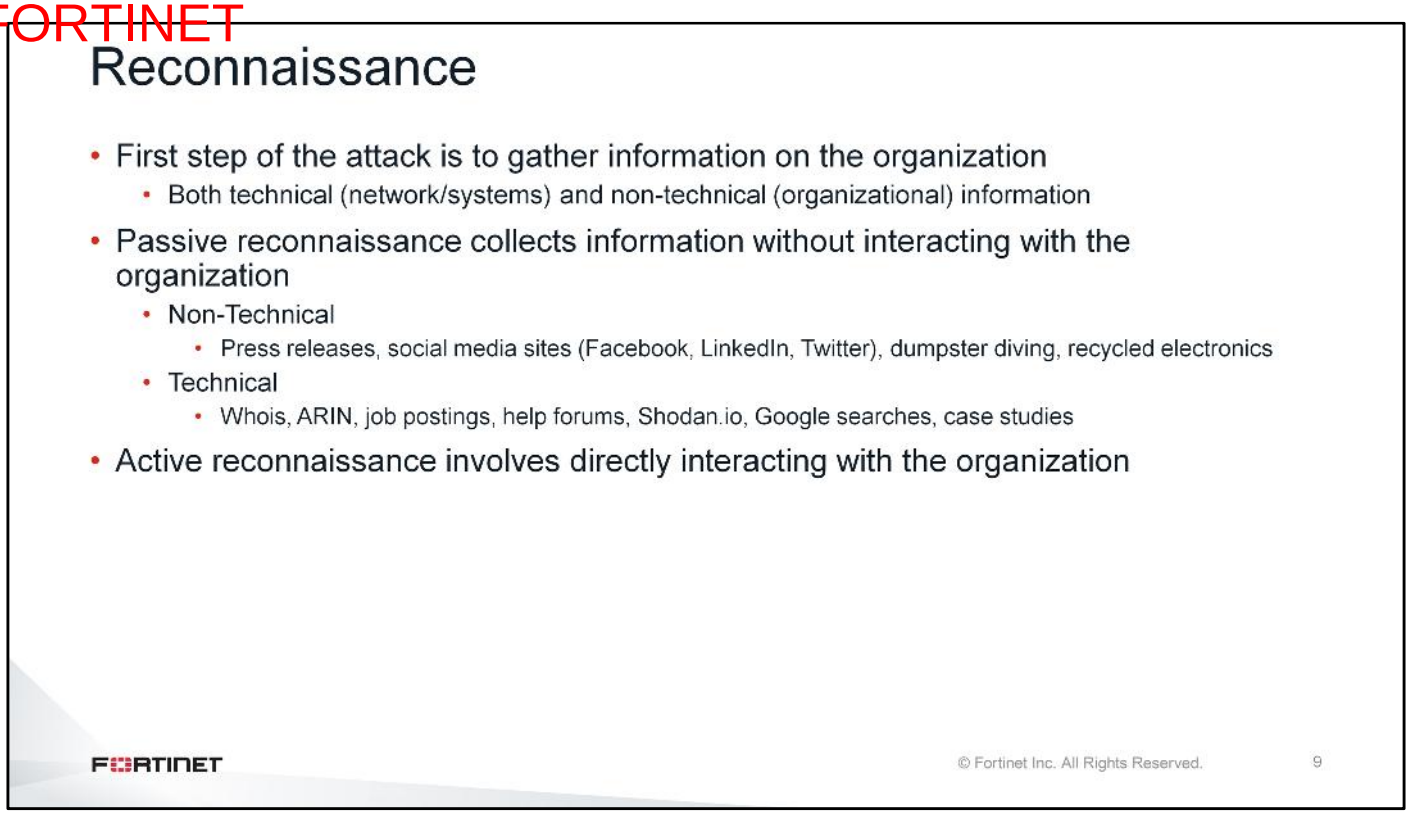
If a threat actor specifically targets your organization for something that it has or to disrupt one of its services, this type of attack is known as a targeted attack.

In this section, you will learn about the anatomy of an attack, which is also known as the kill chain.



The different stages that an attacker might go through in an effort to break into an organization's network, with the ultimate goal of data exfiltration, is also known as the kill chain. Knowing the stages of the kill chain can help identify methods of preventing attacks. The closer to the beginning of the kill chain that you can stop an attack, the less costly and time consuming the clean up will be.

There are many variations on the stages of an attack, but what's shown on this slide are the stages most commonly used. Once you understand the kill chain, then you can learn how to break it.

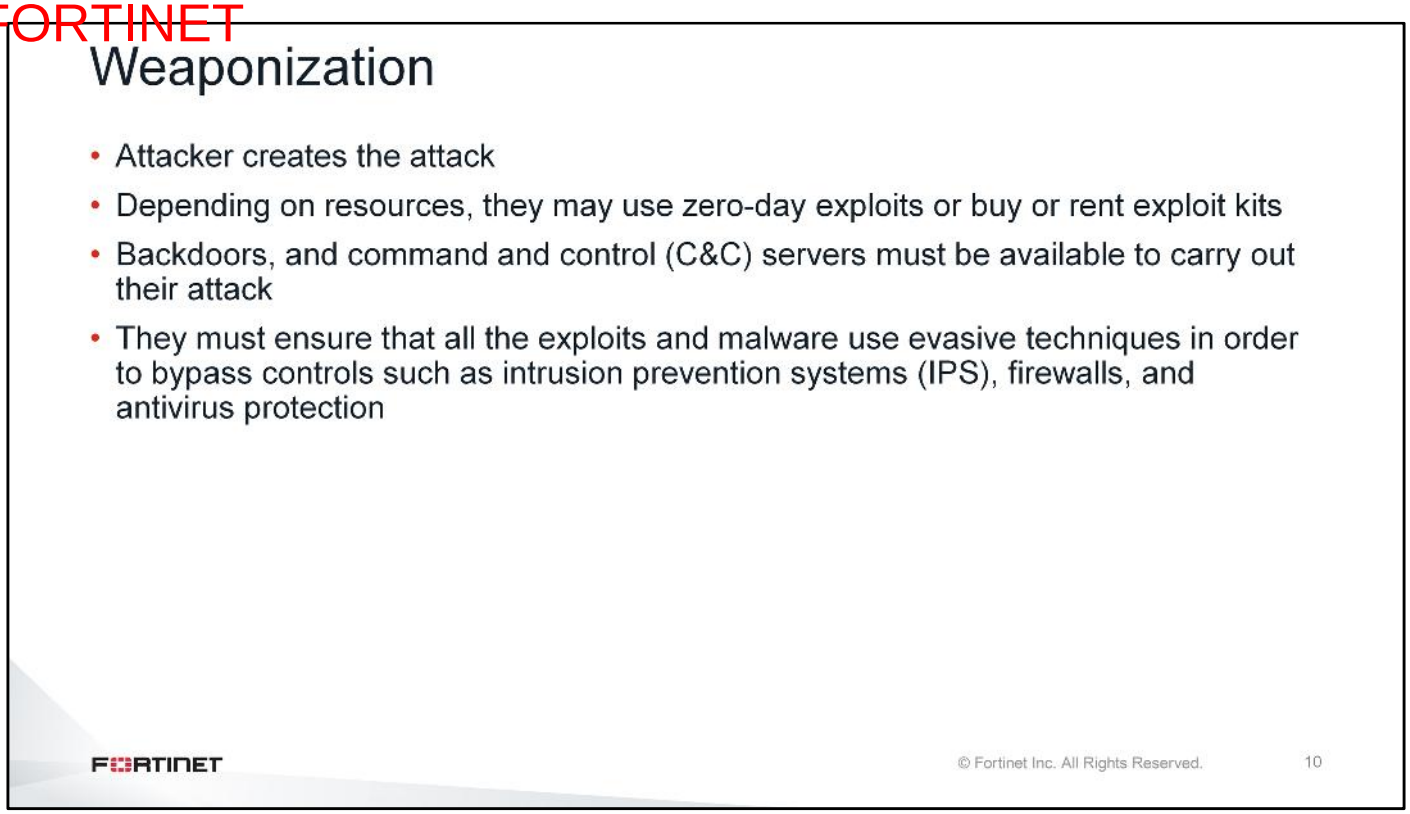


Once a threat actor establishes a target, the first step they will take is reconnaissance. Reconnaissance involves gathering information about the network and systems, as well as about the organization itself. The method of gathering information can be passive or active.

When doing passive non-technical reconnaissance, the threat actor uses public information, such as press releases and social media sites to find out information such as new executive appointments, events and tradeshows that the target organization is participating in, dumpster diving, and so on.

Passive technical reconnaissance involves using resources such as Whois, ARIN (for North American IP address blocks), RIPE NCC (for European IP address blocks) and APNIC (for Asian, Australian, and New Zealand IP address blocks). The threat actor can also browse the target organization's job postings, to find out the technical skills that the organization is looking for, or third-party help forums to see what systems the organization uses and the problems they are facing. Attackers can also find information in case studies on the organization that are published by third parties. For example, Microsoft published a case study on the organization Target, which outlined the solutions that Target used within their organization, in great detail.

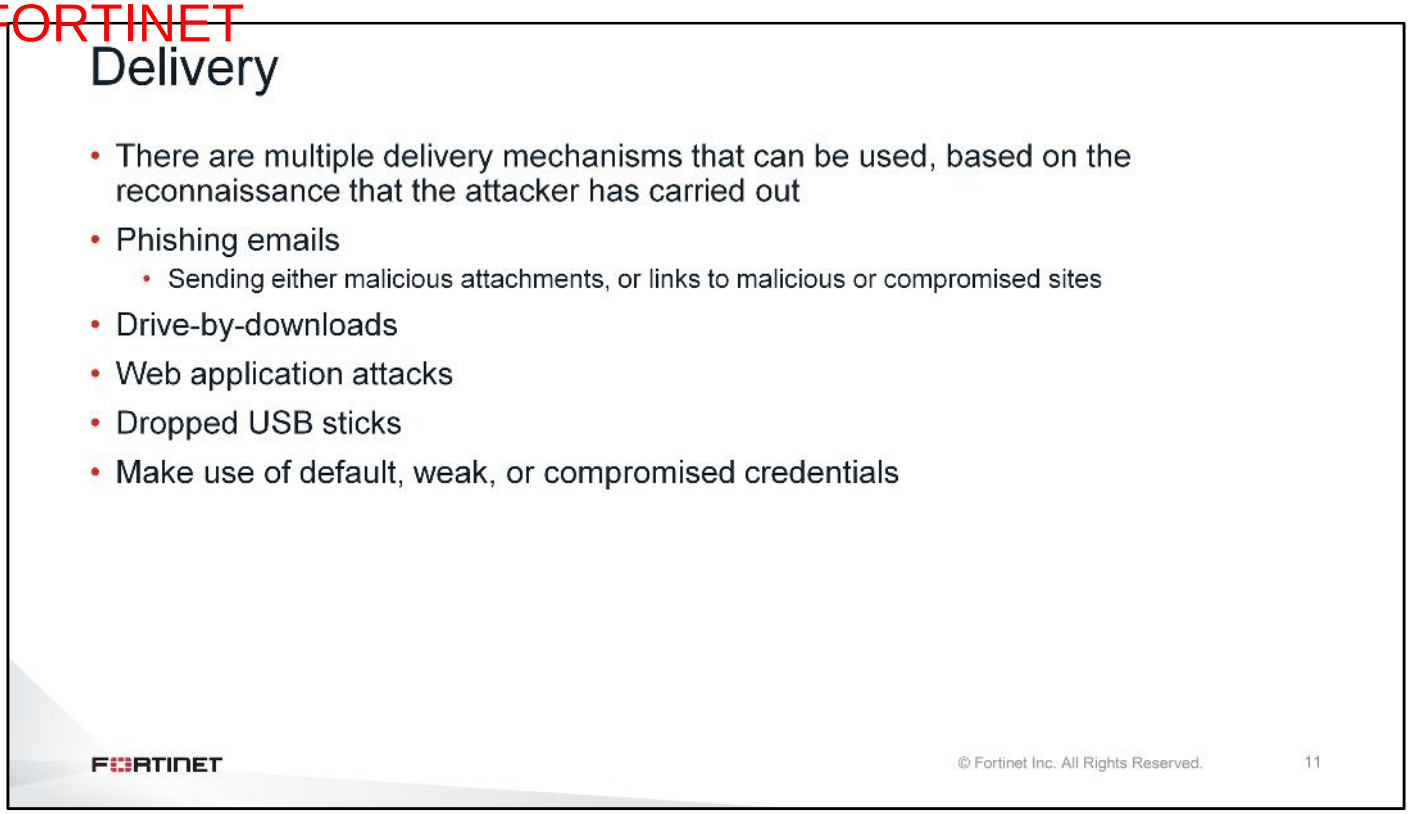
When doing active reconnaissance, the threat actor interacts directly with the organization and, therefore, may be detected. For example, once the threat actor finds the target organization's IP range using ARIN, they can use port scanners like nmap to find running services and the operating system types of Internet-facing servers. Specific protocols, such as HTTP, have banners that display information about the protocol and the computer system the protocol is running on. Attackers can use the information in the banners to gain information about an organization's computer systems. This is called banner grabbing. Once attackers identify the software and versions, they can then research vulnerabilities that the systems may be subject to if they are not properly patched. Telnet, nmap, and netcat are common tools used by attackers for banner grabbing.



Weaponization is the phase in which the attacker creates the attack based on information that they obtained in the reconnaissance stage. The more information the attacker uses, the more compelling a social engineering attack can be.

Attackers could use spear-phishing—a targeted phishing attack—to gain access to internal corporate resources, using the information they found on an employee's LinkedIn page. They could put a remote access trojan in a file that appears to contain crucial information about an upcoming event, in order to entice its recipient into running it. If they know what software the organization’s users or servers run, including operating system version and type, they have a good chance of being able to exploit and install something within the organization's network.

Depending on resources, attackers may use zero-day exploits that they discovered, purchased, or stole. Attackers can also buy or rent exploit kits that take advantage of known vulnerabilities. They also need to have additional tools ready to carry out the attack, like backdoors or C&C servers. They must ensure that all the exploits and malware being used have evasive techniques, in order to bypass controls such as firewalls, IPS, and antivirus scanners.



There are multiple delivery mechanisms that an attacker can use. Which one they use will be based on the reconnaissance they have carried out.

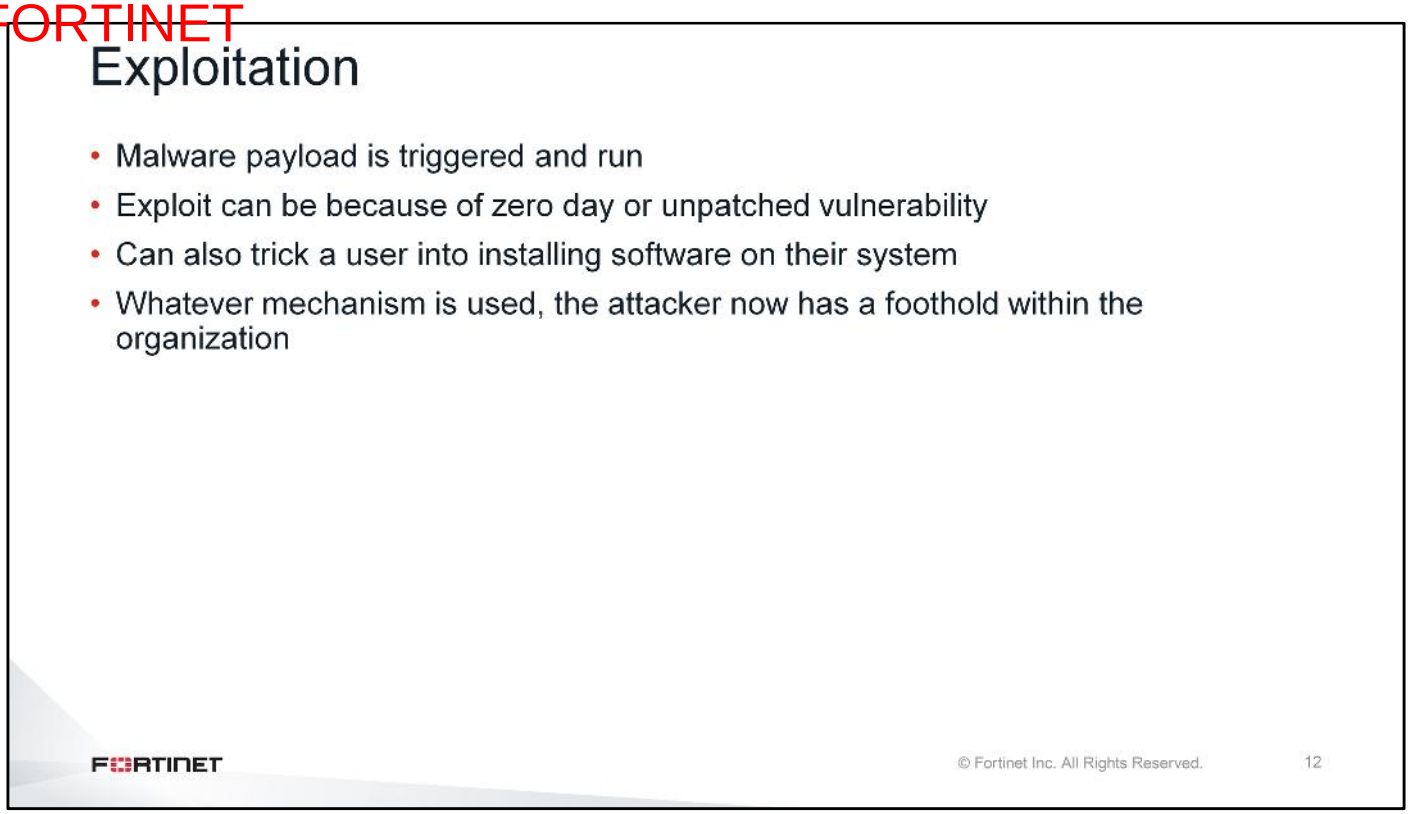
Phishing emails, as the name suggests, use the corporate email system to deliver specially crafted email to the users in the hopes that they will open the email and infect the system.

The drive-by-download method waits for users to access malicious or compromised web sites. The attacker guesses, or observes, which websites users visit frequently and infects one or more of them with malware. Eventually, a member of the targeted group becomes infected.

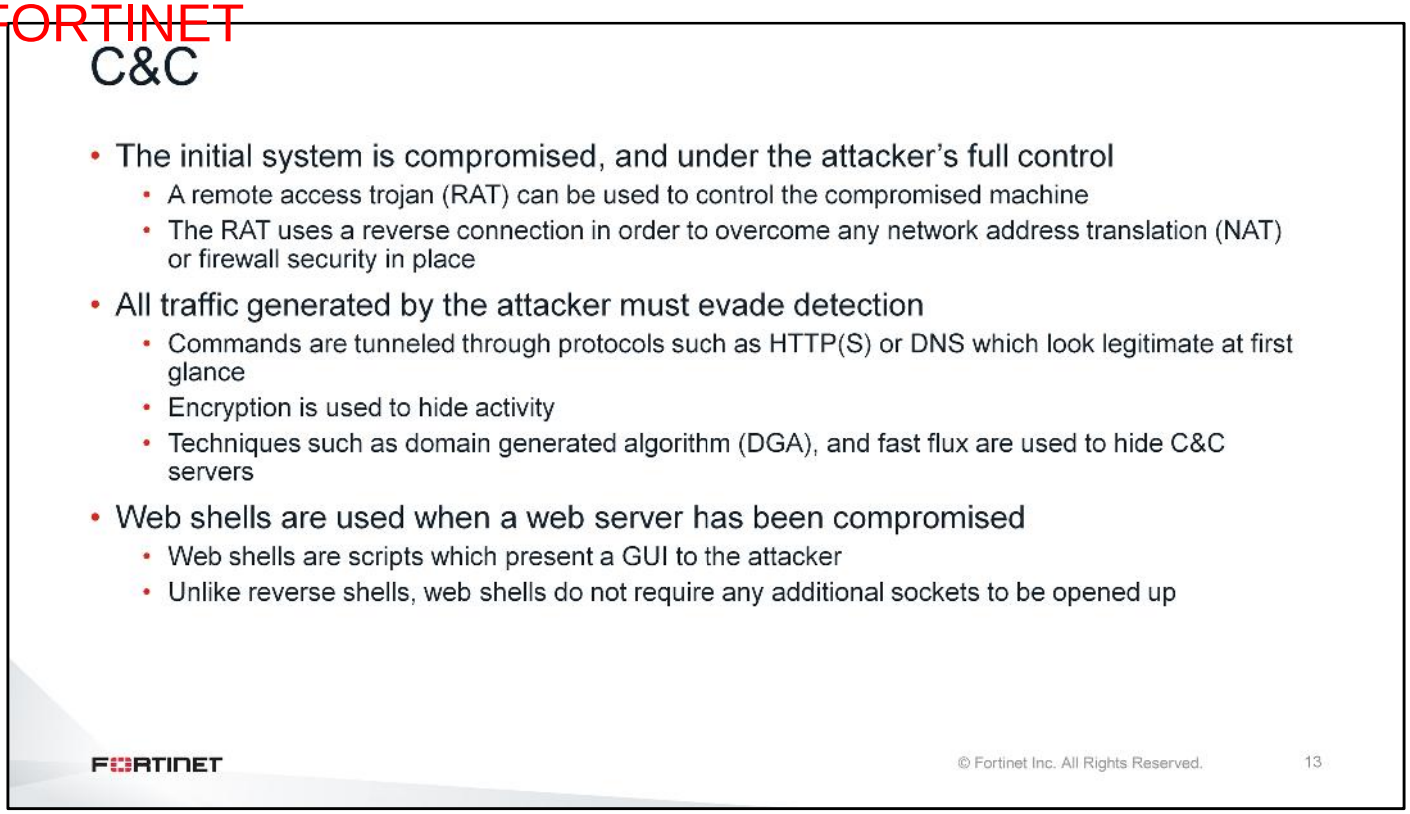
Web application attacks try to circumvent the business logic used by web applications and allow the attacker to gain access to the web server and underlying databases.

Sometimes an attacker will drop USB sticks in the lobby or parking lot of the target organization, in hopes that a user will pick one up and plug it into a computer on the corporate network.

Attackers will also make use of default, weak, or compromised credentials to gain access to the organization's network.



In the exploitation stage, the malware payload is triggered and run, and takes action on the targeted vulnerability. The attacker can exploit the system by taking advantage of zero-day or unpatched vulnerabilities, or by tricking a user into installing software on their computer. Whatever mechanism they use, the attacker can now get into the system, install additional tools, and create new script files for malicious purposes.

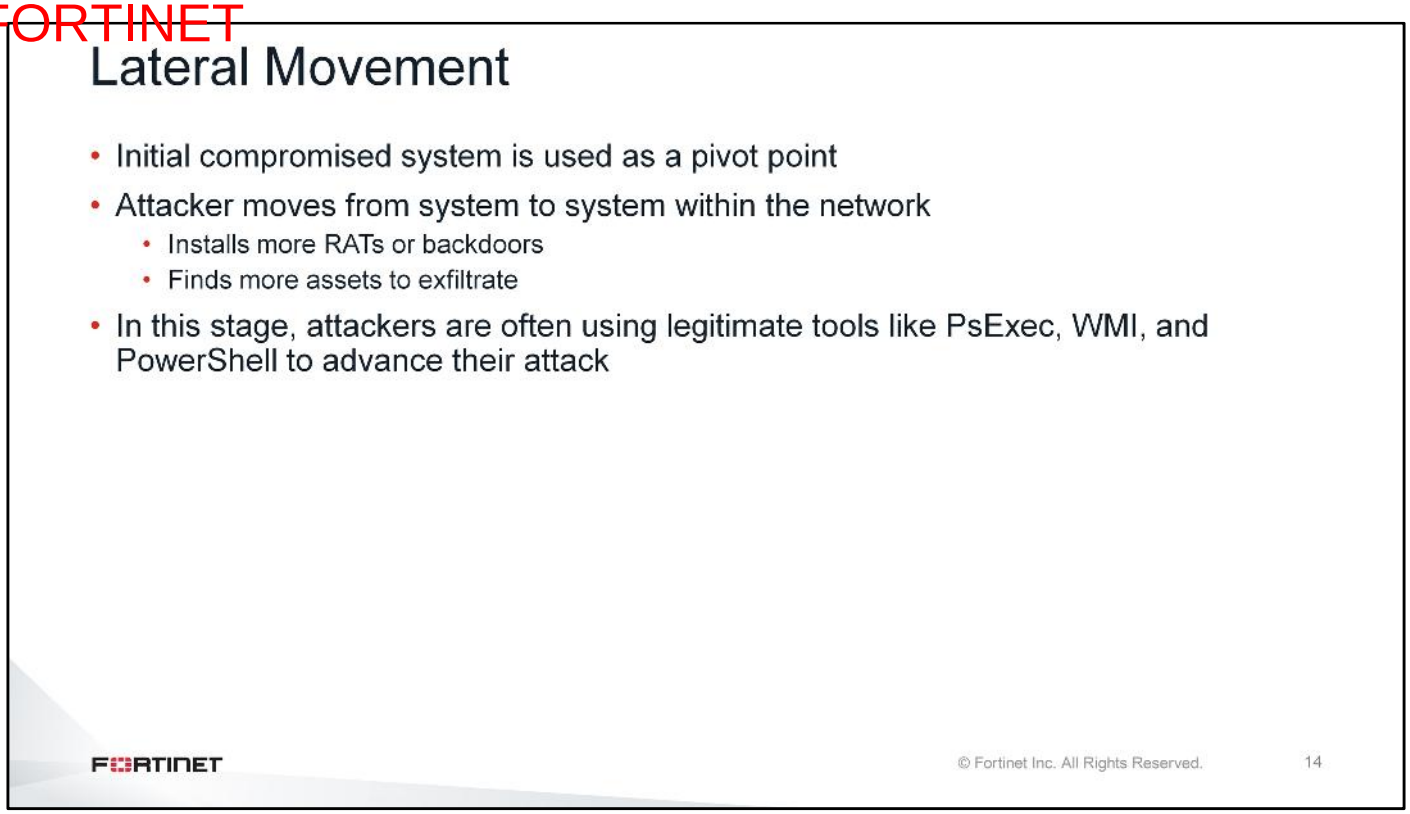


Once the attacker exploits the system, they drop post-exploitation tools in order to control the system and advance the attack. Most of the time, the information the attacker is looking for is not on the initially compromised system. The attacker can use a RAT, which makes a reverse connection to a server that the attacker controls. The RAT uses a reverse connection in order to overcome any NAT or firewall security in place.

Any traffic generated by the attacker must evade detection. Attackers can tunnel commands through protocols such as HTTP(S) or DNS, which look legitimate at first glance. Attackers typically use encryption in order to hide their activity.

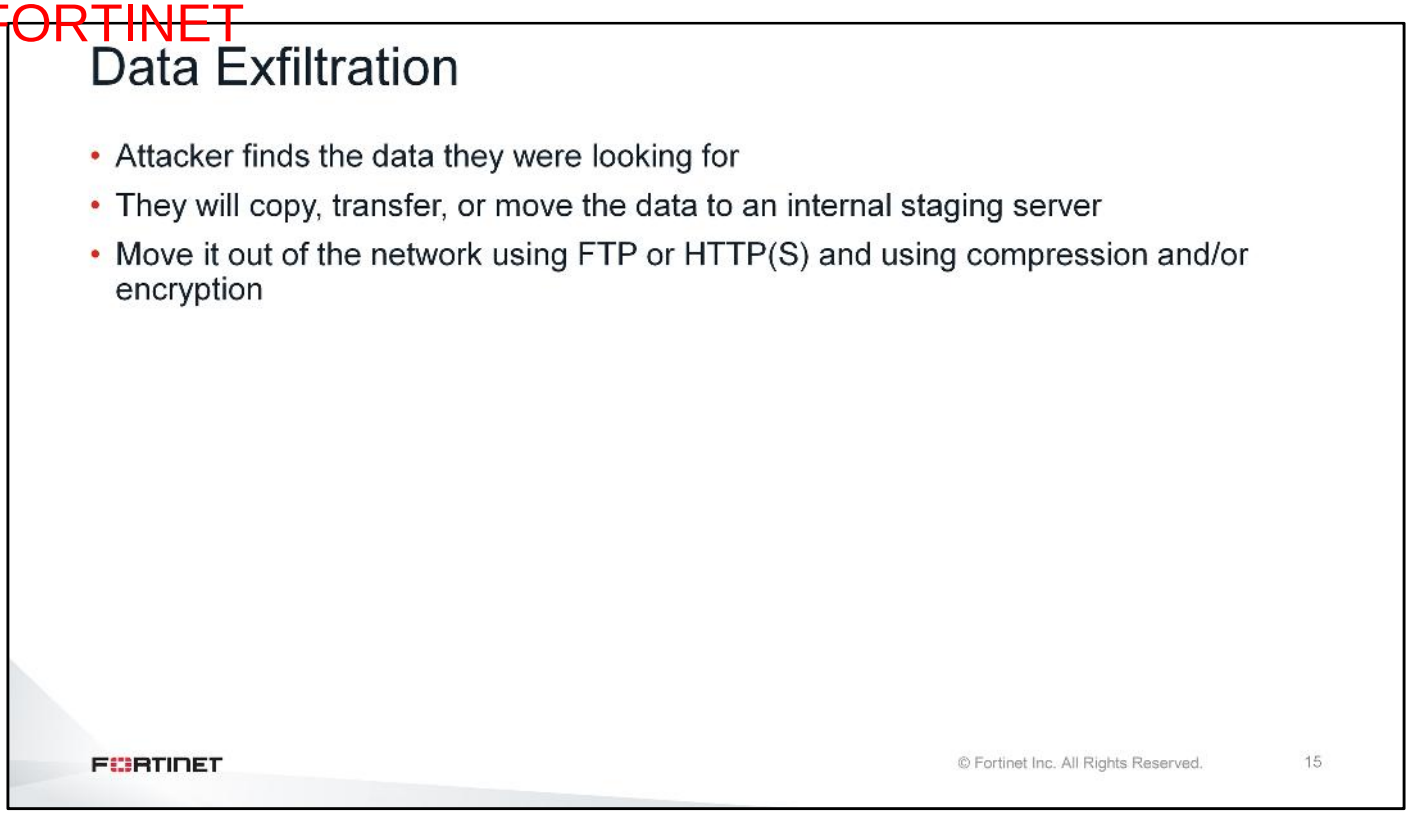
Attackers can use more sophisticated evasion techniques, such as DGA or fast-flux. DGA is used to periodically generate a large number of domain names that are used as rendezvous points for the C&C servers. Fast flux is a DNS technique, where a single domain is associated with numerous IP addresses. The IP addresses are swapped in and out frequently, through changing DNS records.

Attackers can use web shells to take advantage of compromised web servers. Web shells are used by system administrators, and have a wide range of tools to perform management tasks on the server. An attacker can use a web shell to copy entire databases, or use the compromised web server as a pivot point for lateral movement.

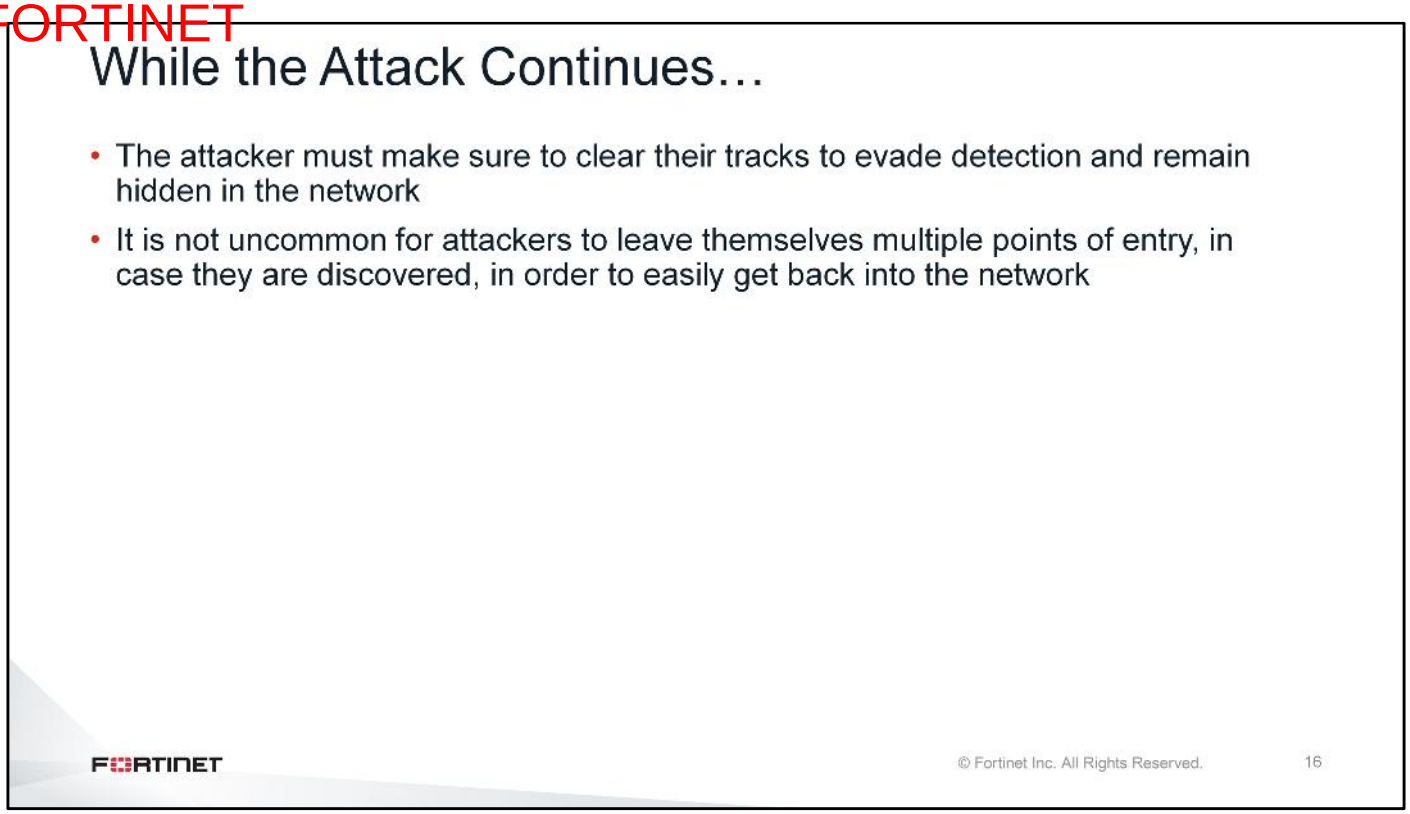


The first system that the attacker compromises, may not have the information that they are looking for. So, they must search for it. During this search, the attacker maps out the internal network and moves laterally through the organization using the compromised machine as a pivot point. As the attacker moves from system to system within the network, they may install more RATs or backdoors on those systems.

At this stage, attackers are often using legitimate tools like PsExec, Windows Management Instrumentation (WMI), and PowerShell. These are tools used for management purposes in a network. These are expected to be seen in a corporate environment and, therefore, would not raise any red flags.



When the attacker discovers the data they are looking for, they will save it to an internal staging server and then move it out of the network to a system that they control. At this point, they can do whatever they want with this data—ransom it, auction it off, or just release it to the public for defamation.

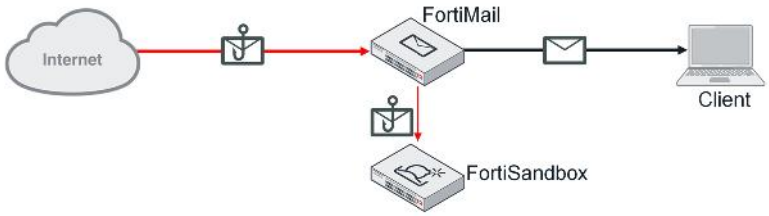


While they carry out the attack, the attacker must make sure to clear their tracks in order to evade detection and remain hidden on the network. It is not uncommon for attackers to leave themselves multiple points of entry, so that they can easily get back into the network, if they are discovered.

In this section, you will learn how to use the different components of the ATP solution to break the kill chain. Advanced threats are the main point of interest. While FortiGate can play a role in helping discover reconnaissance activity, such as remote scanning, this will not be discussed here. Instead, you will focus on how to detect threats that want to evade detection.

Breaking the Kill Chain—Delivery

- Attack Vector: email attachments
  - Advanced threats can evade antispam, and antivirus scanning
  - Solution: integrate FortiMail with FortiSandbox to address unknown malicious email attachments



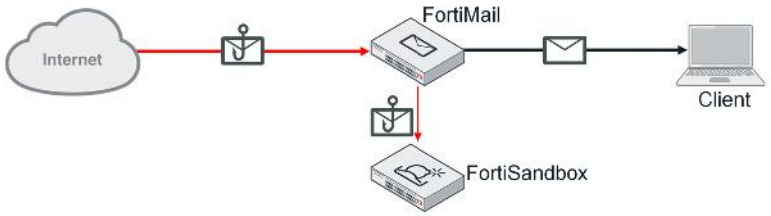
- FortiMail receives an email with an attachment bound for an internal user
- FortiMail sends the attachment to FortiSandbox for analysis
- FortiSandbox opens the attachment and analyzes its behaviors
- FortiSandbox sends the results of the analysis back to FortiMail
- FortiMail, based on result and policy configuration, applies action to email

 18

One of the most common attack vectors is phishing emails containing malicious attachments or malicious URL links. Advanced threats are able to evade traditional spam and antivirus scanning engines. Using the ATP solution, FortiMail is able to send suspicious attachments to FortiSandbox for analysis. After analyzing the file, FortiSandbox sends the results back to FortiMail, which then takes action.

Breaking the Kill Chain—Delivery

- Attack Vector: Email URL links
  - Advanced threats can evade URL filtering
  - Solution: integrate FortiMail with FortiSandbox to inspect URLs



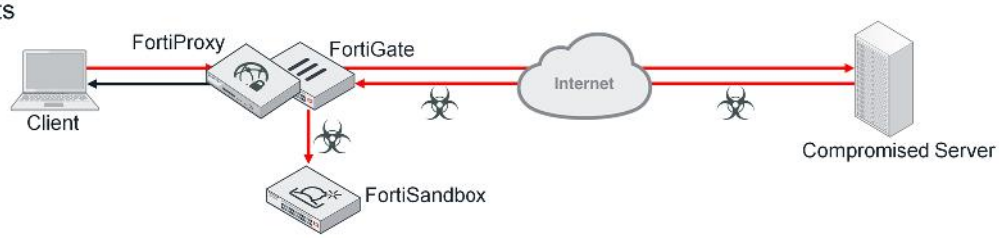
- FortiMail receives an email with embedded URL(s) bound for an internal user
- FortiMail extracts the URL(s) and sends them to FortiSandbox for analysis
- FortiSandbox requests URL(s) to see where it leads and examines the downloaded files, then runs any downloaded files to identify their behavior
- After analysis, FortiSandbox sends the result of the analysis back to FortiMail
- FortiMail, based on result and policy configuration, applies action to email

 19

Another common method of delivery is email containing malicious URLs. In this scenario, an email body contains a malicious embedded URL, which is able to bypass traditional security measures. FortiMail can forward URLs like these to FortiSandbox. FortiSandbox accesses the URL and analyses the response to identify whether it is linked to anything suspicious, and reports back to FortiMail with a verdict.

Breaking the Kill Chain—Delivery

- Attack Vector: web browsing
  - Advanced threats can evade IPS, web filtering, and antivirus scanning
  - Solution: integrate FortiGate or FortiProxy with FortiSandbox to detect downloading of malicious objects



  - User accesses a malicious or compromised web site where malicious scripts try to exploit their browser and download malware
  - At download time, FortiGate or FortiProxy sends the sample to FortiSandbox for analysis
  - FortiSandbox sends the results back to FortiGate or FortiProxy, which, based on scan policy, can detect and block any future access to the malicious object

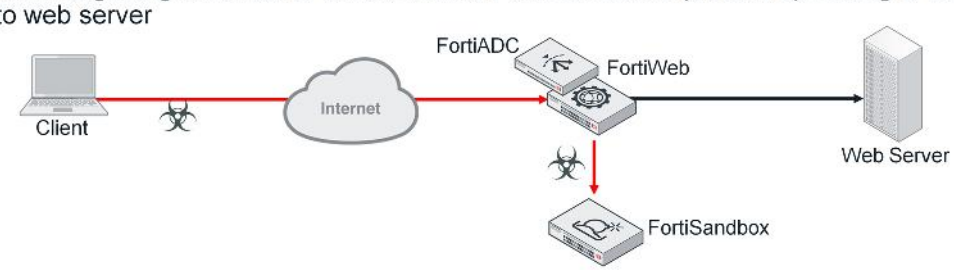
FORTINET

20

Drive-by-downloads are another popular delivery mechanism. In a drive-by-download, users are infected after visiting a malicious website or a website that has been compromised to serve malicious content. The website delivers payloads to exploit the browser, which then leads to malware being downloaded. FortiGate or FortiProxy is able to send the downloaded files to FortiSandbox for analysis.

Breaking the Kill Chain—Delivery

- Attack Vector: web application attacks
  - Advanced threats can be uploaded to a poorly written or compromised website
  - Solution: integrating FortiWeb or FortiADC with FortiSandbox to prevent uploading of malicious files to web server



- Web server allows or has been compromised to allow uploading of files
- Attacker uploads file to web server
- FortiWeb or FortiADC sends the file to FortiSandbox for analysis
- FortiSandbox opens the file and analyzes its behaviors
- FortiSandbox sends the results back to FortiWeb or FortiADC

 21

Web applications, such as HR systems, sometimes allow for the uploading of files. This feature can be exploited by attackers to compromise these web servers. Whether it's because of poorly written code, or misconfigurations on the web servers, attackers can upload malicious files, like web shells, and gain complete management access to the server.

You can use FortiWeb or FortiADC to monitor for web server file uploads and send such files to FortiSandbox for analysis.

Breaking the Kill Chain—Delivery

- Attack vector: USB drives
  - Advanced threats may reside on USB drives which users may insert into their computers
  - Solution: integrating FortiClient with FortiSandbox

- User inserts into their computer a USB drive, which contains malware
- Before allowing access, FortClient sends files to FortiSandbox for analysis
- FortiSandbox opens each file and analyzes its behaviors
- FortiSandbox sends results back to FortiClient
- FortiClient quarantines any files it finds suspicious

FORTINET

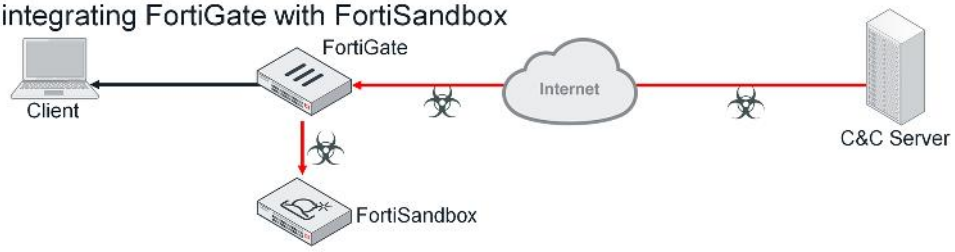
22

USB drives are another potential source of malware. In some attacks, the attackers leave USB drives containing malware in public places, such as office lobbies and parking lots, with the hopes that an employee will pick it up and insert it into their computer.

This type of delivery can be counteracted using FortiClient integrated with FortiSandbox. When a USB is attached to a host protected with FortiClient, FortiClient can send the files on the USB drive to FortiSandbox for analysis, before allowing the user access to the files.

Breaking the Kill Chain—C&C

- After the host is compromised, additional tools are downloaded and updated over time
  (This slide focuses on the malware that has been packaged to evade detection)
- Solution: integrating FortiGate with FortiSandbox



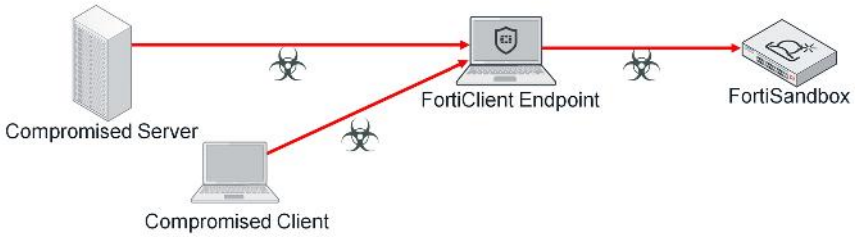
- C&C software running on compromised host makes call outs to a server, which the attacker controls
- When additional tools are downloaded, they are sent by FortiGate to FortiSandbox for analysis
- FortiSandbox opens the files and analyzes the behaviors
- FortiSandbox sends the results of the analysis back to FortiGate to take action on the result

 23

After a host is compromised, attackers download additional tools to further their attack. For example, banking malware often downloads keyloggers to steal user credentials. Since communication with a compromised host is ongoing, FortiGate can monitor the network traffic for any additional or updated malware coming into the organization. FortiGate sends any new files being downloaded to FortiSandbox to identify whether they are malicious.

Breaking the Kill Chain—Lateral Movement

- As the attack propagates into the network, internal hosts are targeted
- Solution: integrating FortiClient with FortiSandbox (hosts on same or different network)



- The compromised host tries to exploit and drop malware on additional hosts in the network
- Target host's FortiClient sends files to FortiSandbox for analysis
- FortiSandbox opens the files and analyzes their behaviors
- FortiSandbox analyzes the file and sends results back to FortiClient to take action

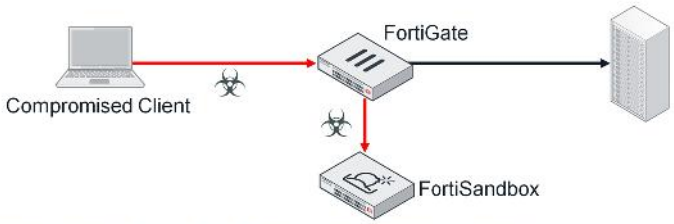
FORTINET

24

During the lateral movement stage, the attacker is trying to compromise and infect other computers in the network. If these computers are protected with FortiClient, FortiClient can send any file that the computer downloads, to FortiSandbox for analysis. If FortiSandbox finds the file to be suspicious, FortiClient can take action and quarantine the file.

Breaking the Kill Chain—Lateral Movement

- As the attack propagates into the network, eventually data center hosts are targeted
- Solution: integrating internal segmentation firewall (ISFW) FortiGate with FortiSandbox



- FortiGate sends the files to FortiSandbox for analysis
- FortiSandbox opens the files and analyzes their behaviors
- FortiSandbox sends the result back to FortiGate which can then take action on the results

FORTINET

25

If the attacker is looking for sensitive data, at some point they will try to target hosts in the data center. Normally, these hosts are in a different subnet than the first compromised host. In this case, if you deploy FortiGate as an ISFW firewall, FortiGate can analyze the traffic moving across subnets and send any files to FortiSandbox for analysis to prevent propagation.

Breaking the Kill Chain—Summary

- Delivery

Delivery Methods	Solution
Email attachments	FortiMail and FortiSandbox
Email URL links	FortiMail and FortiSandbox
Web browsing (drive-by downloads)	FortiGate/FortiProxy and FortiSandbox
Web application attacks	FortiWeb/FortiADC and FortiSandbox
Out of band (USB)	FortiClient and FortiSandbox

- Command and Control

Command and Control	Solution
Additional malware is downloaded (keyloggers, and so on)	FortiGate/FortiProxy and FortiSandbox FortiClient and FortiSandbox

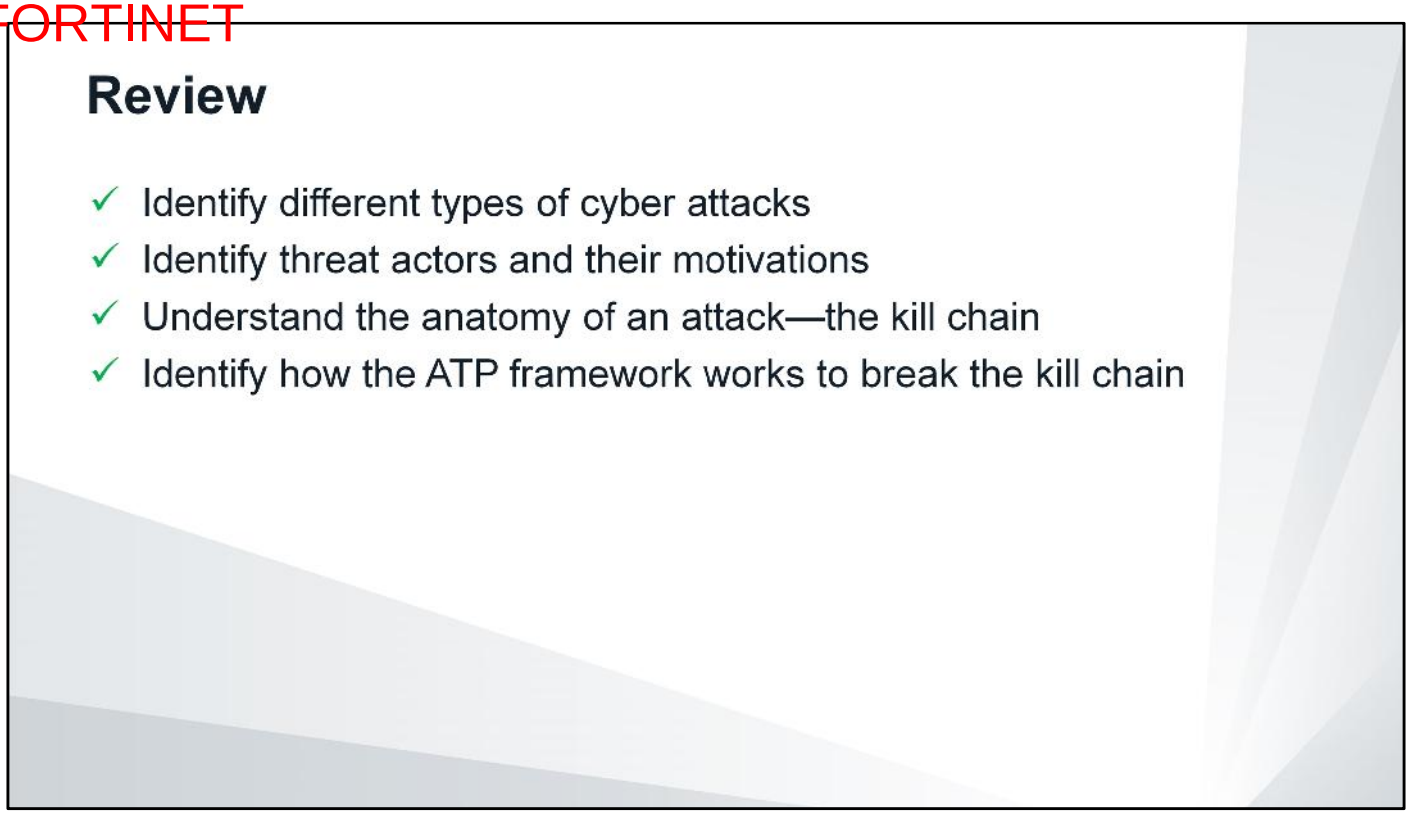
- Lateral Movement

Lateral Movement	Solution
Additional hosts are targeted	FortiGate/FortiProxy and FortiSandbox FortiClient and FortiSandbox

FORTINET

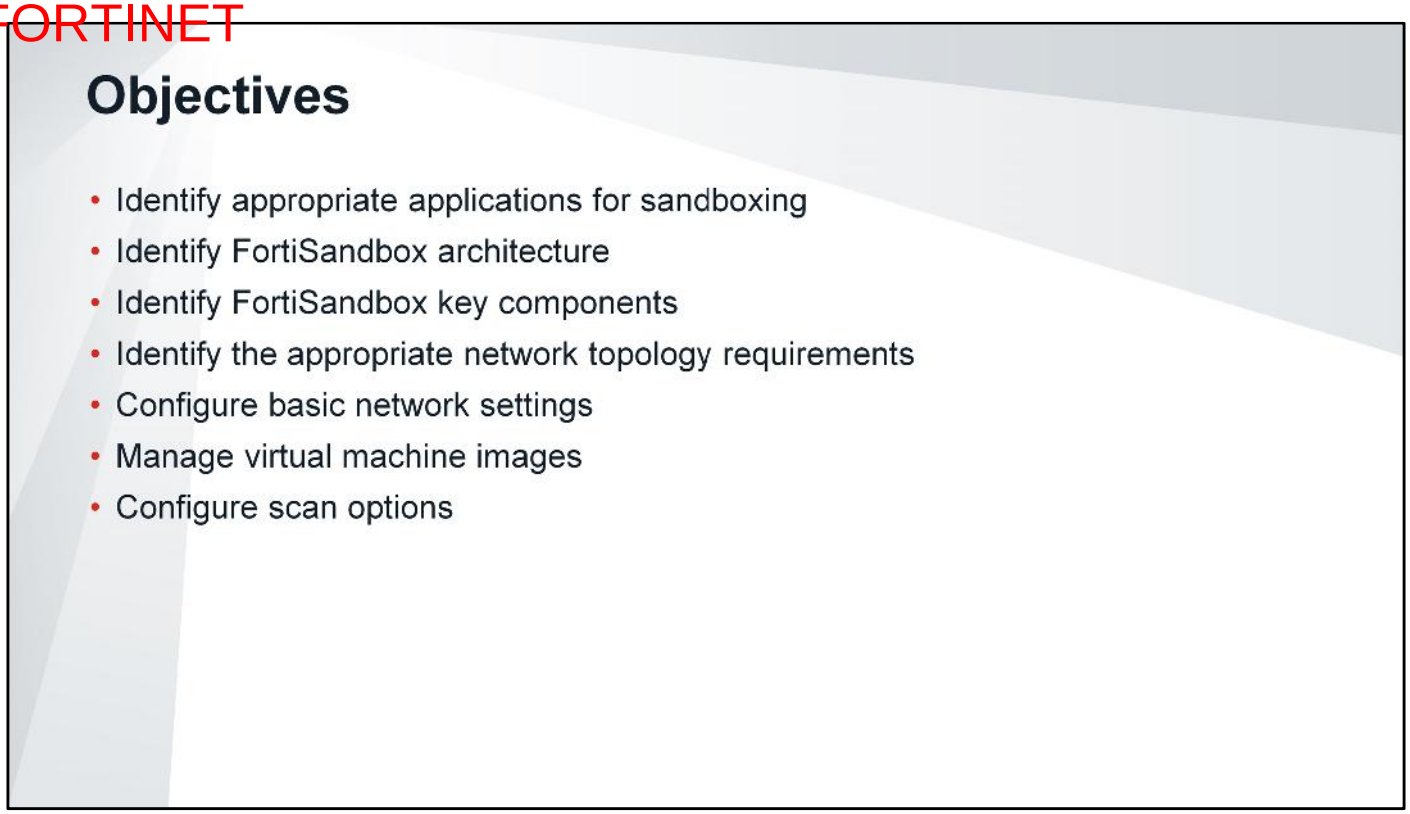
26

This slide shows a summary of the kill chain stages that can be blocked using specific ATP components.



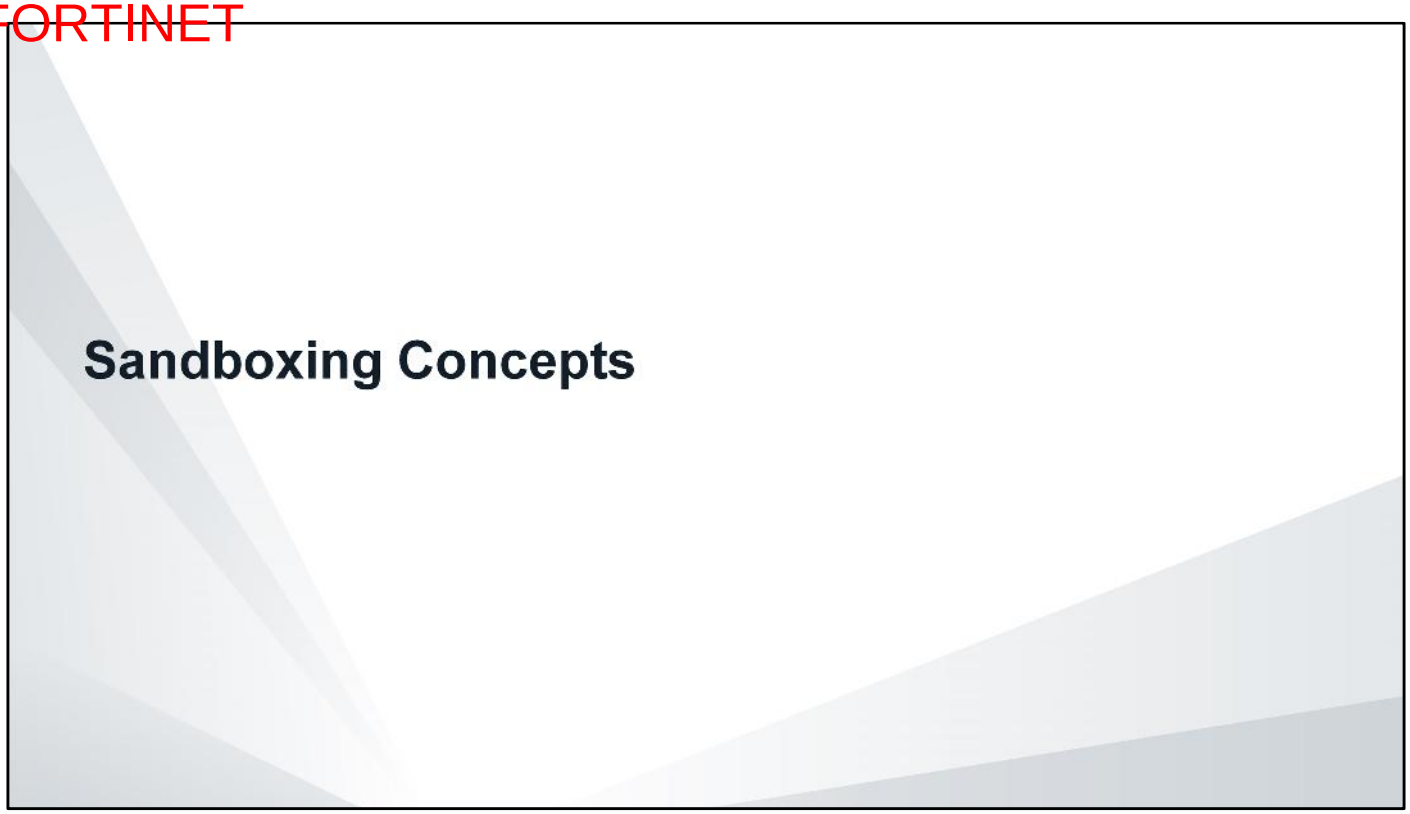
This slide shows the objectives that you covered in this lesson.

In this lesson, you will learn the appropriate applications for sandboxing. You will also learn basic FortiSandbox concepts, including an overview of the architecture, key components, supported input methods, and networking requirements. As well, you will learn the basic configuration requirements to deploy a FortiSandbox in your network.



After completing this lesson, you should be able to perform the objectives shown on this slide.

By demonstrating competence in basic FortiSandbox concepts and configuration requirements, you will be able to design, configure, and maintain a FortiSandbox deployment in your own network, that is suitable for your security needs.



In this section, you will learn the appropriate applications for sandboxing. You will also learn the basic concepts of FortiSandbox, which include the architecture, key components, and input methods.

Why use a sandbox?

- Traditional virus detection relies on pattern matching
  - Can't effectively protect against new viruses
- Heuristics can identify virus-like attributes
  - Better chance of identifying new variants of viruses
  - Based on probability; can cause false-positive detection
- Code emulation can detect viruses with much more certainty
  - Full execution is rarely done
  - Real-time systems have more constraints: RAM, session volume, packet buffers, and so on
- Full code execution requires an isolated and protected environment
  - Suspicious files can be fully executed
  - Each aspect of the file's behavior can be observed

FORTINET

4

Traditional virus detection relies heavily on pattern matching. Some vendors use patterns that detect one virus per pattern, while others use patterns that are more flexible, and can catch multiple viruses with a single pattern. It varies by the vendor's engine. Because signatures require an exact match, they don't provide much protection against new viruses–ones where no signature exists yet.

Heuristics can identify virus-like attributes, but they are based on probability. This can increase the possibility of false positive detection.

Some network virus scanners can do some runtime code execution. Full execution is generally not done by a network virus scanner due to system resource constraints.

Full code execution requires a separate, protected environment where suspicious files can be fully executed, and every aspect of the file's behavior can be observed. This requires system resources and time that's not normally available on a network device. In other words, it requires a sandbox.

FortiSandbox Architecture

- The FortiSandbox host has FortiGuard engines and packages, including the extreme database for the FortiGuard antivirus
- The VM host is based on a modified hypervisor
  - Various OS support for virtual machines (VMs)
    - Windows 7, Windows 8.1, Windows 10, MAC OS, and Android
    - Windows XP only supported in a custom VM
- License keys are activated in the master VM
- The master VM contains the main image, plus a snapshot
  - The snapshot is taken in a running state, so each clone does not need to wait for system initialization
- As files are accepted for sandboxing, the master VM is cloned
  - Files are executed in the cloned VM
  - After terminating the execution of a sample, the cloned VM reverts to the snapshots

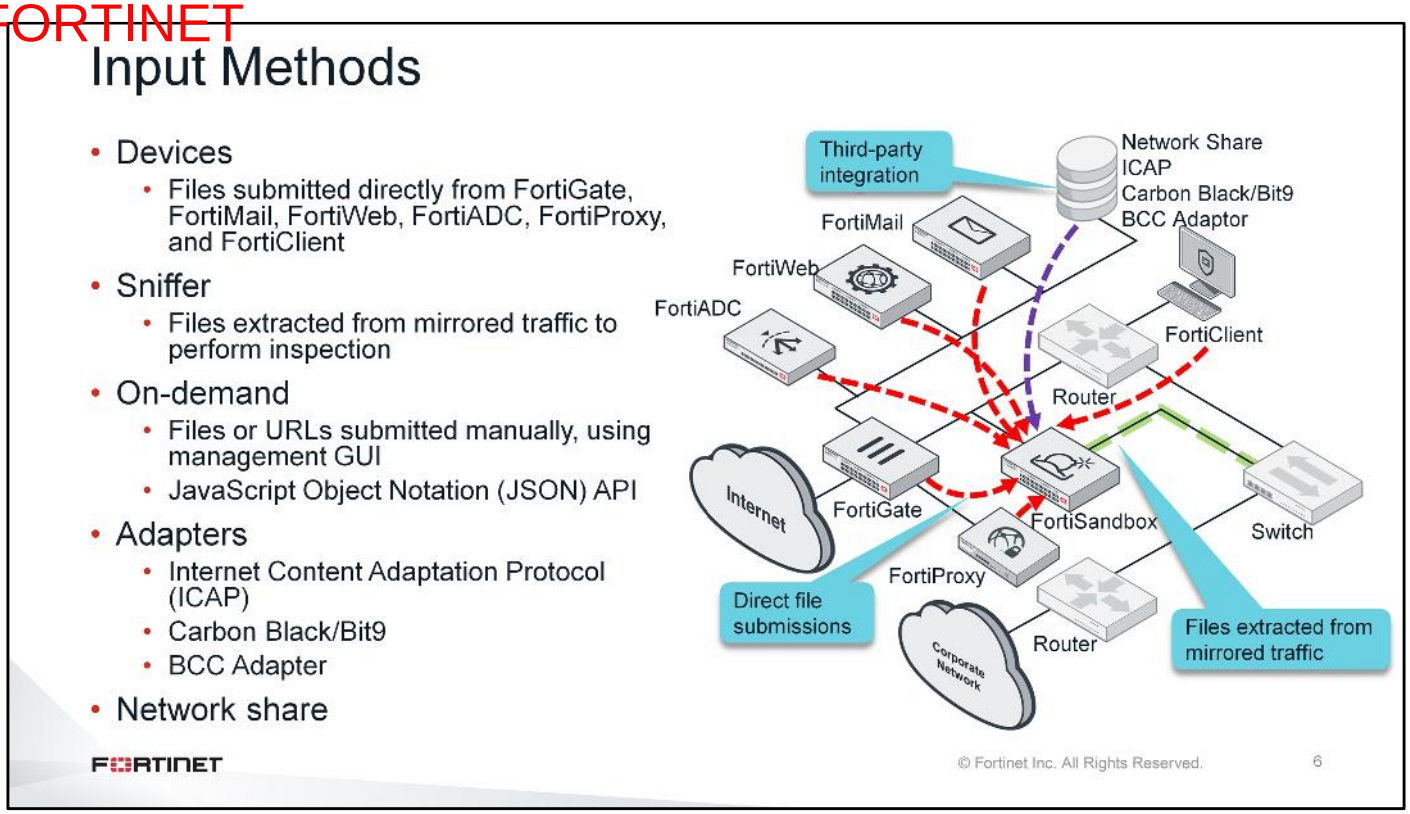
FORTINET

5

The FortiSandbox OS has FortiGuard engines and packages, including the extreme database for FortiGuard antivirus. The VM host is based on a modified hypervisor that natively supports Windows 8, Windows 8.1, Windows 10, MAC OS, and Android. You can also install custom VM images to support other operating systems, such as Windows XP. You must have the appropriate license keys for each VM image you want to maintain.

The master VM is the original VM image in which the Windows license key is activated. FortiSandbox creates a snapshot, so the master VM contains the main image plus a snapshot. The snapshot is taken in a running state, in order to achieve a faster startup for each clone.

As files are accepted for sandboxing, the master VM is cloned. Each new VM is set up so that after terminating the execution of a sample, it reverts to the snapshots. This set up eliminates the risk of system infection, because each sample runs in a clean environment, that is started from the snapshot.



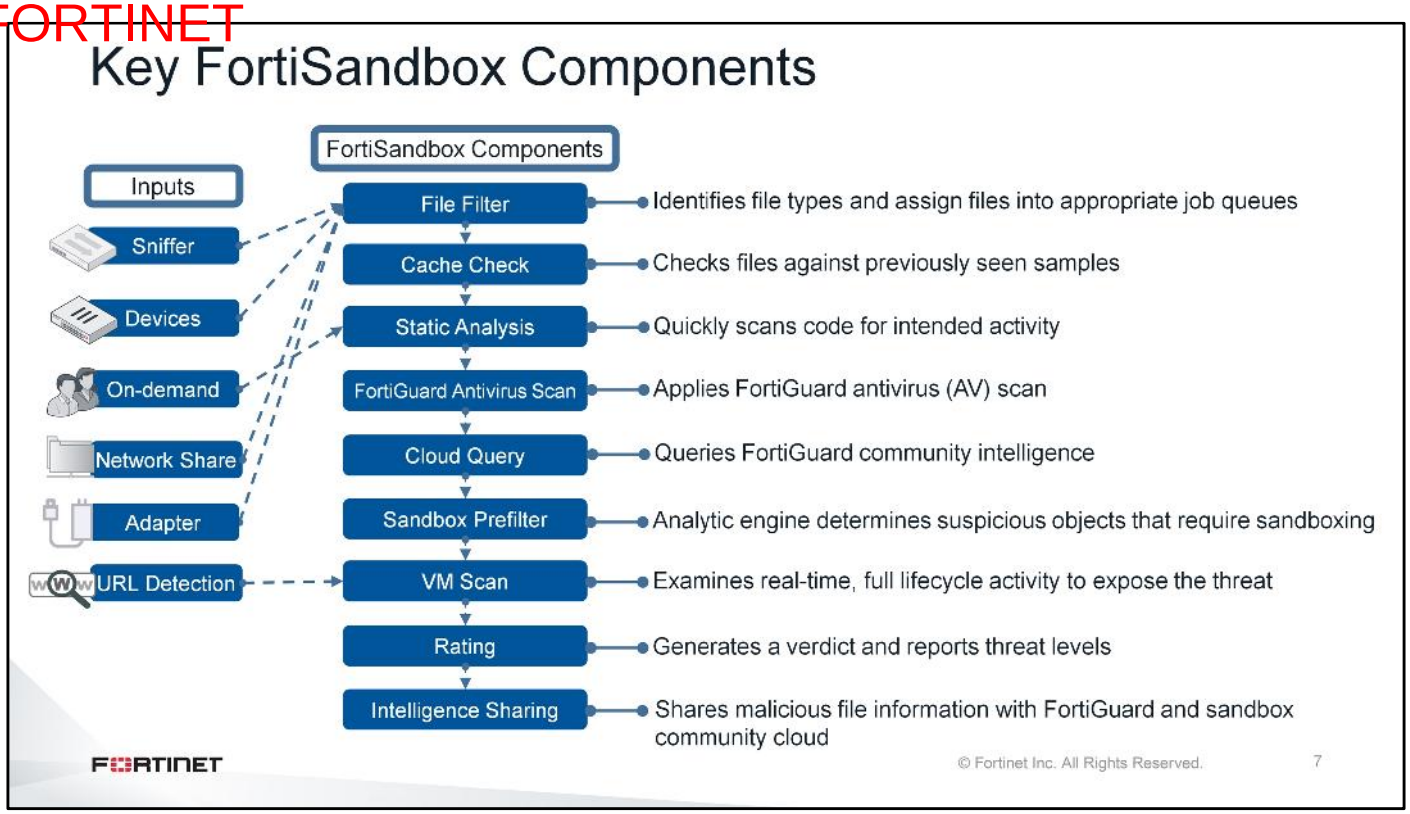
A FortiSandbox is capable of scanning files from different sources. The input methods are not a mode of operation for the device. They are simply methods of receiving files that can be used concurrently, or in any combination.

The most common method of deploying FortiSandbox is integrated with another Fortinet device. In this deployment, the devices submit files directly to FortiSandbox. FortiSandbox can accept input from FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy, and FortiClient.

When FortiSandbox is deployed in a network that does not have other supported Fortinet appliances, you can use sniffer input to inspect files. In this deployment, you must use port-mirroring or a network tap device to send a copy of all the traffic you want to inspect, to FortiSandbox. FortiSandbox will extract files from that mirrored traffic for inspection. Keep in mind that, if you want to inspect encrypted traffic, it should be decrypted before being mirrored to the FortiSandbox.

You can manually submit files and URLs on-demand, using the FortiSandbox management GUI, or using JSON API. JSON API can automate the process of uploading samples and downloading actionable malware indicators.

Advanced threat protection (ATP) is the concept of detecting new threats as early as possible. The ideal sandboxing solution must check all samples collected from all locations. FortiSandbox is an open solution that can be configured to integrate with most third-party devices. FortiSandbox can act as an ICAP server, to accept inputs from ICAP-enabled clients, as well as accept files from a Carbon Black/Bit9 server. If none of these methods are supported, the third-party device can post files to a network share, which can be monitored and scanned by FortiSandbox. You can submit emails from an upstream MTA server to FortiSandbox using a BCC adapter. FortiSandbox will extract attachment files and URLs in an email body.

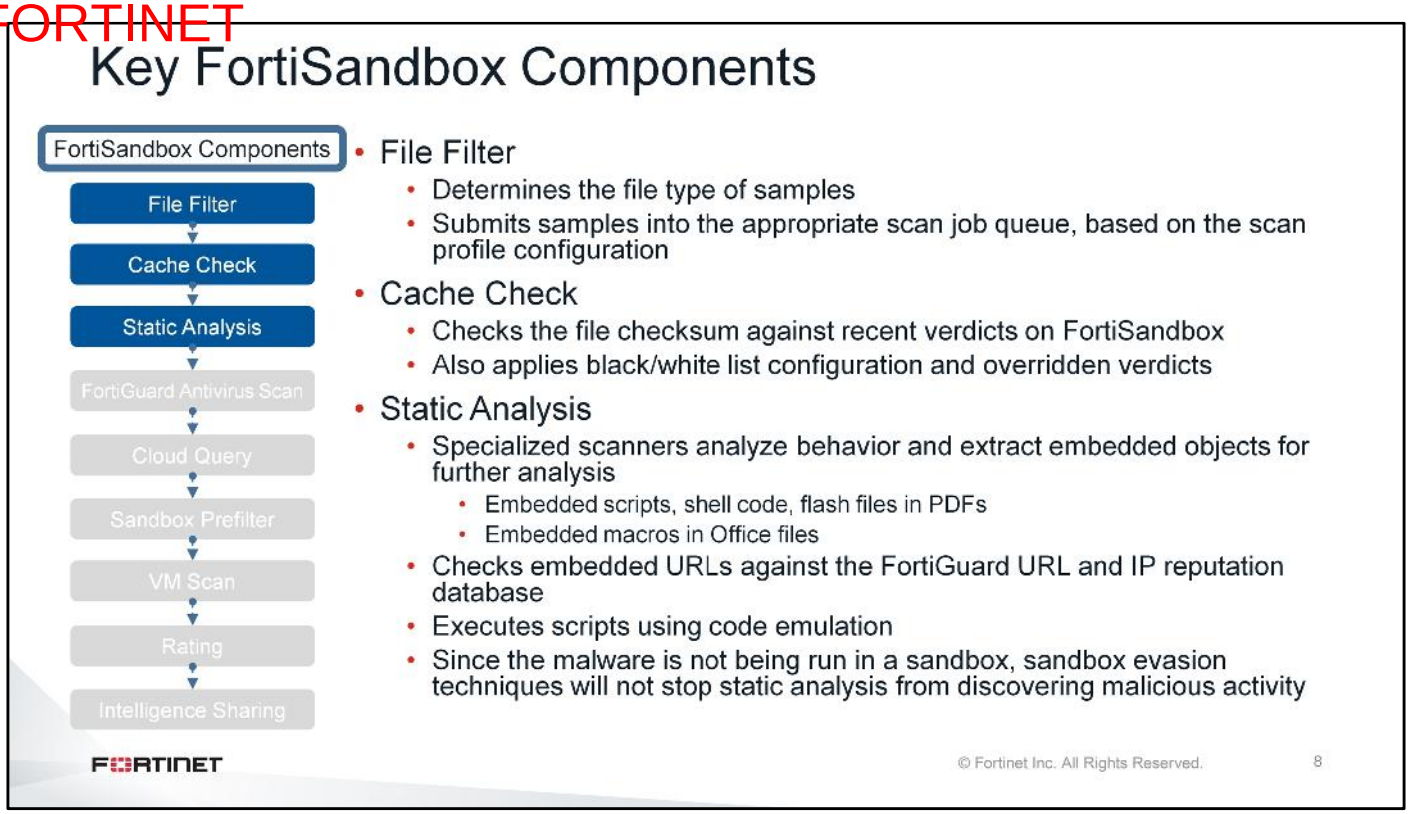


FortiSandbox can receive samples from several different input methods. It analyses the samples using a filtering approach, to assess the sample's behavior and rate the risk of potential malicious behavior.

Input from sniffer, devices, and network share is submitted to the file filter, which is the first component of FortiSandbox inspections. A file may have to be processed through every inspection component, before FortiSandbox can generate a verdict for it. This is usually the case for zero-day malware, which is typically detected by the VM scan engine before a verdict is generated.

Certain samples may be caught by the cache check or AV scan, depending on how long the malware has been active. This inspection approach allows FortiSandbox to filter out files that can be easily detected using other methods of inspection. Using this approach reduces the number of files that need to be submitted to the VM scan engine for sandboxing. The only exception to this, are URL inputs. These inputs are submitted directly to the VM scan engine for sandboxing.

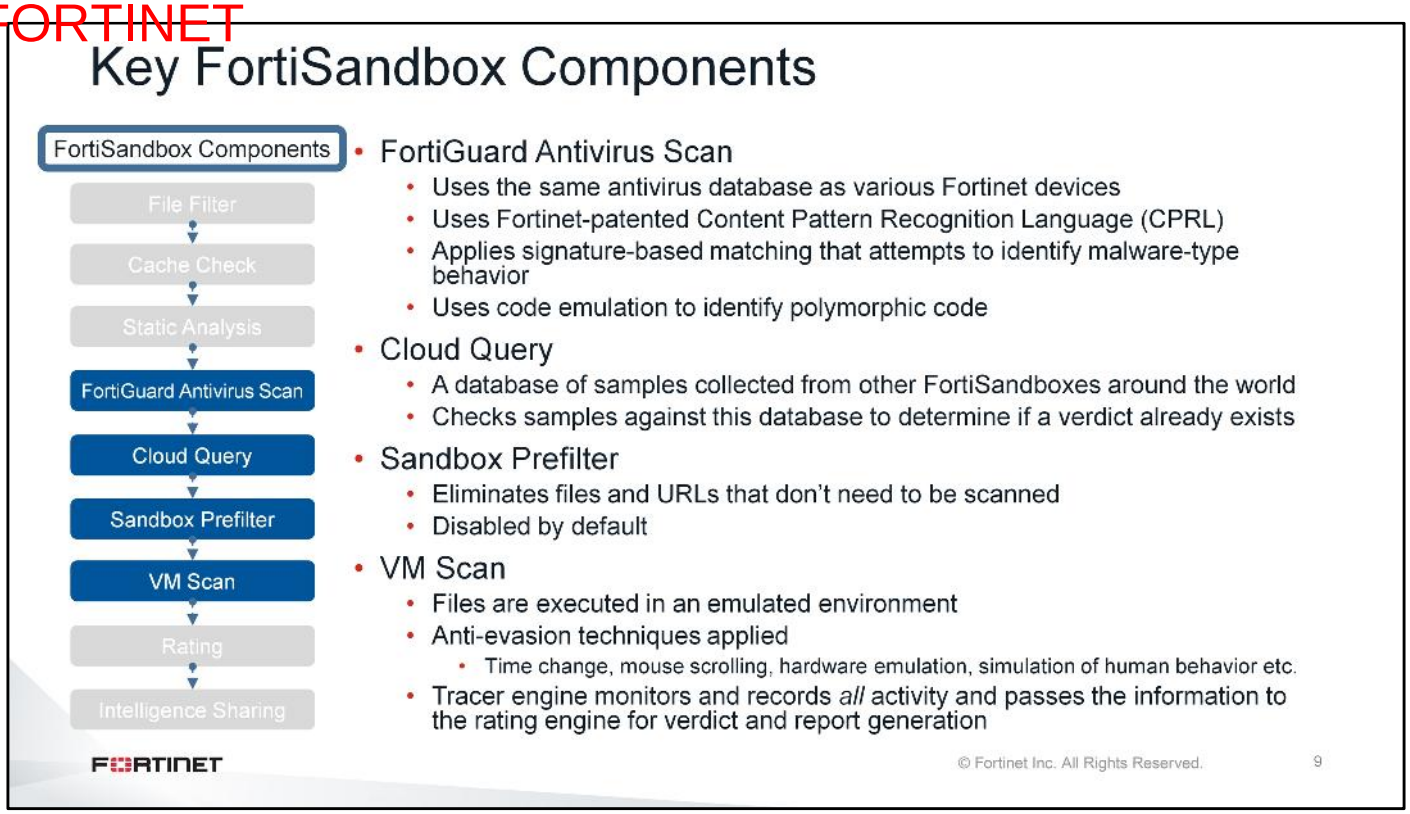
It is important to understand that FortiSandbox does not *physically* block any malware; it simply provides feedback on whether or not the file is malicious.



The file filter determines the sample file type. The file filter also submits the samples into the appropriate scan job, based on the scan profile configuration.

After FortiSandbox has determined the file type, the sample is checked against cached verdicts on FortiSandbox to see if there is an existing verdict for the sample. This is also where FortiSandbox applies the black/white lists configuration, and any existing overridden verdicts.

Next, the file is submitted for a static analysis scan, where specialized scanners analyze the behavior of the sample, as well as extract embedded objects for further analysis. Code emulation is applied to simulate the intended activity of any embedded scripts or macros. Embedded URLs are extracted and checked against the FortiGuard URL and IP reputation databases. In this step, since the malware is not being run in a sandbox, any evasion or anti-debugging techniques built into the malware will not affect the static analysis scanners from discovering malicious activity.



In the next step, FortiSandbox employs the FortiGuard antivirus engine, which utilizes Fortinet's patented Content Pattern Recognition Language (CPRL), and attempts to identify malware-type behavior within the file. CPRL allows one signature to match many different code variations of the same malware. This keeps the signature databases small, and allows efficient pattern matching. The antivirus engine also applies code emulation to identify polymorphic code.

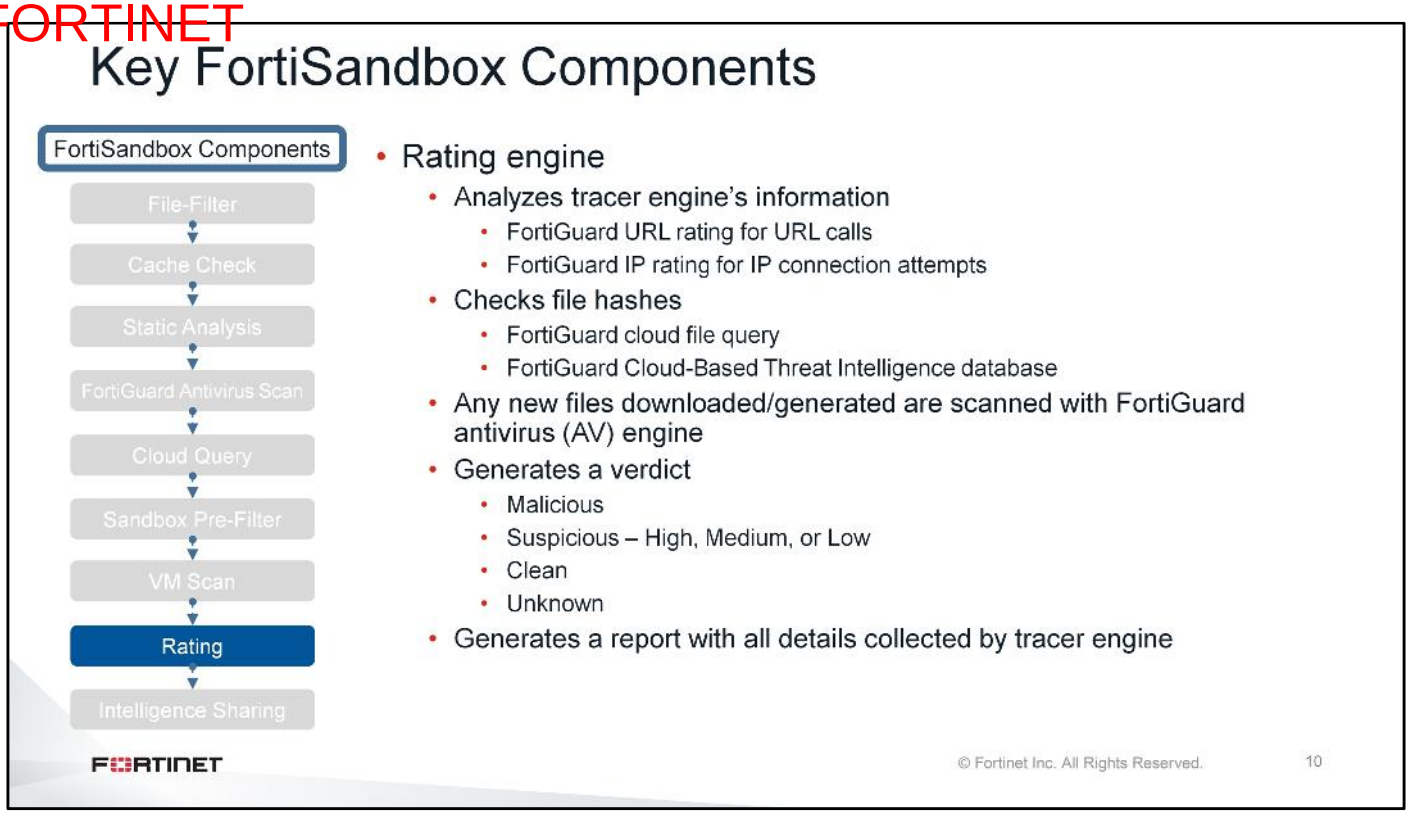
The FortiSandbox Community Cloud is a database of samples and verdicts collected from other FortiSandbox devices around the world. A checksum of the file is sent to the FortiSandbox Community Cloud and is checked against the database. If the verdict is generated using an up-to-date antivirus engine and database, then FortiSandbox uses the verdict as-is; otherwise, FortiSandbox passes the file to the next process.

The Sandbox prefilter can further reduce the number of files and URLs that are submitted for sandboxing. For example, if a PDF doesn't contain any scripts, it doesn't need to be scanned. Therefore, that file would be filtered out by the Sandbox prefilter process. You'll learn more about the sandbox prefilter later in this lesson.

For each file that requires sandboxing, FortiSandbox generates a new VM instance, and starts the execution of the file. As the file is executed, a tracer engine monitors a wide range of behavior, including the following:

- System files being modified or deleted
- Registry keys being created, modified, or deleted
- New files and processes being generated
- Web URLs being accessed
- Connection attempts to IP addresses

The tracer engine forwards all the recorded activity to the rating engine, for verdict and report generation.

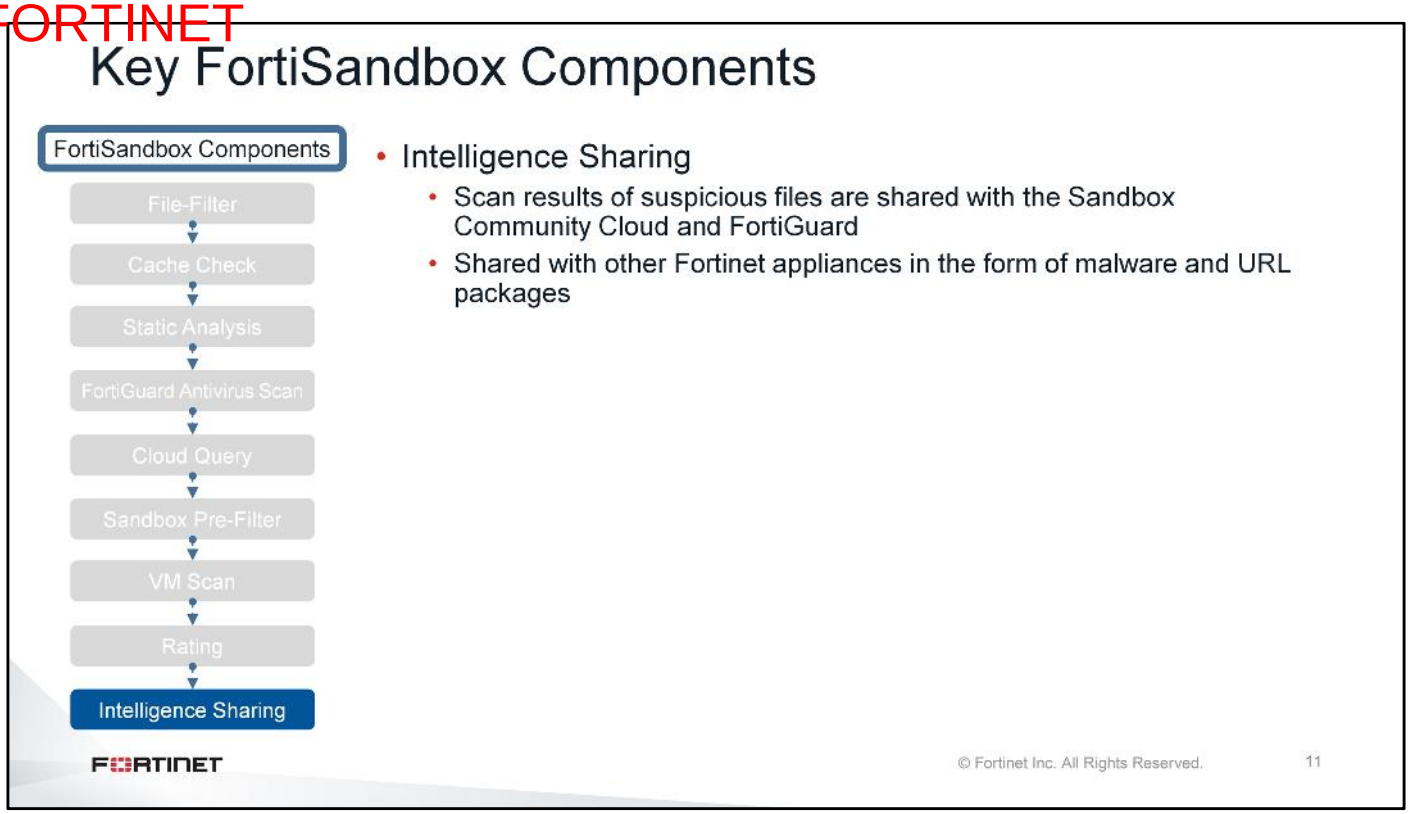


The rating engine analyzes the tracer engine's information.

Connections attempts to any URLs are checked against the FortiGuard web filtering database. All IP connection attempts are checked against the FortiGuard IP rating database to determine if they are known command-and-control (C&C) servers. Hashes for files generated during the sandbox analysis are submitted to the Sandbox Community Cloud, to query for any existing verdicts. The file hashes are also checked against another database called the FortiGuard Cloud-Based Threat Intelligence database. This database is a repository of threats with feeds from the Cyber Threat Alliance and other threat-intelligence sharing sources that Fortinet is partnered with.

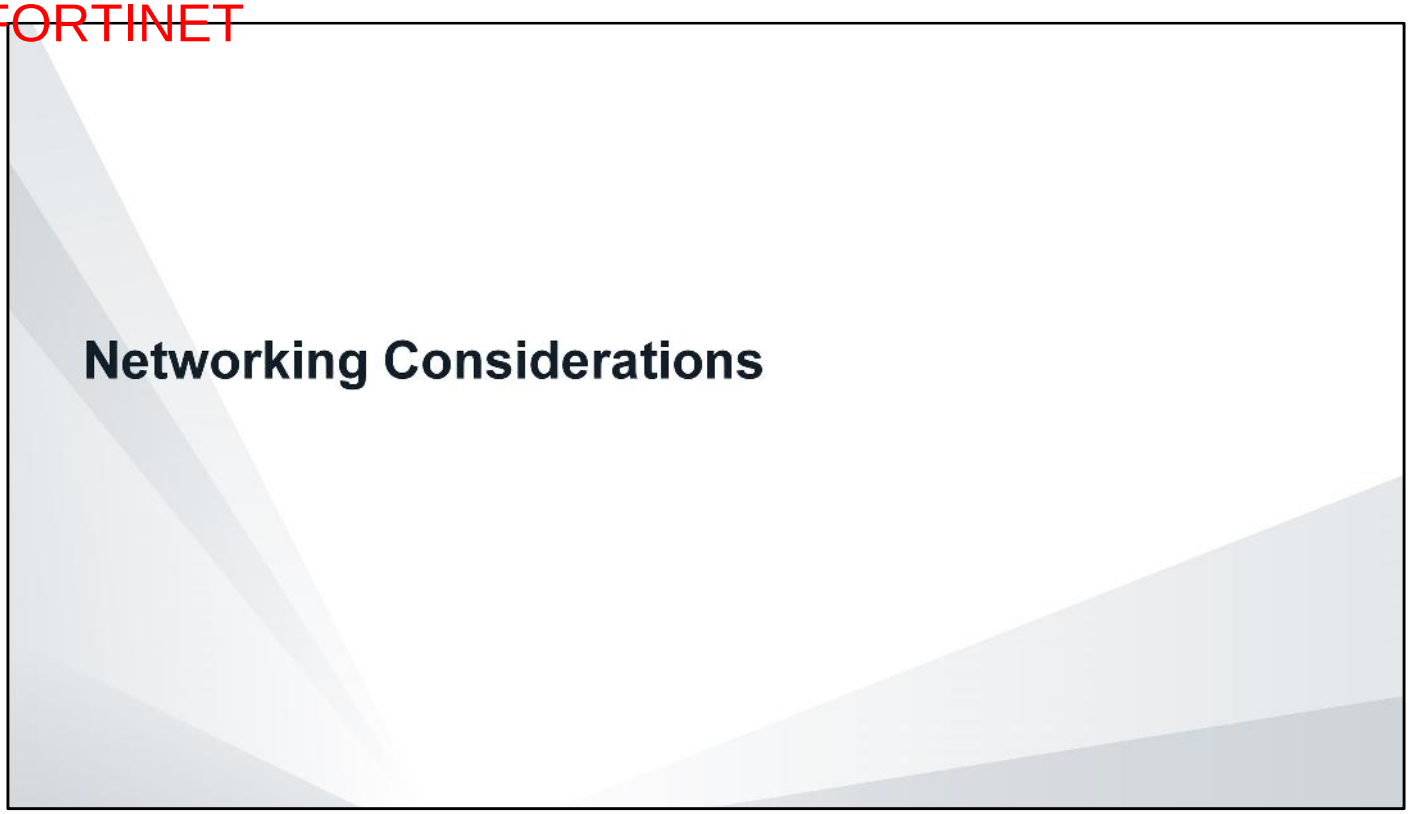
After analysis is complete, the rating engine generates a verdict. All files scanned in FortiSandbox can are put into one of three categories: malicious, suspicious, and clean/unknown. Malicious files are 100% known malware. Files are rated as suspicious can have three severity levels to further classify the risks. Fortinet devices, such as FortiMail, can make granular decisions based on these severity levels. The clean rating is assigned to any files that do not match any known antivirus signatures, cloud query verdict or display malicious behavior during sandboxing. The unknown rating is assigned to any files the FortiSandbox cannot process before the scan timeout expires. This could be due to not enough resources being available to generate a new VM instance for the scanning. FortiSandbox will try to reprocess the file at a later time, as resources become available.

Finally, the rating engine generates a report with all details collected by the tracer engine. This report is available for download.

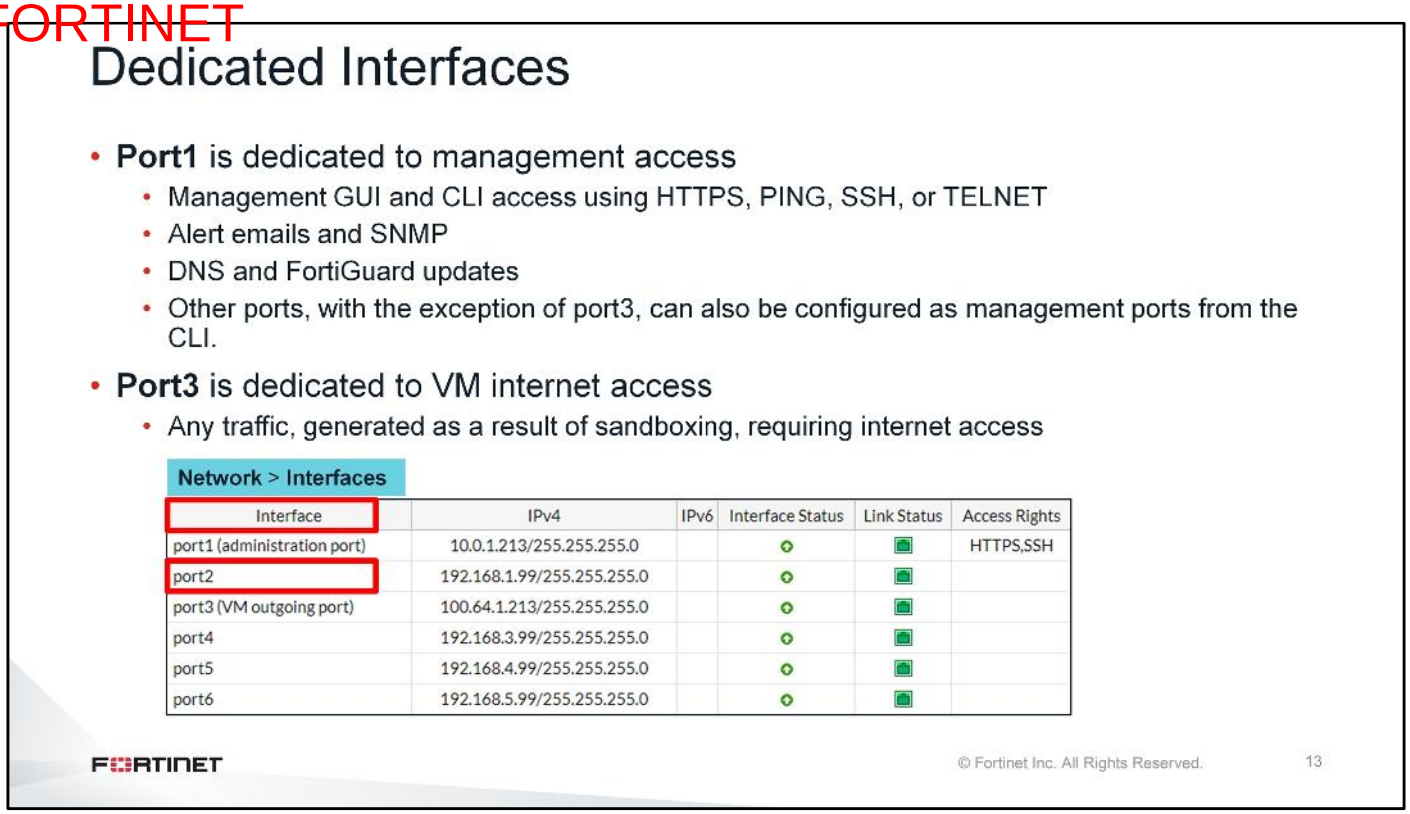


For any files with a suspicious rating, FortiSandbox will submit the file to FortiGuard along with the verdict report. FortiGuard Labs will verify the verdict and, if necessary, provide a new signature through an antivirus database update. FortiSandbox will also upload similar information to the Sandbox Community Cloud, so other subscribers can have access to the same information.

FortiSandbox also shares verdicts with other Fortinet appliances, in the form of malware and URL packages



In this section, you will learn the topology requirements for deploying a FortiSandbox in your network.

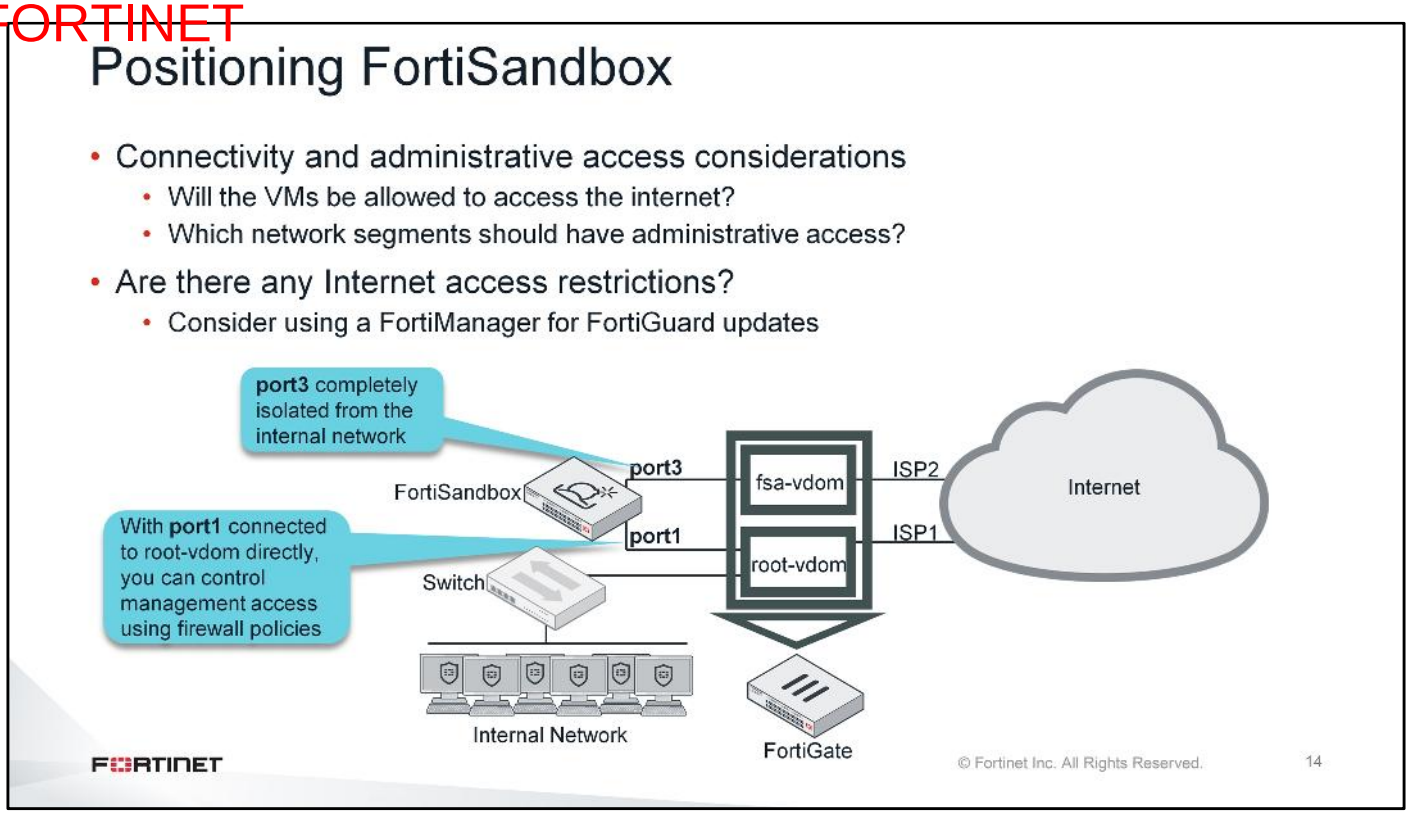


FortiSandbox has two interfaces that are dedicated to a specific function.

Port1 is dedicated to all management-related traffic. This includes management GUI and CLI access, alert emails, SNMP, DNS, and FortiGuard access. Port1 can also be used to accept files from Fortinet devices; however, it cannot be used for sniffer mode.
Other ports, with the exception of port3, can also be configured as management ports from CLI.

Port3 is used for outgoing communication, triggered as a result of sandboxing a file. This port is also used for license key activation for all Windows guest VM license keys. Port3 cannot be used to accept file inputs from any sources.

The rest of the ports can be used for network access as well as sniffer input, Fortinet device input, and internode communication within a cluster.

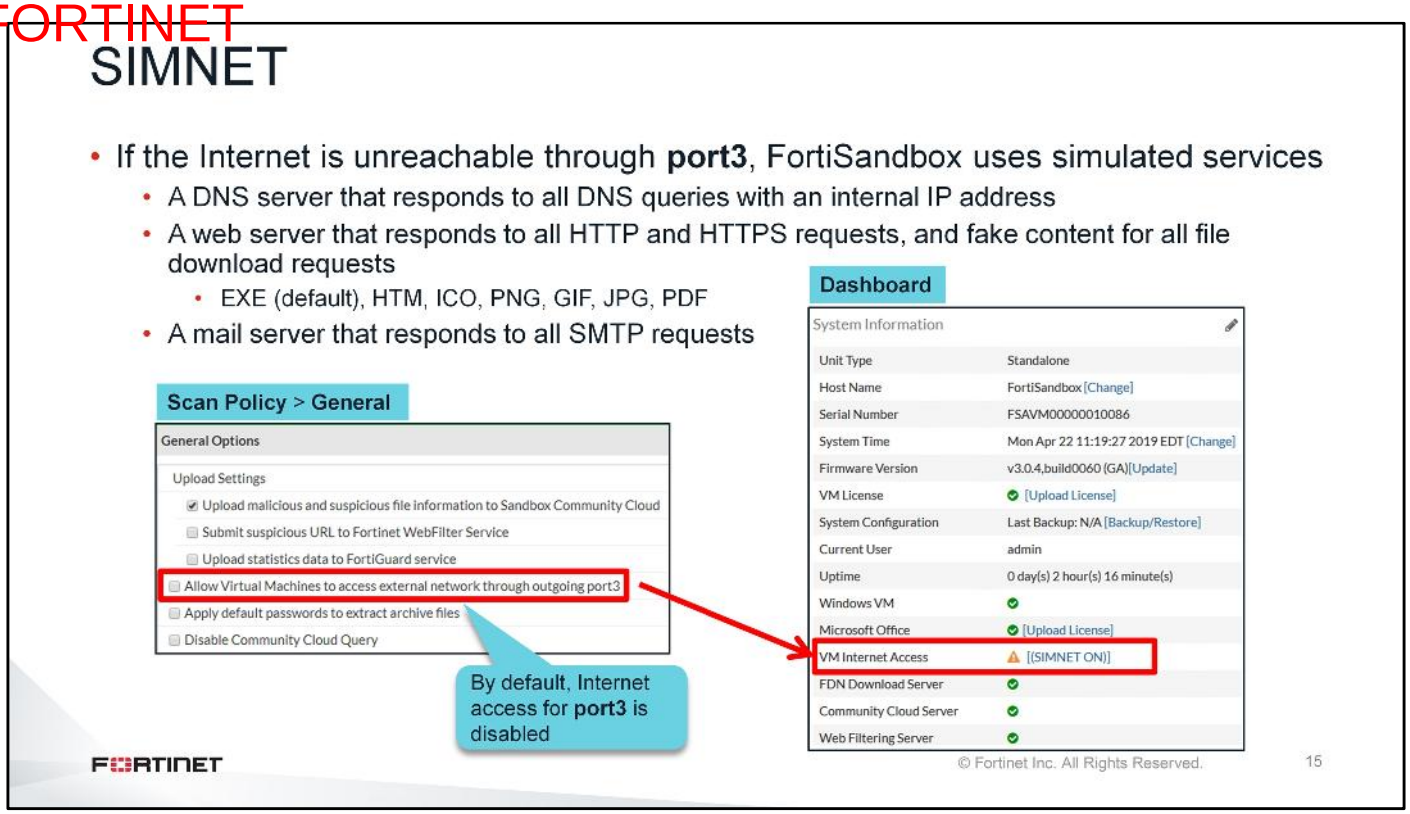


When deploying FortiSandbox in your network, you should consider connectivity and administrative access. For example, will the VMs running on the sandbox be allowed to access the Internet? Which network segments should have access to the management GUI? Finally, should there be any access restrictions to the Internet for the FortiSandbox itself? If you want to have access restrictions, then you may want to consider using a FortiManager for FortiGuard updates.

FortiSandbox uses **port3** to allow scanned files to access the Internet. This behavior is crucial in generating a reliable verdict on a file. To eliminate the risk of any malware propagating and replicating internally, it is *highly* recommended to that you put **port3** on an isolated network behind a firewall.

If you're using a FortiGate, you should create a separate VDOM to isolate all FortiSandbox **port3** traffic. Configure the firewall policies to allow *only* outbound traffic.

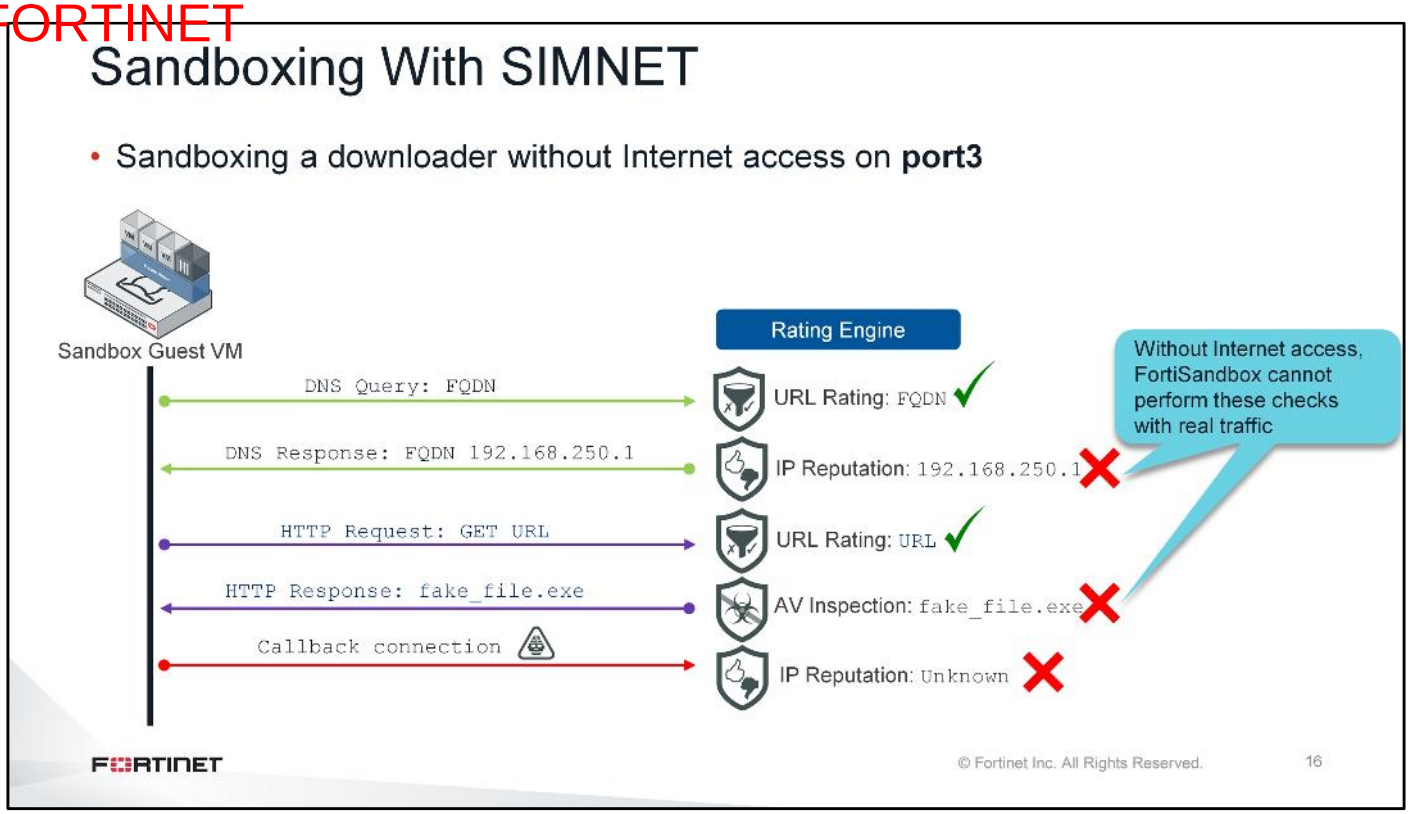
Due to the nature of traffic sandboxed malware could generate, this traffic can lead to a bad reputation for the Internet-facing IP. If you have legitimate services running on that connection, it could result in a service disruption due to a bad IP rating. Sandbox execution is very short. So while it is unlikely to result in a poor reputation, it is still a possibility to consider. The *best* option is to use a dedicated Internet connection for **port3** traffic. This will ensure your primary ISP's public IP address reputation scores are not compromised by the nature of the traffic the FortiSandbox VMs will generate.



If VM traffic cannot pass through **port3**, FortiSandbox will switch into SIMNET mode and display **SIMNET ON** in the **System Information** widget. SIMNET tricks the file being analyzed by responding to different Internet queries with these fake responses:

- A DNS server that responds to all DNS queries with an internal IP address
- A web server that responds to all HTTP and HTTPS requests, and fake content for all file download requests
- A mail server that responds to all SMTP requests

Without Internet access, some of the inspection features while sandboxing will not result in accurate detection. This means that certain types of malware detection will not work as well as they could. The decision of whether or not to allow Internet access to the VMs is not just about increasing the risk to the reputation of your IPs—it also directly improves the ability of FortiSandbox to accurately detect malware. The best results occur when Internet access is allowed, so this is the preferred deployment.



(slide contains automated animation)

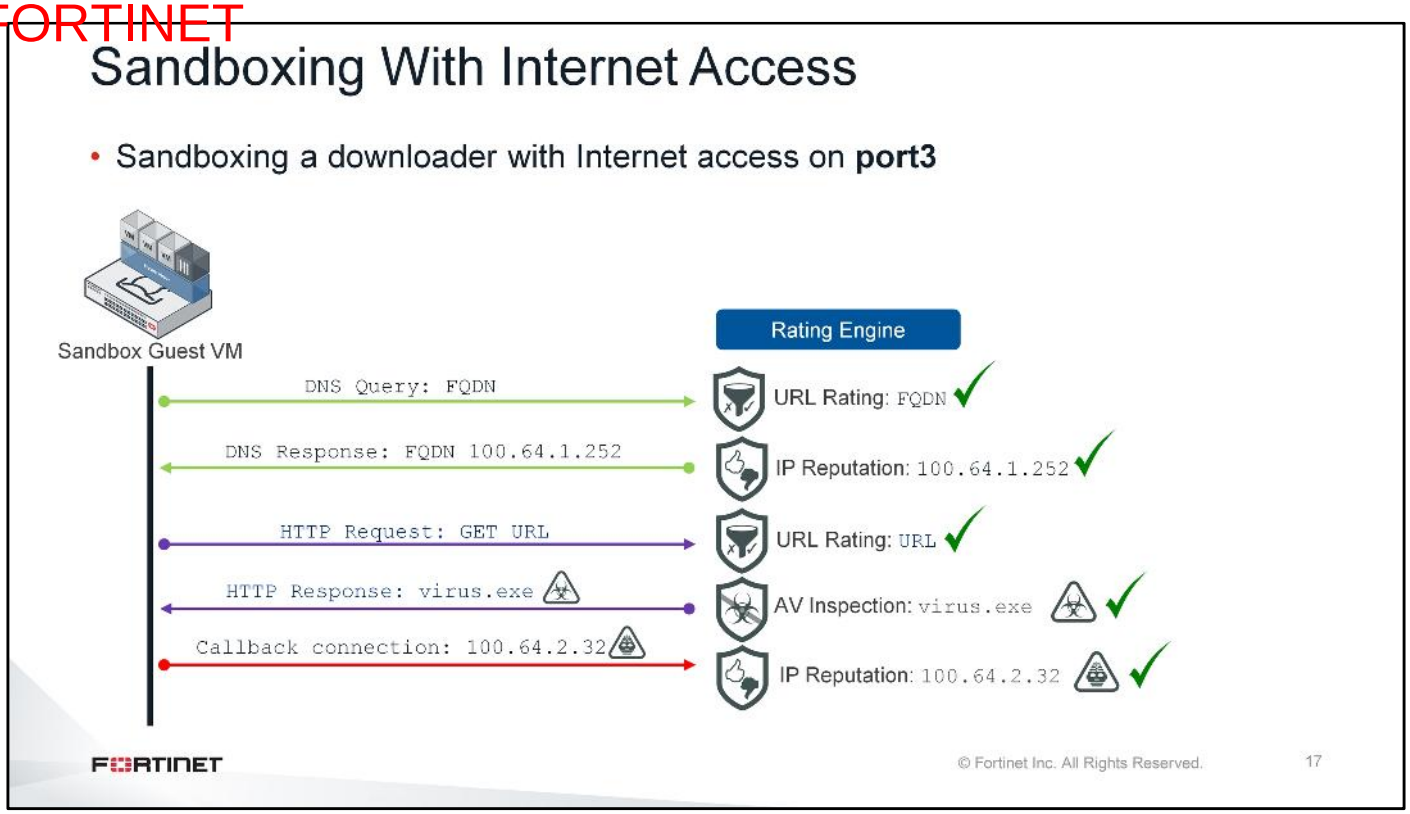
If you decide not to allow Internet access to the VMs, certain requests generated by the malware sample are replied to with fake responses.

When the malware does a DNS query, FortiSandbox responds with an internal IP address. Performing an IP reputation lookup on an internal IP would be meaningless.

When the malware attempts to download a file, FortiSandbox provides a fake download package. This allows the downloader to successfully execute; however, FortiSandbox cannot run it's antivirus inspection on the file.

If the malware creates a callback connection to an IP, FortiSandbox cannot rate the IP, to determine if it's a botnet server.

The reduced subset of inspection features can potentially generate a verdict that's not 100% reliable.



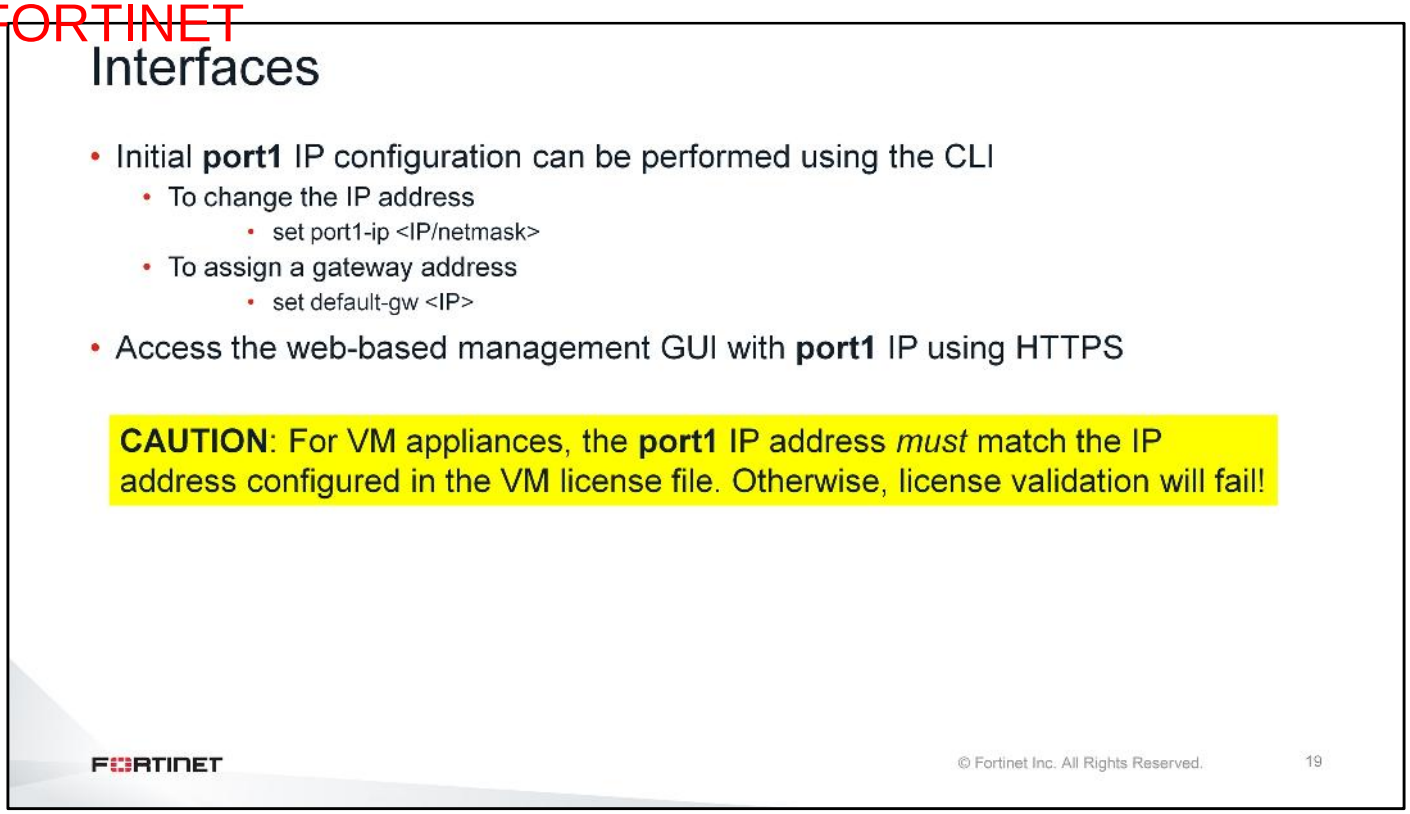
(slide contains automated animation)

With Internet access on **port3**, FortiSandbox is able to perform the full set of inspections.

This time, the DNS query receives a genuine public IP address in the response, which can be rated against the FortiGuard IP reputation service. If the malware attempts to download some payload, it can be inspected using the FortiGuard antivirus engine, which could result in a specific malware detection. If that payload creates a callback connection to an IP, FortiSandbox can also rate that IP against the FortiGuard IP reputation service, to determine if it's a botnet IP.

With the full set of inspection features, the resulting verdict is more reliable than if there was no Internet access. If you decide to allow Internet access, then it must be unrestricted and unfiltered.

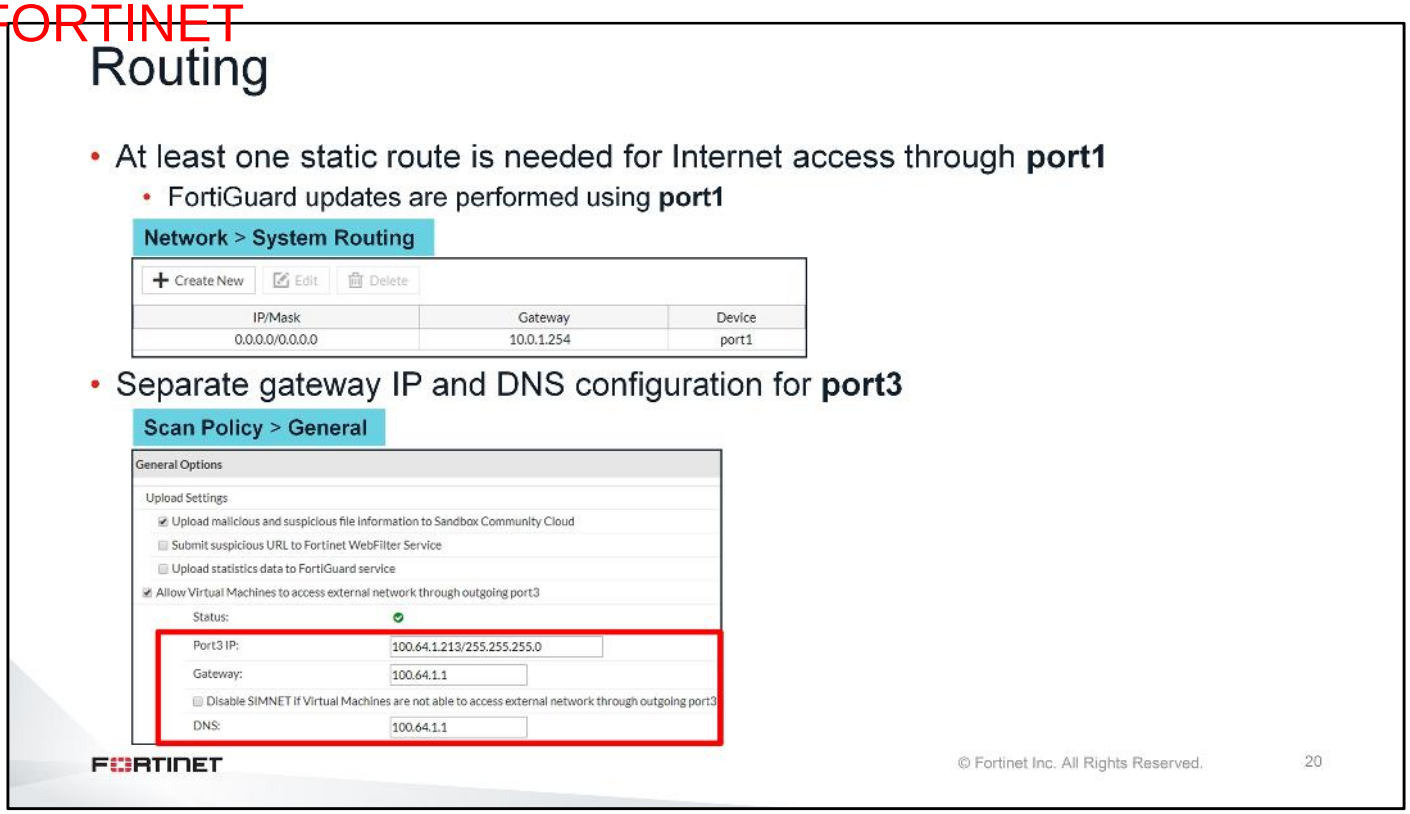
In this section, you will learn the basic configuration required to install FortiSandbox.



All FortiSandbox devices are preconfigured with default IP addresses. Initial **port1** IP configuration must be performed from the console, using the commands shown on this slide. If your management computer is on a separate subnet from FortiSandbox, you must specify a gateway address using the commands shown on this slide.

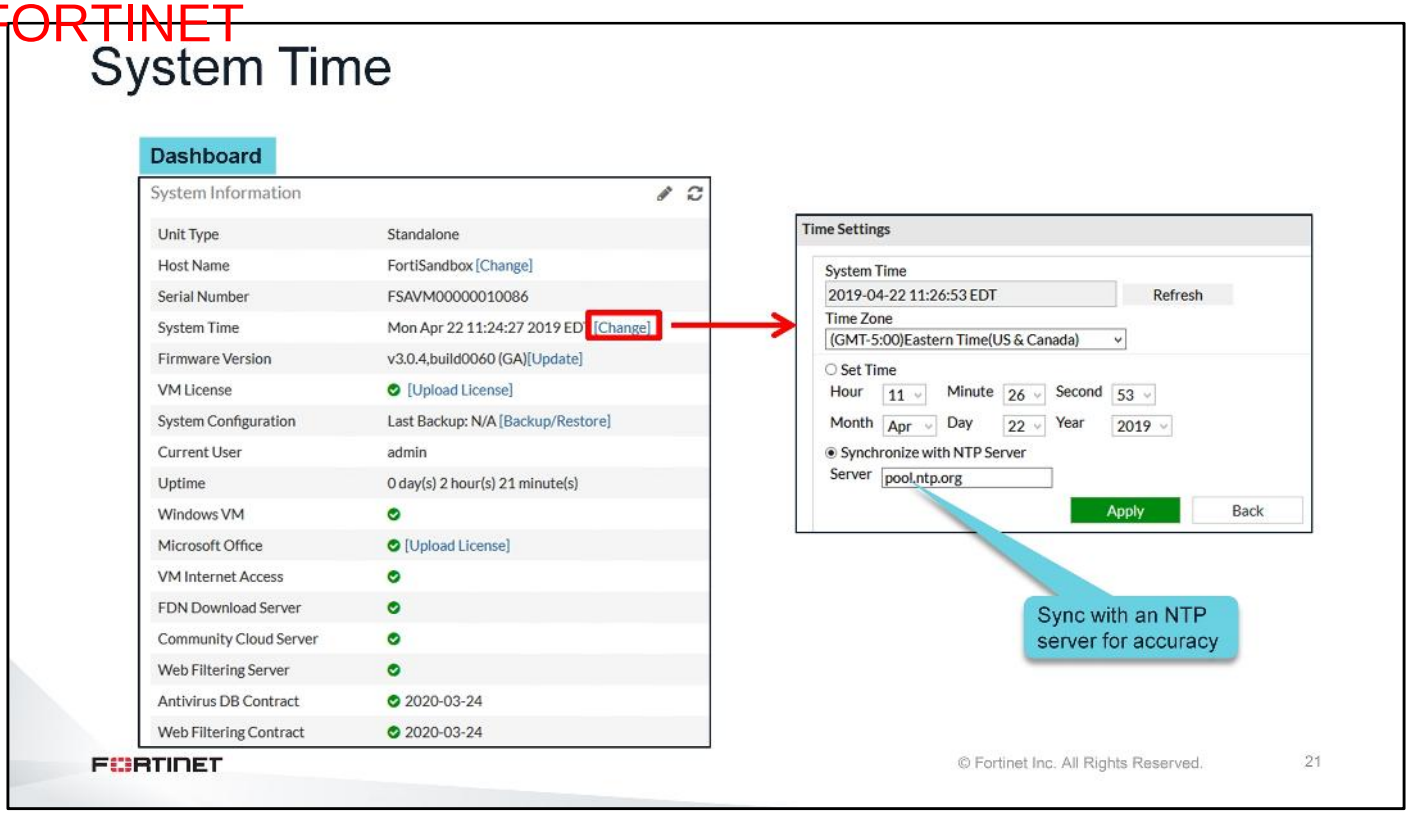
After you have assigned an IP from your own network's management subnet to **port1**, you can access the web-based management GUI with the **port1** IP, using HTTPS to complete the rest of the configuration tasks.

Keep in mind, for VM appliances, the **port1** IP address must match the IP address assigned to your VM license. Otherwise, license validation will fail.



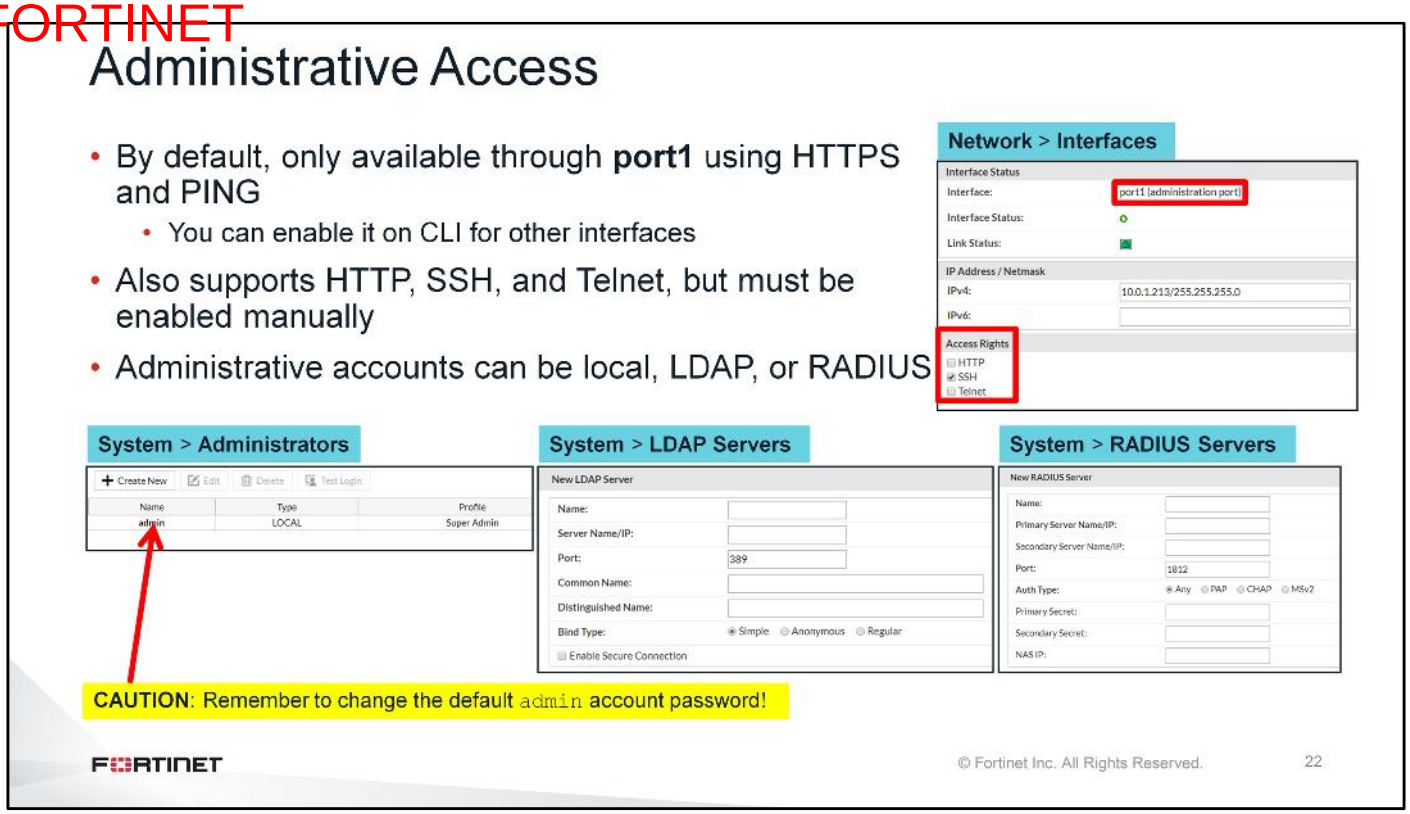
You will need to configure at least one static route for Internet access through **port1**, so the FortiSandbox can receive FortiGuard updates for the various packages.

The **port3** gateway and DNS configuration is separate from the regular static routing configuration. The gateway, and the DNS server assigned to **port3**, is strictly dedicated to traffic generated by VM sandboxing. It will not affect traffic from any other interface.



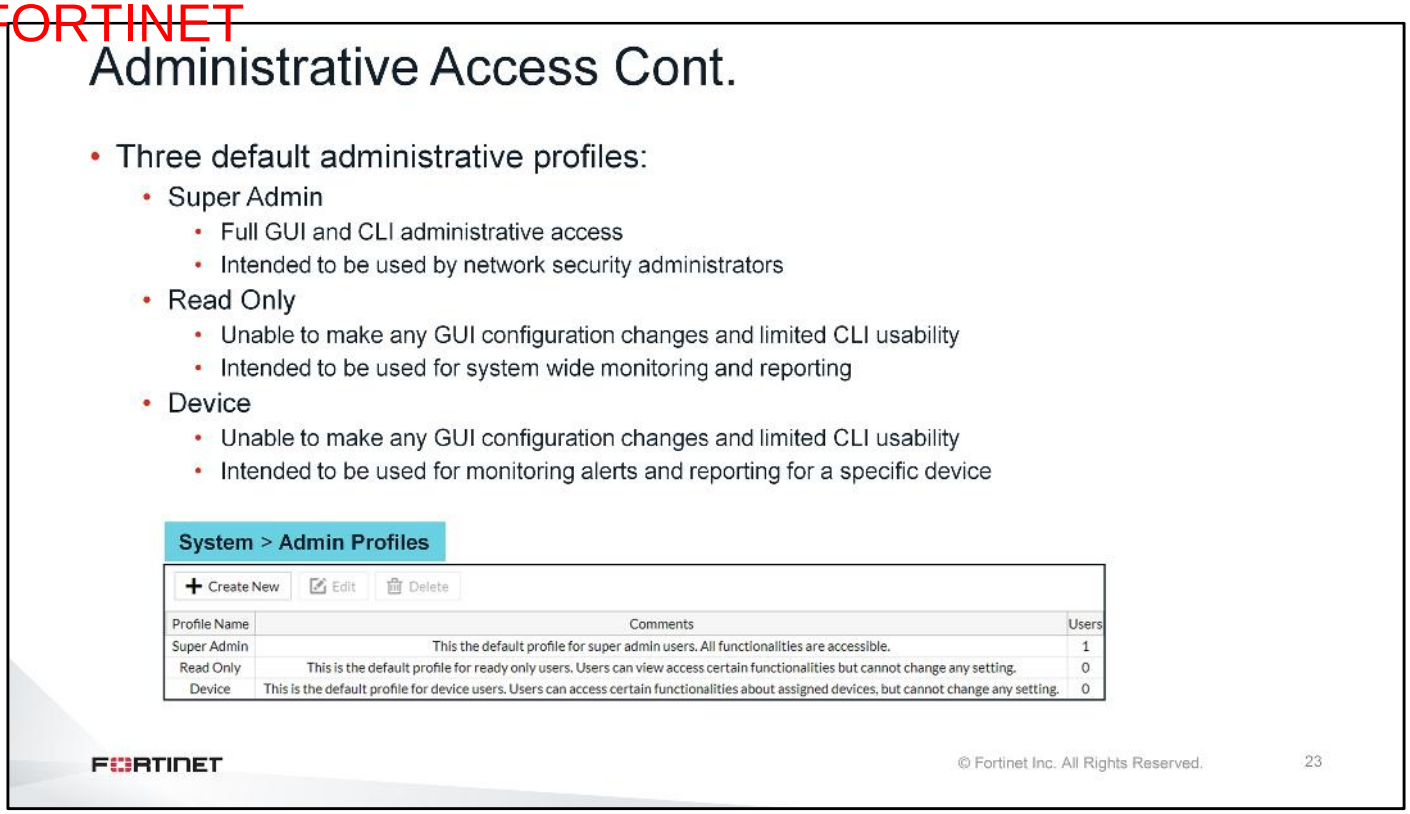
Accurate time information is crucial, especially when it comes to investigating new malware. Any investigation into new malware needs to be traced back to when that malware was first seen by FortiSandbox. In order to make sure this information is determined with precision, the clock must be accurate; otherwise, it will be difficult to determine how far this malware has spread.

In order to make incidence response easier (or perhaps even possible), it is important to make sure that all the network devices have their clock set accurately. For best results, synchronize your devices to the same NTP server.



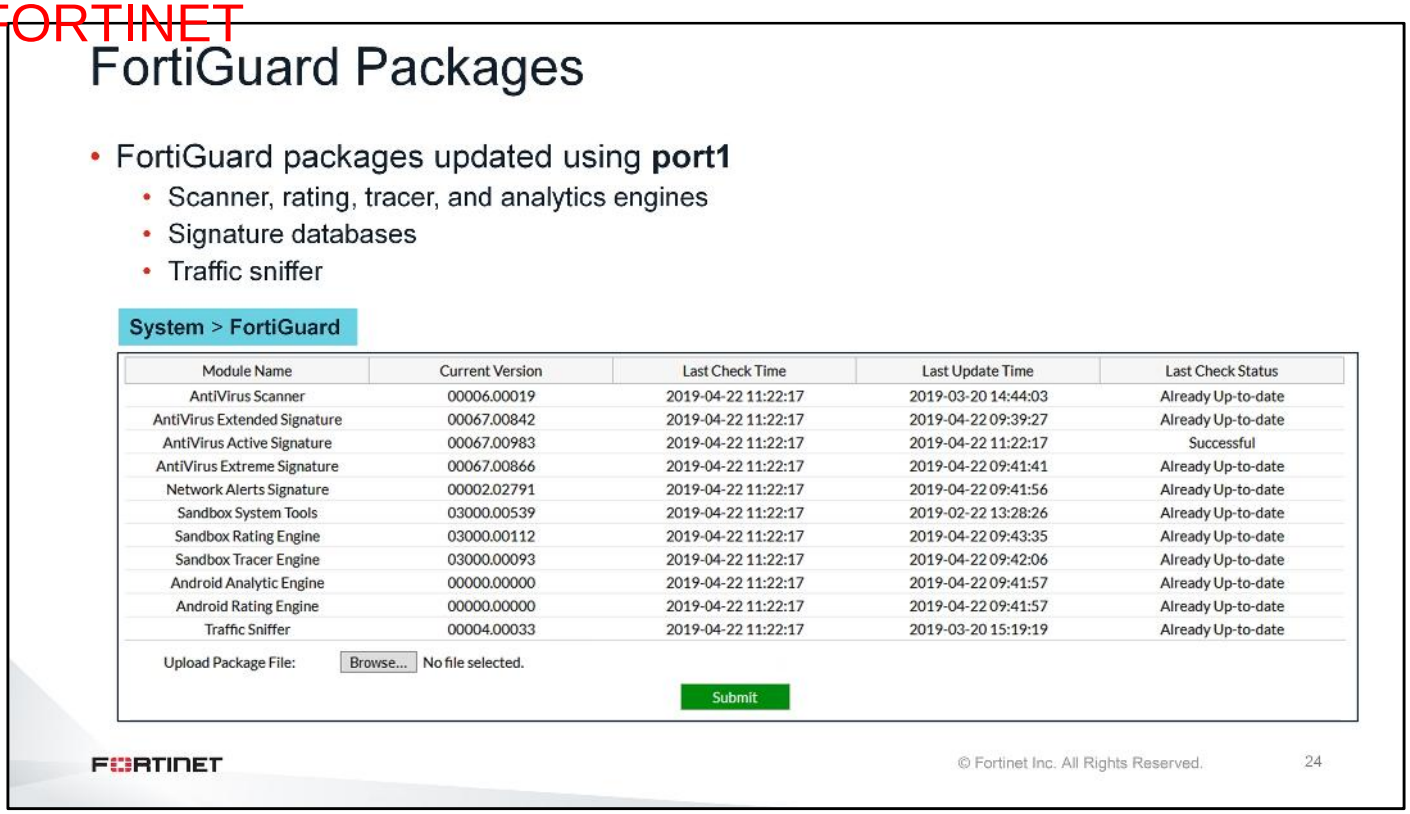
Responding to HTTPS and ping is hard-coded **port1** behavior. You can also enable additional protocols like HTTP, SSH, and Telnet. All other interfaces respond to ping only by default. You can modify other interfaces on the CLI to respond to other administrative protocols.

The default admin account has an empty password. This should be changed as soon as possible, for all Fortinet appliances. Aside from local accounts, FortiSandbox also supports LDAP, and RADIUS.



FortiSandbox has three default administrative profiles. The **Super Admin** profile allows full GUI and CLI administrative access, which is intended to be used by network security administrators.

The **Read Only** and **Device** profiles do not allow any GUI configuration changes and provide limited CLI usability. The **Read Only** profile is intended to be used for system-wide monitoring and reporting tasks; whereas the **Device** profile is intended to be used for monitoring alerts and reporting for a specific device.



FortiSandbox uses multiple packages that are updated dynamically by FortiGuard. Regular updates ensure your FortiSandbox is equipped for accurate and efficient detection mechanisms. Updated antivirus signatures allow for detection of malware, without the need to use sandboxing. An up-to-date database of IPs allows for more accurate botnet callback detection. Updates to the various engines help improve detection accuracy and reporting.

In this section, you will learn how to download, install, and manage guest VM images in FortiSandbox.

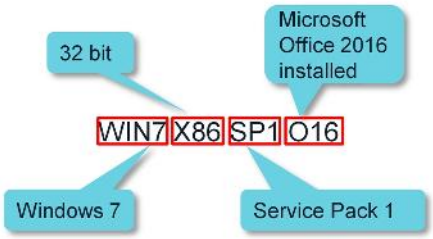
Guest VM Image Management

- Default VMs are preinstalled and preactivated on hardware appliances
  - VM names indicate OS version, service pack level, and whether or not Microsoft office is installed

Virtual Machine > VM Images

	Name	Version	Status	Enabled	Clone #	Load #	Extensions
−	Default VMs (1/1)						
	WIN7X86VMO16	1	activated	✓	1	1	

- Default VM types vary by model
  - VM00 – No default images



FORTINET

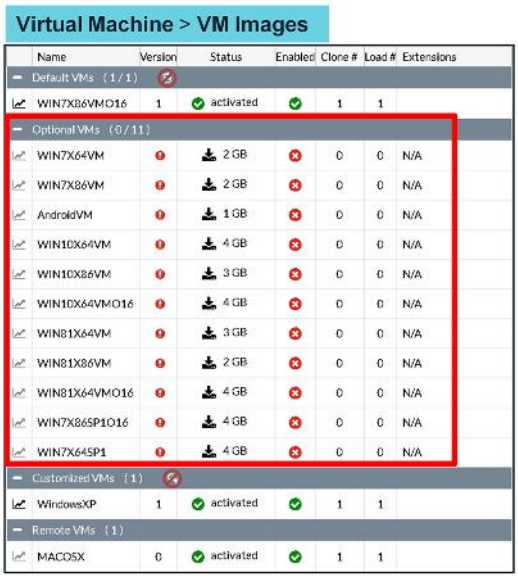
26

Default VMs are preinstalled and preactivated with the necessary license keys on hardware appliances. The VM name indicates the OS version and software installed. For example, WIN7X86SP1O16 VM runs Windows 7 32-bit with service pack 1 and Microsoft Office 2016. It's important to note that not all VM image will have Microsoft Office installed.

The types of default VMs vary by model. The VM00 virtual appliances do not have any preinstalled VM images. They must be downloaded and installed manually. For a VM to be useable in sandboxing, it must be in the **activated** state.

Guest VM Image Management

- Optional VMs are published by FortiGuard
  - Must be downloaded and installed manually
  - Appropriate license keys must be available for the images to activate
- Default VMs and optional VMs have default software installed:
  - Adobe Flash Player
  - Adobe Reader
  - Java Run Time
  - Microsoft Visual C++ Run Time
  - Microsoft.NET Framework
  - Microsoft Office (only on VMs ending with O16)
  - Web browsers



 27

The optional VMs are published by FortiGuard and must be downloaded and installed manually. If the default VMs in hardware appliances are not suitable for your organization, you can install an optional VM that fits your organization's needs. The optional VM list provides various configurations of VM images, such as Windows 10 32-bit, Windows 10 64-bit, and Windows 10 64-bit with Microsoft Office 2016.

By default, Default VMs and optional VMs have the following software installed:

- Adobe Flash Player
- Adobe Reader
- Java Run Time
- Microsoft Visual C++ Run Time
- Microsoft .NET Framework
- Microsoft Office (only on VMs ending with O16)
- Web Browsers

Guest VM Image Management

- Users can generate customized VMs
  - Windows XP supported as a custom image
  - Refer to the *VM Installation Guide* found at `docs.fortinet.com` for step-by-step instructions

Virtual Machine > VM Images

	Name	Version	Status	Enabled	Clone #	Load #	Extensions
−	Default VMs (1/1)						
	WIN7X86VMO16	1	activated	✓	1	1	
−	Optional VMs (0/11)						
	WIN7X64VM		2 GB	✗	0	0	N/A
	WIN7X86VM		2 GB	✗	0	0	N/A
	AndroidVM		1 GB	✗	0	0	N/A
	WIN10X64VM		4 GB	✗	0	0	N/A
	WIN10X86VM		3 GB	✗	0	0	N/A
	WIN10X64VMO16		4 GB	✗	0	0	N/A
	WIN81X64VM		3 GB	✗	0	0	N/A
	WIN81X86VM		2 GB	✗	0	0	N/A
	WIN81X64VMO16		4 GB	✗	0	0	N/A
	WIN7X86SP1O16		4 GB	✗	0	0	N/A
	WIN7X64SP1		4 GB	✗	0	0	N/A
−	Customized VMs (1)						
	WindowsXP	1	activated	✓	1	1	
−	Remote VMs (1)						
	MACOSX	0	activated	✓	1	1	

FORTINET

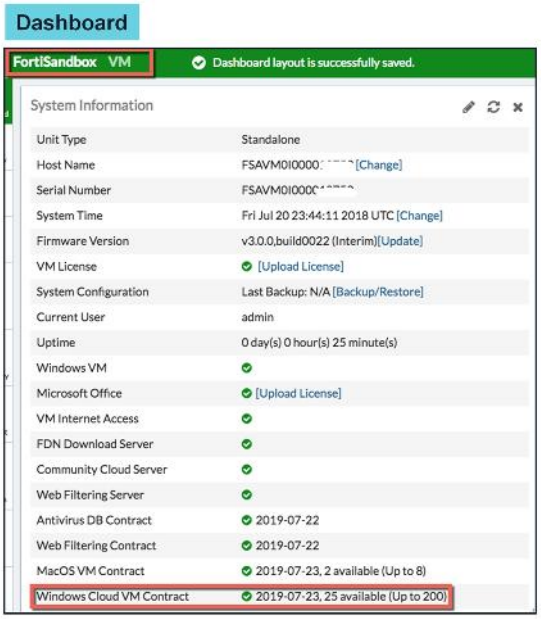
28

The VM images provided by Fortinet might not suit your needs. For example, the default software installed on the VM images might not mirror what you have installed in your organization's computers. You can generate a custom VM, that fits your organization's needs, and upload it to FortiSandbox. Refer to the *VM Installation Guide* found at `docs.fortinet.com` for step-by-step instructions for creating custom VMs.

The custom VM image allows you to customize a VM image with any software that can be installed and run on a Windows computer.

Windows Cloud VM

- FortiSandbox VM supports Windows cloud VM
- Windows Cloud VM service for (5) Windows VMs and maximum expansion limited to (200) per FortiSandbox VM
- Windows Cloud VMs are remote cloud VMs hosted in Fortinet

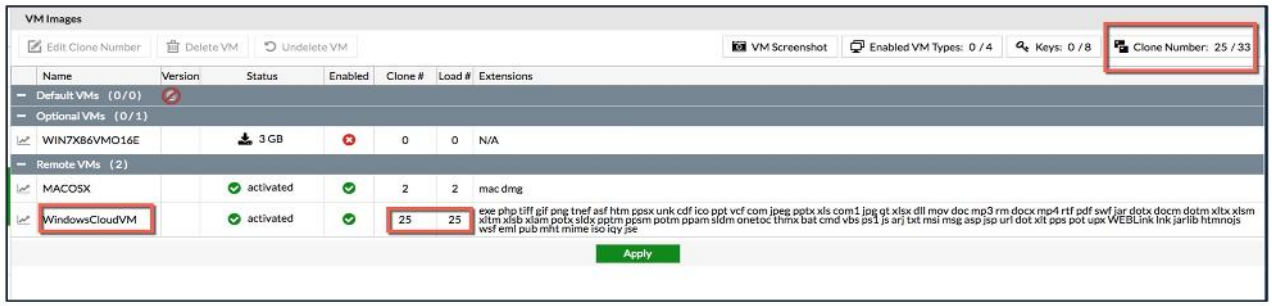


FORTINET

29

Starting at firmware release 3.0, FortiSandbox supports Windows cloud VM. The Windows cloud VM's are hosted on Fortinet data centers. Customers would require an additional license to subscribe to this service. A Windows cloud license supports five Windows VMs, but it can be expanded to support 200 Windows VMs per FortiSandbox VM, based on license type.

FSA-VM00 with Windows Cloud VM

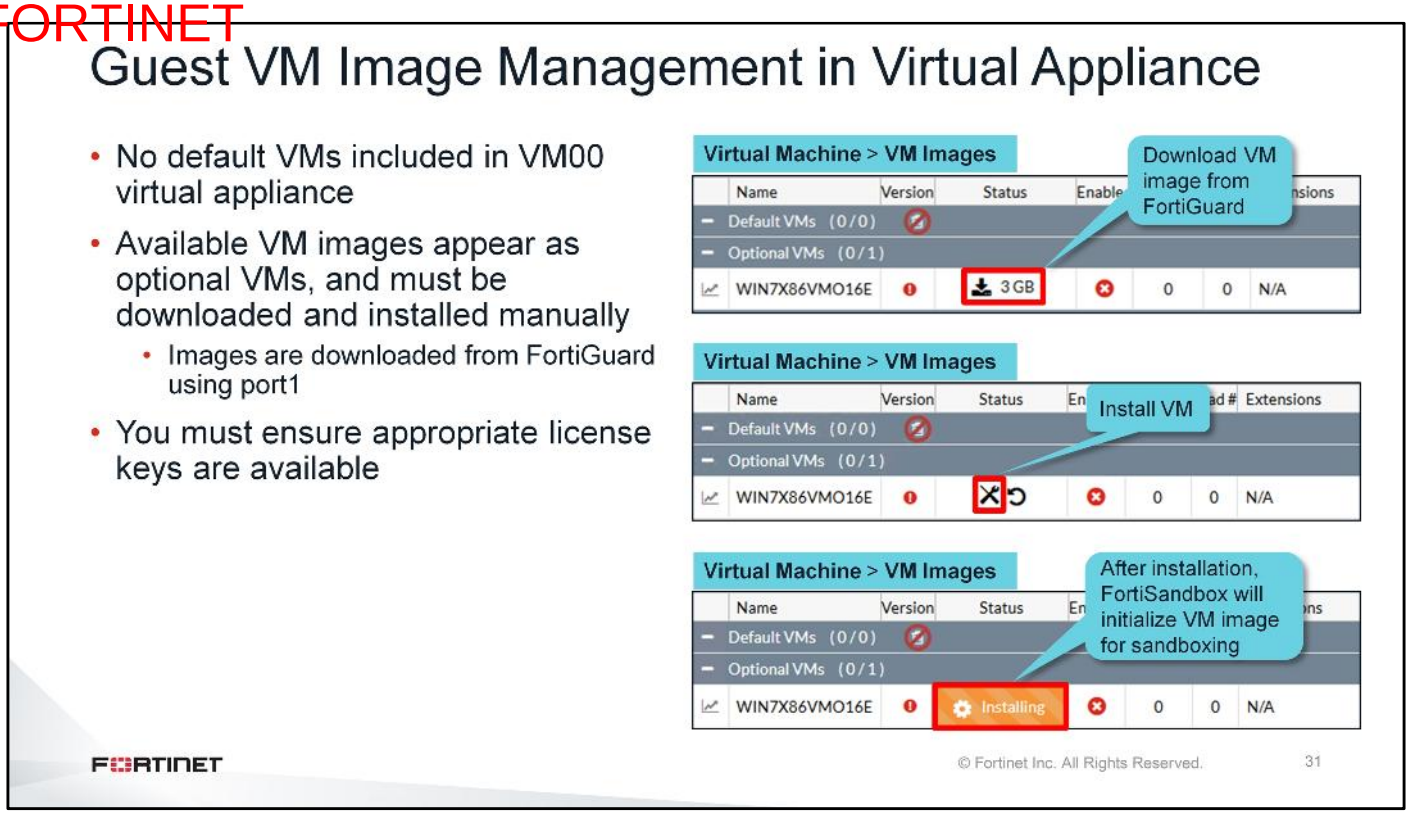


- FSA-VM00 supports 8 local VMs
- FSA-VM00 with local VM still needs port3 access
- Average scan time in VMs is currently 5 minutes per file
- Windows cloud VMs need one main (port1) interface

FORTINET

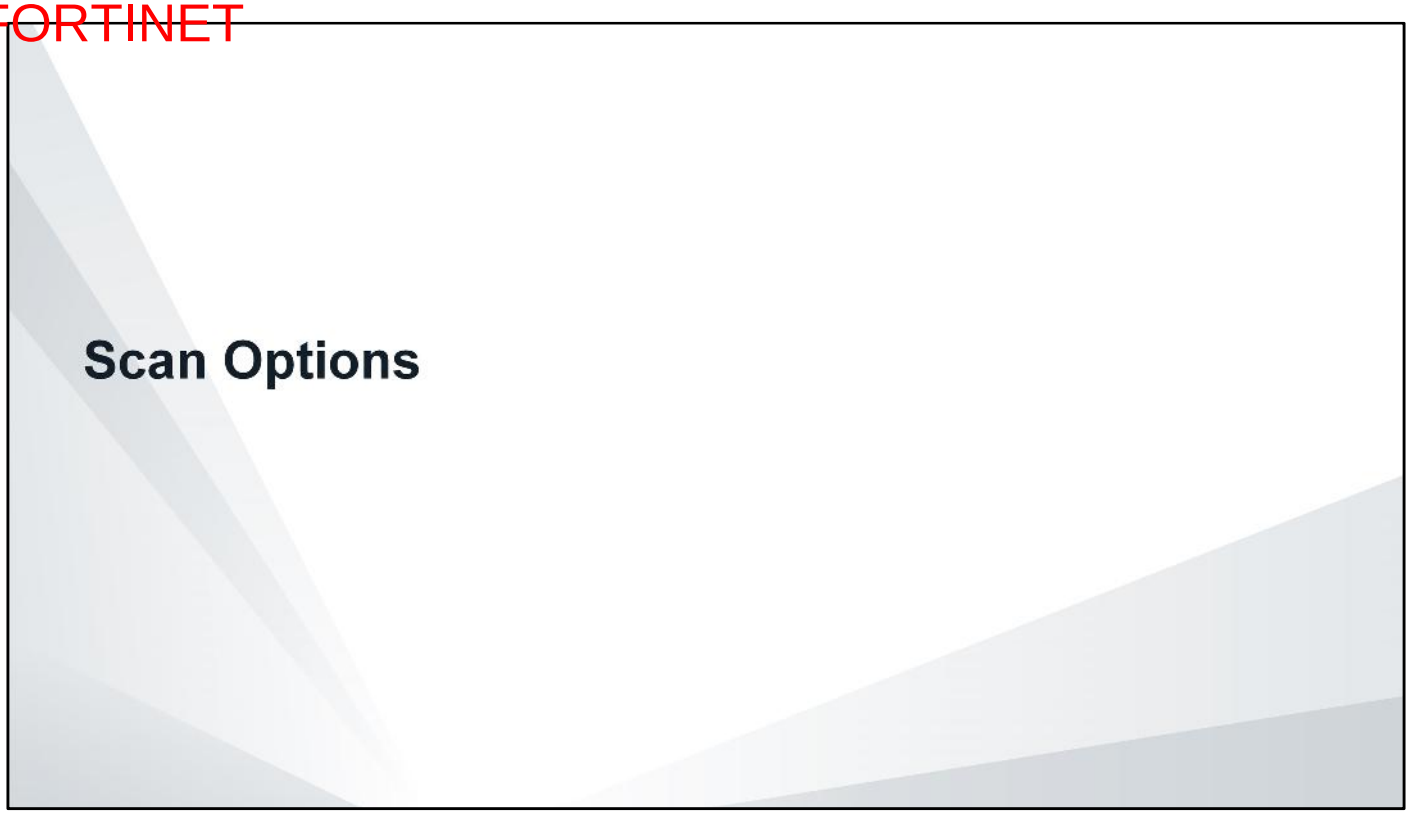
30

Once you have subscribed to Windows cloud VM, it will show up under remote VMs as activated. The average scan time for a file on Windows cloud VM is 5 minutes and you need to configure one main interface to communicate with the Fortinet data center server where the Windows cloud VM is hosted.



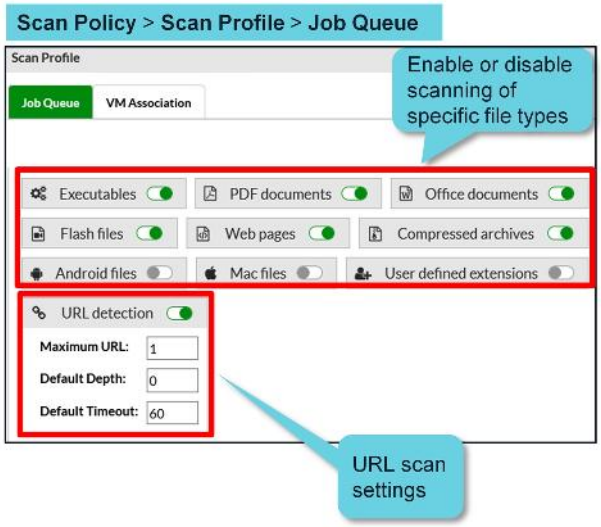
As mentioned before, FortiSandbox VM00 virtual appliance does not ship with any default VMs. Any available VM images will appear under **Optional VMs**, which means that they must be downloaded and installed manually. This process may take a substantial amount of time, so take that into consideration when you're planning your initial configuration. This procedure also applies to any Optional VMs you want to download on hardware appliances.

VM images are downloaded from FortiGuard, using port1. So, you must ensure FortiSandbox has a default route and Internet connectivity for **port1**.



In this section, you will learn how to control various scan options to optimize scan job performance and modify scanning behavior on FortiSandbox.

Scan Profile



- Control which file types or URLs will be accepted into the sandbox job queue
- Affects files received from device, sniffer, network share, and adapter inputs
  - On-demand, JSON API, FortiMail and Network Share file submissions will always be accepted
- URL detection depth defines how deep FortiSandbox will inspect links on a page
  - 0: inspect the contents of the page directly specified by the URL
  - 1: inspect the contents of the page directly specified by the URL, as well as all links on that page
- URL detection timeout defines how long FortiSandbox will spend scanning a specific URL

FORTINET

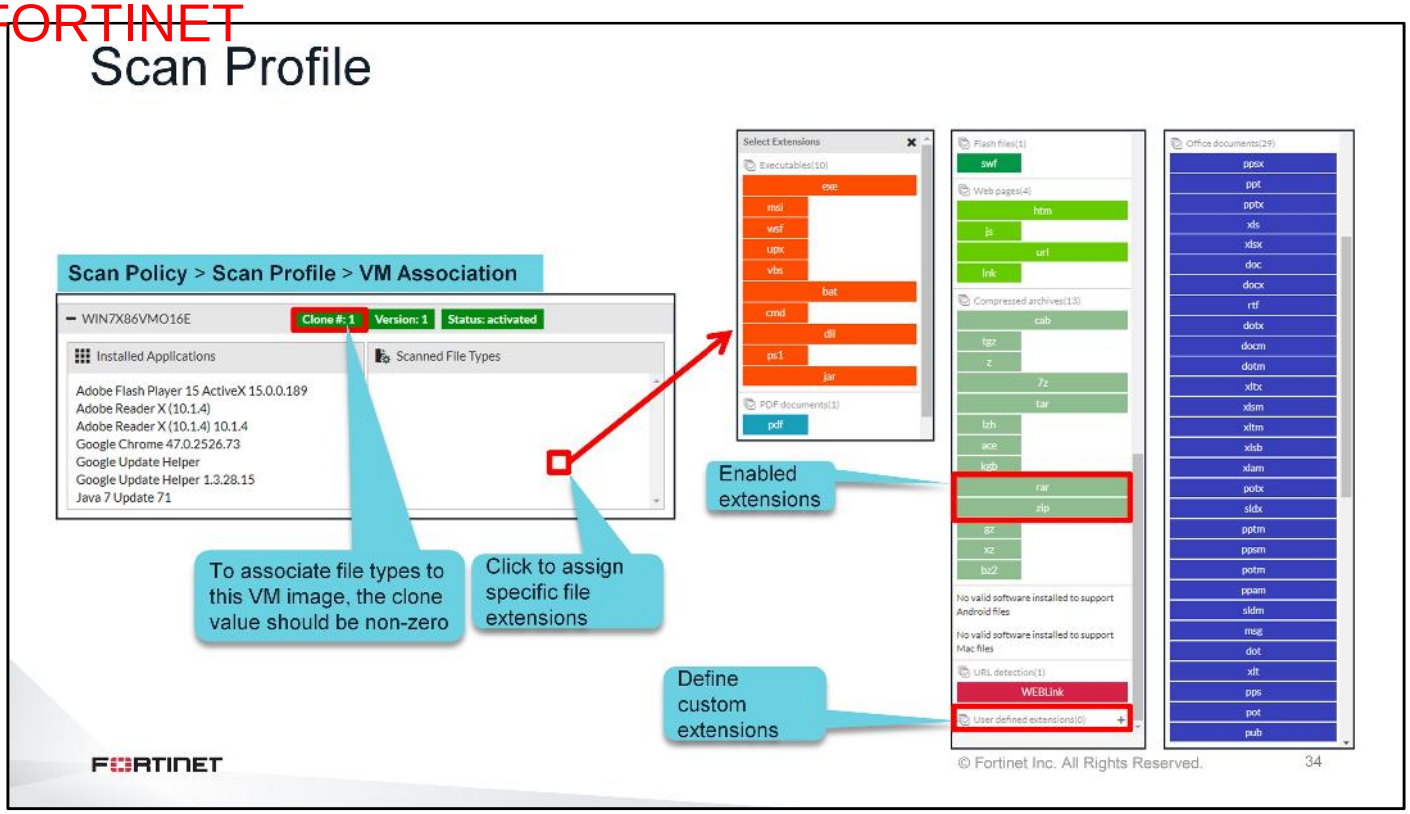
 33

The **Scan Profile** is divided into two sections. The first section of profile is used to enable or disable scanning of specific file types or URLs. Keep in mind that these settings only affect files received from device, sniffer, and adapter (ICAP, Carbon Black/Bit9, BCC Adapter) inputs. Files or URLs submitted on-demand or through JSON API, email attachments submitted by FortiMail and files from Network Share will always be put into the scan job queue, even if their file types are disabled.

When URL detection is enabled, FortiSandbox will scan URLs using the installed web browsers in the guest VM images. You can adjust the URL detection settings to ensure FortiSandbox does not spend too much time and resources to follow URLs. Set the values based on the amount of investigation you wish to do on the web page.

The **Default Depth** value controls how deep FortiSandbox will inspect links on a page. For example, a depth of `0` means that FortiSandbox will only inspect the page directly specified by the URL, and a depth of 1 means that FortiSandbox will inspect the contents of the immediate page, as well as all links on that page. The **Default Timeout** value defines how long FortiSandbox will spend scanning a specific URL. The **Maximum URL** value defines how many URLs FortiSandbox will accept per submission using on-demand URL submission using management GUI or JSON API.

It is important to note that a timeout value of `60` seconds does not mean it will take exactly 60 seconds for a URL to be scanned. A submitted URL might wait in the pending job queue for a guest VM to become available. The URL detection timeout value does not take that into consideration. It starts the moment the FortiSandbox starts to scan the contents of webpage inside guest VM during sandboxing.

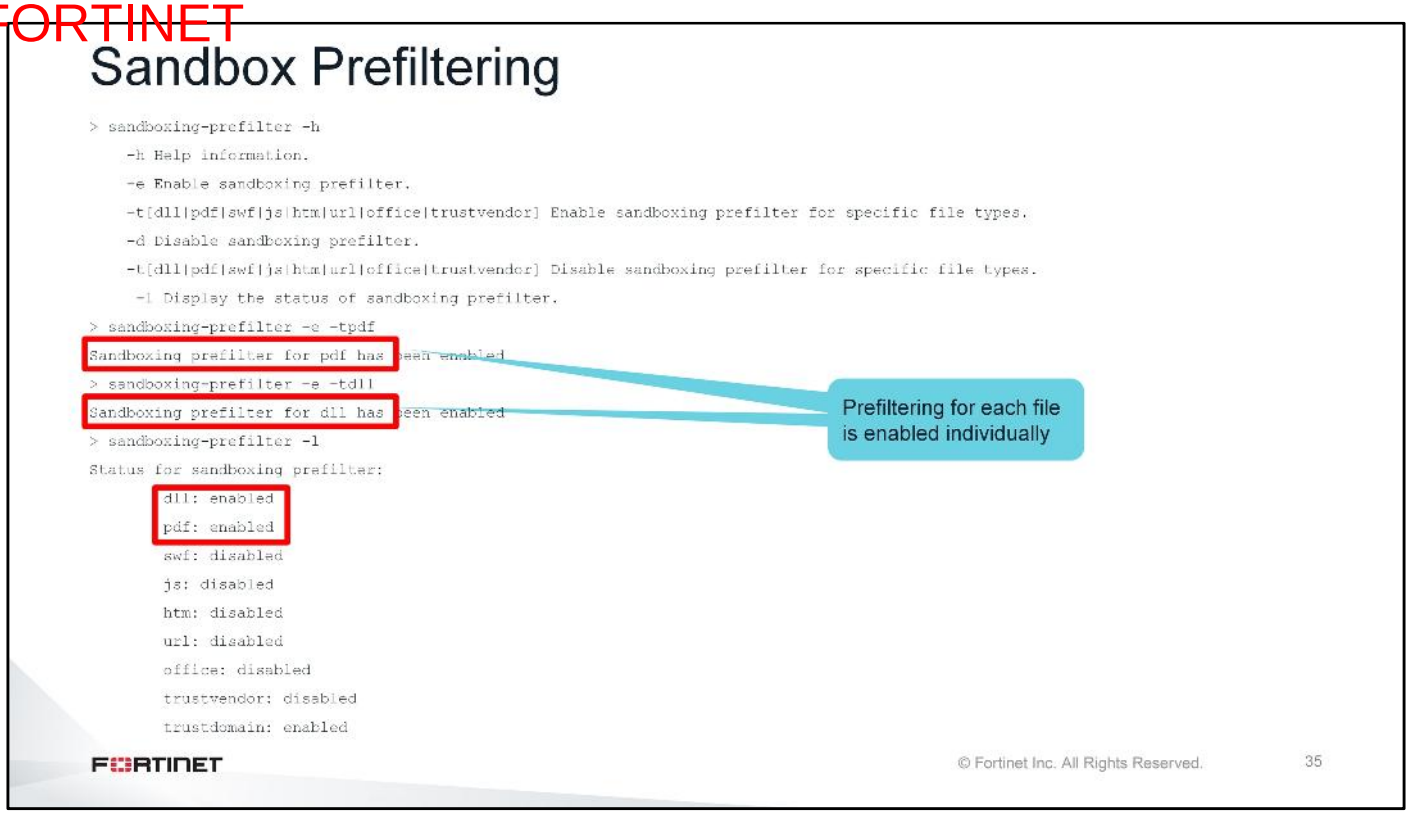


The second section of the **Scan Profile** allows you to define file extensions and VM image associations. This means that specific files will be sandboxed by the associated VM image. To assign a file to a VM image, the following conditions must be true:

- The file type has to be configured to enter the job queue (first section of the scan profile)
- The VM image clone value should be a non-zero number

File types are grouped into different categories. You can select the entire category, or individual file extensions. You can also define custom extensions.

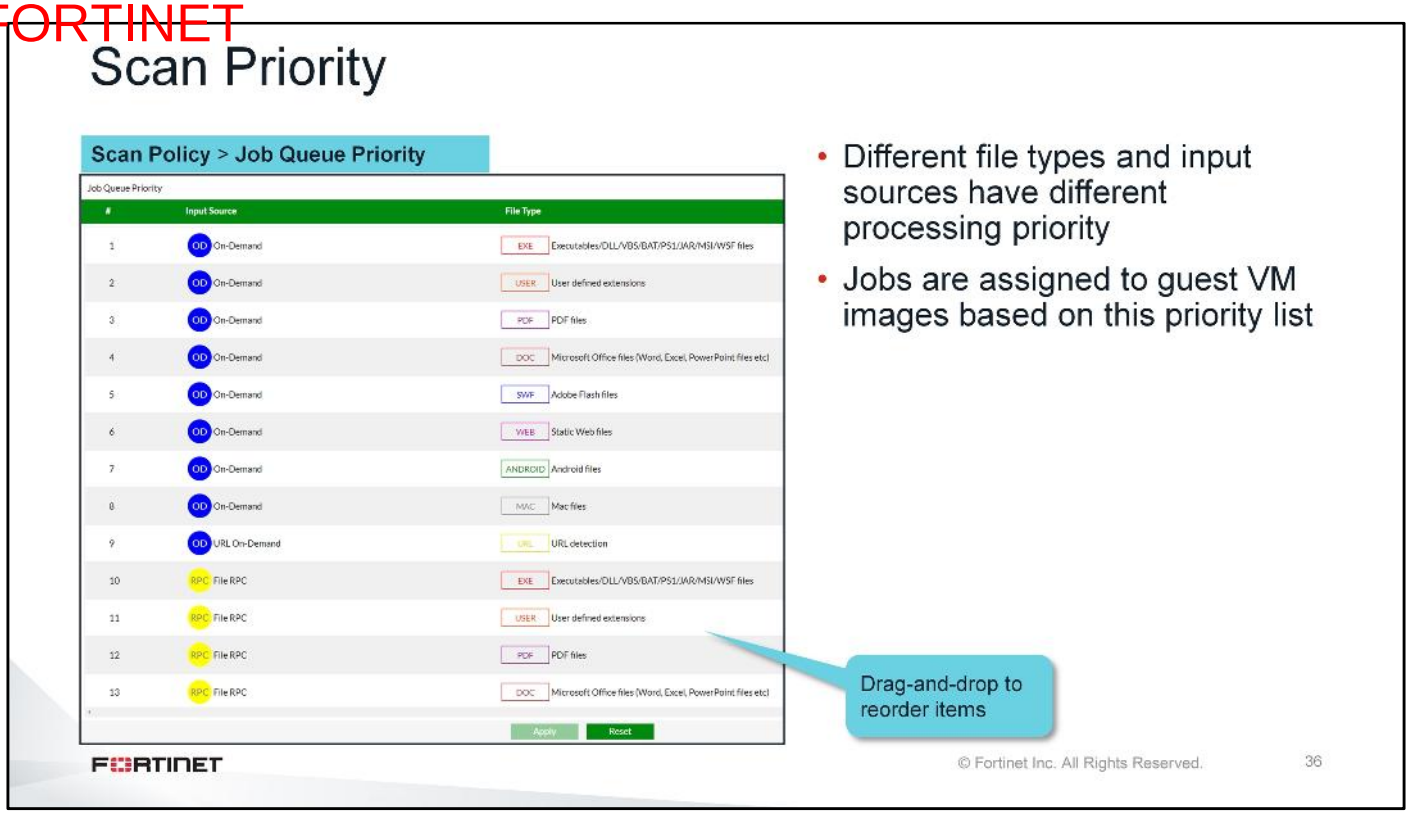
After any change to the scan profile, the VM images are reinitialized, which can take a while. When VMs are being reinitialized, they are not available for sandboxing. It is recommended that you make changes to the scan profile during a maintenance window.



Sandbox prefiltering is another feature that can greatly save resources by reducing the amount of files and URLs submitted into the sandbox job queue. If the sandbox prefilter is enabled, files and URLs are scanned first by an advanced analytic engine, and only suspicious ones are submitted to the sandbox queue. The sandbox prefilter validates specific conditions, and checks for suspicious behavior in files and URLs. If a file or URL matches the conditions below, it will be submitted for sandboxing:

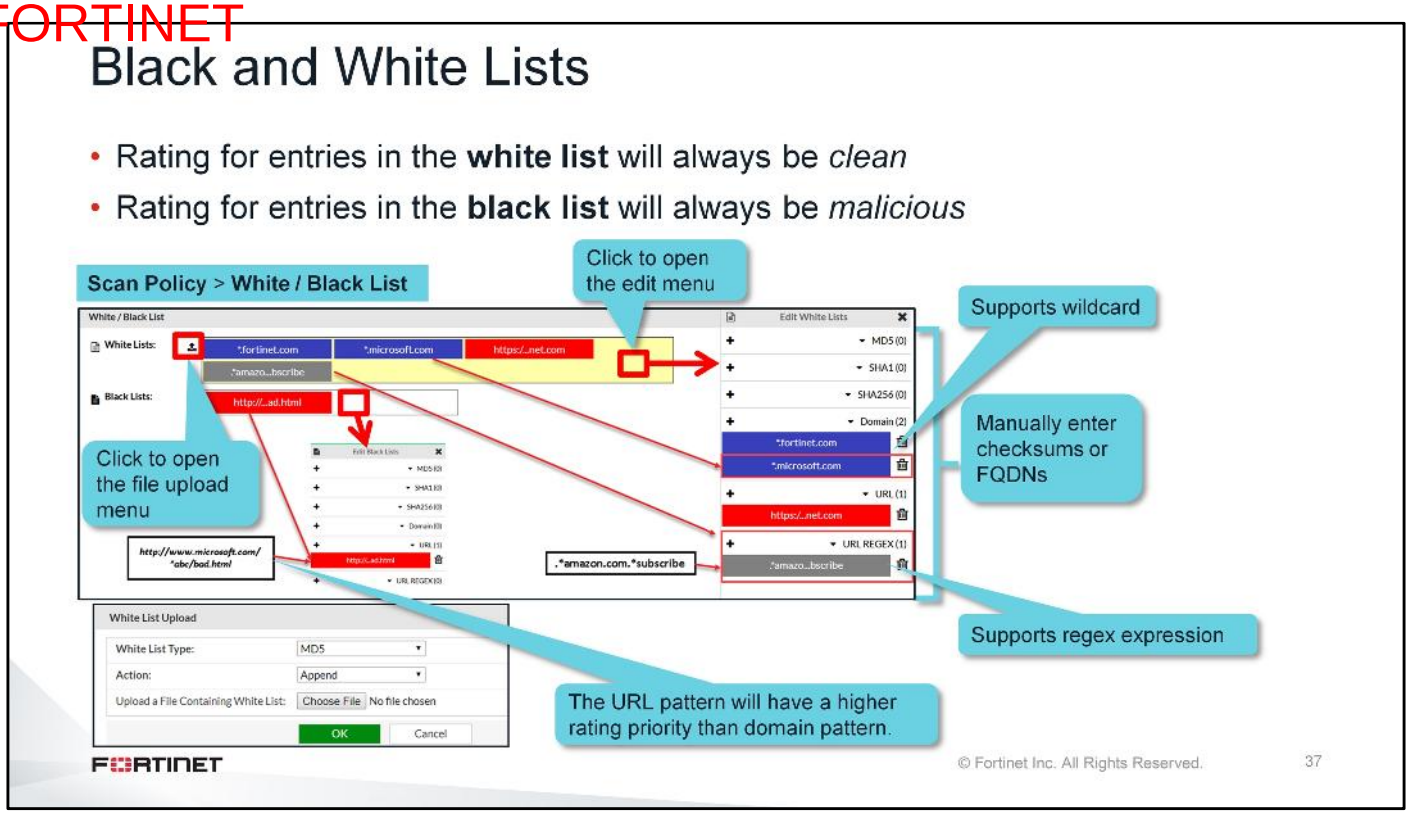
- Proper dependencies exist in the guest VM image for DLLs to be executed, and that DLL file is not corrupted
- Active scripts exist in PDF, and Office files
- Callback behavior in SWF files
- Suspicious behavior in JS and HTML files
- Macros in Office files
- URL rating is Unrated, Phishing, Malicious, Hacking, Spyware, or Spam

Sandbox prefiltering is disabled by default. The CLI commands shown here control the sandbox prefilter behavior. It can improve the system's scan performance; however, if resource utilization is *not* an issue in your FortiSandbox, it is recommended to keep this feature disabled.



Different file types and input sources have different processing priority. Jobs are assigned to guest VM images based on this priority list. This means if a VM image is configured to scan two different file types, the files with higher priority will be scanned first, and only when that list is empty will FortiSandbox start assigning the lower priority files to the VM. Therefore, it is recommended, at least from an efficiency standpoint, that you assign file types with higher priority to one VM image, and files with lower priority to another VM image. This ensures lower priority file types are not ignored in the event there is an influx of higher priority files.

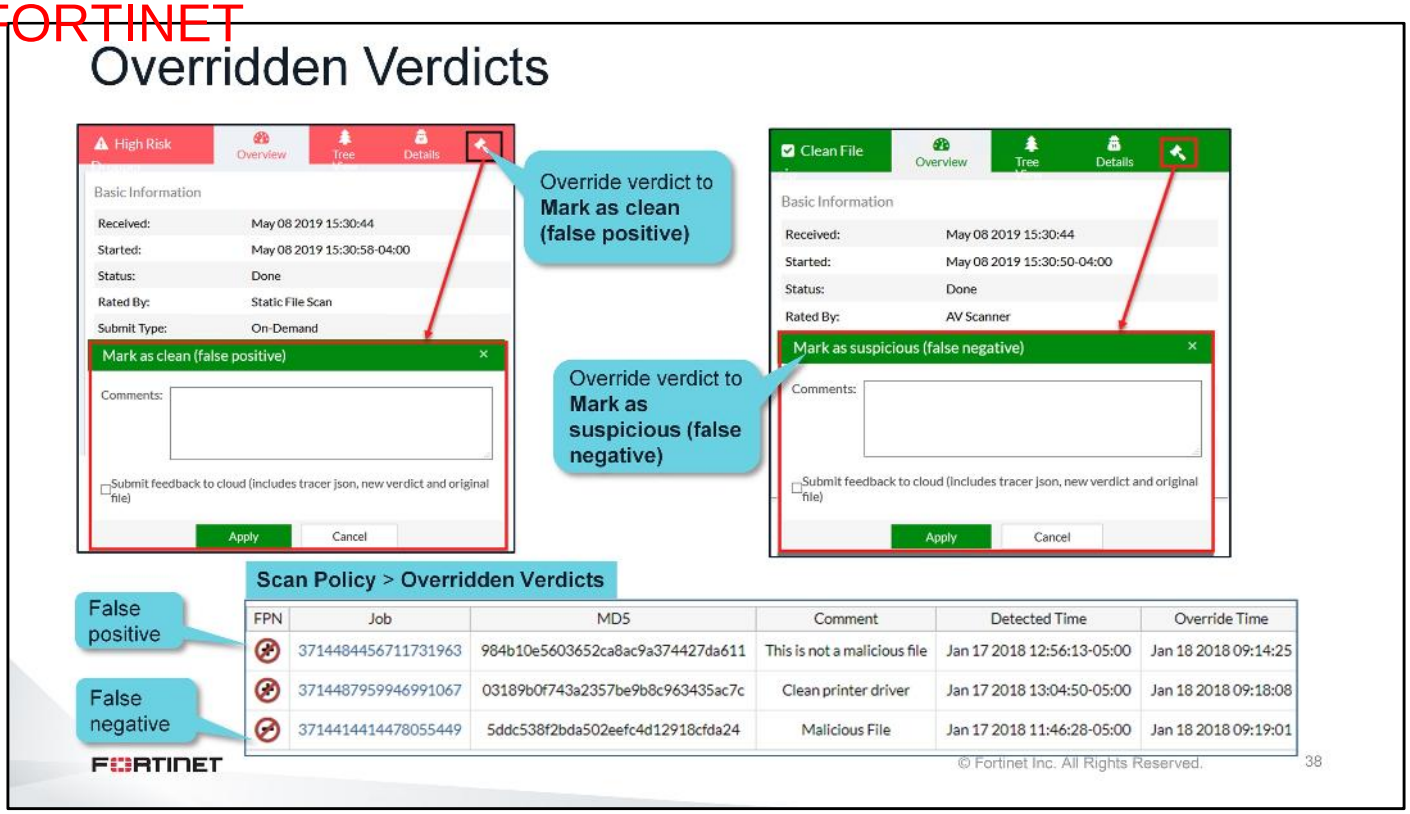
The priority list can be modified by dragging and dropping entries.



The black list can help improve scan performance by immediately generating a *malicious* rating on matched files. The white list allows you to address false positive detection events by rating matching files as *clean*. Since these static lists are applied at the cache check stage, FortiSandbox processes them early in the scanning cycle. FortiSandbox now supports regex expression. For example, if a user adds `.*amazon.com.*subscribe` to the white list, then all subscription URLs from `amazon.com` will immediately be rated as clean. In this way, all such subscription links won't be accidently opened inside a VM and become invalid.

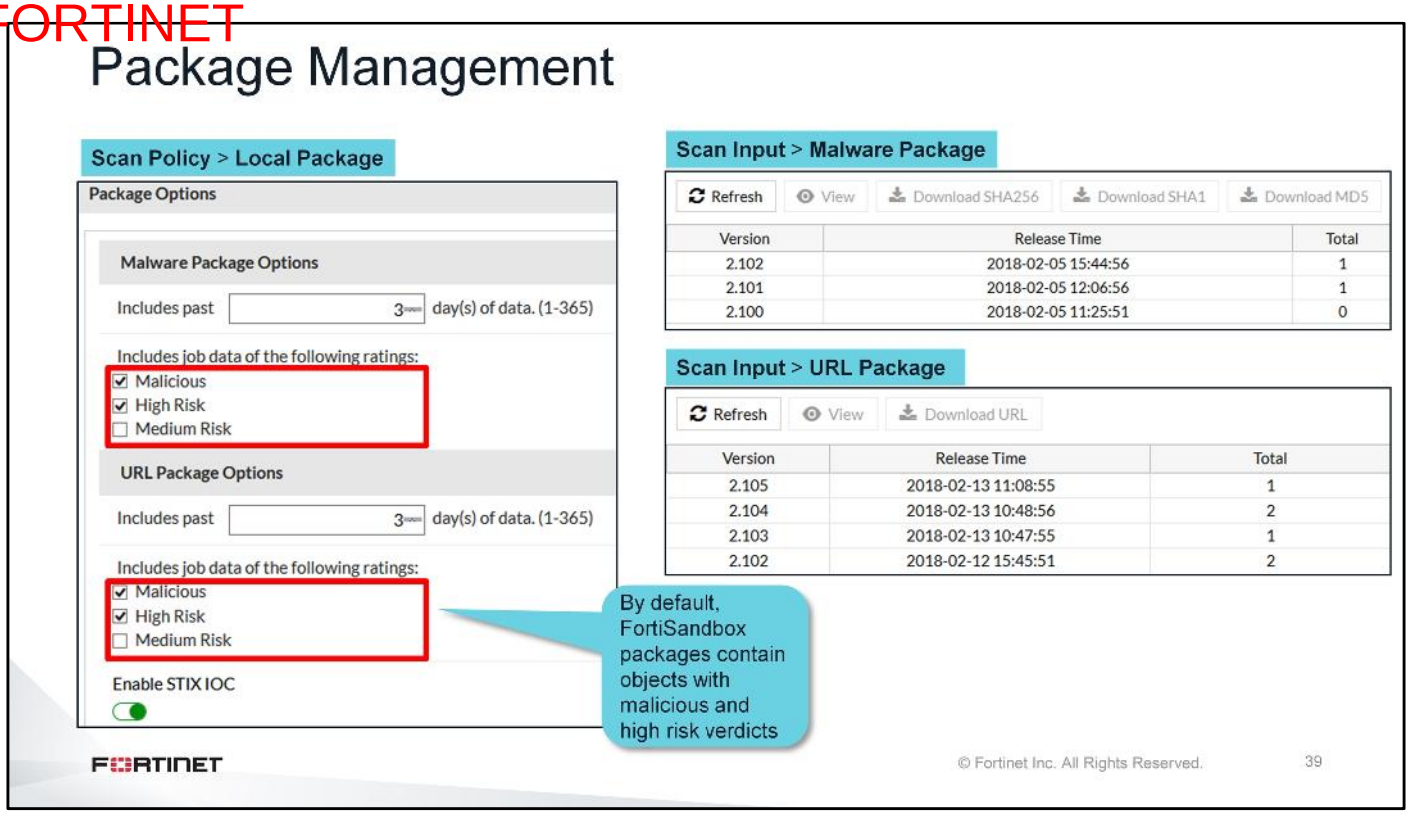
The lists contain checksum values in MD5, SHA1, or SHA256 format, as well as domain FQDNs where files can be downloaded from. You can manually enter the checksums one by one, or upload a large list of checksums in a file. FortiSandbox supports the wildcard format for the domain field. For example, if you add `*.microsoft.com` to the domain white list, all files downloaded from the subdomains of `microsoft.com` will be rated as *clean*. However, the URL pattern has a higher rating priority than domain pattern. If you add `http://www.microsoft.com/*abc/bad.html` to the URL black list, then any file from that URL will be rated as malicious, even though you have whitelisted `microsoft.com` in the domain filed.

Be very careful about adding entries to the white list. Matched entries bypass all scanning. So, if you're adding white list entries to your FortiSandbox, you should be absolutely certain that files of that type are safe.



You can also override a file's verdict using a scan job report. The **Overridden Verdicts** page displays all entries that have been manually marked as false positive or false negative. These verdicts are applied in the cache check step of FortiSandbox's inspection sequence, so marking a scan job report as either false positive or false negative should be done only if you're absolutely certain. Mistakenly marking a scan verdict as false positive can potentially allow dangerous malware to bypass detection.

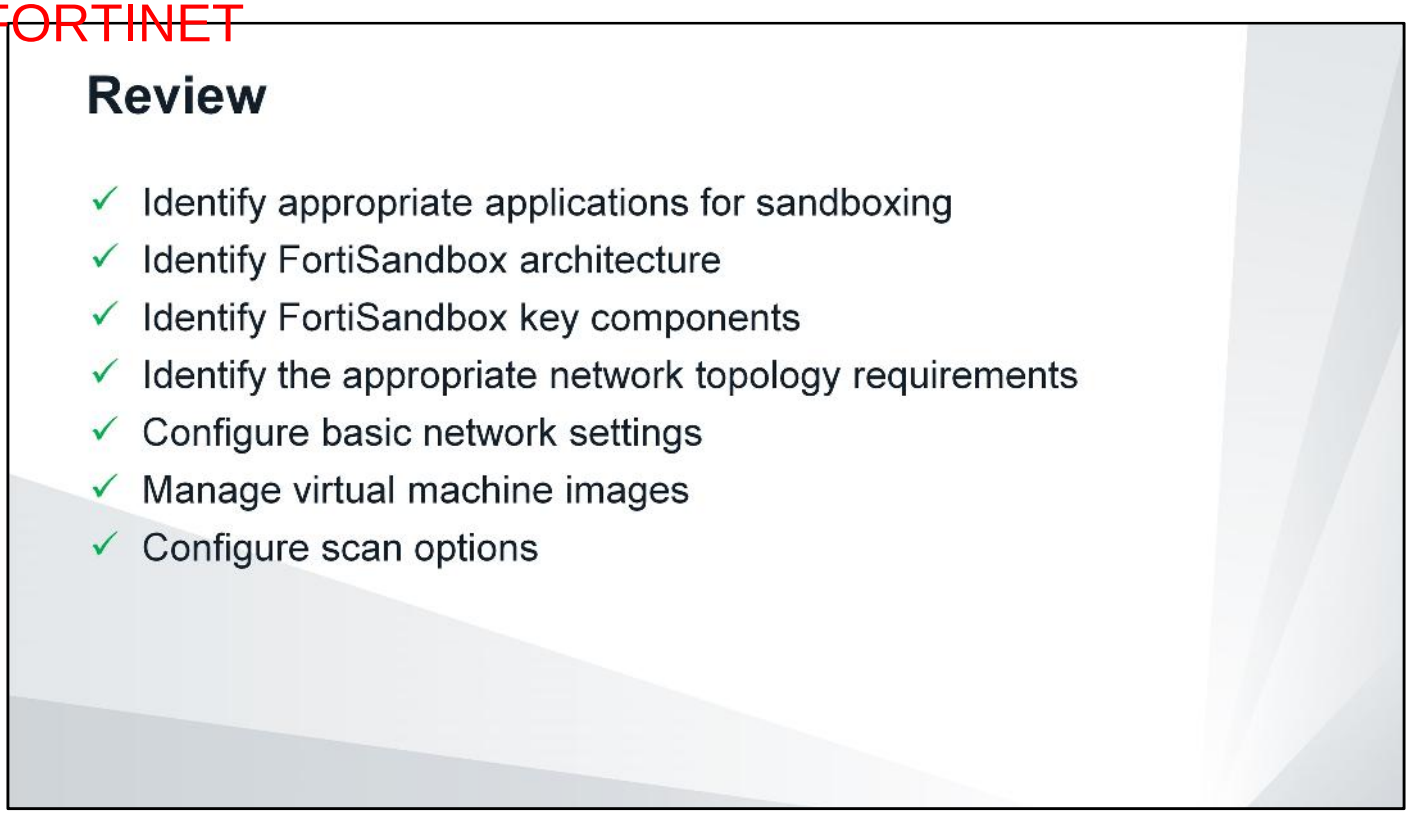
Administrators can delete an entry on the **Overridden Verdicts** page, if a verdict has been marked erroneously.



FortiSandbox can generate antivirus and URL packages from scan results, and distribute them to various Fortinet devices. A new package is generated every time FortiSandbox detects a new malware whose rating falls into one of the enabled package options ratings (Malicious, High Risk, or Medium Risk). Low risk objects are not included in these packages.

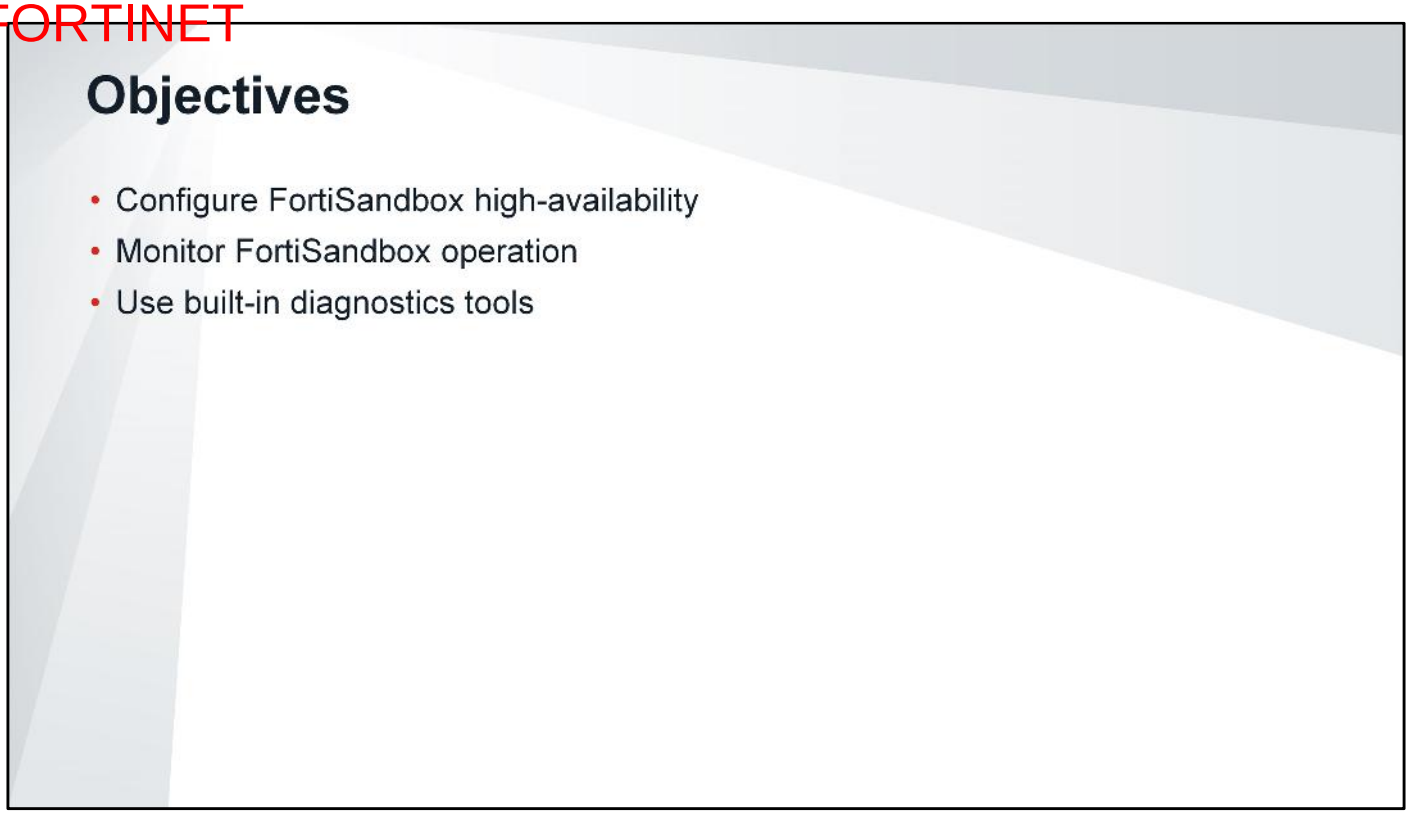
The supported Fortinet device sends a package request to FortiSandbox every two minutes. The request includes its installed version. The FortiSandbox receives the request, then compares the version with its own local package version number. If the received version is different, FortiSandbox sends the latest package to the device.

The malware package contains hashes for all suspicious files detected by FortiSandbox. The URL package contains direct URLs for suspicious webpages detected by FortiSandbox.



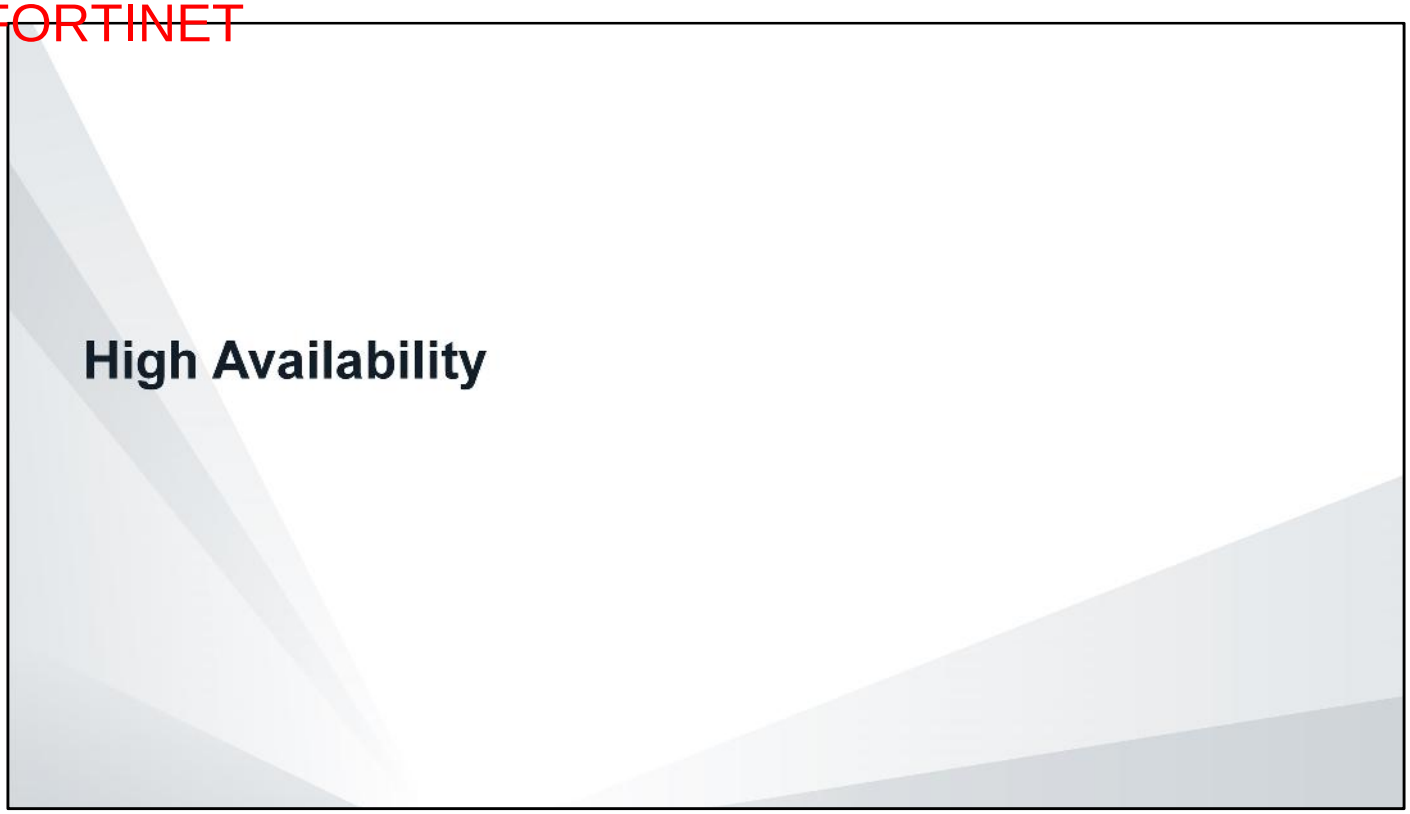
All the objectives covered in this lesson are listed on this slide.

In this lesson, you will learn about high-availability on FortiSandbox. You will also learn about built-in diagnostic tools available on FortiSandbox for troubleshooting and monitoring it's performance.

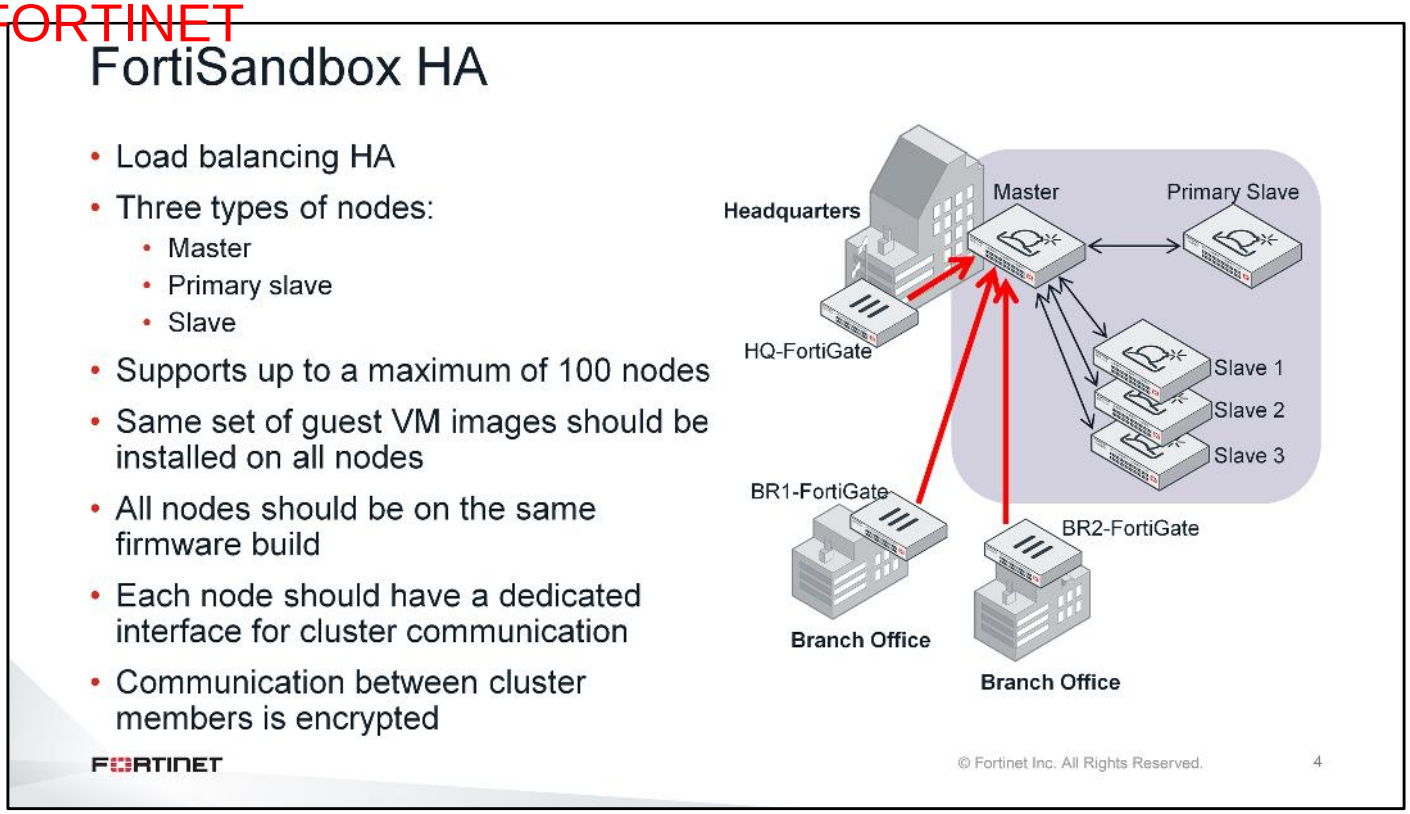


After completing this lesson, you should be able to perform the objectives shown on this slide.

By demonstrating competence in basic FortiSandbox concepts and configuration requirements, you will be able to design, configure, and maintain a FortiSandbox deployment in your own network, that is suitable for your security needs.



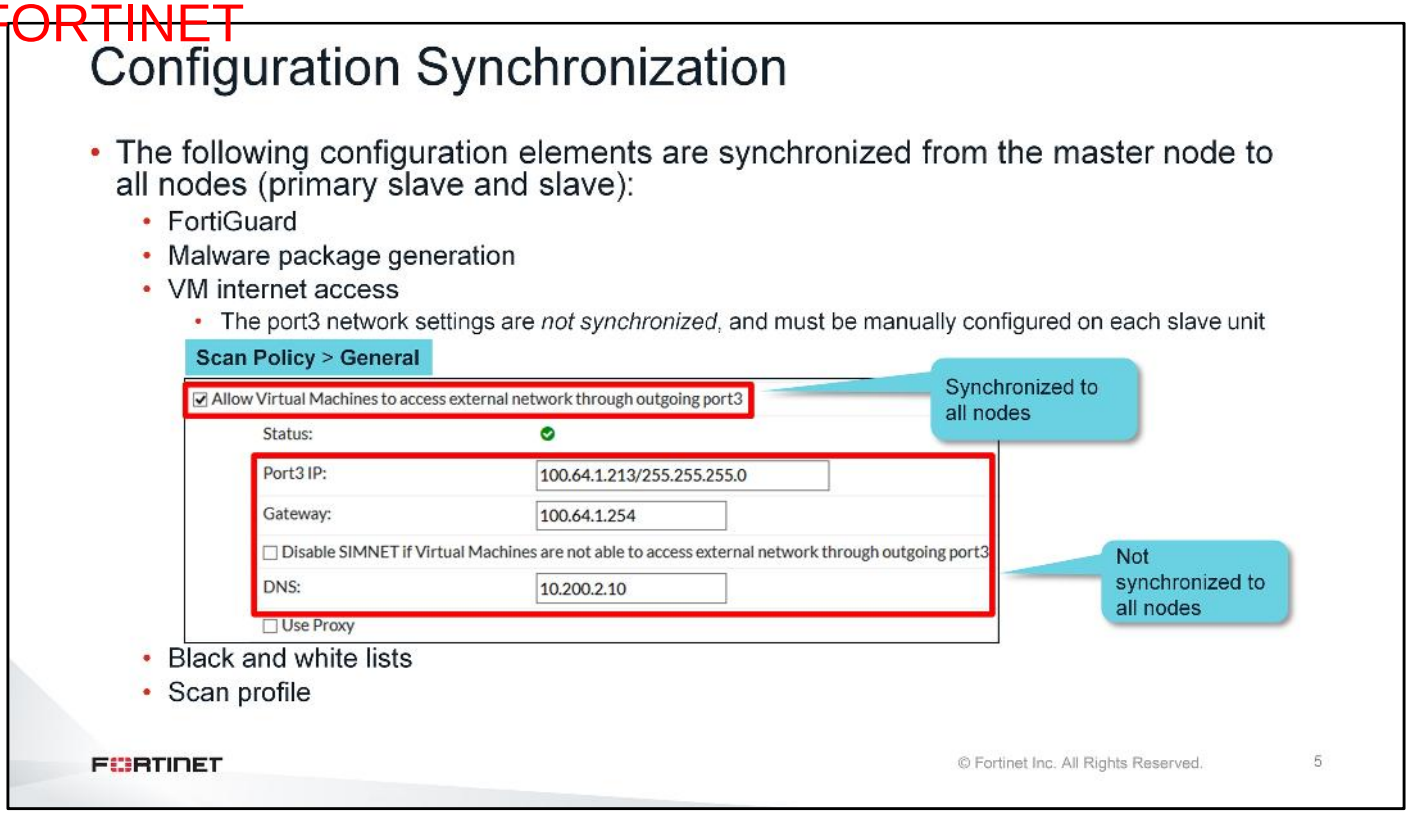
In this section, you will learn about FortiSandbox high-availability (HA) cluster requirement, functionality, and configuration.



FortiSandbox HA provides both load balancing and failover protection. There are three types of nodes in a cluster:
- Master
- Primary slave
- Slave

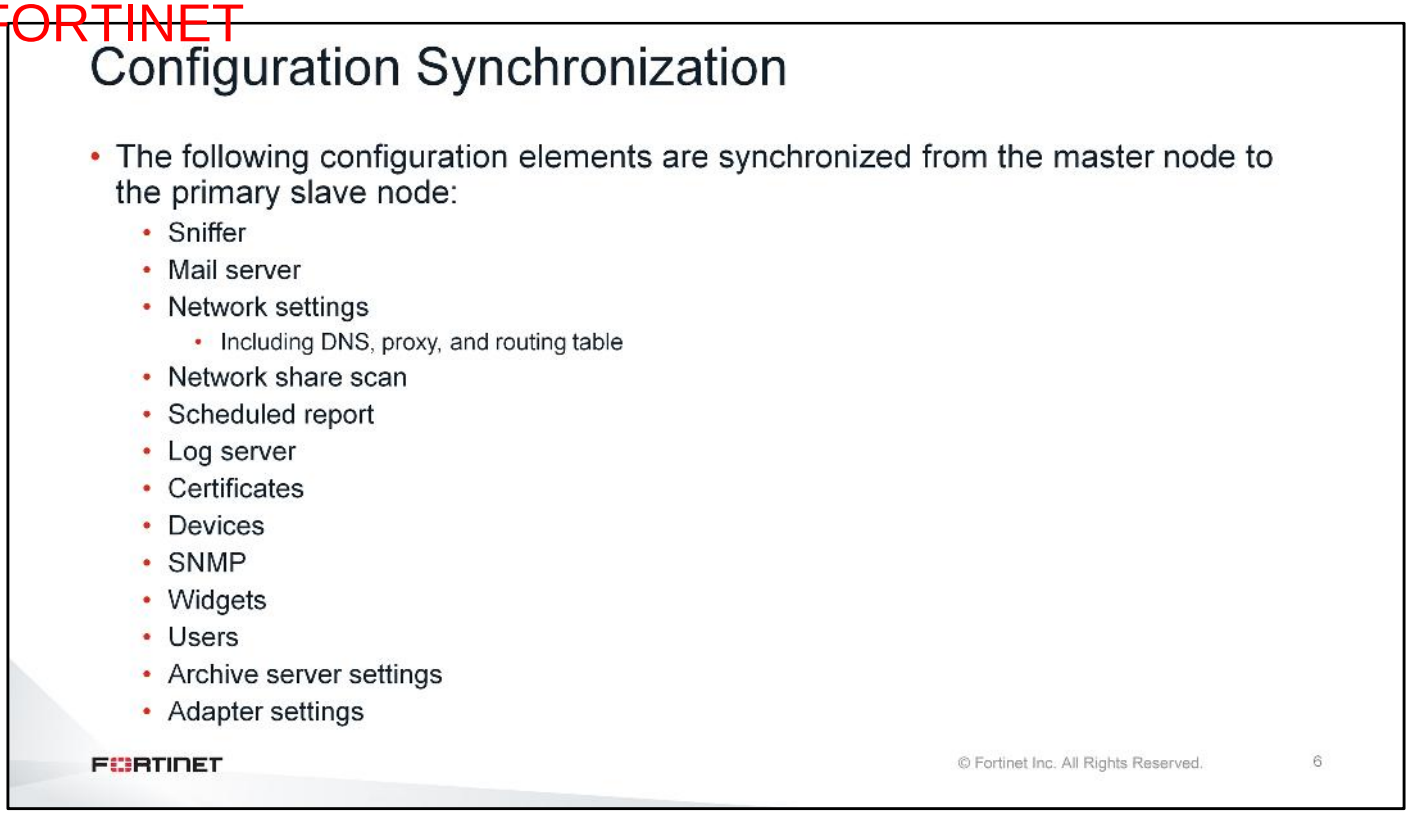
As well as normal scanning duties, the master node also manages the cluster, distributes jobs, and gathers the verdicts. Devices integrate with the master node. All scanning-related configurations, such as scan profiles, and sandbox pre-filter, are done on the master node. The master node propagates the configuration to all other nodes in the cluster. The primary slave node provides failover protection for the master node. It monitors the master node, and stands ready to take over in the event the master node fails. The master, and primary slave nodes should be the same model. The slave nodes provide load balancing. The master node distributes scan jobs to the slave nodes. After scanning completes, the slave nodes send the verdict back to the master node. Slave node models in an HA cluster do not need to match. The communication between cluster members is encrypted.

Before configuring a FortiSandbox HA, you must ensure:
- Each node has the same set of guest VM images
- All nodes are on the same firmware build
- Each node has a dedicated interface for internal cluster communication



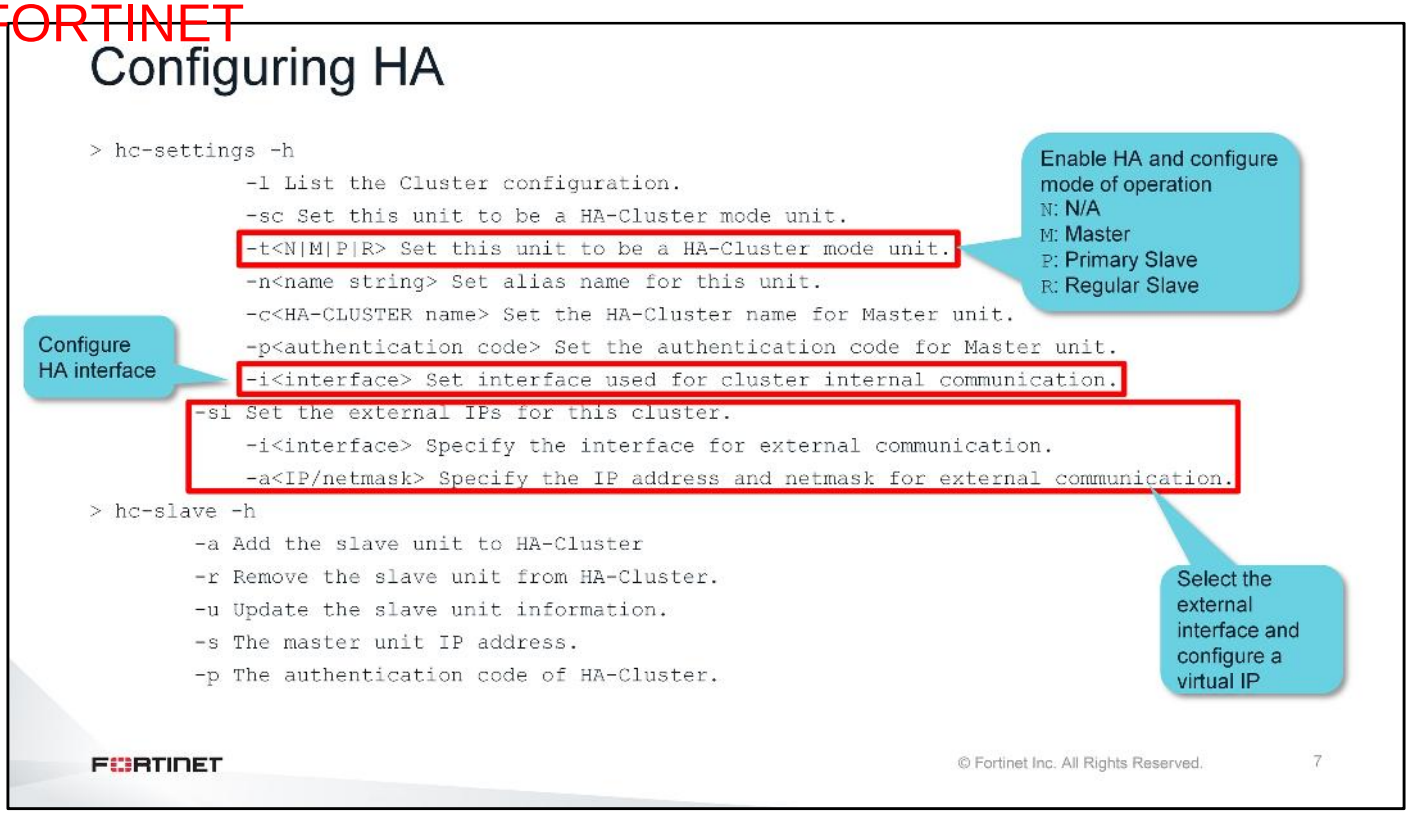
The following configuration elements are synchronized from the master node to all other nodes. This includes the primary slave, and all slave nodes. These configuration elements should be managed only on the master node:

- FortiGuard
- Malware package generation
- VM internet access setting, but not the interface, gateway, and DNS settings.
- Black and White lists
- Scan profile
- Yara rules
- Job cleanup schedule



The master node also synchronizes the following configuration elements to the primary slave node:

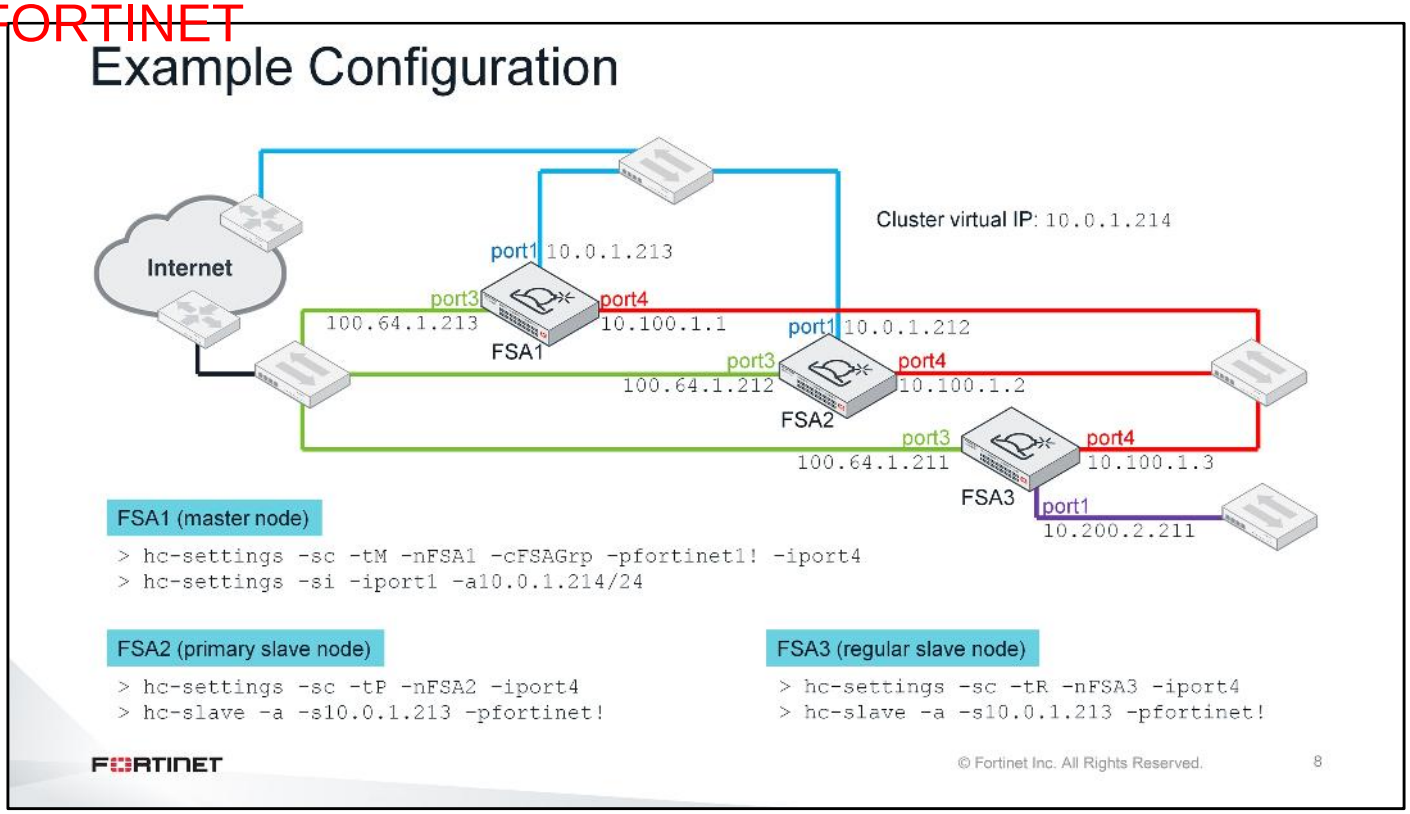
- Sniffer
- Mail server
- Network settings, which includes DNS, proxy, and routing table
- Network share scan
- Scheduled report
- Log server
- Certificates
- Devices
- SNMP
- Widgets
- Users
- Archive server settings
- Adapter settings
- Others (login disclaimers)



HA configuration on FortiSandbox is done on the CLI. The main HA cluster CLI commands are `hc-settings`, `hc-slave`, and `hc-status`

You use the `hc-settings` command and options to configure the main HA settings, such as enable HA, and to configure the node's mode of operation, node alias, group name, group password, and the HA interface. You must also configure an external interface for external communication and an IP address that will be used as a virtual IP for the whole cluster. Devices will interact with the cluster using this virtual IP.

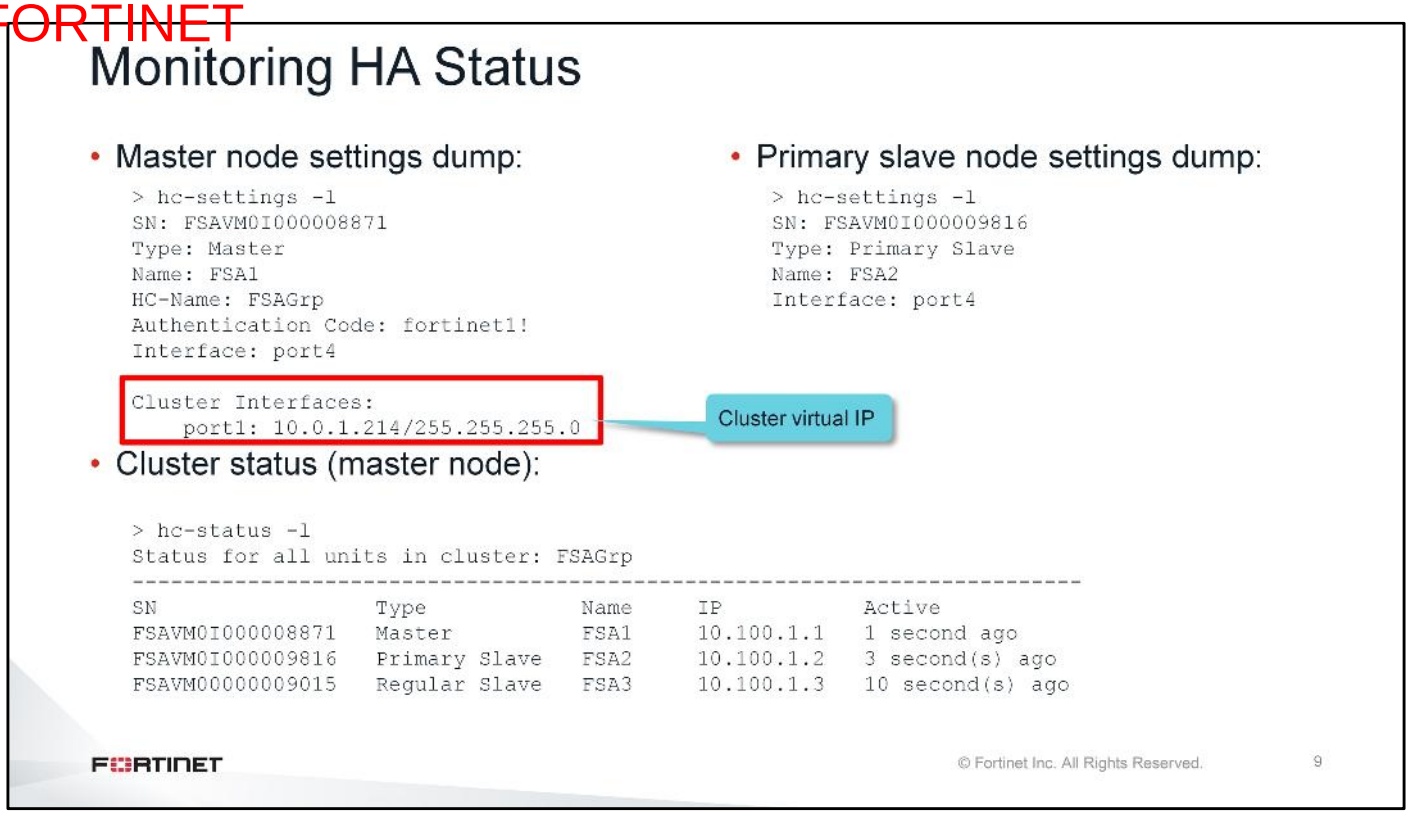
The `hc-slave` command and options are used to join the primary slave, and regular slave nodes to the cluster.



This slide shows an example topology with the relevant CLI commands.

The physical cabling on the master node and primary slave node should be identical; that is, all active interfaces should belong to the same respective subnets. The slave node's management port may be connected to a different subnet, but the HA communication interface (port4 in this example) must be connected to the same Layer 2 network as the master and primary slave nodes.

You must configure the HA group name, password, and the virtual IP only on the master node. After those are configured, the primary slave, and regular slave nodes can be added to the group using the commands shown here on this slide.

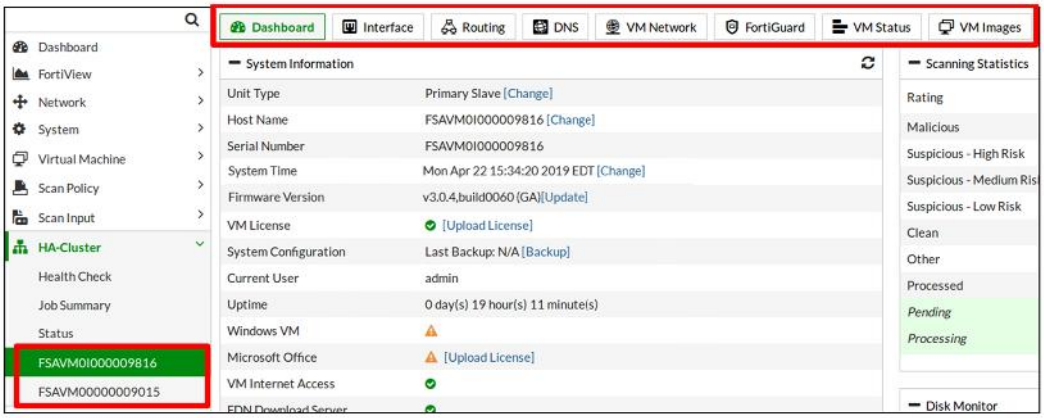


The CLI commands used to dump each node's cluster settings, and list all clustered node's status, are shown here.

The `hc-status -l` command on the master node produces the complete list of clustered nodes in the group. The other nodes (primary slave and regular slave) do not have the same visibility into the cluster. They only see the master and primary slave nodes.

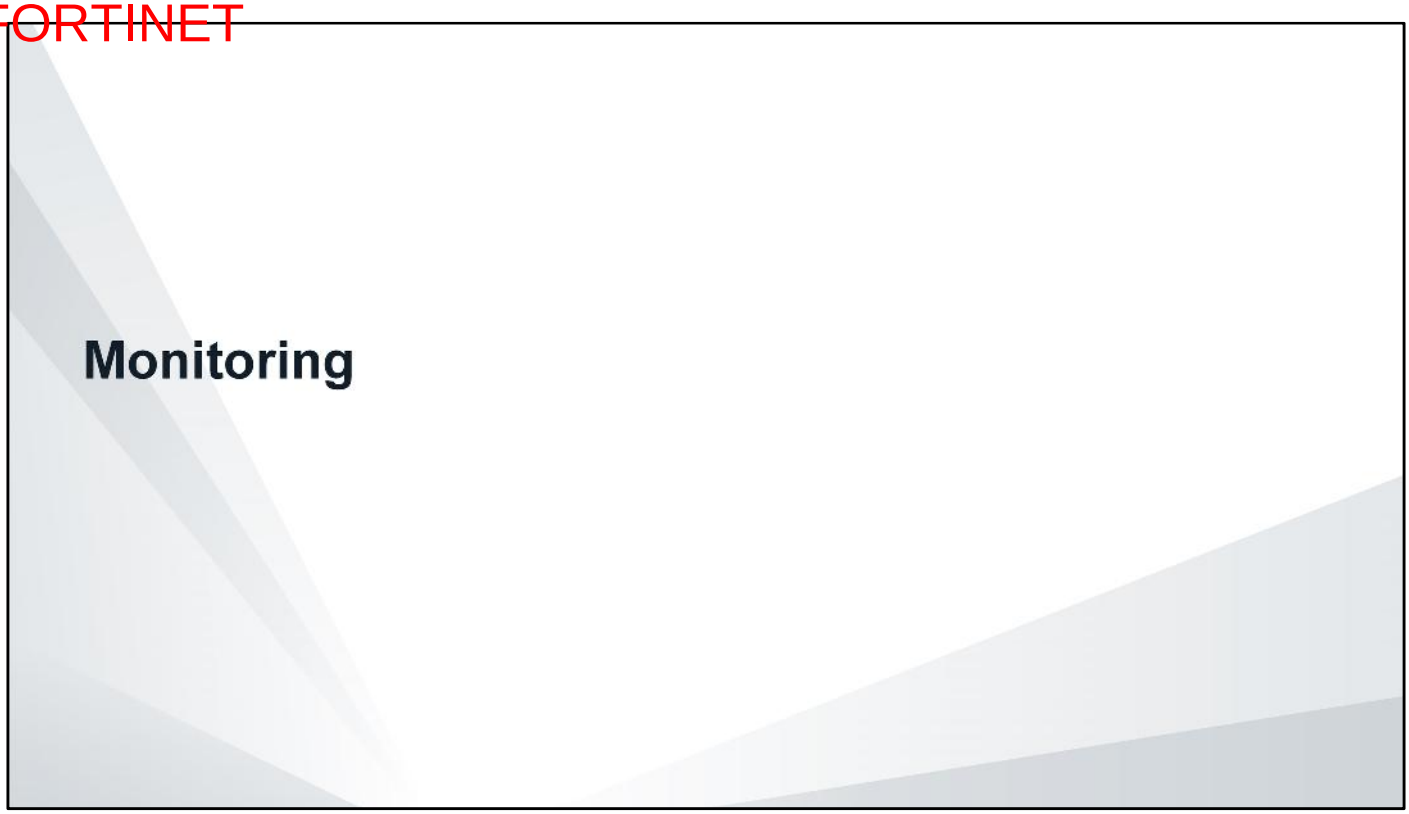
Cluster Management

- Each cluster node's management GUI is accessible through it's network access port (port1)
- Each cluster node can also be managed from the master node

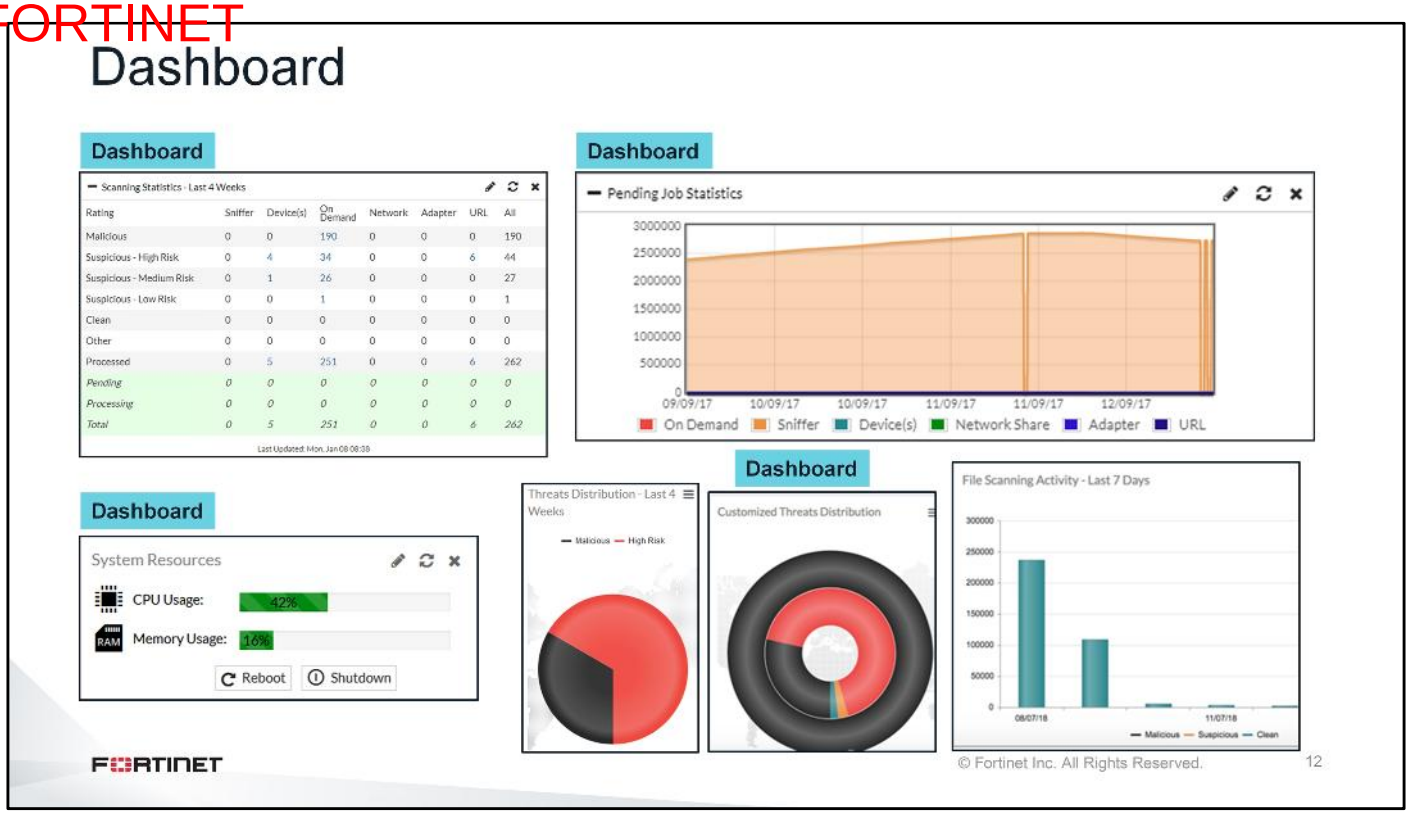


10

Cluster node management options are centralized on the master node. Each node's configurable settings are accessible from the master node's management GUI.



In this section, you will learn the various methods of monitoring available on FortiSandbox.

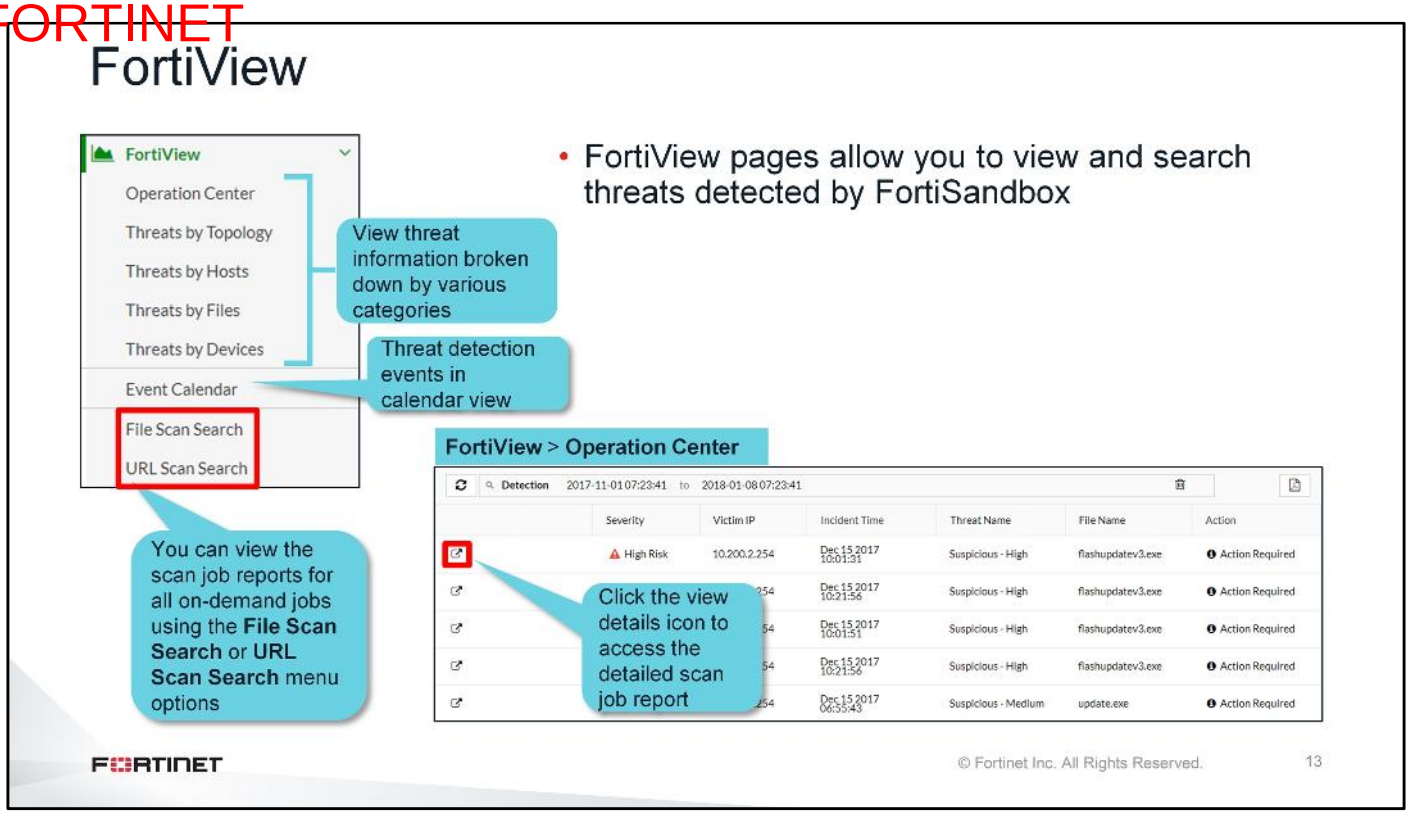


There are various widgets on the FortiSandbox **Dashboard** page that you can use to monitor various aspects of FortiSandbox's performance.

The **Scanning Statistics** widget displays information about the files that have been scanned over a specific time period. The default period is 24 hours, but you can modify this to display data for up to four weeks. This widget is updated in real time. Information about files being scanned or pending scanning will be reflected in this widget.

Another performance monitoring tool is the **Pending Job Statistics** widget. This displays the total number of pending jobs for all input sources. It is good practice to monitor this information, specifically for high volume FortiSandbox deployments. It may reflect a need to modify the scan profile, if the pending job queue keeps increasing.

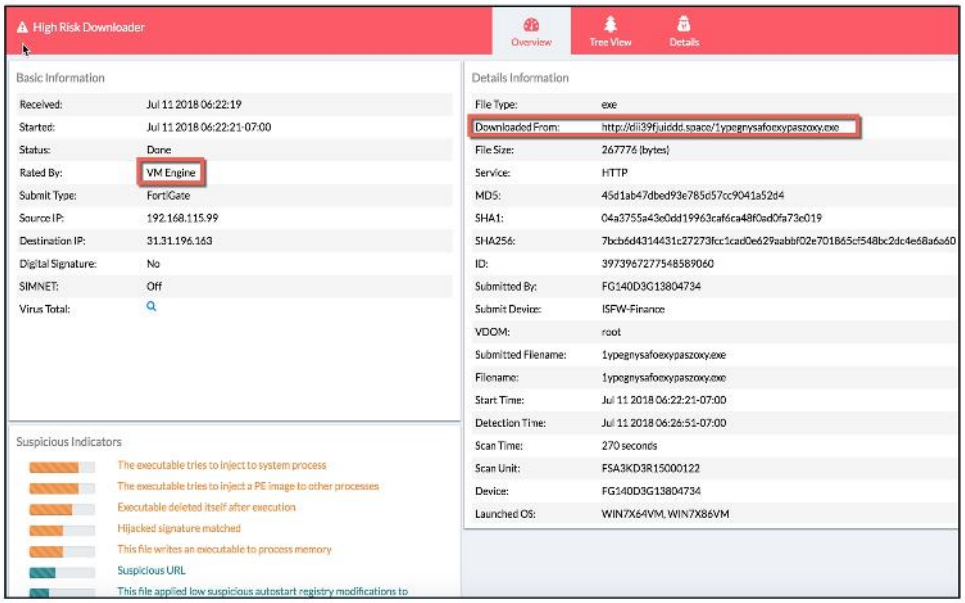
There are other useful widgets such as **Threat Distribution, Customized Threat Distribution**, **File Scanning Activity**, and more.



The **Operation Center** view lists all detected threats in a given time period. This view displays severity levels, victim IP addresses, incident time, and threat name. If the detected virus' name is not available due to there not being an active signature in the antivirus database, the malware's severity will be used as its threat name. The information in the **Action** column provides you and your security team to track any action taken in response to the incident. In **Operation Center** view, you can click the **View Details** icon to access the detailed scan job report.

The rest of the FortiView pages show the same threat information, but broken down by various categories, including topology, hosts (usernames, email addresses, or end-user devices), files, and input devices. The **Event Calendar** view shows threat detection events in a calendar view. The **File Scan Search** and **URL Scan Search** pages allow you to search specific files or URLs using various search criteria.

Scan Job Report Overview



 14

Every scan event on FortiSandbox generates a scan job report. You can access the scan job reports from the any of the FortiView pages. The scan job report contains all the information used by the rating engine to generate a verdict on a file or URL.

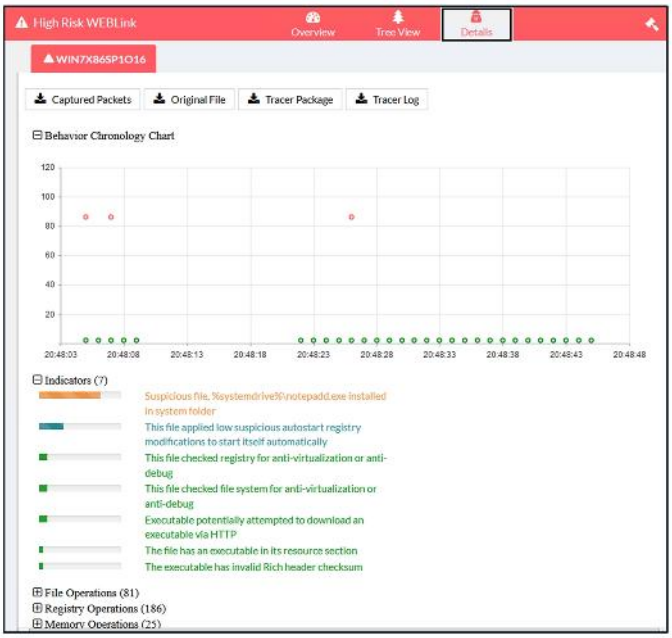
Scan job reports contain very detailed information, especially if the file was sandboxed inside a guest VM. You will learn how to analyze these results in another lesson.

Scan Job Report Tree View

15

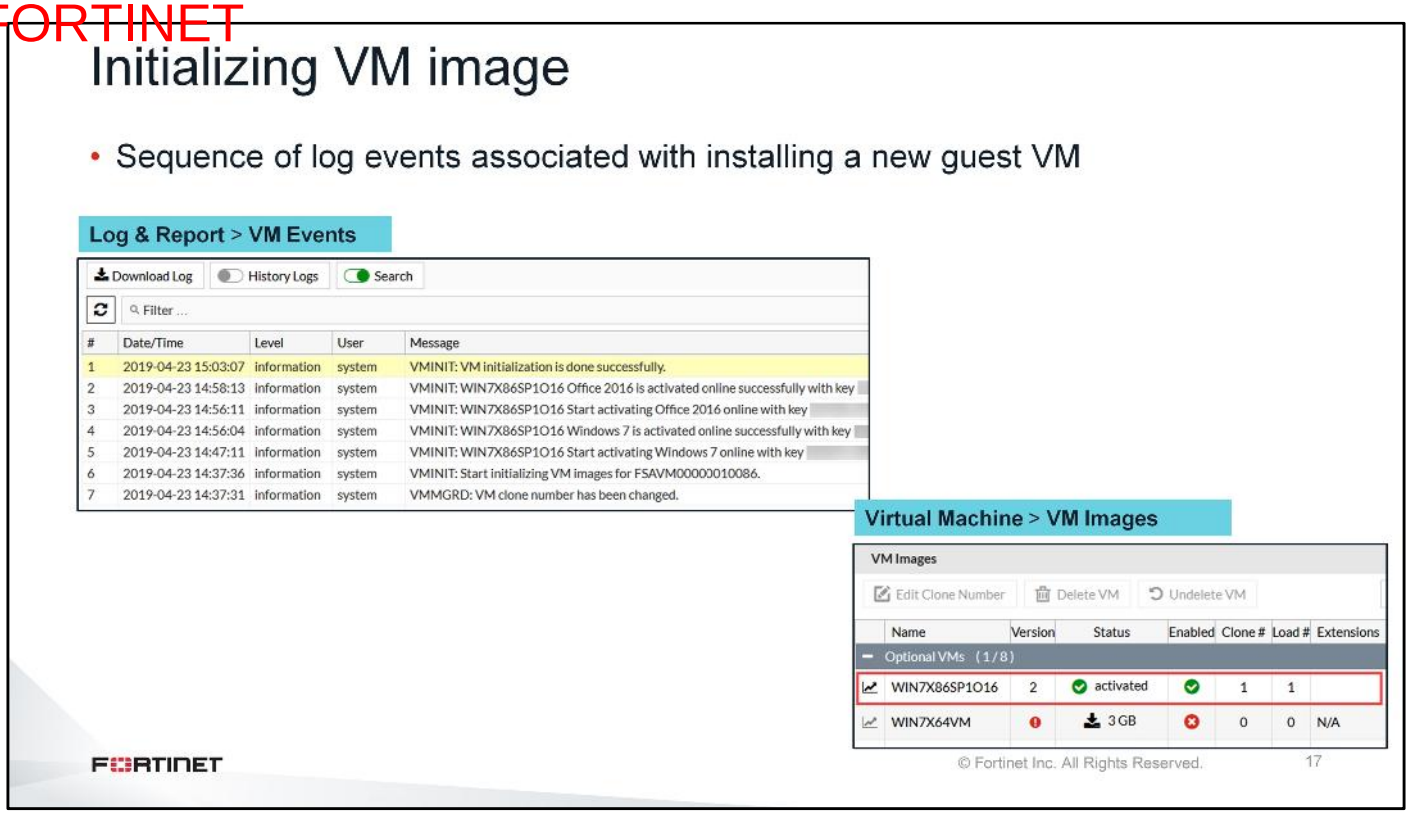
The **Tree View** breaks down the activity for each process when a file was being scanned. You will learn how to analyze these results in another lesson.

Scan Job Report Details



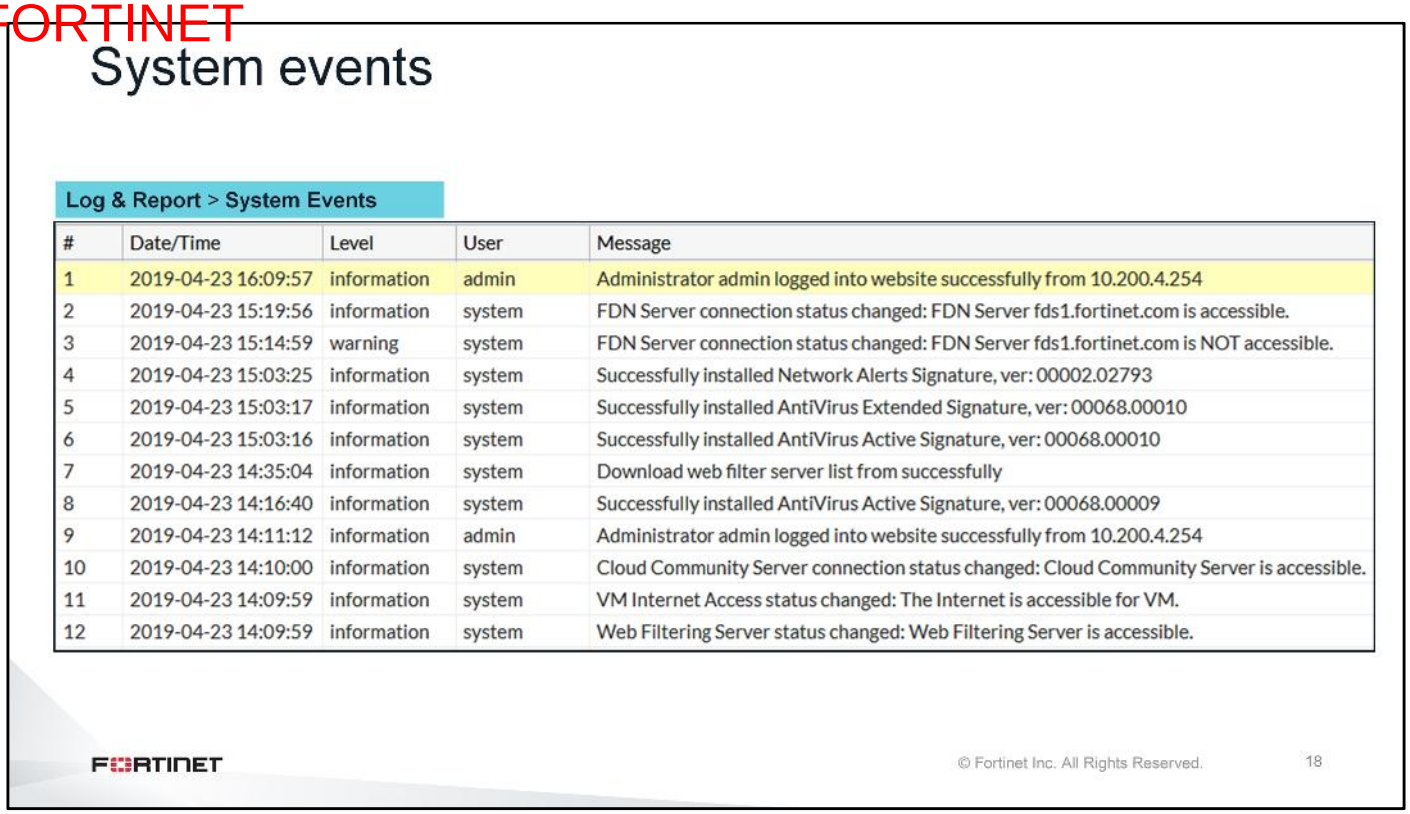
16

The **Details** view shows analysis details for each detection OS that is launched during the scan. The details of each detection OS are shown in a separate tab. The infected OS will have a VM infected icon in its tab title.

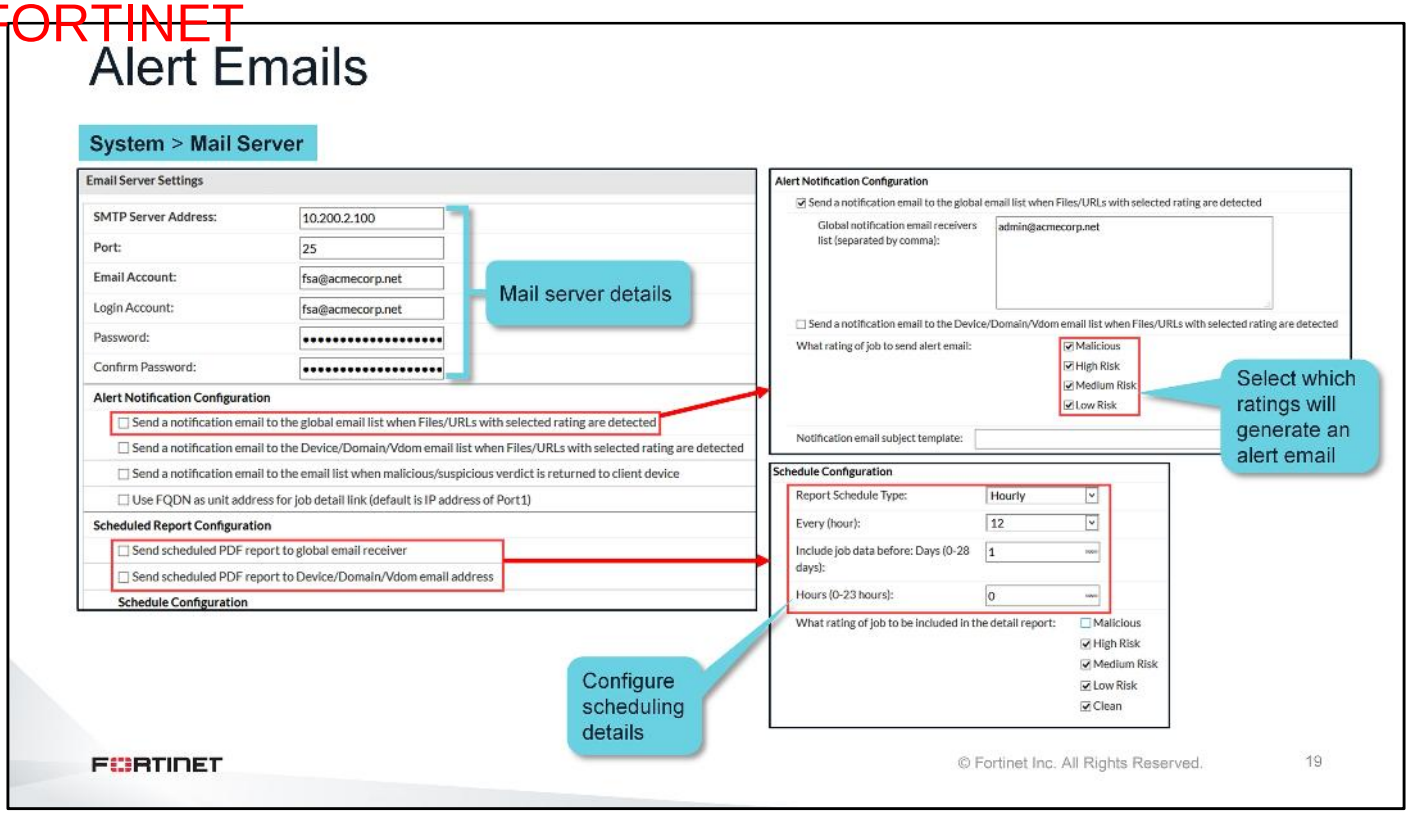


Installing a new guest VM takes a considerable amount of time. You can monitor the status of the installation from **VM Events.** For example, when you install a Windows 7 guest VM with Office 2016, FortiSandbox will validate the license key for Windows and, if you have purchased the license from Fortinet, then it should be successfully activated. After that, it will activate Office 2016. Once the activation is completed, the VM should be initialized successfully.

From **Virtual Machine** > **VM Images** you can check the status of the VM, it should be activated and enabled.



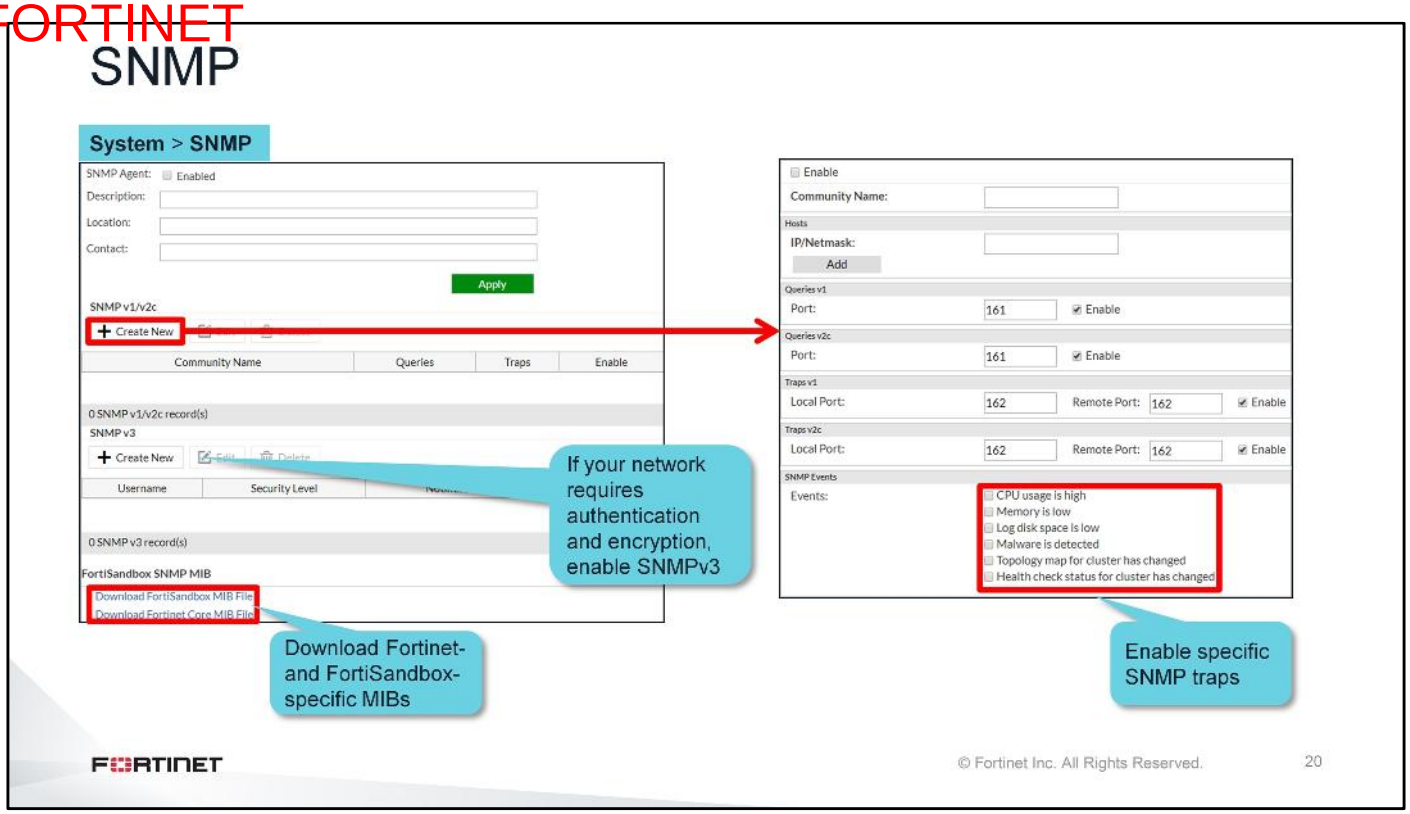
When you initially deploy FortiSandbox, give sufficient time for downloading the FortiGuard databases, such as Antivirus signature database and Network Alerts Signature database. You can verify the such events from **Log & Report** > **System Events**, you can also monitor other activities such as FDN server connection status, cloud community server connection status, web filtering server connection status, VM Internet access status and more.



When malware is detected, it is important that administrators receive proper and timely notification. One method for doing this is through alert emails.

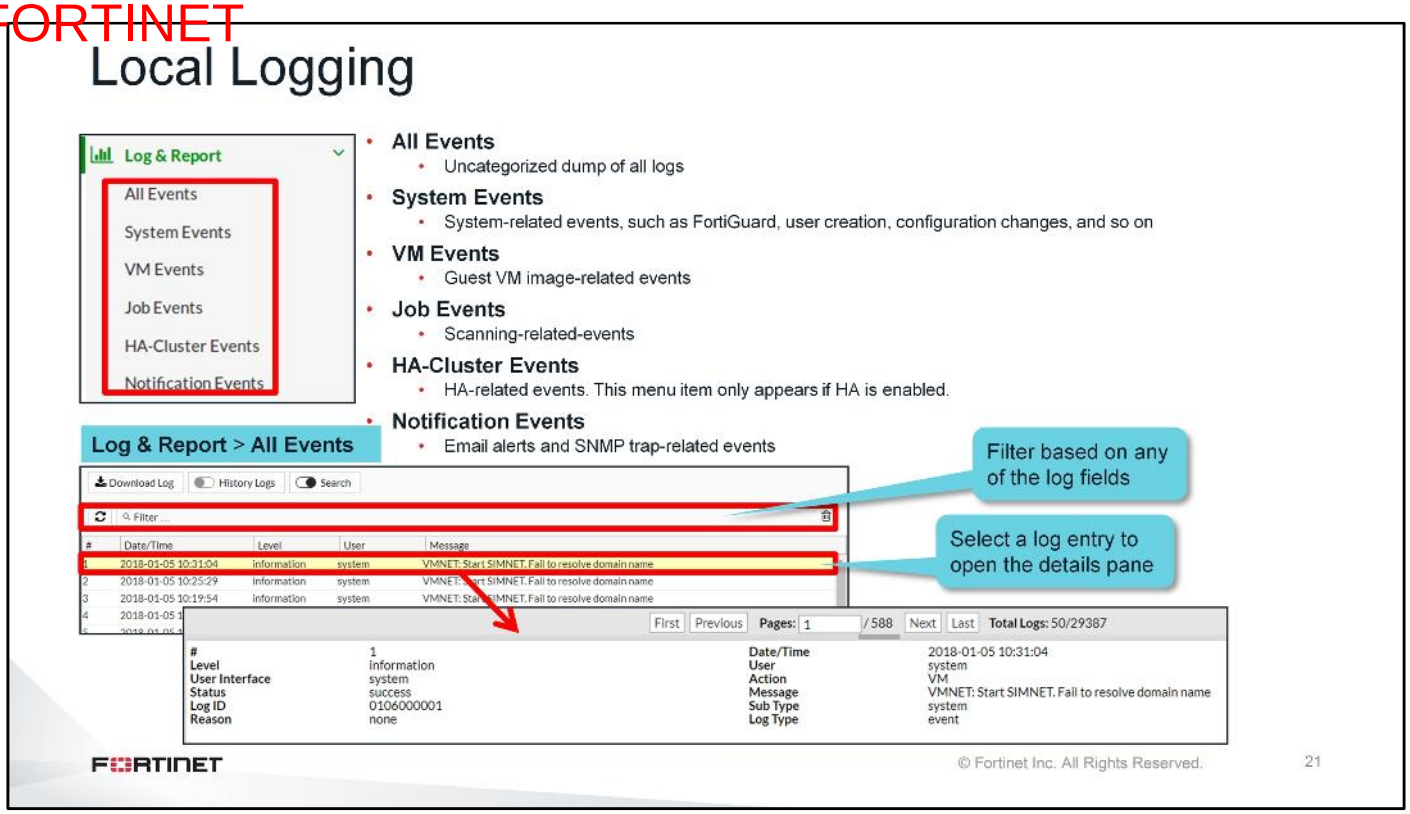
To configure, you must configure the mail server settings and provide the email of one or more administrators to receive the alert notifications. You can also specify which ratings will generate an alert email. Based on this configuration FortiSandbox will generate an alert email for every scan job with that specific rating. Depending on how busy your FortiSandbox is, this can amount to a lot of alert emails.

Another alternative is to configured a scheduled report. You can specify the scheduling details, and select specific ratings. FortiSandbox will generate and send a PDF report based on the scheduling configuration, and ratings which can reduce the frequency of emails being sent out.



You can monitor FortiSandbox with SNMP. FortiSandbox supports SNMPv1, SNMPv2c, and SNMPv3. FortiSandbox can generate traps for high CPU, low memory, low disk space, malware detection, and cluster changes.

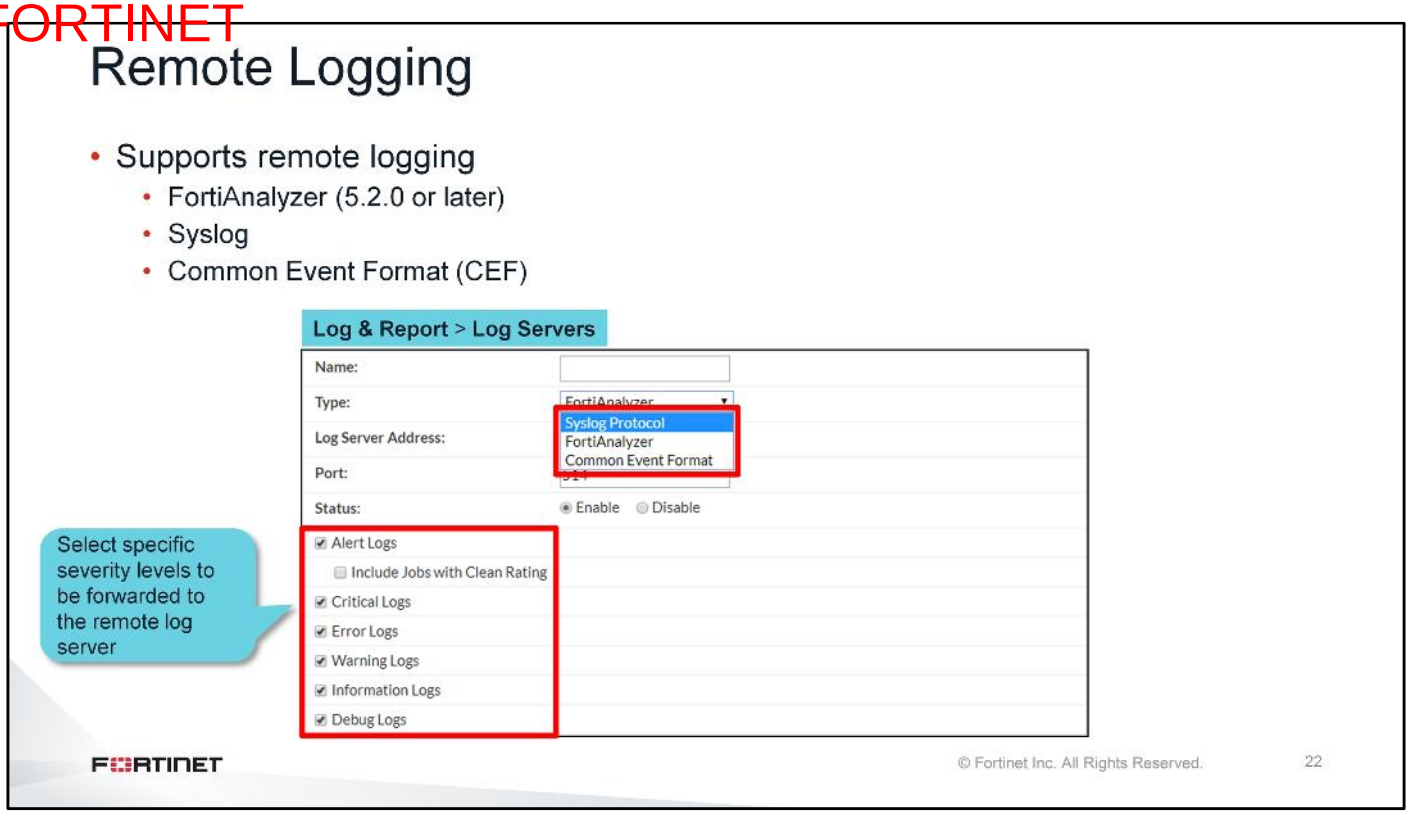
The SNMP configuration page can also provide download links to Fortinet- and FortiSandbox-specific MIB files.



FortiSandbox logs a lot of information. You can view an uncategorized dump of all logs by clicking **All Events**, or by using one of the specific categories shown on this slide. Clicking on a log entry opens the details pane at the bottom of the page which, depending on the log entry, may show more details related to the event. You can also filter logs based on any of the log fields.

This is a summary of the type of logs you may find under each category:

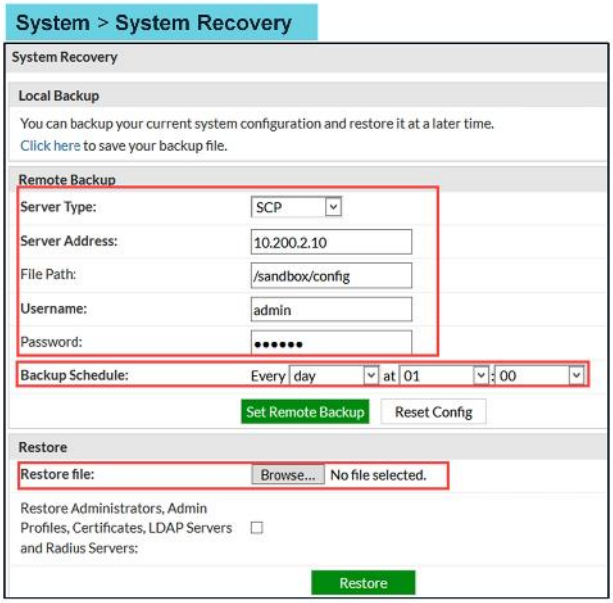
- **System Events**
  - All system-related event logs such as FortiGuard updates, admin account logons, configuration changes, SIMNET status, and more
- **VM Event**
  - All guest VM image-related event logs such as download status, initialization, cloning, and configuration changes
- **Job Events**
  - Tracer engine logs related to jobs, which you can use to trace the scan flow of each file or URL
- **Notification Events**
  - Events related to SNMP traps and alert emails



Logs can be sent to a remote logging server. FortiSandbox supports syslog, CEF, or FortiAnalyzer (5.2.0 or later). You can choose to send all logs, or logs with a specific severity level. By default, FortiSandbox will send logs for only scan jobs with a non-clean rating. You can select **Include Jobs with Clean Rating** to send alert logs for jobs with a clean rating as well.

Remote Backup

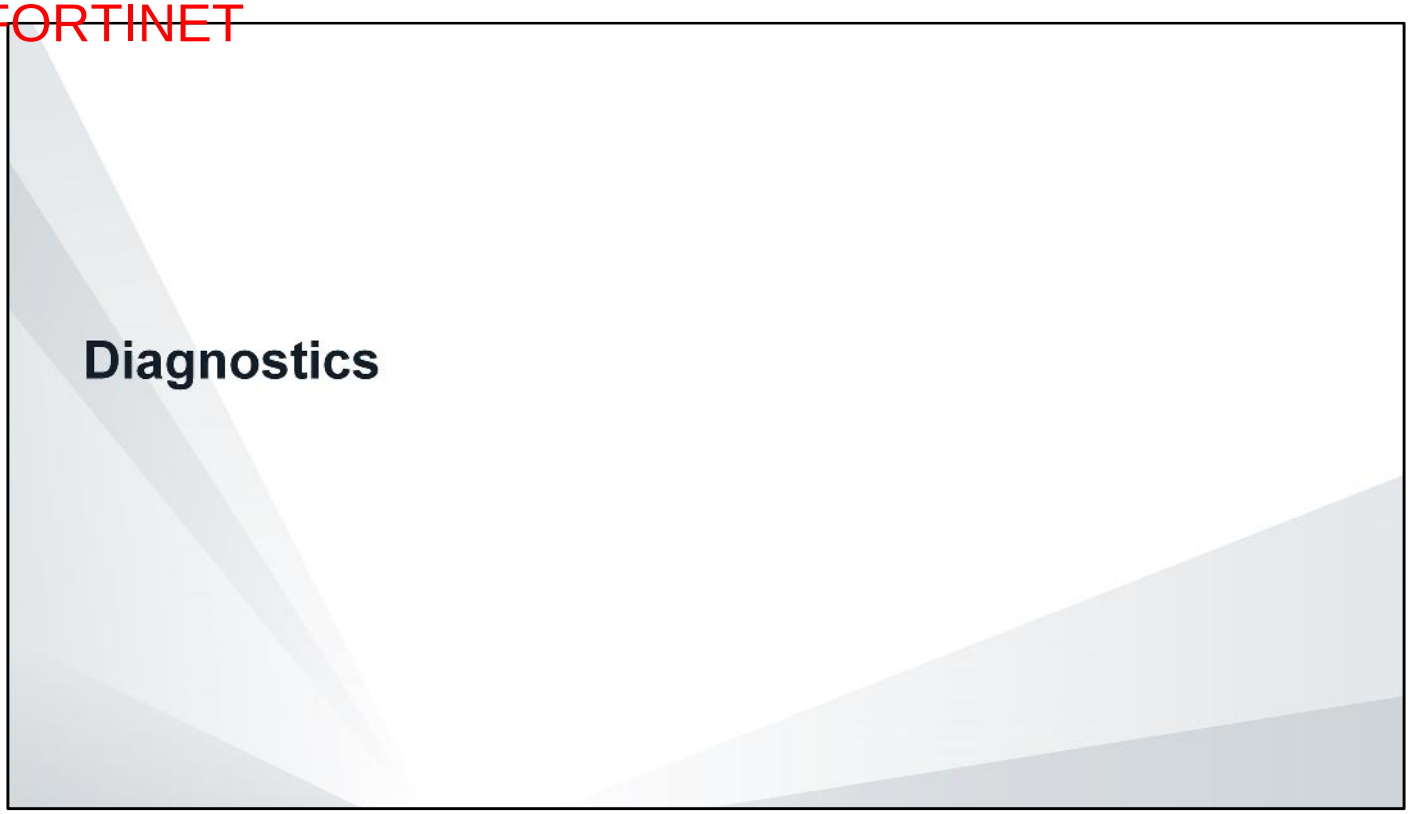
- Schedule automatic configuration backup to a remote server
- Cluster nodes support restore option
- Network and HA configuration is not restored in cluster setup



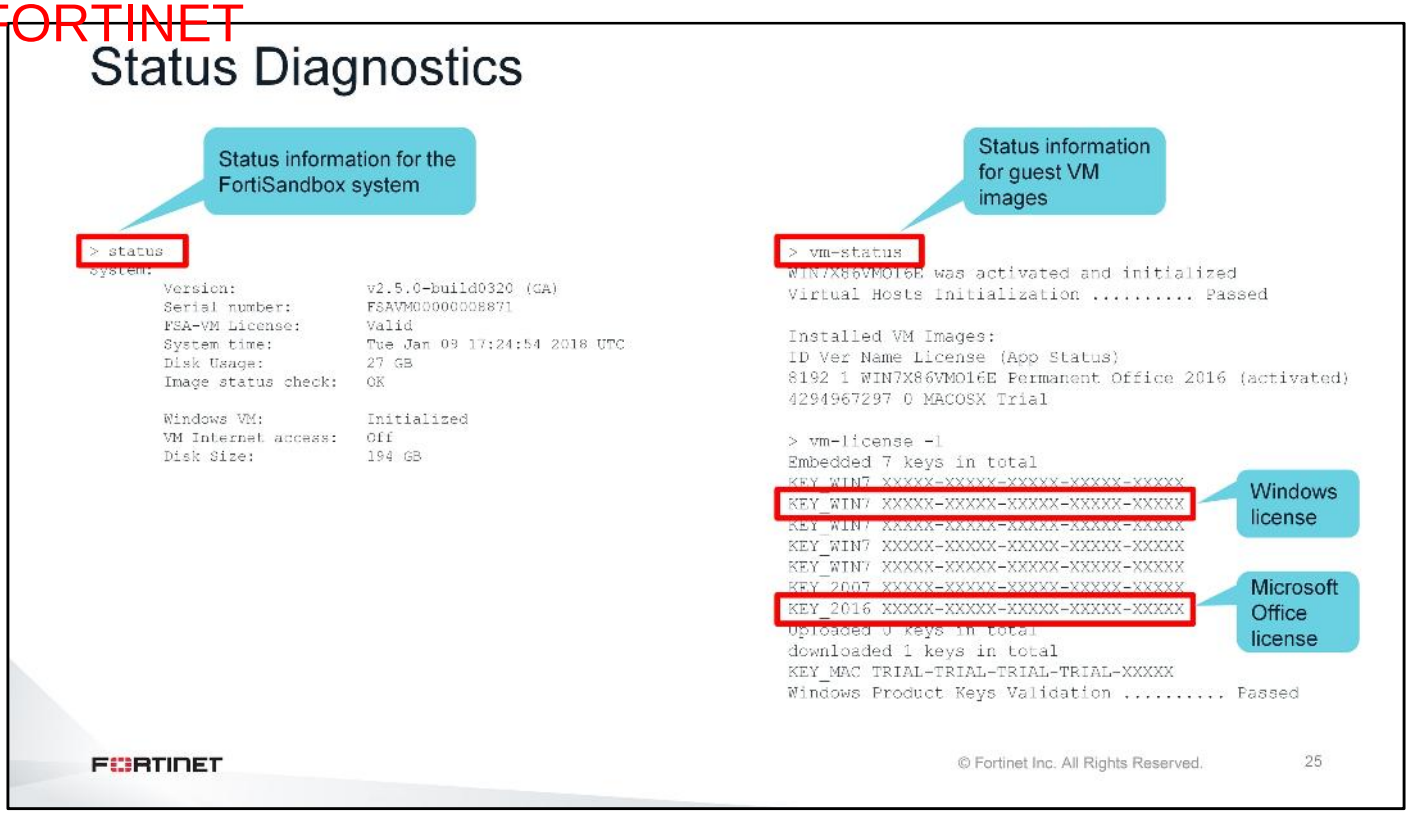
23

You can configure remote backup so that FortiSandbox saves a copy of the configuration file on a remote server. You can set the backup to occur on an hourly, daily, weekly, monthly, or yearly basis.

You can restore the system configuration for a standalone FortiSandbox and cluster node FortiSandbox. To avoid confusing the original configuration file with current cluster settings, FortiSandbox does not restore network and HA-related configuration.

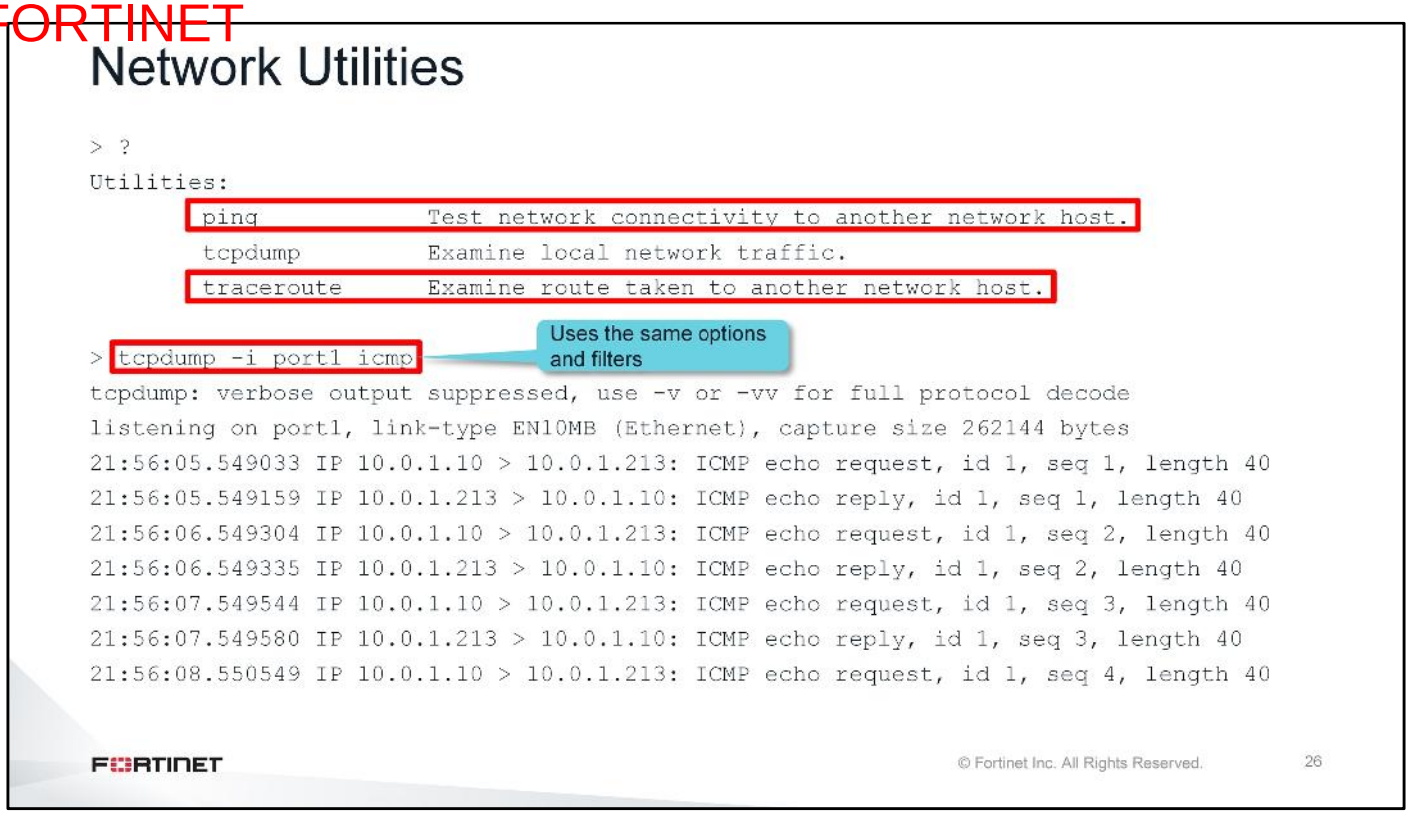


In this section, you will learn about various diagnostics tools available on the FortiSandbox CLI.



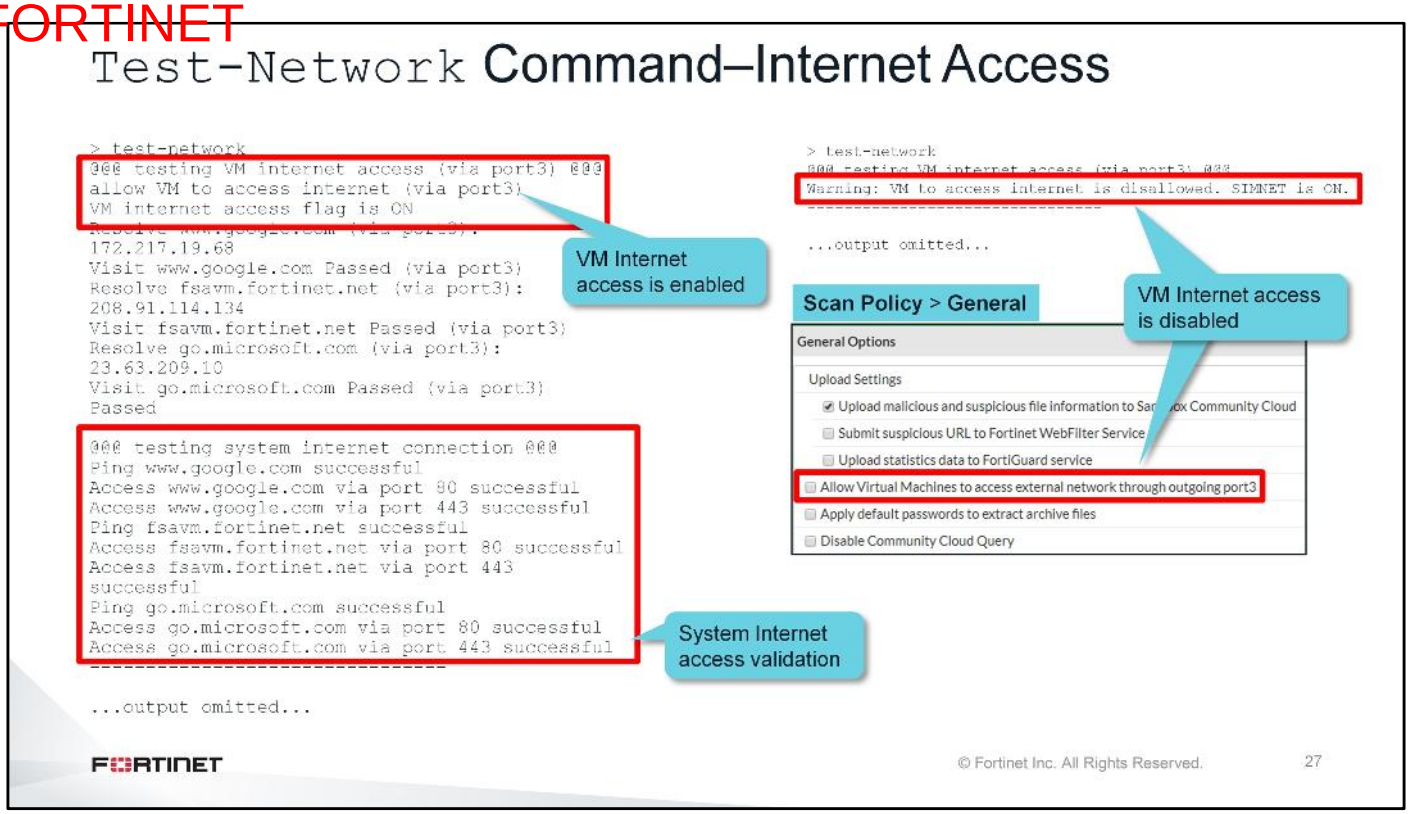
The `status` command shows information about the system, including firmware level, device serial number, disk usage, Windows VM status, and more. For VM appliances, it will also show the FortiSandbox license status.

The `vm-status` command works similarly, but shows information for the guest VM images. You can use this command to verify the activation and initialization status of the guest VM images. You can use the `vm-license` command to see the list of Windows and Microsoft Office licenses installed and activated on your FortiSandbox.



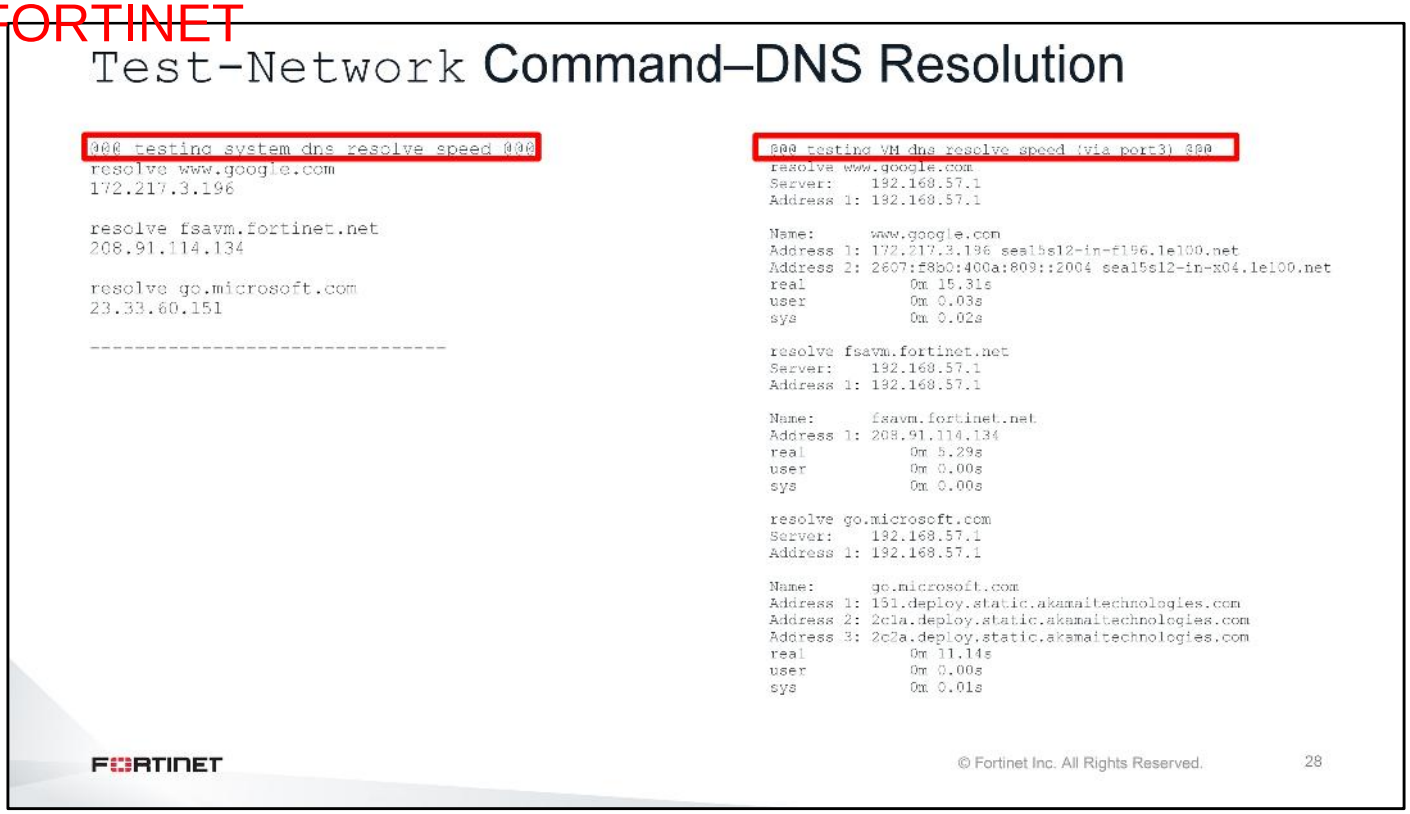
To diagnose any network issues, you can use the ping or traceroute commands available on FortiSandbox.

If you need to verify ingress or egress traffic, or you want to take a deeper look into the packets, you can use the built-in `tcpdump` tool. It is an open-source, command line packet analyzer, and uses the same options and filters. You can find more information on `www.tcpdump.org`.

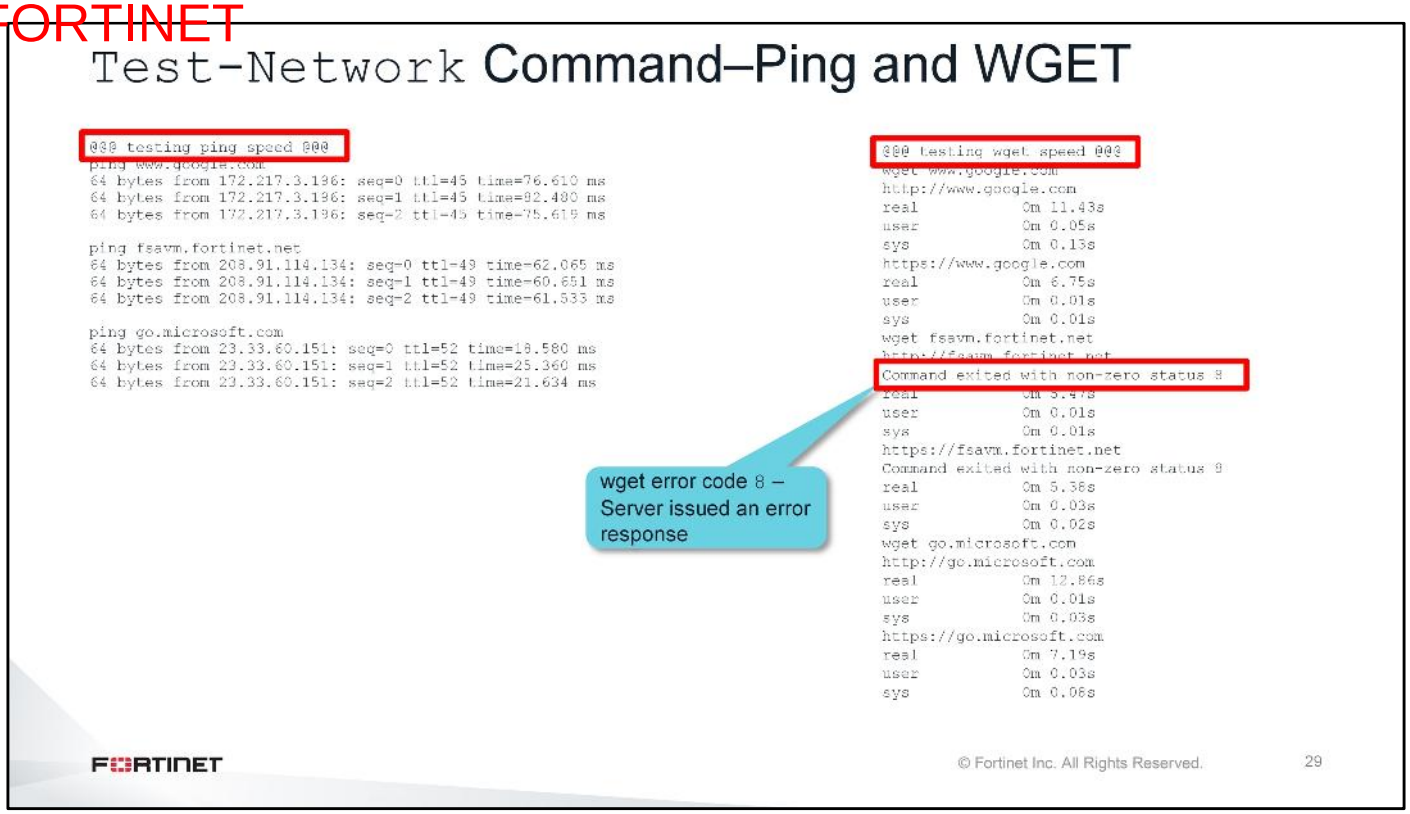


In addition to the `ping` and `traceroute` utility commands, FortiSandbox has a specialized command that runs a series of validations for Internet connectivity: the `test-network` command.

This CLI command can be used to validate various system and VM Internet connectivity metrics. Using this command, you can quickly verify whether or not system Internet and VM Internet access on port3 are enabled and working. The output for this command is formatted so that it is easy to identify which parts of the output are related to the system and which are related to the VMs.

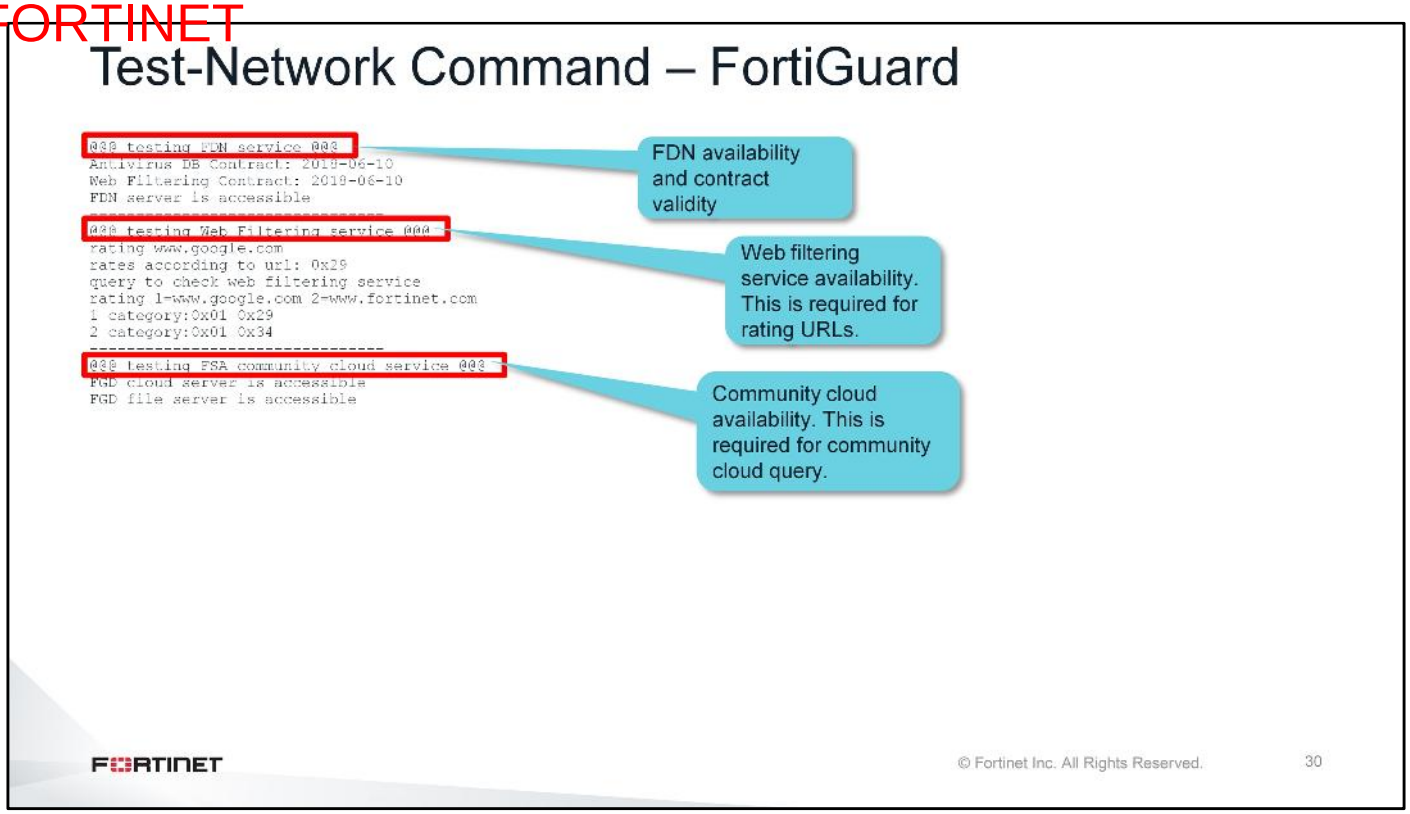


One of the other metrics that the `test-network` command validates is DNS resolution speed. While this command validates both the system and VM, what's more important, are the VM resolution speed numbers. If the DNS resolution speeds for the VMs start to increase, it may affect scan job performance.

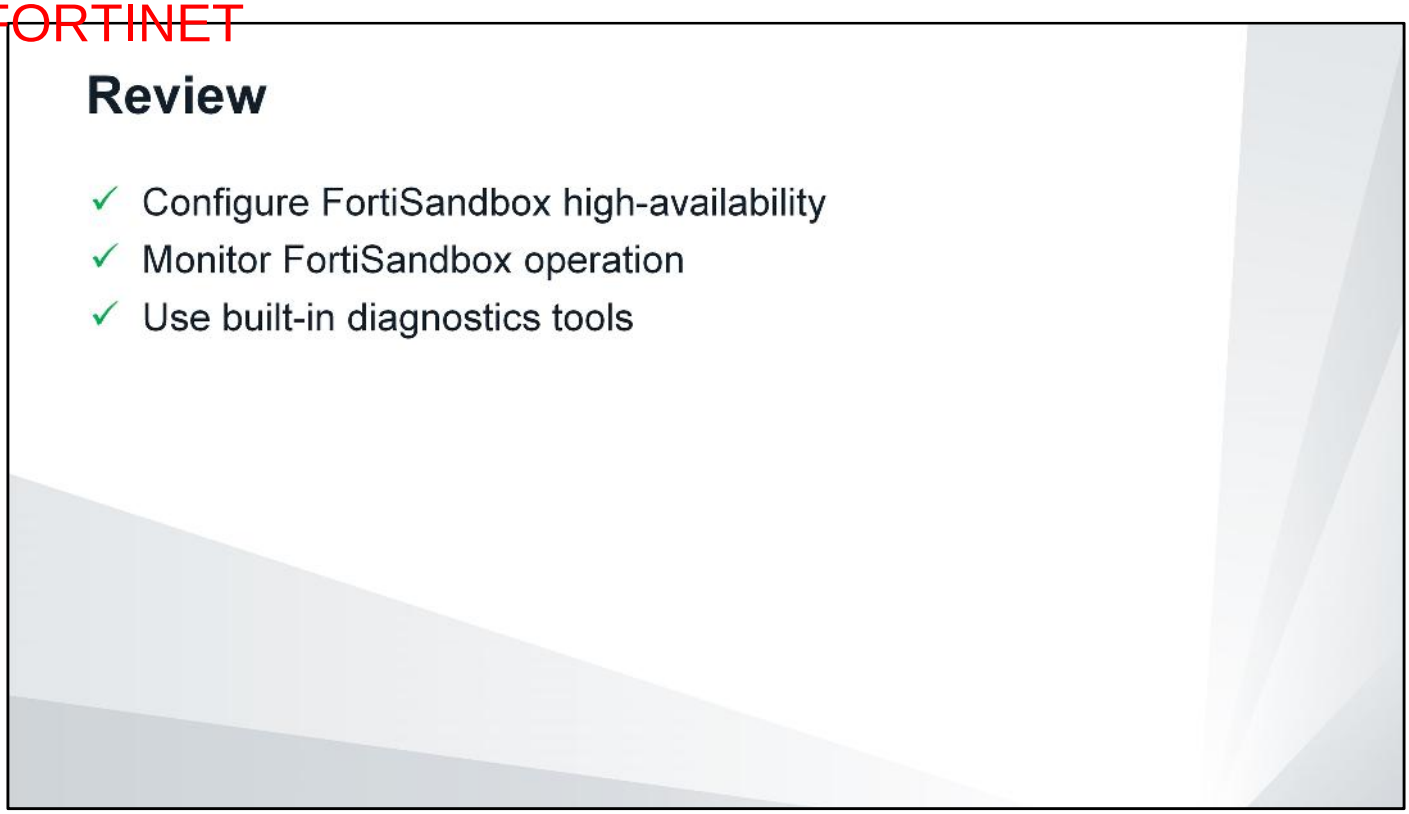


The `test-network` command also checks ping and Wget speeds. Wget is a another open source command line utility that is used to retrieve files using HTTP, HTTPS, FTP, and FTPS. The command output will print any error codes generated by Wget. For more information about these error codes, you can refer to the *WGET Manual* on `www.gnu.org`.

High speed times for ping and Wget can indicate link latency or congestion, and should be addressed as soon as possible.

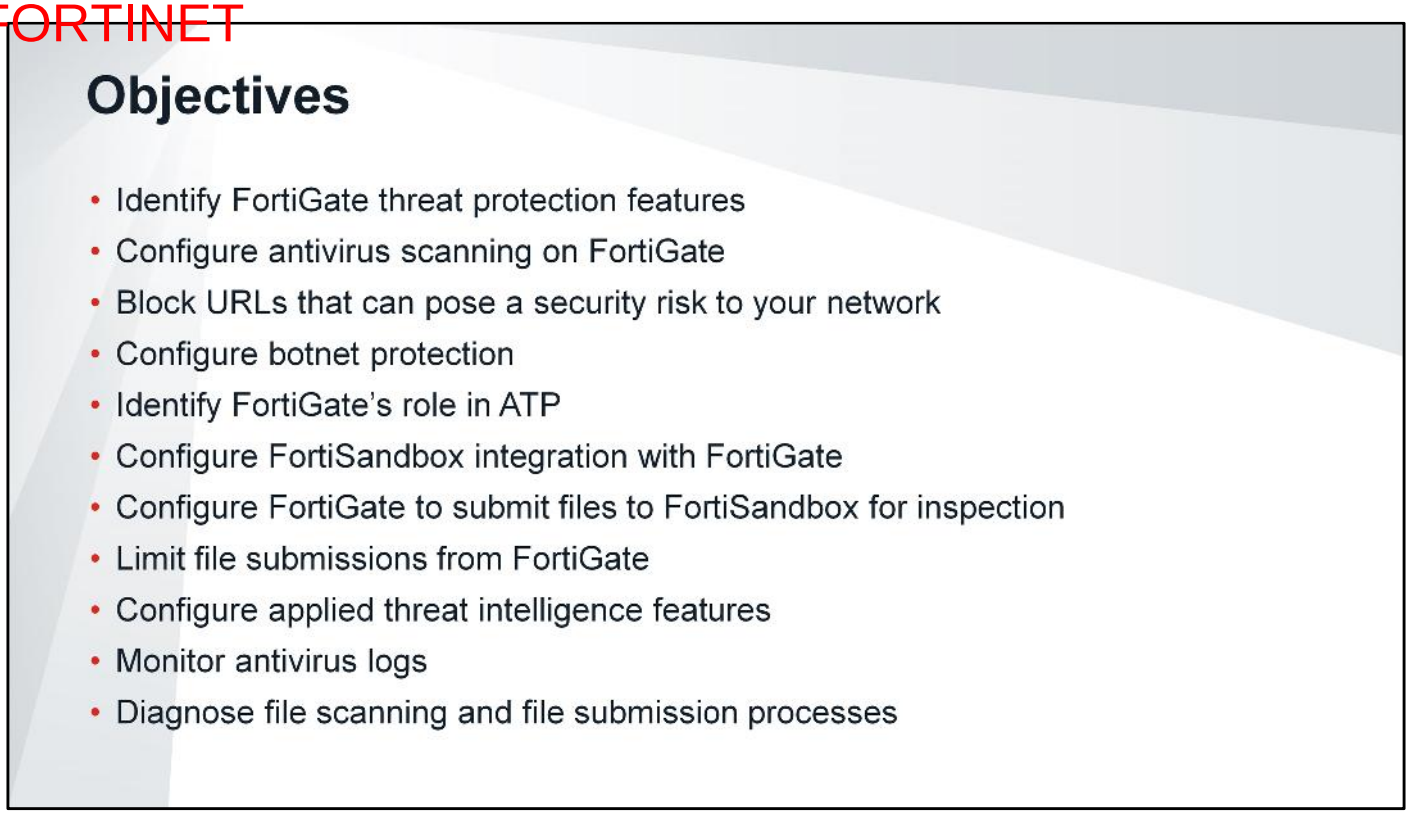


The `test-network` command checks FortiGuard services as its last set of validation tests. These include the FortiGuard distribution network (FDN) accessibility, FDN contract expiration, web filtering service, and the community cloud service. All these FortiGuard services should be reachable and valid for FortiSandbox to be effective.



This slide shows the objectives that you covered in this lesson. By mastering the objectives covered in this lesson, you learned how to learned how to use built-in diagnostic tools to troubleshoot and monitor FortiSandbox performance.

In this lesson, you will learn how to protect your organization's network traffic from advanced threats.



After completing this lesson, you should be able to perform the objectives shown on this slide.

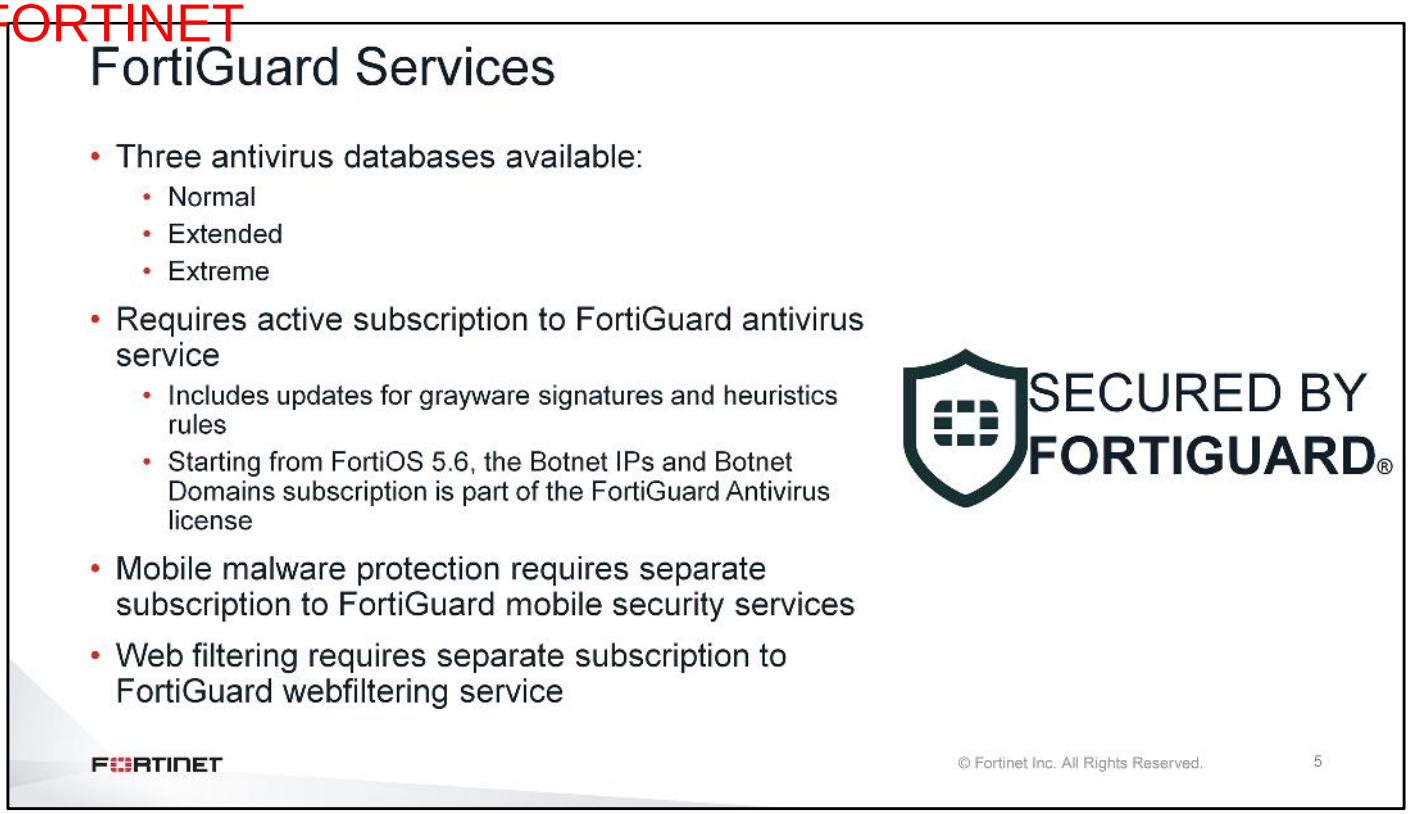
By demonstrating competence in FortiGate's threat protection and ATP integration concepts and configuration requirements, you will be able to protect your network from advanced threats.

In this section, you will learn about the threat protection features available on FortiGate, and how to configure them.

The threat protection features available on FortiGate are aimed at preventing known threats and specific advanced threats.

FortiGuard antivirus scanning protects against the latest viruses, spyware, and other content-level threats using signature-based detection. Fortinet's patented Content Pattern Recognition Language (CPRL) is used to create signatures that can detect many variants of a virus using a single signature. Grayware scanning detects unsolicited, annoying programs that are not traditional malware, but can worsen the performance of a computer system and may cause security risks. Heuristics scanning detects virus-like behavior using probability-based rules. While heuristics scanning may detect zero-day viruses, it is prone to false positives.

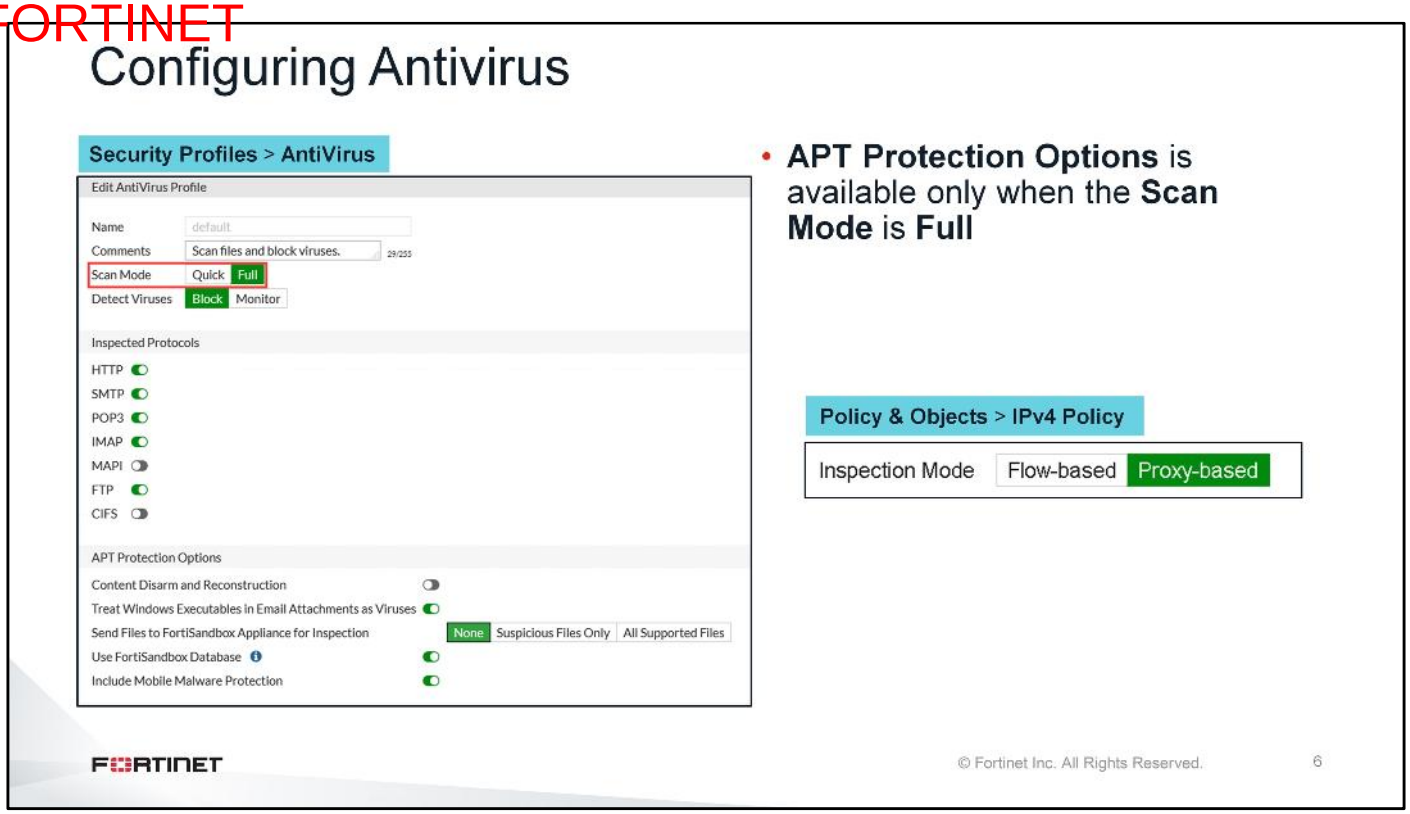
Botnet protection detects and blocks connections to botnet servers and phishing sites. A wider range of malicious and suspicious sites can be blocked using the FortiGuard category-based web filter feature. There are also protection features for mobile platforms using the mobile malware scan service.



There are three antivirus databases available. The normal database, which includes common recent attacks, is usually the default database on most entry-level FortiGate units. The extended database includes all signatures from the normal database, as well as additional, recent, non-active viruses. By default, mid-range to high-end FortiGate devices use the extended database. The extreme database includes all the signatures in the previous two databases, as well as dormant viruses and viruses aimed at legacy systems. This database is typically used in high-security networks and networks with legacy systems.

Regular updates to the antivirus databases ensures you are protected. Your organization must have a current subscription to the FortiGuard antivirus service. This subscription also includes updates for grayware signatures and heuristics rules, and, starting from FortiOS 5.6, botnet database (IPs and domains).

Mobile malware protection, and web filtering require your organization to have separate subscriptions to the FortiGuard Mobile Security Service, and FortiGuard Web Filtering service, respectively.



FortiGate has two distinct inspection modes: flow-based and proxy-based. Beginning at FortiGate 6.2, the inspection mode is configured per policy, which means you can have some policies in flow-based mode and others in proxy-based mode.

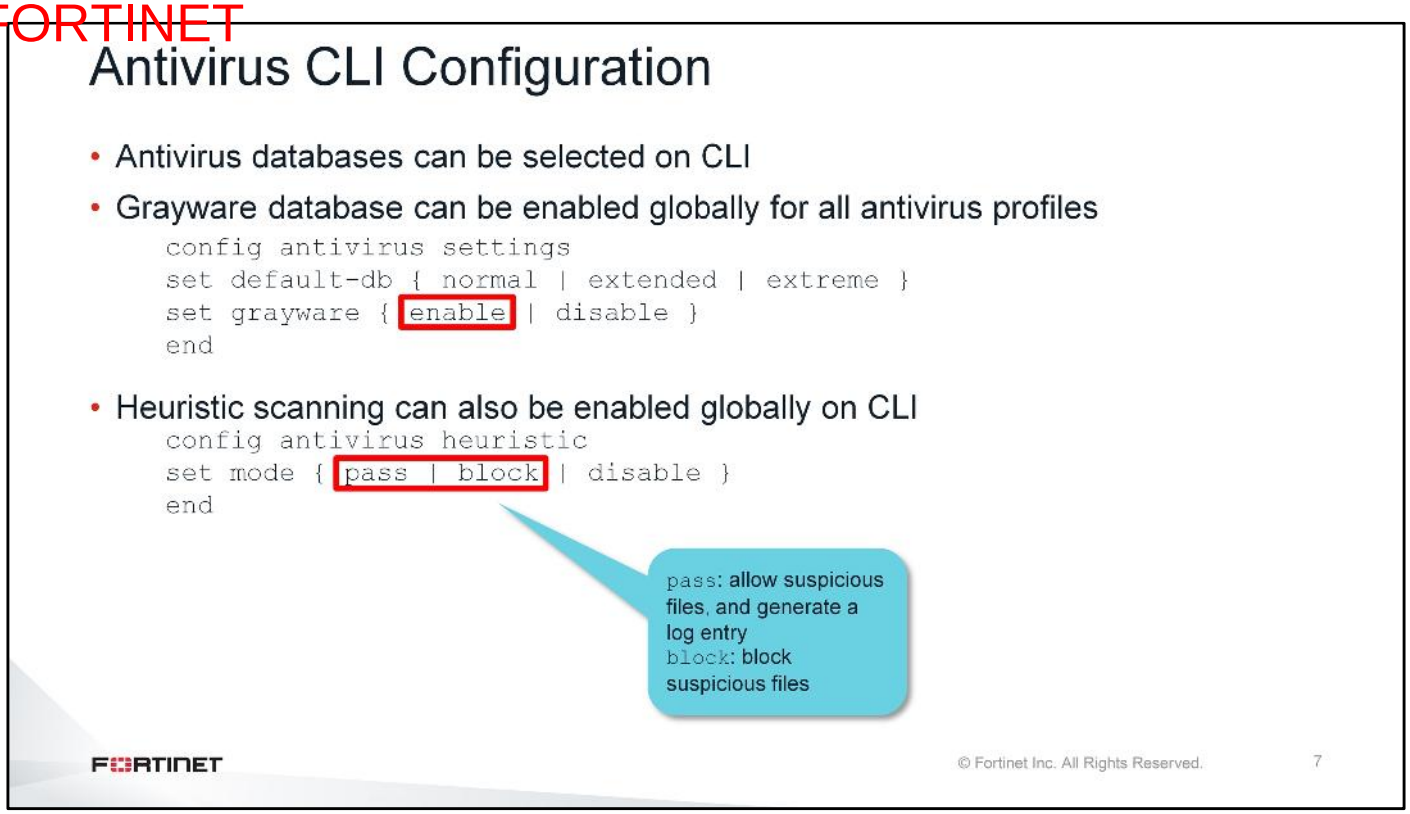
Whether the antivirus profile is operating in flow-based or proxy-based inspection mode, two scanning mode options are available: full scan mode and quick scan mode. Full scan mode uses the full antivirus database (normal, extended, or extreme–depending on what is configured in the CLI) and the IPS engine to examine network traffic. **APT Protection Options** are only available when the **Scan Mode** is **Full**, which means that the **Scan Mode** must be **Full** if you want FortiGate to send files to FortiSandbox for analysis.

Quick scan mode uses an IPS engine with an embedded compact antivirus database containing fewer signatures. Quick scan mode does have some limitations compared to full scan mode in flow-based inspection mode. Quick scan mode cannot do the following:

- Send files to FortiSandbox for inspection
- Use advanced heuristics
- Use mobile malware packages

Some entry-level FortiGate models don’t support this method.

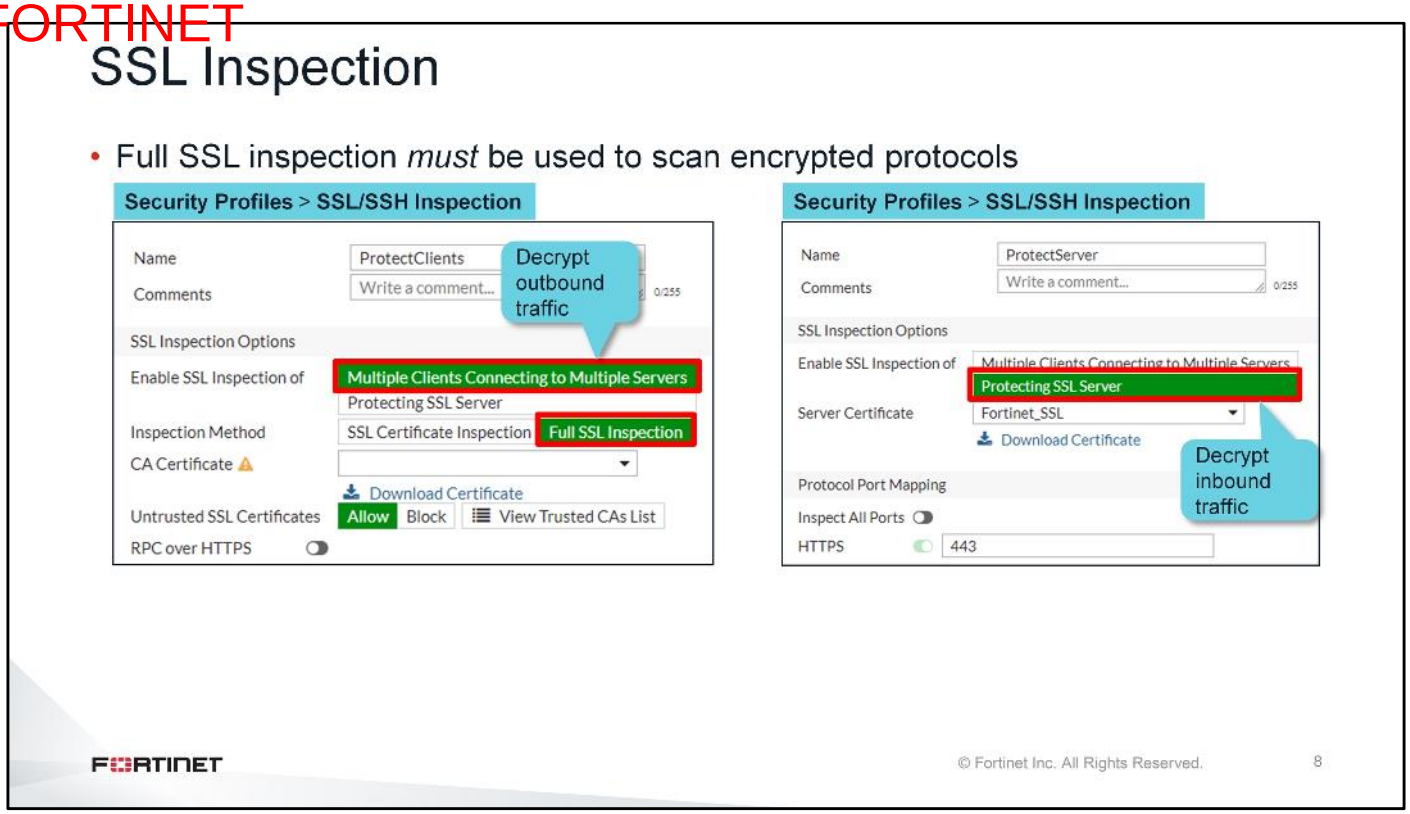
Beginning at FortiOS 6.2, you can apply quick scan mode to policies that are running in proxy-based inspection mode.



You configure the default antivirus database using the CLI. The available databases will depend on the FortiGate's model.

By default, the grayware database is disabled. You can enable it globally for all antivirus profiles using the CLI.

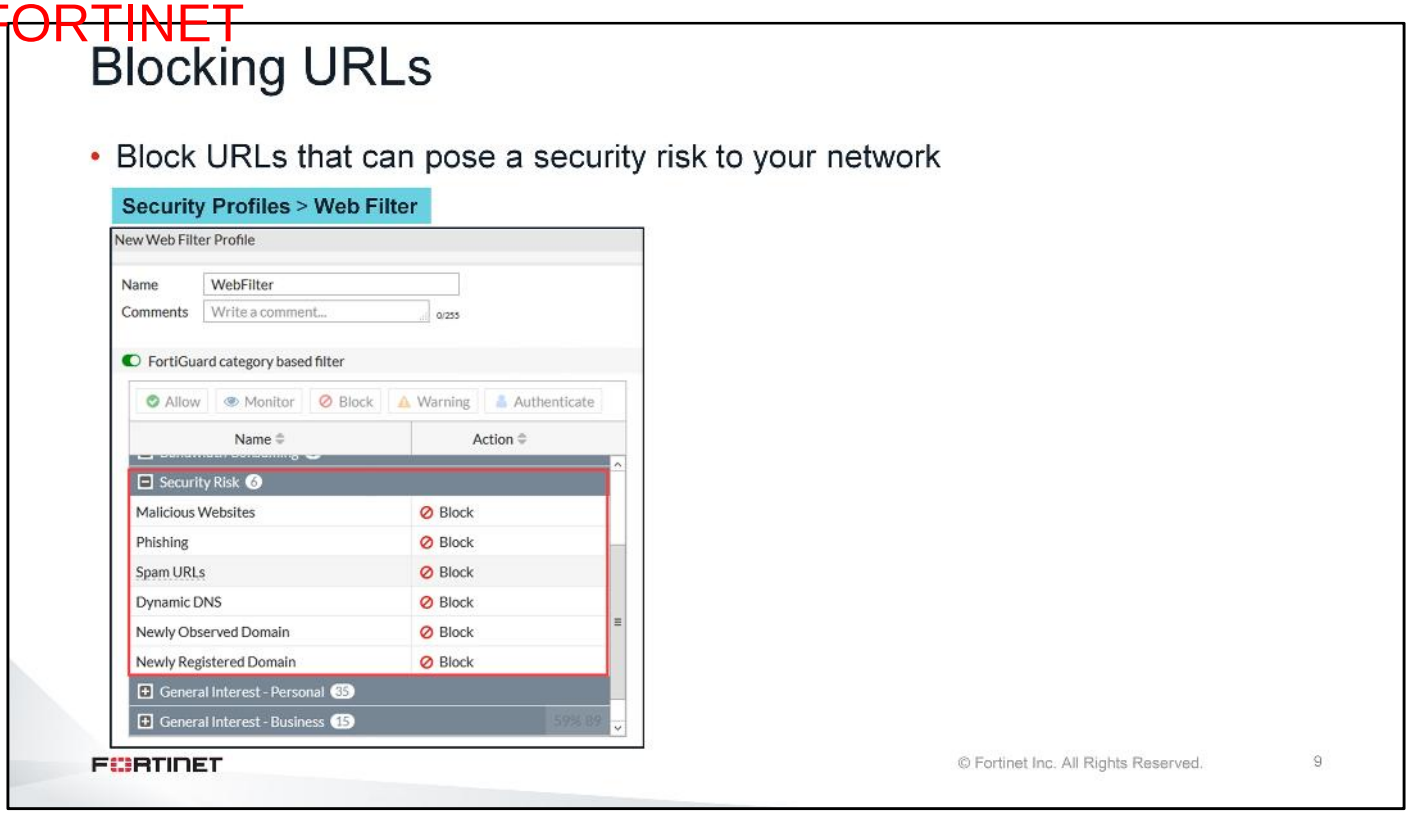
By default, heuristics is also disabled. You have two options to enable heuristics—pass or block. Pass allows suspicious files through and generates a log file. Block prevents suspicious files from passing through.



Viruses reside in the payload of a packet. For antivirus to be effective, FortiGate must have access to the packet payload. So how can FortiGate inspect packets that are encrypted?

FortiGate has two methods of inspecting outbound encrypted sessions—SSL certificate inspection, and full SSL inspection. SSL certificate inspection inspects only the SSL handshake and identifies the destination server using the server name identifier (SNI) or common name (CN) of the certificate. This information is enough to identify some applications, as well as most URLs. However, certificate inspection is unable to inspect encrypted packet contents and therefore it is not effective for antivirus scanning. Full SSL inspection is capable of inspecting all of the packet contents, including the payload. FortiGate does this by proxying the SSL connection. There are two SSL sessions that are established—client-to-FortiGate, and FortiGate-to-server. This allows FortiGate to encrypt and decrypt packets using its own keys. For antivirus to be effective, you *must* use full SSL inspection to scan outbound traffic.

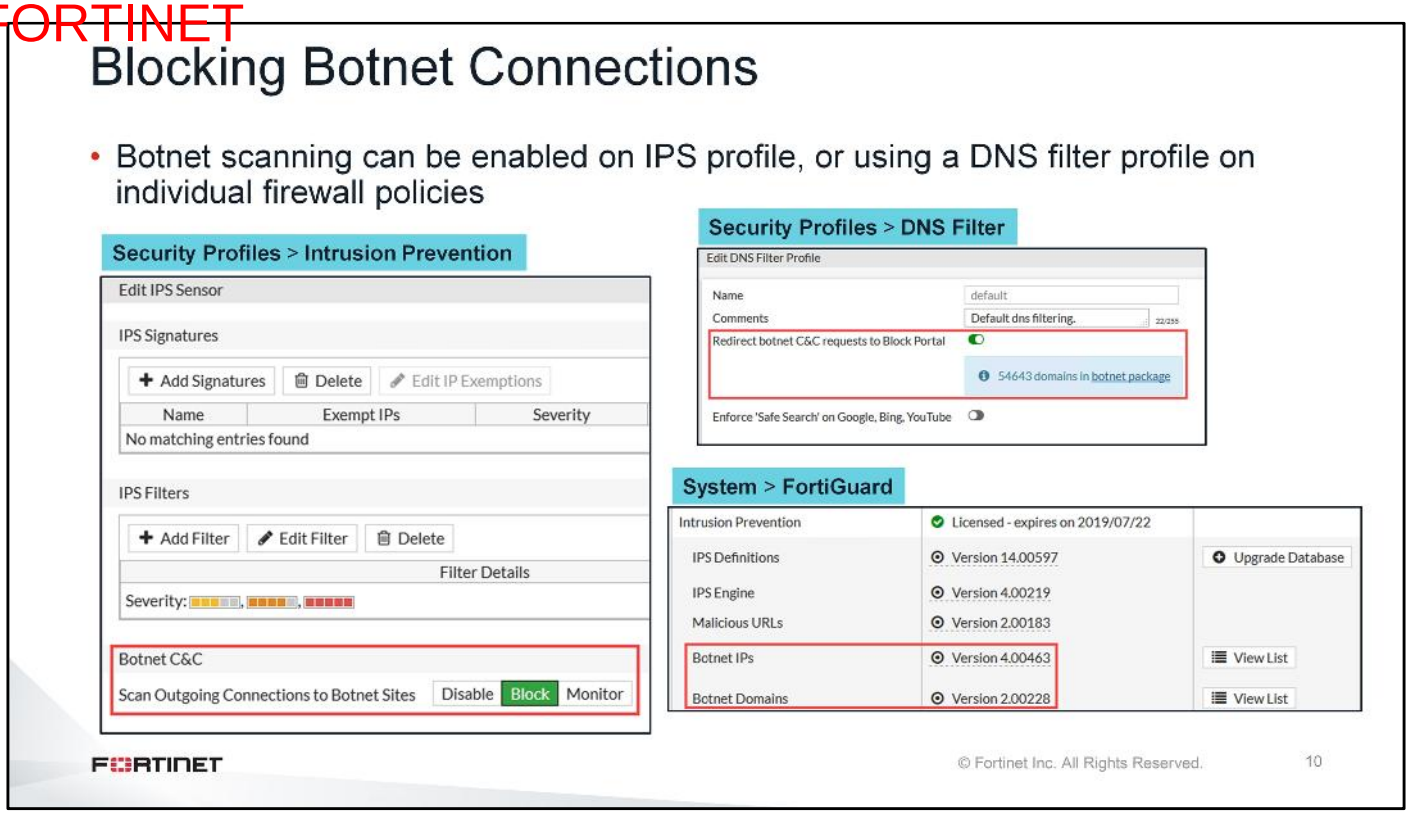
To inspect encrypted inbound traffic, FortiGate acts as a reverse proxy server. You should import the back-end server's key pair to FortiGate, and apply it to the SSL inspection profile. If you have multiple servers to protect, you will need to add an SSL inspection profile for each server, unless the servers share the same certificate (wildcard certificate).



You can also use the web filter profile to block access to websites that can pose a security risk. There are FortiGuard categories for malicious, phishing, and spam URLs.

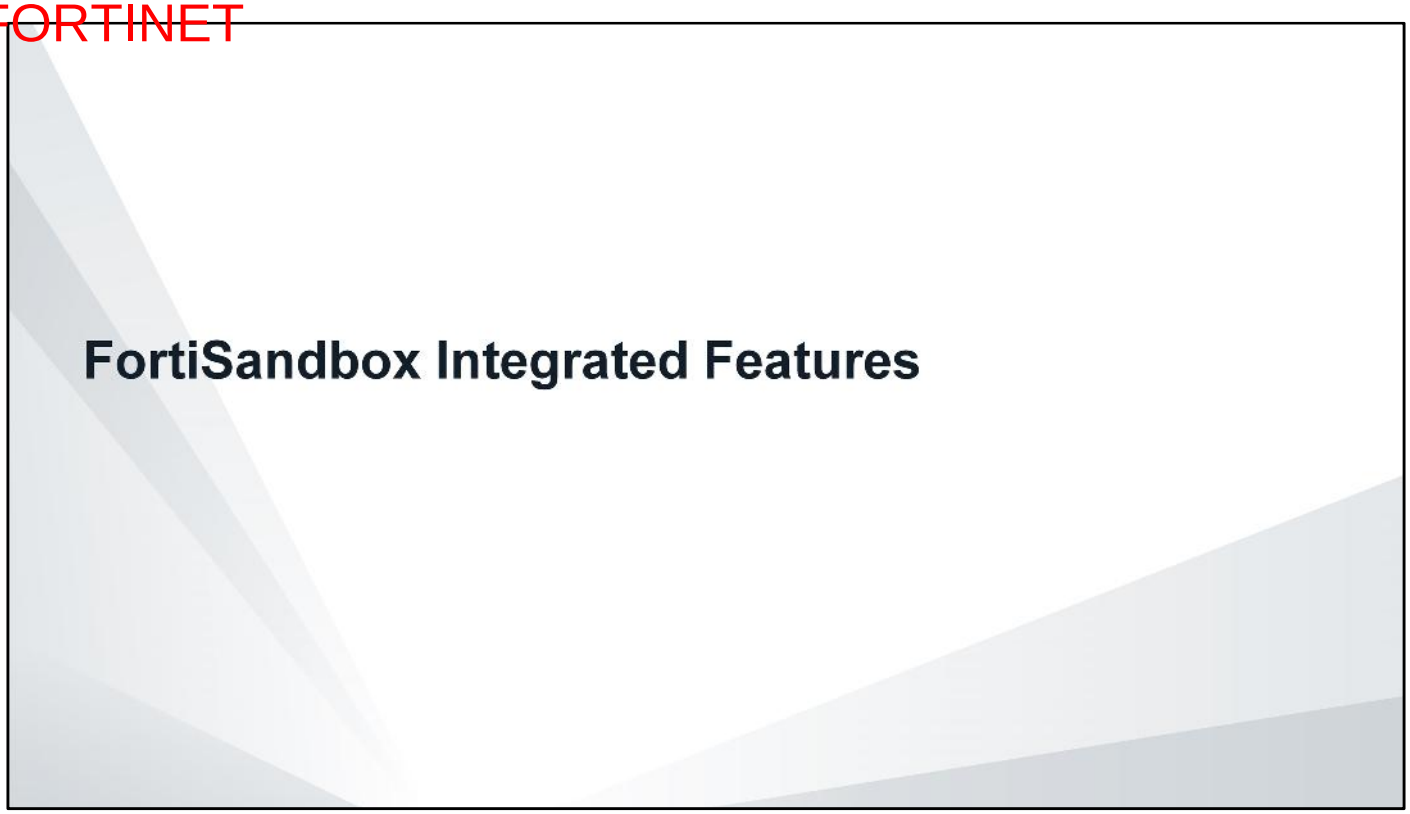
Newly Observed Domain applies to URLs whose domain name is not rated and were observed for the first time in the past 30 minutes. **Newly Registered Domain** applies to URLs whose domain name was registered in the previous 10 days. FortiGuard's auto-rating system attempts to rate the URL using various methods. If auto-rating cannot rate the URL, FortiGuard applies the **Not Rated** rating.

If you do not block the **Newly Observed Domain** and **Newly Registered Domain** categories, you should, at a minimum, use the warning action to warn users when they might be accessing a suspicious URL.

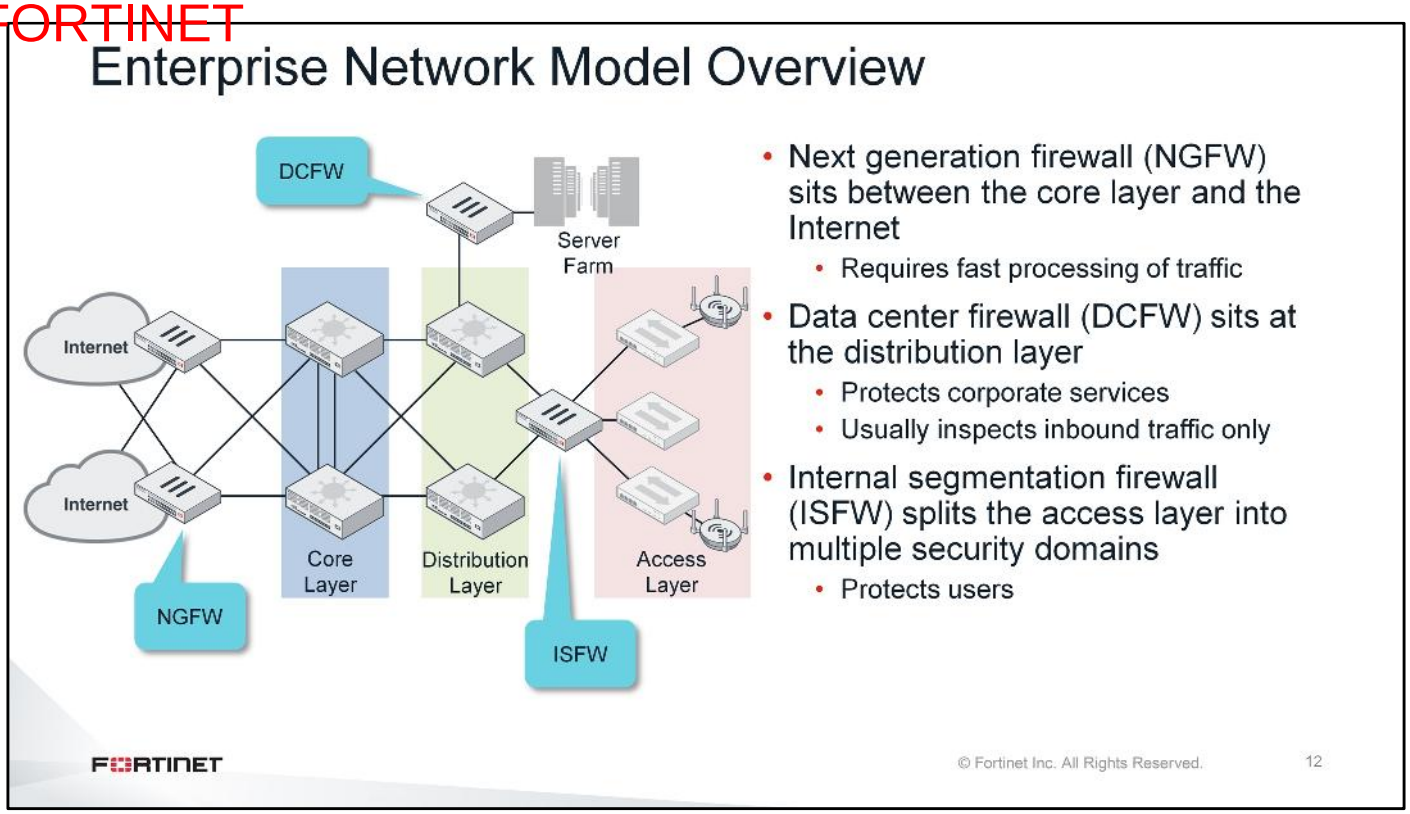


A key event in the attack kill chain on an organization occurs when the threat communicates with a command-and-control server—either to download additional threats or to exfiltrate stolen data. IP and domain address reputation blocks this communication. You can enable blocking of botnet connections on IPS profile and apply it to specific firewall policies.

FortiGuard maintains a database containing a list of known botnet C&C addresses. This database is updated dynamically and stored on the FortiGate and requires a valid FortiGuard antivirus subscription.
When you block DNS requests to known botnet C&C addresses, DNS lookups are checked against the botnet C&C database. All matching DNS lookups are blocked and redirected to a FortiGuard block portal. Matching uses a reverse prefix match, so all subdomains are also blocked. To enable this feature, click **Security Profiles** > **DNS Filter** and enable **Redirect botnet C&C requests to Block Portal**. Finally, apply the profile to specific firewall policies.



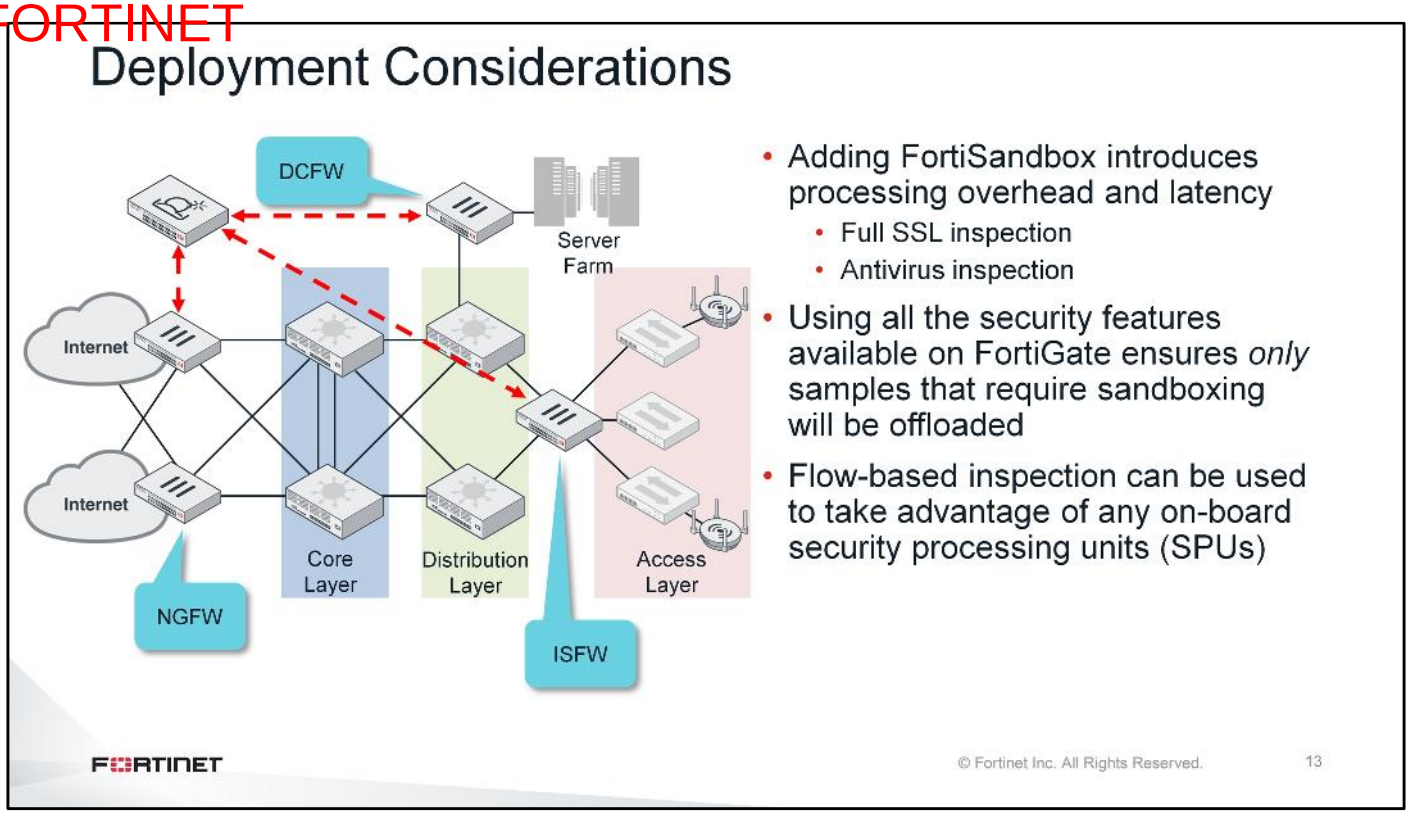
In this section, you will learn how to integrate FortiGate with FortiSandbox. You will also learn how to configure threat intelligence sharing between FortiSandbox and FortiGate, and how to block URLs that are identified as suspicious by FortiSandbox.



NGFW FortiGate devices are the first line of defense in an enterprise network. These are traditional entry-point firewalls that sits at the edge of your organization's network and inspect all inbound and outbound traffic. Typically, this inspection requires fast firewall and traffic processing capabilities. The features that are usually enabled in NGFW FortiGate devices are firewall, application control, VPN, and IPS.

DCFW firewalls are installed at the distribution later. They typically protect corporate services and are usually inspecting only inbound connections. These low-latency, high-throughput FortiGate devices are typically used for IPS and firewall functionalities.

ISFW firewalls are used to split the access layer into multiple security segments. In the event of an outbreak, you can safely quarantine a single segment without affecting others. ISFW FortiGate devices are typically used for firewall, application control, web filtering, antivirus, and IPS.



When discussing FortiSandbox integration, you have to consider the processing overhead. Where is the optimal location to implement advanced threat protection? The location depends solely on the network setup, and corporate network security policies.

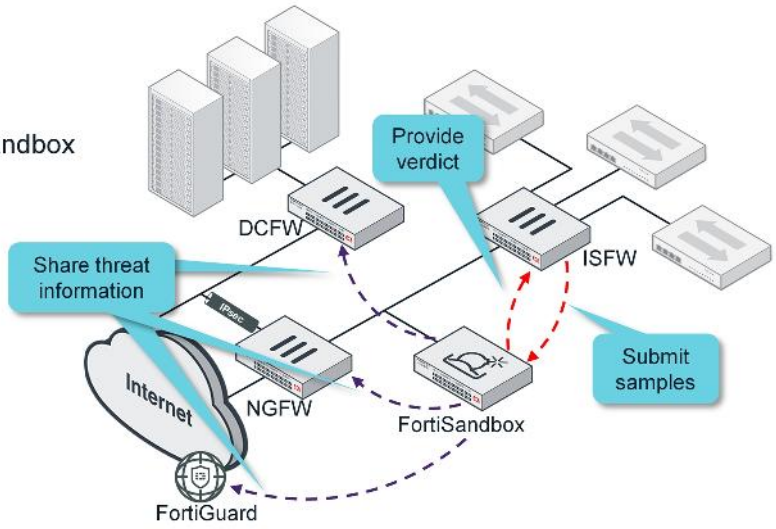
You could implement ATP at the entry-point using an NGFW FortiGate. Stopping malware closest to the source prevents any risks of propagation, especially when using threat intelligence sharing with DCFW and ISFW FortiGate devices. However, you have to keep in mind that enabling antivirus and full SSL inspection will add processing overhead. If the FortiGate has SPUs, you can use flow-based inspection mode to take advantage of any on-board content processors (CPs) or security processors (SPs).

The same concept applies when integrating FortiSandbox with a DCFW FortiGate. Typically, you configure DCFW devices for inbound-traffic inspection. Using flow-based inspection to take advantage of any on-board SPU will keep performance impact to a minimum.

ISFW FortiGate devices are located closest to the users. For greater accuracy, you can use proxy-based inspection.

FortiSandbox Integration

- FortiGate's role:
  - Decrypt content
  - Detect and block known threat
  - Offload suspicious samples to FortiSandbox
  - Prevent outbreak
- FortiSandbox's role:
  - Inspect submitted samples
  - Generate a verdict
  - Share threat information

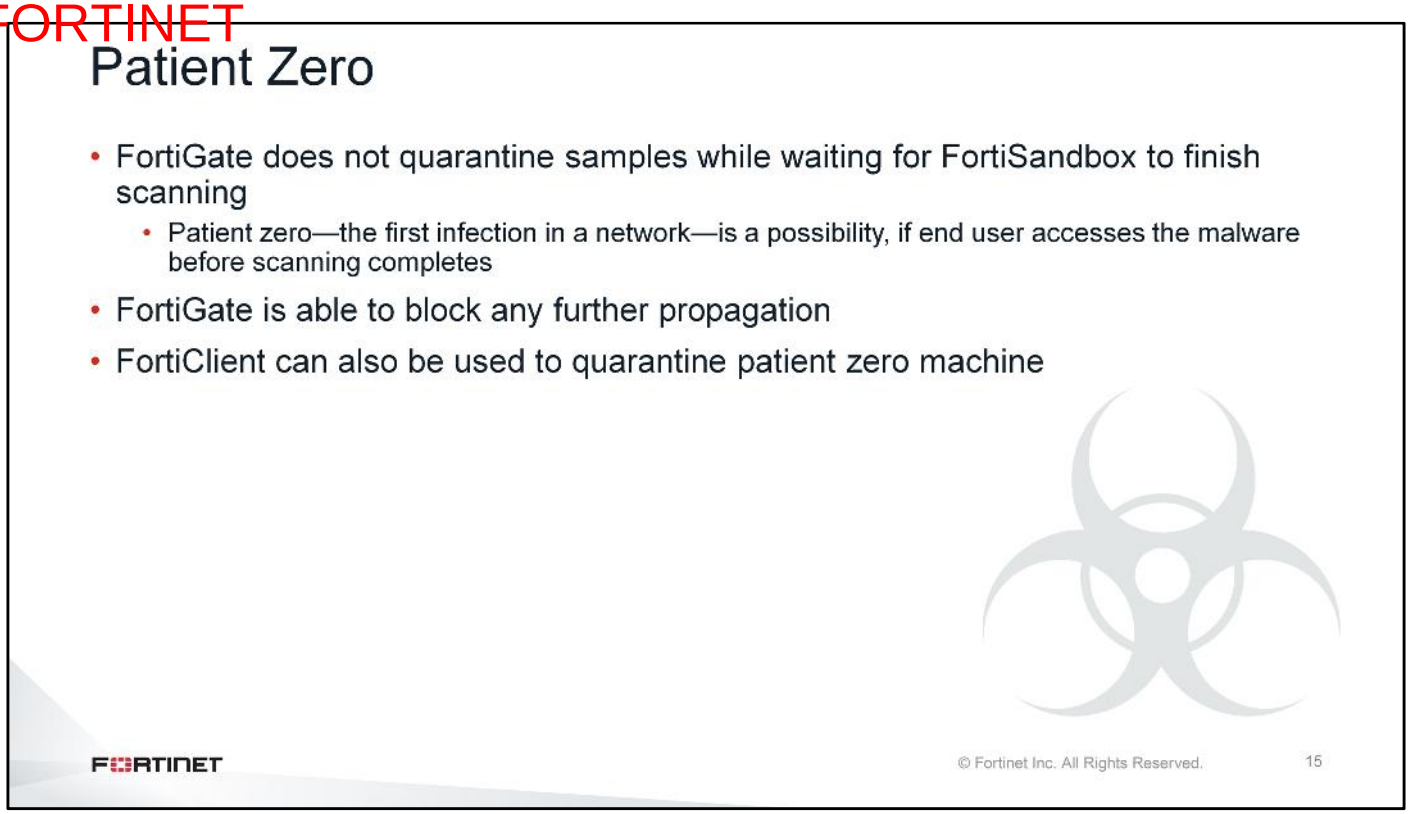


FORTINET

14

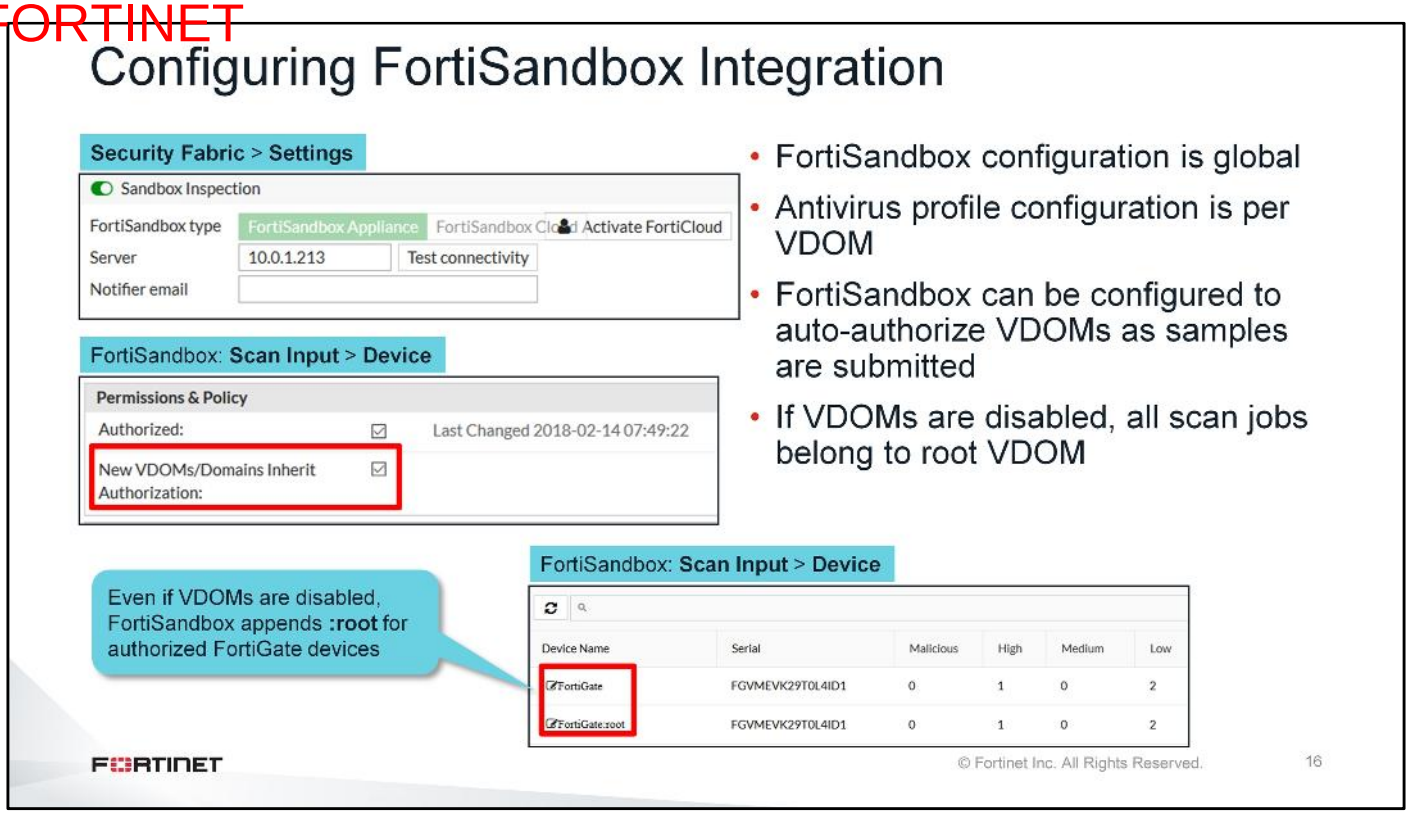
Before offloading samples to FortiSandbox, FortiGate must decrypt content, and detect and block known threats (using any or all of the threat protection features you've learned about so far). An ATP solution is not just about integrating a FortiSandbox and starting to scan samples. The features you've learned about so far must work in unison with FortiSandbox to be efficient and effective. Sandboxing is not fast enough to scan *everything* moving through an enterprise network.

After FortiSandbox inspects the submitted samples and generates a verdict, FortiGate acts based on the verdict. FortiSandbox also shares threat information in the form of malware and URL packages that can be shared all through the network with other FortiGate devices to prevent an outbreak.



FortiGate is a real-time firewall. As such, it does not queue files while waiting for FortiSandbox to finish scanning. So patient zero—the first infection in the network—is a possibility if the end user accesses the malware before scanning completes.

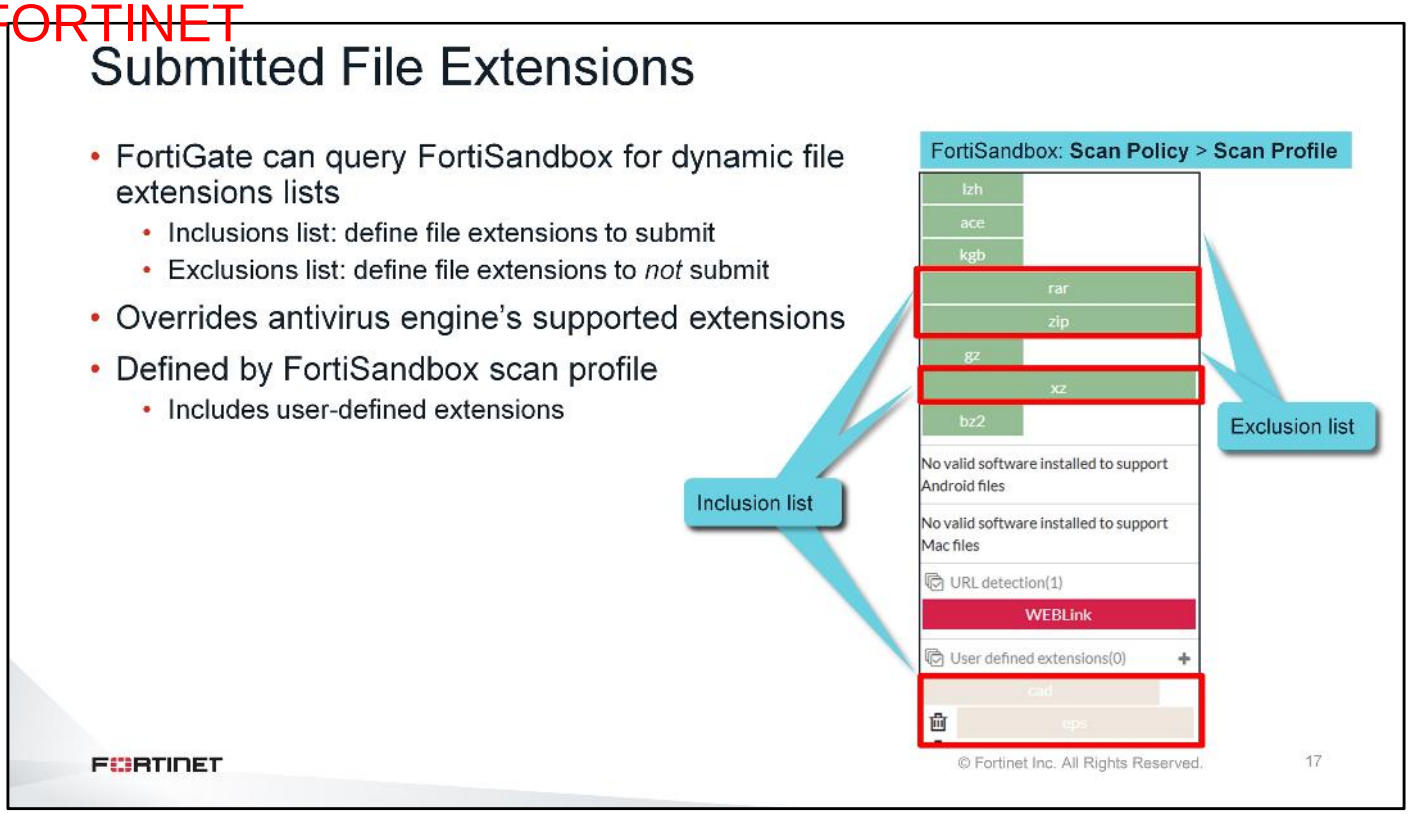
FortiGate is able to block any further propagation of the malware by using FortiSandbox-generated malware signatures and malicious URL lists. You can also use FortiClient to quarantine patient zero's computer.



You must authorize each device on FortiSandbox before it will start accepting samples.

If you enable VDOMs on FortiGate, each VDOM is treated as a separate input device on FortiSandbox. If you enable auto-authorization, FortiSandbox will automatically authorize VDOMs as files are submitted.

If you do not enable VDOMs, all scan jobs belong to the root vdom.



Starting in FortiOS 5.6, FortiGate can query FortiSandbox for two dynamic file extensions lists—an inclusion list, and an exclusion list.

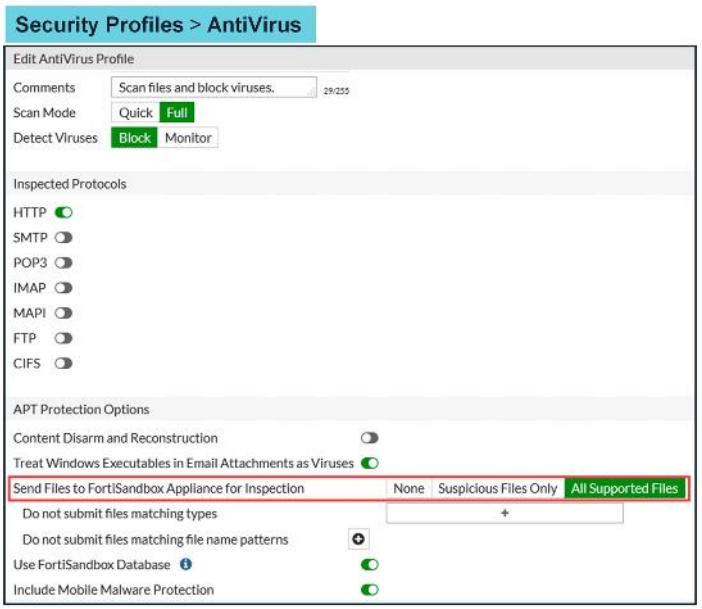
These lists correspond to the scan profile configuration on FortiSandbox. Each extension that you enable is added to the inclusions list, and the rest are added to the exclusion list.

These lists override the FortiGate antivirus engine's supported extensions. For example, even if the antivirus engine supports offloading of `.docx` files to FortiSandbox, if that extension is in the exclusion list, FortiGate will not send any `.docx` samples.

These dynamic lists also support user-defined extensions.

Submitting Files From FortiGate

- Configure FortiSandbox settings
- Configure antivirus profiles to offload samples to FortiSandbox
- Apply antivirus profile to firewall policy
- Ensure an full SSL inspection is being used
- FortiGate *only* offloads files; URL offload is FortiMail-specific

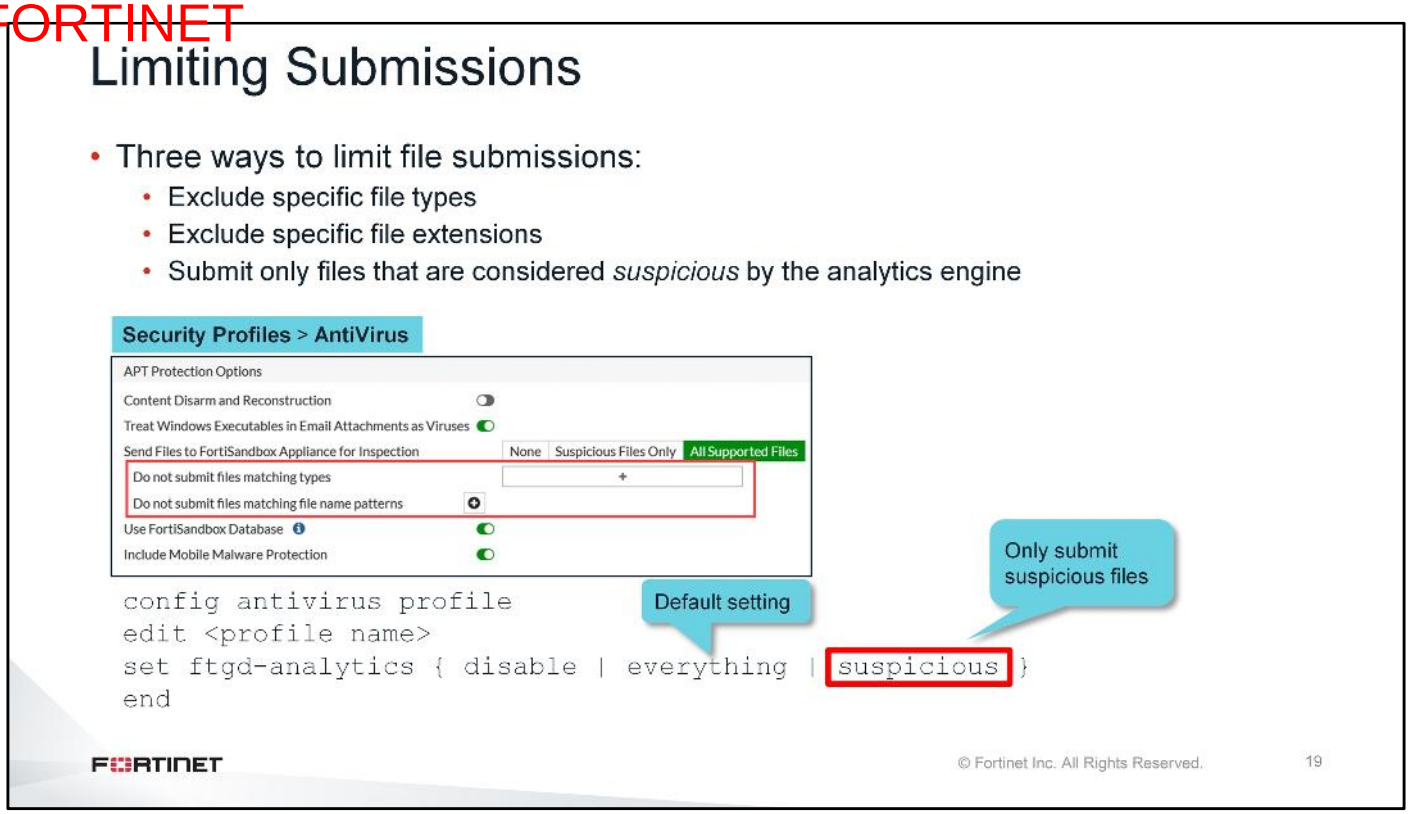


FORTINET

18

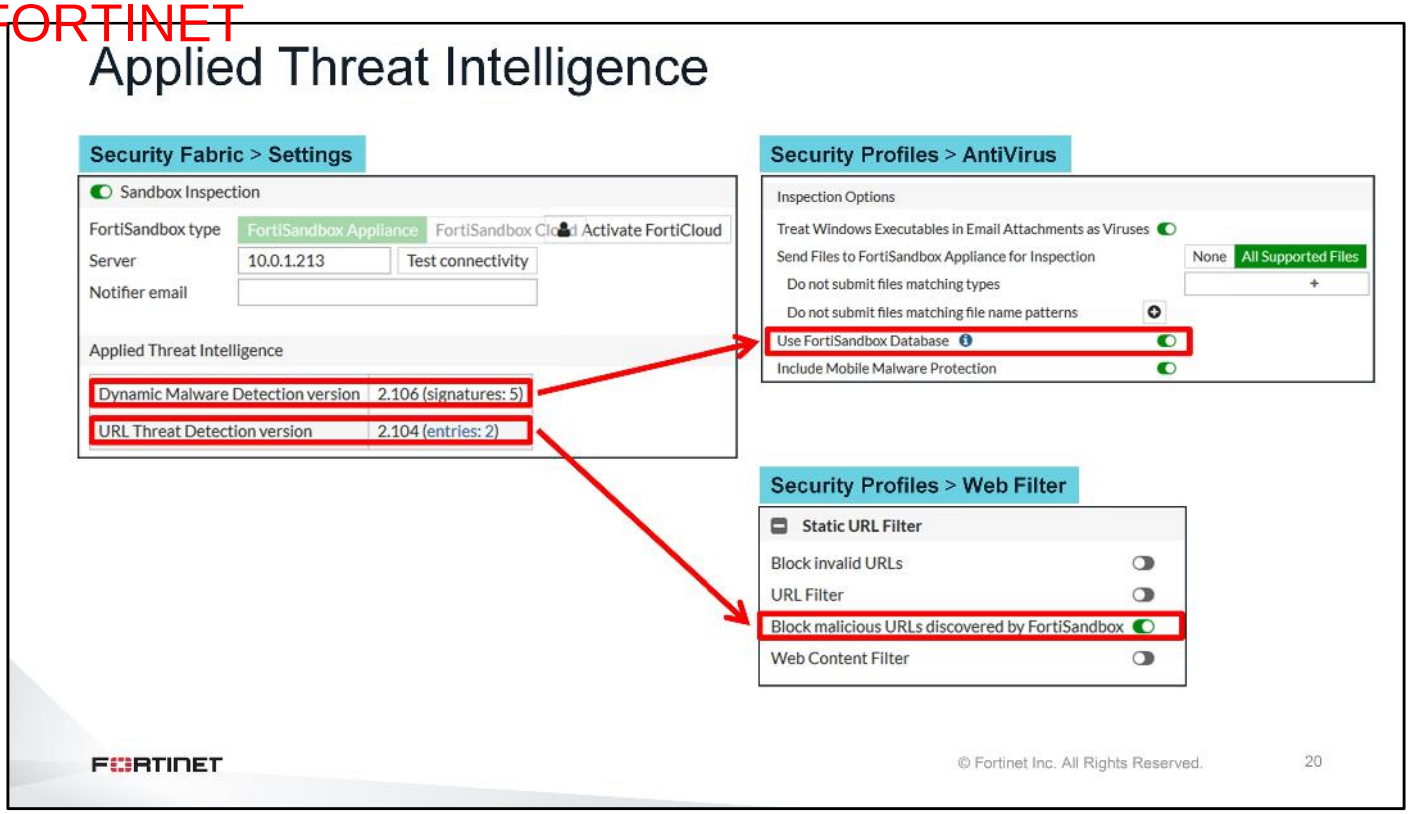
After configuring FortiSandbox on FortiGate, any new antivirus profile you create will automatically be configured to send all supported files to FortiSandbox.

When using proxy-based inspection, you can specify precisely which protocols are inspected. Regardless of which protocols are selected for inspection, keep in mind that FortiGate *only* offloads files. URL offload is a FortiMail-specific feature.



There are three ways to limit the number of files FortiGate may submit to FortiSandbox. You can configure the exclusion of specific file types or file extensions. You can configure these exclusions in the antivirus profile configuration page on the management GUI.

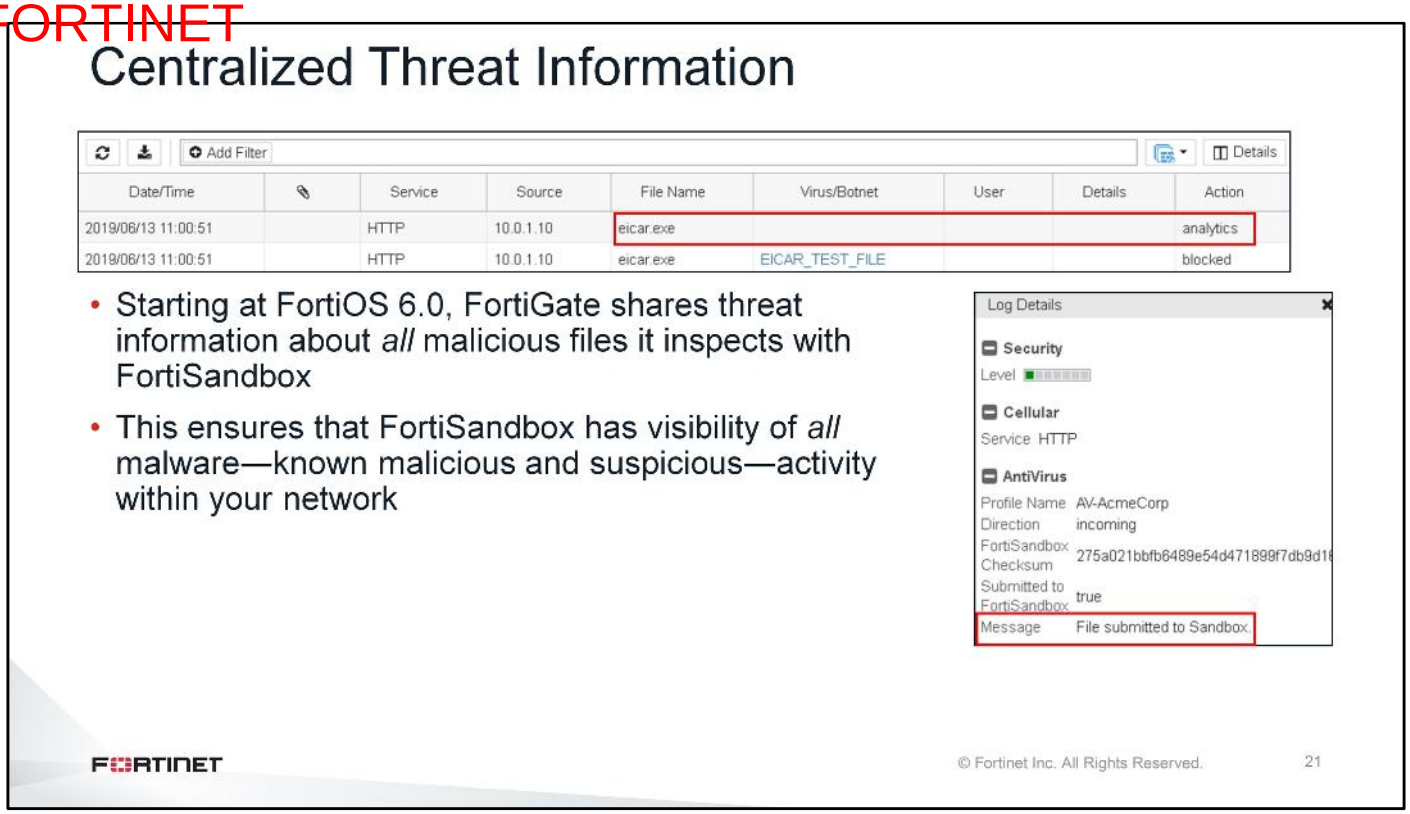
Using the CLI, you can configure the antivirus profile to submit only files that are considered *suspicious* by the analytics engine. When enabled, FortiGate *greatly* limits the number of files that will be submitted to FortiSandbox. So, unless FortiSandbox load is an issue, for highest security, it is better to use the default setting (`everything`).



FortiSandbox shares threat intelligence with FortiGate in the form of two databases—the malware package, and the URL package. If FortiGate is configured to use the FortiSandbox database, it will generate a periodic request to FortiSandbox and query for the latest malware and URL package versions. The malware package contains hashes for all suspicious files detected by FortiSandbox. The URL package contains direct URLs for suspicious webpages detected by FortiSandbox.

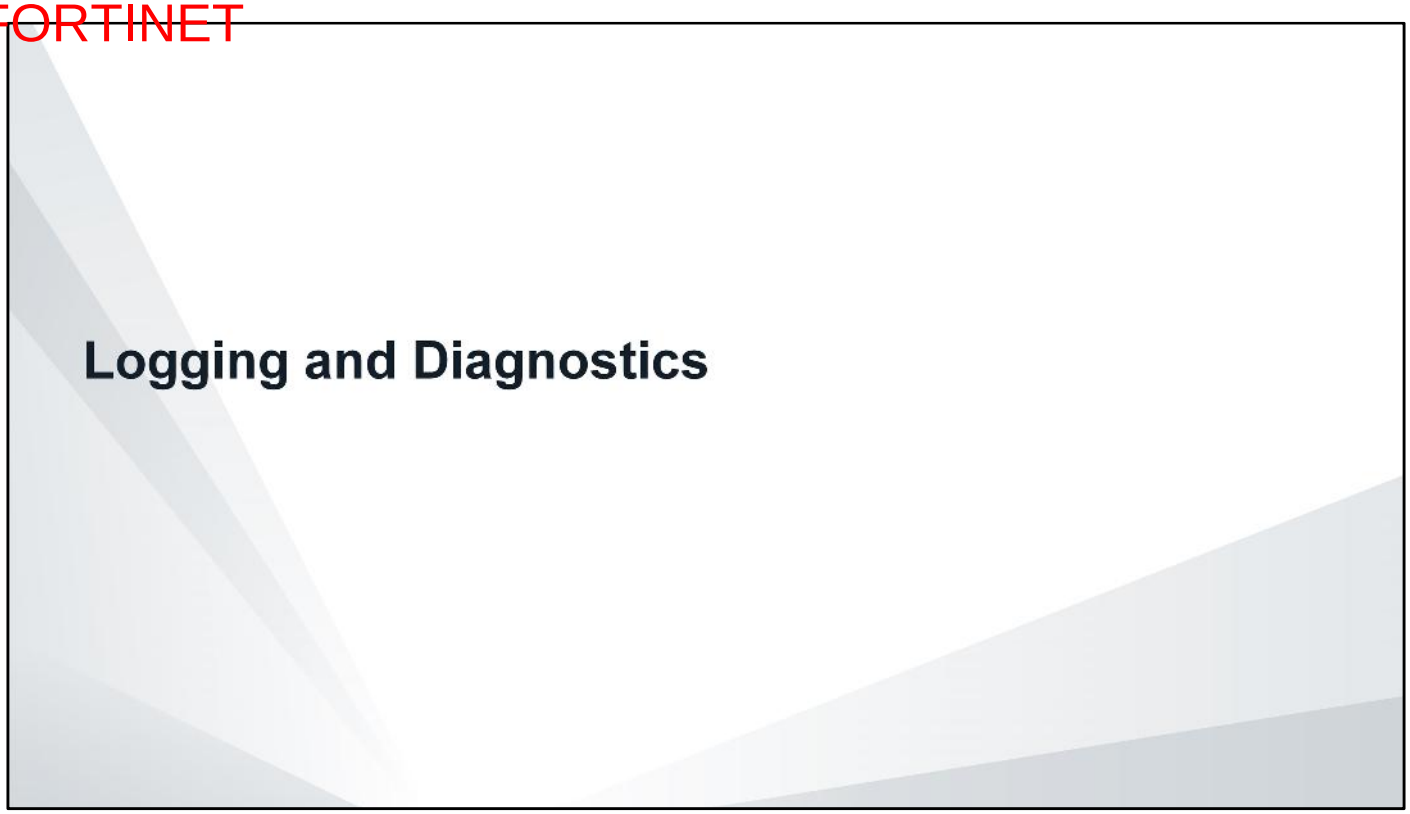
You can use this feature to share the same advanced threat intelligence throughout your organization's entire network, regardless of which FortiGate is submitting samples to FortiSandbox. For example, if your NGFW FortiGate is configured to submit samples, you can share that threat information with your remote office FortiGate devices, DCFW FortiGate devices, and ISFW FortiGate devices. This information sharing prevents any malware that has entered your organization's network to propagate to other segments.

If you're using FortiSandbox, you *should* use these threat intelligence features.

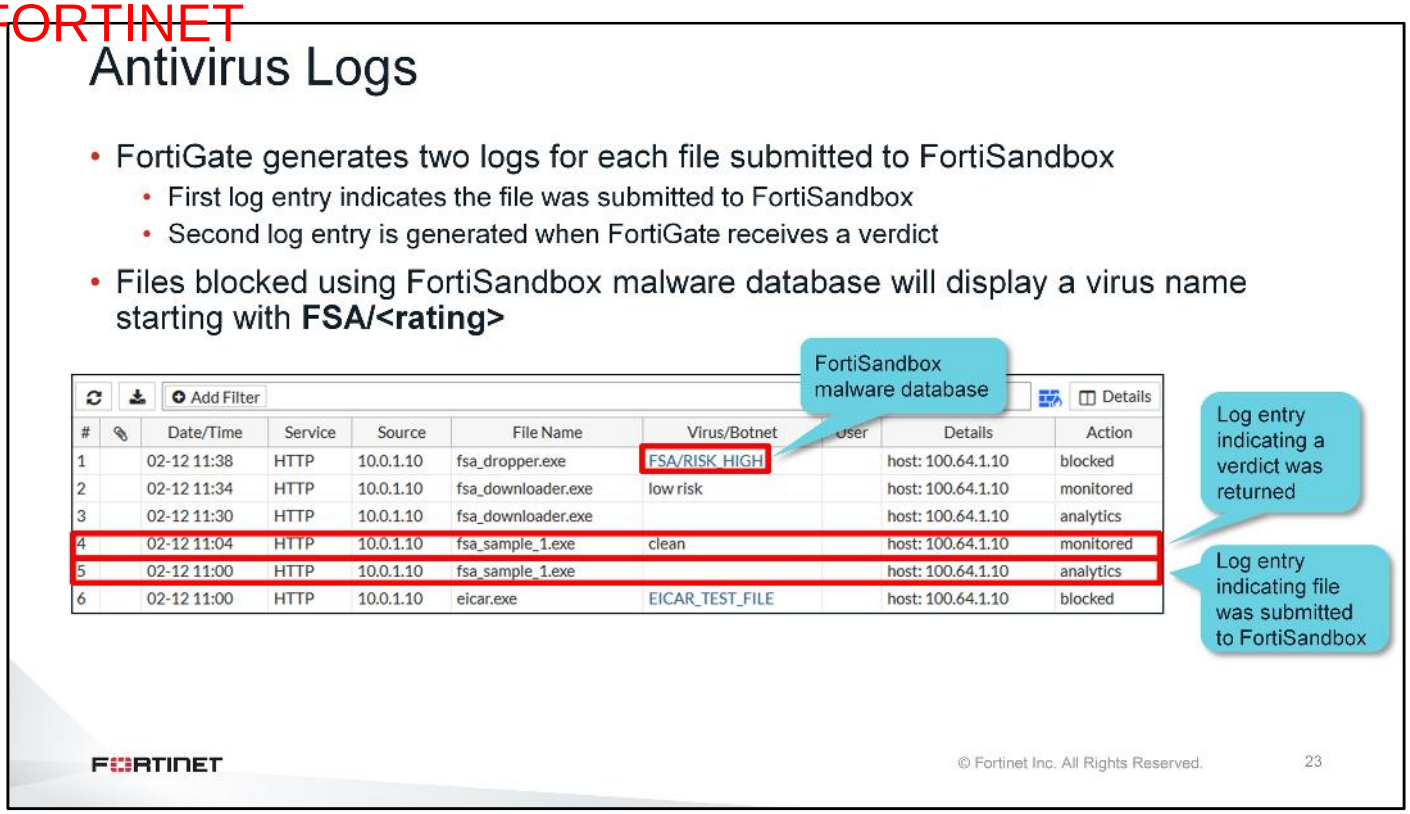


Starting at FortiOS 6.0, FortiGate shares threat information about all malicious files it inspects with FortiSandbox. This includes malware detected by FortiGate using local antivirus signatures. This ensures that FortiSandbox has visibility of all malware activity within your network.

As shown on this slide, if FortiGate is integrated with FortiSandbox, you will see a second analytics log for all viruses detected using FortiGuard antivirus signatures. If you review the analytics log details, you will see that FortiGate sent the file to FortiSandbox.



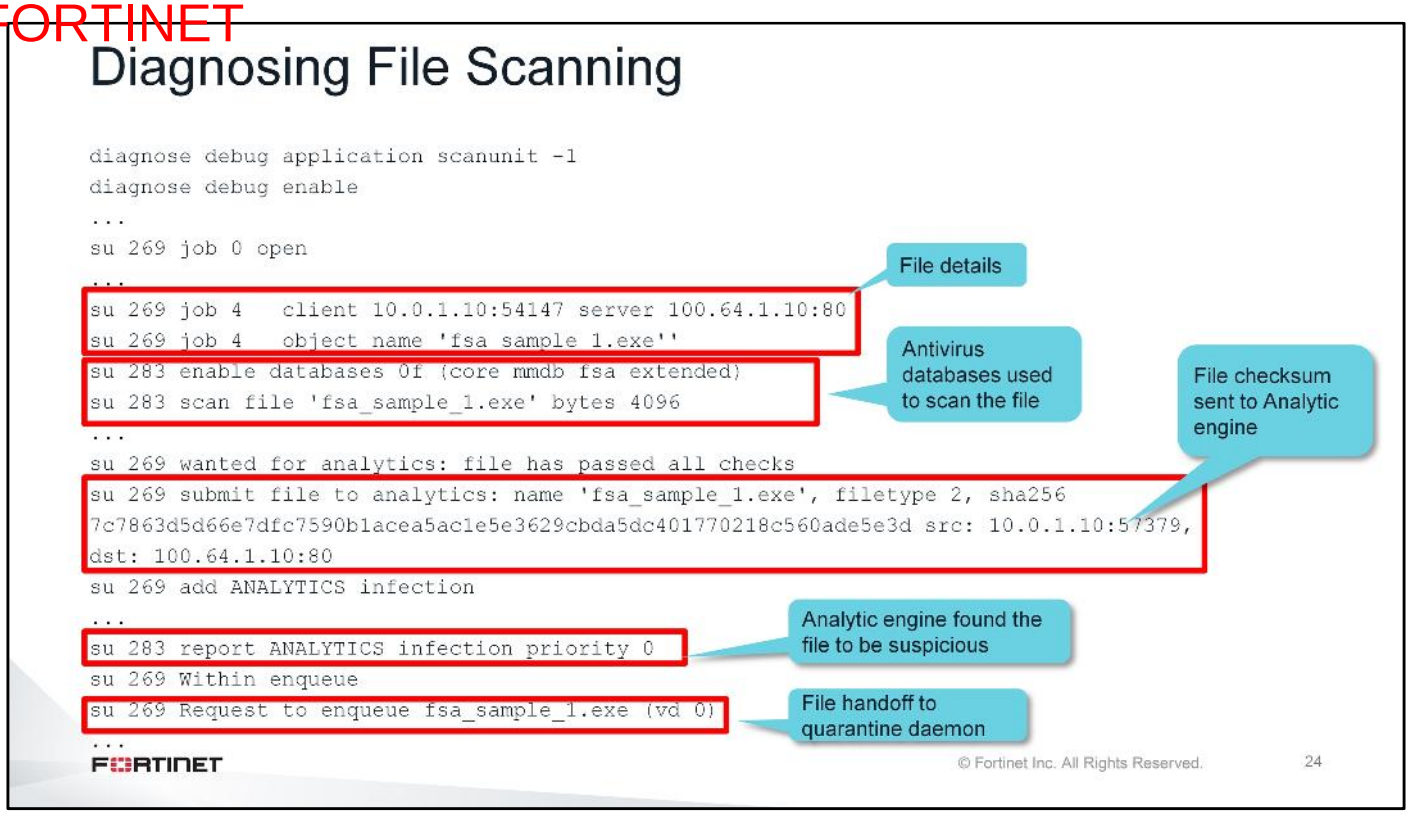
In this section, you will learn how to verify FortiSandbox operation using FortiGate logs. You will also learn how to debug the daemons involved in scanning and offloading files to FortiSandbox.



FortiGate generates two logs for each file submitted to FortiSandbox. FortiGate generates the first log entry when the file is submitted to FortiSandbox. You can quickly identify this log entry because the **Virus/Botnet** column will be empty, and the **Action** column will indicate **analytics**.

FortiGate generates the second log entry after FortiSandbox returns a verdict. The **Virus/Botnet** column will indicate the FortiSandbox rating (high risk, medium risk, low risk, or clean).

Any file blocked using the malware database generated by FortiSandbox will display a virus name starting with **FSA/** followed by the rating.

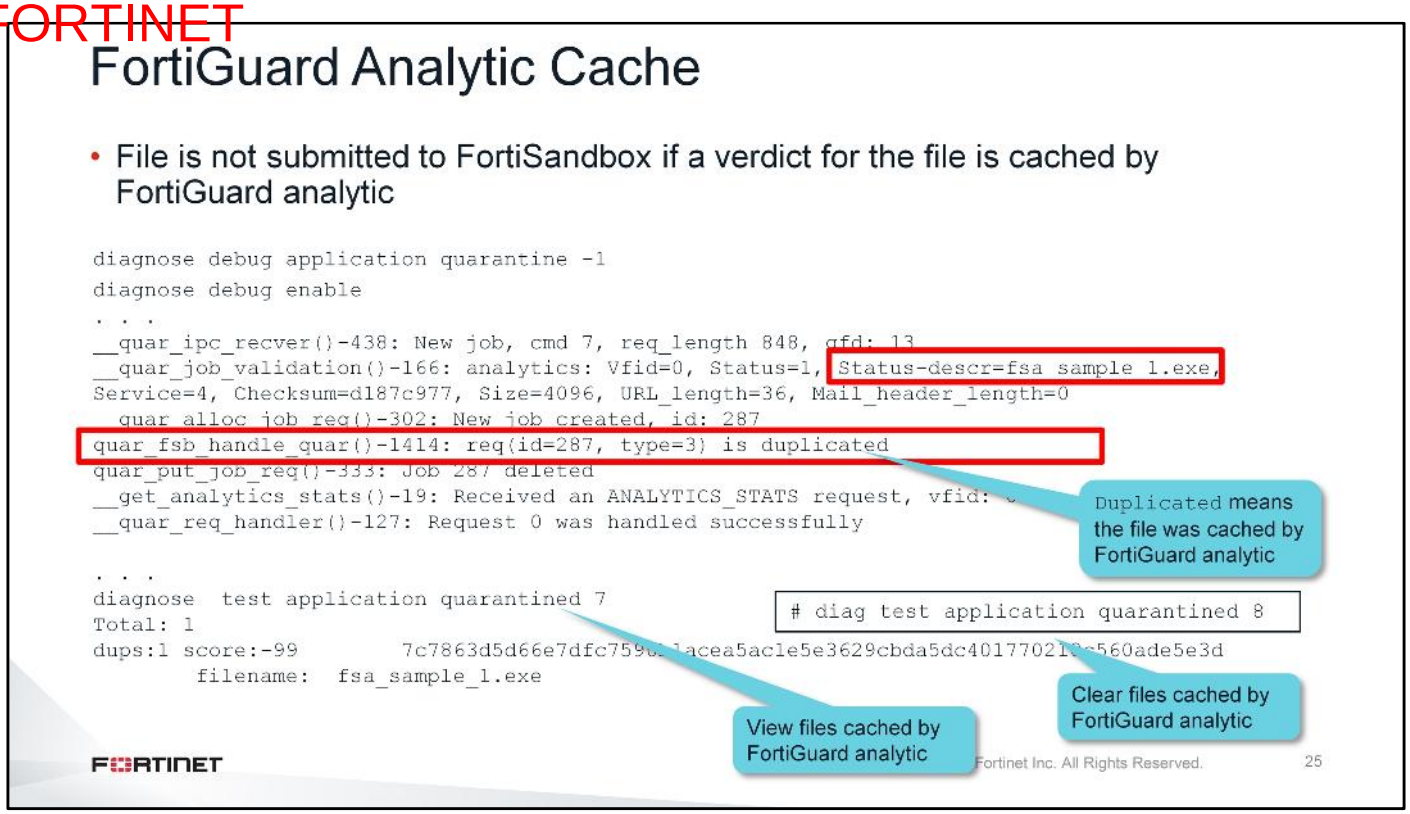


There are two daemons involved in submitting files to FortiSandbox. The first daemon is scanunit. The scanunit daemon performs multiple types of scanning for web pages, files, and email messages. The scanunit daemon also decompresses archives and scans files inside archives.

To view the real-time debug messages, use the command shown on this slide. The debug output lists the session details (client and server IPs), as well as the name of the file being scanned. This is especially useful when dealing with large amounts of debug output. You should log the debug output to a file, and then search for specific file names.

The debug output lists the databases being used to scan the file. In this example, you can see that the `fsa_sample_1.exe` file is being scanned with the default (`core`), mobile malware (`mmdb`), FortiSandbox (`fsa`), and `extended` antivirus databases.

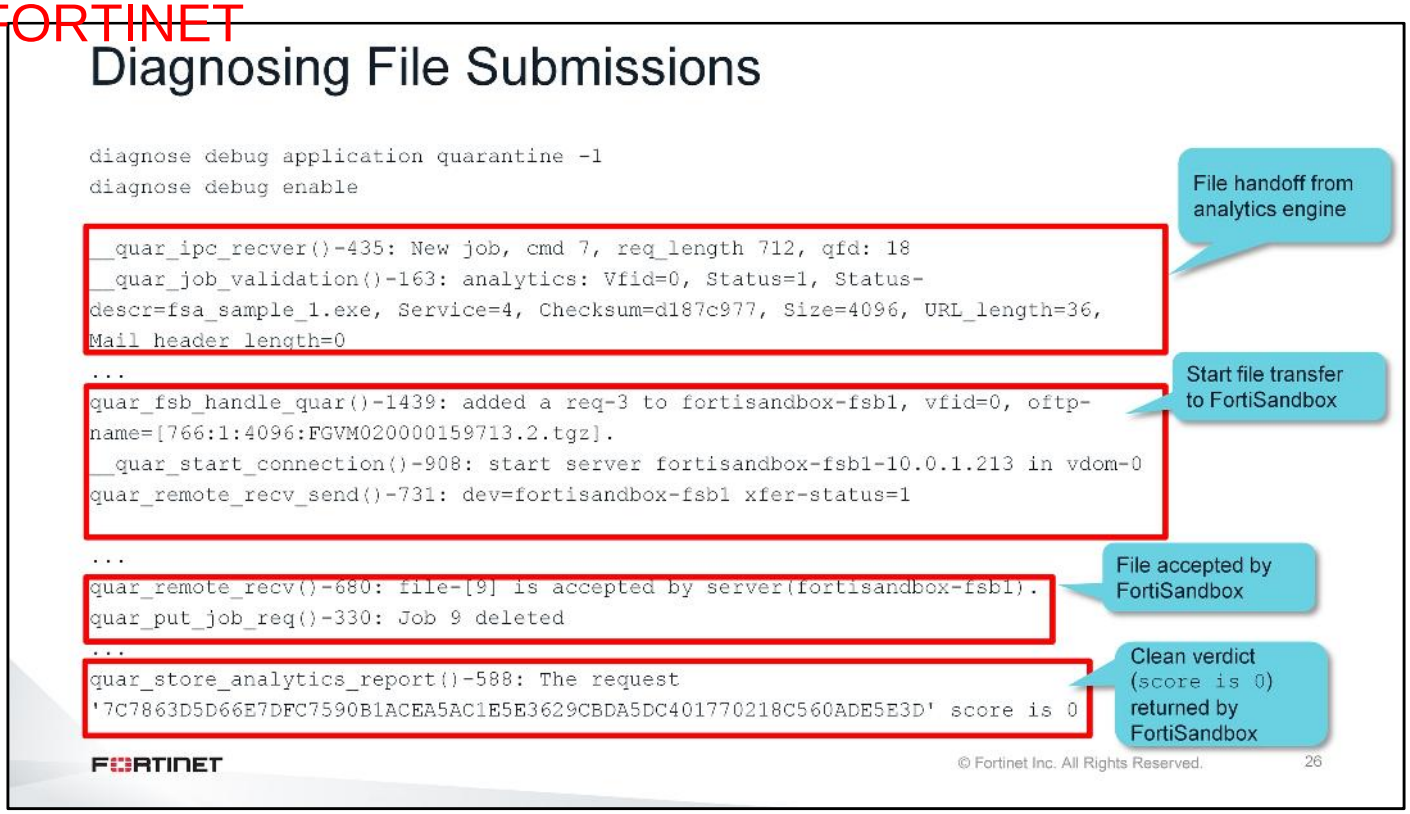
The scanunit daemon also does a quick check by sending the file checksum to Analytic engine. If Analytic engine determines that the file is suspicious, it will return a verdict of infection. The file is then handed off to the quarantine daemon.



When you run a diagnostic and the quarantine handler return a verdict of `duplicated`, that means the file has a verdict that is cached locally on the FortiGate. The checksum of the file that is currently being scanned matches the checksum of a file that was quarantined previously, so FortiGate will not send that file to FortiSandbox.

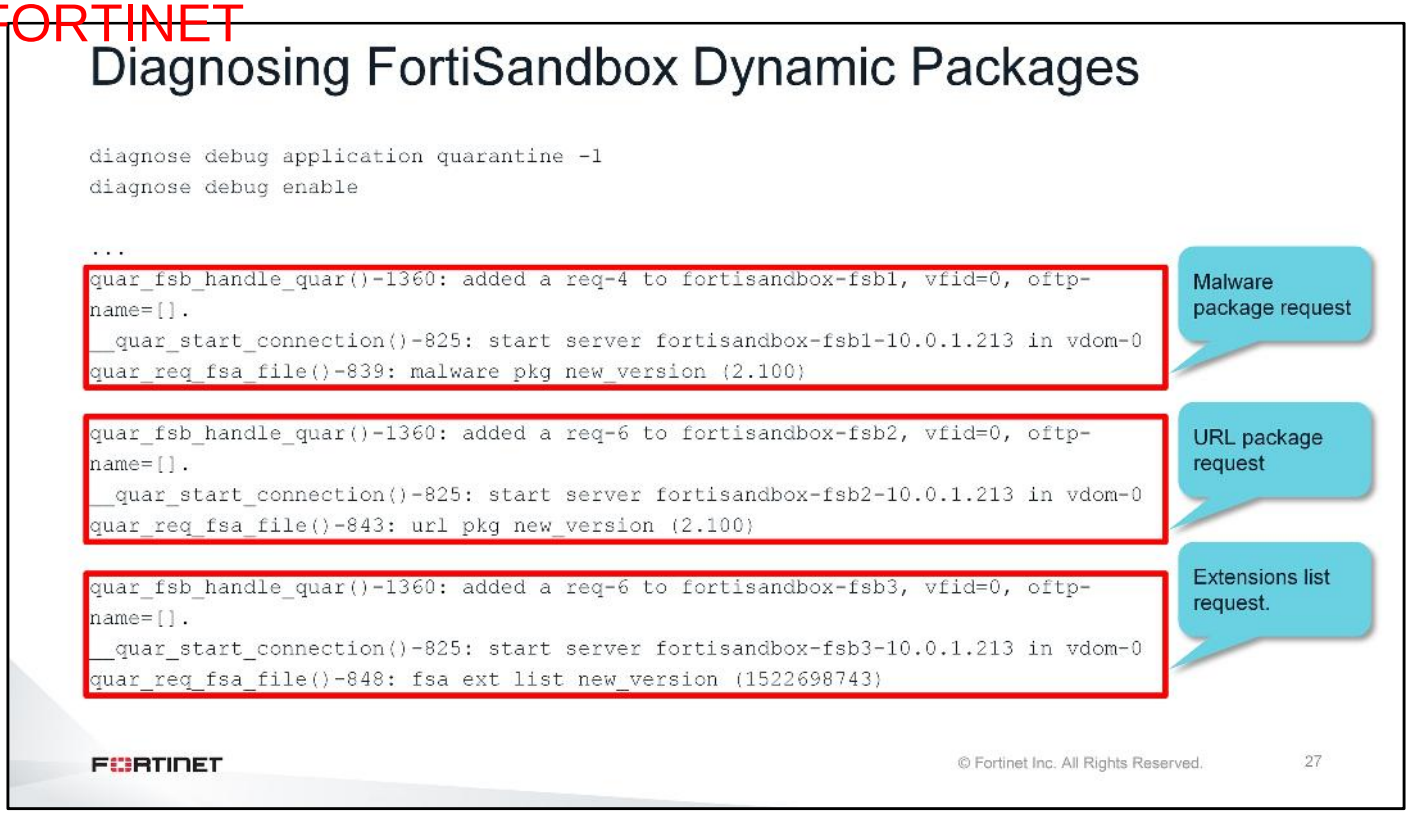
You can view the files that have been cached by FortiGuard analytic by running the command `diagnose test application quarantined 7`, which will show the score, checksum, and file name.

You can also clear the FortiGuard analytic cache by running the command `diagnose test application quarantined 8`.

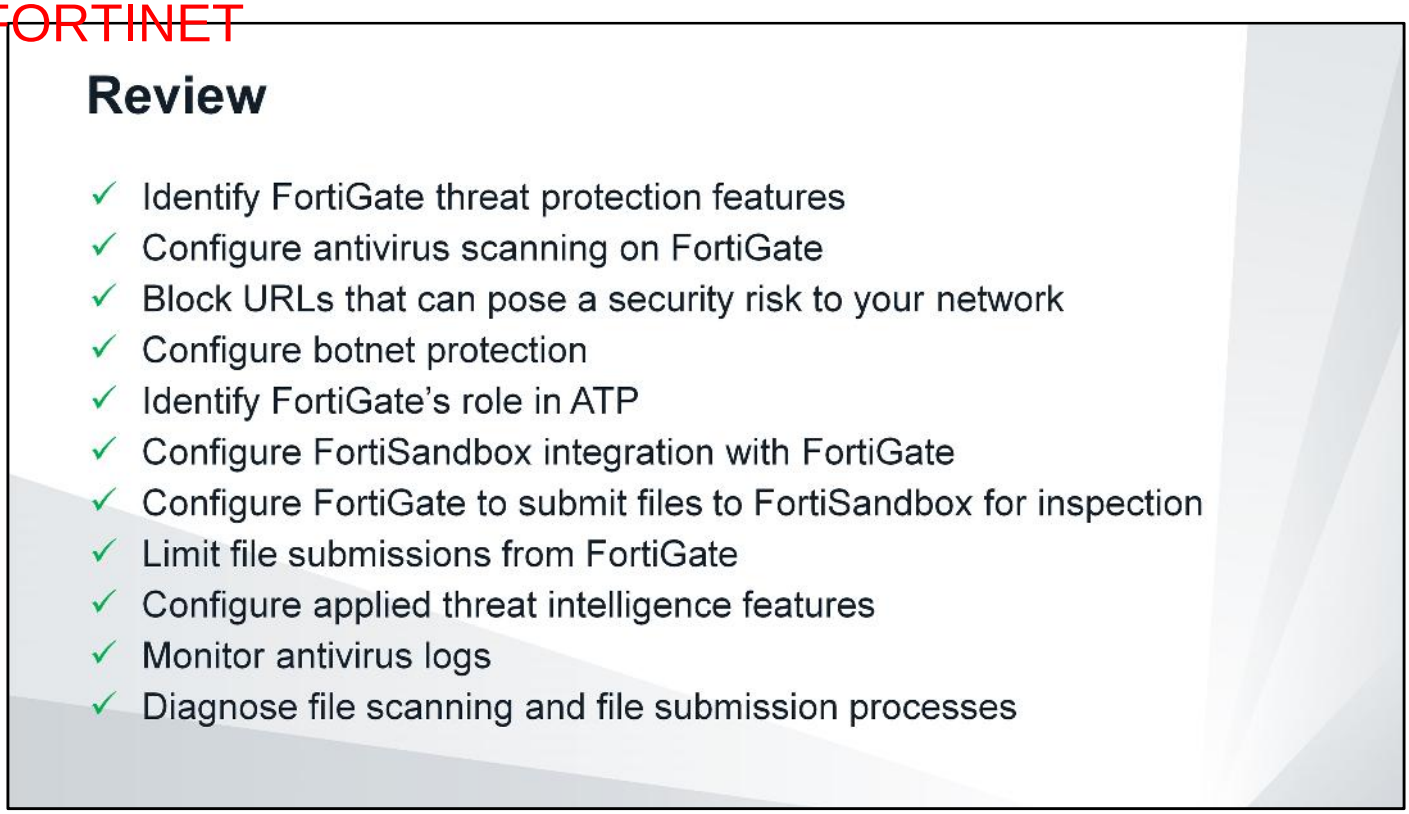


The quarantine daemon is involved in submitting files to FortiSandbox. For identification purposes, the serial number of FortiGate, and the VDOM name are included in the transfer.

The quarantine daemon uses OFTP to transfer files on port 514. By default, encryption is enabled, but you can modify that on the CLI. The quarantine daemon also receives the verdicts returned by FortiSandbox.

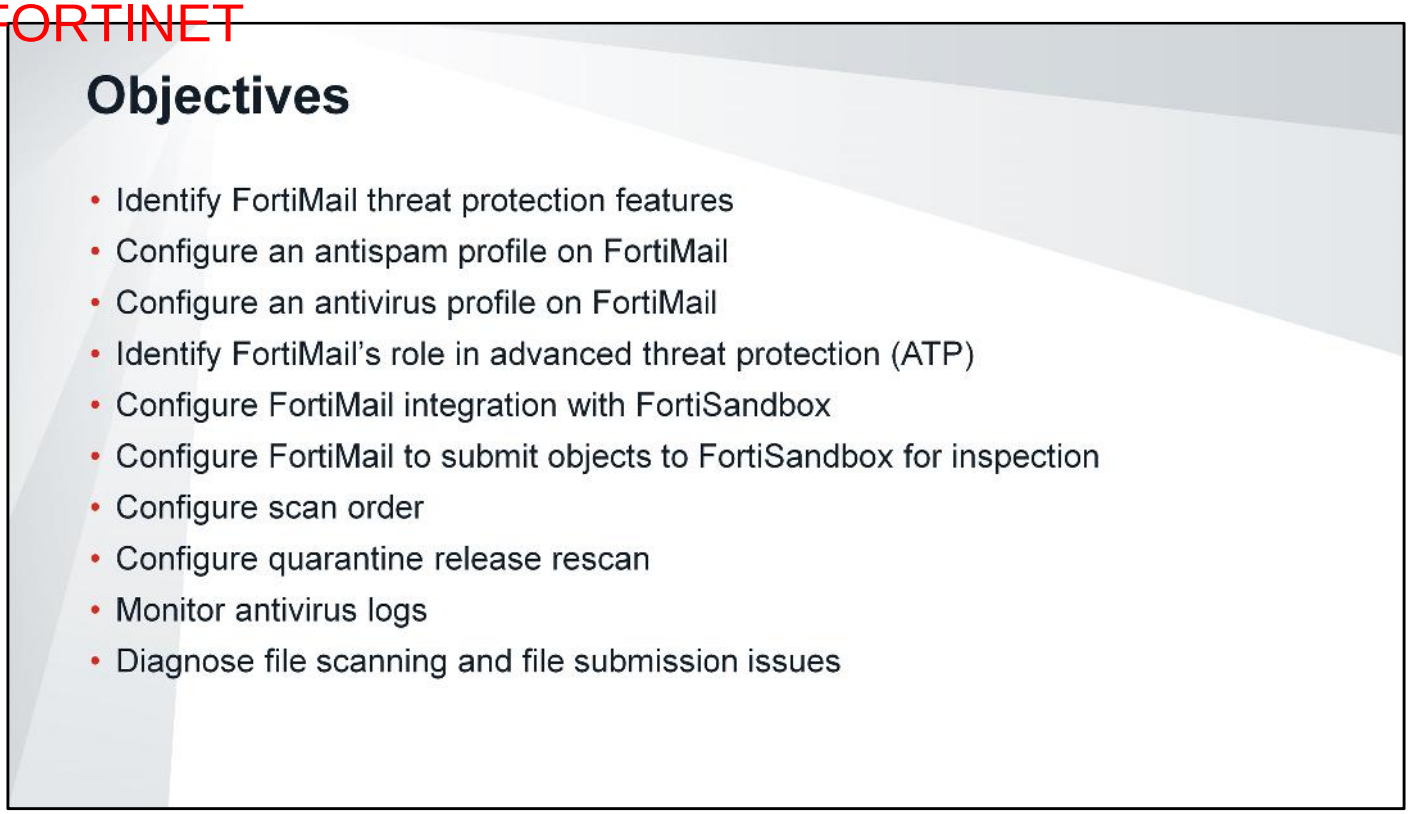


The quarantine daemon is responsible for sending requests for the dynamic lists generated by FortiSandbox. This includes the malware package, URL package, and the extension lists. FortiGate sends the version number of its current packages to FortiSandbox. FortiSandbox compares FortiGate's package version with its own. If the package version on FortiGate is earlier than the package version on FortiSandbox, then FortiSandbox will send the new packages.



This slide shows the objectives that you covered in this lesson. By mastering the objectives covered in this lesson, you learned how to protect your network from advanced threats.

In this lesson, you will learn how to protect your email network from advanced threats.



After completing this lesson, you should be able to perform the objectives shown on this slide.

By demonstrating competence in FortiMail's threat protection and ATP integration concepts and configuration requirements, you will be able to protect your email network from advanced threats.

In this section, you will learn about the threat protection features available on FortiMail and how to configure them.

FortiMail Overview

- Gateway mode
  - Mail is delivered to FortiMail, scrubbed of threats, and forwarded to destination mail server

- Transparent mode
  - Deployed physically in line of the SMTP path
  - Commonly used by ISPs and carriers

- Server mode
  - Full featured mail server
  - Receives, inspects, and delivers email to user mailboxes stored in a local database

FORTINET

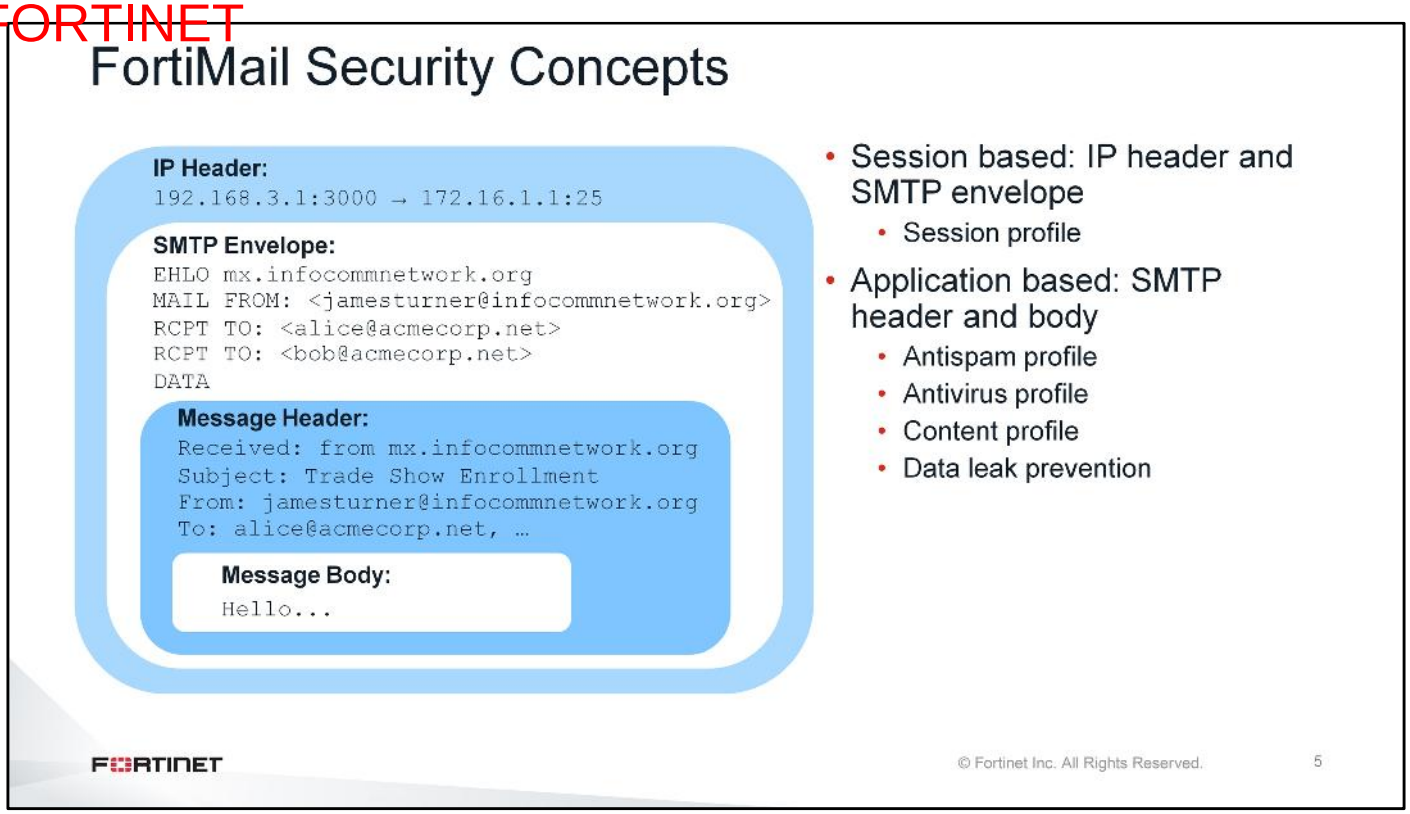
4

FortiMail is an email security device that provides inbound and outbound threat protection, as well as data loss prevention and encryption. You can deploy FortiMail in three distinct operating modes: gateway, transparent, and server. The mode you select depends on the type of network in which you will be using FortiMail.

In gateway mode, FortiMail provides full mail transfer agent (MTA) functionality. In the email path, FortiMail sits in front of an existing email server and scans email. If FortiMail detects any spam email, it discards them or stores them in the user quarantine mailboxes on the local FortiMail. FortiMail delivers all clean email to the back-end mail server.

In transparent mode, FortiMail is physically located on the email path so that it can intercept email traffic transparently for inspection. When operating in transparent mode, FortiMail isn't the intended IP destination of the email; therefore, no DNS or destination NAT (DNAT) rule change is required. When you deploy FortiMail in transparent mode, you don’t have to make any DNS or IP address changes in your environment. Transparent mode is often used in large MSSP or carrier environments.

In server mode, FortiMail provides all of the typical functions of an email server as well as security scans. You can use FortiMail operating in server mode as a drop-in replacement for retiring email servers. It is also an excellent choice for environments where you are deploying internal email servers for the first time.

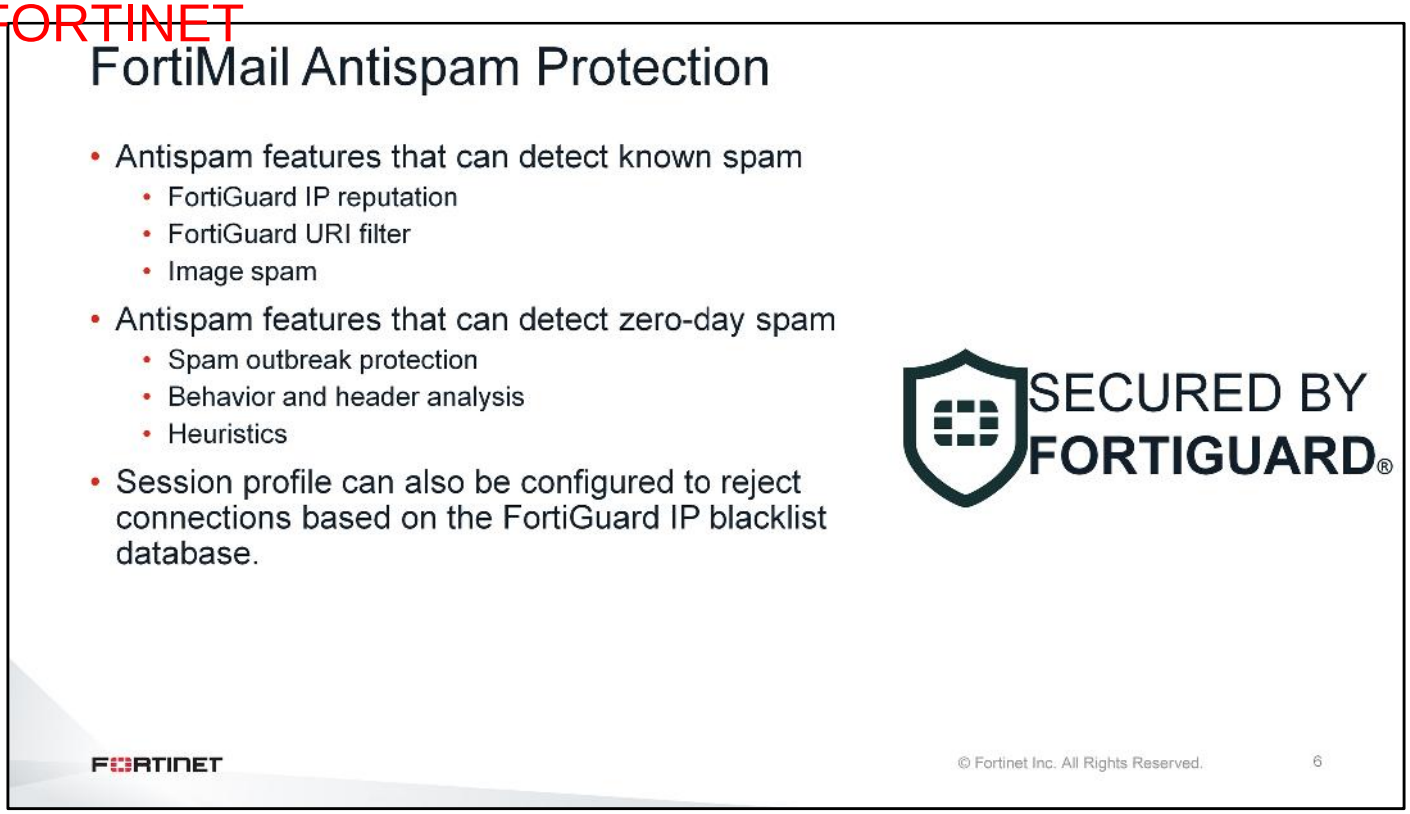


FortiMail's threat protection features can be broken into two categories: session-based features, and application-based features.

The overall purpose of session profile inspections is to detect suspicious activities as soon as possible. This allows FortiMail to take action early and eliminates the need to perform some, or all, of the more resource-intensive scans that would be required after the entire email message arrives. You can configure a session profile to control email session volume based on sender reputation, reject sessions from blacklisted servers, validate senders using sender policy framework (SPF) records and domainkeys identified mail (DKIM) keys, detect abnormalities in SMTP sessions, and so on.

The application layer inspection features are spread across the antispam, antivirus, content, and data leak prevention profiles. You can configure the antispam profile to detect and block spam emails based on various spam characteristics. You can configure the antivirus profiles to inspect and strip malicious attachments. You can configure the content and data leak prevention profile to inspect and block emails based on various email characteristics—specific message headers or attachment type, size, content or count, and so on.

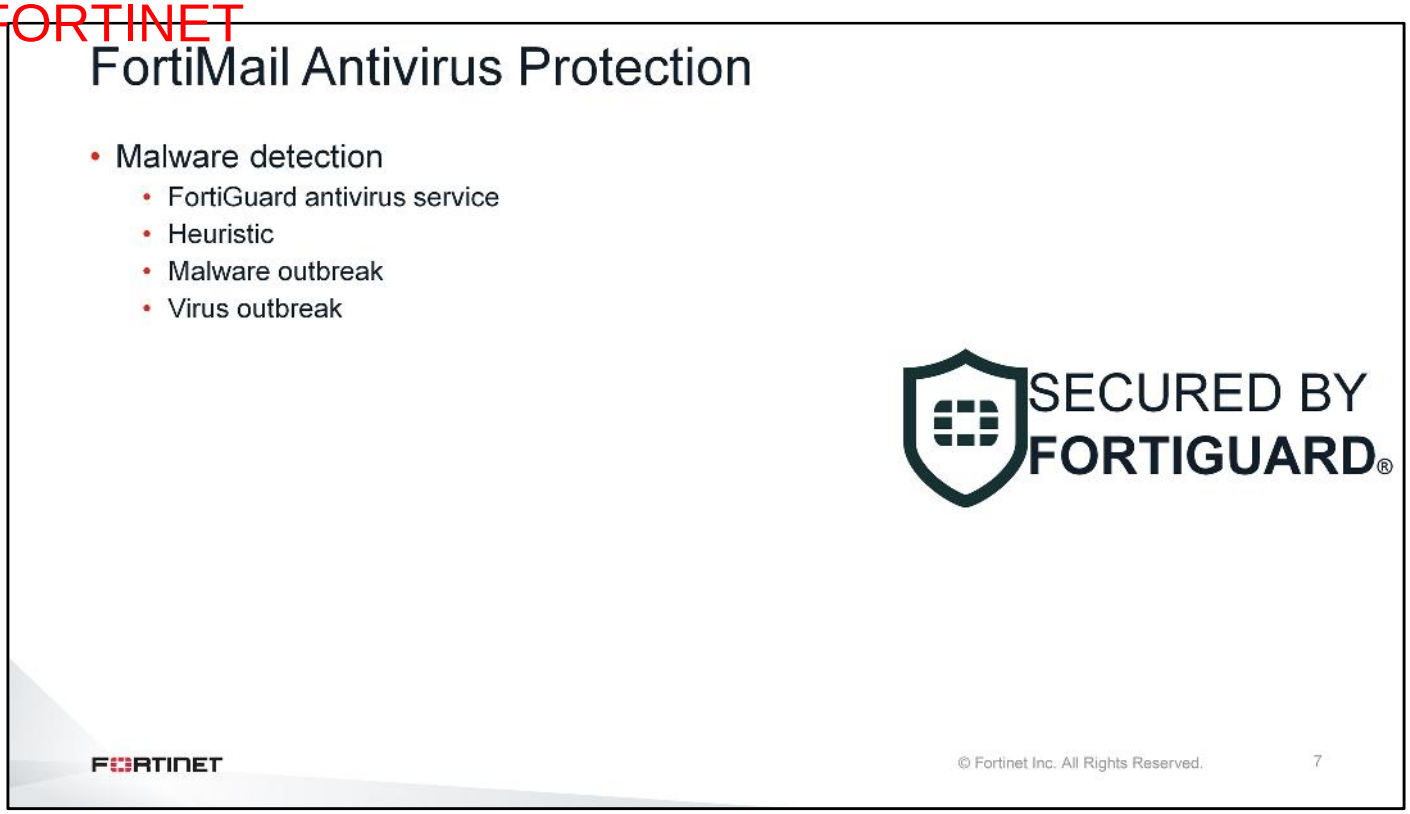
You will learn about the threat protection features available in the antispam and antivirus profiles—specifically the ones that leverage FortiGuard services.



The antispam profile features can be broken down into two categories—features that can detect known spam, and features that can detect zero-day spam.

The FortiGuard IP reputation feature queries the FortiGuard antispam service to determine if the remote sender's IP address is in the FortiGuard blacklist database. The FortiGuard URI filter sorts known URIs into categories, such as phishing, spam, and malicious. If an email message contains any URIs that match the enabled categories in the URI filter, FortiMail treats that message as spam. The IP reputation and URI filter features combined will block majority of the known spam emails being processed by FortiMail. The image spam feature analyzes embedded images for spam characteristics. While image-based spam emails aren't as common, this feature should still be used to catch the random occurrences.

Of the features that can detect zero-day spam, the spam outbreak protection feature is the most effective. This feature detects email that shares similarities to recently-observed, known spam, but doesn't have a FortiGuard rating yet. FortiMail will queue these emails for a specified period, and requery for ratings from FortiGuard, after the hold period ends. The default hold period of 30 minutes is usually long enough for FortiGuard to update its various rating databases to properly identify the email. Behavior analysis uses a variety of methods to identify spam not caught directly by FortiGuard. By applying elements of heuristics and a fuzzy matching algorithm, which compares spam recently detected (within the past 6 hours) by FortiGuard signatures on the device in question, behavioral analysis can detect changing spam samples. Header analysis looks for the presence of specific header entries that are commonly found together in spam email. Heuristics uses a set of rules that are created from known spam content. These rules use PERL-compatible regular expressions (PCRE) to locate spam attributes within each email. Heuristics is resource intensive, and, if improperly configured, prone to false positives.

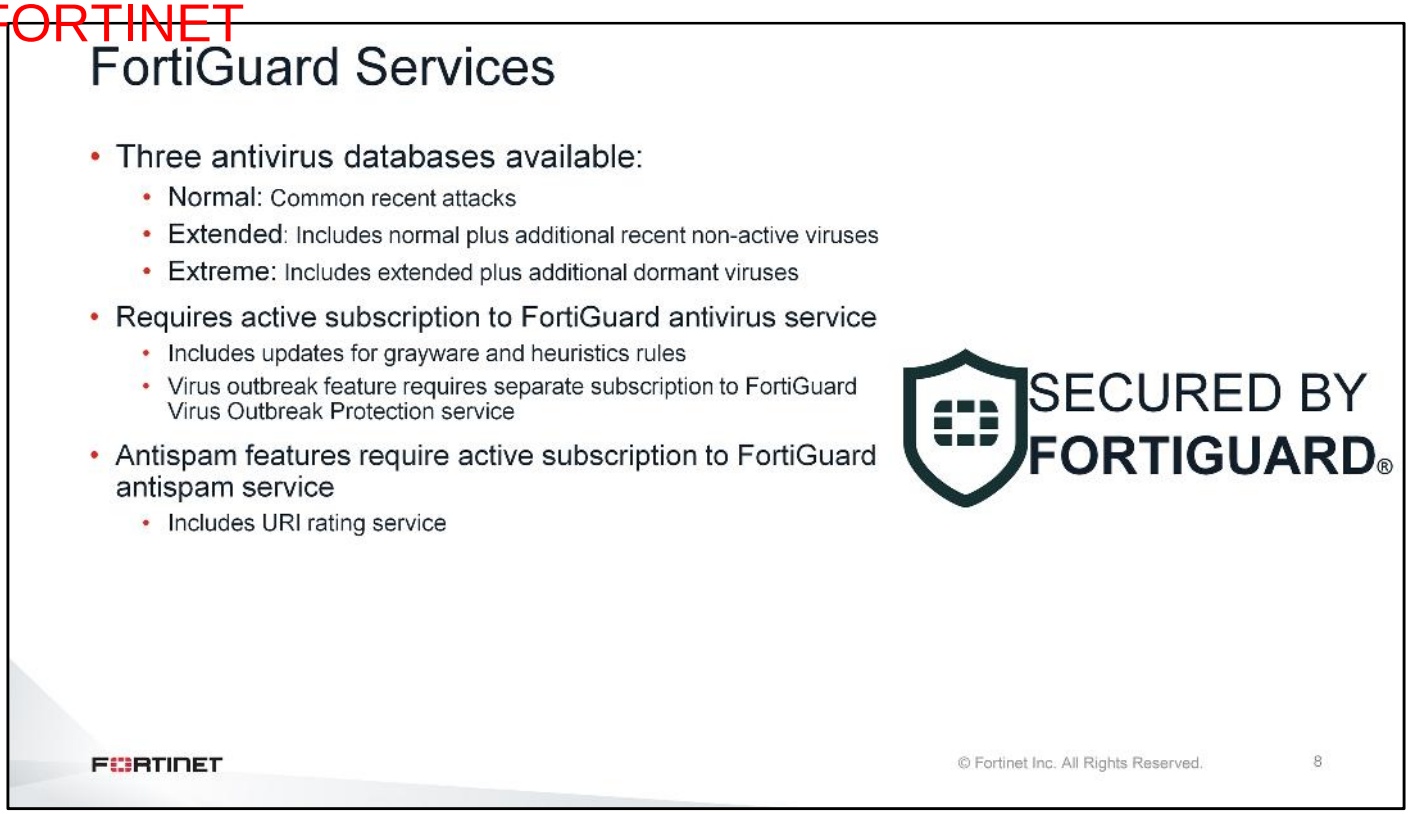


The FortiGuard antivirus service performs signature-based detection to detect known malicious attachments. Fortinet's unique content pattern recognition language (CPRL) allows single signatures to protect against multiple different malware strains. FortiMail's antivirus scanning uses the same FortiGuard virus signature databases that are used in FortiGate firewalls. This database also includes grayware signatures.

You can enable heuristics for some light sandboxing. FortiMail uses the local sandbox to examine the construction of files to look for characteristics commonly found in viruses. It also emulates the execution of the content to look for typical virus behavior.

The malware outbreak feature uses data analytics by FortiGuard to generate rating information on malicious email content. FortiGuard labs receive global requests for ratings of sender IPs, content, and attachments. A sudden uptick of requests for a specific IP reputation, or a file checksum, can indicate a new outbreak. The malware outbreak feature can detect such occurrences.

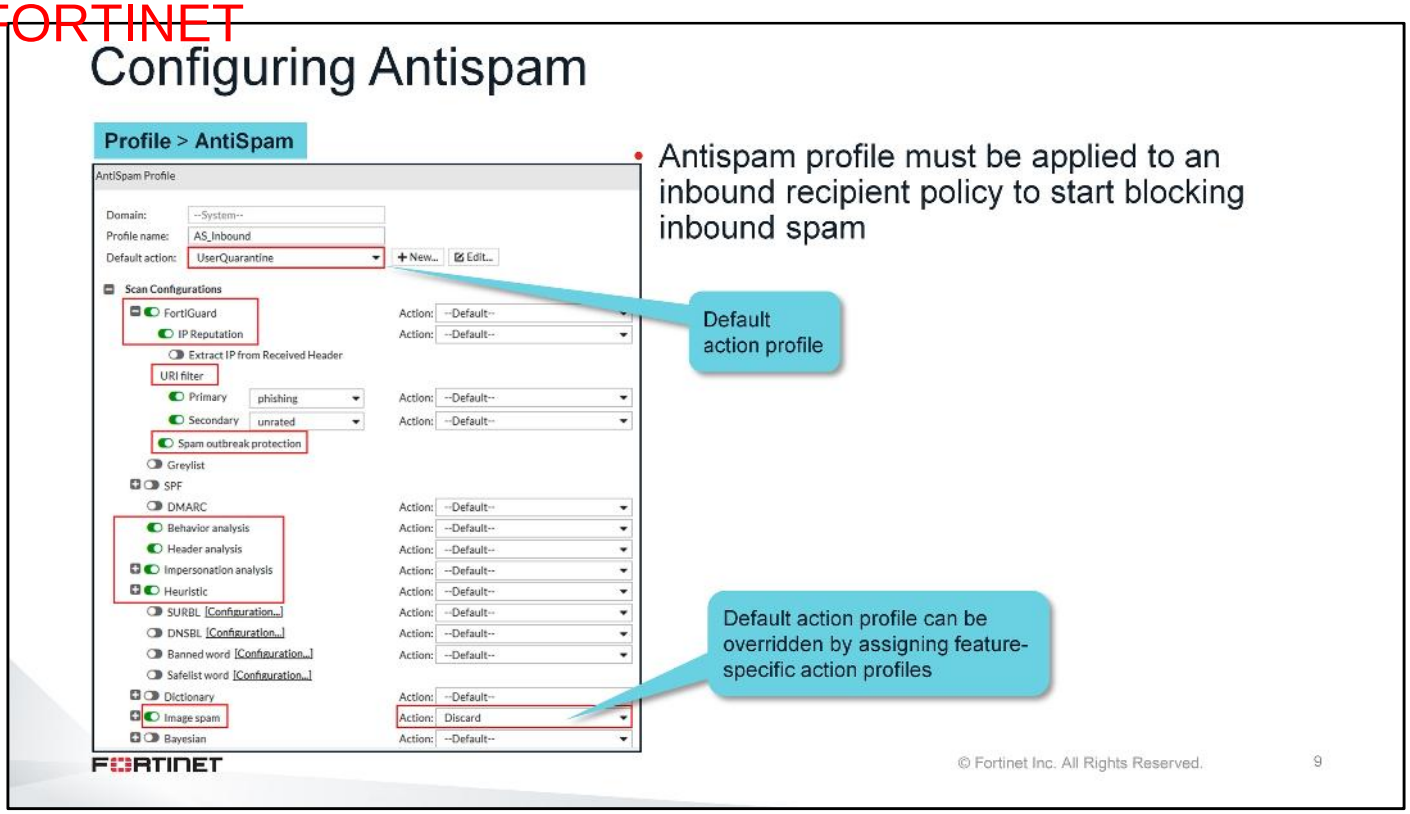
The virus outbreak features allows FortiMail to query the global threat intelligence network, which is comprised of various sources such as global sandbox intelligence, Cyber Threat Alliance, and other third-party sources.



Just like FortiGate devices, FortiMail has access to three antivirus databases. The normal database includes signatures for common recent attacks. The extended database contains all signatures from the normal database, as well as additional recent non-active viruses. The extreme database contains signatures from the previous two databases a well as dormant viruses, or viruses aimed at legacy systems. The extreme database is available on only high-end models.

The FortiGuard Antivirus Service subscription includes regular updates for the antivirus database, the grayware database, heuristics rules, and the malware outbreak service. The virus outbreak service requires a separate subscription to FortiGuard Virus Outbreak Protection service.

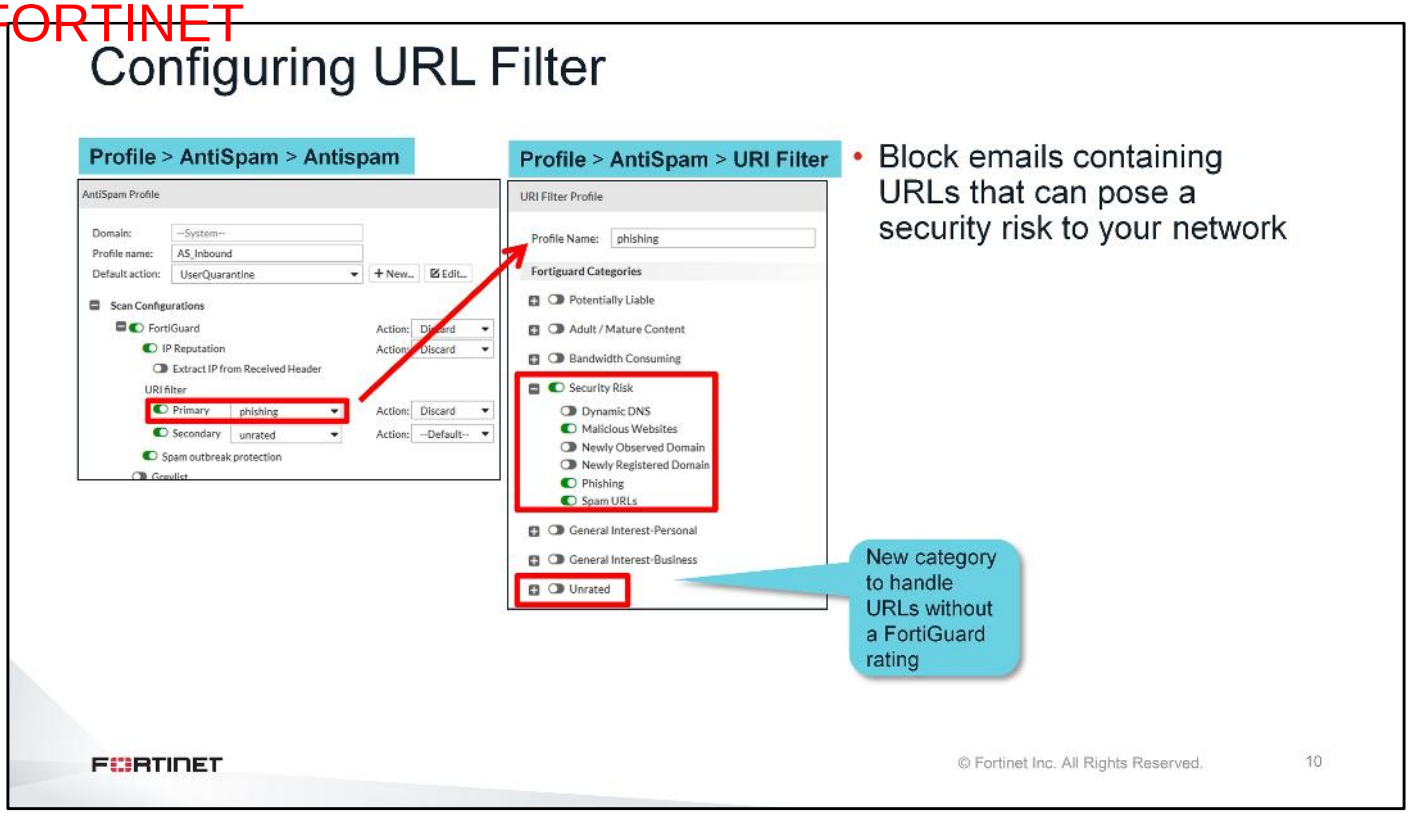
The antispam features requires an active subscription to FortiGuard Antispam Service, which also includes the URI rating service.



You can configure security inspections on FortiMail in profiles. Each security profile can have an action profile associated with it. The action profile defines what FortiMail will do when it detects a security violation.

The antispam profile has a default action profile, which you can configure as the default action to take when FortiMail detects spam email using any of the enabled inspections. You can also assign a feature-specific action profile to override the default action profile. You can use the default action profile combined with the feature-specific profile to build an antispam configuration profile that uses mail storage space efficiently. For example, you can configure the antispam profile to use a default action of user quarantine, but use a discard action for emails identified as spam using the IP reputation and URI filter features. This configuration will ensure emails that are known spam are not wasting FortiMail's mail disk space by being sent to user quarantine.

After configuring the antispam profile, you must apply it to an inbound recipient policy to start blocking inbound spam. You should also consider configuring a separate antispam profile for outbound emails, and apply it to an outbound recipient policy to block outbound spam. Usually, the outbound antispam profile has different requirements than the inbound antispam profile.

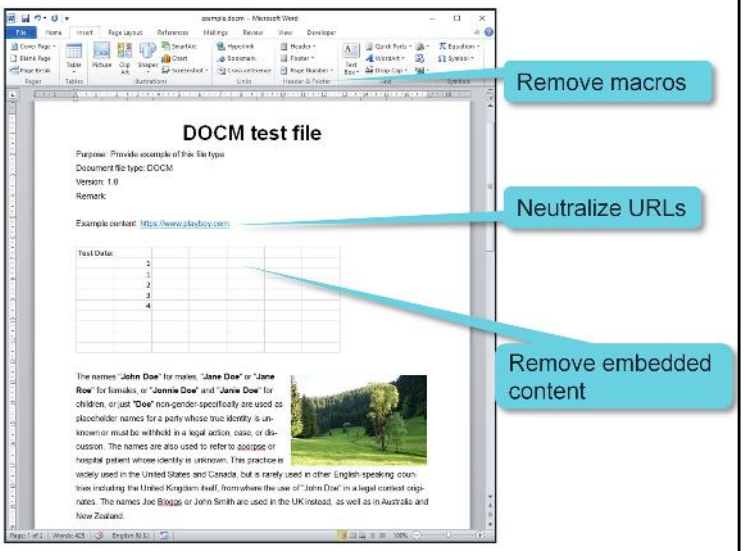


You must configure a URI filter that includes URI categories that you want to block, and apply it to the antispam profile. Each antispam profile supports two URI filter profiles. This allows you to configure two different sets of URI categories with different actions. For example, you may want to discard all emails with URIs from the security risk category, but send emails with URIs from the unrated category to user quarantines.

The URI filter feature allows for a lot of customization. In most deployments, you should filter malicious websites, phishing, and spam URLs in the security risk category; however, you can customize the URI filter profile to filter email messages containing URIs that, traditionally, would not be considered spam.

Content Disarm and Reconstruction

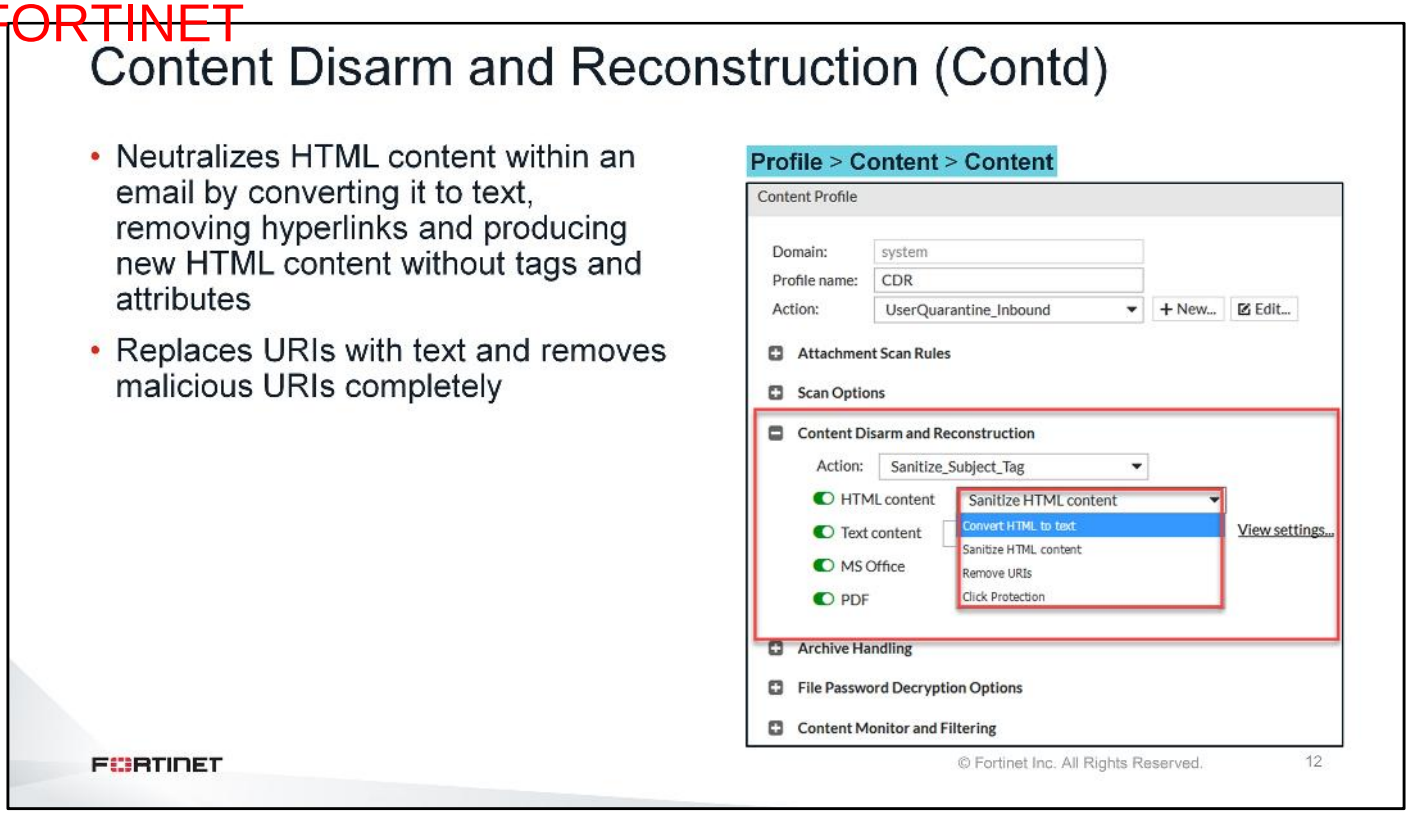
- Removes potentially exploitable content and replaces it with content that's known to be safe
- Disarms MS Office and PDF attachments from hazardous macros, active scripts, and other active contents



FORTINET

11

HTML content in the email body and attachments may contain potentially hazardous tags and attributes (such as hyperlinks and scripts). MS Office and PDF attachments may contain potentially hazardous macros, active scripts, and other active content. FortiMail provides content disarm and reconstruction (CDR) to remove or neutralize the potentially hazardous content and reconstruct the email message and attachment files.



If you enable **HTML content**, FortiMail detects HTML tags in email messages. Select one of the following actions in the **HTML content** drop-down list to specify the action FortiMail will take:

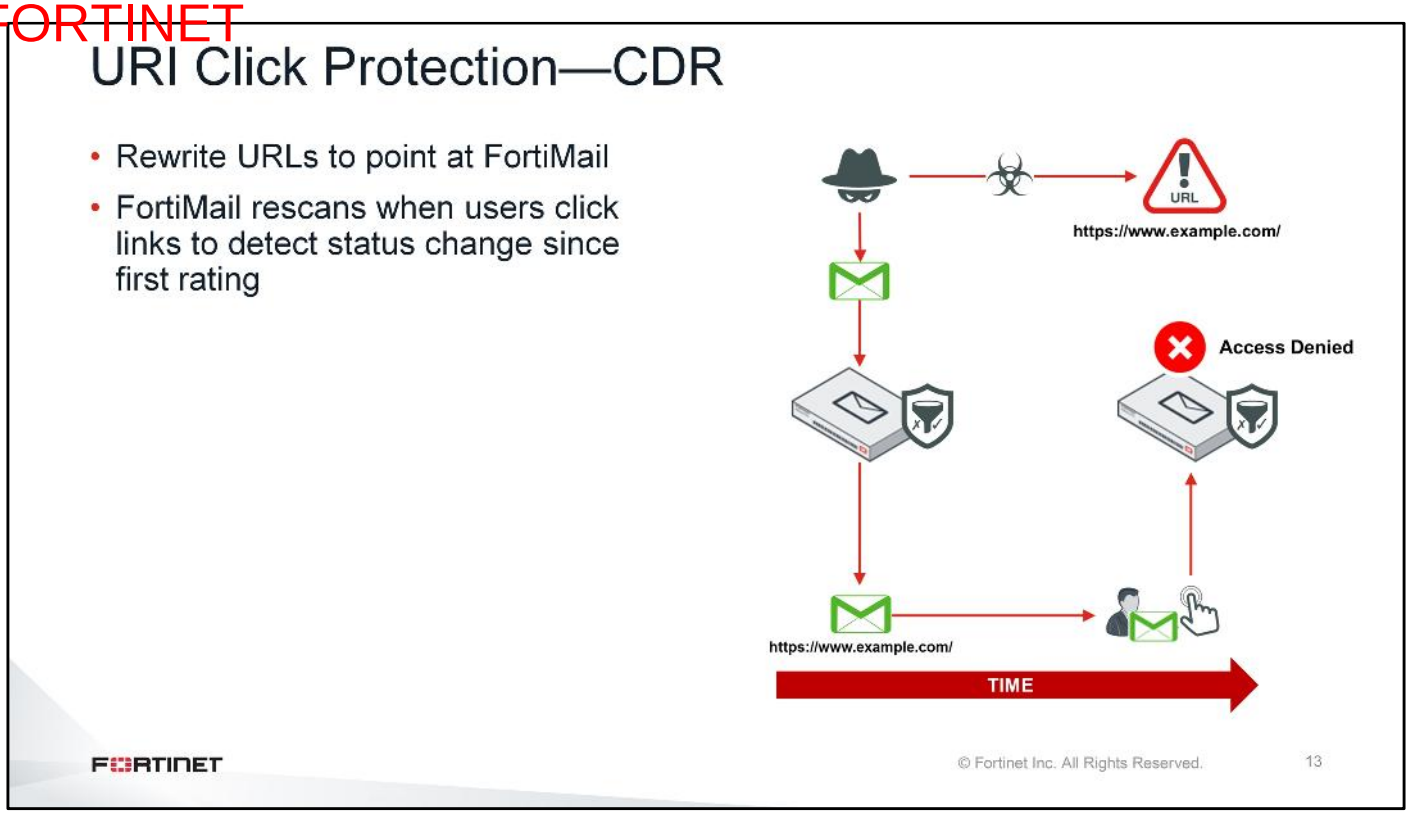
- **Convert HTML to text:** Converts HTML text to text-only content
- **Sanitize HTML content:** Produces new HTML content by removing the potentially hazardous tags and attributes (such as hyperlinks and scripts) and preserving only the safe and essential tags (such as formatting tags)
- **Remove URIs:** Removes URIs in the email message
- **Click Protection:** Rewrite the URIs and, in case users click the URIs, scans the URIs and then takes the configured actions

If you enable **Text content**, FortiMail detects URIs in email messages. Select one of the following actions in the **Text content** drop-down list to specify the action FortiMail will take:

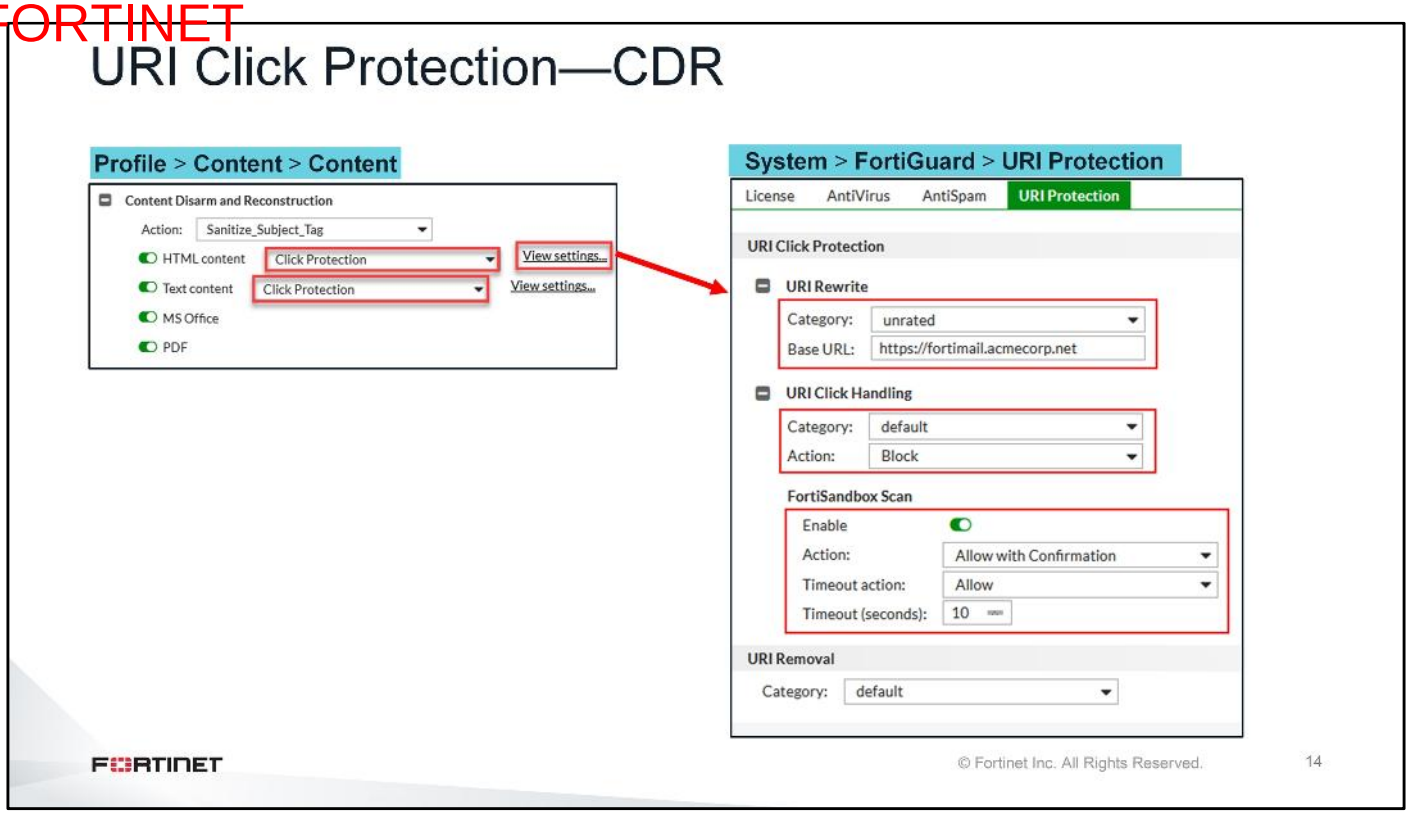
- **Remove URIs:** Removes URIs in the body of the email message
- **Click Protection:** Rewrites the URIs and, in case the user clicks the URIs, scans the URIs and then takes the configured actions

If you enable **MS Office**, FortiMail disarms and reconstructs MS Office attachments, including .zip files that have been compressed once.

If you enable **PDF**, FortiMail disarms and reconstructs the PDF attachments, including .zip files that have been compressed once



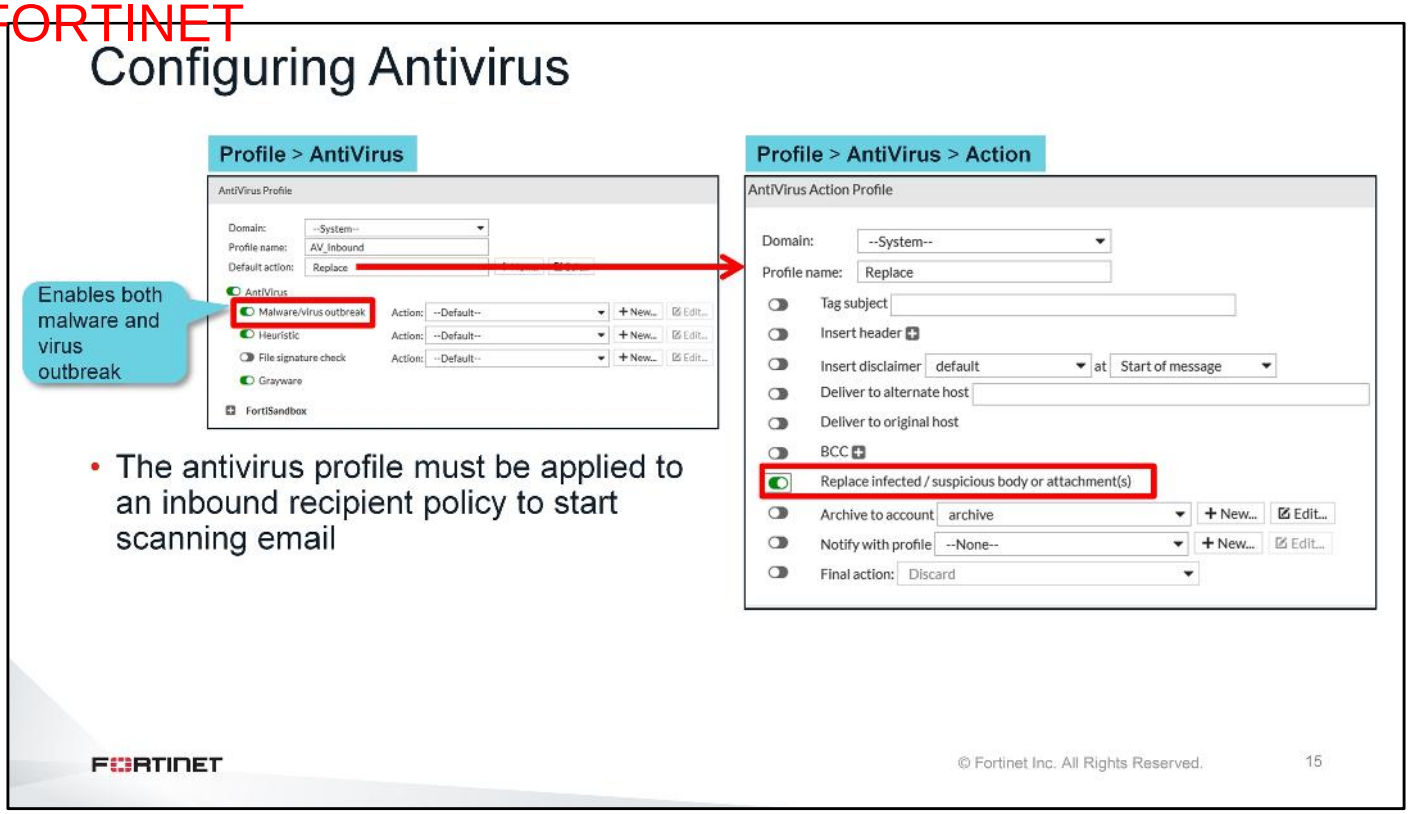
FortiMail can rescan URLs that have previously passed the security inspection. When an attacker sends an email with a URL link, initially that link might be safe and it will pass the inspection check on the FortiMail. However, it is possible that the link could be compromised after a certain period of time. Attackers use this method to avoid detection and will only compromise the server after a certain period of time. To avoid this kind of attack, FortiMail rewrites the URL to point to itself. So, when the user clicks on the link, that now points to FortiMail, and the original URL is inspected again, if the link is compromised, FortiMail takes the configured action.



URI Click Protection is available for HTML content and text content. To protect users from harmful or spam URIs, such as phishing or advertising web sites, FortiMail uses the FortiGuard URI filter service and FortiSandbox to scan the URIs after the users clicks on them. Depending on the inspection results from FortiGuard and FortiSandbox, you can decide if you will allow users to access the URIs, or if you will block the URIs.

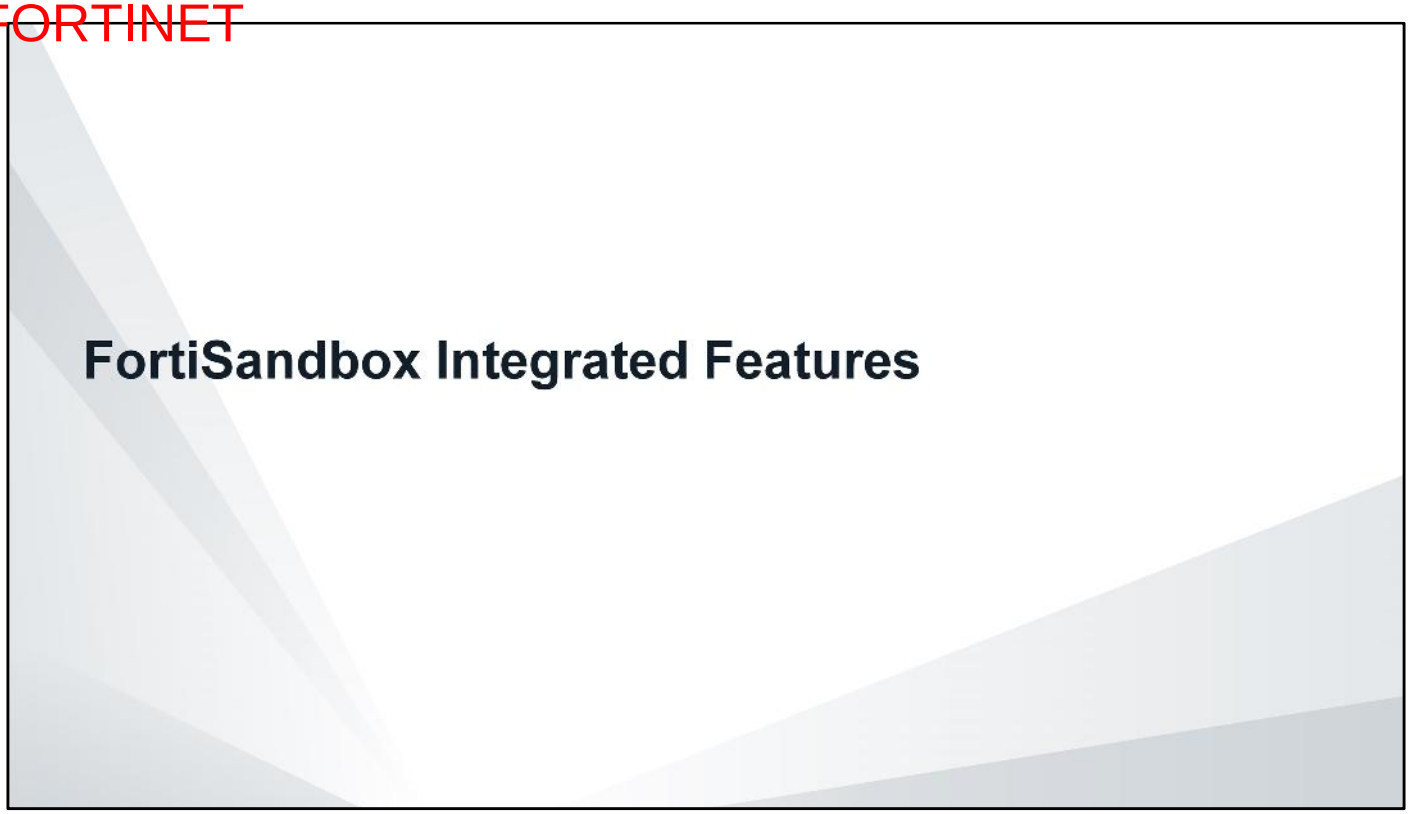
If you select **Allow with Confirmation** FortiMail allows access with a warning. If you select **Block,** FortiMail blocks access. If you select **Submit only**, FortiMail allows access while it sends the URIs for scanning.

When FortiMail sends URIs to FortiSandbox for scanning, it may take a while for FortiSandbox to return the results. In the **Timeout (seconds)** field, specify how long you want to wait for results *before* you select **Block**, **Allow**, or **Allow with Confirmation** in the **Timeout action** drop-down list.



To enable local antivirus scanning techniques and actions, you must create an antivirus profile first. You should configure the antivirus action profile to replace any malicious content. This will make sure that the email body is still delivered to the original recipient, but with the malicious attachment removed.

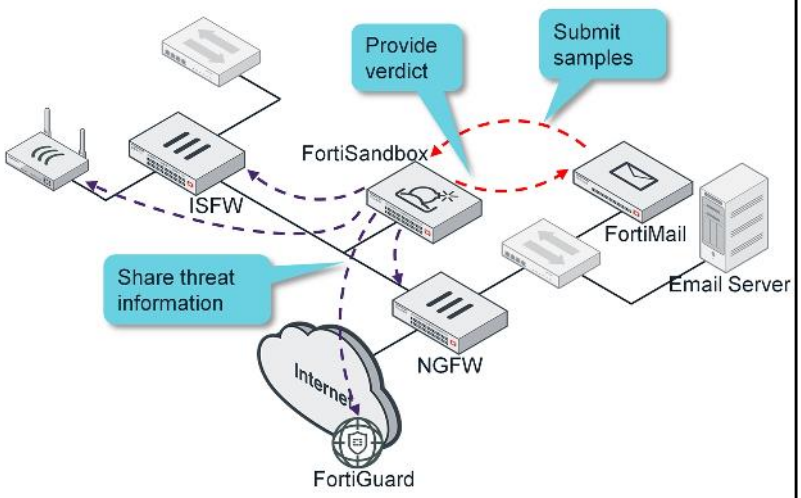
It is highly recommended that you enable antivirus scanning in both inbound and outbound recipient policies.



In this section, you will learn how to integrate FortiMail with FortiSandbox. You will also learn how to enable quarantine release re-scan of emails with malicious attachments.

FortiSandbox Integration

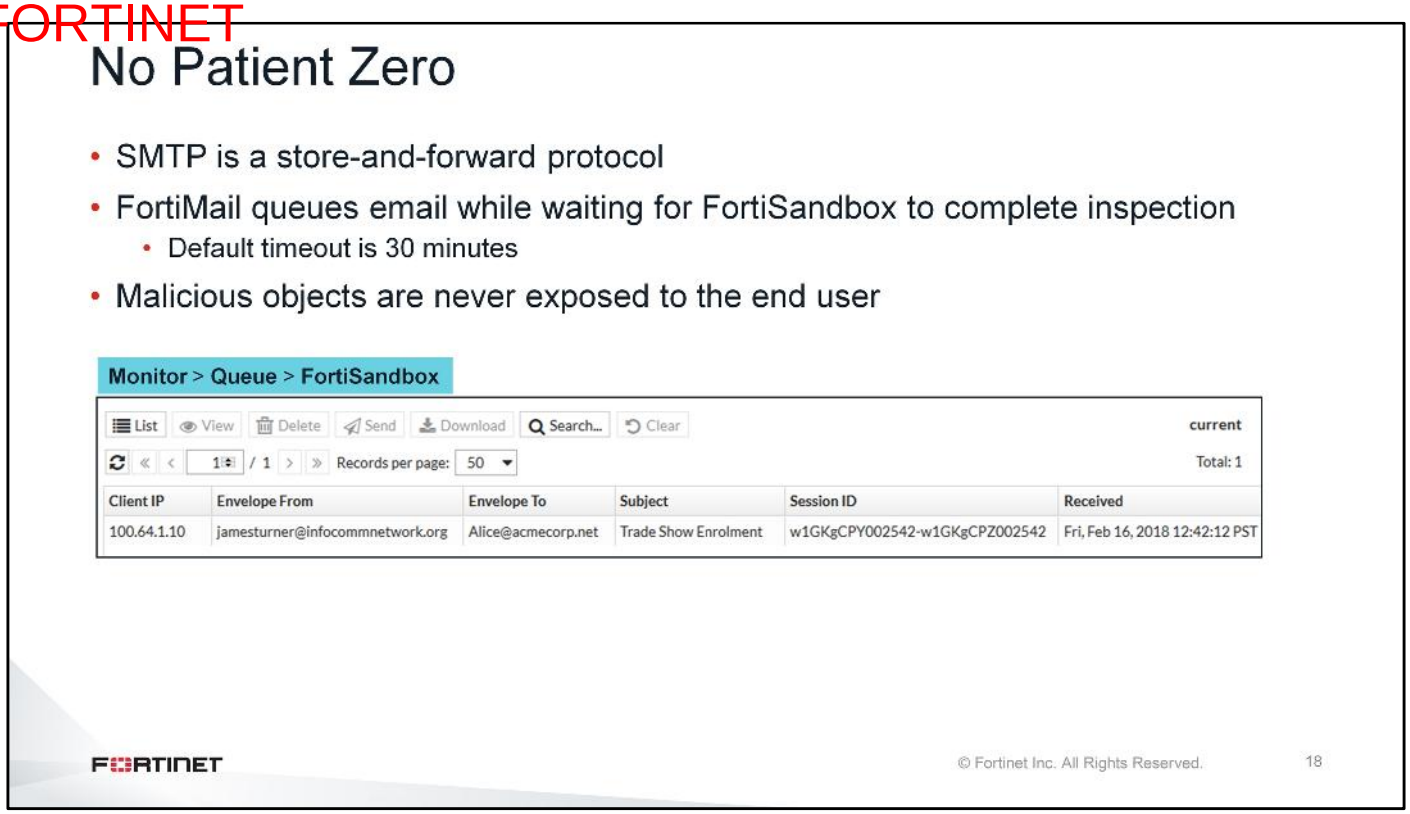
- FortiMail's role
  - Submit files and URLs to FortiSandbox
  - Queue email during analysis
  - Apply configure action to email based on verdict
- FortiSandbox's role
  - Inspect submitted files and URLs
  - Generate a verdict
  - Share threat information



17

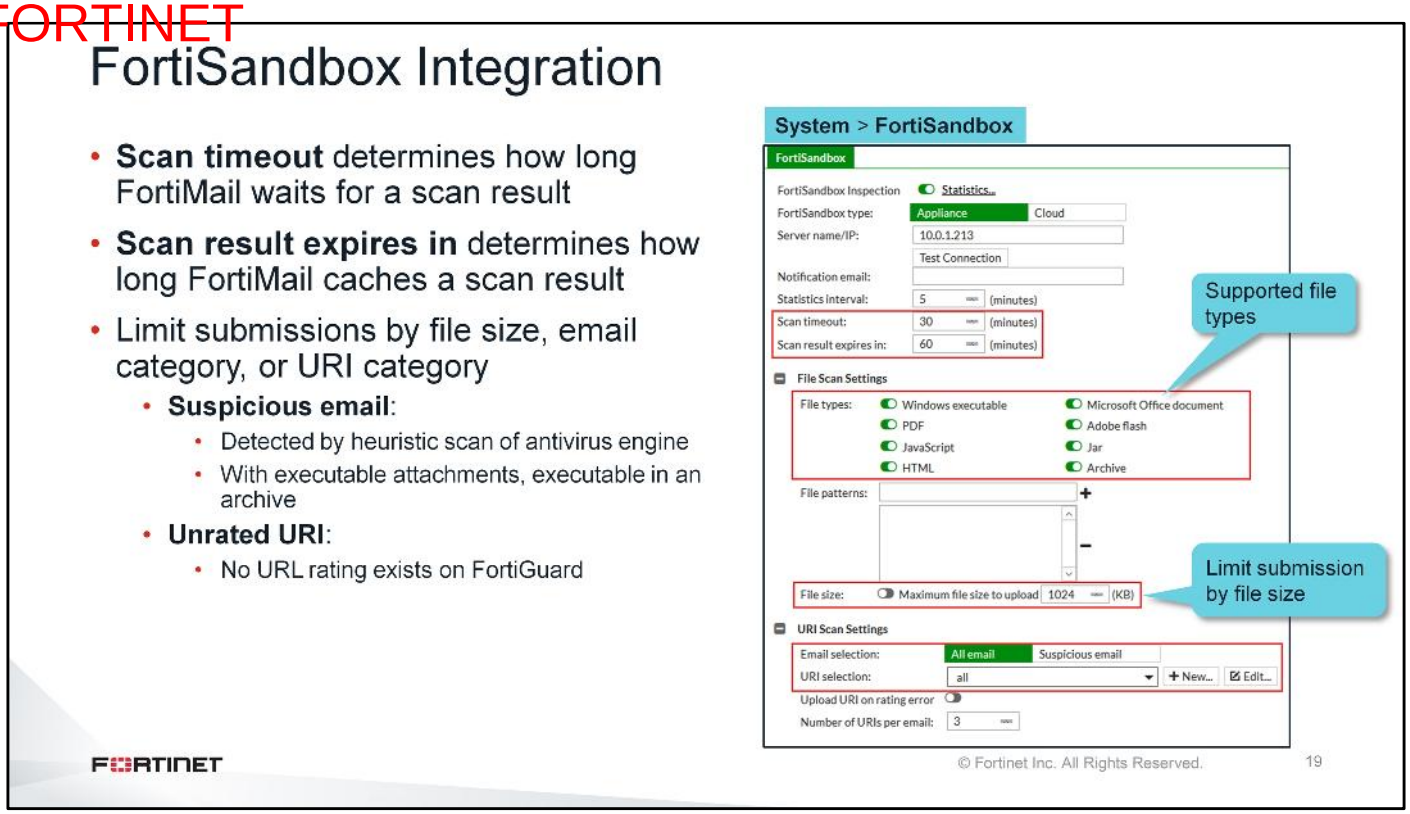
On top of file submissions, FortiMail can also submit extracted URLs from emails to FortiSandbox for inspection. FortiMail queues the email while waiting for a verdict. FortiSandbox inspects all submitted files and URLs. FortiSandbox then generates a verdict and sends that verdict in reply to FortiMail. FortiMail uses the verdict to apply the configured action.

FortiMail does not use FortiSandbox threat intelligence. However, FortiSandbox can share the threat information learned from FortiMail submissions, with other devices (FortiGate, FortiWeb, and FortiClient).



SMTP is a store-and-forward protocol. This allows FortiMail to queue the email while FortiSandbox inspects all submitted samples. FortiMail will release the email only if there is a scan timeout event, or FortiSandbox returns a clean verdict. This ensures that the malicious content is never exposed to the end user.

There is a dedicated FortiSandbox mail queue where FortiMail stores emails while waiting for FortiSandbox to finish inspecting submitted samples.

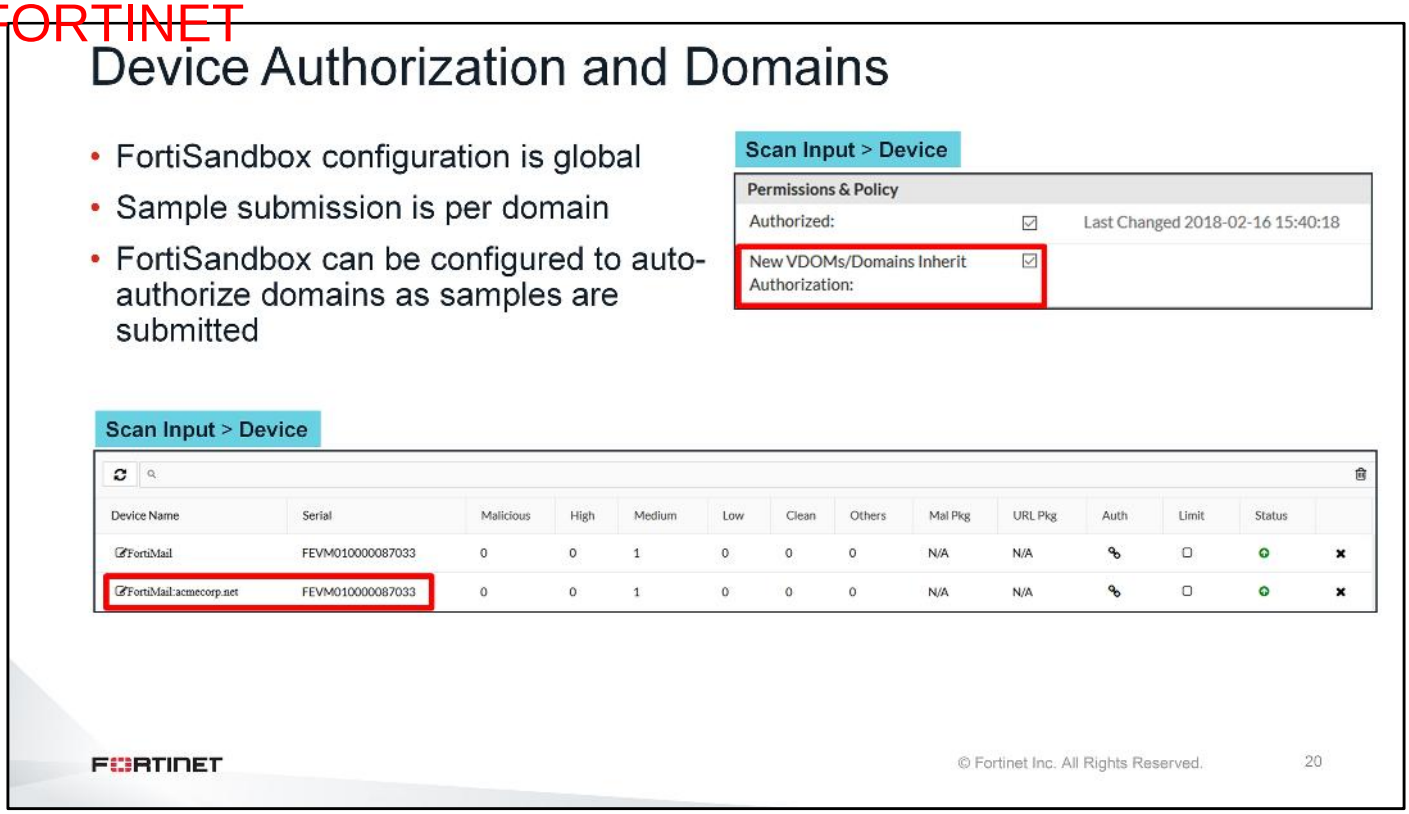


When configuring FortiSandbox integration on FortiMail, you should consider the **Scan timeout** and **Scan result expires in** settings. These settings can greatly affect the performance of your FortiMail and FortiSandbox.

The **Scan timeout** value determines how long FortiMail will wait for a response from FortiSandbox. The default is 30 minutes. So, if after 30 minutes FortiSandbox is unable to generate a verdict, FortiMail will release the email to the end user. You must decide whether or not 30 minutes is sufficient or too long to wait for an email that may require sandboxing.

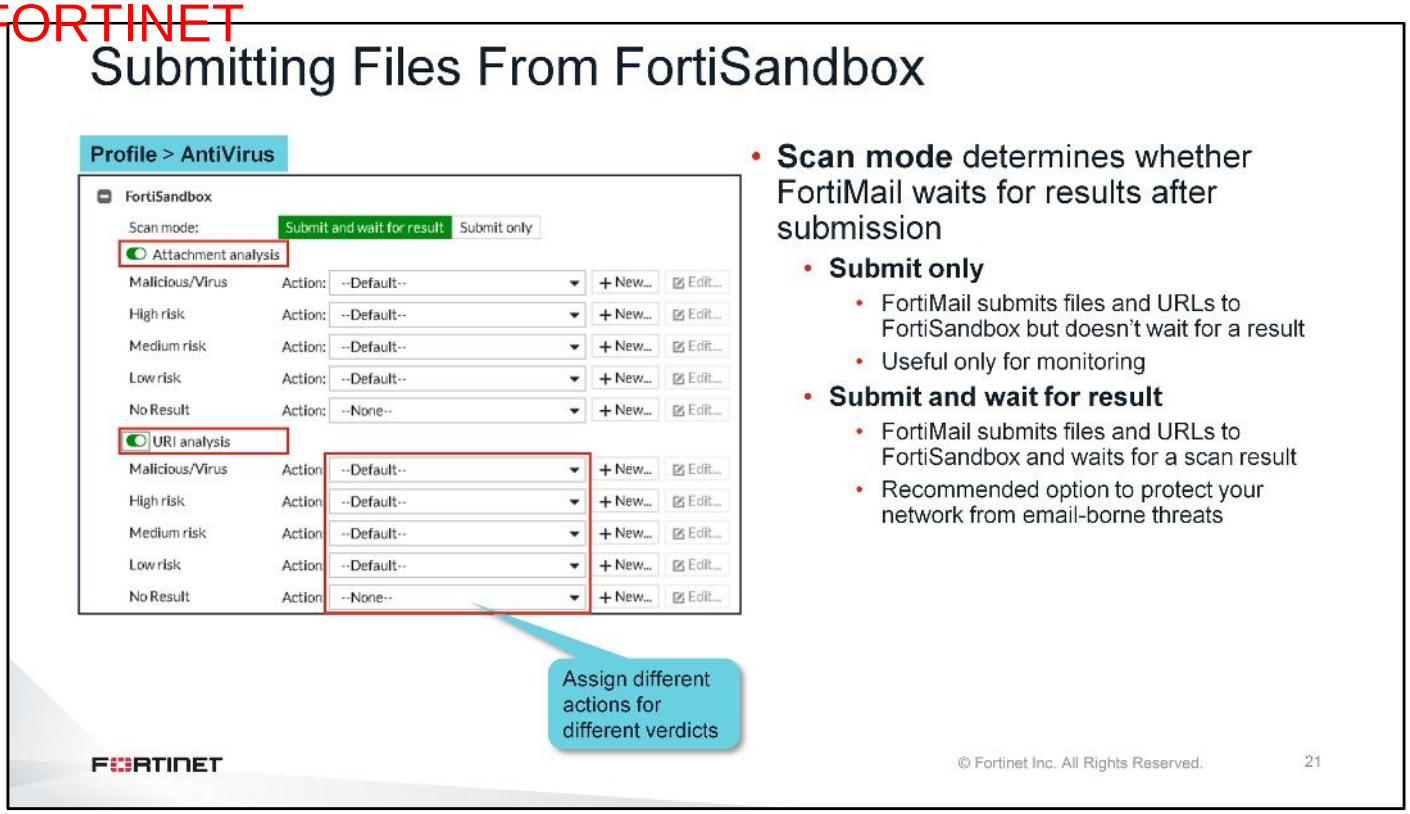
The **Scan result expires in** value determines how long FortMail will cache a verdict. Because FortiMail doesn't use the FortiSandbox-generated malware and URL databases, this timer determines how often FortiMail will query FortiSandbox for repeat occurrences of the same malicious samples (file checksum and URL query).

You can also limit submissions from FortiMail by file size, email category, or URL category. You can configure FortiMail to send only suspicious emails, or unrated URLs. However, it is recommended that you configure FortiMail to send all emails and all URLs, unless your FortiSandbox is experiencing performance issues.



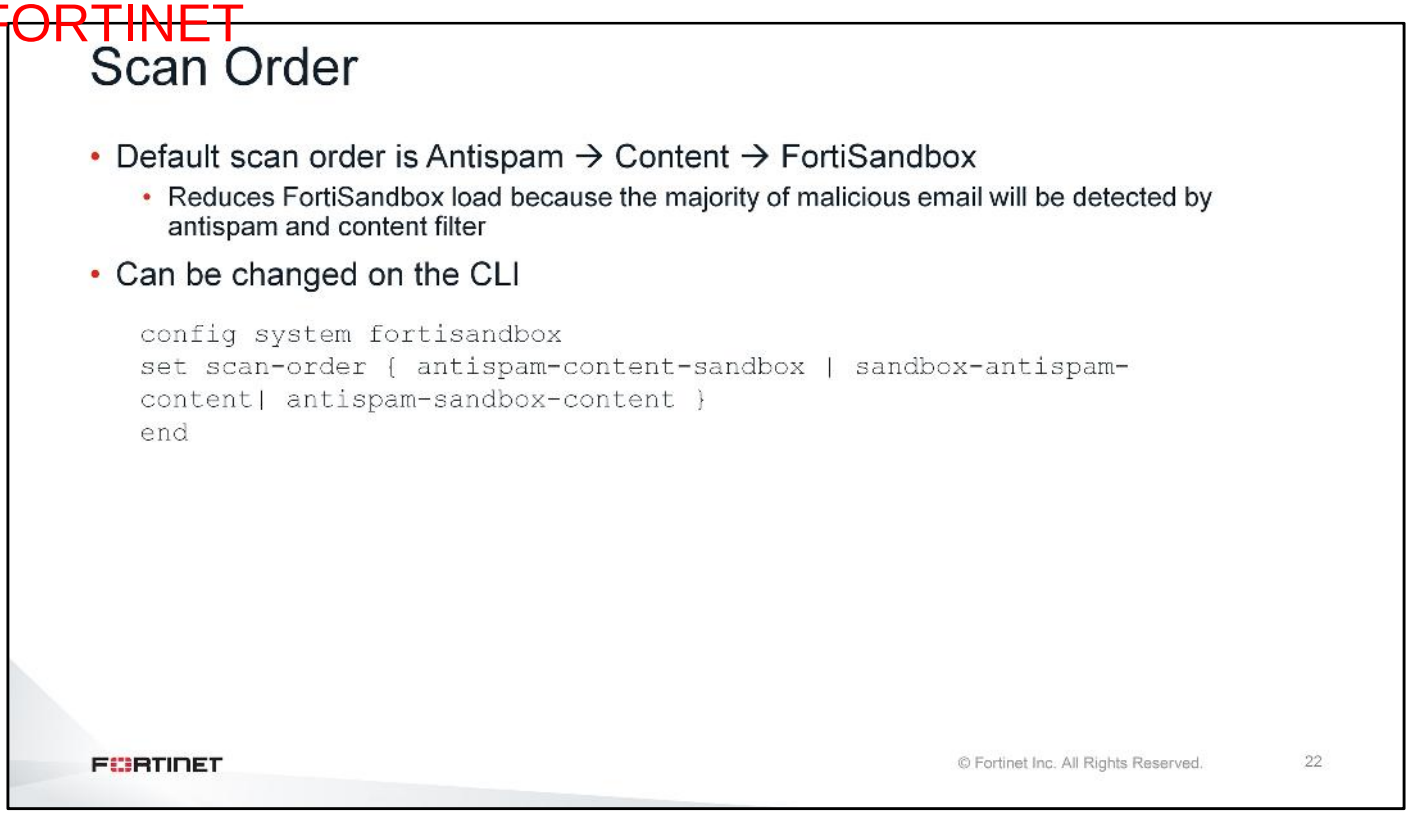
Similar to FortiGate VDOMs, FortiMail has domains. FortiSandbox configuration is global, but antivirus profile and FortiSandbox sample submission is done for each domain. With auto-authorization enabled, each domain will be automatically authorized as samples are submitted.

Each domain will appear as a separate input device on FortiSandbox.



You can configure FortiSandbox submission in an antivirus profile by enabling **Attachment analysis** and **URI analysis**. You can assign different action profiles for different FortiSandbox verdicts.

The **Scan mode** setting determines whether FortiMail waits for results after sample submission. If you select **Submit only**, FortiMail will submit the sample, and deliver the email to the end user without waiting for a response. This is useful for monitoring only. The **Submit and wait for result** setting is recommended. With this setting, FortiMail will wait for a verdict or until the scan timeout value is reached, before taking action on the email.

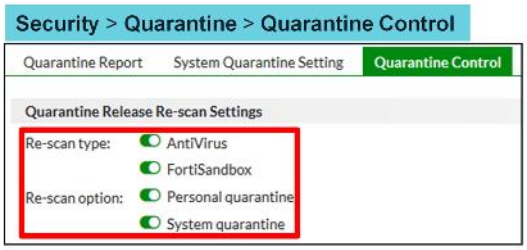


The default scan order is antispam, followed by content filter, followed by FortiSandbox. This scanning order reduces the number of submissions to FortiSandbox because the majority of malicious emails are detected by antispam and content profile features.

The scanning order can be changed on the CLI. However, using the default order is recommended.

Quarantine Release Rescan

- Rescan on release prevents malware from being released to end users



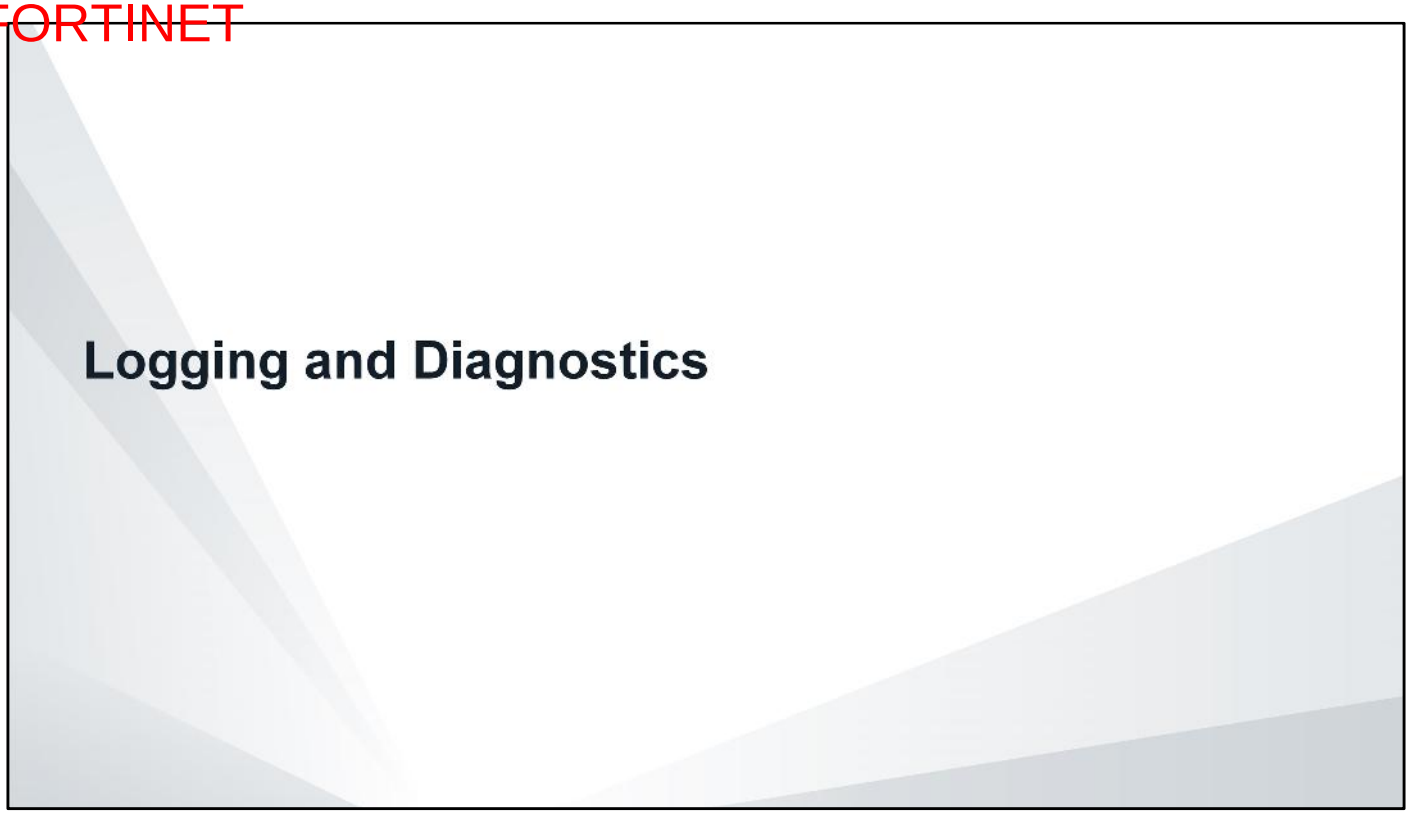
- Released content can be scanned by both antivirus and FortiSandbox
- Quarantine release rescan action depends on the matching inbound recipient policy's antivirus profile

FORTINET

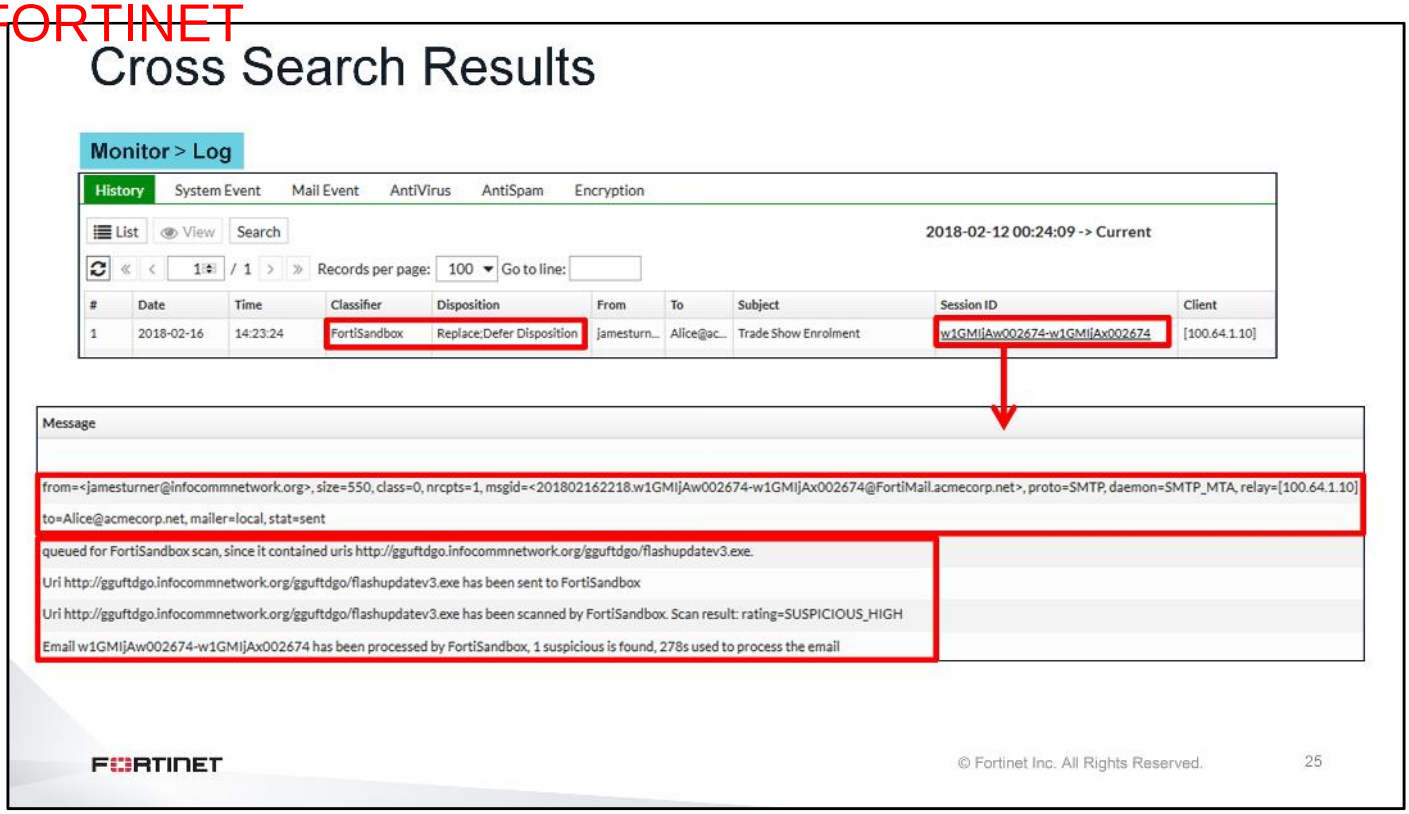
23

The default scan order may allow an email containing a malicious attachment or URL to be sent to and be released from, user quarantine. If you are using the quarantine action in any action profile, you should also configure quarantine release re-scan.

This features allows content released from user or system quarantine to be scanned by both antivirus and FortiSandbox. The action FortiMail takes depends on the matching recipient policy's antivirus profile.



In this section, you will learn how to verify FortiSandbox operation using FortiMail logs. You will also learn how to debug the daemons involved in queuing emails, and offloading samples to FortiSandbox.

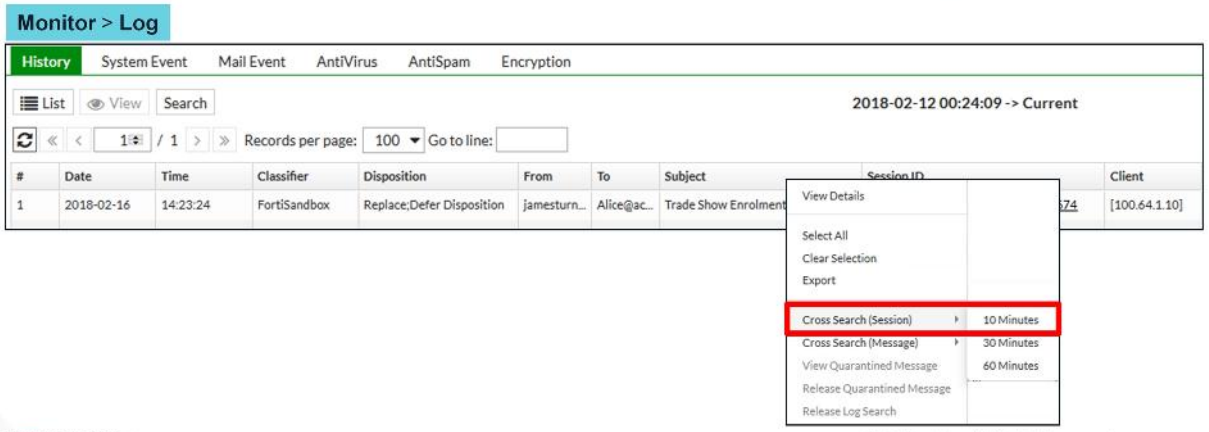


A single email can potentially generate four to five different log types, depending on which inspection profiles are triggered. The easiest way to retrieve all associated logs in the context of an email session, is to use the cross search results. You can access the cross search result for an email session from the history logs by clicking the session ID link.

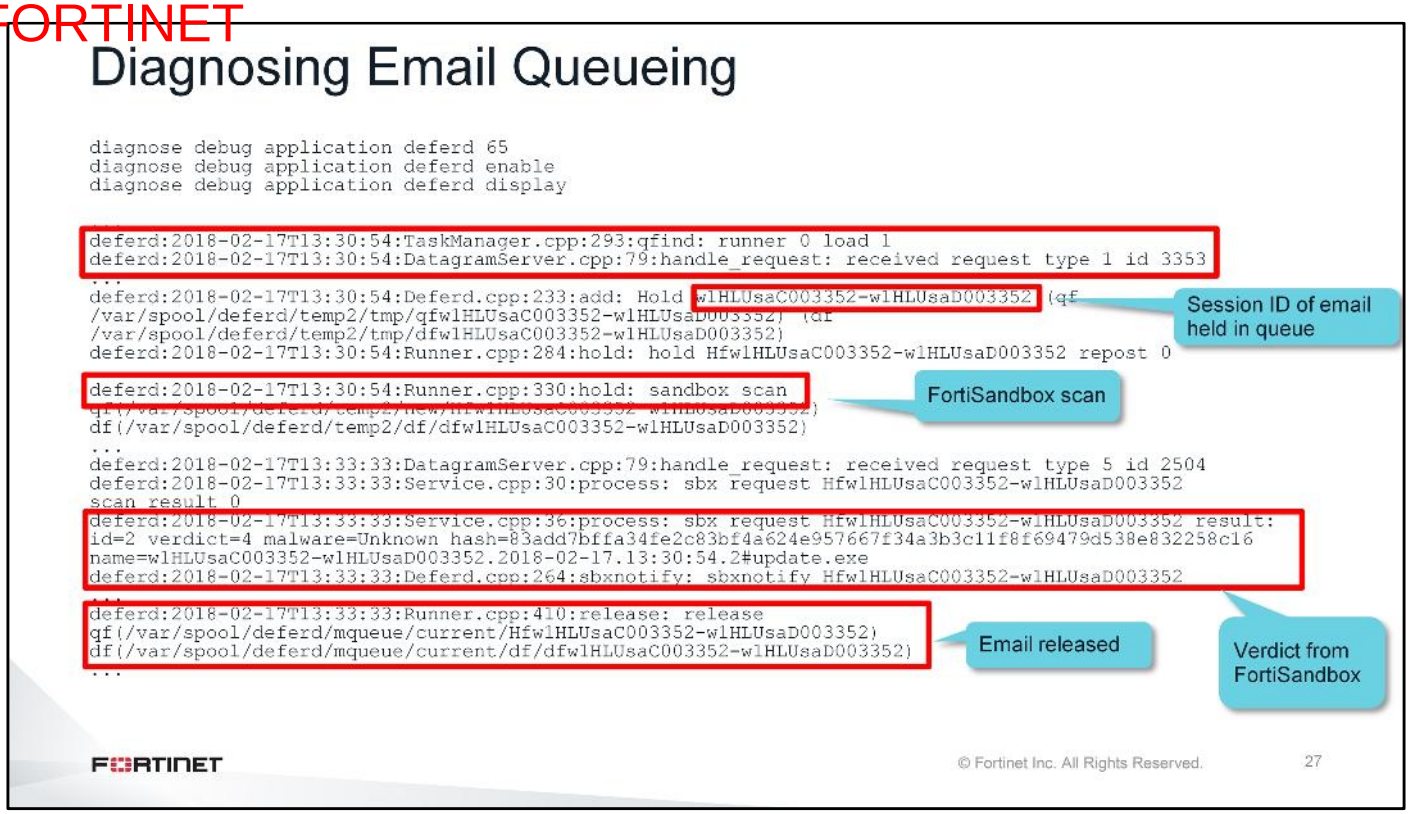
You can examine the cross search results to learn details about the events generated by FortiSandbox integrated virus scanning. The logs show what type of file triggered the FortiSandbox scan, the file checksum, and the scan result. FortiMail also logs how long it took to process the email.

Cross Search Results Time Period

- The default time period for cross search results is 5 minutes
- If FortiSandbox takes longer than five minutes to complete a scan, the generated logs will not appear when accessing the cross search results
- Use the right-click context menu in the history logs to select longer time periods

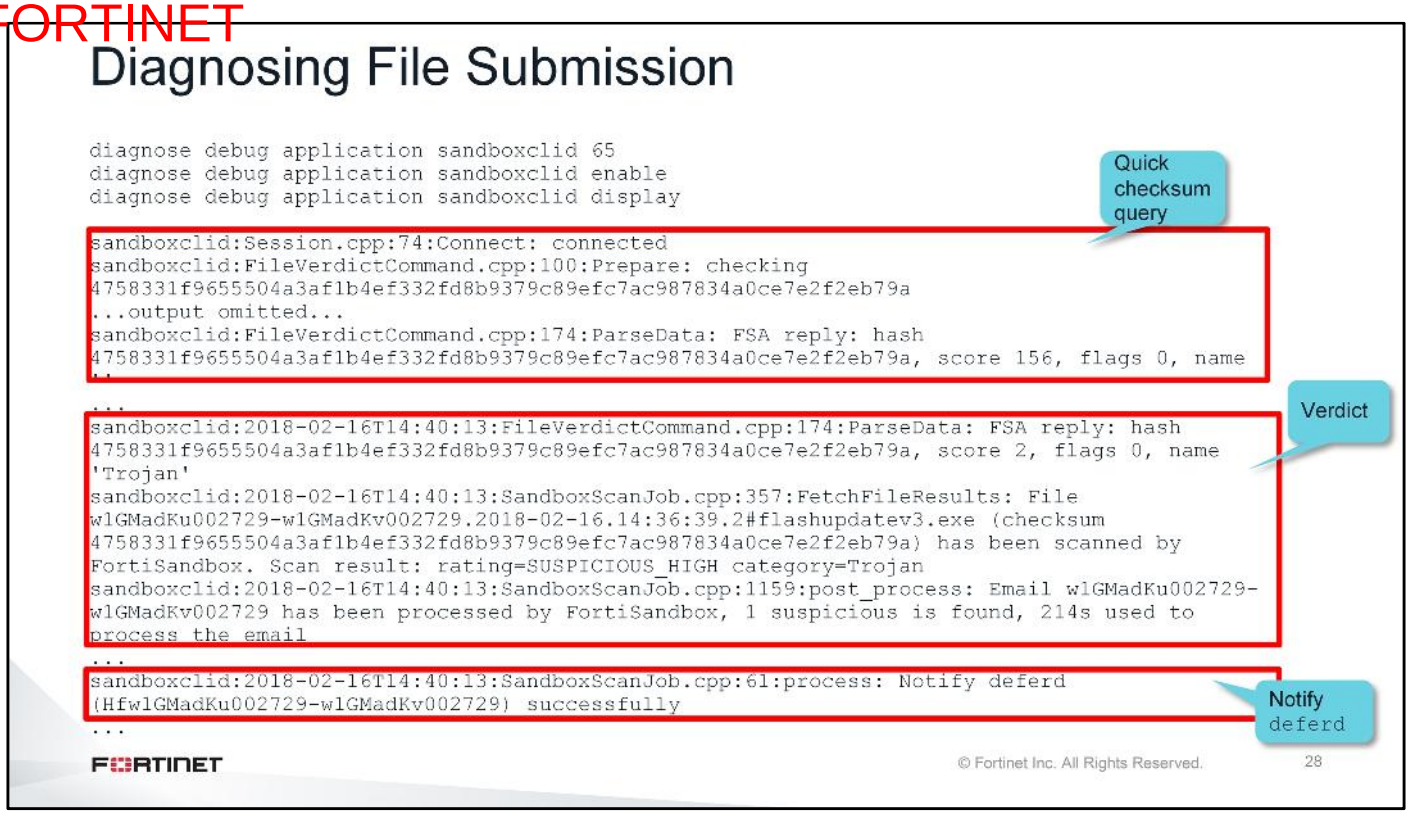


The cross search result is time based, and the default period is 5 minutes. If FortiSandbox takes longer than five minutes to complete a scan, the generated logs will not appear when accessing the cross search results. You can use the right-click context menu in the history logs to select longer time periods.



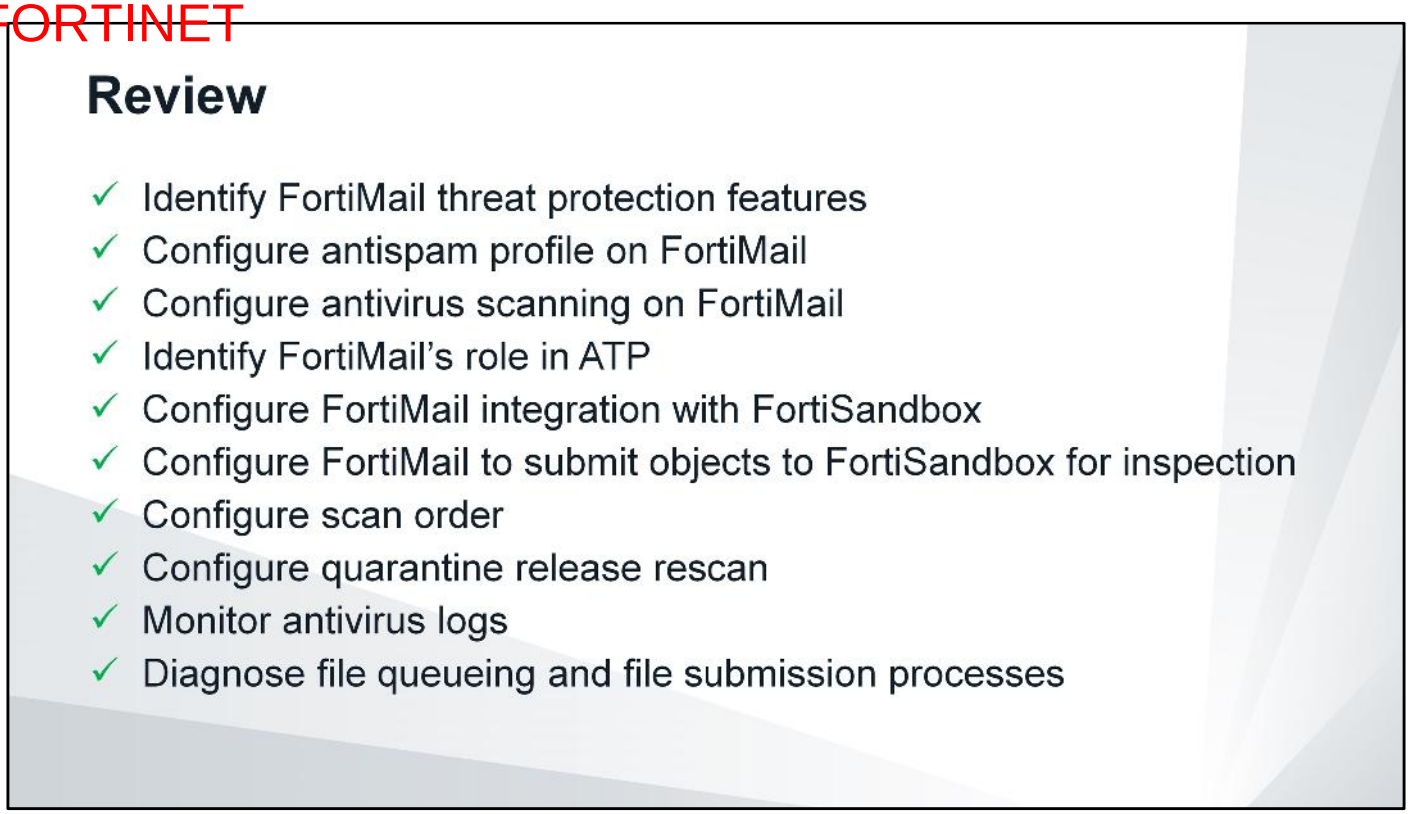
The deferd daemon handles the queuing of emails while samples are being scanned by FortiSandbox. To view the real-time debug messages, use the command shown on this slide. When dealing with large amounts of debug output, you can use an email's session ID or submitted sample detail (file name or URL) to search for specific debug output sections.

The deferd daemon waits for notification from the sandboxclid daemon, to release the queued email.



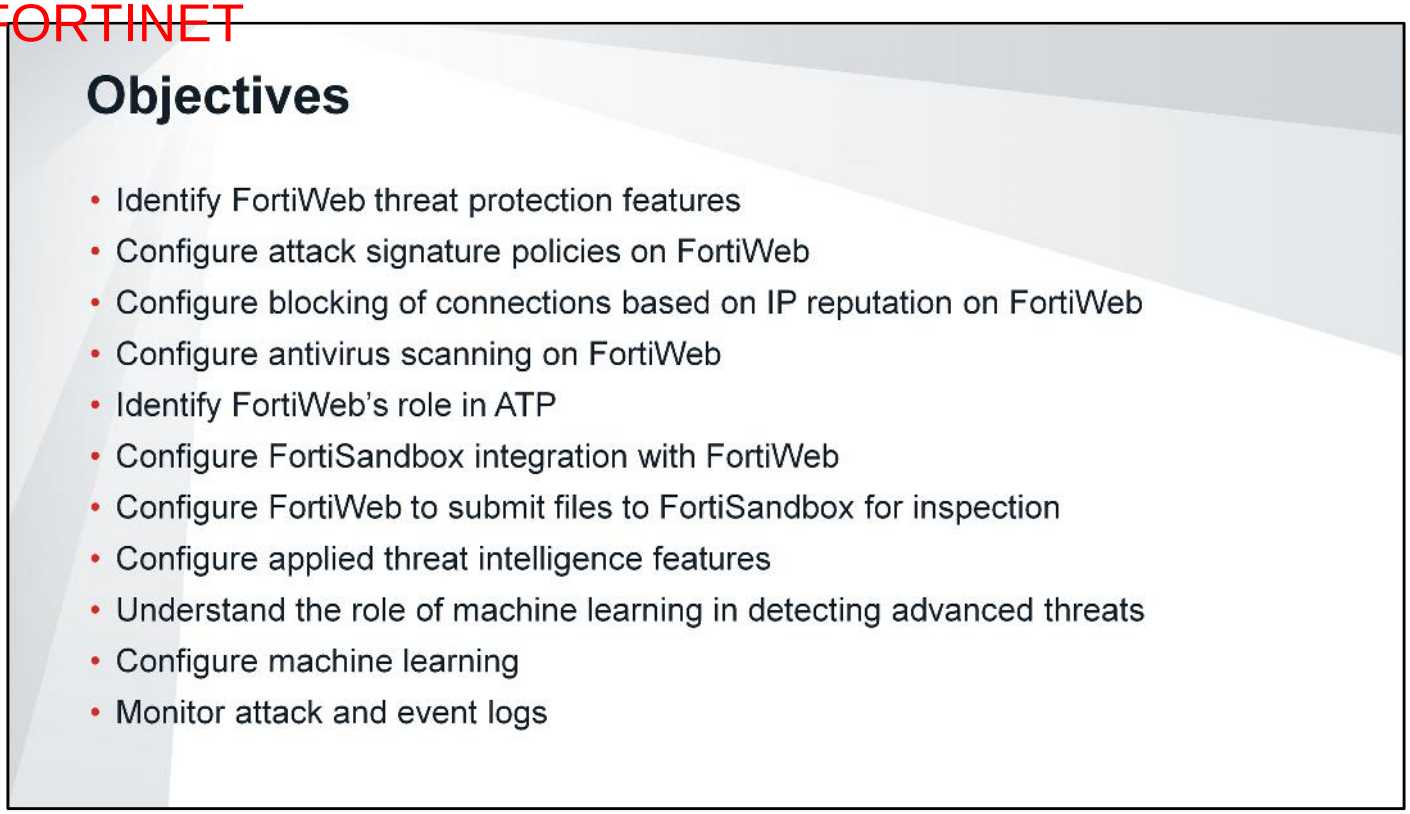
The sandboxclid daemon handles preliminary queries, Odette File Transfer Protocol (OFTP) job preparation, file submission, and verdict handling. Use the commands shown on this slide to view the sandboxclid daemon real-time debug messages.

For each job, sandboxclid will perform a quick check against FortiSandbox to query for existing verdicts. If a verdict does not exist, sandboxclid will transfer the sample to FortiSandbox for full analysis. After FortiSandbox completes the inspection and reports back with a verdict, sandboxclid notifies deferd to release the queued email.



This slide shows the objectives that you covered in this lesson. By mastering the objectives covered in this lesson, you learned how to protect your email network from advanced threats.

In this lesson, you will learn how to protect your web servers from advanced threats.



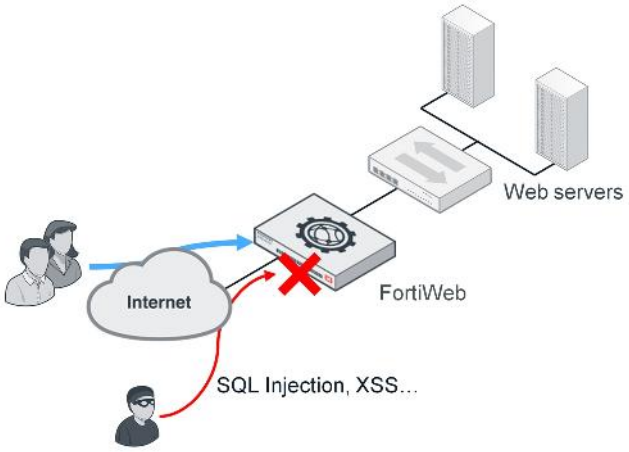
After completing this lesson, you should be able to perform the objectives shown on this slide.

By demonstrating competence in FortiWeb's threat protection and advanced threat protection (ATP) integration concepts and configuration requirements, you will be able to protect your web application servers from advanced threats.

In this section, you will learn about the threat protection features available on FortiWeb, and how to configure them.

FortiWeb Overview

- Protects web-based applications from code-based attacks
  - SQL Injection or other injection types
  - Cross Site Scripting and Request Forgery
  - Layer 7 DoS/DDoS attacks
  - Cookie poisoning
- Protects against application vulnerabilities in custom code and commercial platforms
- Learns "normal" behaviors and stops anomalies
  - URL parameters, HTTP methods, session IDs, cookies and so on

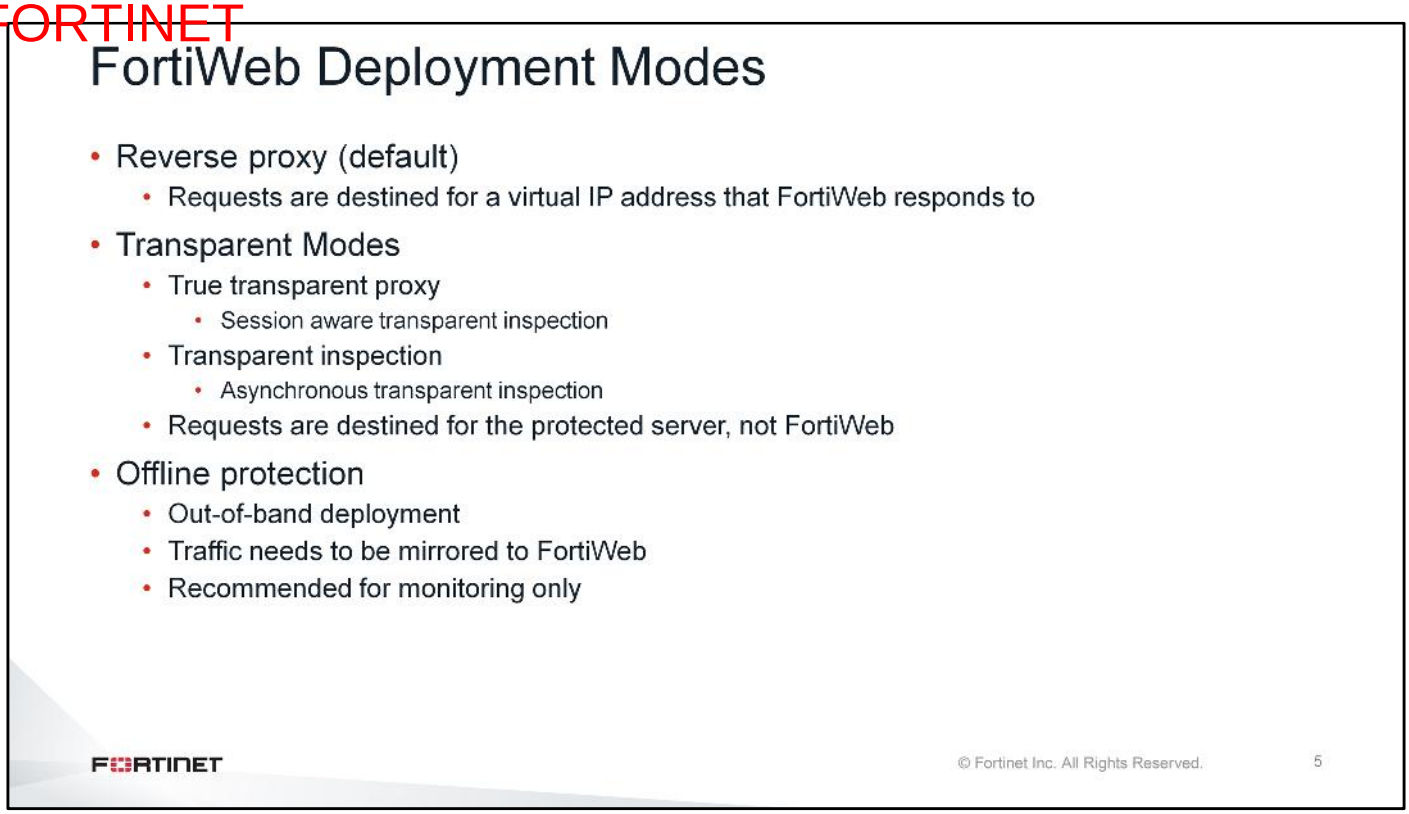


FORTINET

4

FortiWeb is a web application firewall (WAF) that is specifically designed to protect your web servers from threats. FortiWeb provides specialized application-layer threat detection and protection for HTTP or HTTPS. FortiWeb's application-aware firewalling and load balancing engine can:

- Secure HTTP applications that are often gateways into valuable databases
- Improve application stability
- Monitor servers for downtime and connection load
- Accelerate SSL sessions
- Learn normal behavior and detect anomalies

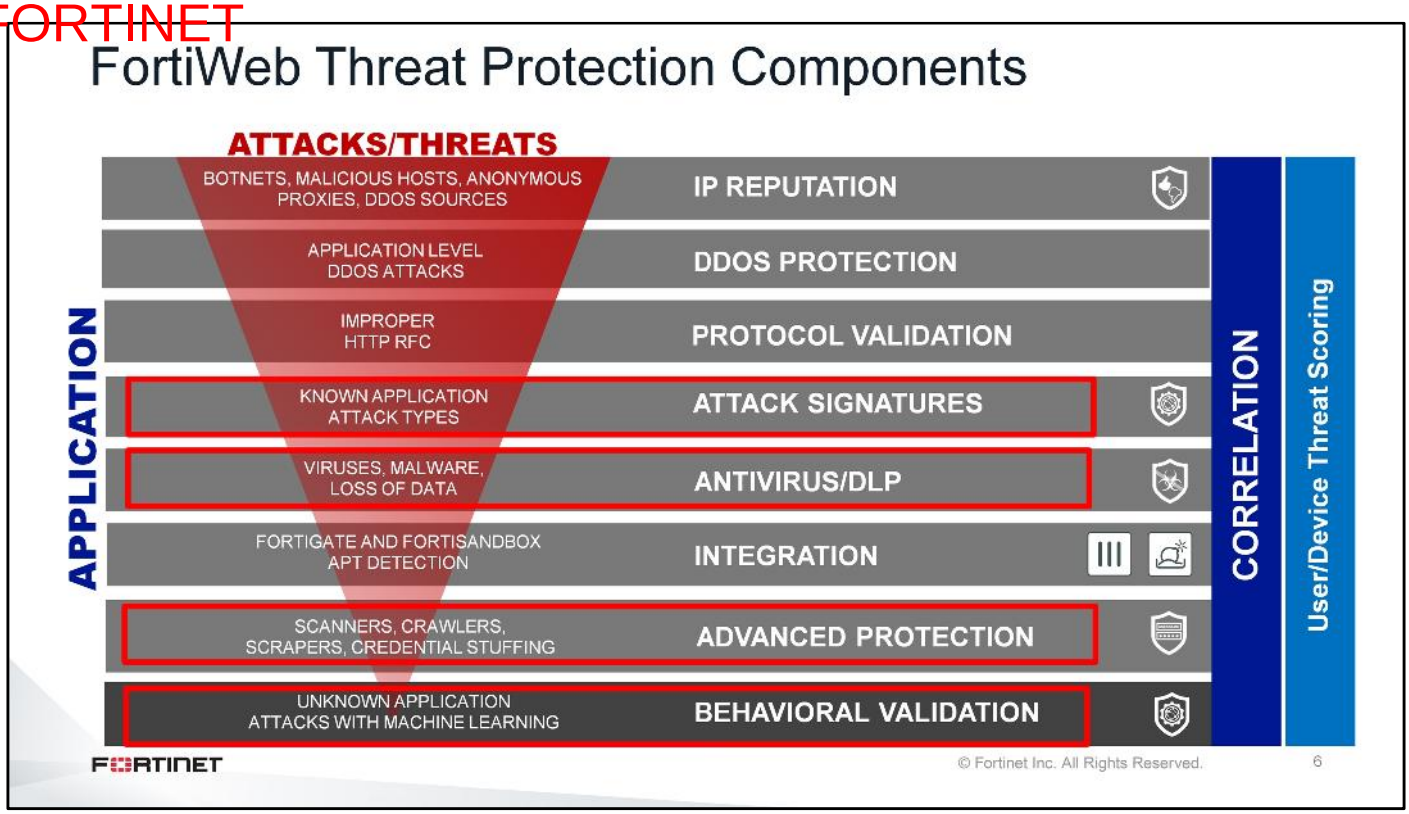


FortiWeb has multiple deployment modes. You can deploy FortiWeb in reverse proxy mode either physically inline or as a one-arm setup. All client requests go to a virtual IP address that FortiWeb responds to.

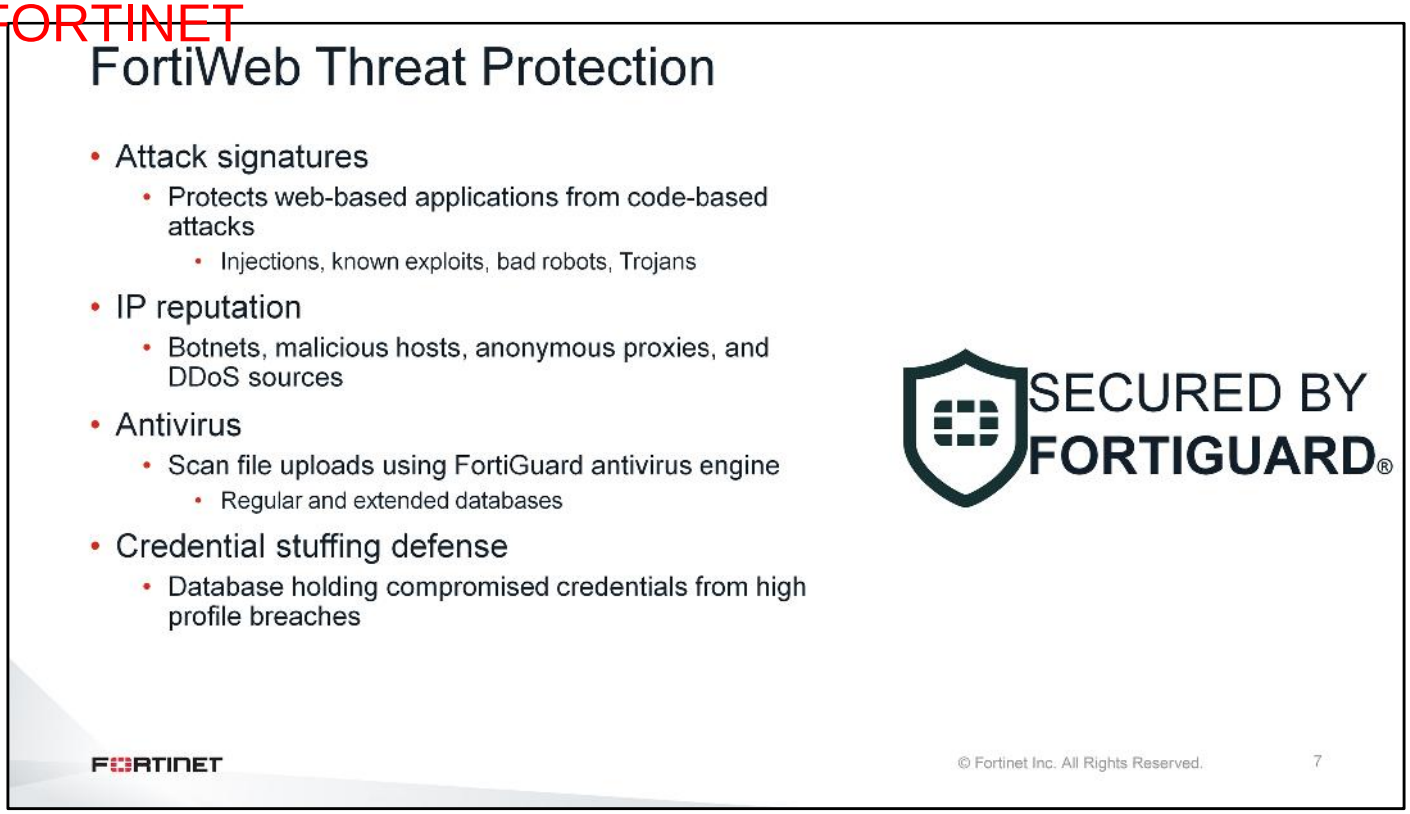
FortiWeb also has two different transparent inspection methods—true transparent proxy and transparent inspection. True transparent proxy mode is session aware, but transparent inspection mode is not. You can deploy both transparent inspection modes in-line, without changing the IP address scheme of your network.

FortiWeb also supports an offline protection mode, which is more suited for monitoring rather than inspection and blocking. If you're using offline protection mode, you need to mirror all traffic that requires inspection on FortiWeb.

The most common method of deployment is reverse proxy mode.



As shown on this slide, FortiWeb includes a wide range of components than you can configure to detect and block a wide range of threats. In this lesson, you will learn about the FortiWeb components that rely on FortiGuard intelligence to provide threat protection for your web servers.



FortiWeb has a large database of attack signatures that you can configure to mitigate attacks and data leaks. These signatures are attack patterns that FortiWeb can use to detect attacks, such as Cross Site Scripting (XSS), SQL injections, information disclosure, and so on.

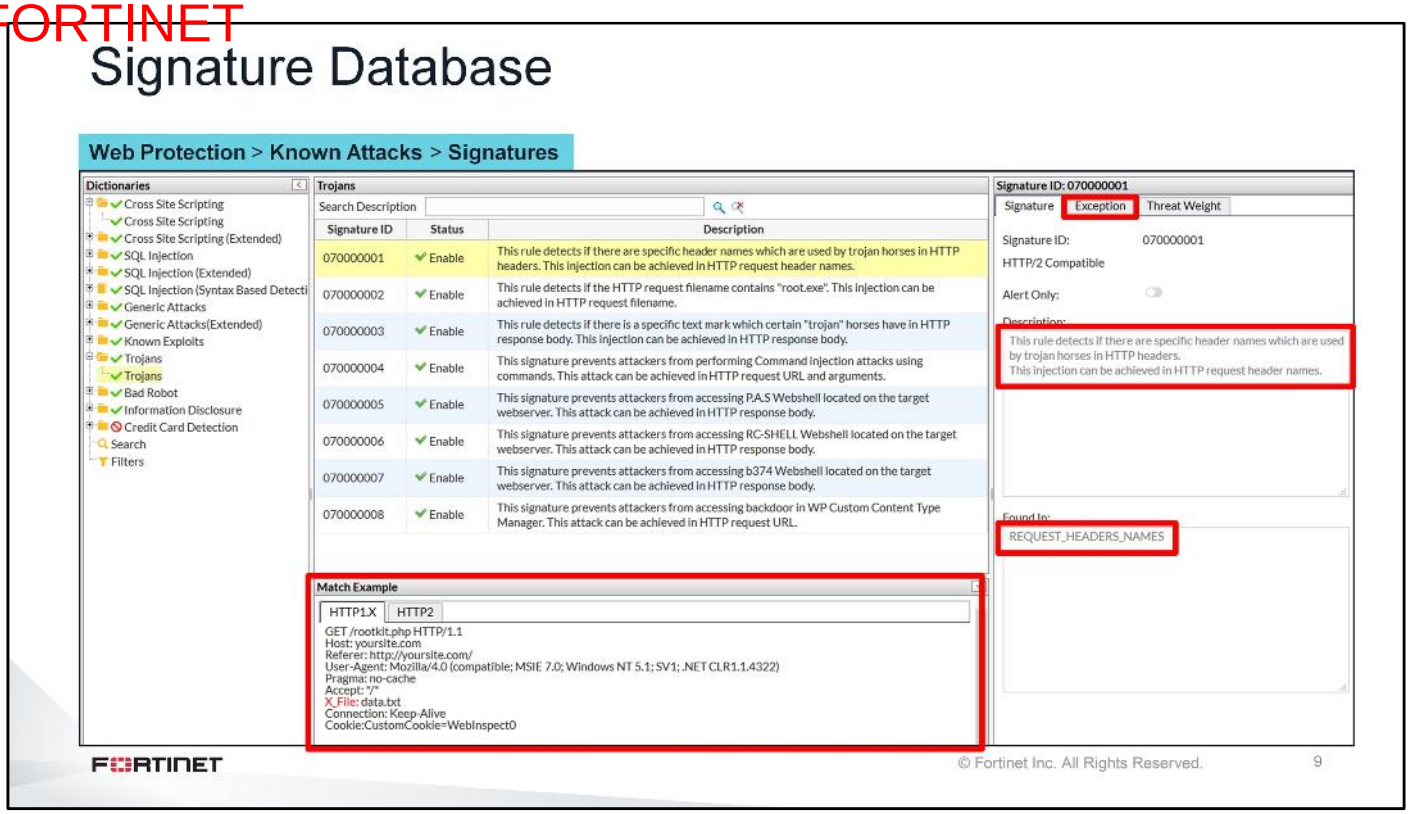
FortiGuard maintains a list of public IP addresses, along with their reputation and category. An IP's reputation is poorer if it is known to have participated in attacks. You can configure FortiWeb to block connections from IP addresses that are known to be botnets, malicious hosts, anonymous proxies, and DDoS sources.

You can also configure FortiWeb to scan files using the FortiGuard antivirus engine and databases. FortiWeb supports both regular and extended databases.

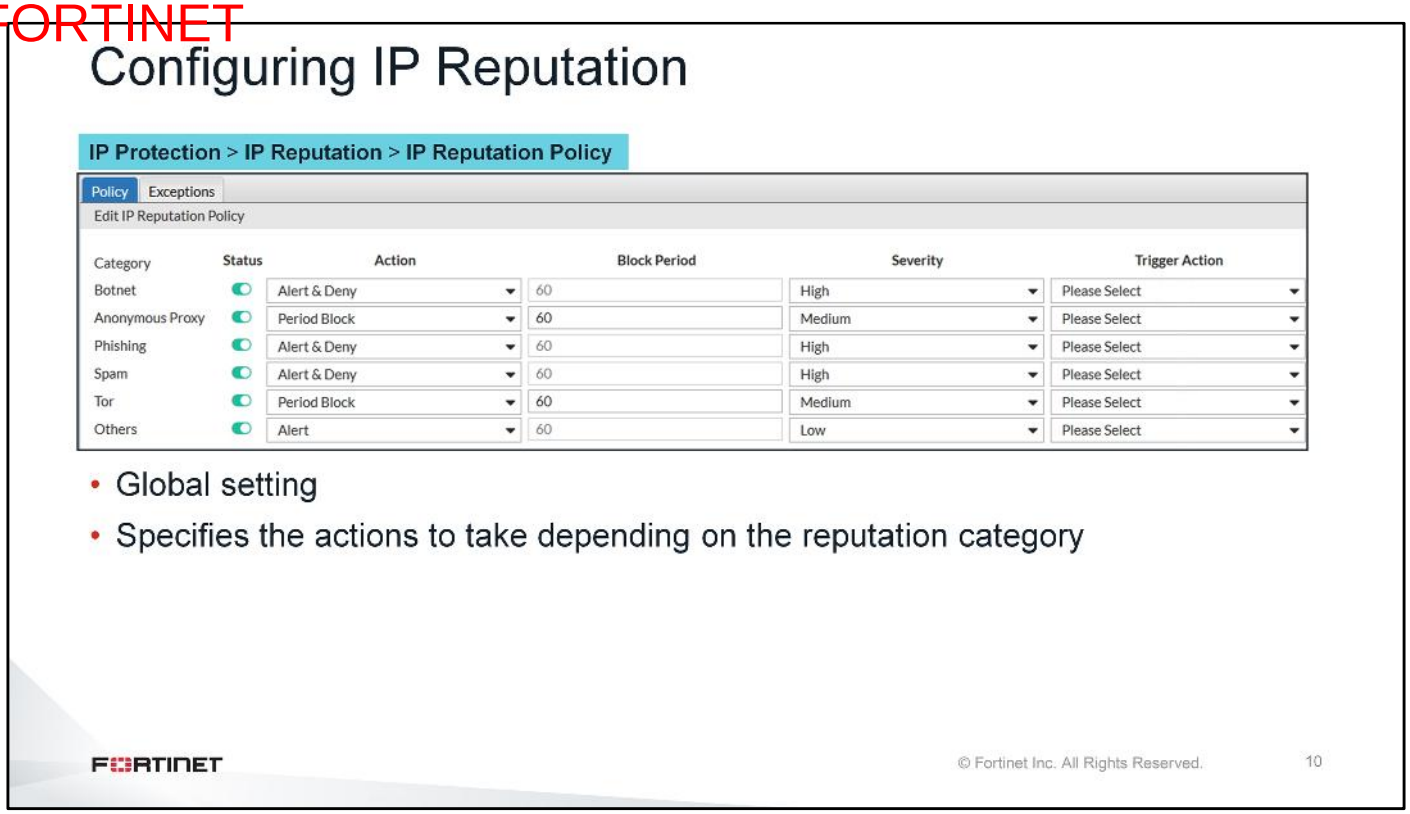
The credential stuffing database contains compromised credentials from high-profile breaches. You can configure FortiWeb to detect usage of these known compromised credentials.

You can configure signature rules to mitigate attacks and data leaks. There are various categories of signatures containing thousands of signatures for each category. Some categories contain extended versions that may cause false positives, but might be required in high-security networks. You can assign actions to each category, or assign actions to individual signatures to handle exceptions.

You can click **Signature Details** to access the signature database.

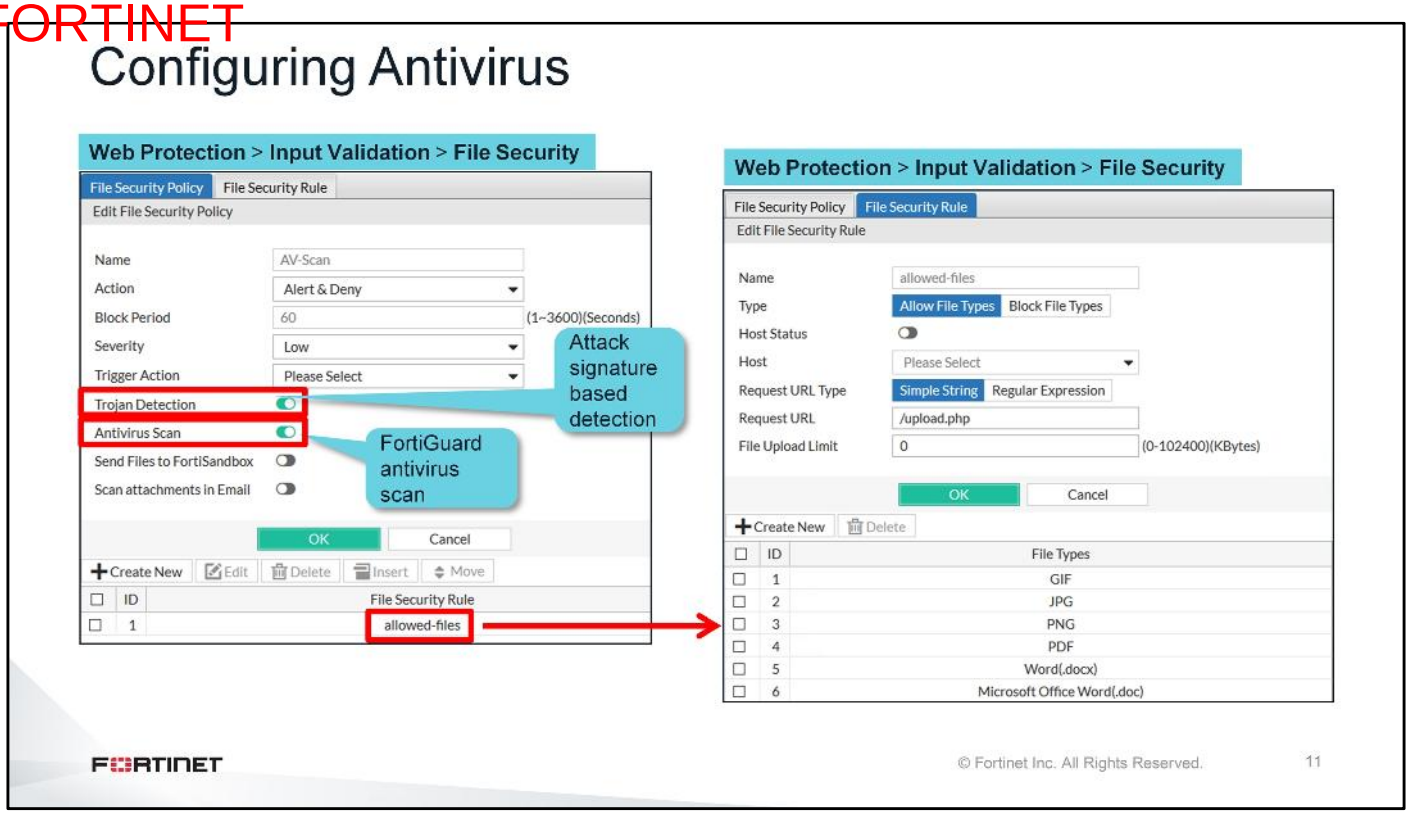


You can use the signature database as an information source or to fine-tune your configuration. The database lists signature ID, description, and match examples. You can also add exceptions to each signature.

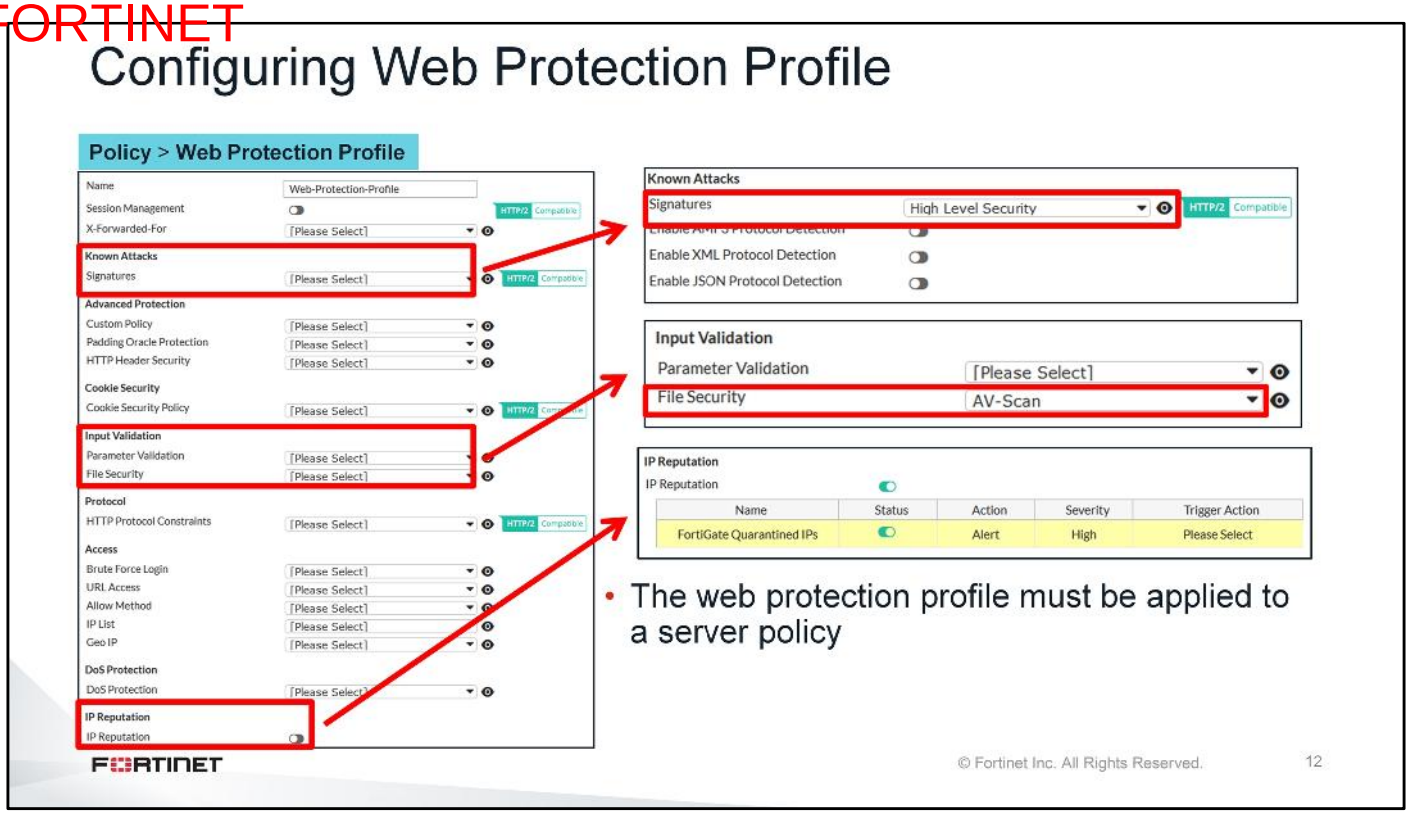


You can configure FortiWeb to use the FortiGuard IP reputation database and block connections from known compromised and malicious clients. A client will have a poor reputation if they have been participating in attacks. FortiGuard Labs continuously monitors the status of IP reputations, and adjusts the score based on recent activity.

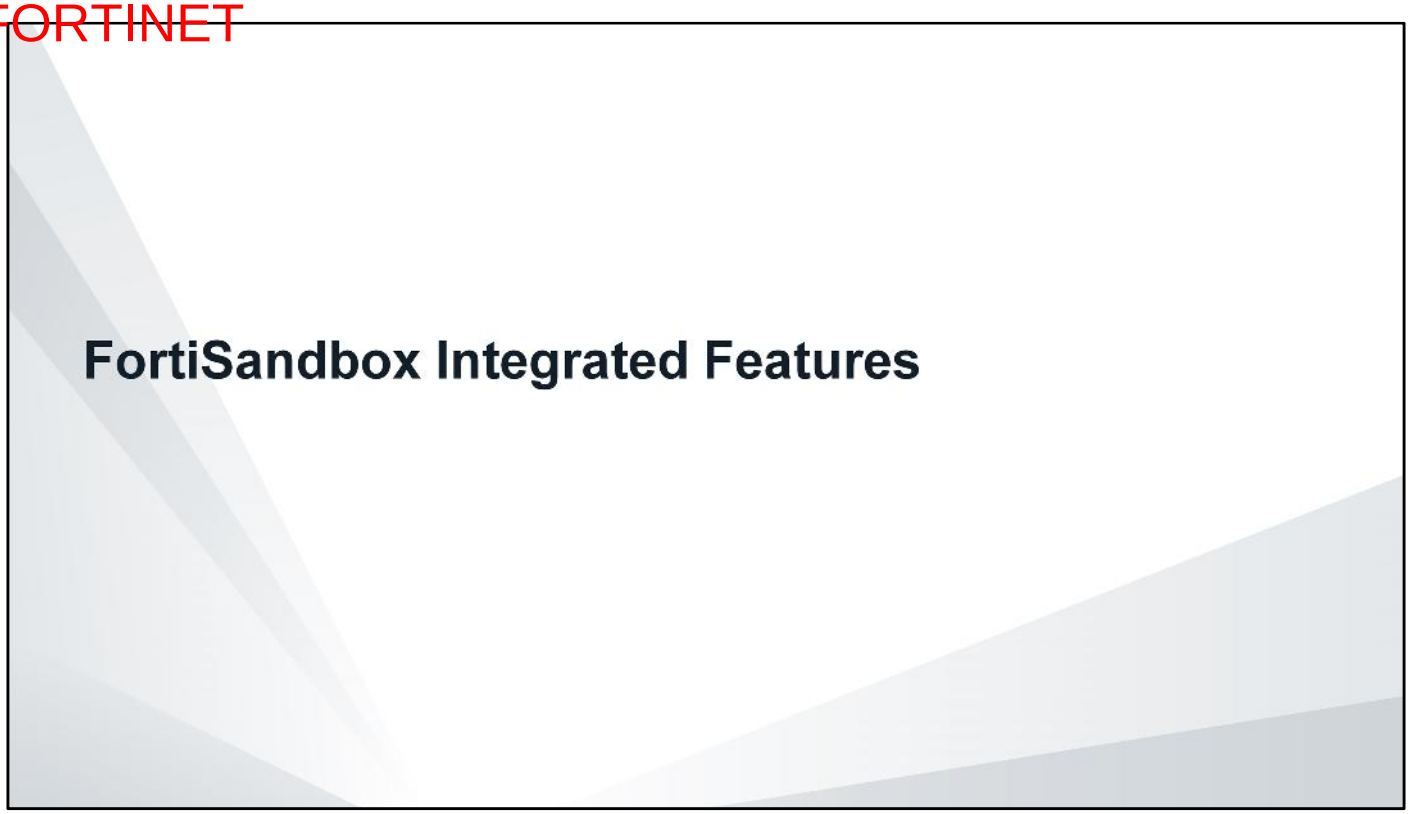
On FortiWeb, you can assign actions to IP reputation categories. The category defines the type of attack an IP address has been involved in. The categories are botnet, anonymous proxy, phishing, spam, Tor, and others.



On FortiWeb, you can configure file security policies to protect file upload repositories on web servers that accept file inputs. You can use file security rules to control size, file type, and location where files can be uploaded. Files that pass size, type, and upload location requirements can then be scanned for viruses by the antivirus engine.



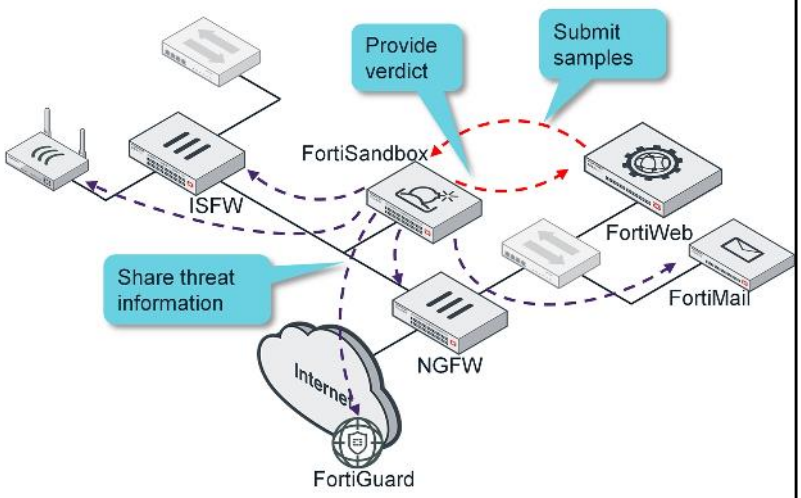
Signature policies and file security policies must be applied to a web protection profile, which then must be applied to a server policy. The **IP Reputation** feature is enabled using a toggle switch in the **Web Protection Profile**.



In this section, you will learn how to integrate FortiWeb with FortiSandbox.

FortiSandbox Integration

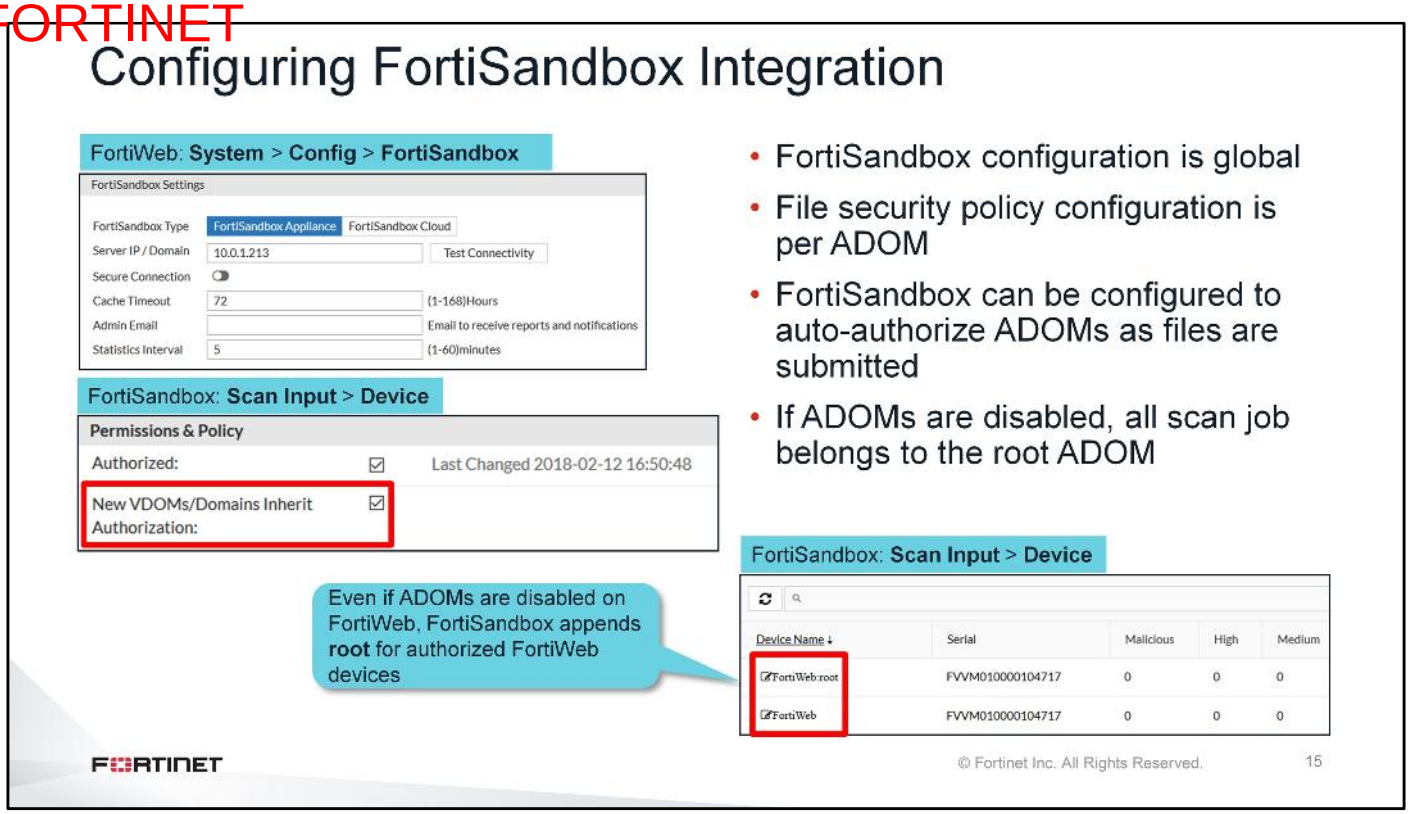
- FortiWeb's role
  - Detect and block known threats
  - Offload suspicious files to FortiSandbox
  - Prevent outbreak
- FortiSandbox's role:
  - Inspect submitted files
  - Generate a verdict
  - Share threat information
- FortiWeb can hold a session for up to 30 minutes while file is being analyzed



FORTINET

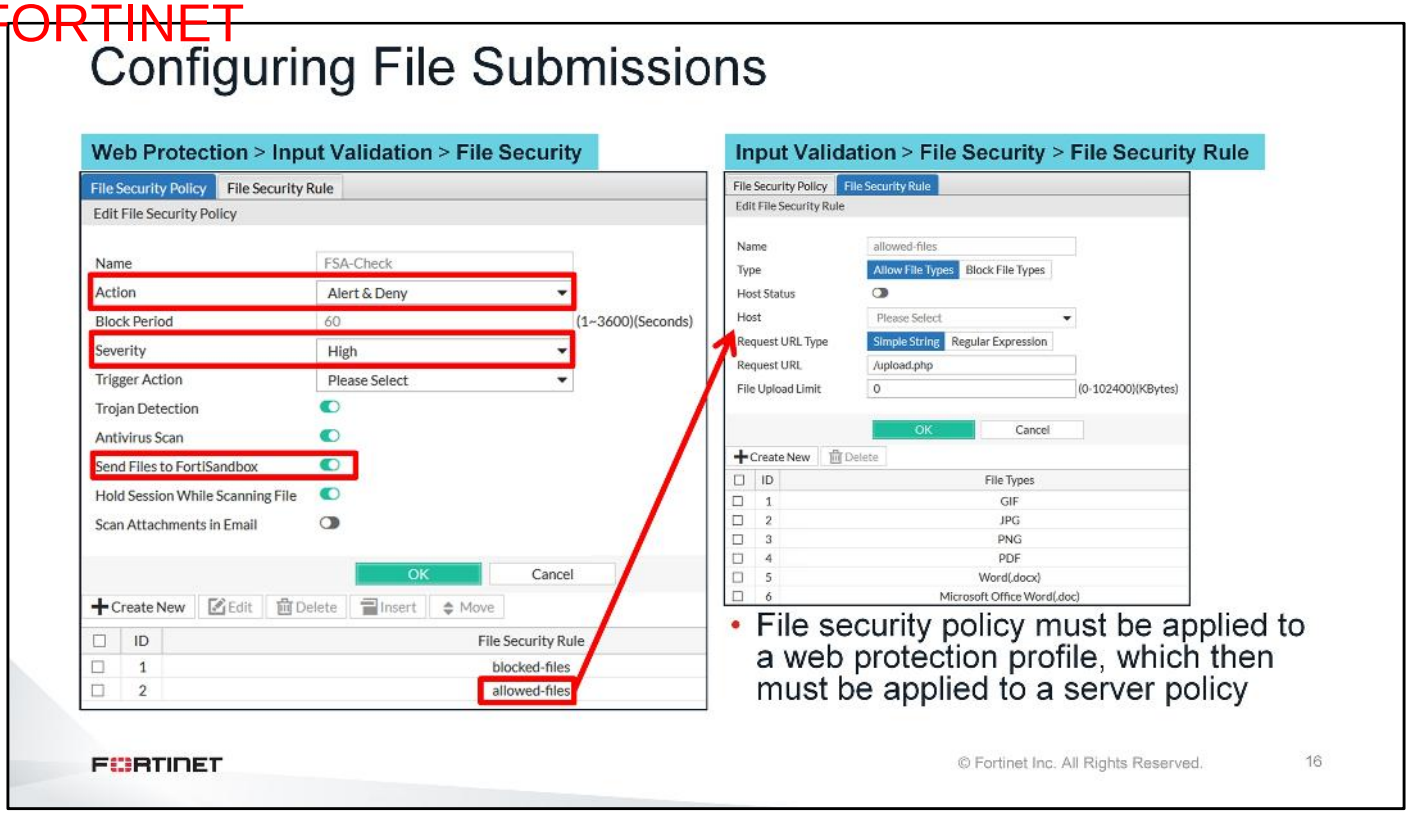
14

File uploads cleared by the antivirus scanner, are offloaded to FortiSandbox for analysis. While FortiSandbox is analyzing the file, FortiWeb has the ability to hold the session for up to 30 minutes. If a file in that session is malicious, then FortiWeb can drop that session based on the verdict from FortiSandbox.



Similar to FortiGate VDOMs, FortiWeb has administrative domains (ADOMs). FortiSandbox configuration is global, but security configuration (file security, web protection profile, and server policy), and FortiSandbox file submission is done for each administrative domain. When you enable auto-authorization, each ADOM is automatically authorized as files are submitted.

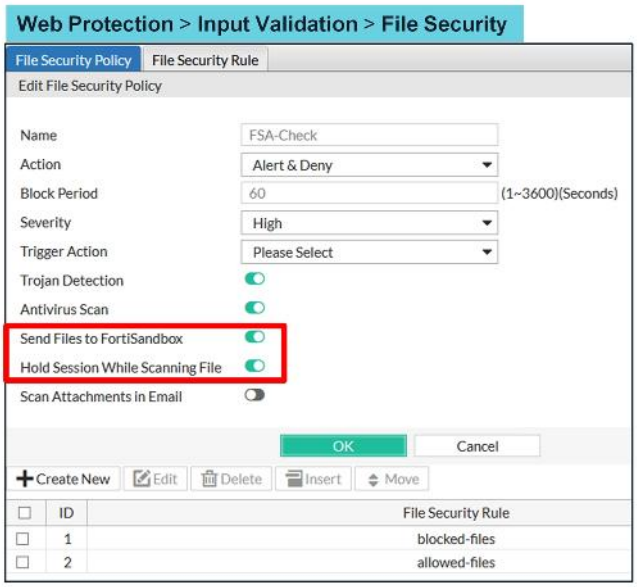
Each ADOM will appear as a separate input device on FortiSandbox. If ADOMs are disabled, all scan jobs belong to the root ADOM.



You can configure FortiSandbox file submission in a file security policy. Any files not detected by Trojan detection and the FortiGuard antivirus engine will be uploaded to FortiSandbox.

Hold Session While Scanning File

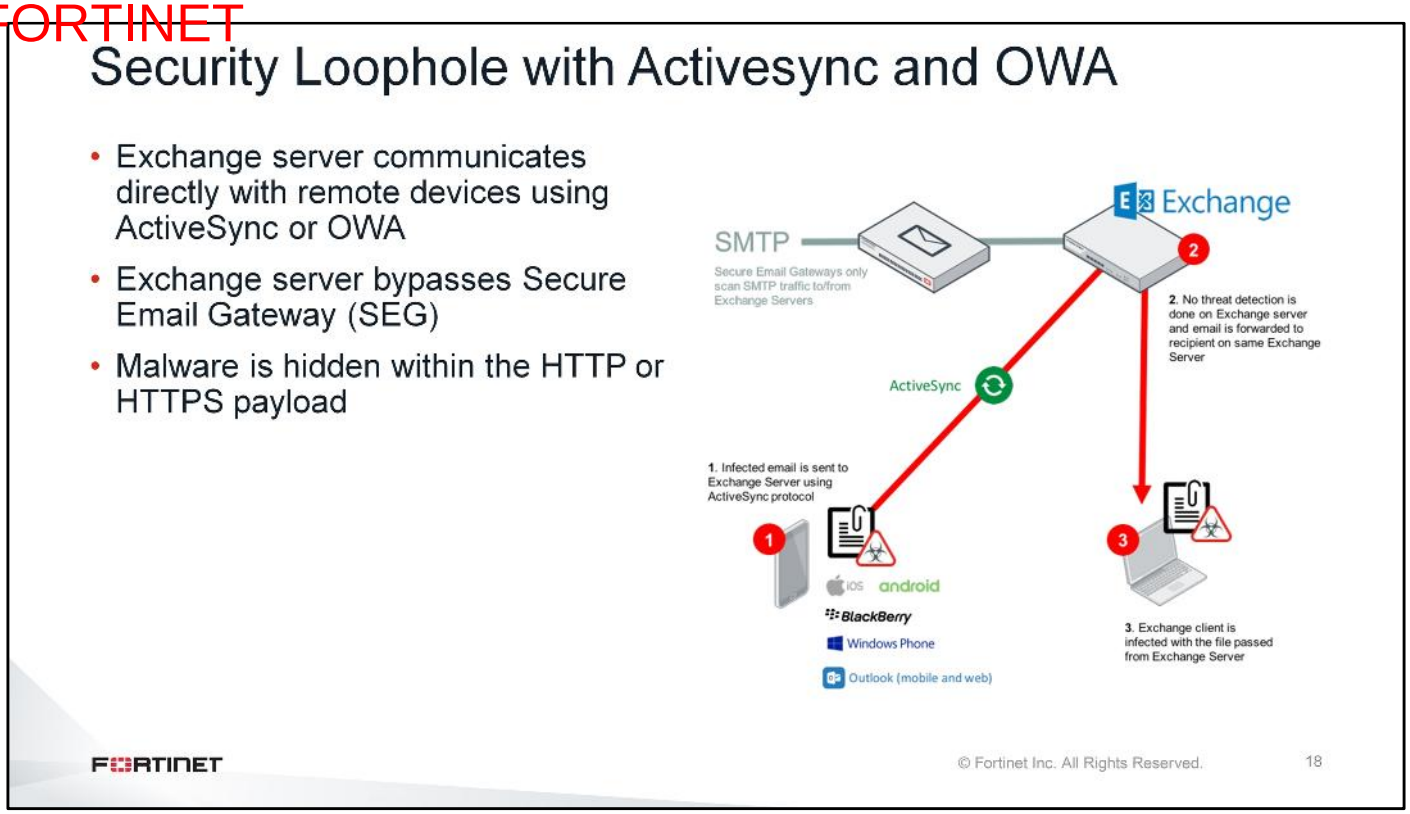
- FortiWeb waits for up to 30 minutes while FortiSandbox scans the file
- Only available when you enable **Send Files to FortiSandbox**



FORTINET

17

FortiWeb can hold sessions for up to 30 minutes while FortiSandbox is scanning the file. If FortiWeb holds the session for more than 30 minutes while FortiSandbox scans the file in the request, FortiWeb will forward the session without taking any other actions.



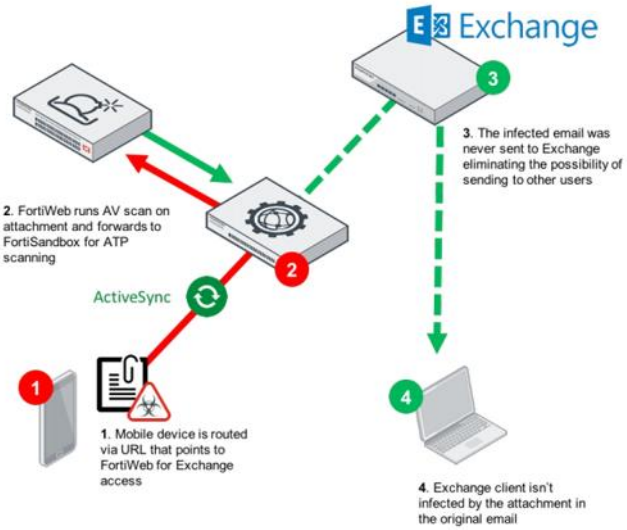
When remote users send and receive emails using ActiveSync or OWA, the server directly communicates with the devices, bypassing email protection services that scan SMTP traffic. SEGs only scan inbound and outbound emails from users that are external to the communications server using SMTP.

The ActiveSync protocol is based on XML and uses HTTPS to communicate to the server. OWA is a browser-based method that communicates to the server using HTTP and HTTPS. SEGs have no visibility to this traffic and can't intercept threats that may be hidden inside.

Using Microsoft Exchange as an example, if a remote user sends an email infected with malware using their mobile device or OWA to a recipient outside the organization's Microsoft Exchange Server, the email would be flagged and acted upon by the SEG. However, recipients on the same Microsoft Exchange Server as the mobile or OWA user would receive the infected email, spreading the threat or possibly sending it to other users on the Microsoft Exchange Server.

Protecting ActiveSync and OWA with FortiWeb

- FortiWeb can be deployed as a proxy for ActiveSync and OWA
- Inspects traffic and intercepts any attachments sent from remote devices or web browsers
- Send attachment to FortiSandbox to detect advanced persistent threats or zero-day attacks



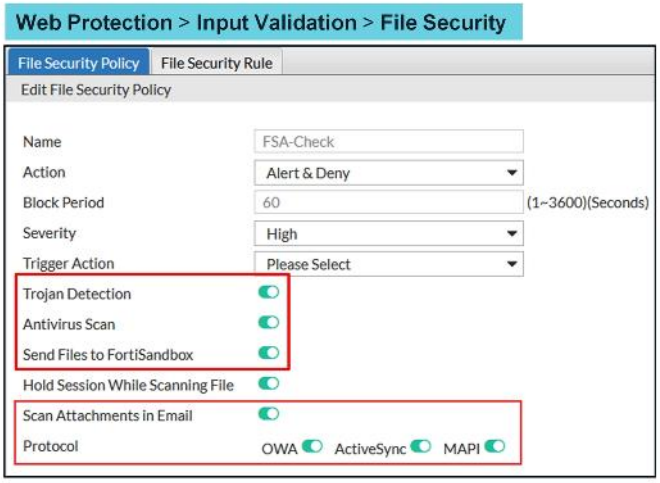
FORTINET

19

FortiWeb can be deployed as a proxy for ActiveSync and OWA. This means that any remote mobile user or email client would be directed to FortiWeb. Here FortiWeb would inspect the traffic and intercept any attachments sent from the device or web browser. These attachments are then processed by FortiWeb's antivirus engine to check for threats. You can also configure FortiWeb to send attachments to Fortinet's sandboxing solutions for additional scans to detect advanced persistent threats or zero-day attacks.

Scan attachments in Email

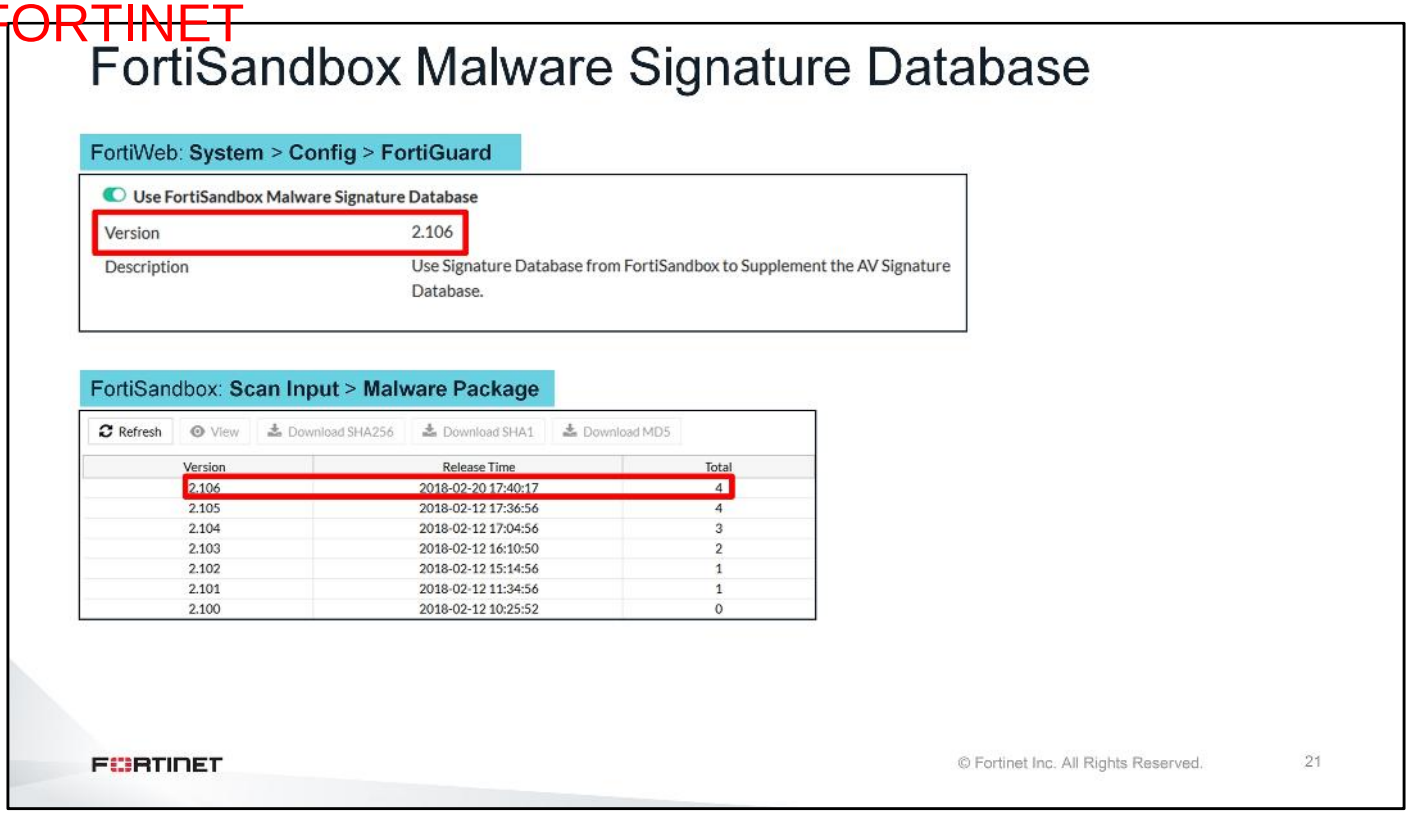
- FortiWeb will perform Trojan detection, antivirus scan, and will send the attachments to FortiSandbox



FORTINET

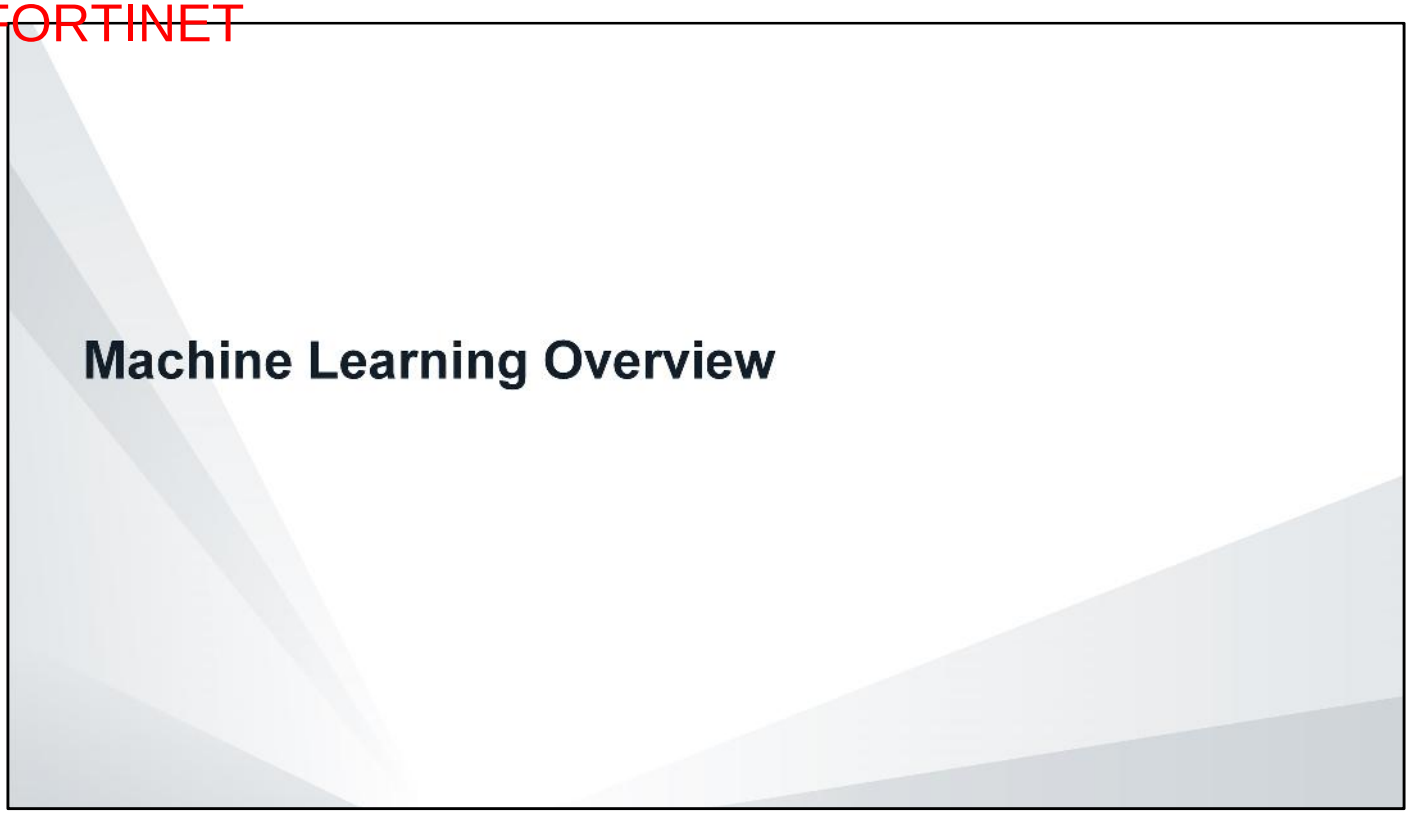
20

For FortiWeb to send attachments in email to FortiSandbox, you must enable **Scan Attachments in Email** and select the desired protocols. If you select **OWA**, then FortiWeb will scan attachments in email sent and received through the web browser login. If you select **ActiveSync**, then FortiWeb will scan attachments in email sent and received through a mobile phone login. If you select **MAPI**, then FortiWeb will scan attachments in email sent and received through the Message Application Programming Interface (MAPI), a new transport protocol implementation on the Microsoft Exchange Server.

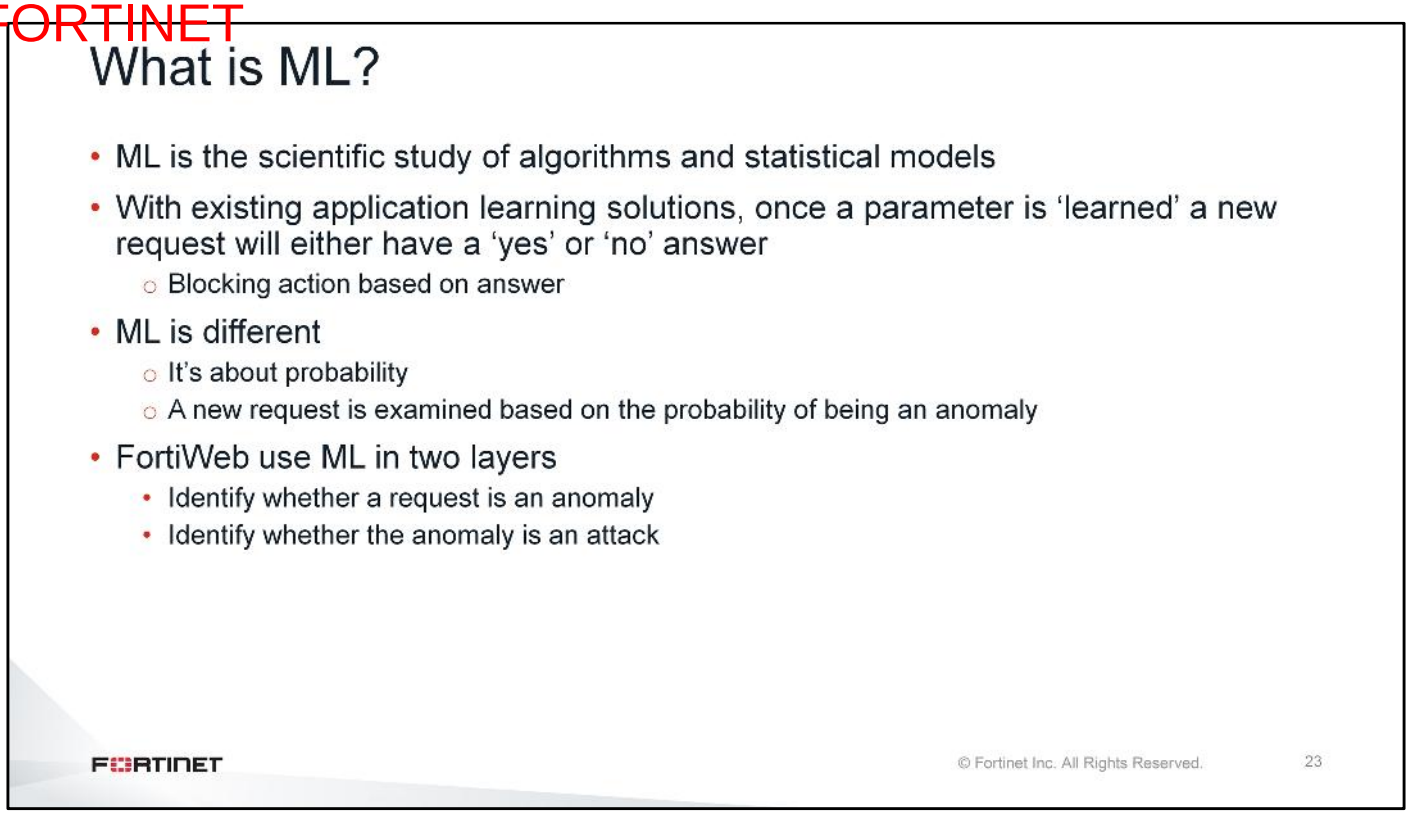


You can also configure FortiWeb to use the malware package generated by FortiSandbox. The malware signature database contains signatures for all suspicious files discovered by FortiSandbox.

FortiWeb does not use the URL package.

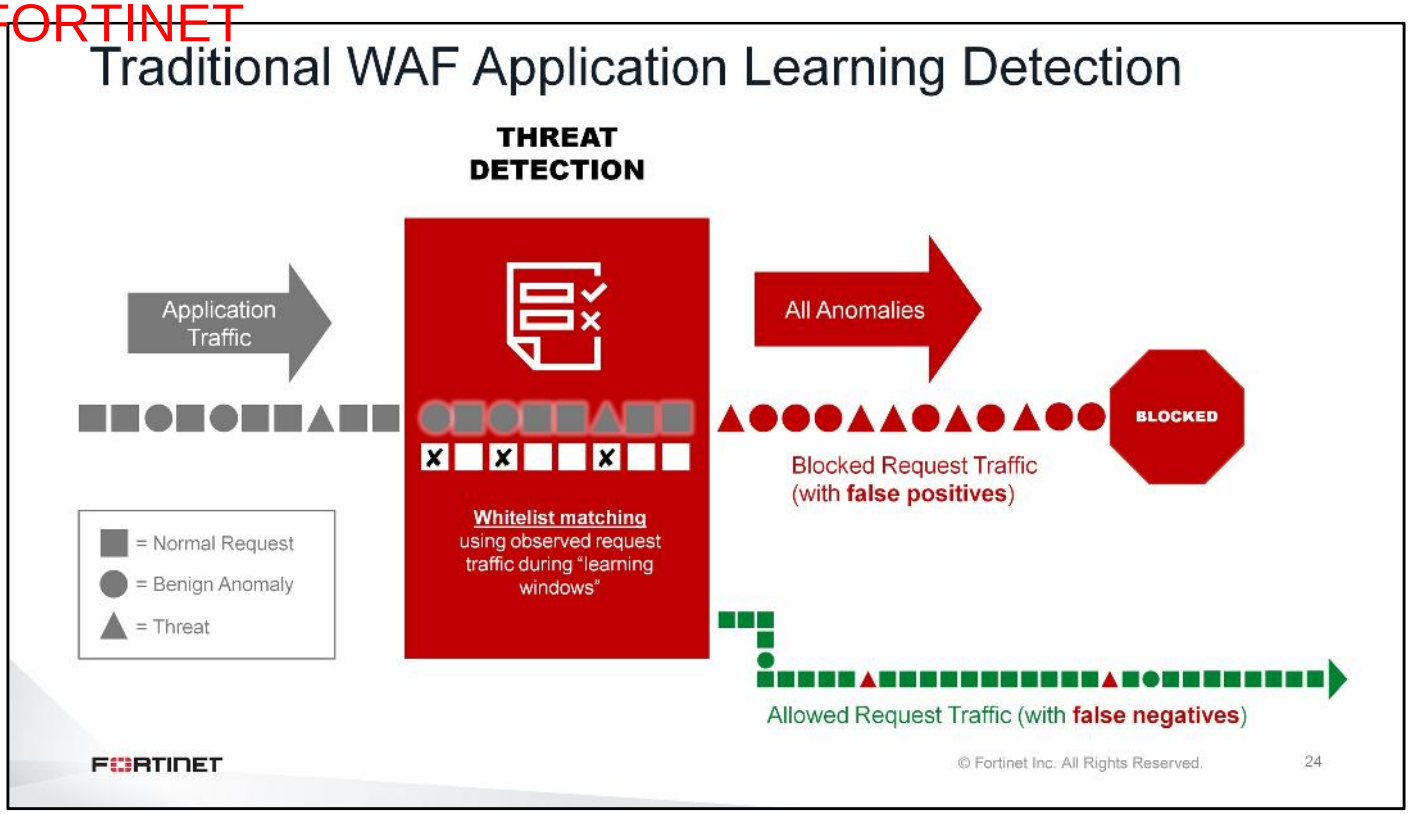


In this section, you will learn about machine learning (ML) on FortiWeb and how FortiWeb leverages probability to identify threats rather than running exacting matches against observed activities.

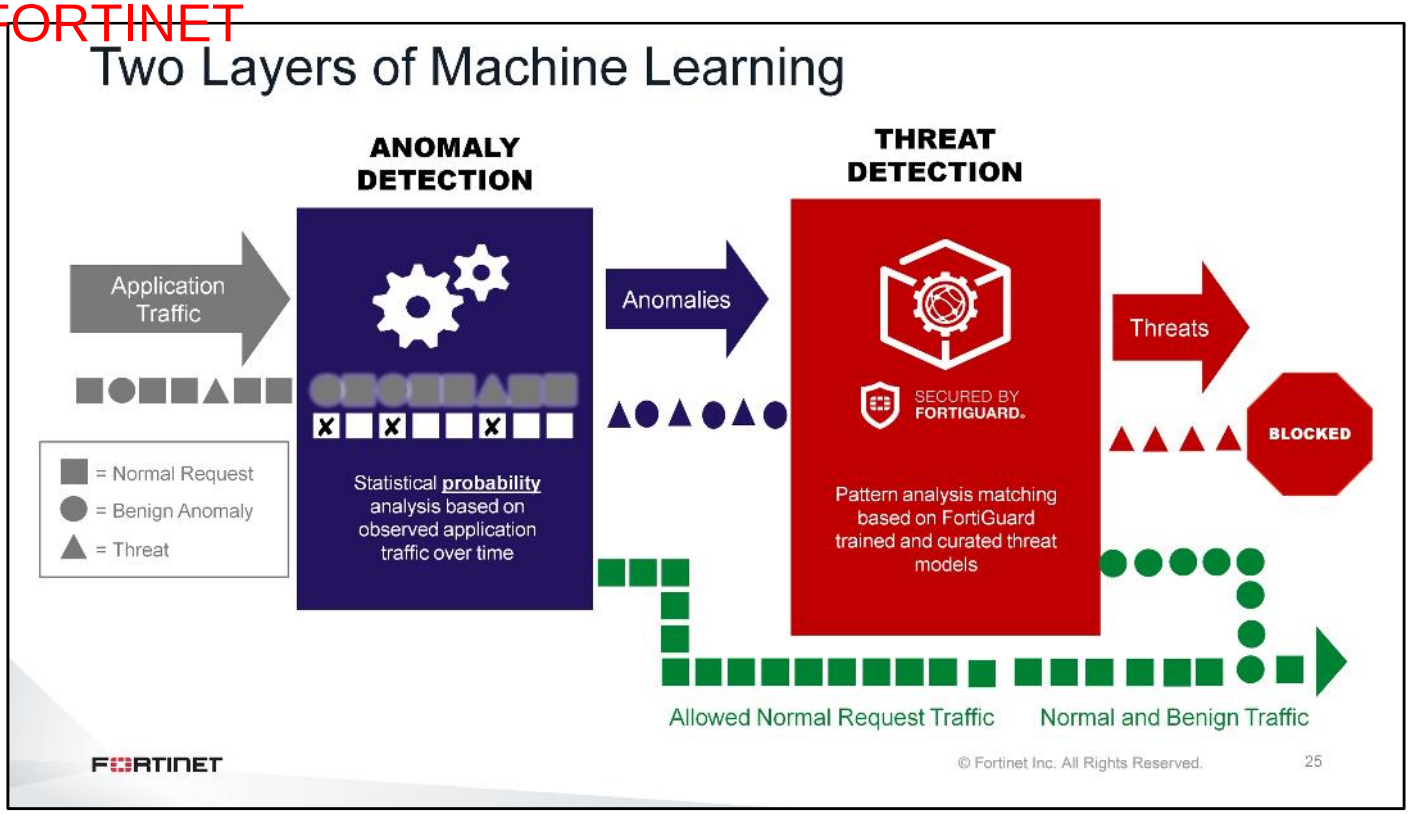


FortiWeb uses two machine layers. The first layer checks if the request is an anomaly, the second verifies if the anomaly is an attack. This is very different from today's solutions, which immediately block upon every anomaly, causing false positives and the frustration we see with customers. Additionally, with ML every request gets a probability value that is different from a yes/no match to an existing learned profile.

FortiWeb uses probability and argument length as two learning dimensions. Others dimensions might be added in the future.

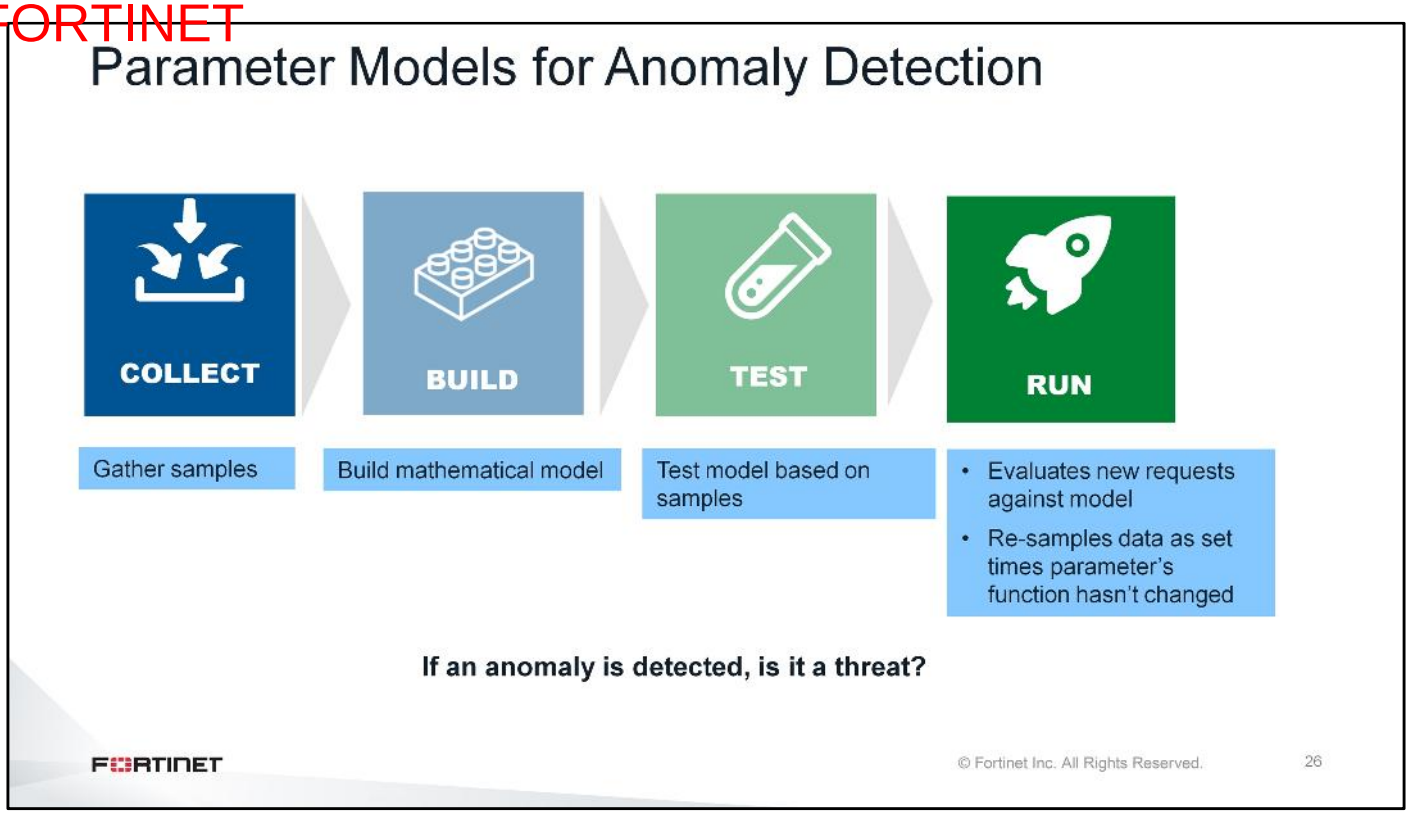


For traditional WAF blocking, all anomalies lead to high false positives, and accuracy requires labor intensive fine-tuning. Unobserved variations will trigger anomalies, and whitelisting characters used in attacks leads to threats evading detection. If you make any changes to applications, then that would require relearning.



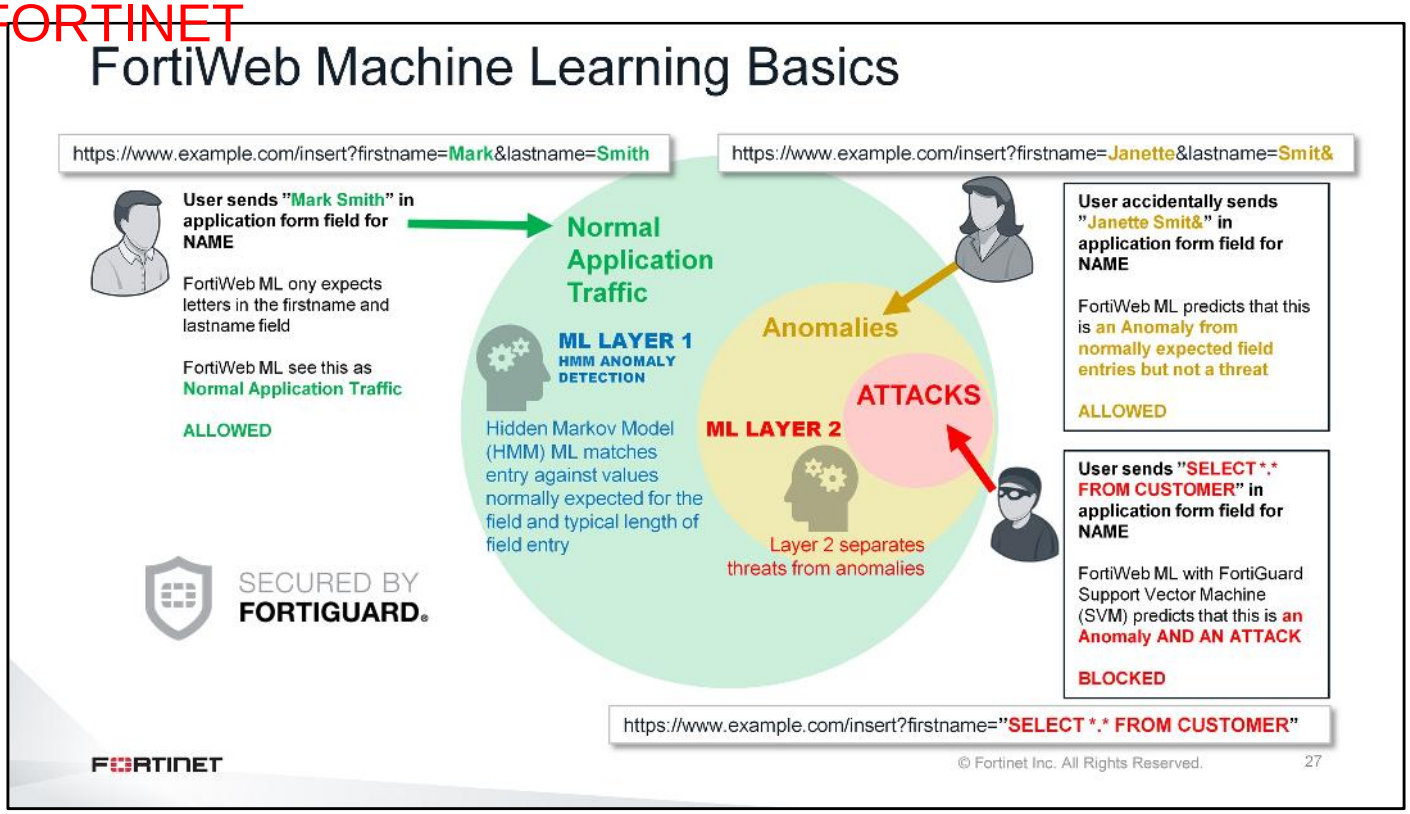
The second layer of ML is used to decide whether an anomaly detected by the first layer ML is an actual attack, a mistake entered by the user, or changes to the application that made new types of entries legitimate.

FortiWeb is loaded with threat models, each for a different attack vector (SQLi, XSS, and so on). These threat models are based on work done by the FortiWeb engineering team, which analyzed thousands of attacks from various sources. FortiWeb arrives with pre-built threat models that are updated periodically through the FortiGuard Security Service subscription.



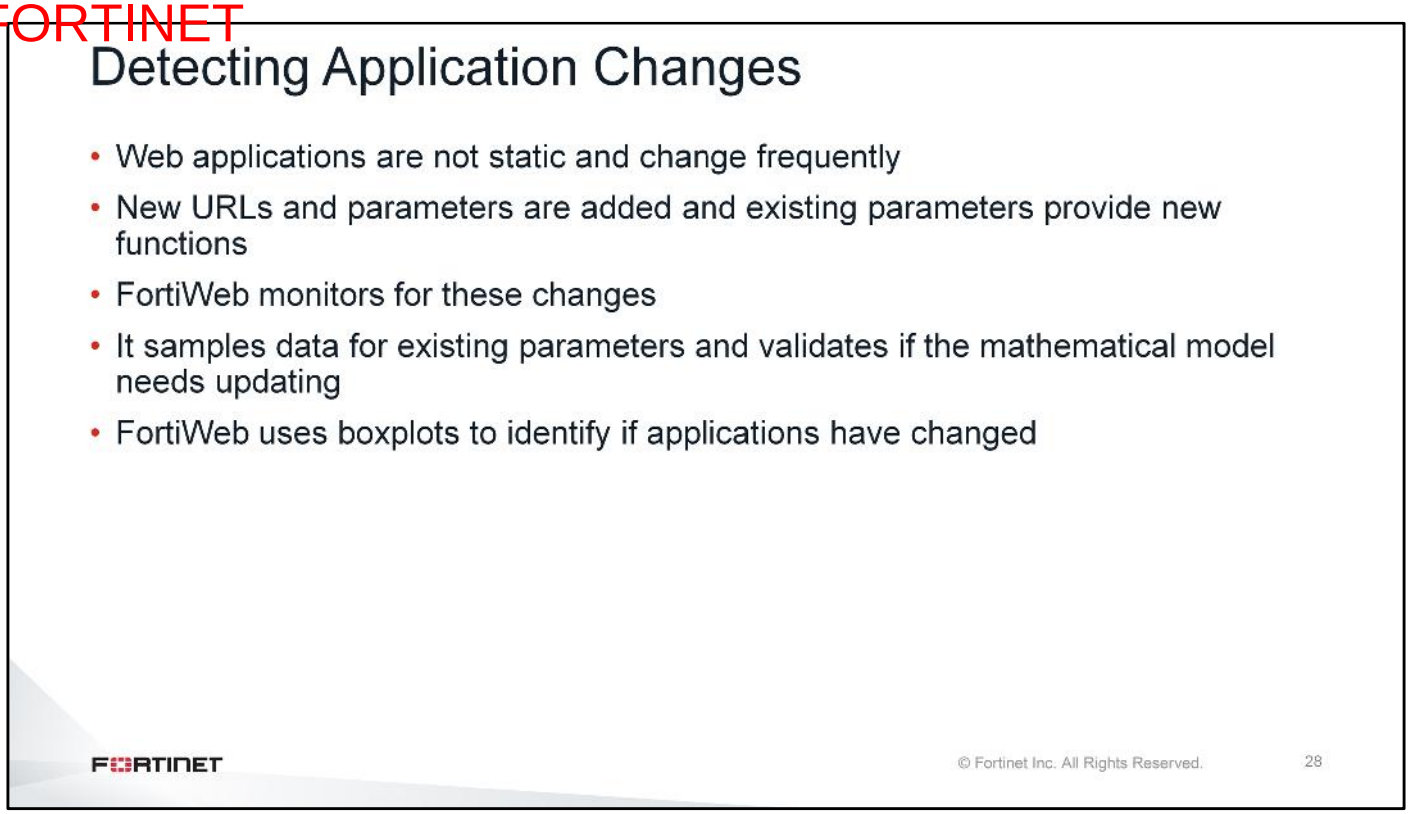
The example on this slide shows how FortiWeb's first layer ML works:

- Collects up to 5000 requests maximum or stops if it observes an obvious pattern
  - In Fast mode the number of requests needed is halved
- Builds the mathematical model for the parameter
- Tests the model against new requests
- Running mode: In this phase, the mathematical model for the parameter is already built and tested. Every request is evaluated based on it and anomalies will move to the second ML layer (threat detection). Additionally, in this phase FortiWeb uses a sophisticated mechanism to identify whether a parameter has changed. You will explore this on the next slide.



This slide shows a very simplified example of the client experience:

1. User Mark enters his first and last name correctly in the form field. These entries are inserted in the URL parameters and adhere to the ML profile FortiWeb built. No anomaly. User is allowed.
2. User Janette mistakenly enters the character '&' which triggers an anomaly by the first layer ML. However the second layer ML checks it against the threat models and verifies it's not a threat. Notice that with existing WAF solutions with standard application learning this would trigger an anomaly that would be blocked, causing a false positive. With FortiWeb ML the legitimate request passes through.
3. An attacker injects SQL code into a parameter. The first layer ML identifies it as an anomaly and the second layer ML identifies it as an attack.

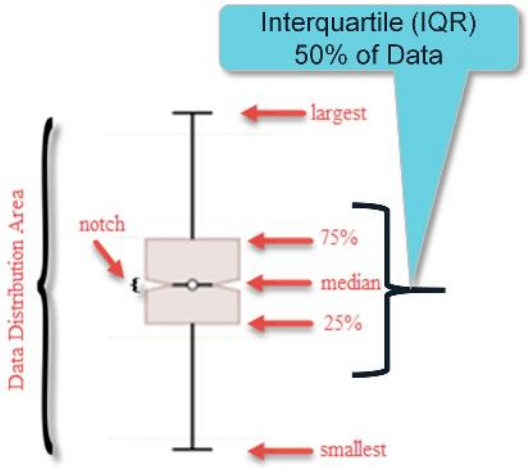


Applications change frequently as new URLs are added and existing parameters provide new functions. This means the mathematical model of the same parameter might be different than what FortiWeb originally observed during the collection phase. In this case, FortiWeb needs to relearn the parameter and then update the mathematical model for it.

FortiWeb uses boxplots to determine that the functions of the parameter have changed.

Boxplots

- Boxplots display the probability distribution of the samples with regard to the mathematical model built for the parameter
- During the running stage, FortiWeb continues to sample data at predefined times and these samples are then displayed in a boxplot
- It then compares the latest boxplot(s) to the boxplots gathered during the collection stage
- If the new boxplots do not overlap, FortiWeb will collect the samples again and regenerate the mathematical model to adapt to the new parameter's function

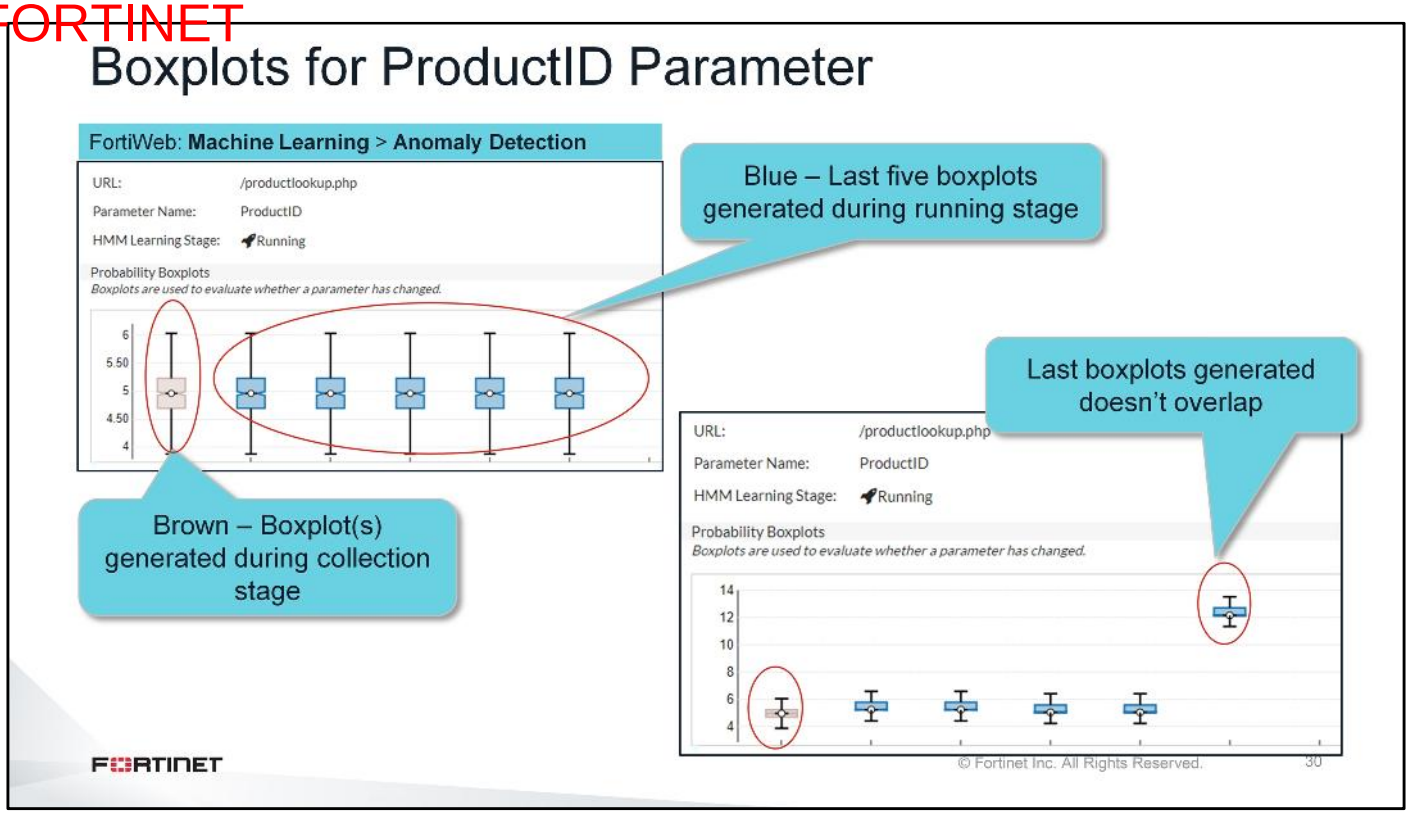


FORTINET

29

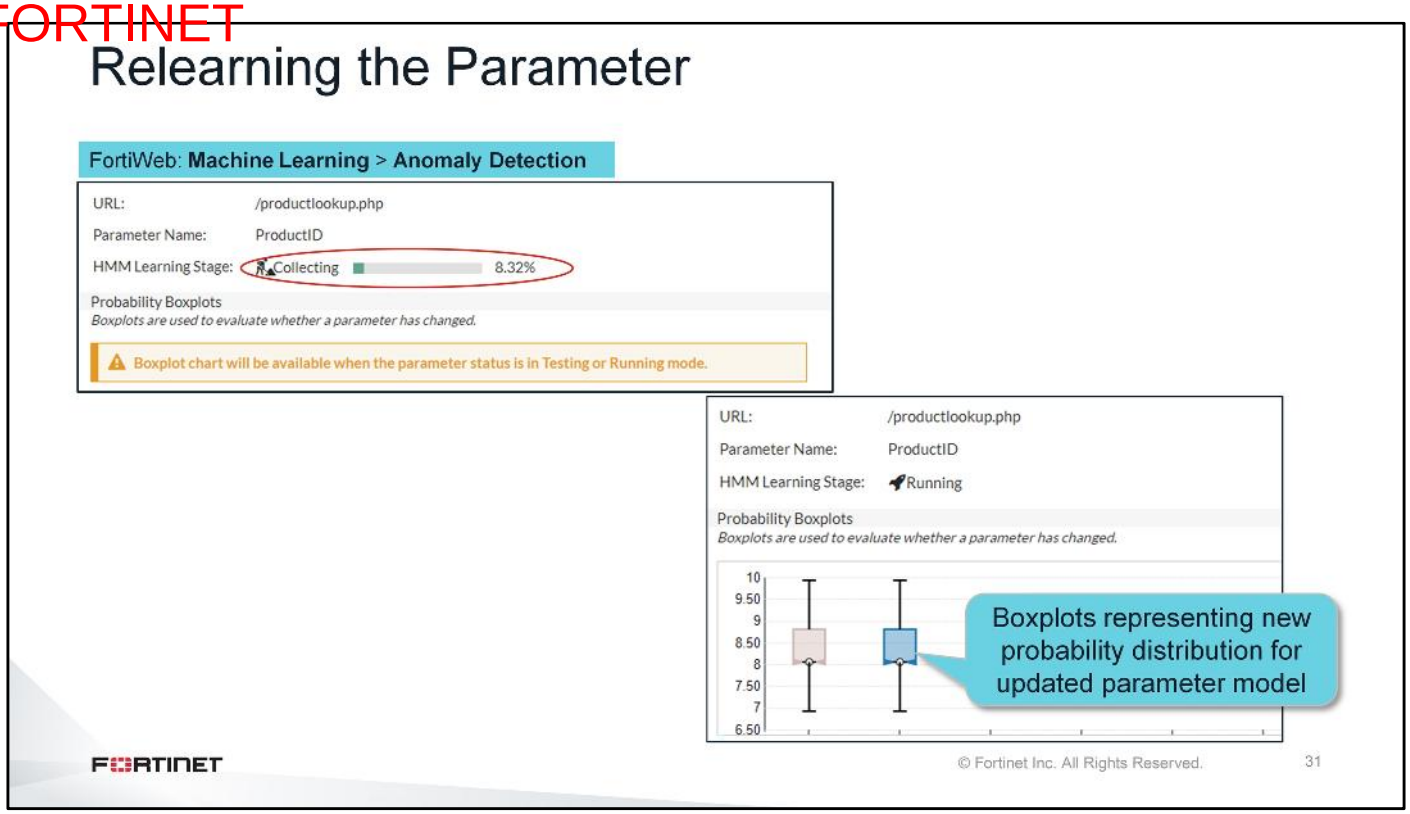
Boxplots depict numerical data and the probability distribution of a specific number of parameter values.

During the sample collection period, the system generates 1 to 4 boxplots (sample boxplots). After the machine learning model is built, the system will keep on generating new boxplots to display the probability distribution of the new inputs. If the new boxplots do not overlap with the sample boxplots, the machine learning model for that parameter will be rebuilt.



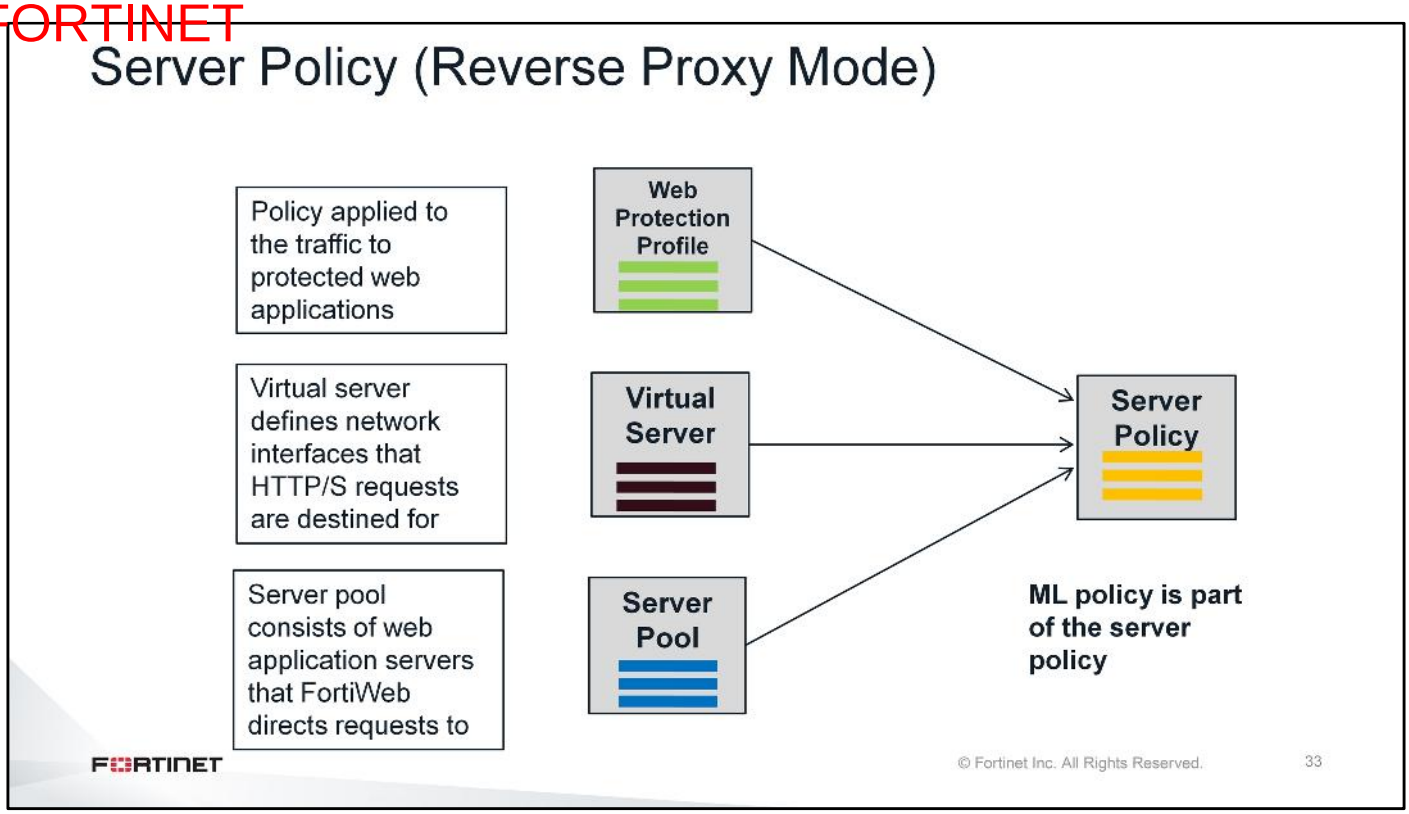
FortiWeb compares previous boxplots for newly created boxplots to see if the parameter has changed and then if the HMM mathematical model needs to be updated.

The slide shows an example of the boxplot diagram. The new boxplots are shown in blue, whereas the sample boxplots are brown. The system displays, at most, five new boxplots. With new inputs coming in and new boxplot generated, the system will remove the oldest one at the left to create a place for the new boxplot.



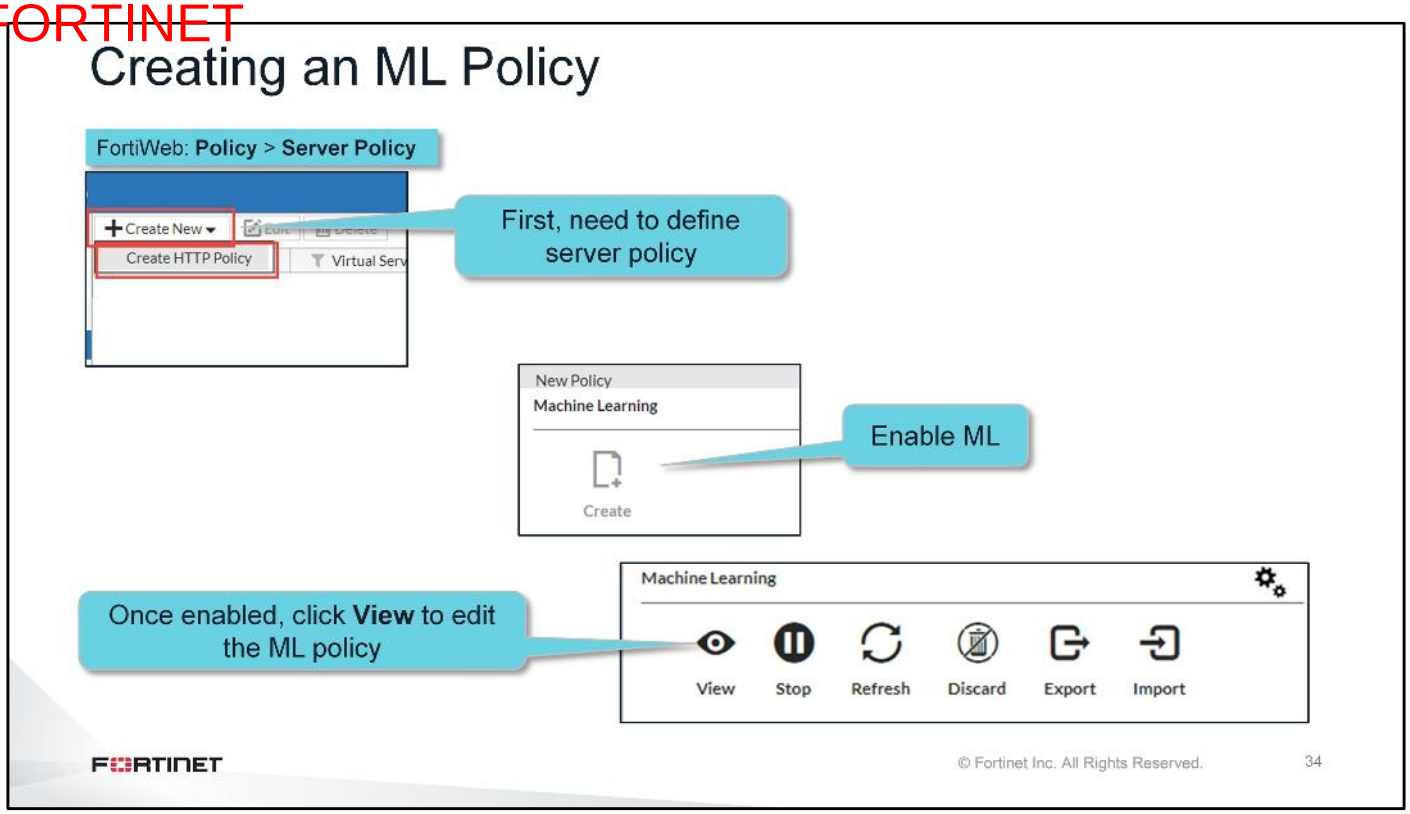
Continuing from the previous slide, this slide shows that the mathematical learning model for the **ProductID** parameter is being rebuilt.

In this section, you will learn how to enable ML on FortiWeb and configure various parameters on the ML policy.



To enable ML, at a minimum you need to define a **Server Policy**, which requires you to create the two server objects, **Virtual Server** and **Server Pool**. While a **Web Protection** profile doesn't need to be created, it is through this profile that the signatures can be applied to monitor traffic. Although technically not required when using ML, signatures easily eliminate known attack types before they get to the ML layers. This reduces strain on system resources and yields cleaner application parameter profiles.

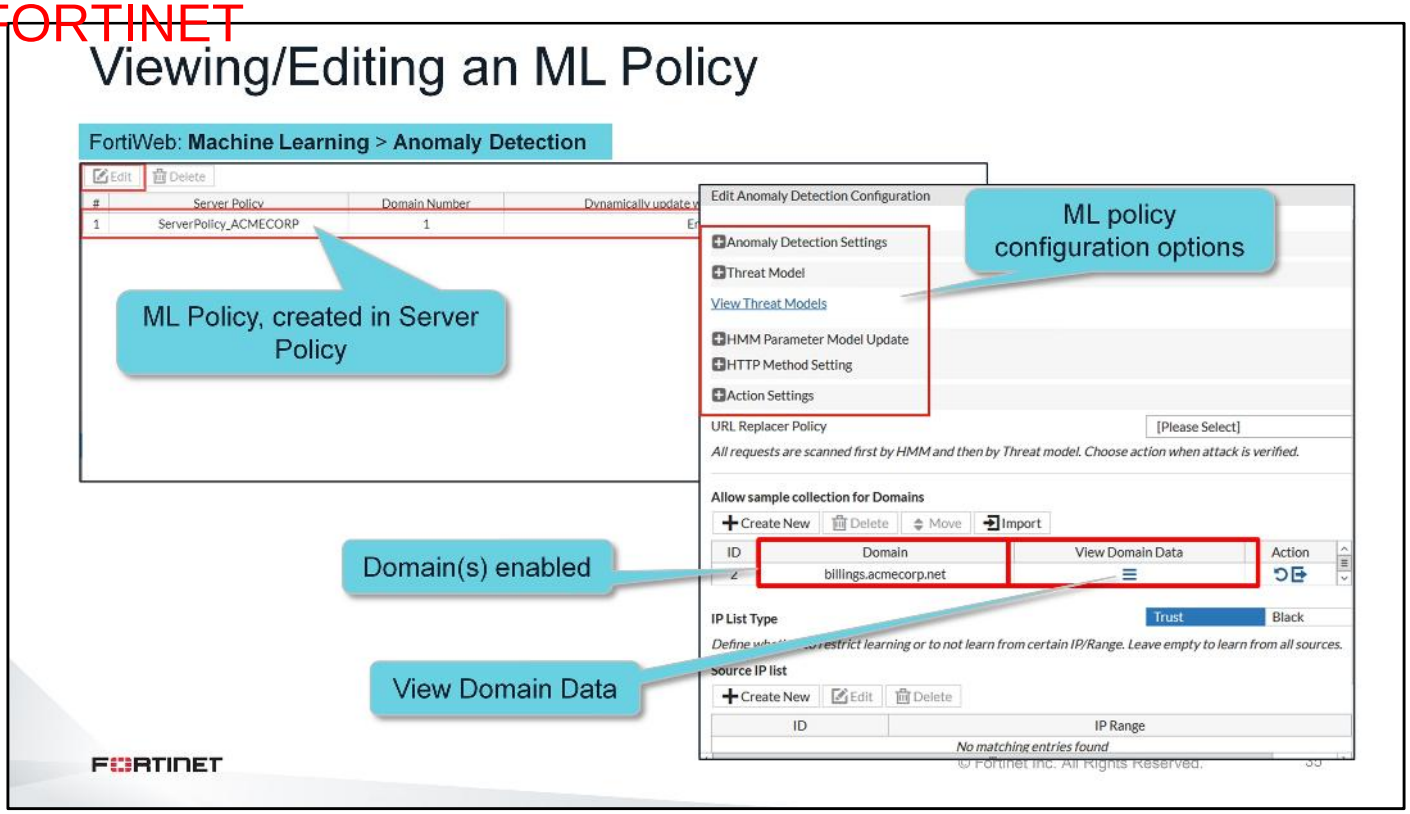
If there is no matching policy, then FortiWeb handles traffic based on the mode it is configured in. If FortiWeb is configured in reverse proxy mode, then non-matching traffic is denied. If it is configured in any other mode, then non-matching traffic will be allowed.



To create a machine-learning policy:

1. Click **Policy** >**Server Policy**.
2. Select **Create New** > **Create HTTP Policy**. The **New Policy** page opens
3. Scroll down to the **Machine Learning** section at the bottom of the page, and click **Create.** The **New Machine Learning** dialog opens.
4. Add the desired domains and IP addresses.
5. Click **Create** to enable machine learning.

Once enabled, the **Machine Learning** section will show four control buttons, as shown on the slide.



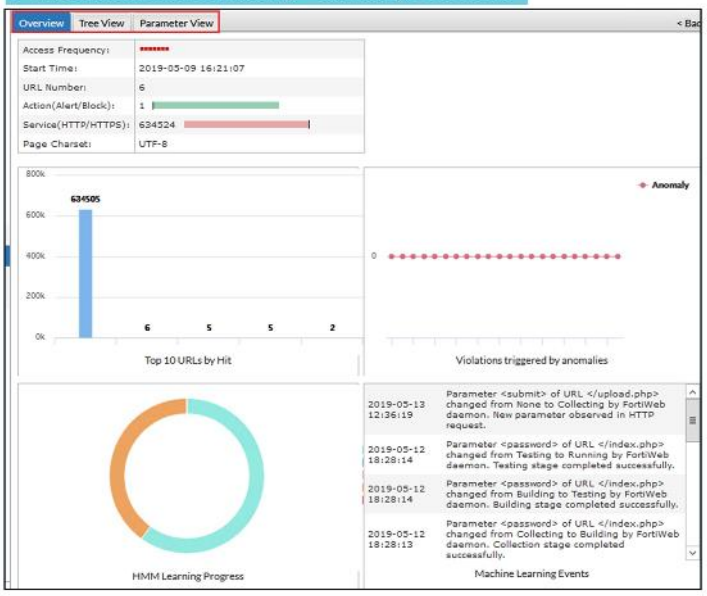
To **View** or **Edit** the ML policy:

1. Click **Machine Learning** > **Anomaly Detection**.
2. Select the corresponding **Server Policy** and then click **Edit**

Viewing Domain Data—Overview

- Summary of data collected for the domain through the use of the ML profile
- It reports the
  - Domain overview info
  - Top 10 URLs by Hit
  - HMM Learning Progress
  - Violations Triggered by Anomalies
  - Machine Learning Events

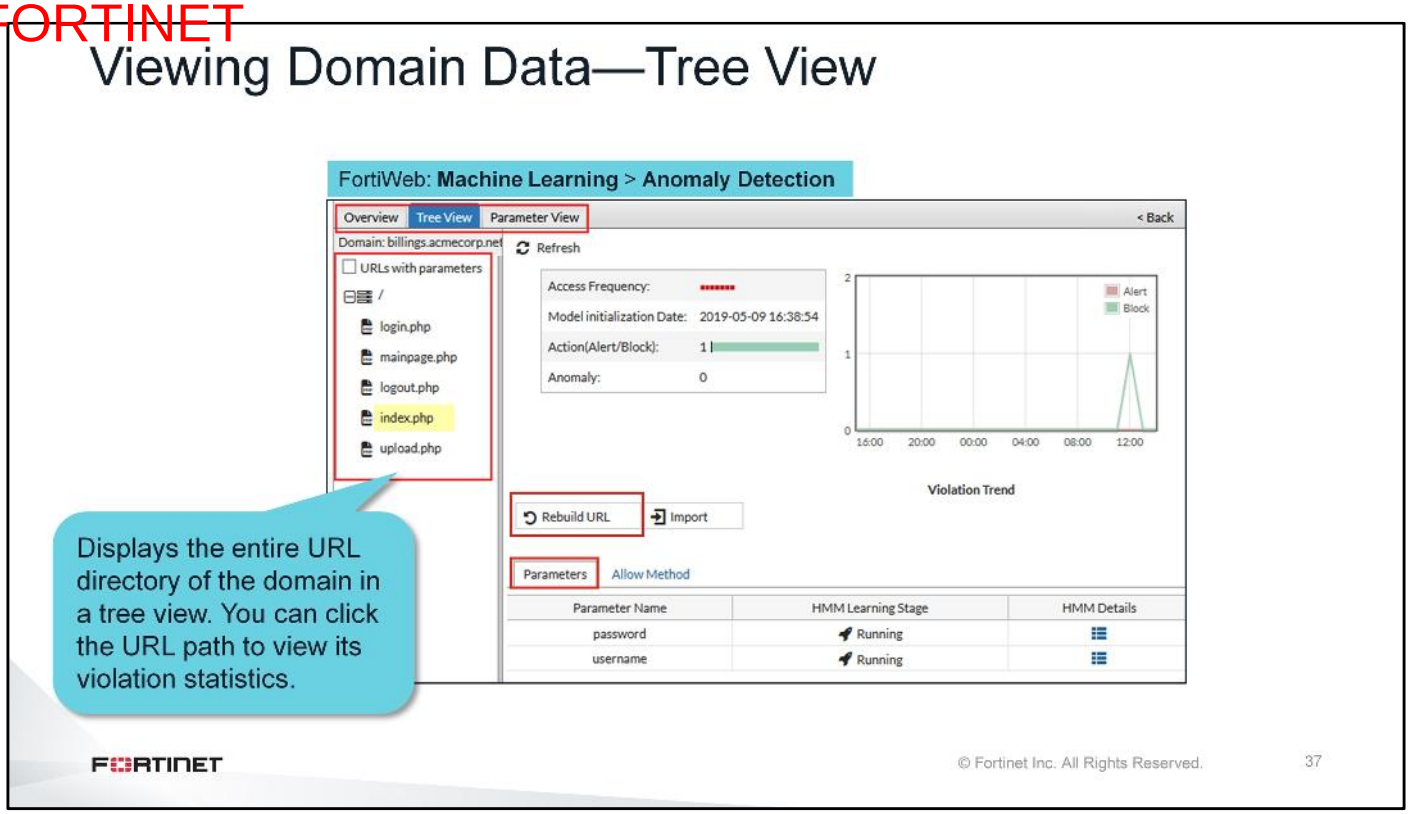
FortiWeb: **Machine Learning** > **Anomaly Detection**



FORTINET

36

The **Overview** tab provides a summary of data collected for the domain through the use of the ML profile. It reports information about the entire domain, including the domain overview, Top 10 URLs by Hit, HMM Learning Progress, Violations Triggered by Anomalies, and Machine Learning Events dashboard.

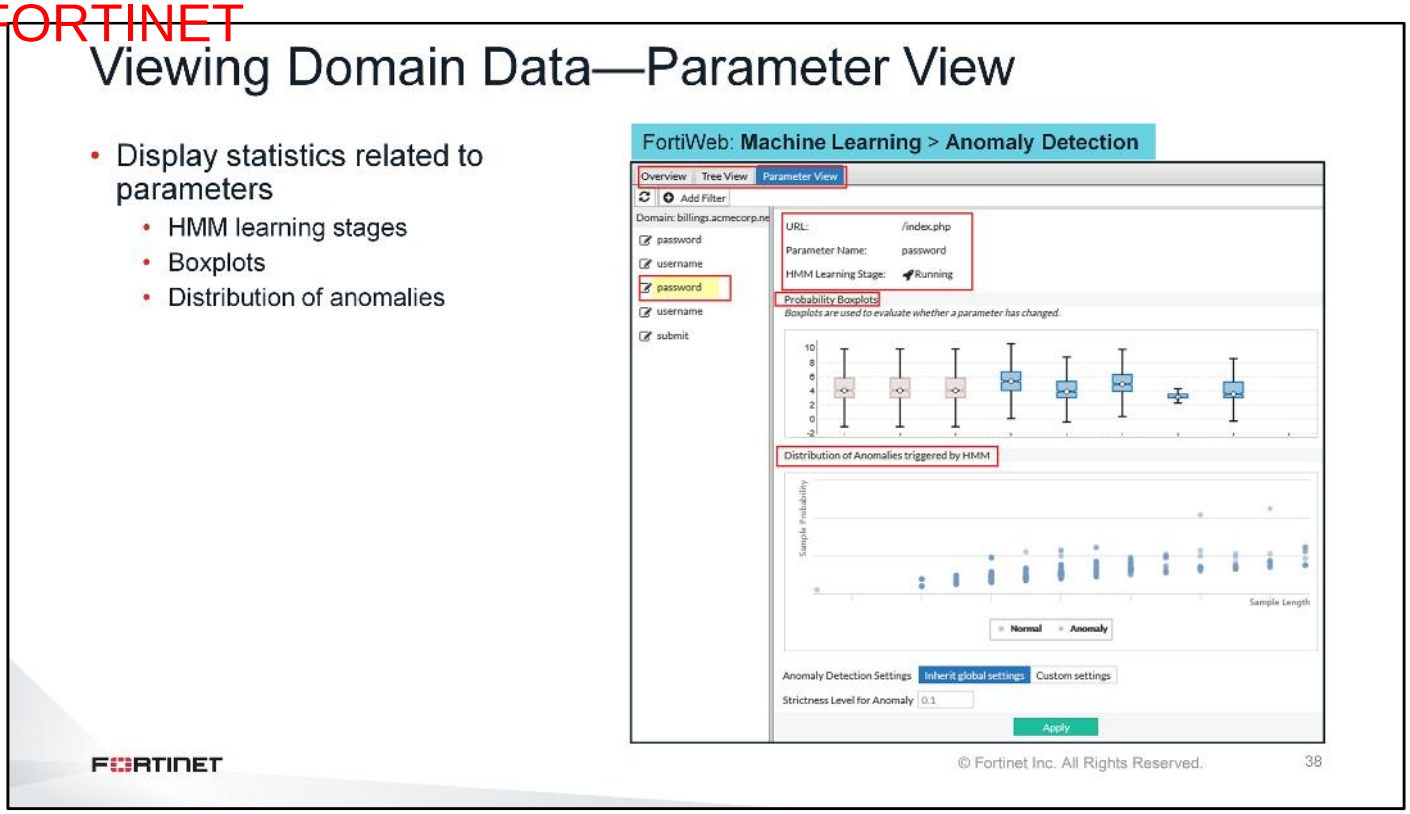


The **Tree View** displays the entire URL directory of the domain in a tree view. You can choose either one of the URLs to view its violation statistics.

Web site directory: The left panel of the **Tree View** page shows the directory structure of the website. The / (backslash) indicates the root of the site. You can click a URL in the directory tree, then the violation statistics of this URL will be displayed on the right side of the **Tree View** page. You can also click a directory, then click **Rebuild Directory** to rebuild ML models for all the URLs under the selected directory.

Parameters: The Parameters tab shows the HMM learning states of all the parameters attached to the URL. For example, if the URL is `http://www.demo.com/1.php?user_name=jack`, then `user_name` is the parameter. A URL can contain multiple parameters.

Allow Method: You can set the HTTP request methods that are allowed to access the URL.



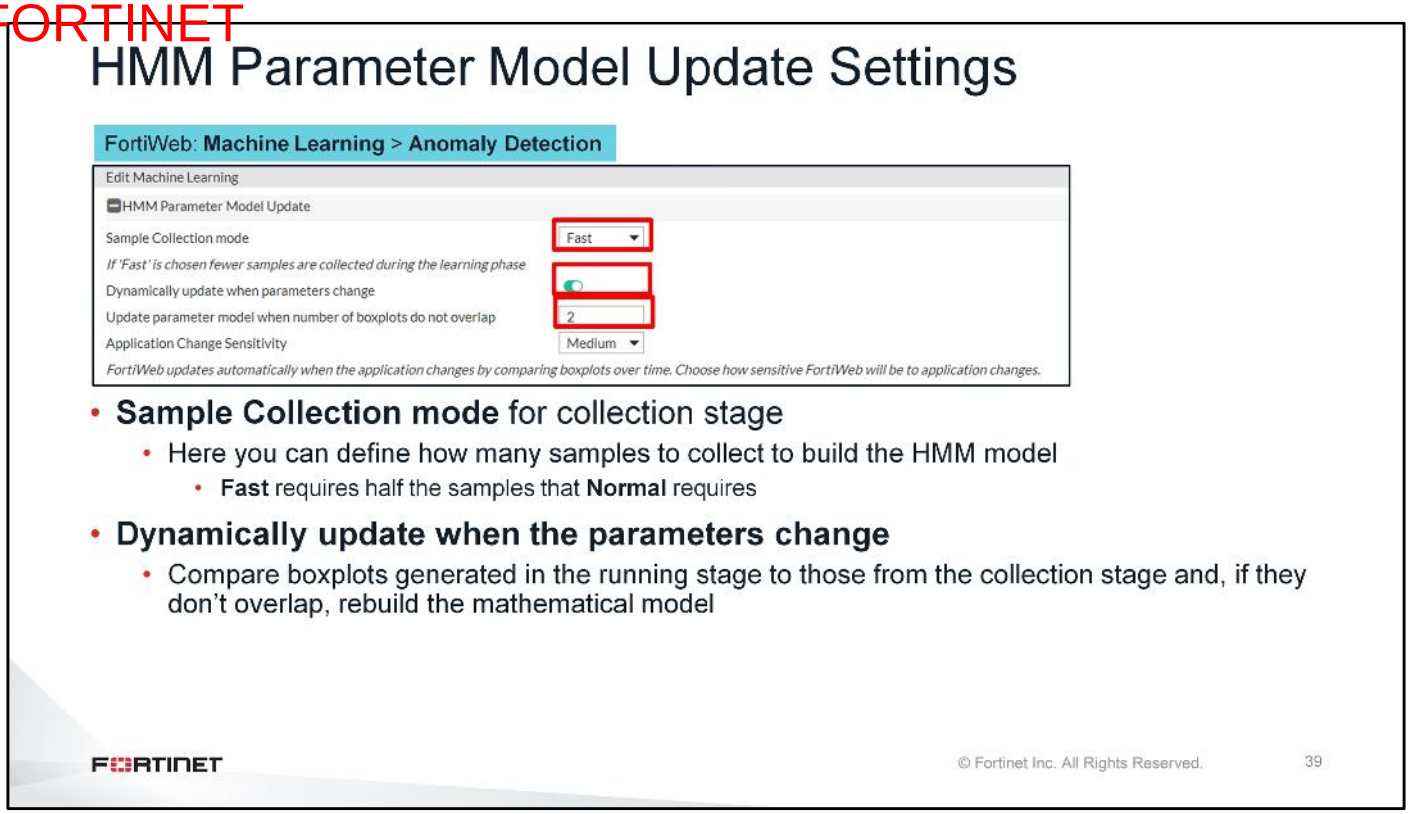
Parameter View displays machine learning statistics for all the parameters. You can click **Add Filter** on the upper-left corner of the page, and filter the parameters by name or learning status.

Applications change frequently as new URLs are added and existing parameters provide new functions. This means the mathematical model of the same parameter might be different than what FortiWeb originally observed during the collection phase. In this case, FortiWeb needs to relearn the parameter and then updates the mathematical model for it.

First of all, FortiWeb needs to determine that the functions of the parameter have changed. To do that, it uses boxplots to depict numerical data and the probability distribution of a certain number of parameter values.

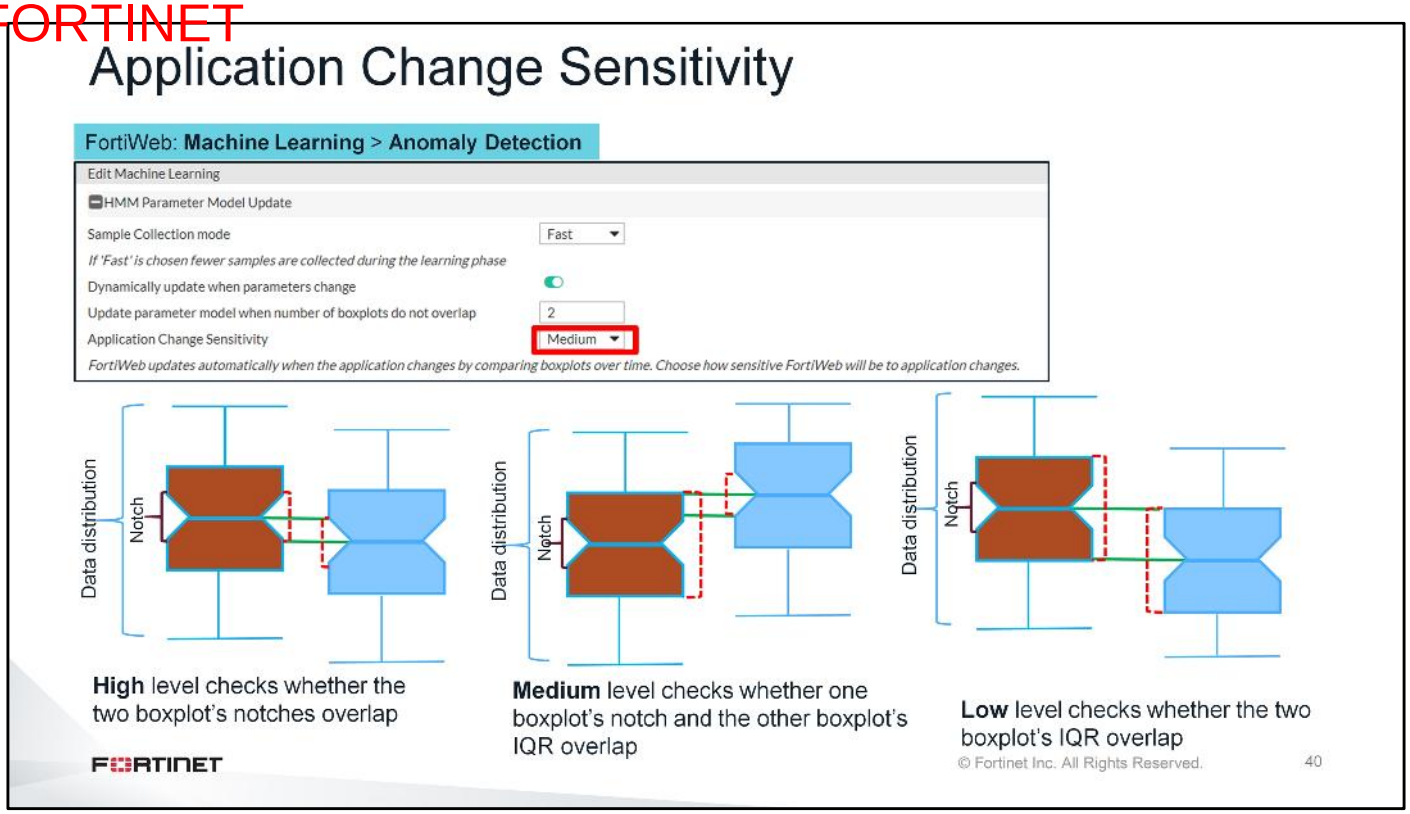
Every time the system observes 500 valid parameter values, it generates one boxplot to display the probability distribution of these values. During the sample collection period, the system generates two or four boxplots (sample boxplots). After the anomaly detection model is built, the system will keep on generating new boxplots to display the probability distribution of the new inputs. The slide shows an example of the boxplot diagram. The new boxplot is shown in blue, whereas the sample boxplots are brown. The system displays, at most, five new boxplots. With new inputs coming in and new boxplots generated, the system will remove the oldest one at the left to create a place for the new boxplot.

Distribution of Anomalies triggered by HMM displays the potential anomalies in red and the normal requests collected during the sample collection phase in blue. The system judges whether a request is normal or not based on its probability and the length of the parameter value.



There are two modes for sample collection, **Normal** and **Fast**. In normal mode FortiWeb collects up to 5000 samples to build an ML model for the parameter and in fast mode it collects 2500 samples.

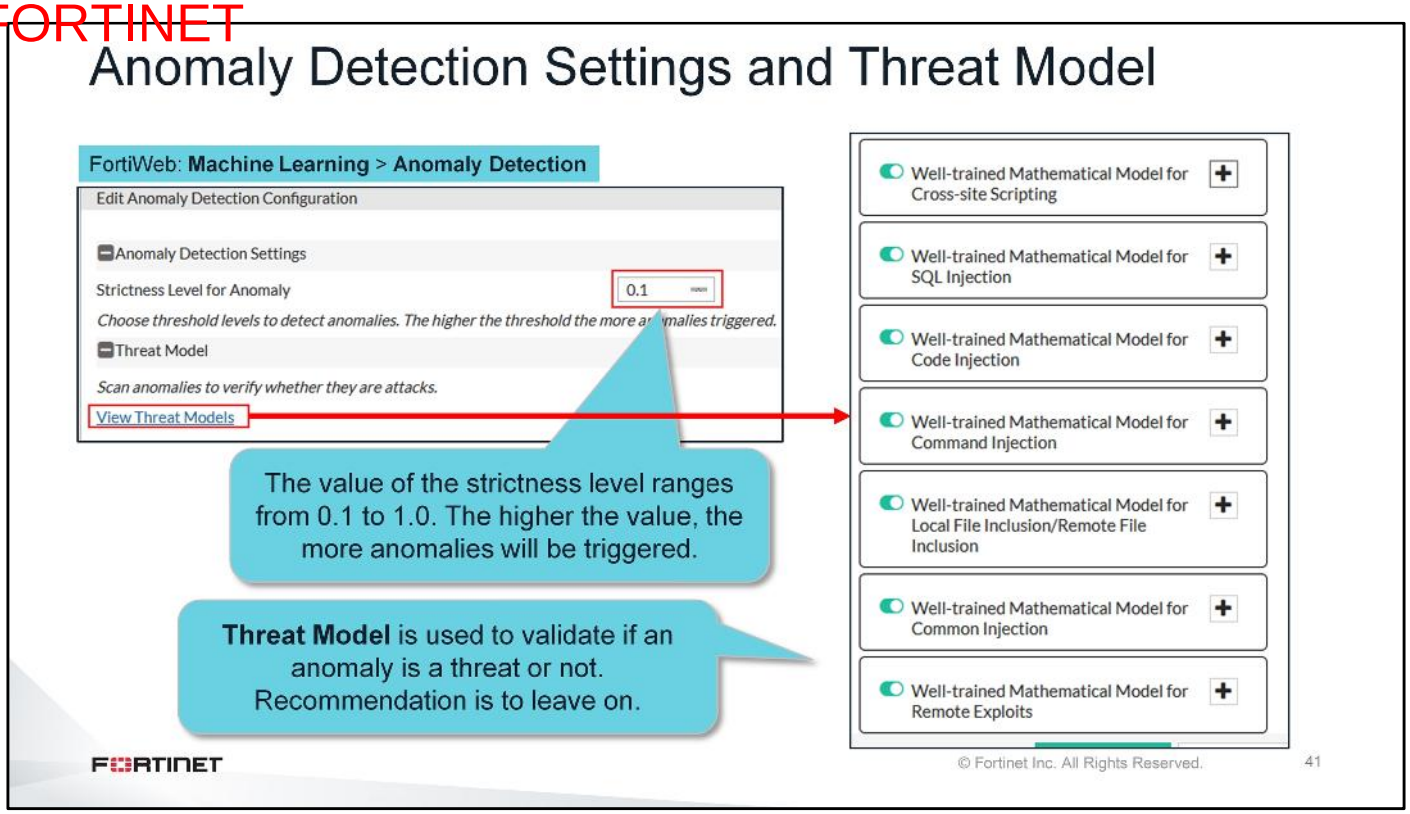
Applications on the backend servers change frequently as new URLs are added and existing parameters provide new functions. This means the mathematical model of the same parameter might be different from what FortiWeb originally observed during the collection phase. In this case, FortiWeb needs to relearn the parameter and updates the mathematical model for it. For that reason you need to enable the option **Dynamically update when parameters change** and select a value between 1 to 3 for the field **Update parameter model when number of boxplots do not overlap**. The default value is 2, which means if two newly generated boxplots don't overlap with any one of the sample boxplots, FortiWeb automatically updates the ML model.



The system uses boxplots to determine whether a parameter has changed. The boxplot displays the probability distribution of the parameter value. During the sample collection period, the system generates two or four boxplots. After the ML model is built, the system will keep on generating new boxplots to display the probability distribution of the new inputs. If the probability distribution area of the newly generated boxplot doesn't overlap with any one of the sample boxplots, the system determines this parameter has changed.

Depending on the **Application Change Sensitivity** level, the system triggers a model update when it observes different extents of overlapping areas.

Low—The system triggers a model update when the IQR area of the new boxplot doesn't overlap with the IQR areas of the sample boxplots.
Medium—The system triggers a model update if the notch area of the new boxplot doesn't overlap with the IQR areas of the sample boxplots.
High—The system triggers a model update when the notch area of the new boxplot doesn't overlap with the notch area of the sample boxplots.

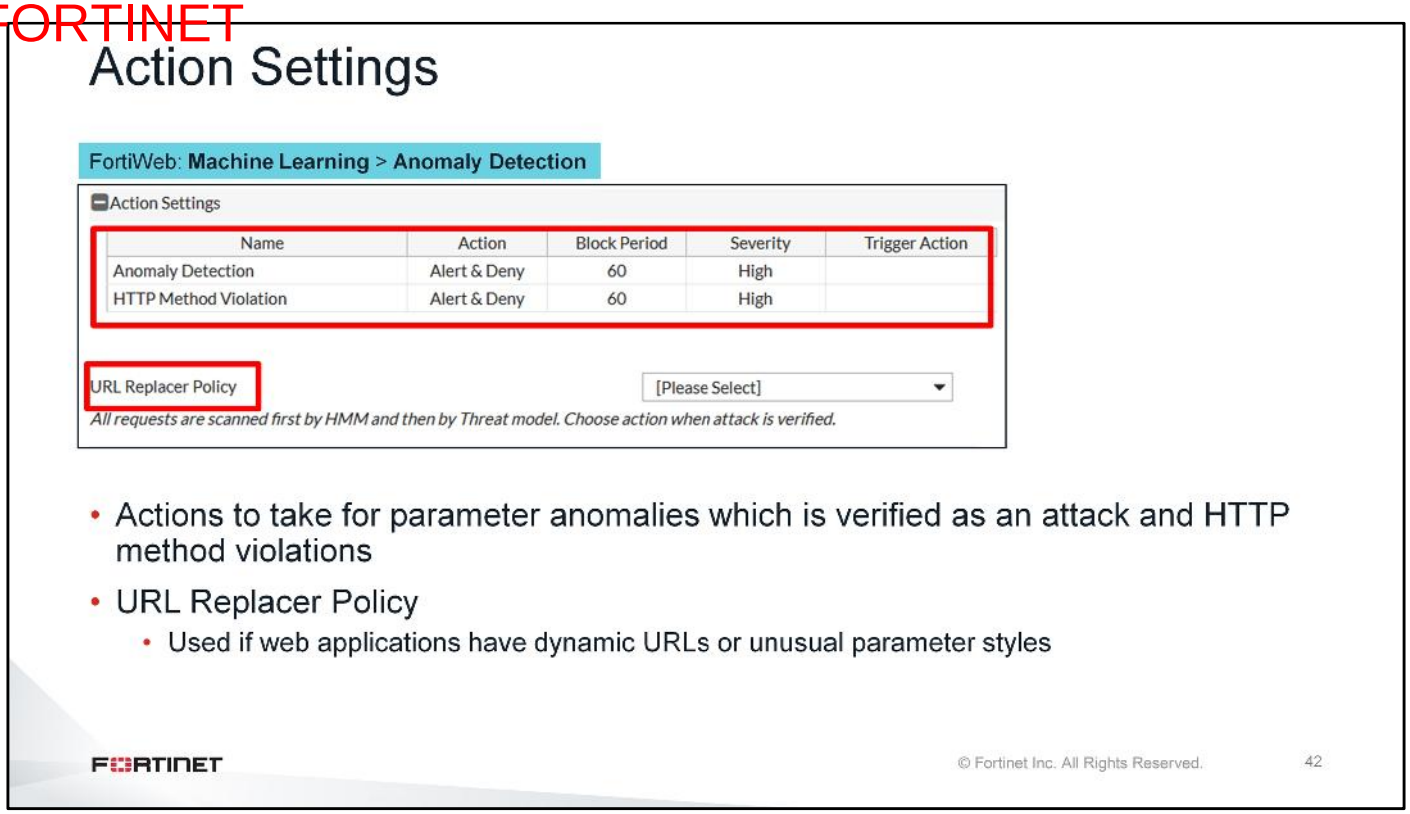


The ML model judges whether a request is normal or not based on its HMM probability and the length of the parameter value.

You can set the strictness level for the model. The value of the strictness level ranges from 0.1 to 1.0. The higher the value, the more anomalies will be triggered. For example, 0.1 means that the 0.1% of all samples with the largest HMM probability and length will be treated as anomalies.

The system scans anomalies to verify whether they are attacks. It provides a method to check whether an anomaly is a real attack by the trained SVM Model.

Click the **View Threat Models** link to enable or disable threat models for different types of threats such as XSS, SQL injection, and code injection. Currently, seven trained Support Vector Machine Models are provided for seven attack types. The threat model is updated periodically through the FortiGuard server update and has been extensively trained and tested by the FortiGuard team. They are created using thousands of real attack samples from various sources. These include well-known third-party databases such as CVE and Exploit DB, FortiGuard Labs, and leading third-party vulnerability scanners.



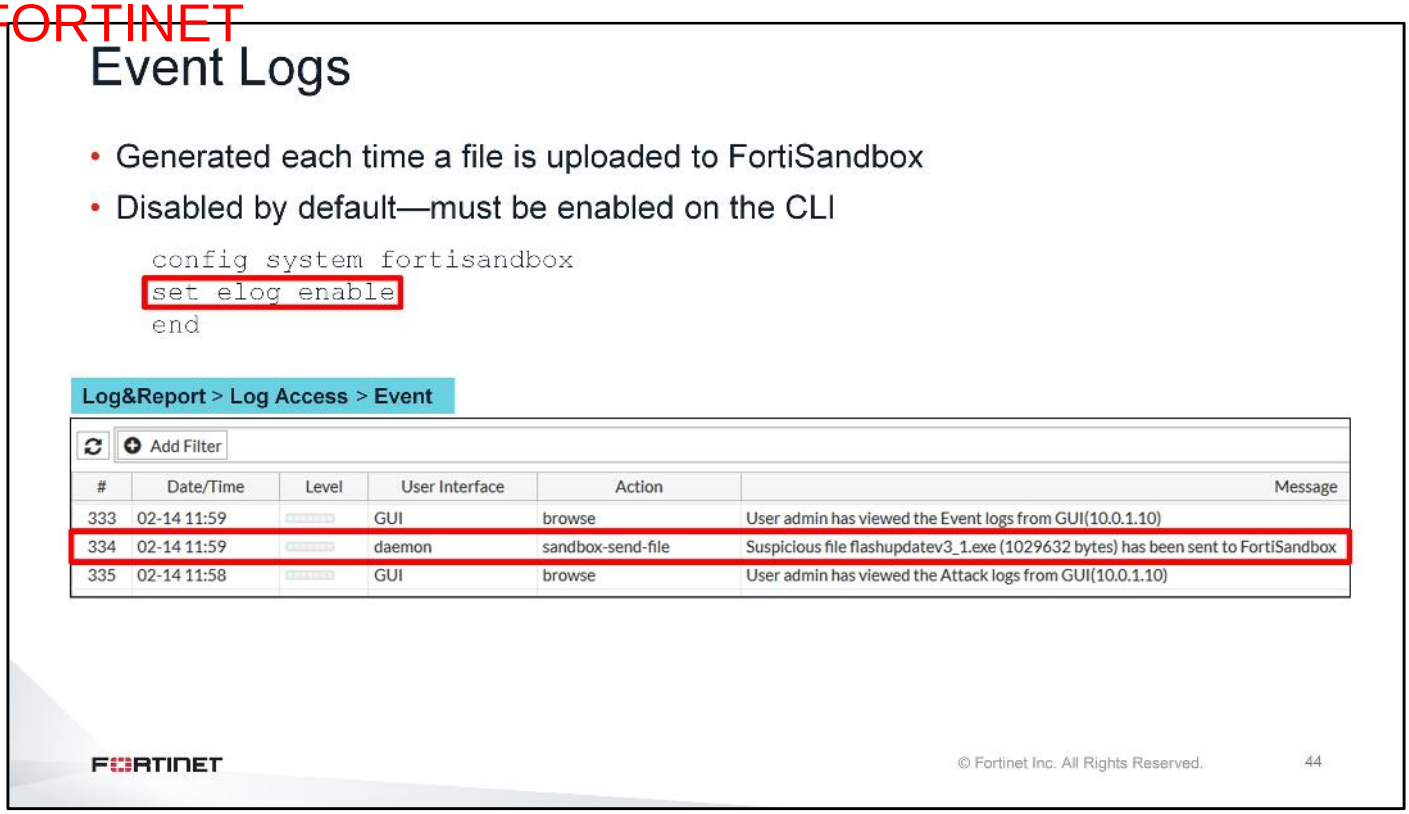
All requests are scanned first by HMM and then by threat model.

Double-click the cells in the **Action Settings** table to choose the action FortiWeb takes when an attack is verified for each of the following situations:

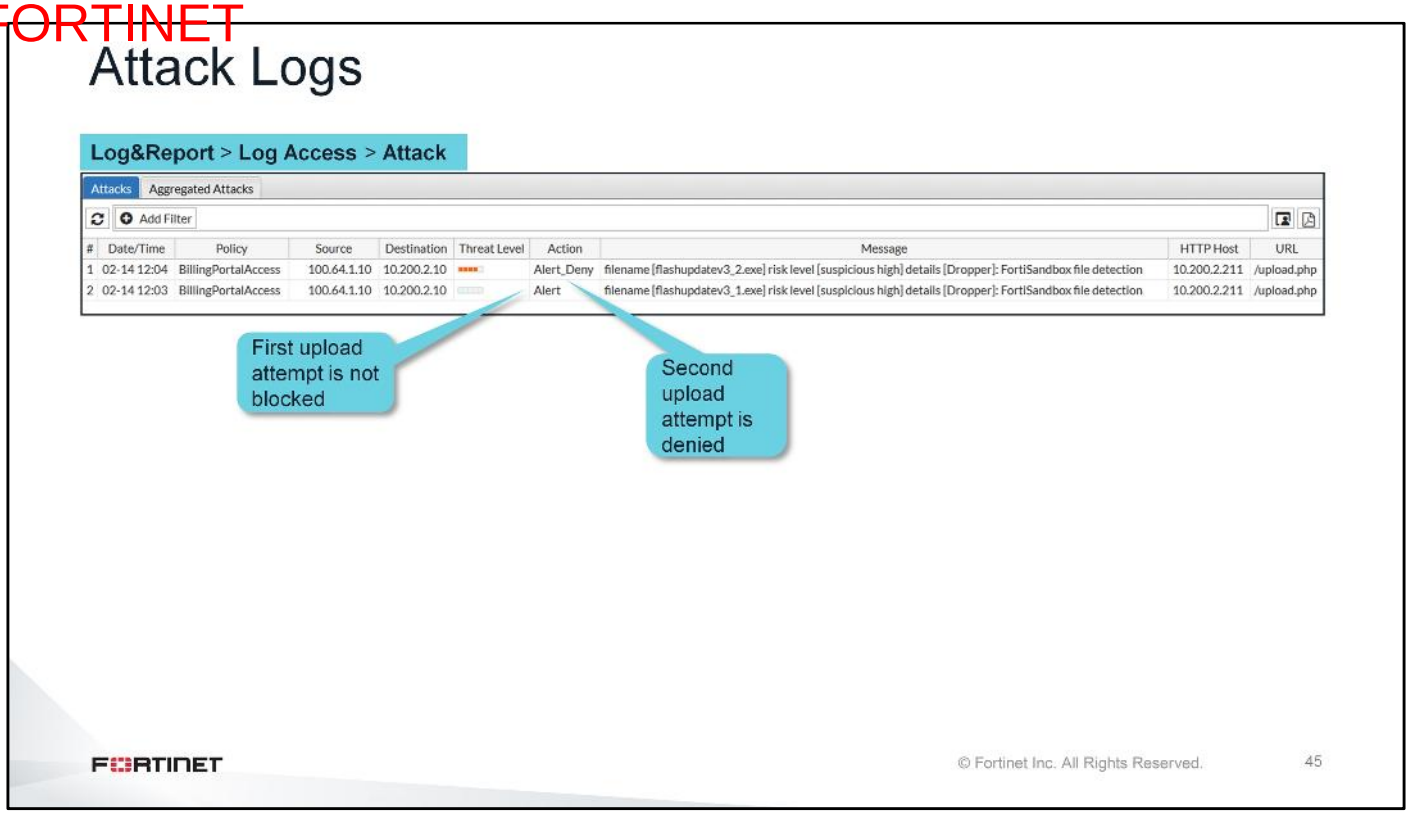
- **Alert**: Accepts the connection and generates an alert email and/or log message
- **Alert & Deny**: Blocks the request (or resets the connection) and generates an alert and/or log message
- **Period Block**: Blocks the request for a certain period of time

If the web application has dynamic URLs or unusual parameter styles, you must adapt the URL Replacer Policy to recognize them. You need to first create a **URL Replacer Policy** in **Machine Learning Templates**.

In this section, you will learn how to verify FortiSandbox operation using FortiWeb logs.

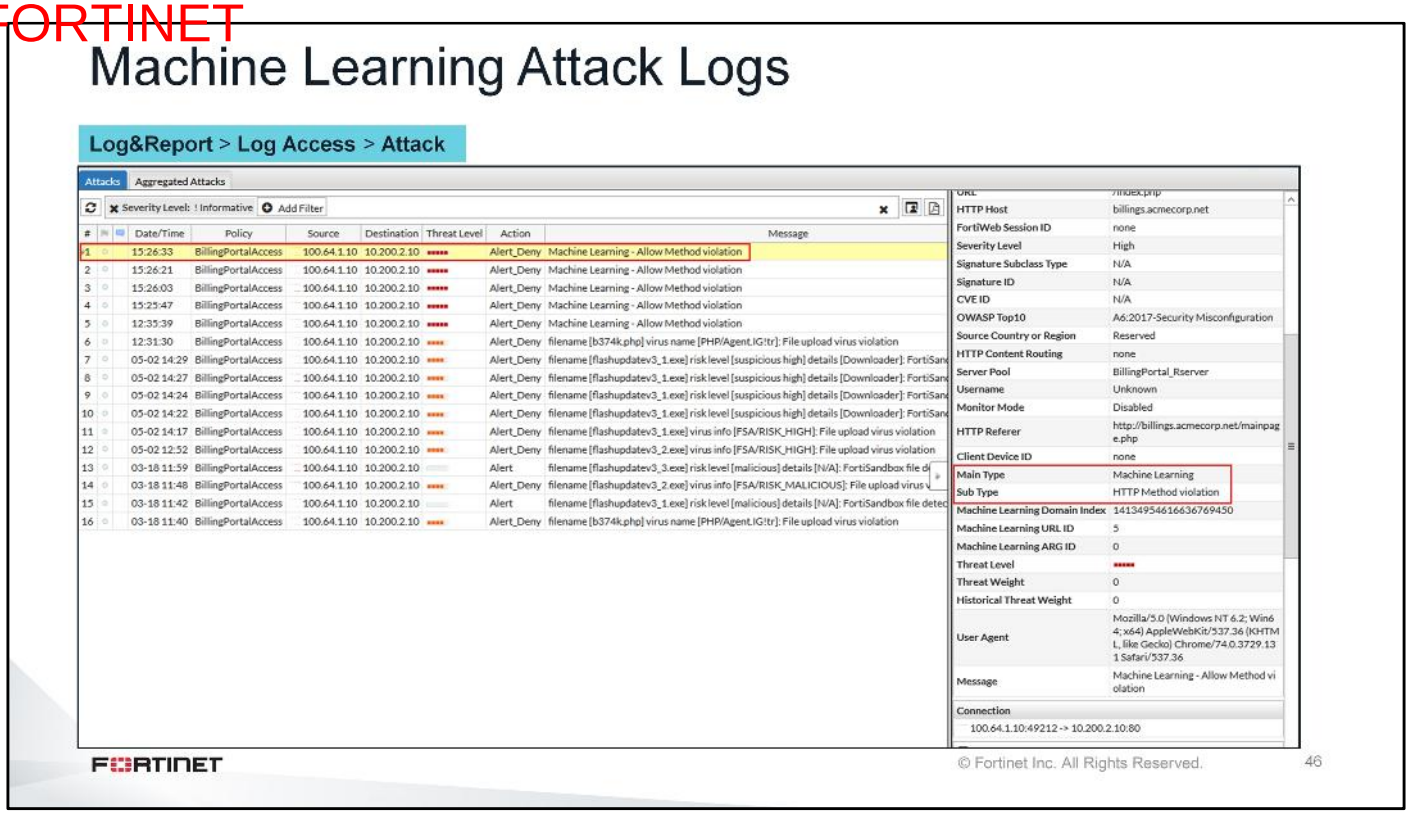


FortiSandbox file submissions are logged in event logs. These logs are generated every time a file is uploaded to FortiSandbox. This feature is disabled by default and must be enabled on the CLI using the commands shown on this slide.



If the hold session feature is disabled in the file filter ruile, FortiWeb generates an alert the first time a suspicious file is detected. Any future upload attempts of the same malicious file will generate an alert and a deny action. FortiWeb logs these events in attack logs.

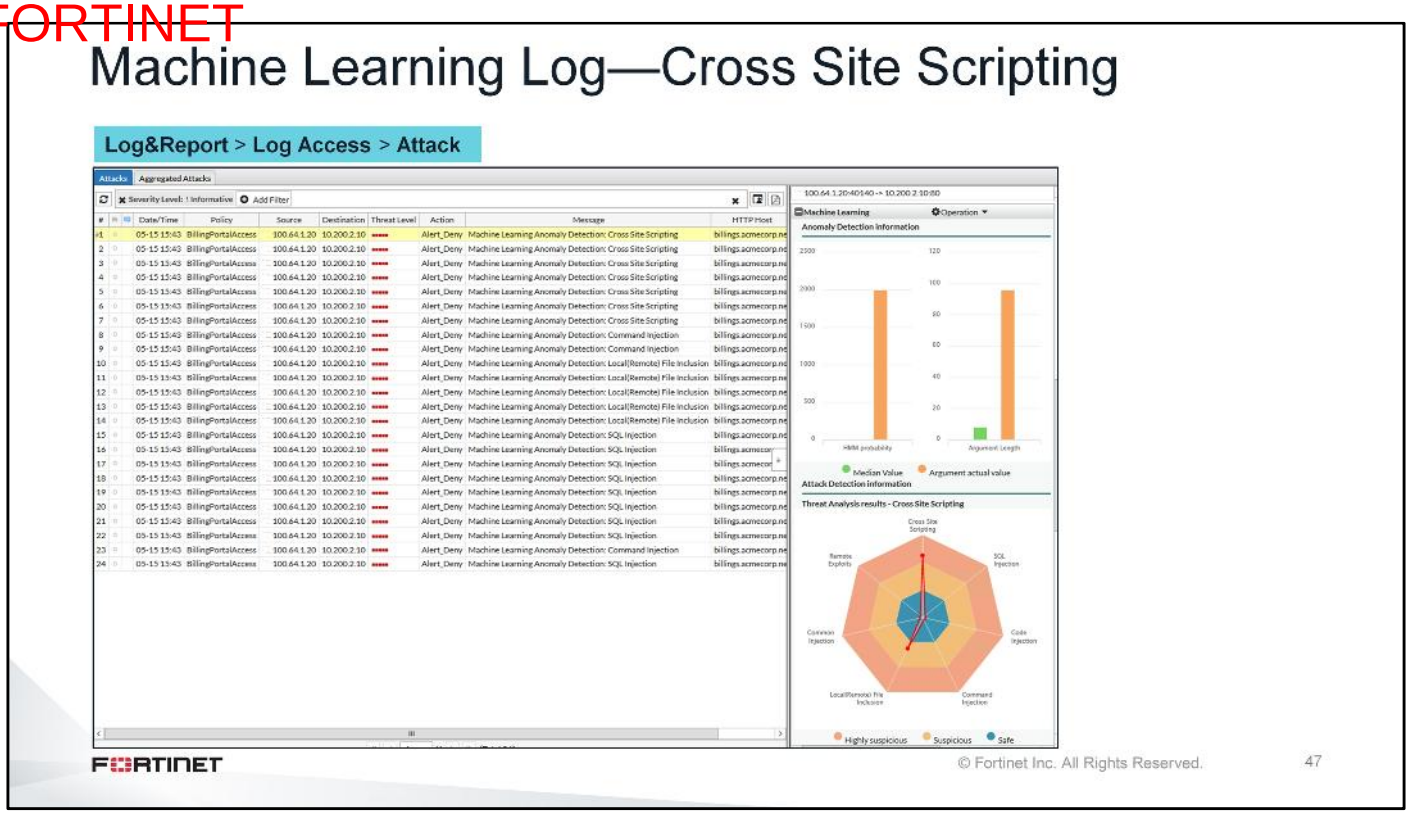
With the hold session feature enabled, FortiWeb will only generate the **Alert_Deny** log message.



This slide shows an example of a Machine Learning log. **Main Type** is **Machine Learning** and **Sub Type**, might have one of the following values:

- Anomaly in http argument
- HTTP Method violation
- Charset detect failed

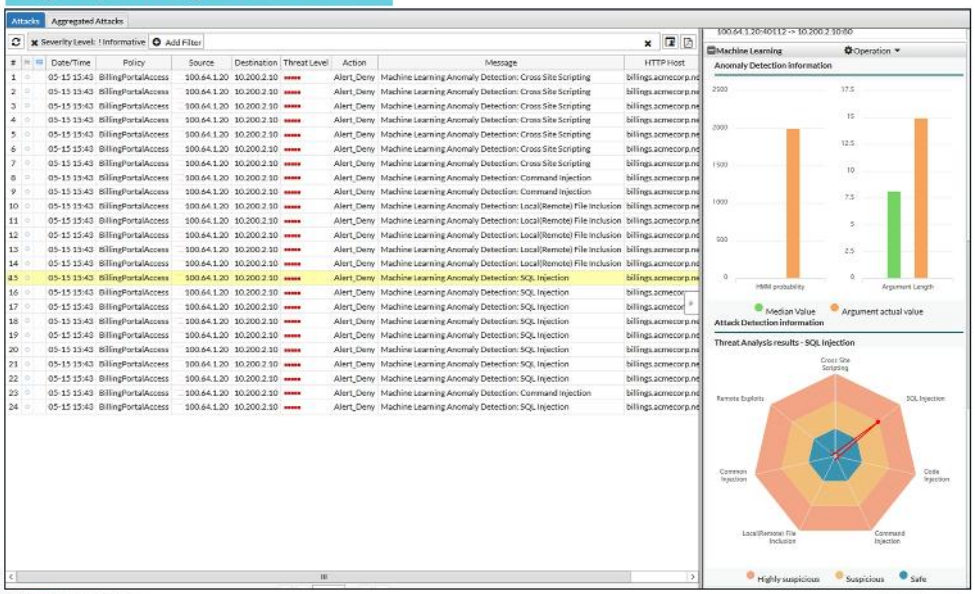
Machine Learning Log—Cross Site Scripting



Under the **Machine Learning** heading in the log details section you can see the input from the attack, in orange, being compared to both the **HMM probability** and **Argument Length** observed for the parameter, in green. Anomaly is triggered when the **Argument actual value** is significantly different from the **Median value**. The anomaly is checked against the **Threat Model** from FortiGuard and the verdict is that the anomaly is a threat that is categorized as **Cross Site Scripting**.

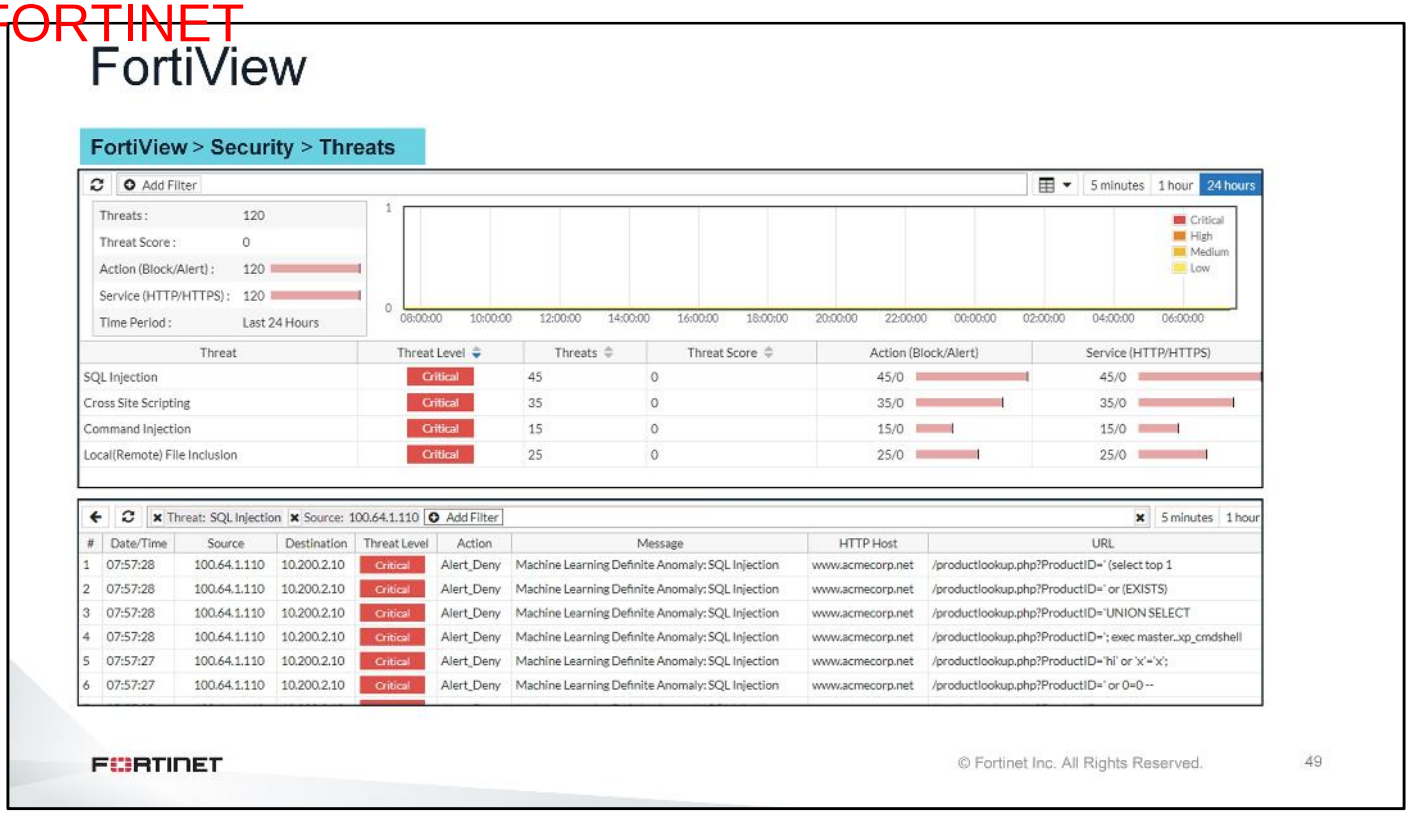
Machine Learning Log—SQL Injection

Log&Report > Log Access > Attack

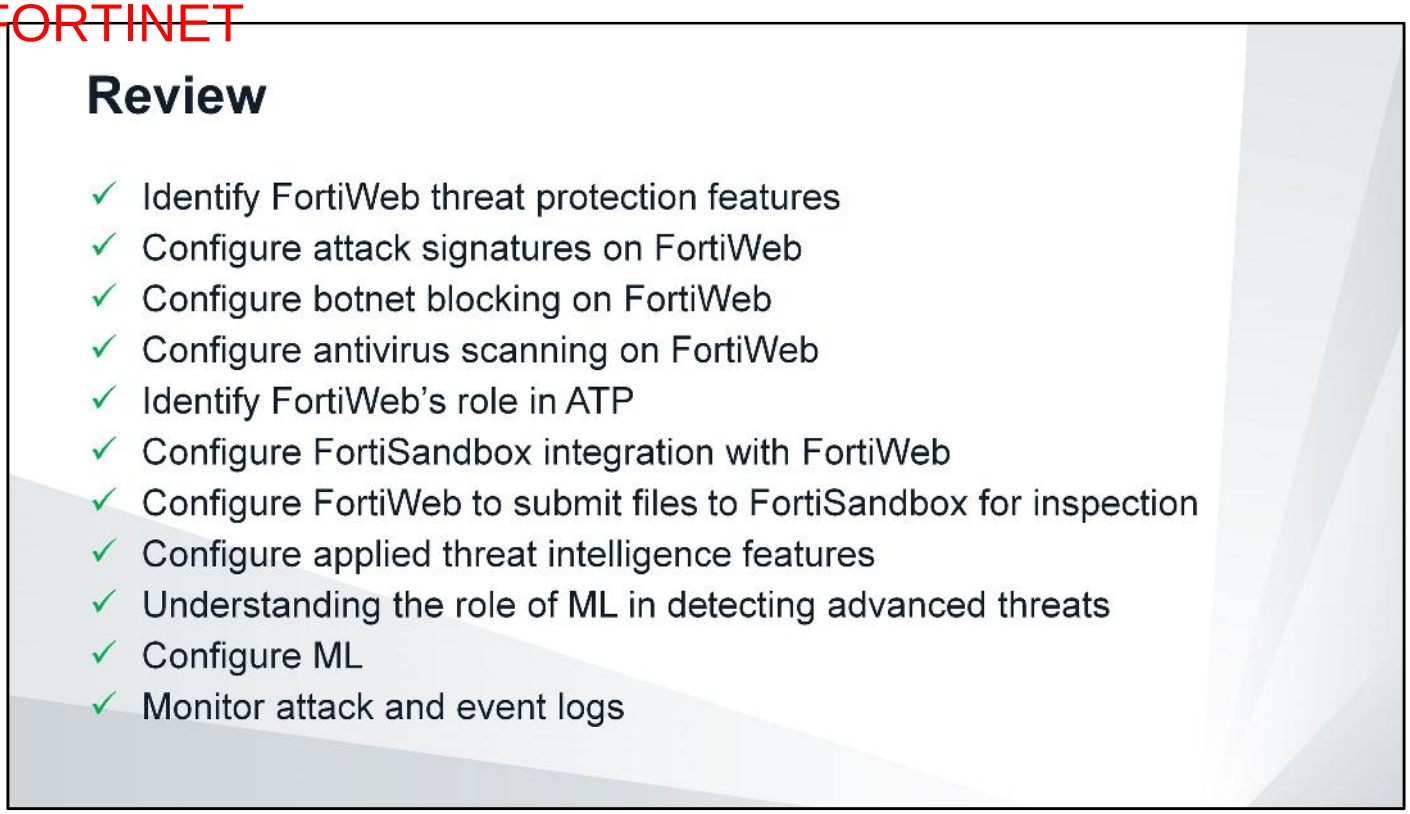


48

This is an ML attack log of a SQL injection attack. The FortiGuard threat model has determined the anomaly as a SQL injection attack.

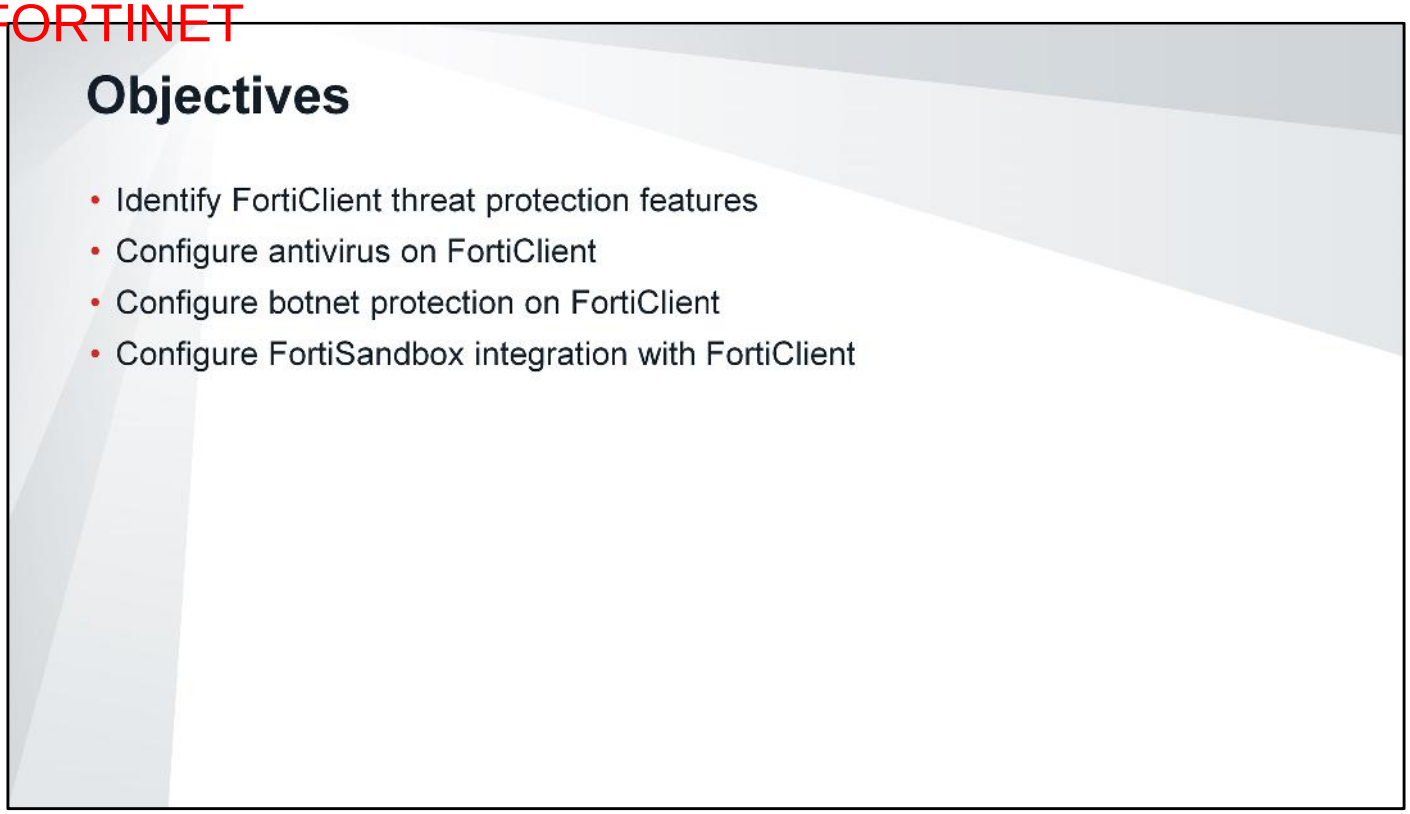


Using **FortiView**, you can visualize and easily drill down into key elements of FortiWeb, such as server or IP configurations, attack and traffic logs, attack maps, and user activity. This means you can achieve a much deeper understanding of threats to the organization's web applications.



By mastering the objectives covered in this lesson, you learned how to protect your web servers from advanced threats.

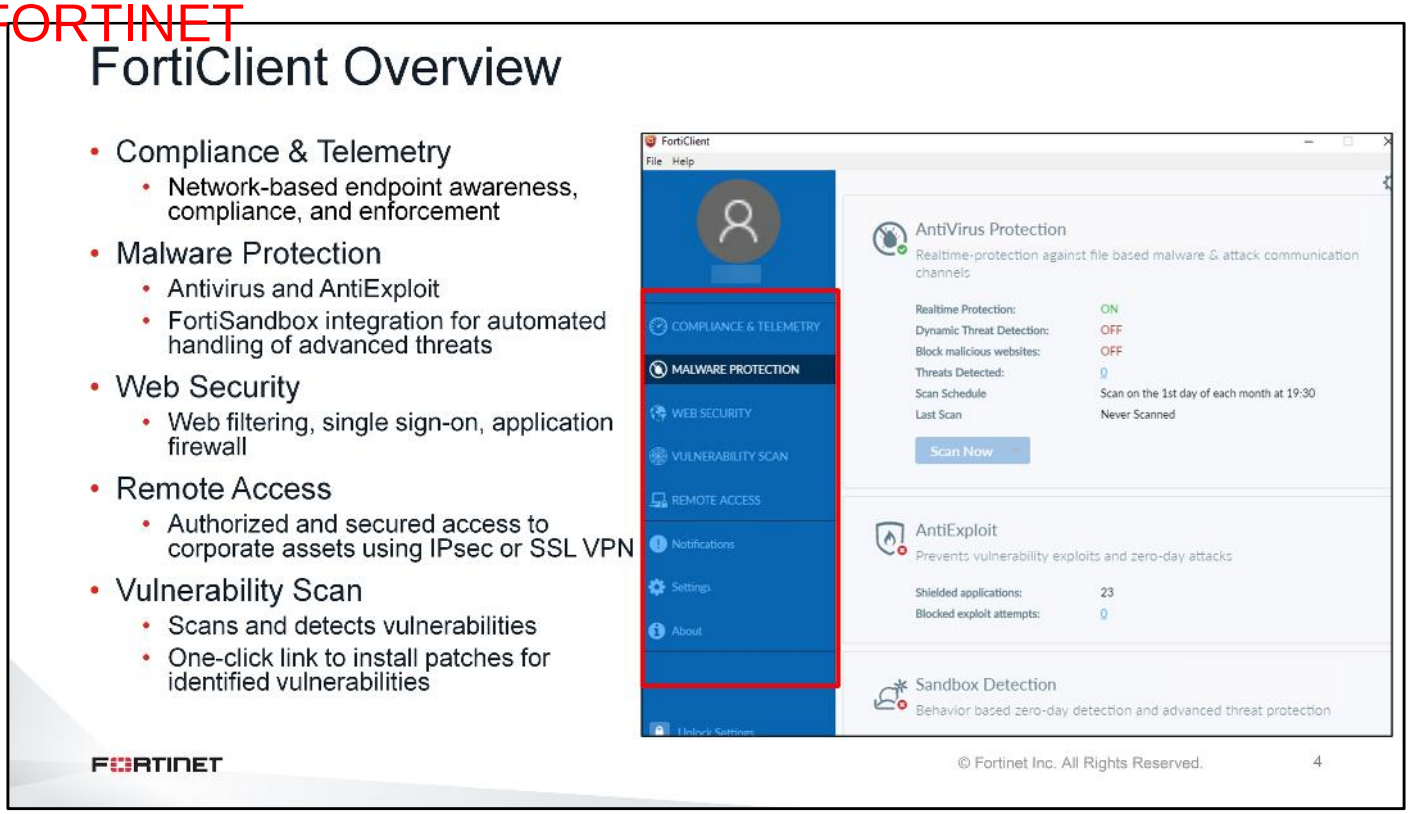
In this lesson, you will learn how to protect end users from advanced threats.



After completing this lesson, you should be able to perform the objectives shown on this slide.

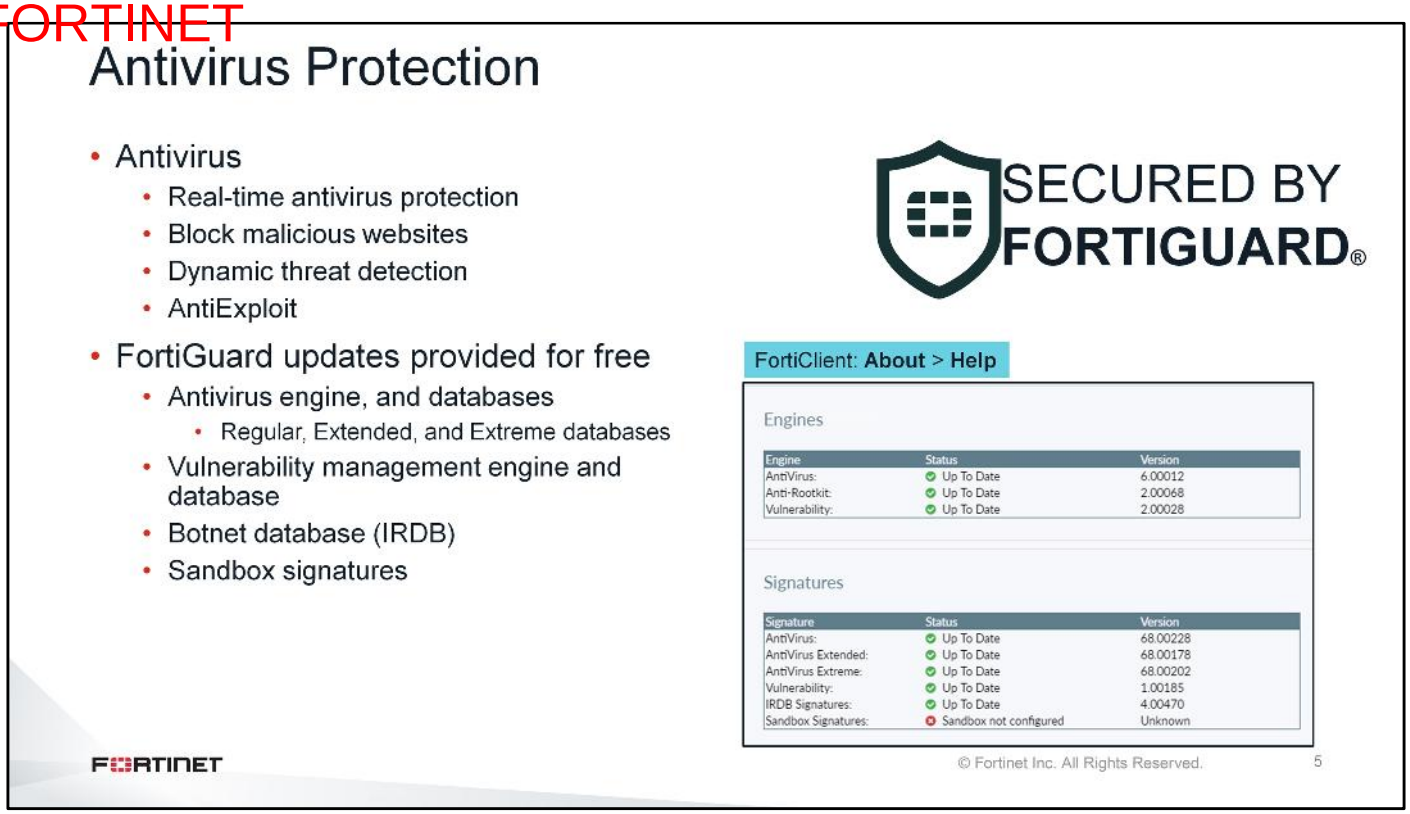
By demonstrating competence in FortiClient threat protection and advanced threat protection (ATP) integration concepts and configuration requirements, you will be able to protect end users from advanced threats.

In this section, you will learn about the threat protection features available on FortiClient and how to configure them.



FortiClient is a unified endpoint protection platform. FortiClient integrates with Fortinet's Security Fabric to provide endpoint awareness, compliance, and enforcement by sharing endpoint telemetry, regardless of device location. FortiClient automates the prevention of known and unknown threats using FortiGuard global intelligence and integration with FortiSandbox. FortiClient also provides secure remote access to corporate assets using VPN with native two-factor authentication and single sign-on. FortiClient is supported on many devices (PC, Mac, Linux, Chromebook, Apple, and Android).

FortiClient includes a vulnerability scan component to check endpoints for known vulnerabilities. The vulnerability scan results will include a list of vulnerabilities detected, which are rated as critical, high, medium, or low threats. You have the option to install patches and resolve as many identified vulnerabilities as possible using the one-click link.

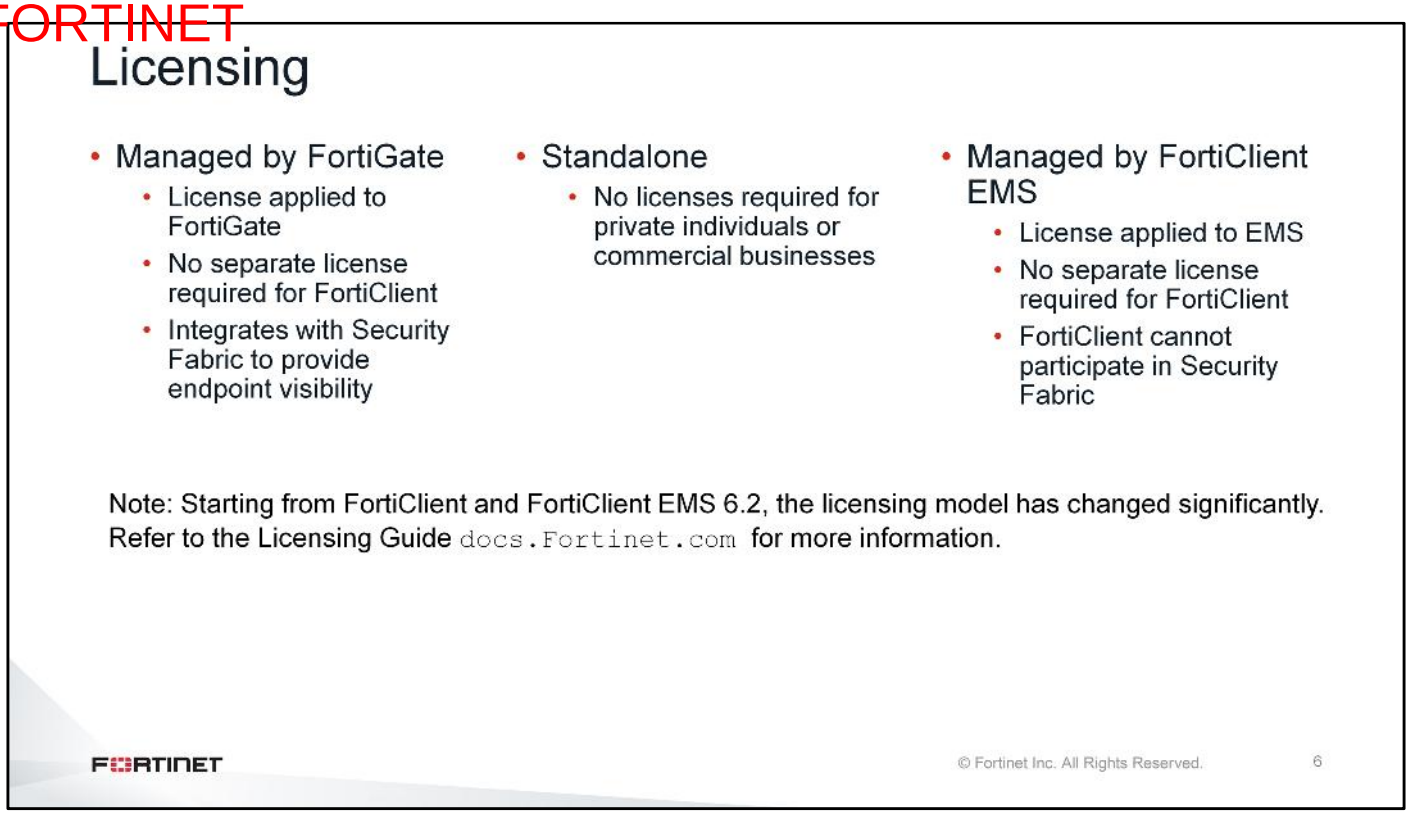


FortiClient antivirus has multiple mechanisms to block advanced threats at multiple stages of the kill chain.

When a user attempts to execute a file that is known malware, FortiClient real-time antivirus protection can block the file. If a user attempts to execute malware that uses a known command and control (C&C) infrastructure, but is polymorphic in nature, FortiClient will block the C&C requests using botnet protection. Similarly, if the malware tries to check a known malicious domain for further instructions, FortiClient will block its communication channels using web filter. FortiClient can also block known drive-by download sites using the web filter.

FortiClient can proactively prevent known exploits by scanning popular applications and operating systems for vulnerabilities. Once detected, FortiClient can recommend patches to address the vulnerabilities.

The antivirus engine and databases, vulnerability management engine and database, and the botnet database are all updated by FortiGuard, free of charge.

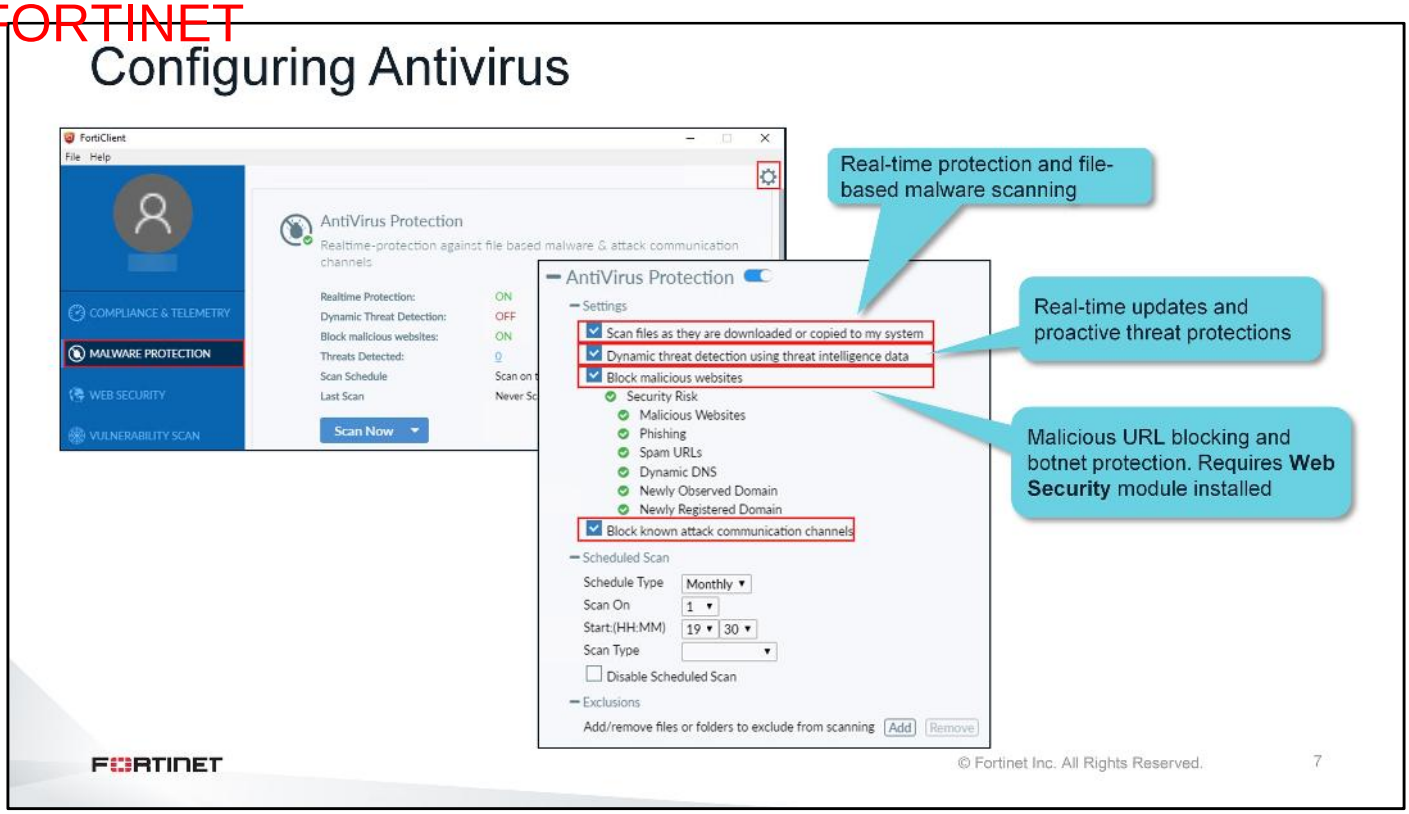


All deployments of FortiClient receive FortiGuard updates free of charge. There is no license requirement for these updates. However, licensing becomes a factor when dealing with large *managed* deployments.

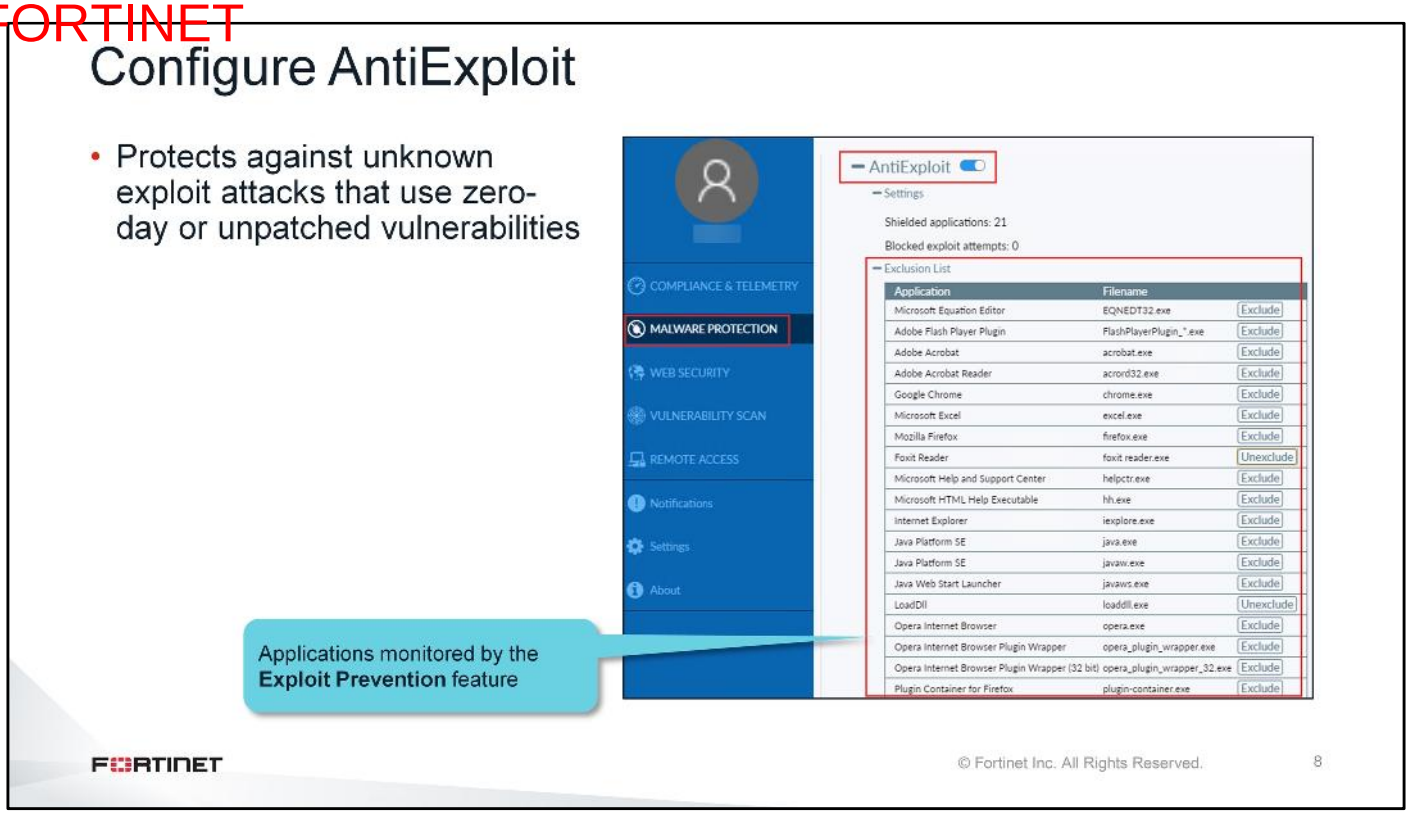
Standalone FortiClient installations don't require any licenses. This is true for both private individuals and commercial businesses. The downside of this deployment type is that there are no central management options; each FortiClient installation needs to be managed individually.

If you're deploying FortiClient with the FortiClient Enterprise Management Server (EMS), you will need to apply the license to FortiClient EMS. Each purchased license allows the management of one FortiClient endpoint. When you manage FortiClient endpoints using a standalone FortiClient EMS, there is no Security Fabric participation. You can deploy a hybrid topology where FortiClient EMS provides FortiClient endpoint provisioning services, while FortiGate provides compliance rules.

You also have the option to manage FortiClient endpoints using FortiGate. There are 10 free licenses available. When managed by FortiGate, you can configure Security Fabric integration for endpoint-level visibility.



You can access all of the FortiClient antivirus features by clicking the settings icon on the **Malware Protection** tab. Real-time protection and file-based malware scanning are standalone features. However, to block malicious sites, and known C&C communication channels, you must install the **Web Security** module.

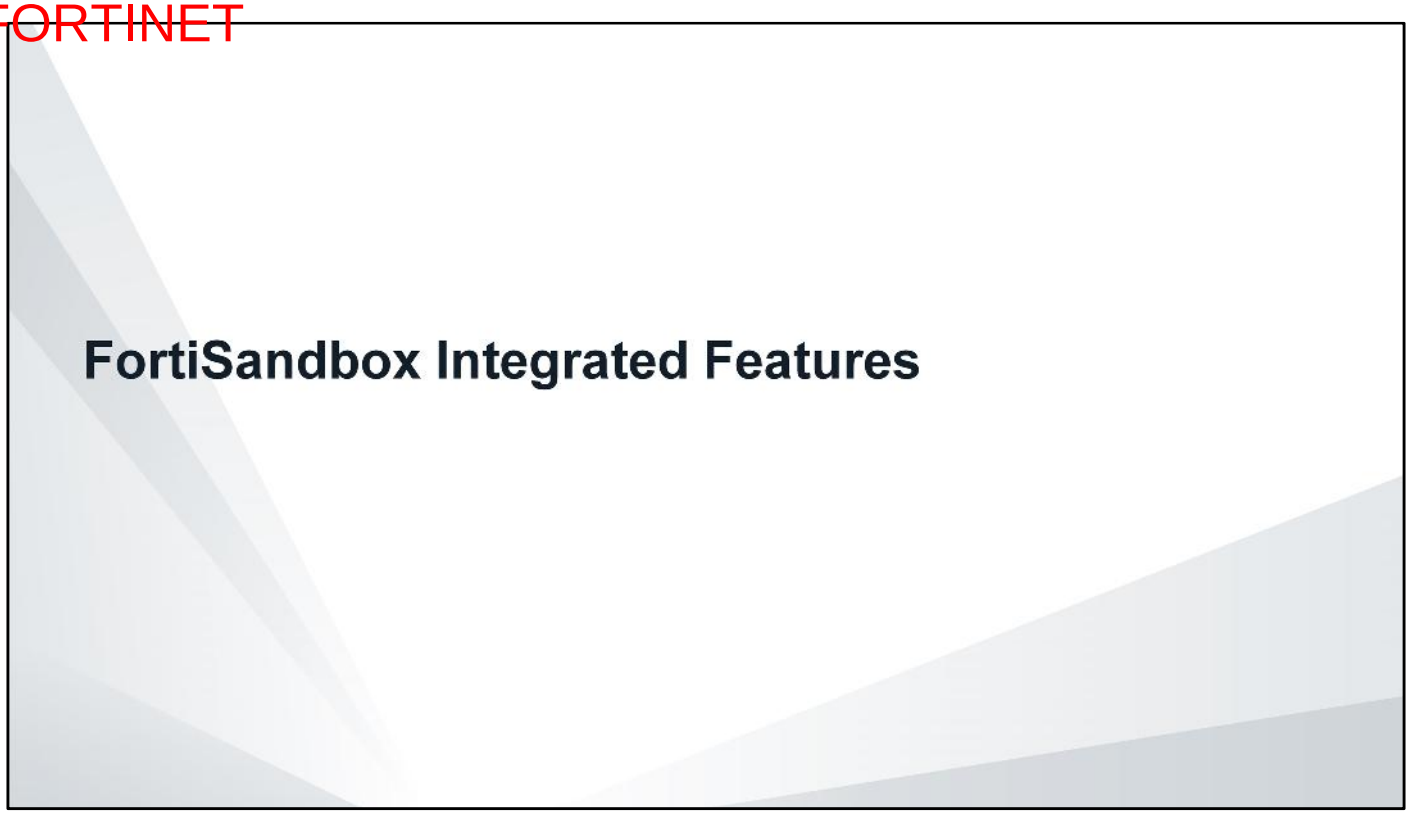


The anti-exploit detection feature also helps protect against memory-based attacks and drive-by download attacks. It also detects and blocks unknown and known exploit kits. It is a solution that does not require any signatures.

You can identify which applications are protected from exploits based on the buttons beside their names.

Applications with an **Exclude** button beside their names are protected from evasive exploits.

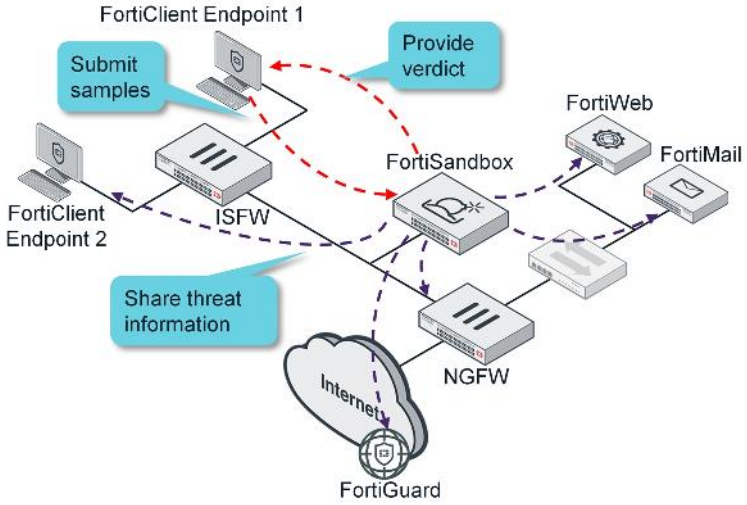
Applications with an **Unexclude** button beside their names are not protected from evasive exploits. You can protect the application by clicking the **Unexclude** button.



In this section, you will learn how to integrate FortiClient with FortiSandbox.

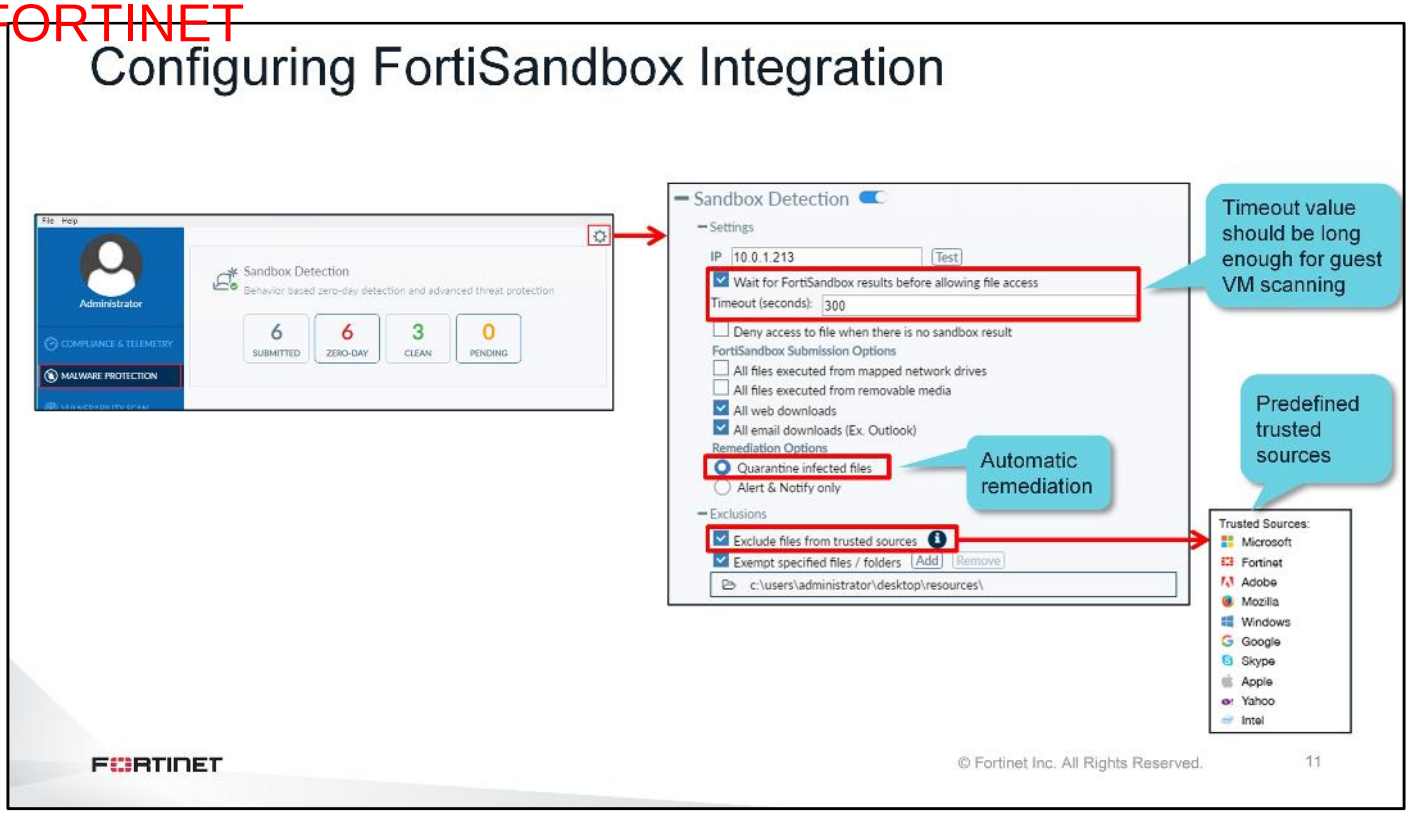
FortiSandbox Integration

- FortiClient's role
  - Submit files to FortiSandbox
  - Block access to file during analysis
  - Quarantine or release file based on verdict
- FortiSandbox's role:
  - Inspect submitted files
  - Generate a verdict
  - Share threat information
- No patient zero
  - FortiClient blocks access to files while it is being scanned
  - Malicious objects are never exposed to the end user

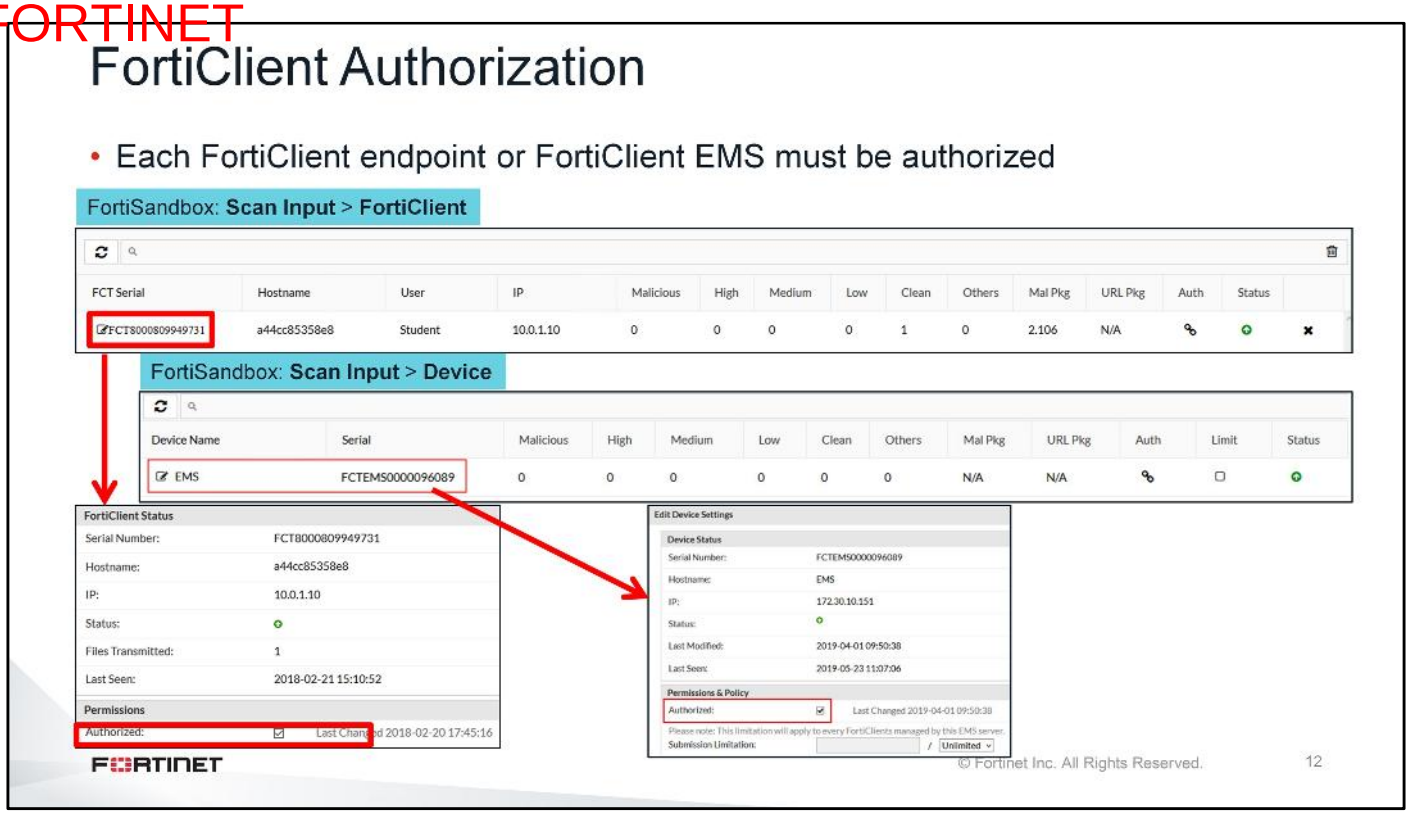


If a user attempts to execute a file that bypasses the threat protection features you've learned about so far, the file is automatically sent to FortiSandbox for file hash inspection and deeper analysis. While the file is being scanned, FortiClient blocks access to the file, so malicious objects are never exposed to the end user. Based on the verdict, FortiClient can quarantine or release the file.

If the verdict is suspicious, FortiSandbox generates a dynamic signature and distributes it to other endpoints and devices, which completely locks down the threat and prevents it from propagating. This threat intelligence is also shared with FortiGuard.

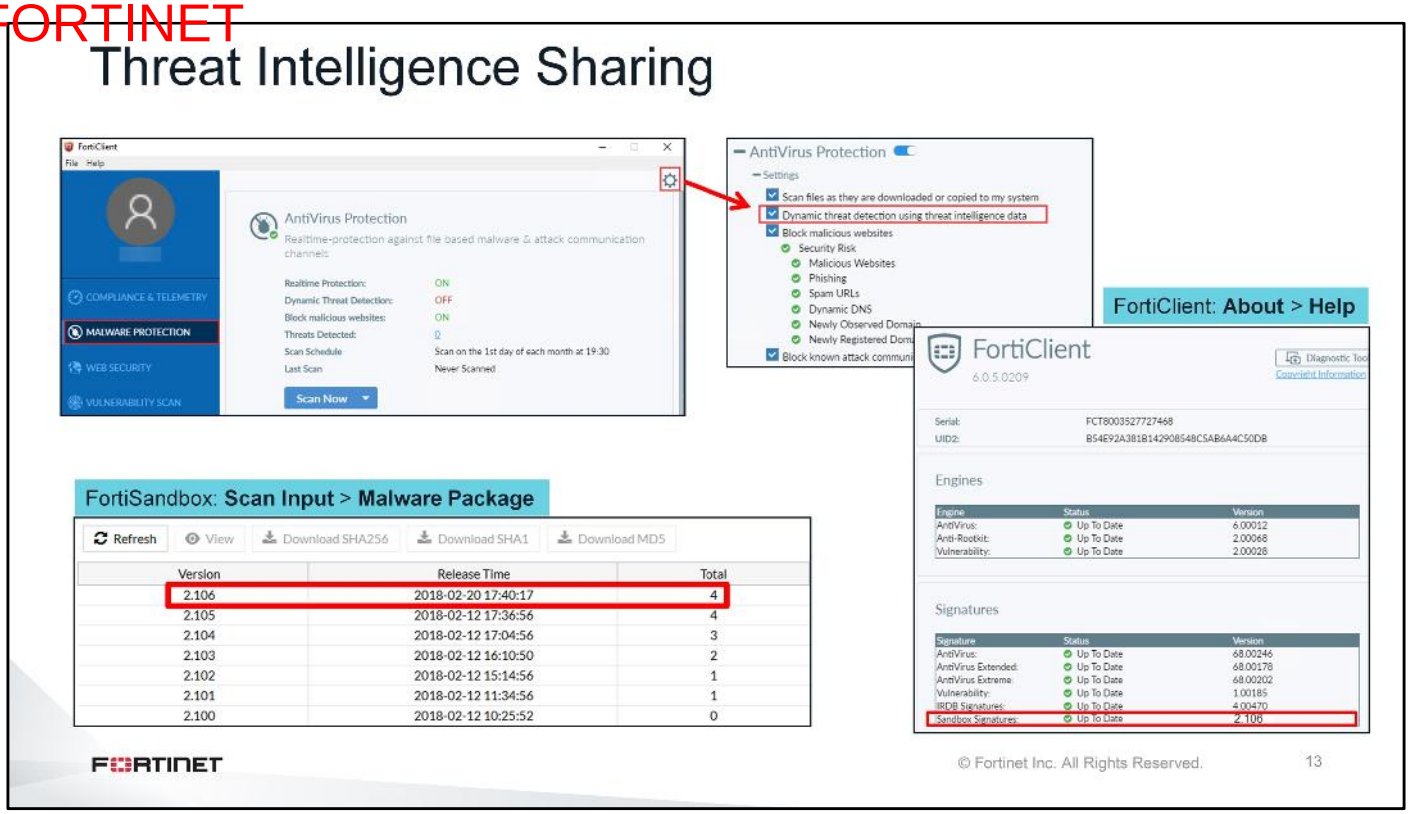


You can configure a timeout value to define how long FortiClient will wait for FortiSandbox to generate a verdict. The timeout value should be long enough for VM scanning to complete. You can configure FortiClient to monitor web and email downloads. You can also configure automatic remediation. FortiClient will automatically quarantine files that generate malicious or suspicious ratings.



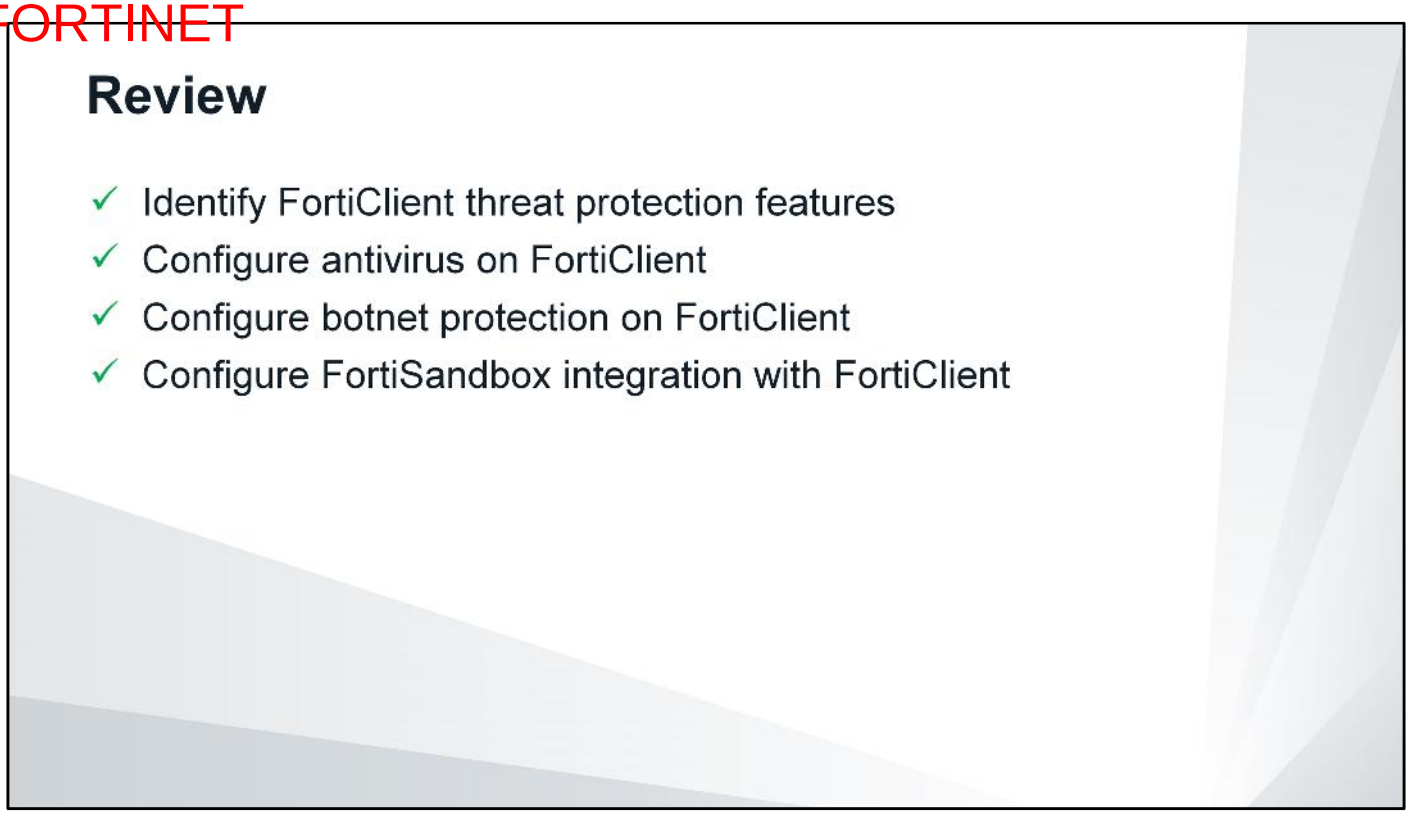
After configuring the FortiClient endpoint, you must authorize it on FortiSandbox. After authorization, each FortiClient endpoint is listed as a separate input device on FortiSandbox.

If you are using FortiClient EMS, then only EMS needs to be authorized. FortiClient will be authorized automatically.



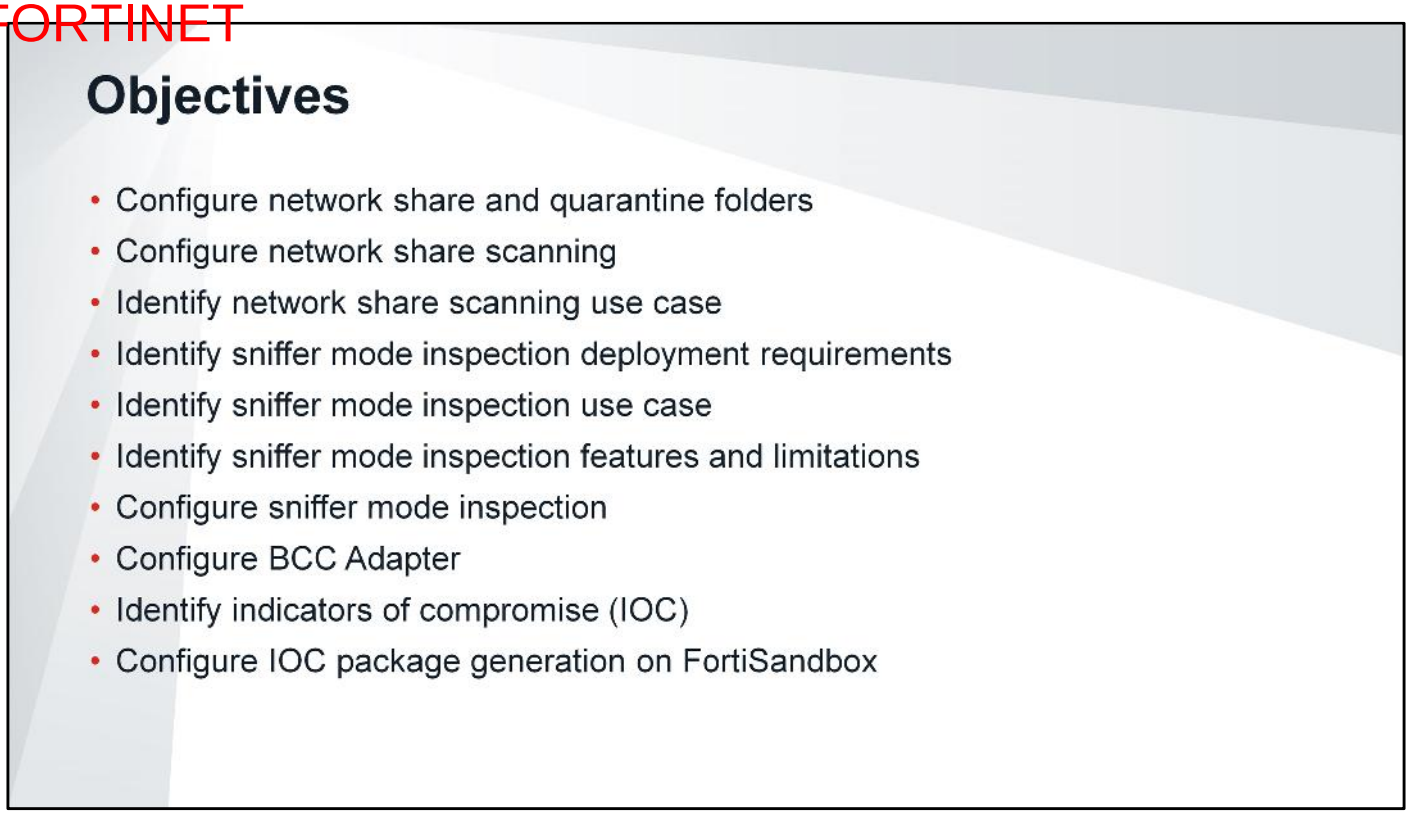
You should configure FortiClient to use the FortiSandbox malware packages. To have FortiClient start using the FortiSandbox malware packages, you must enable **Dynamic threat detection using threat intelligence data**.

FortiClient does not use the FortiSandbox URL package.



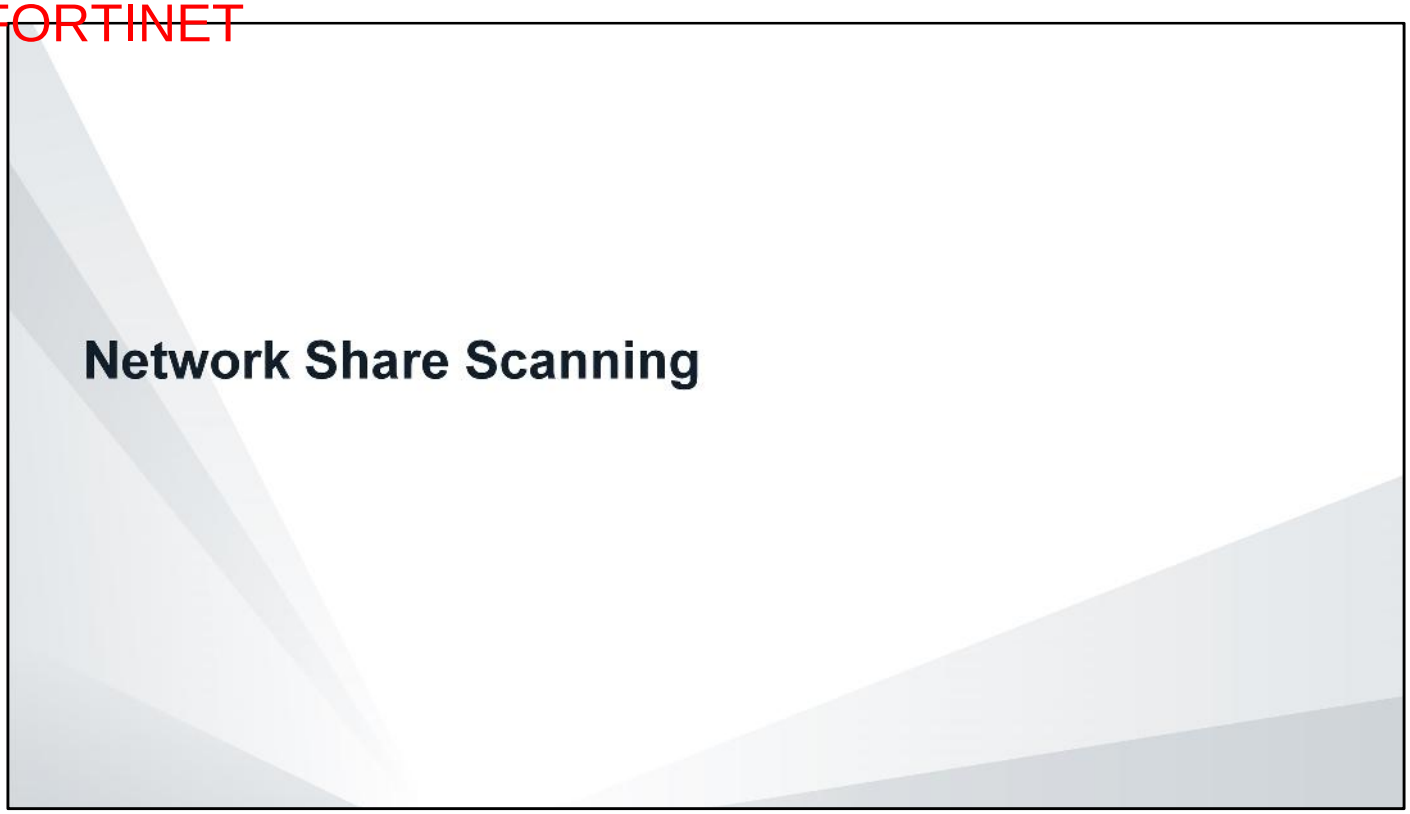
By mastering the objectives covered in this lesson, you learned how to protect end users from advanced threats.

In this lesson, you will learn about the options available options on FortiSandbox to protect third-party appliances.



After completing this lesson, you should be able to perform the objectives shown on this slide.

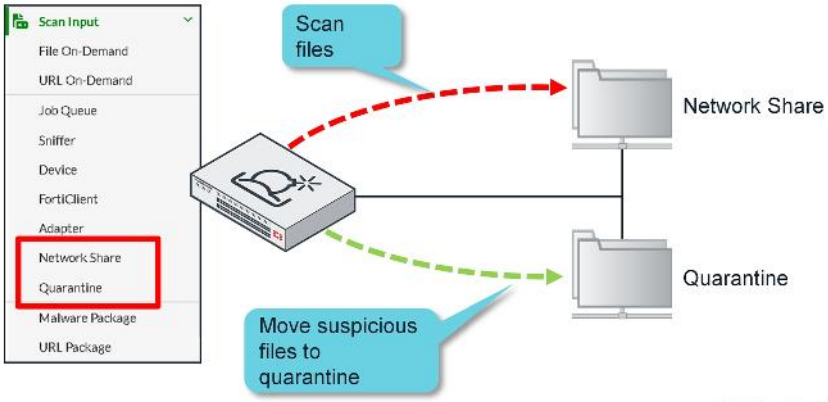
By demonstrating competence in network share scanning and sniffer mode integration concepts and configuration requirements, you will be able to deploy FortiSandbox to protect a network with third-party security appliances.



In this section, you'll learn about the network share scanning feature on FortiSandbox and how to configure it.

Network Share and Quarantine

- Network share
  - FortiSandbox connects to network share and scans files
- Quarantine
  - FortiSandbox connects to quarantine to store suspicious files found while scanning a network share

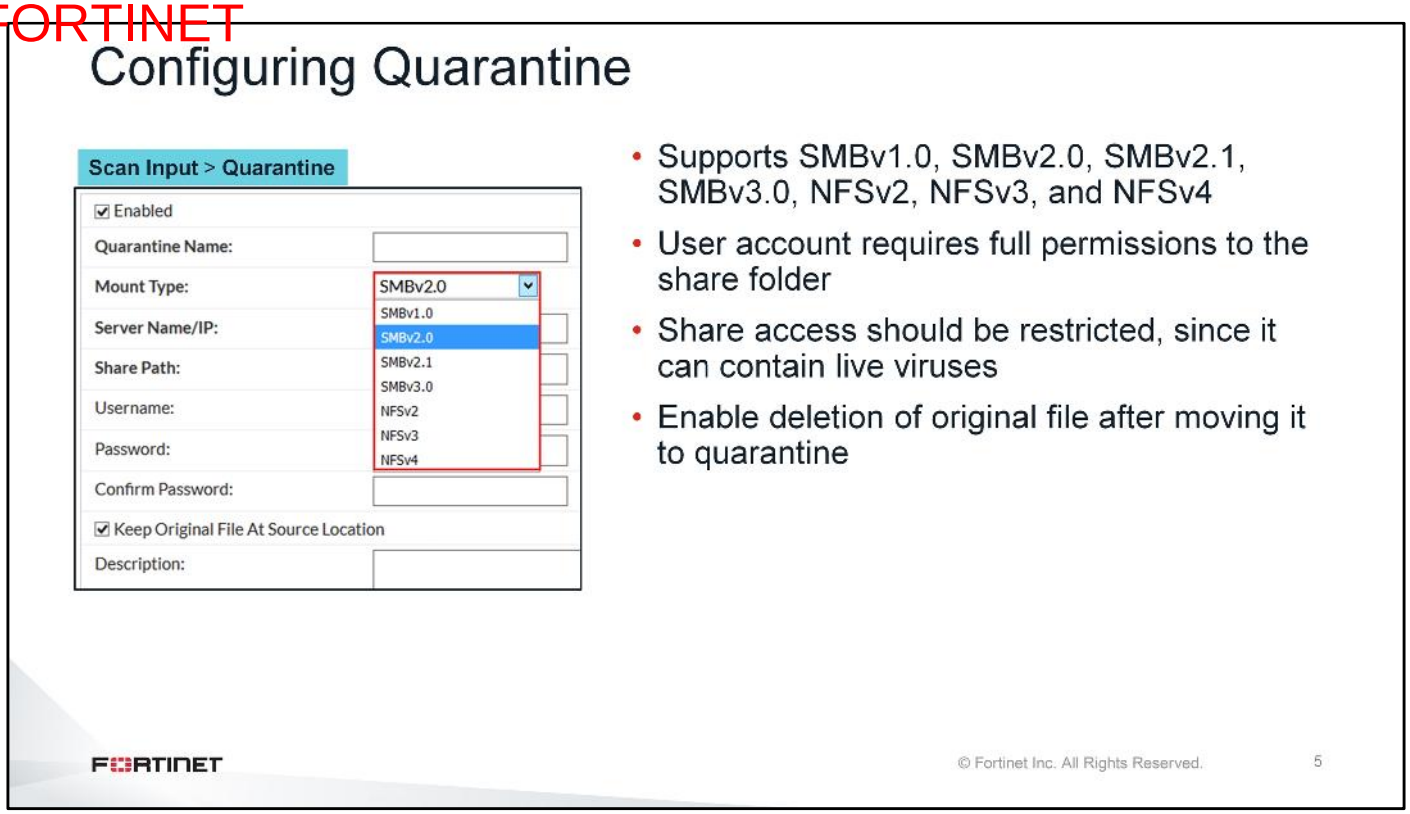


4

On FortiSandbox, a network share and quarantine are both network file shares. The difference is how FortiSandbox uses them.

A network share is used as a file repository that FortiSandbox connects to, to scan files. Any files found to be malicious or suspicious can be moved to a quarantine folder, which is a separate network share folder.

You also have the option to configure a second quarantine location, which FortiSandbox can use to store clean files.

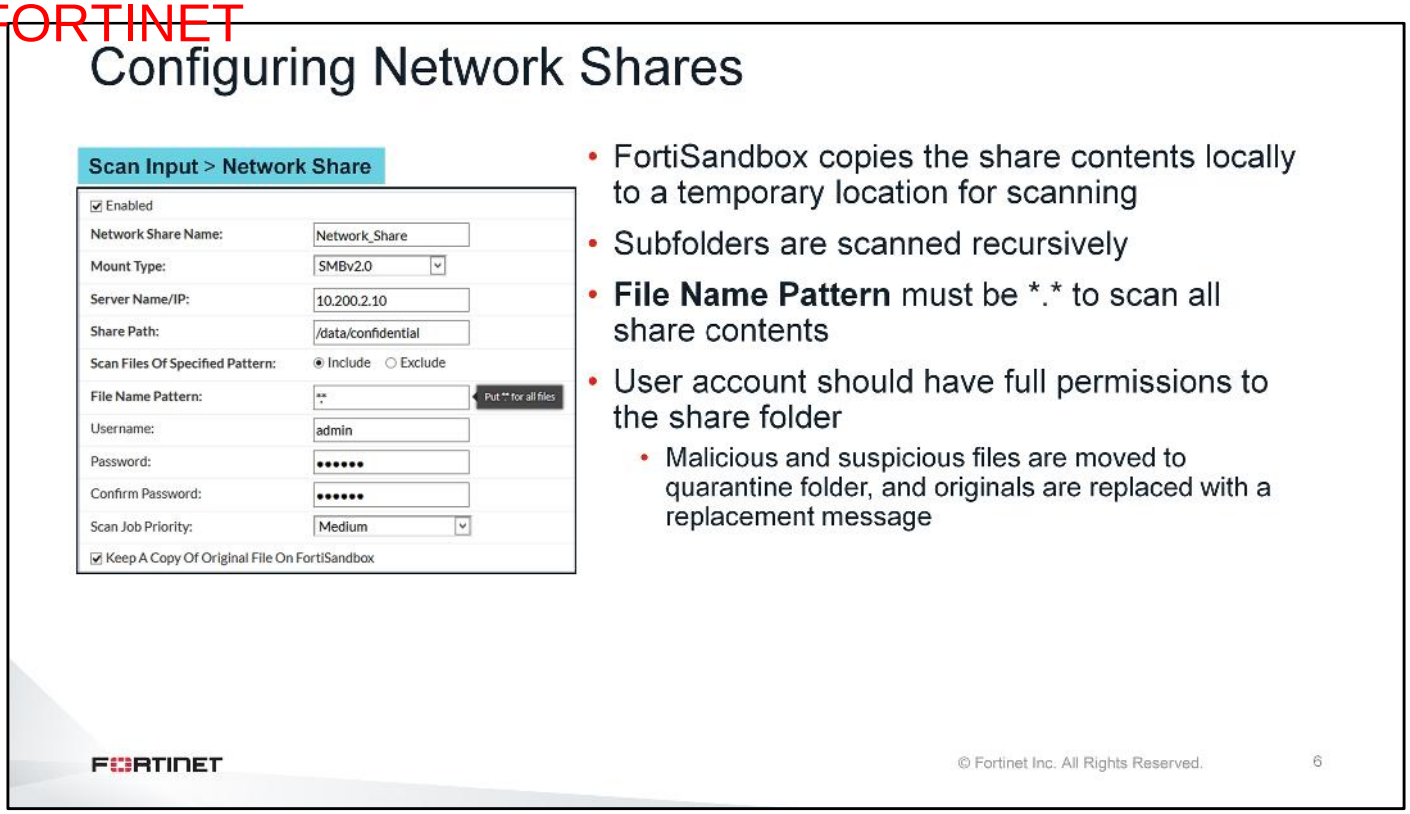


FortiSandbox supports SMBv1.0, SMBv2.0, SMBv2.1, SMBv3.0, NFSv2, NFSv3, and NFSv4 file shares.

You must configure the server location, the share path, a username, and password to the quarantine. The user must have full permissions within the quarantine folder, in order to successfully move the files that are considered suspicious.

Since suspicious files can potentially contain live viruses, you should ensure that the quarantine folder is not accessible to everyone. To prevent further damage, regular users should be not be allowed to access the quarantine folder.

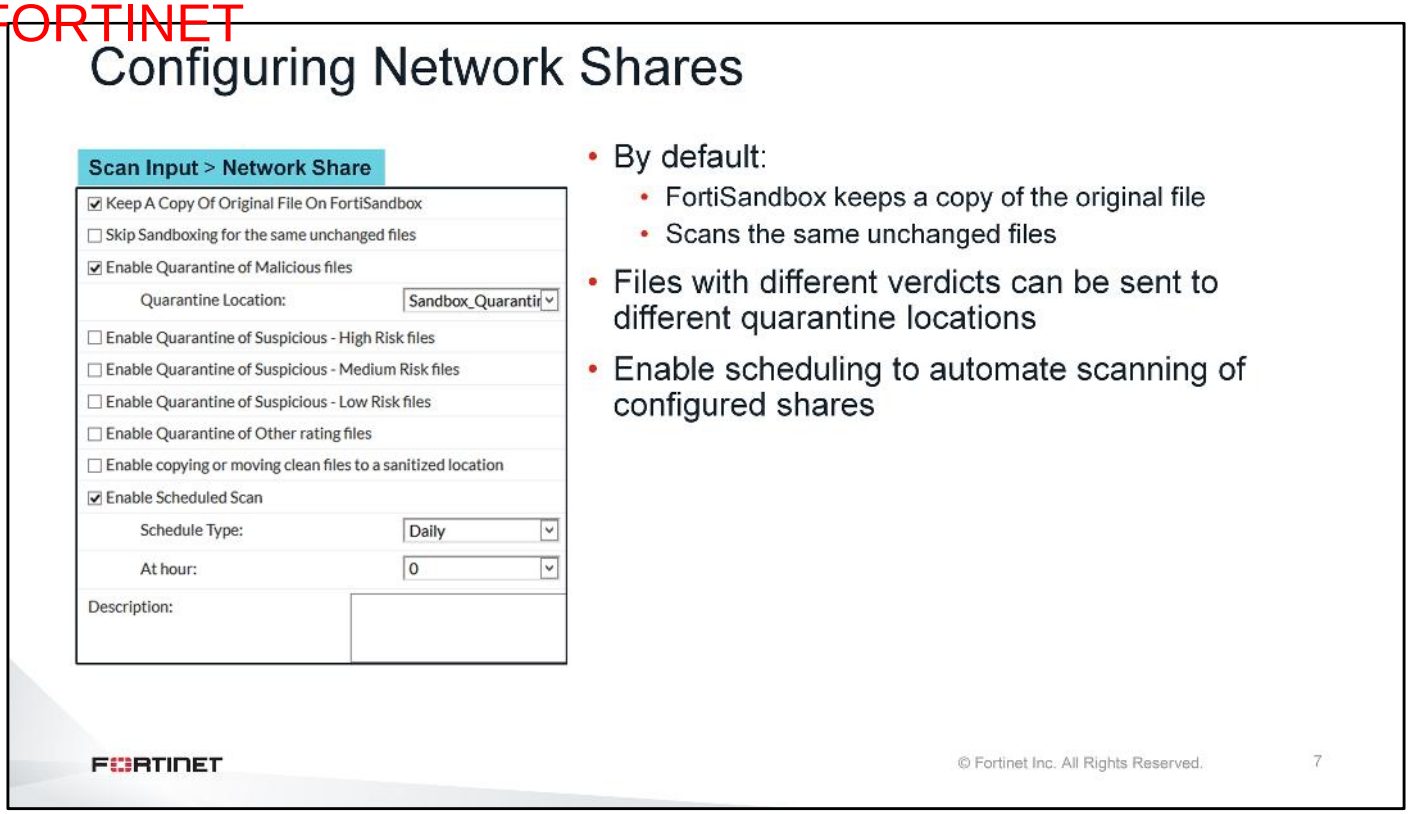
When a file is moved, to leave a copy in its original location, you can select the **Keep Original File At Source Location** checkbox.



The options available for configuring a network share are almost identical to configuring a quarantine, because they are both network shares. You can configure FortiSandbox to scan all files in the network share using a wildcard pattern—`*.*`.

The user account should have full permissions to the share folder, to be able to move malicious and suspicious files to the quarantine folder.

The original file is replaced with a replacement message.



In addition to the connection information, there are some other settings that you can configure for network shares.

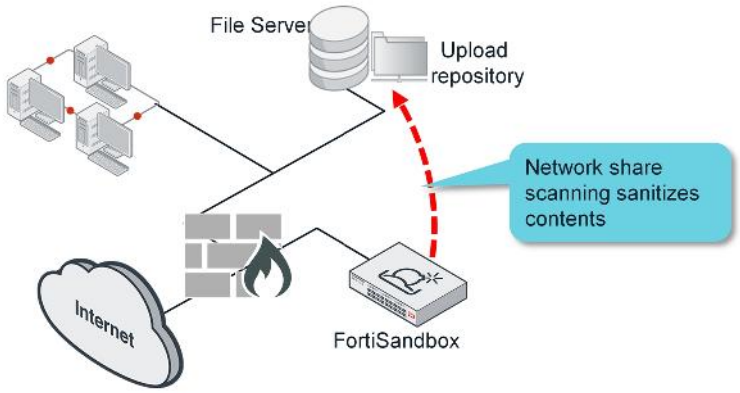
FortiSandbox keeps a copy of the original file, by default. This is convenient, because it allows you to easily to locate the infected file for further analysis, when required. By default, FortiSandbox scans any unchanged files. Scanning the same unchanged file is a waste of resources. So, you should enable **Skip Sandboxing for the same unchanged files**.

You also have the option to send files with different verdicts to different quarantine locations. This can be useful to separate the known malicious files from the suspicious files.

You can also enable scheduling, to automate the share scanning process. This enables an automatic, scheduled scan of the network share. If you do not configure scheduling, a scan will occur only if you initiate it manually.

Network Share Scanning Use Case

- Cover additional attack surface that may otherwise go unprotected
- Configure the upload directory as a file share, and use FortiSandbox to sanitize contents
- Malicious or suspicious files can be moved to a quarantine location

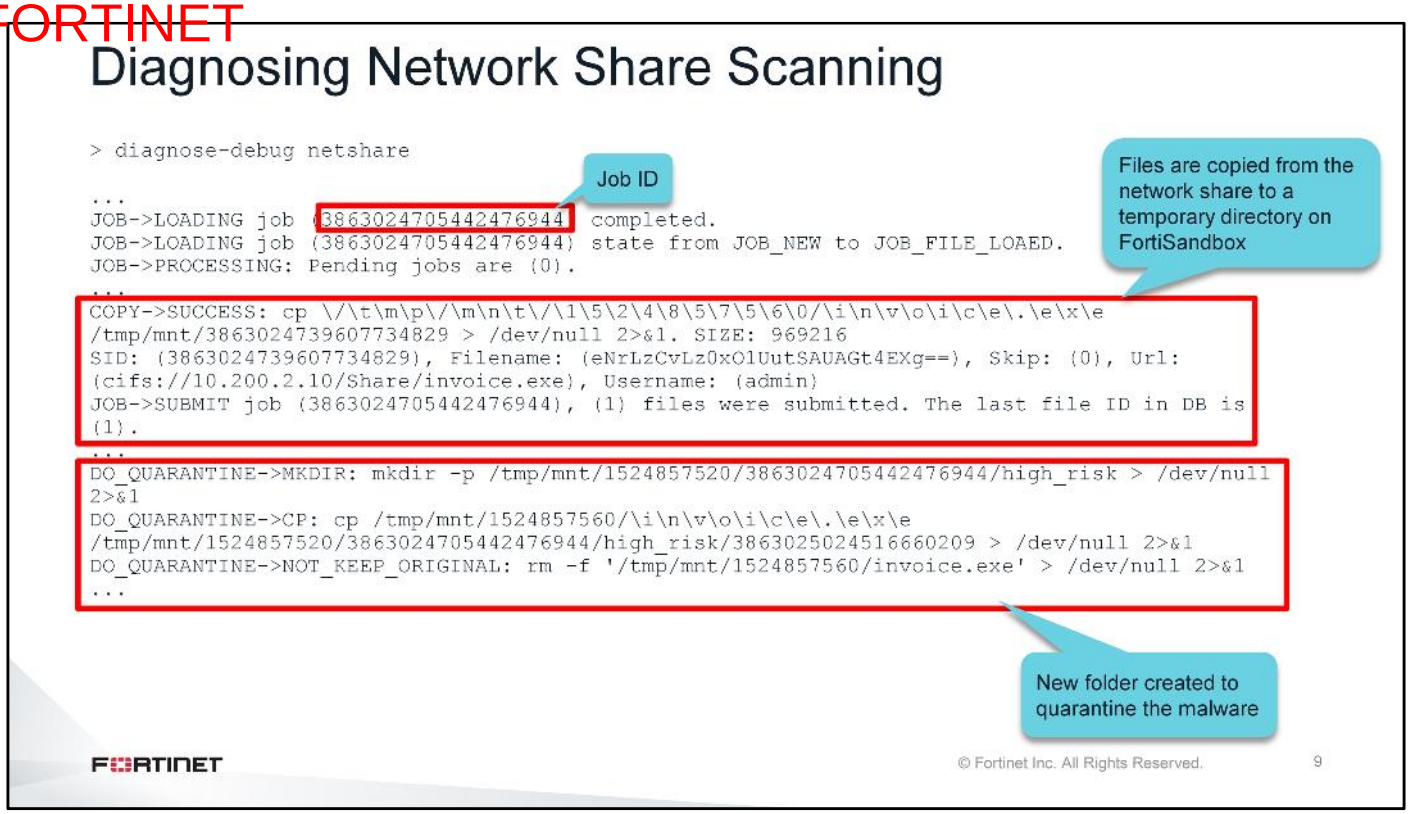


8

You've learned that FortiGate and FortiClient can be used together to address patient-zero infections. FortiMail has built-in queueing of emails, so malicious objects are never exposed to end users. FortiWeb can hold sessions while FortiSandox is scanning files. How can you address third-party devices lack of automatic remediation?

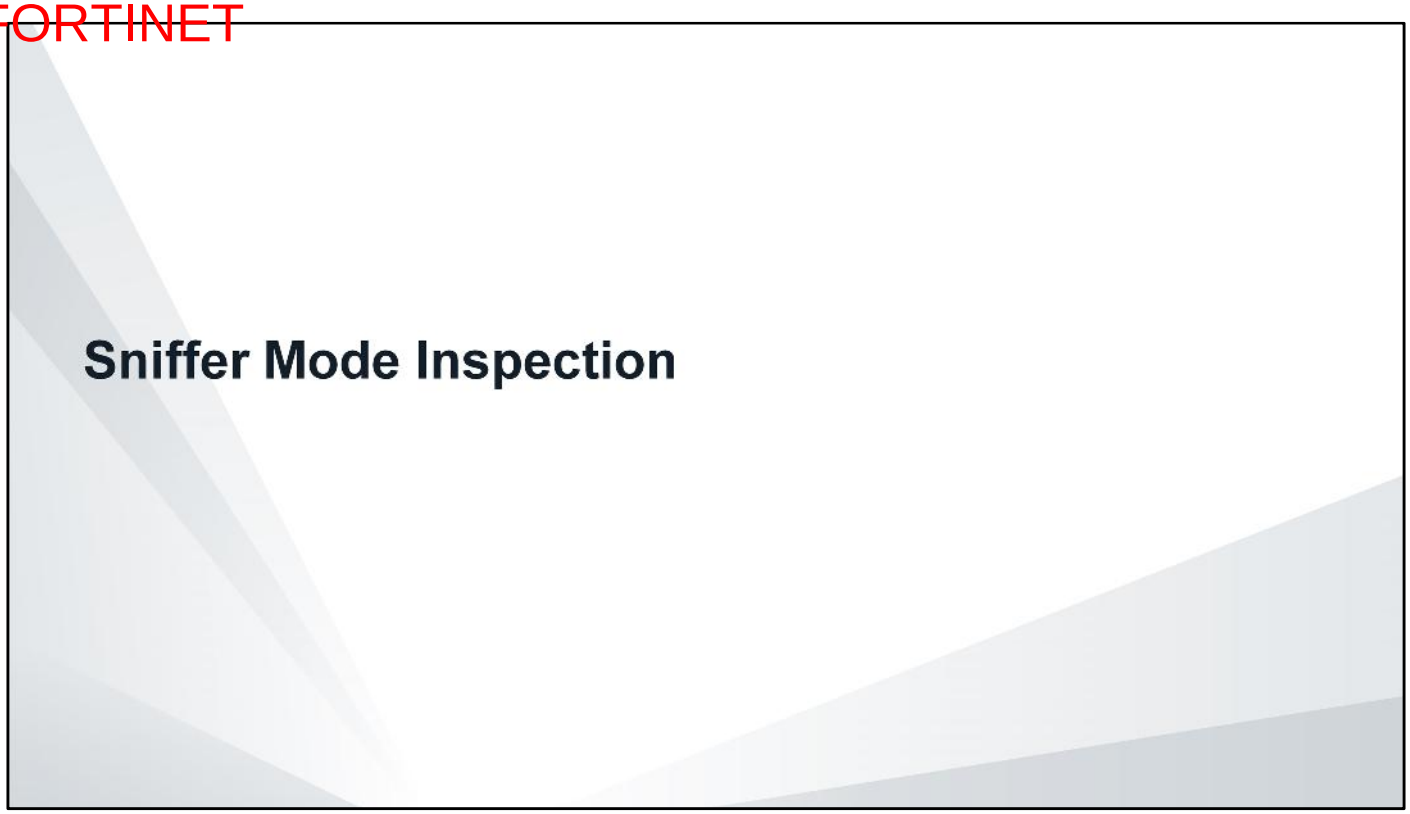
You can configure any upload repository as a file share, and use FortiSandbox's network share scanning feature to sanitize the contents. You can configure the share scanning to run on a schedule. Any malicious or suspicious files will be moved to a separate quarantine location. You can also have the clean files move to a different file share, or to a different file server entirely.

Third-party appliances can save files to a network share. As long as the file share is accessible by FortiSandbox, it can be scanned and sanitized.



You can use the command shown on this slide to view the real-time debug messages related to network share scanning on FortiSandbox.

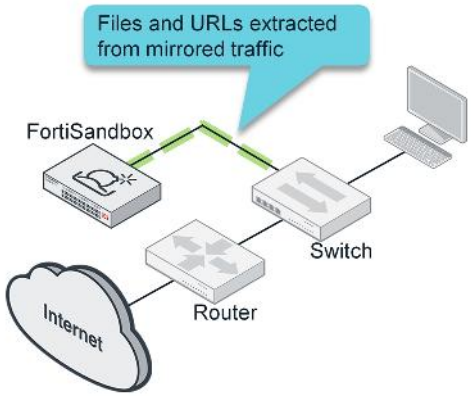
As you can see in the debug output shown on this slide, FortiSandbox copies the files from the network share to a local temporary directory for scanning. Because this file generated a high risk verdict, FortiSandbox creates a new quarantine folder using the job ID as the folder name, and moves the malware to it.



In this section, you will learn about the sniffer mode inspection feature on FortiSandbox and how to configure it.

Sniffer Mode Inspection

- Requires input from spanned switch ports or a TAP device
  - Can use promiscuous mode for virtual infrastructures
- Suited for infrastructure with third-party security appliances
- Traffic must be decrypted before being sent to FortiSandbox
- Supports file and URL inspection
- Supports network alert detection
  - Suspicious URLs (FortiGuard Web Filter)
  - Botnet callback (FortiGuard Web Filter)
  - Intrusion attacks (FortiGuard IPS)



FORTINET

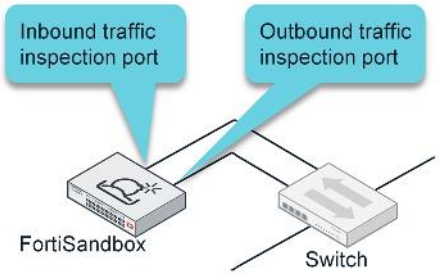
11

Sniffer mode allows you to configure interfaces on FortiSandbox to inspect traffic from third-party devices. In order to do this, a copy of the traffic needs to be sent to FortiSandbox using spanned switch ports, a TAP device, or a promiscuous mode interface in virtual infrastructures. Traffic *must* be decrypted before being sent to FortiSandbox.

FortiSandbox supports file and URL inspection when using sniffer mode inspection. FortiSandbox also supports detection of suspicious URLs and botnet connections using the FortiGuard Web Filter service, and the detection of intrusion attacks using the FortiGuard IPS service.

What Traffic Should be Inspected?

- Inspect traffic closest to the perimeter firewall
- Inspect both inbound and outbound traffic
  - Inbound traffic for malware and intrusion detection
  - Outbound traffic for botnet IP and malicious URL requests
- Recommendation: Use separate ports for inspection, based on traffic direction



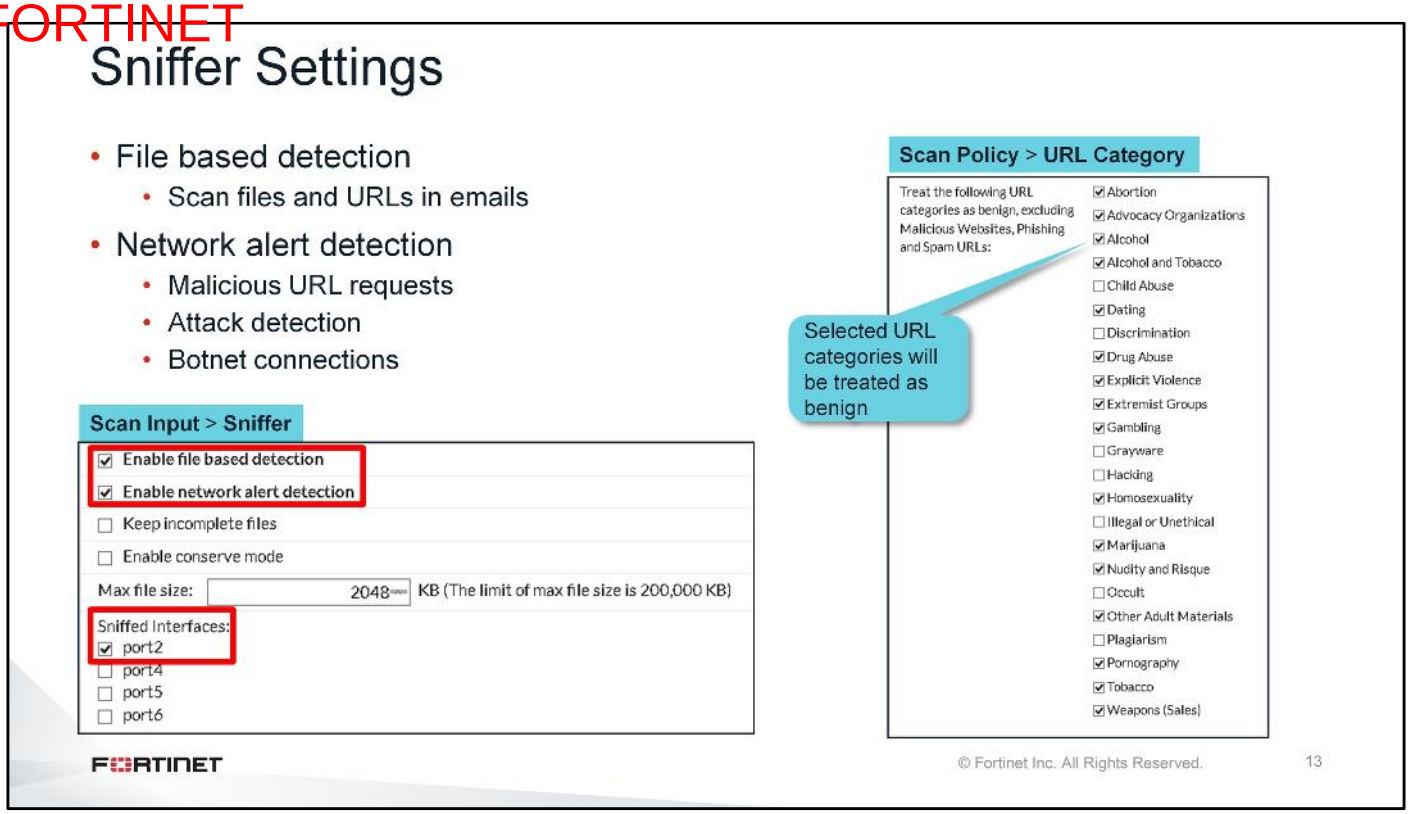
FORTINET

12

Traffic that exists outside the boundaries of your network is not your responsibility. Only traffic that comes in to your organization's network should be considered for inspection.

Generally, the best place to inspect traffic is inside your organization's network, and as close to your perimeter firewall as possible. The closer the traffic is to the border of your network, the better. This will limit the number of paths (ports) you'll have to mirror to the FortiSandbox.

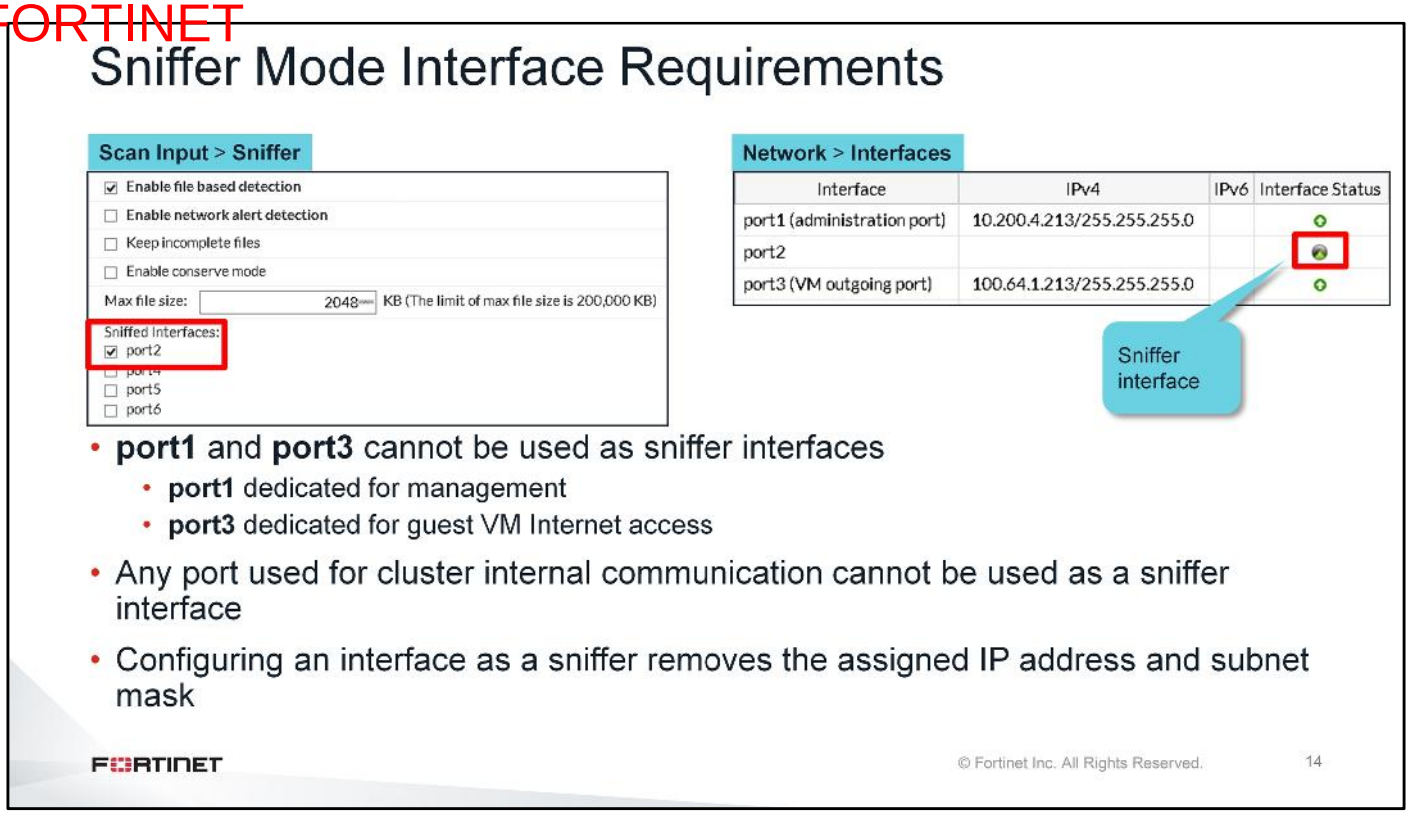
For highest threat detection coverage, you should inspect both inbound and outbound traffic. Inbound traffic should be inspected to detect malware and intrusion attacks. Outbound traffic should be inspected to detect requests for botnet IP and malicious URLs. For performance reasons, it is recommended that you use separate ports for inspection, based on traffic direction.



You must enable file-based detection to start scanning for files, and URLs in emails. You can also enable network alert detection to inspect the mirrored, live traffic for malicious URL requests, network attack attempts, and botnet connection requests.

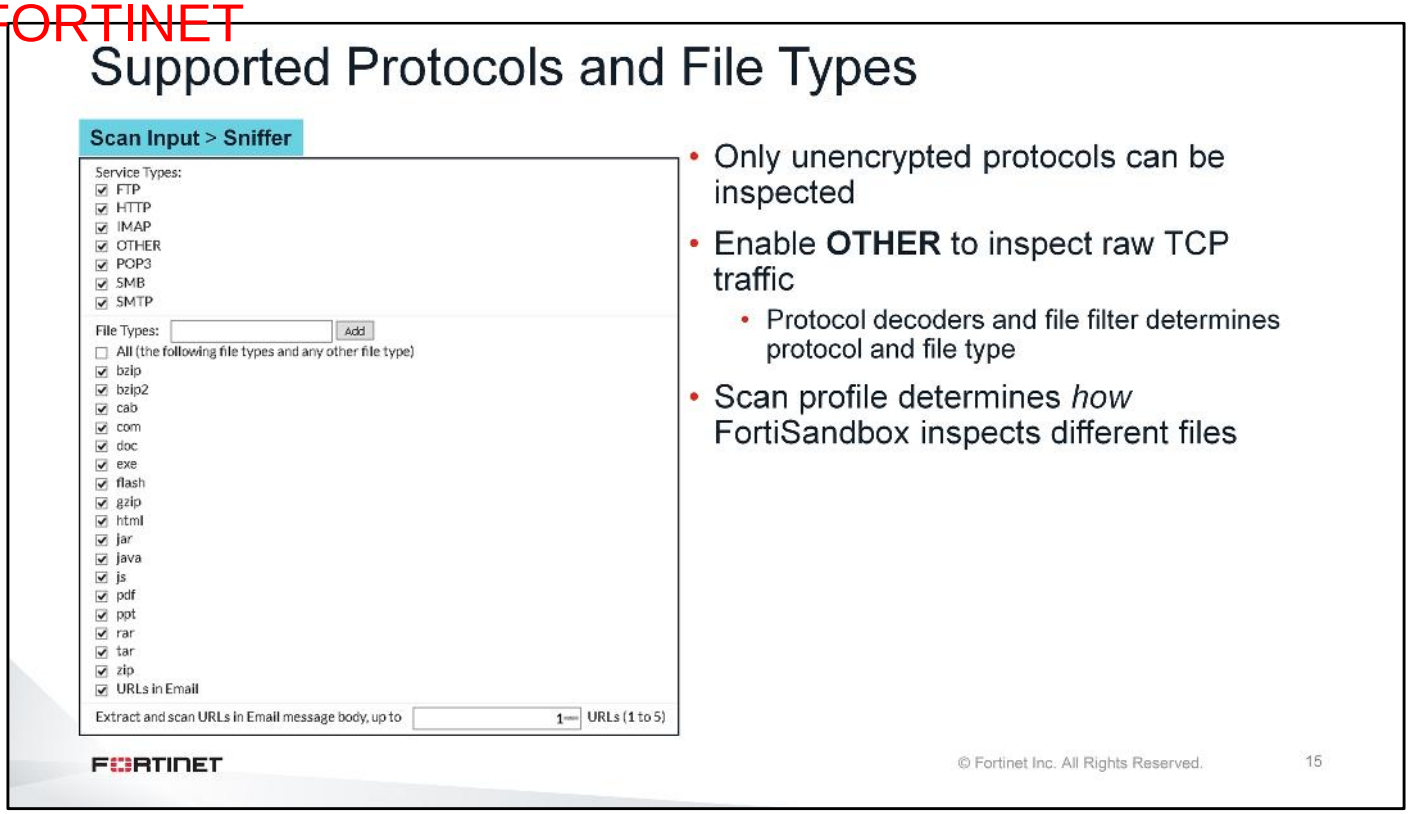
Certain URL categories will always be treated as benign, and will not be scanned by the VM engine. To mark URL categories as safe, you can configure the URL category as shown on this slide.

You must also select an interface that will be used as the sniffer.



Both **port1** and **port3** cannot be used as sniffer interfaces. Those interfaces are dedicated for management and guest VM Internet access, respectively. Any port used for cluster internal communication cannot be used as a sniffer interface either.

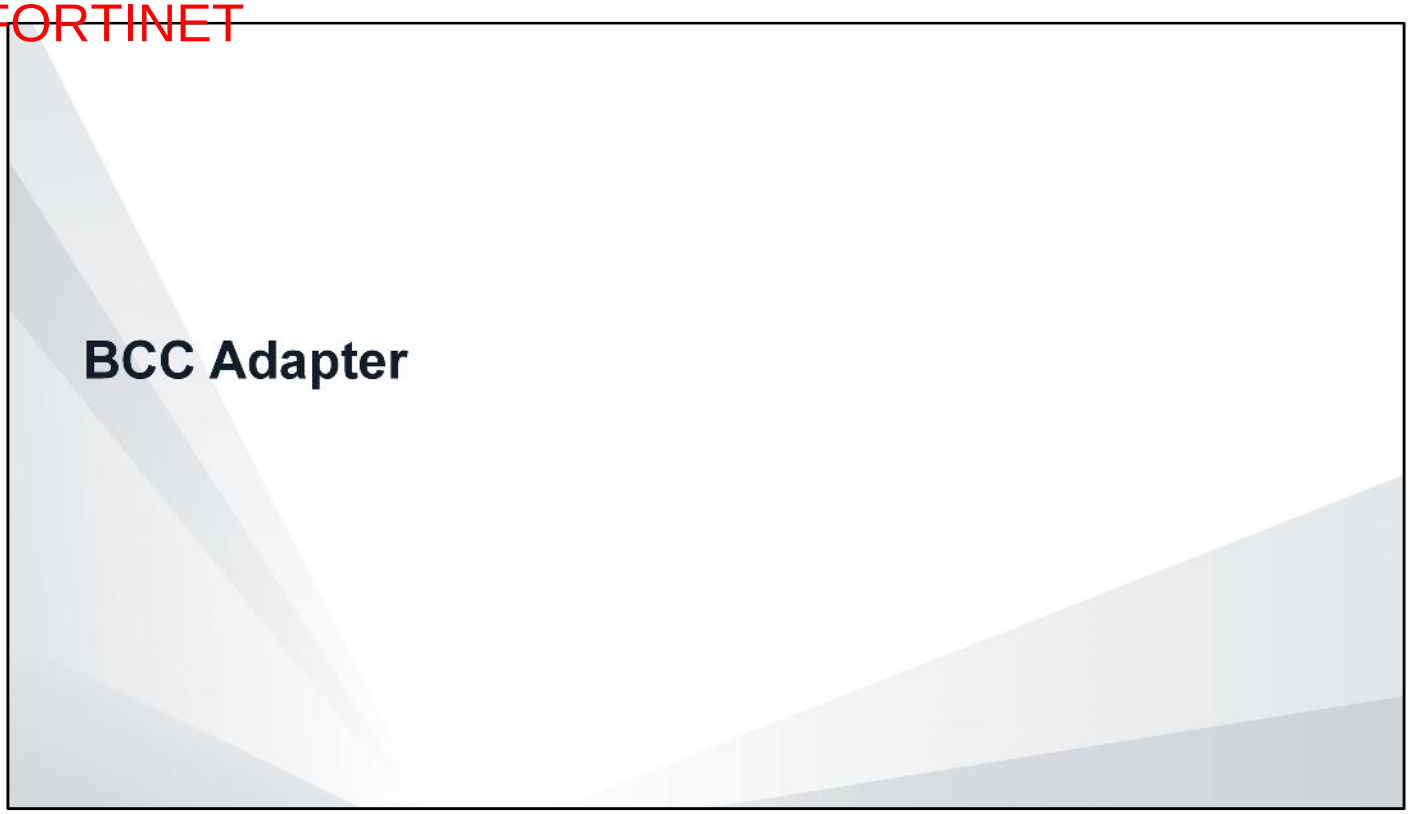
Configuring an interface as a sniffer removes the assigned IP address and subnet mask.



When you enable sniffer mode inspection, all protocols and file types are also enabled, by default. You may want to disable protocols that your organization's network does not use. For example, POP3 or IMAP. You can enable the **OTHER** category to scan for raw TCP traffic.

If you configure URL extraction, URLs embedded inside email body will be extracted and scanned using VM scanning. You can define the maximum number of URLs to extract for each email, from one to five.

Sniffer mode inspection only changes the input method of files and URLs. It does not affect *how* FortiSandbox inspects different files and URLs. The scan profile should be configured to ensure files are being inspected properly and, if required, sandboxed in the correct VM image.



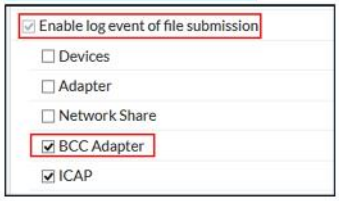
In this section, you will learn about BCC Adapter and how third-party secure email gateways can forward emails to FortiSandbox for scanning.

BCC Adapter

- Receive forwarded emails from upstream MTA server
- Extract attachment files and URLs in email body and send them to job queue
- Enable **Parse URL** to allow FortiSandbox extracts the first three URLs in the email
- Threat remediation may be manual or automated through API
- Enable log event for **BCC Adapter**

Scan Input > Adapter

Scan Policy > General

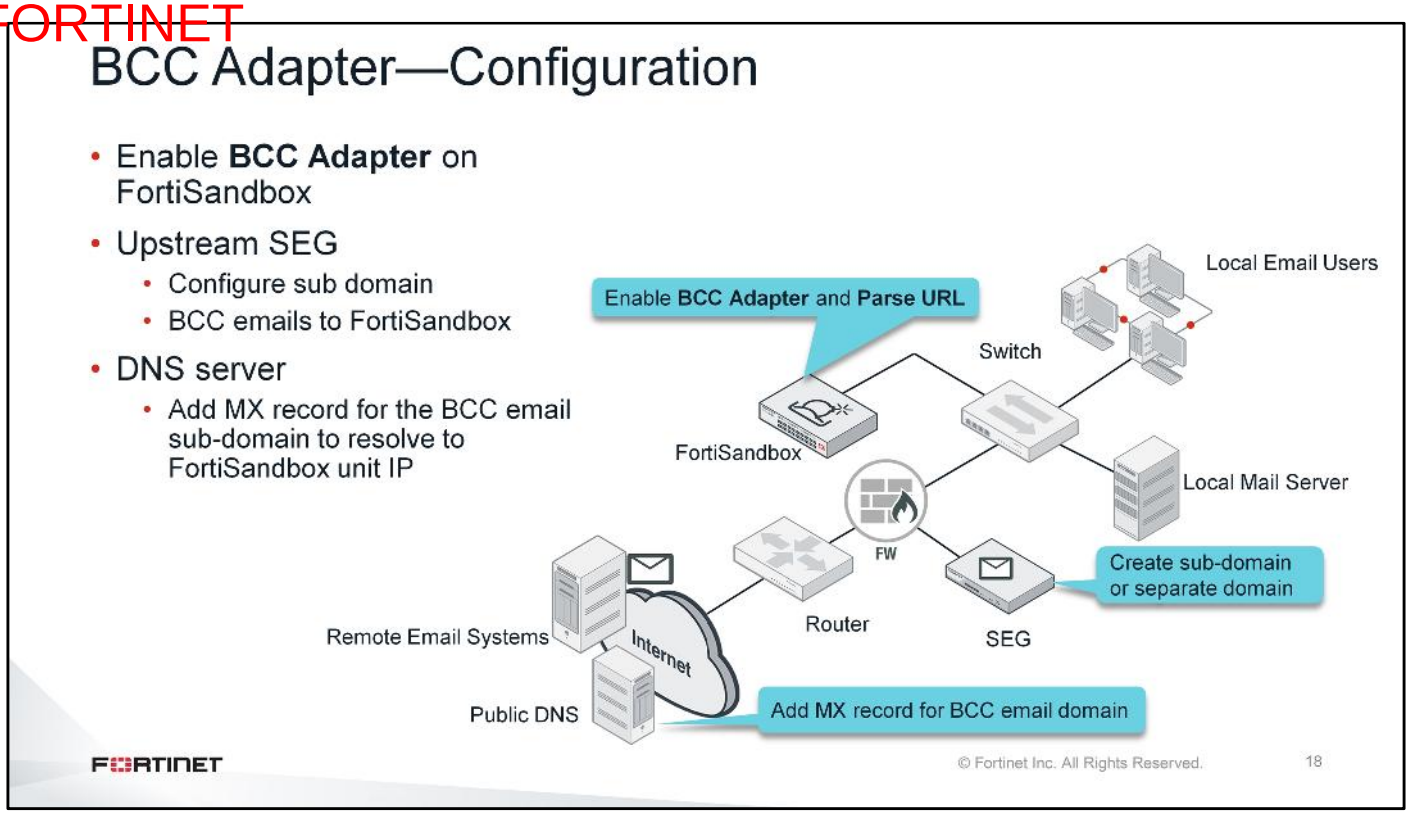


FORTINET

17

To help identify attacks missed by traditional email security technologies, you can enable **BCC adapter** to receive forwarded emails from any upstream MTA server and scan them. FortiSandbox will extract attachment files and URLs in the email body and send them to the job queue. One use cases for the BCC operation is to provide advanced persistent threat analysis (APT) for customers who don't have FortiMail deployed. Customers may have an alternate email security gateway deployed (for example, Proofpoint, Ironport, Microsoft, or others) and would like to gain FortiSandbox's improved detection and response. If you enable **Parse URL** then FortiSandbox will extract the first three URLs in the email.

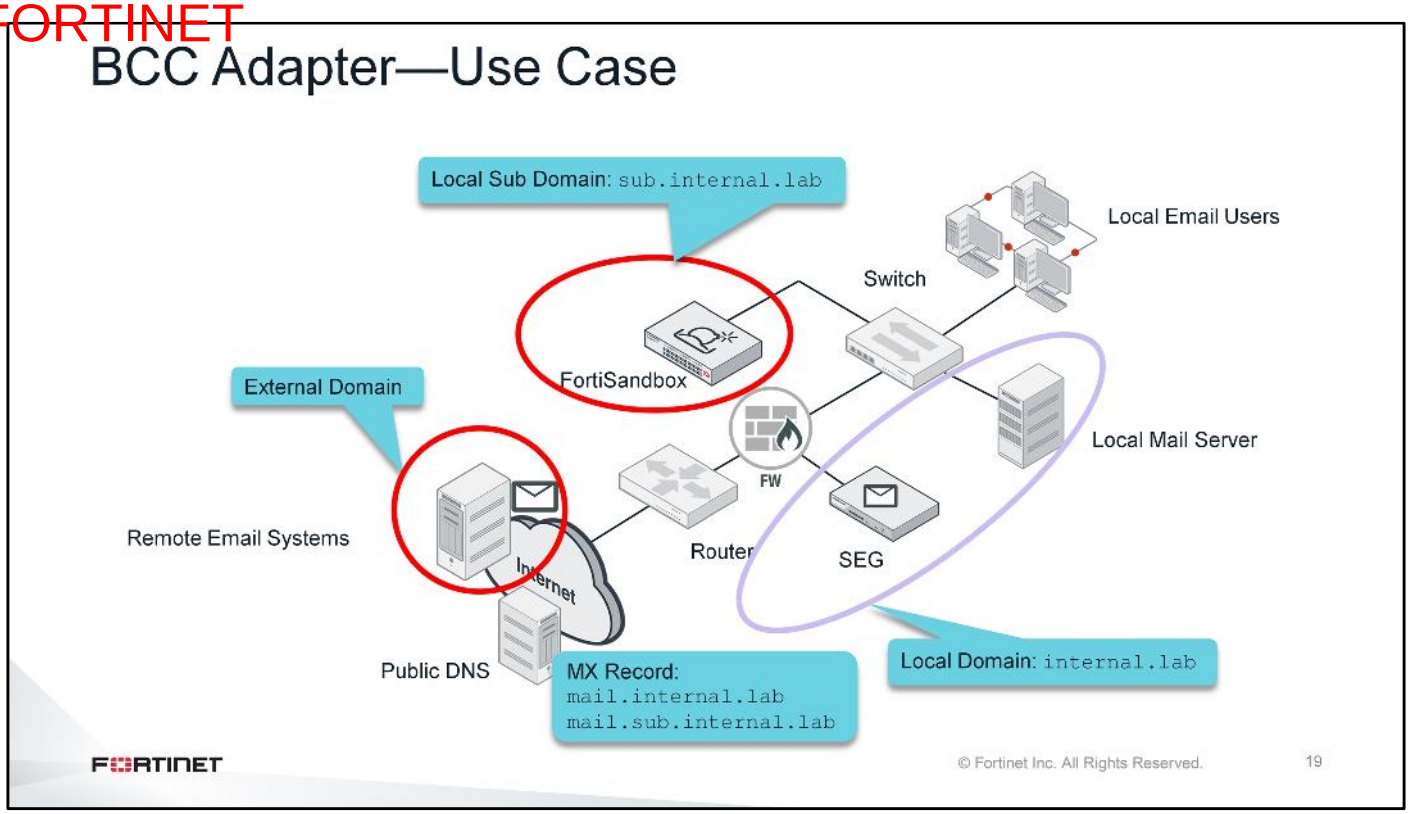
In BCC mode, the submitting Secure Email Gateway (SEG) sends a copy of the email to FortiSandbox for analysis while concurrently delivering the original email, so threats that are identified must still be remediated. Remediation may be manual, automated by sharing threat intelligence from FortiSandbox (natively or via API) to installed network and endpoint security components, or by other methods. If you would like to leverage real-time, proactive prevention from email-based threats, you should implement a FortiMail and FortiSandbox integration.



For FortiSandbox to scan emails from third-party SEG you need to enable **BCC Adapter**, which is disabled by default, and enable **Parse URL** to allow FortiSandbox to extract the first three URLs in the email. You can input the SMTP port that FortiSandbox listens on to receive email. The default port is 25.

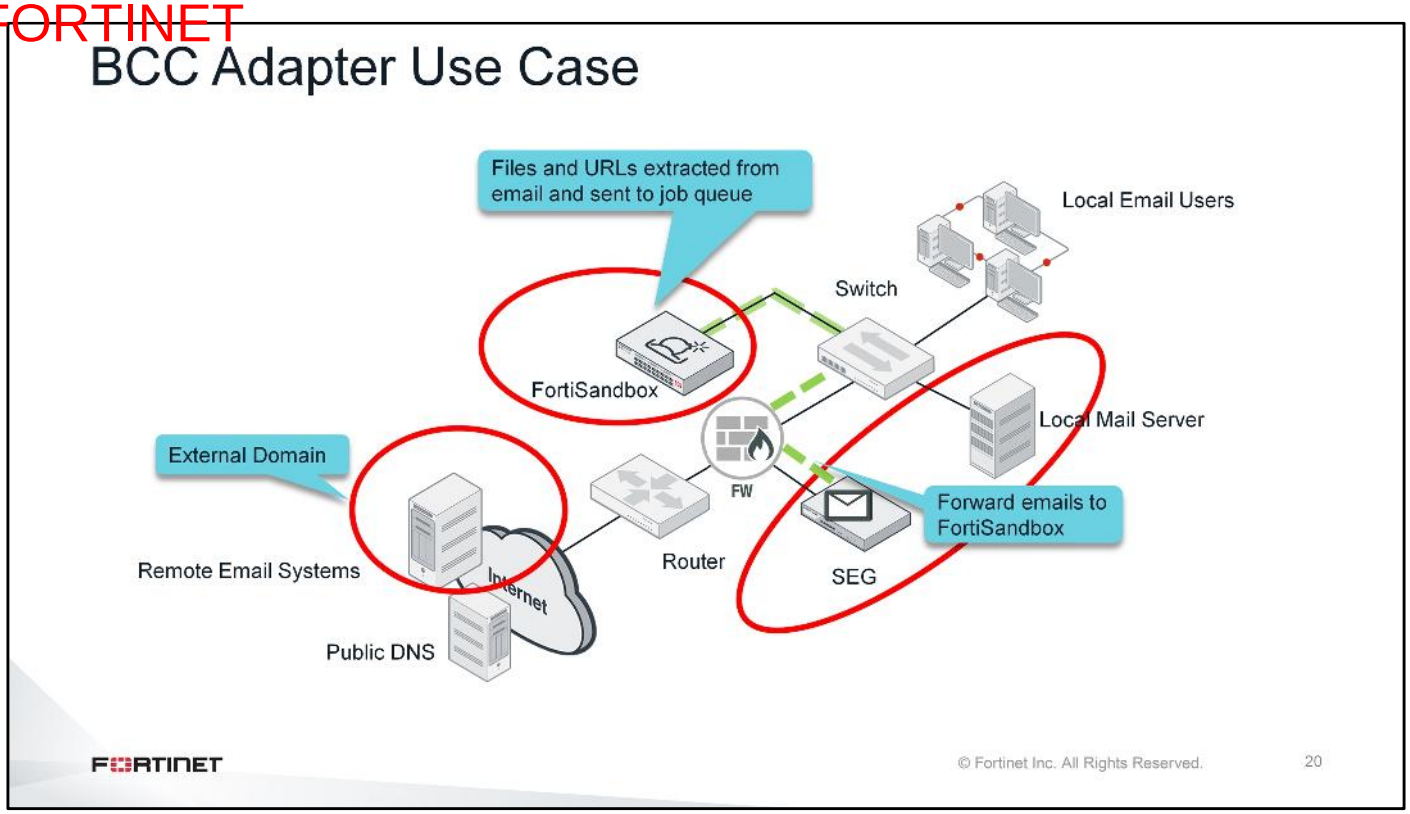
On the SEG, you need to create a sub-domain or a separate domain so that SEG is able to BCC the emails to FortiSandbox. For detailed instructions to configure BCC email on any third-party email gateway, refer to the vendor's manual.

For the DNS server that SEG is accessing, add an MX record for the BCC email domain to resolve to FortiSandbox unit IP.



In this example, there is a local domain `internal.lab` and a sub-domain `sub.internal.lab`. The local and sub-domain need to be configured on the SEG. The MX record `mail.internal.lab` points to the SEG and `mail.sub.internal.lab` points to FortiSandbox.

Inbound emails originating from an external domain will be routed to the SEG.



SEG will forward the email to FortiSandbox and to the local mail server. FortiSandbox will provide additional scanning for zero-day threats, beyond what the SEG may provide. Files and URLs will be extracted from the email for scanning.

While FortiSandbox is scanning the email, the original is available on the local mail server. If the email is malicious then local email users could be infected.

BCC Adapter Scanning Statistics

Scanning Statistics - Last 24 Hours

Rating	Sniffer	Device(s)	On Demand	Network	Adapter	URL	All
Malicious	0	1,878	0	0	3	0	1,881
Suspicious - High Risk	0	51	0	0	2	0	53
Suspicious - Medium Risk	0	0	0	0	0	0	0
Suspicious - Low Risk	0	0	0	0	6	6	12
Clean	0	364	0	0	59,497	14	59,875
Other	0	0	0	0	0	0	0
Processed	0	2,293	0	0	59,508	20	61,821
Pending	*0*	*3*	*0*	*0*	*0*	*0*	*3*
Processing	*0*	*0*	*0*	*0*	*0*	*0*	*0*
Total	*0*	*2,296*	*0*	*0*	*59,508*	*20*	*61,824*

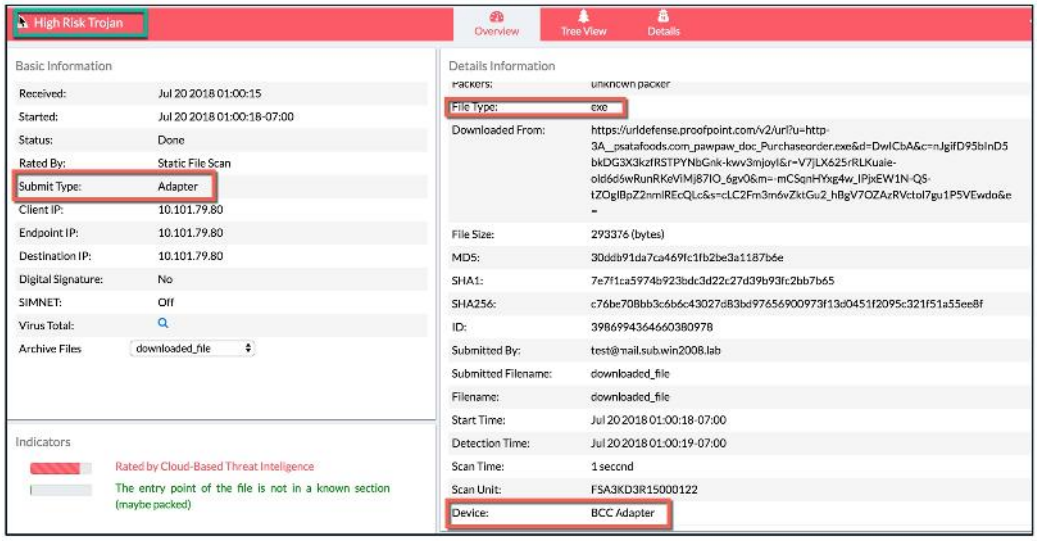
Last Updated: Fri, Jul 20 01:06

FORTINET

21

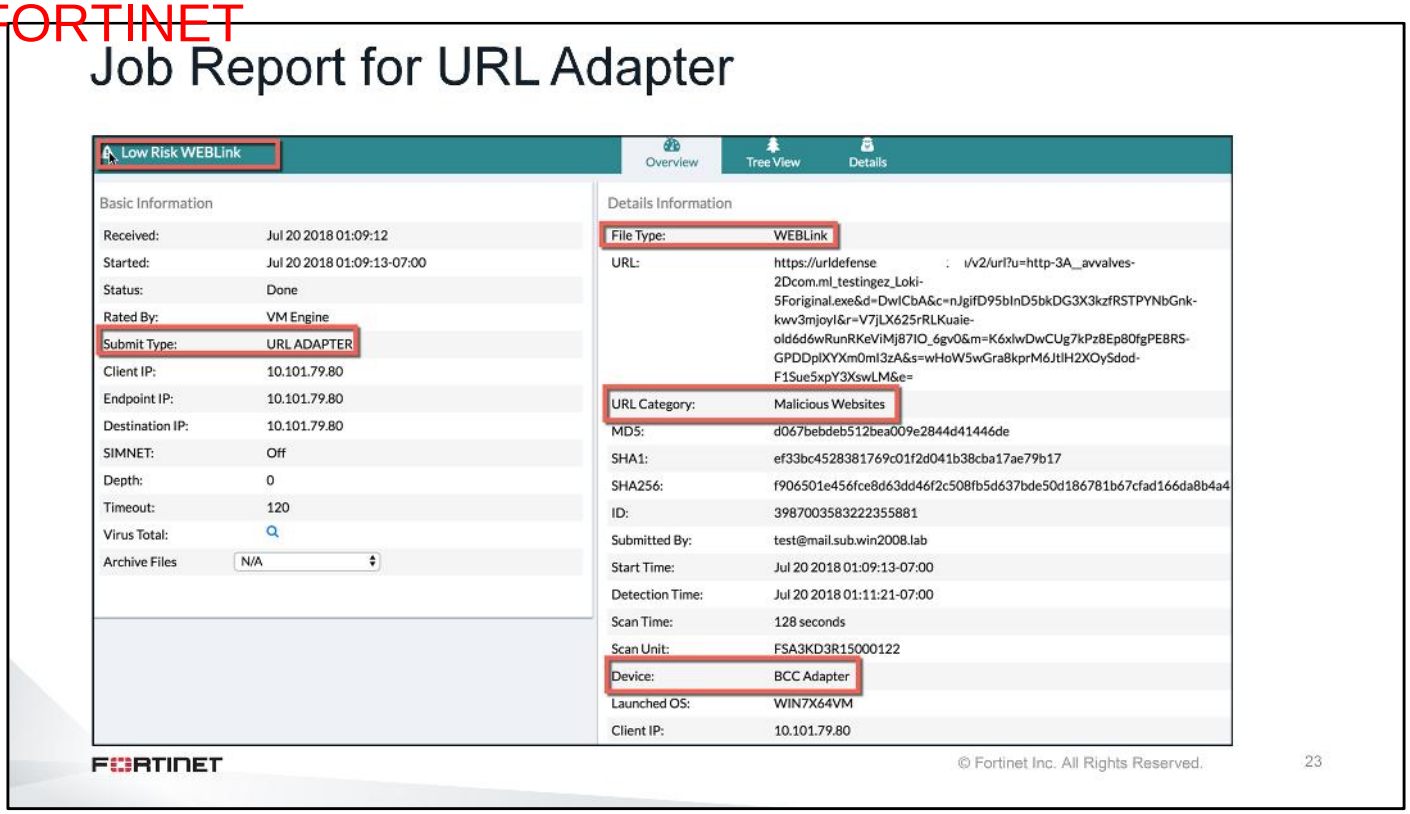
The example dashboard on this slide show scanning statistics for the Adapter and URL categories.

Job Report for BCC Adapter



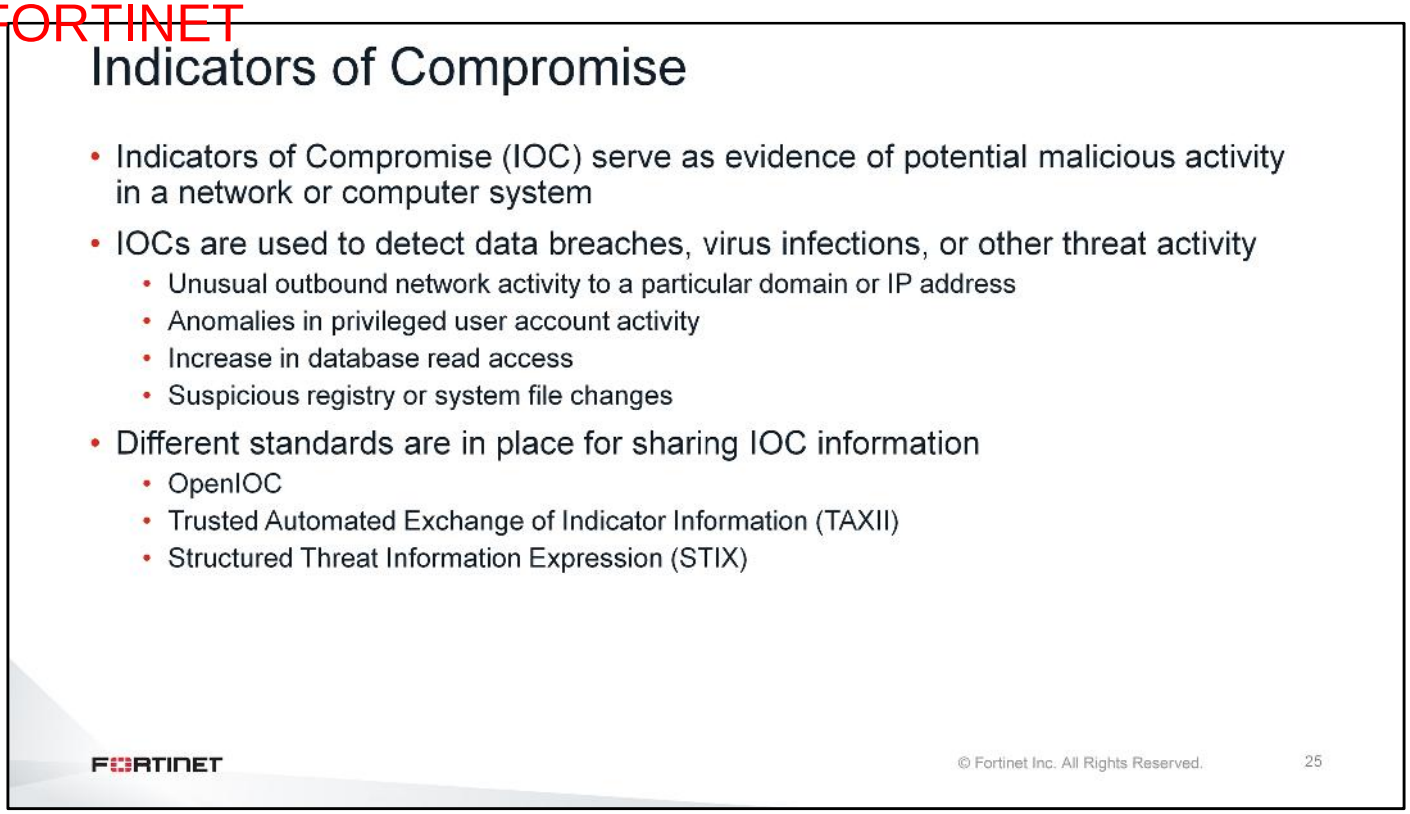
FORTINET © Fortinet Inc. All Rights Reserved. 22

The example job report on this slide shows **Submit Type** as **Adapter**, **File Type** as `exe` and **Device** as **BCC Adapter**. This means that the executable type file was extracted from an email which was submitted by the BCC adapter. After scanning the file, FortiSandbox concluded that the file is a high risk trojan.



The job report on this slide shows **Submit Type** as **URL ADAPTER**, **File Type** as **WEBLink**, **URL Category** as **Malicious Websites**, and **Device** as **BCC Adapter**. This means that the malicious URL was extracted from an email that was submitted by the BCC adapter device and was scanned by the URL adapter.

In this section, you will learn about the available options to share threat intelligence with third-party appliances.



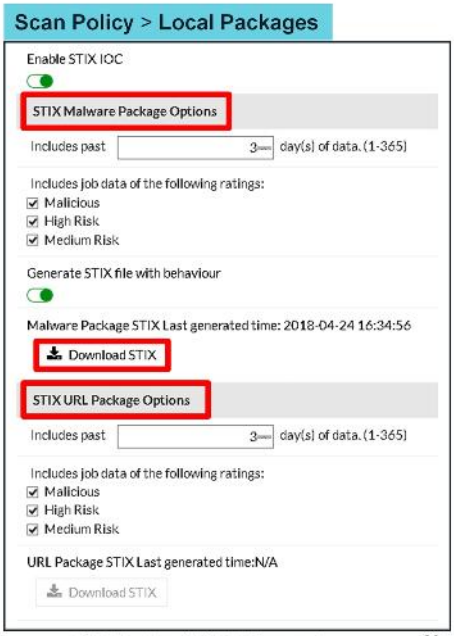
Indicators of compromise (IOC) serve as evidence of potential malicious activity in a network or computer system. IOCs are used to detect intrusion attempts, data breaches, or other malicious activities.

Examples of IOC include unusual outbound network traffic to particular domain or IP address, anomalies in privileged user account activity, an increase in database read access, or suspicious registry or system file changes, and so on. These unusual activities are the red flags that indicate a potential or in-progress attack, that can lead to a data breach.

There are standards in place that standardize IOC documentation and reporting—OpenIOC, TAXII, STIX.

FortiSandbox STIX Packages

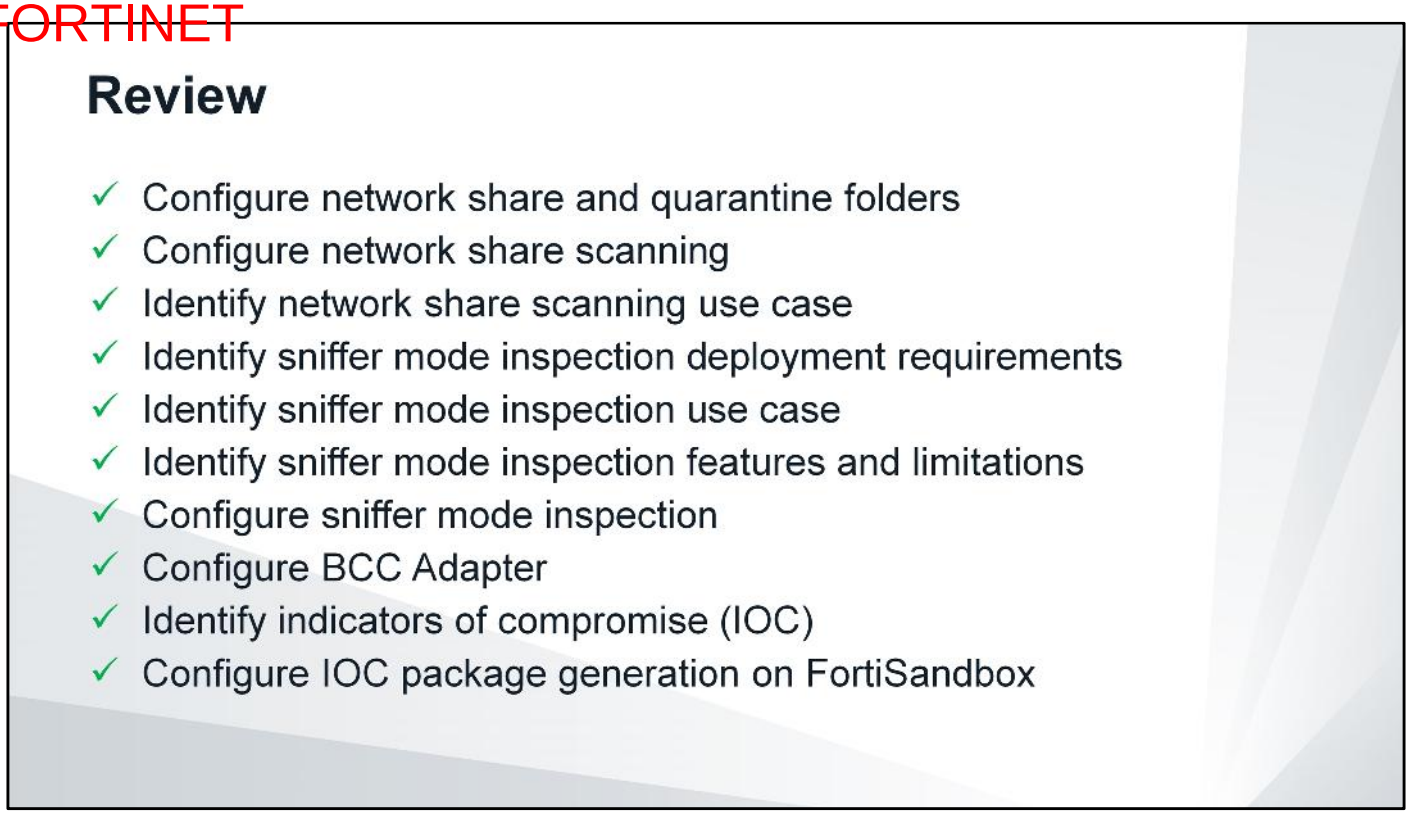
- FortiSandbox can generate IOCs in STIX v1.2 format
  - STIX Malware Package
    - Contains malware file hash and behavioral indicators
  - STIX URL Package
    - Contains download URLs for malware
- Packages can be downloaded and shared with other devices that support same STIX format



 26

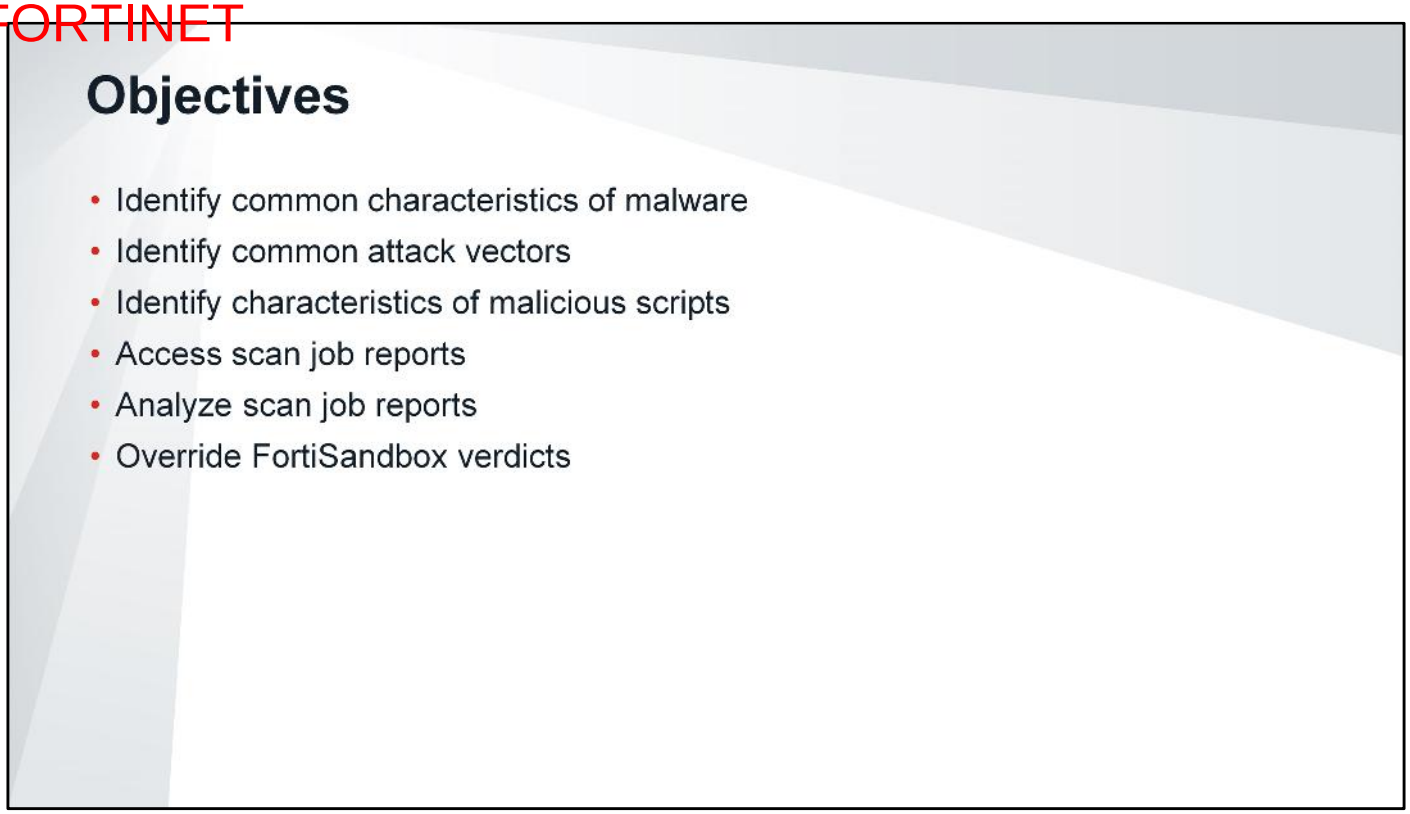
FortiSandbox supports STIX v1.2 format for IOCs. The STIX malware package contains malware file hashes and behavioral indicators. The STIX URL package contains download URLs for malware. These packages are generated at the same time as the FortiSandbox native malware and URL packages.

The packages must be downloaded and shared with other devices that support the same STIX format.



This slide shows the objectives covered in this lesson.

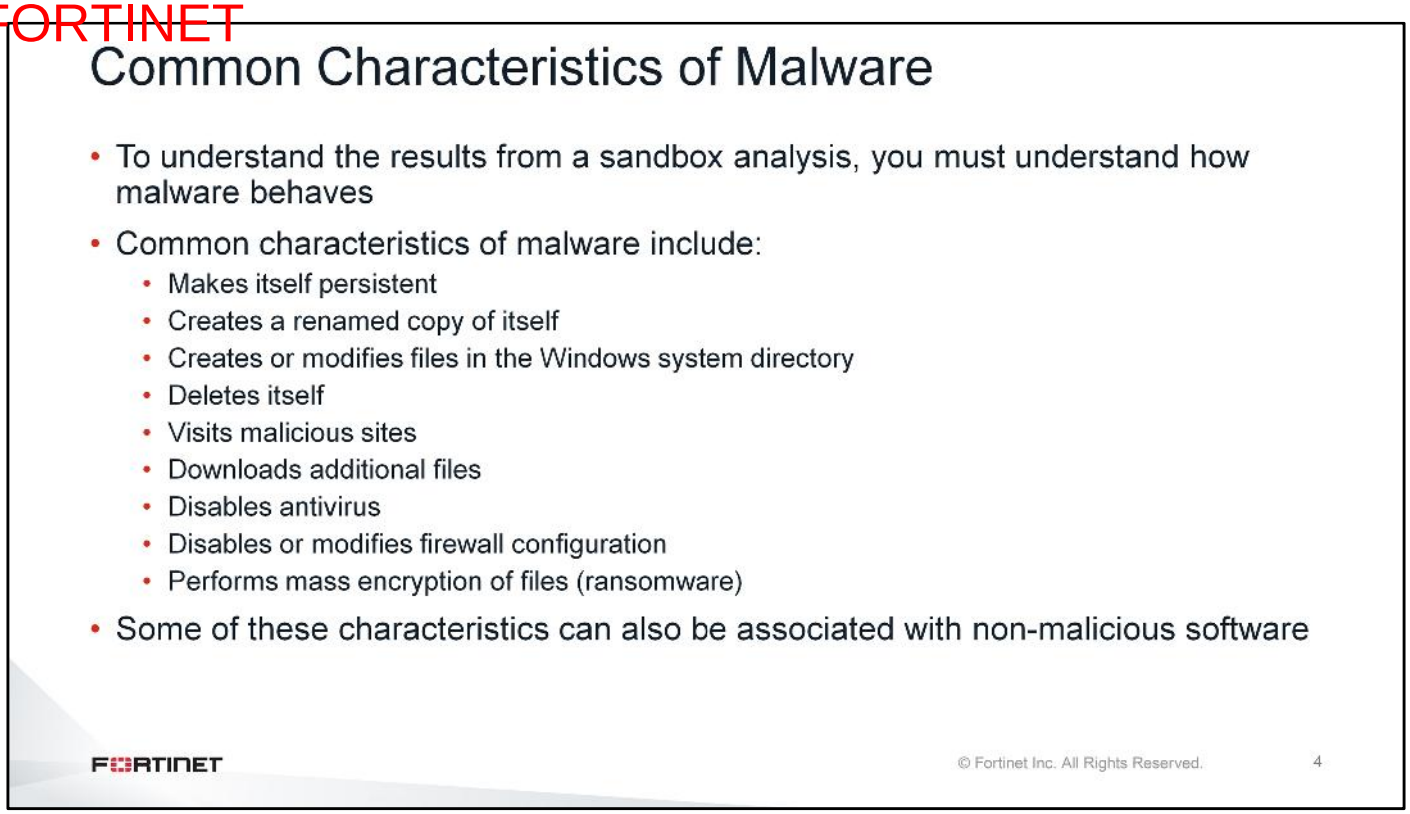
In this lesson, you will learn how FortiSandbox generates verdicts for samples.



After completing this lesson, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in results analysis, you will be able to identify malware traits and understand FortiSandbox scan job reports.

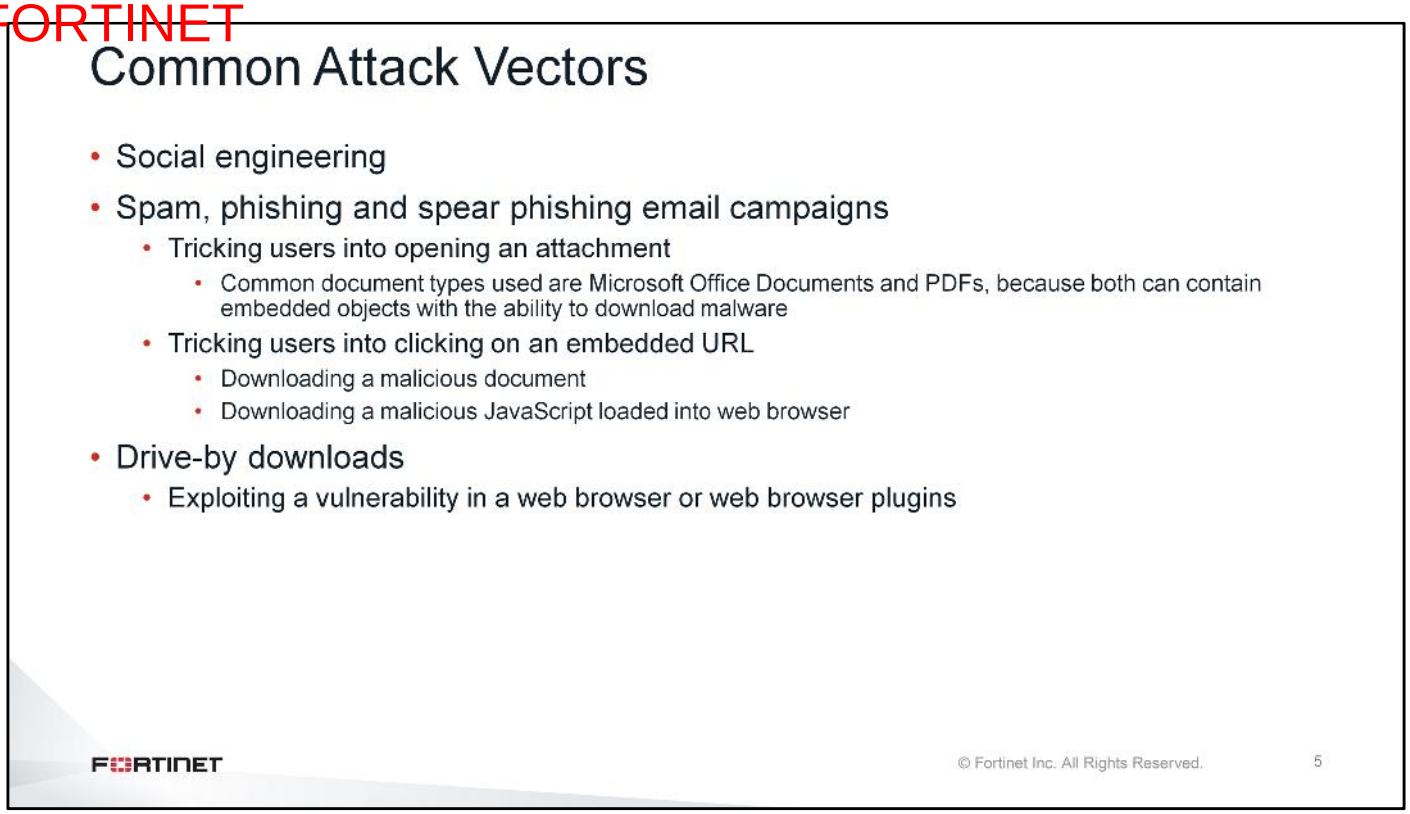
In this section, you will learn about the common characteristics of malware.



FortiSandbox looks for malware traits when it analyzes files. In order to understand the results from the analysis of a sample, you must first understand how malware behaves.

Common characteristics of malware includes:
- Makes itself persistent
- Creates a renamed copy of itself
- Creates or modifies files in the Windows system directory
- Deletes itself
- Visits malicious sites
- Downloads additional files
- Disables antivirus
- Disables or modifies firewall configuration
- Performs mass encryption of files (ransomware)

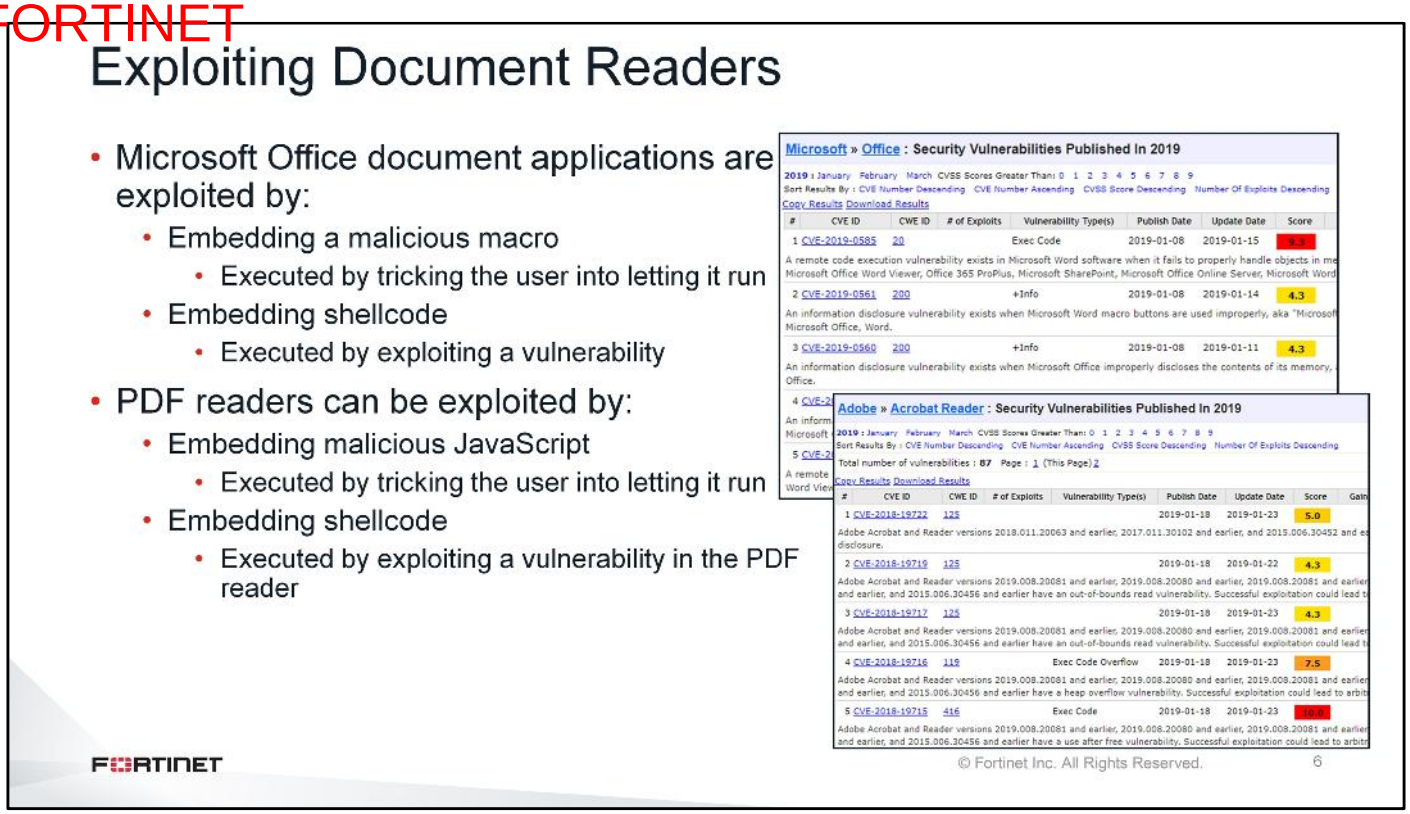
Unfortunately, some of these characteristics are not a clear identifier of malicious behavior. Certain software, like device drivers, may write to system directories, and make itself persistent. So when investigating malware, you have to look at multiple data points to come to a conclusion.



How does the malware get onto the system in the first place? There are multiple attack vectors that can be used to get malware onto a system. Two common attack vectors are social engineering and drive-by downloads. Social engineering is an attack that tries to manipulate users into doing something, such as opening a malicious attachment or clicking on an embedded URL link in an email. If the user does perform the action, the end result is that they will infect their system. Emails containing malicious attachments or embedded URLs can be sent to a user during a spam campaign, in an opportunistic attack, or by a phishing or spear phishing campaign in a targeted attack.

Common documents used as email attachments are Microsoft Office documents and PDFs, because both can contain embedded objects with the ability to download malware.

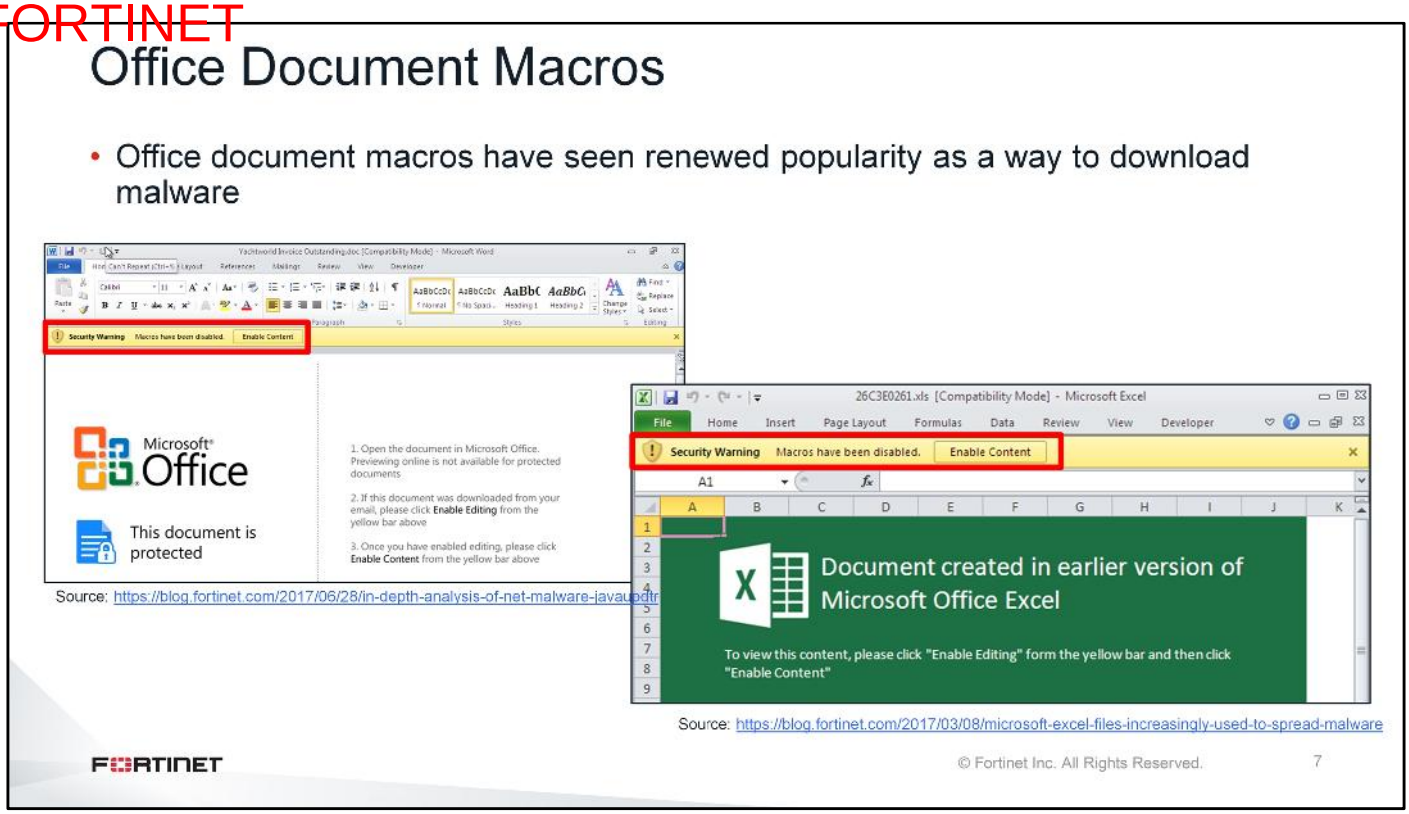
Drive-by downloads are another attack vector in which the user's system can be infected, by the user visiting a compromised website. In the background, the website redirects the browser to a malicious site that downloads malicious code, usually in the form of a JavaScript, and tries to exploit either the web browser or web browser plugins.



Microsoft Office documents can be exploited by embedding a malicious macro that will ultimately download and run code. Macros are small scripts written in Visual Basic for Applications (VBA) to accomplish some form of automation. In modern versions of Microsoft Office, macros are disabled by default and the user must explicitly allow a macro to run. Getting a user to run a malicious macro does not require an attacker to exploit a vulnerability, it only requires the user to be tricked into running it.

The second option that an attacker can use, exploits a vulnerability in how Microsoft Office handles a document. The attacker can craft a document to exploit the vulnerability and have the malicious code executed. This method does require the user to open the document. So far in 2019, five vulnerabilities have been registered for Microsoft Office. In 2018, 76 vulnerabilities were reported.

Like Microsoft Office documents, PDF files are structured documents that contain both static and dynamic elements, such as JavaScript. PDF readers can be exploited in many different ways. One common way is by using embedded JavaScript. The JavaScript can trick the user into allowing it to download and run malicious code. The JavaScript can also be crafted to exploit a vulnerability in the PDF reader and allow the attackers code to run. In 2018, 138 vulnerabilities were reported for Adobe Acrobat reader. So far in 2019, 87 have been reported.



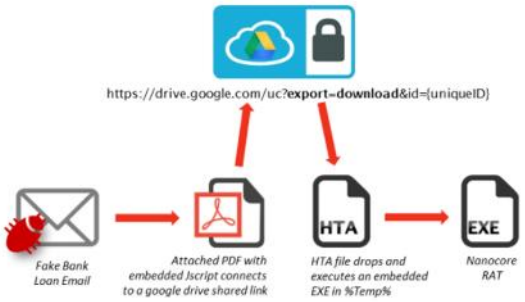
Marcos have seen a renewed popularity as a way to download malware. Both of the examples shown on this slide are taken from malicious samples analyzed by the FortiGuard team. The documents, rather convincingly, display instructions to the user to enable the macros.

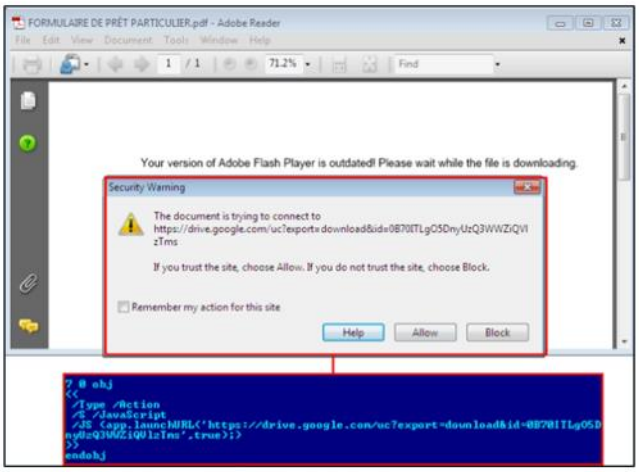
When a user clicks **Enable Content**, the macro is executed silently in the background.

You can find more information on the analysis of these two documents on the Fortinet blog: *https://www.fortinet.com/blog*.

PDF JavaScript

- Kill chain using PDF files





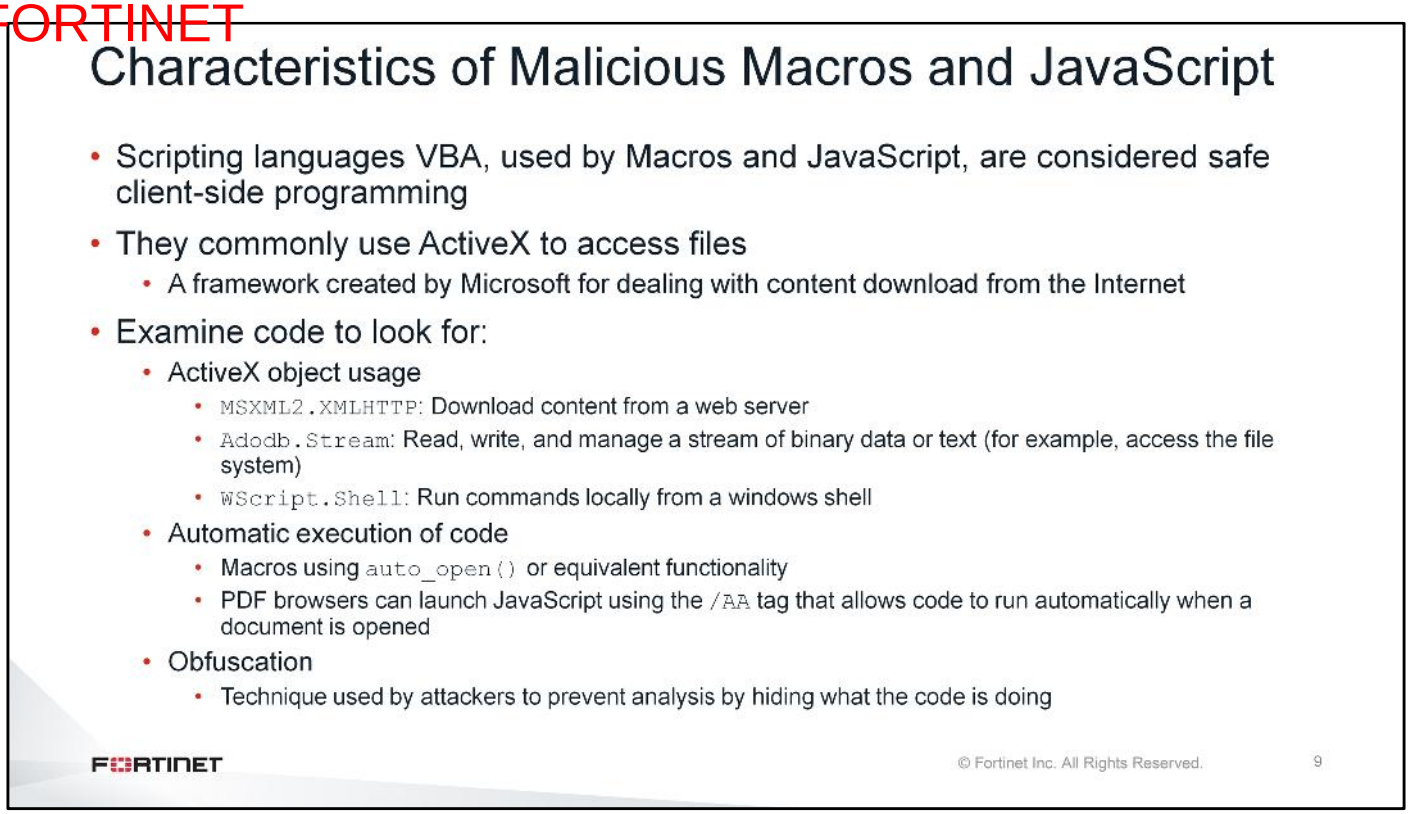
Source: https://blog.fortinet.com/2017/10/12/pdf-phishing-leads-to-nanocore-rat-targets-french-nationals

FORTINET

8

This slide shows an example of a PDF file with an embedded JavaScript, which downloads the payload from a Google Drive shared link. This is also taken from a sample analyzed by the FortiGuard team.

You can find more information on the analysis of these two documents on the Fortinet blog: *https://www.fortinet.com/blog*.



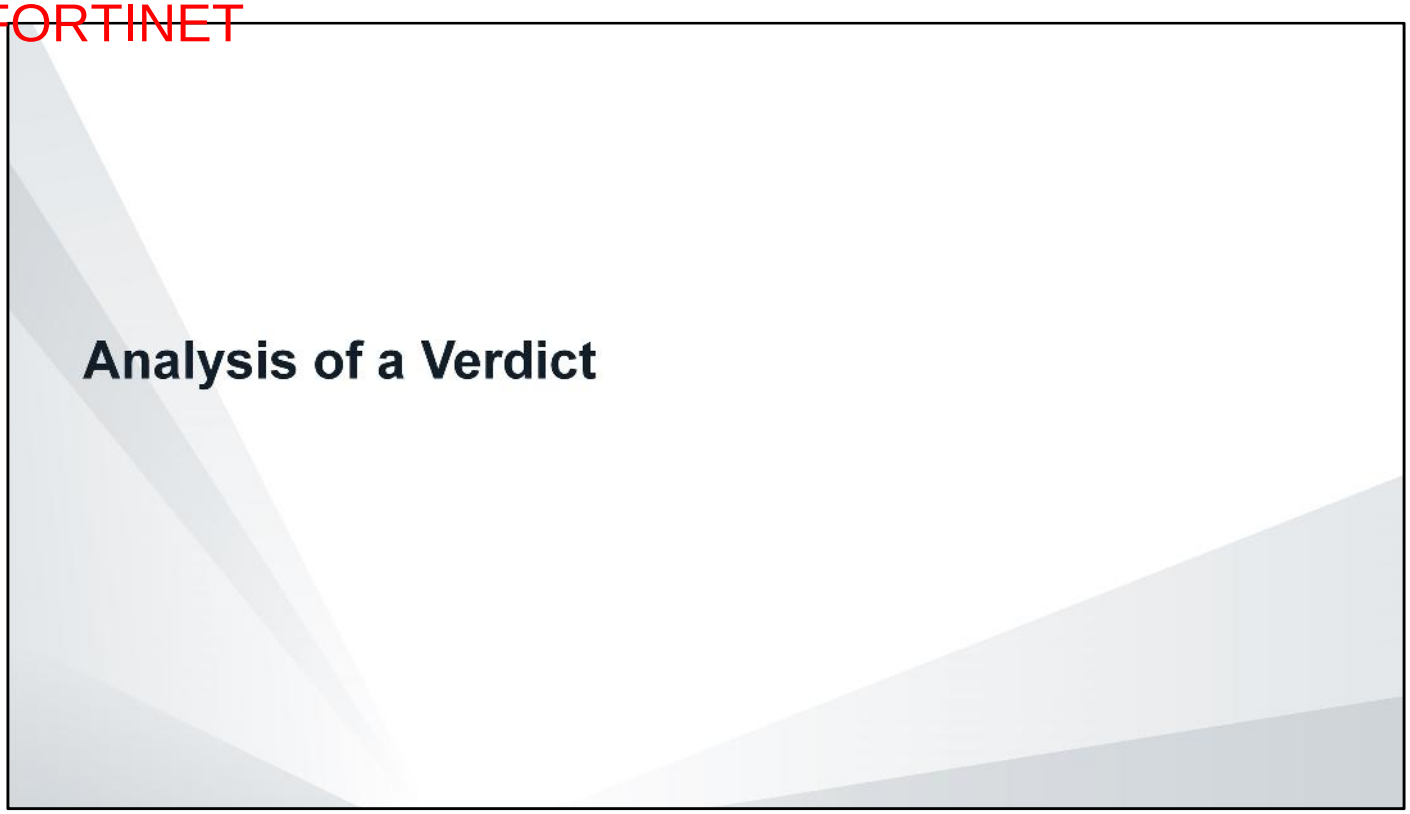
What characteristics should you look for when determining if a script is malicious?

Scripting languages such as (VBA) and JavaScript, are considered safe client-side programming languages. They do not have any native functions that are used to access files. They use ActiveX, a framework created by Microsoft, for dealing with content download from the Internet. The following are some examples of what ActiveX objects can be used to do:

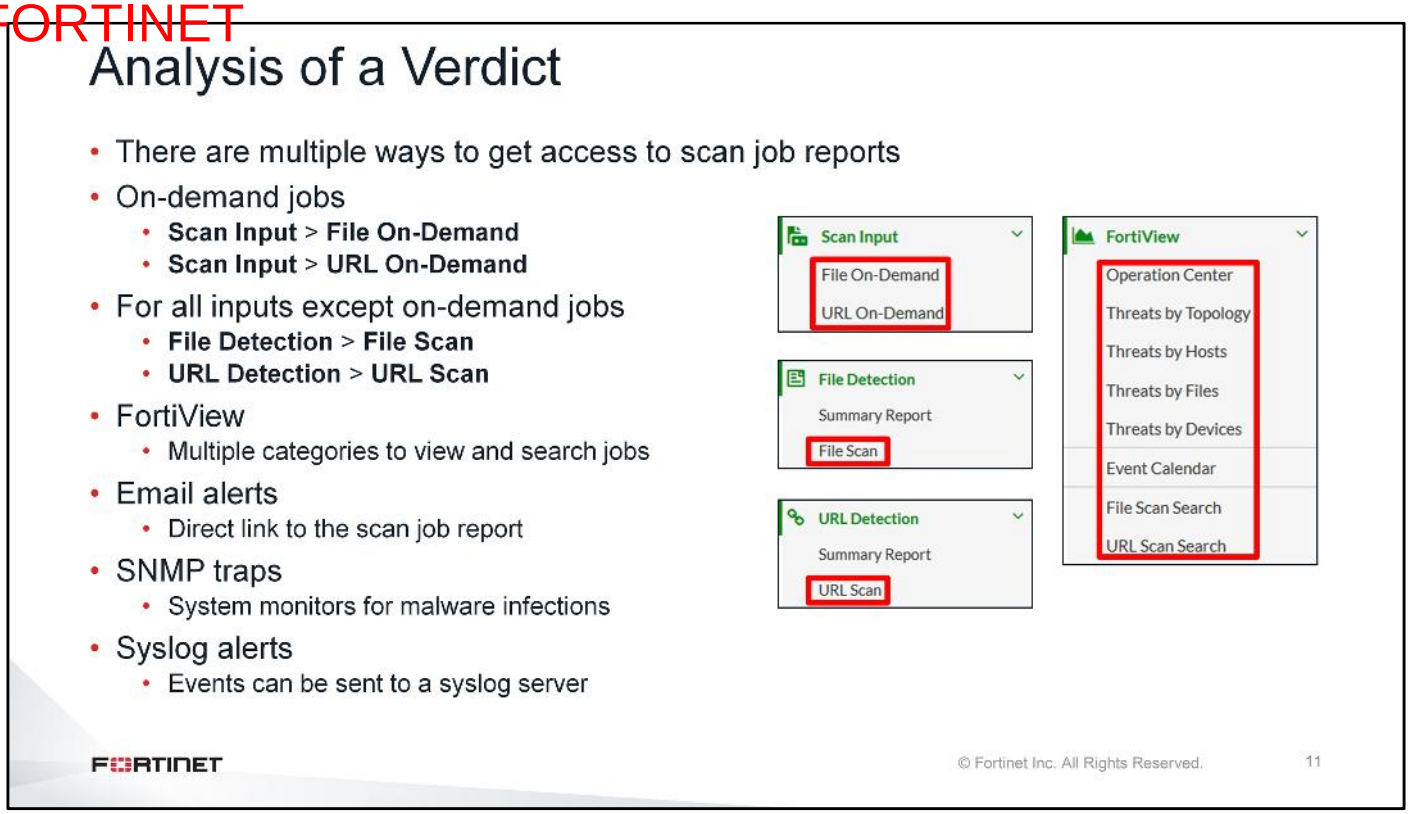
- `MSXML2.XMLHTTP` can be used to download content from a web server
- `Adodb.Stream` can be used to read, write, and manage a stream of binary data or text
- `WScript.Shell` can be used to run commands locally from a windows shell

Since these objects can be used to download content from the web, save it to disk, and run it, these objects are looked for when analyzing scripts for suspicious behaviors. You also want to see if scripts are automatically executing code. Macros have built-in functions, such as `auto_open()`, which will run when the document is opened. PDF readers can use tags such as `/AA` to automatically launch JavaScript.

Attackers also use obfuscation to hide what their scripts are doing and hinder any analysis; therefore, signs of obfuscation is also characteristics to look for.



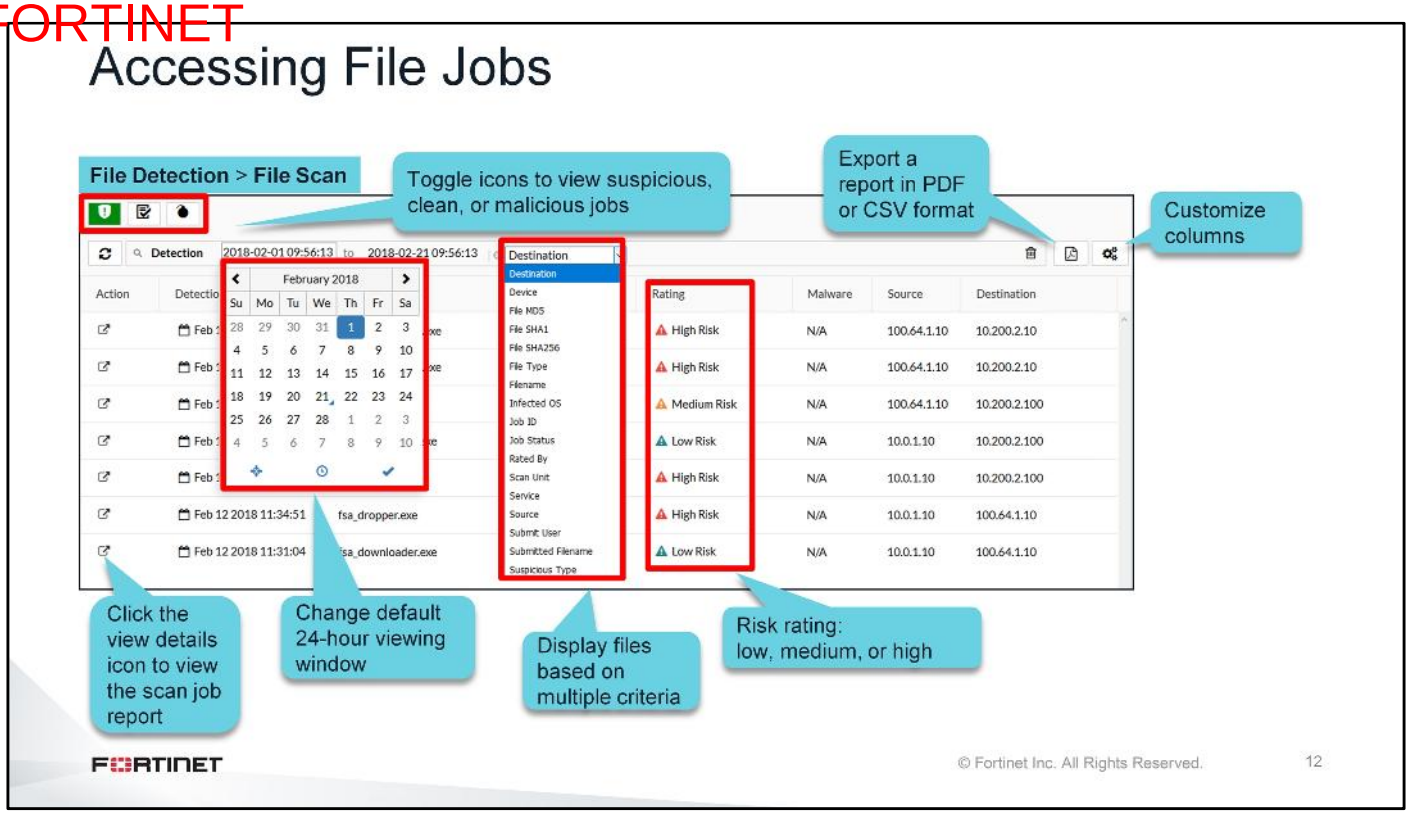
In this section, you will learn how to access and analyze FortiSandbox scan job reports.



Now that you know the characteristics of malware, some of the common ways it lands on a user's system, and the characteristics of malicious scripts used to deliver malware, you will look at how FortiSandbox determines its verdict when analyzing a sample.

There are multiple ways to access FortiSandbox verdicts on the GUI as well as from external applications. You can use the **Operation Centre** menu item to access all suspicious and malicious file scan jobs. You can use the **URL Scan** menu item to view URL scan jobs.

Externally, you can use alert emails, which can be sent to security analysts any time a suspicious file has been analyzed by FortiSandbox. You can also use SNMP and syslog alerts from third-party monitoring tools.



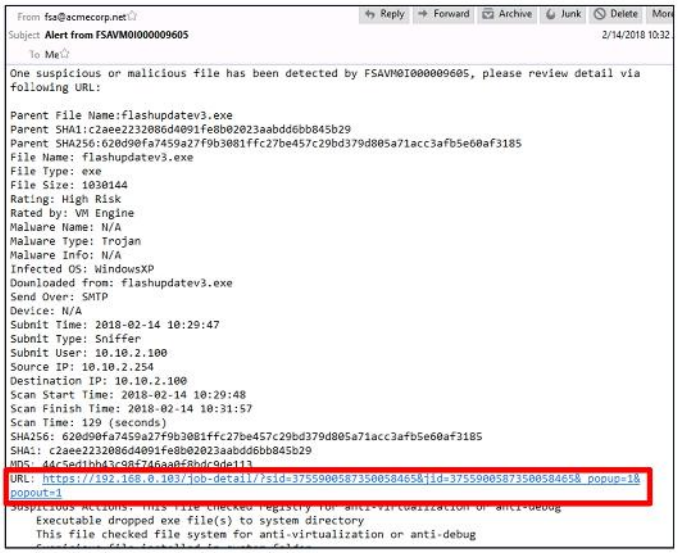
The **File Scan** view shows file-based scan jobs grouped by their ratings. The **URL Scan** view shows URL-based scan jobs grouped by their ratings. By default, only jobs with a suspicious verdict for the last 24 hours are displayed.

Here you have the ability to:

- Toggle between suspicious, clean, and malicious verdicts
- Display verdicts over desired time spans and with various filters
- Export scan job reports in PDF and CSV formats
- Customize the column headers
- Display the scan job report

Accessing a Scan Job Report Using Alert Email

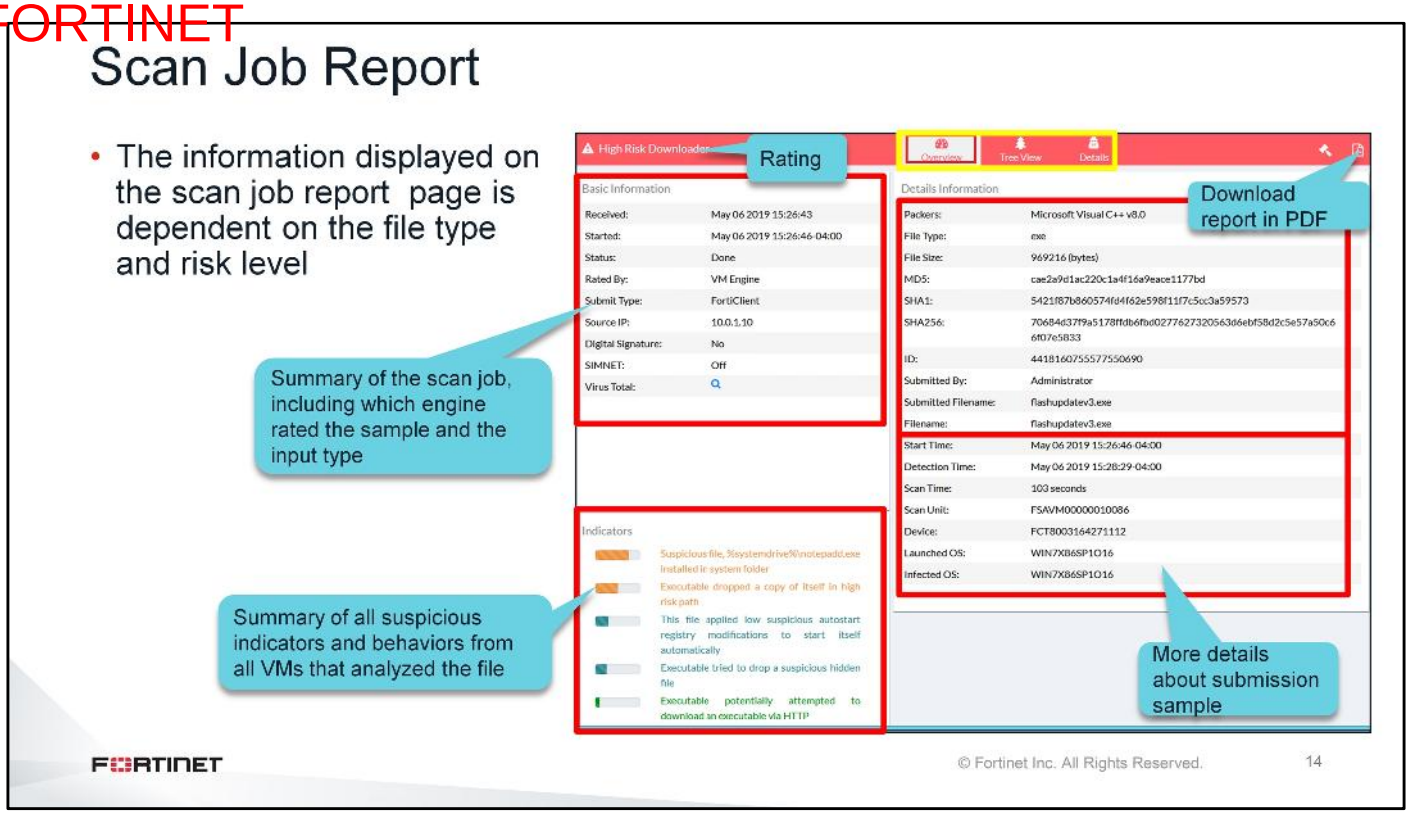
- Alert emails include a summary of detected activity
- Include URL for quick access to detailed scan job report



FORTINET

13

Security analysts will likely want to receive alerts about suspicious activity, so that they are informed of incidents as soon as incidents are detected. This slide shows an example of an alert email sent from FortiSandbox, indicating that a suspicious file has been detected. The alert email includes a summary view of all the information about the file, how it was obtained, its rating, the suspicious actions it performed, and a URL which will take you directly to the scan job report of the analysis.



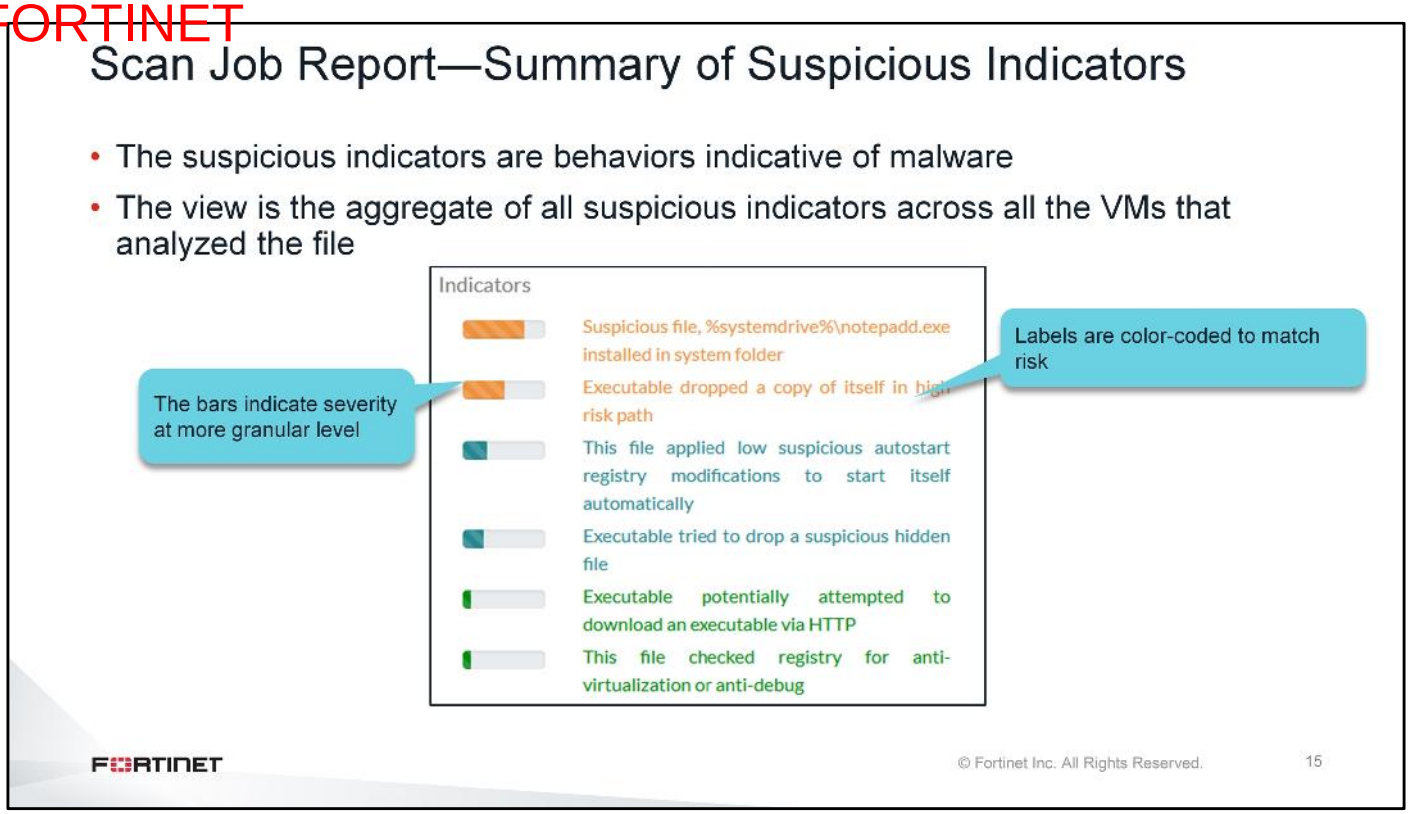
The scan job report gives you all the information from FortiSandbox's analysis of the sample. The top header displays the sample's rating and malware type. This header is color coded to reflect the risk level. High risk is red, medium risk is orange, low risk is blue, and clean is green.

The information is grouped into three categories: overview, tree view, and details.

The overview information is broken into three sections:

- **Basic Information**: Overview information about the scan job, when it was received, the input source, the scan conditions, and so on
- **Indicators**: Summary of the suspicious behaviors the sample exhibited when it was analyzed. These are indicators that were picked out based on the traits that malware exhibits.
- **Details Information**: Information on the sample: the file type, which OS it was analyzed on, and so on

You will learn about each section of the scan job report, what information the sections contains, and how the information is used to rate the sample.



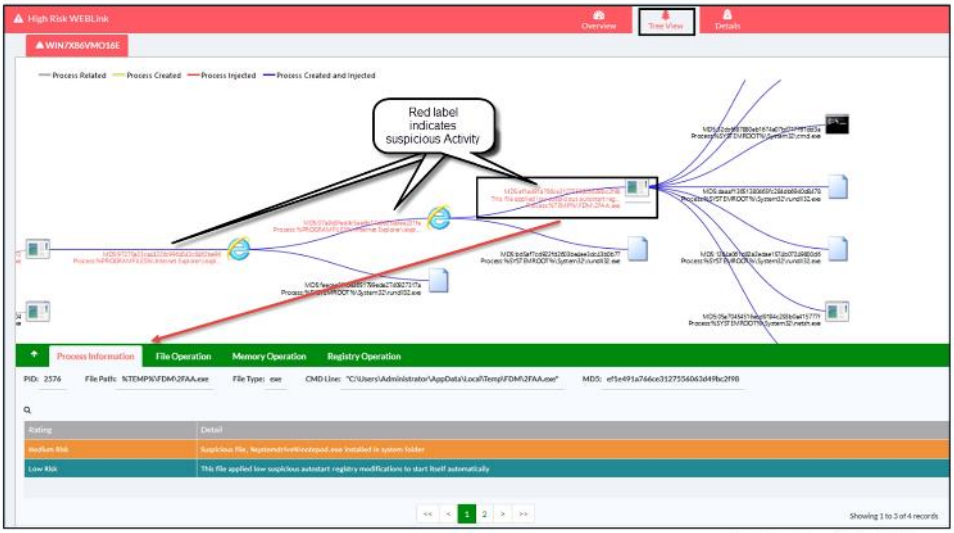
The suspicious indicators are what the rating engine parsed out of the tracer's log as behaviors indicative of malware. These are behaviors from the VM scan as well as any behaviors observed from the static analysis. The suspicious indicators are all based on a set of rules used by the rating engine, which is constantly updated by FortiGuard.

The labels are also color coded to reflect the risk level–blue for low risk, orange for medium risk, and red for high risk.

While some of these suspicious indicators give you an idea about what the malware did in the sandbox, there are others that you need to look at in more detail to get a better understanding. For example, what registry changes were done, and what suspicious files were installed in the system folder? The **Tree View** and **Details** section of the report provides this information.

Scan Job Report—Tree View

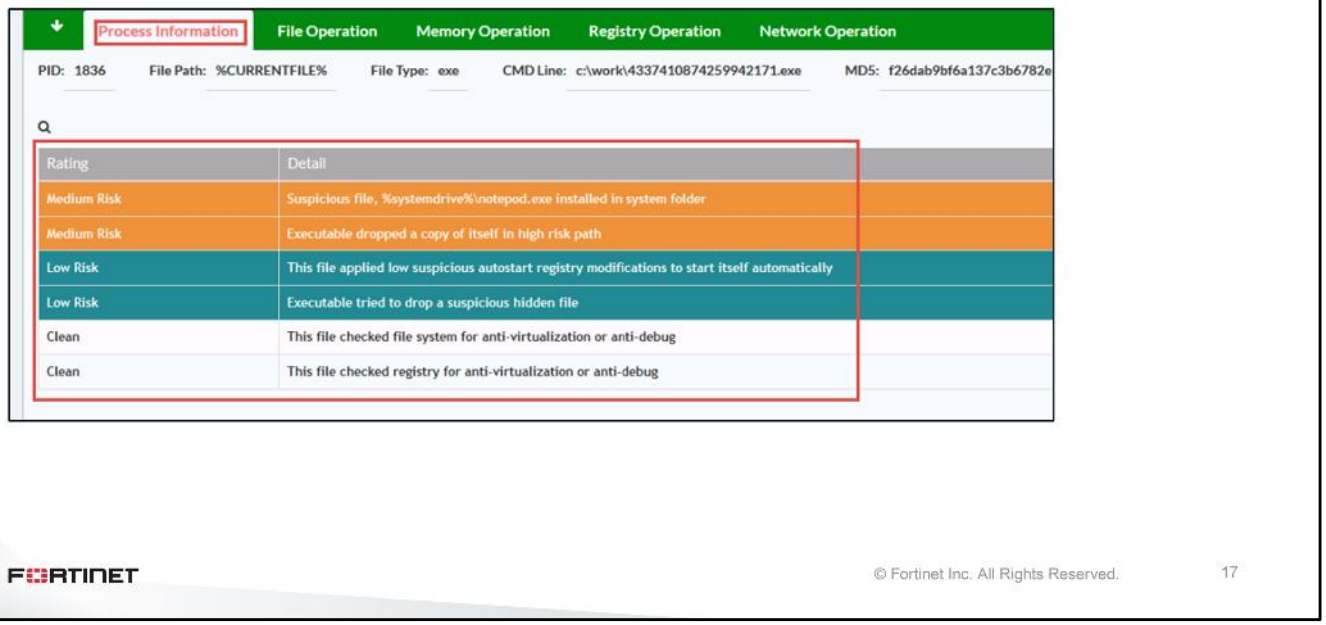
- The **Tree View** shows a file's parent-child process relationship when it executes inside a guest VM



16

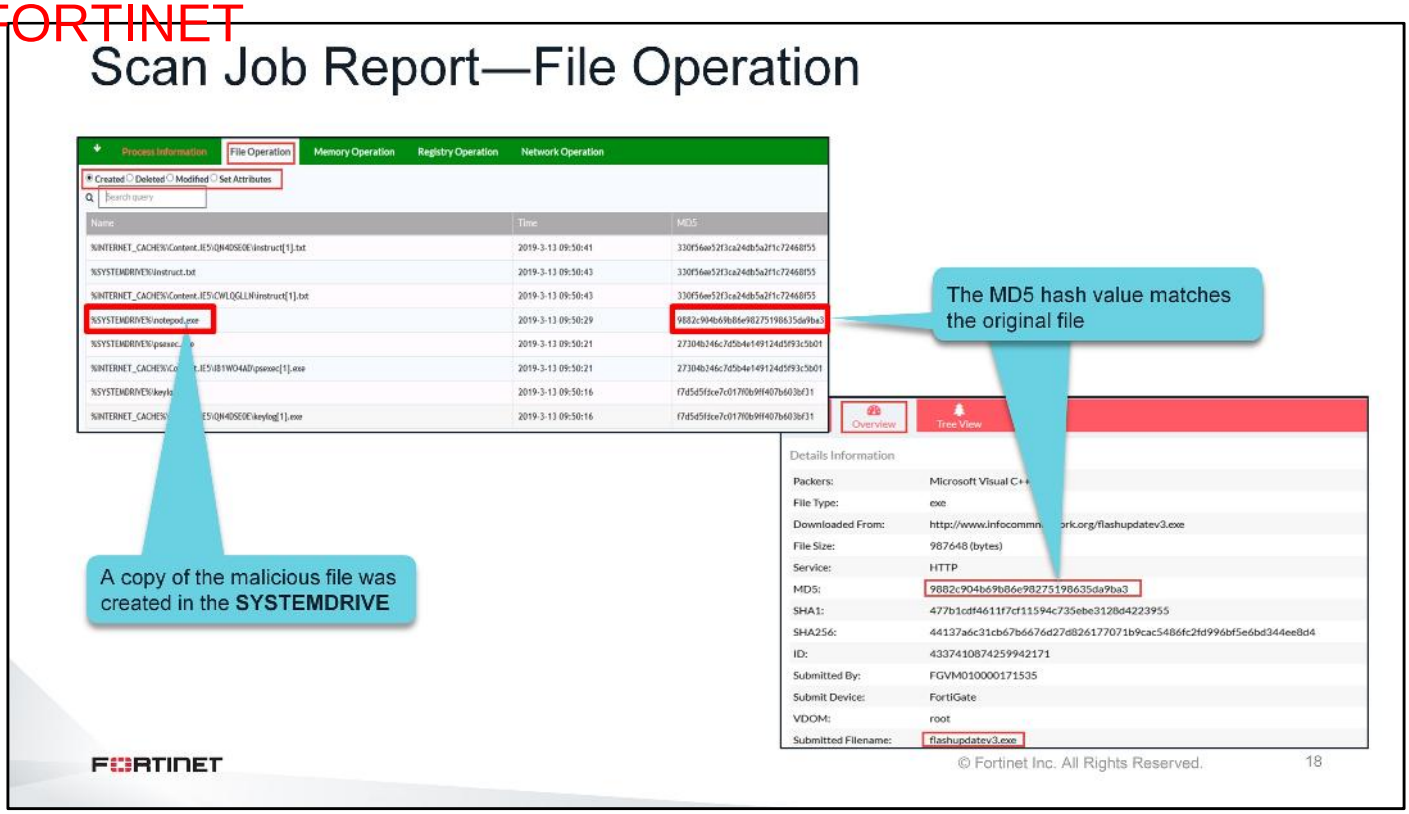
The **Tree View** shows a tree for a file's static structure or a file's parent-child process relationship when it executes inside a guest VM. You can drag the tree using the mouse, and you can zoom in or out using the mouse wheel. If there is suspicious activity with one tree node, its label will be colored red. Clicking a node in the tree will open more information in tab format. Suspicious information is shown in the color red, so you can quickly locate it.

Scan Job Report—Process Information

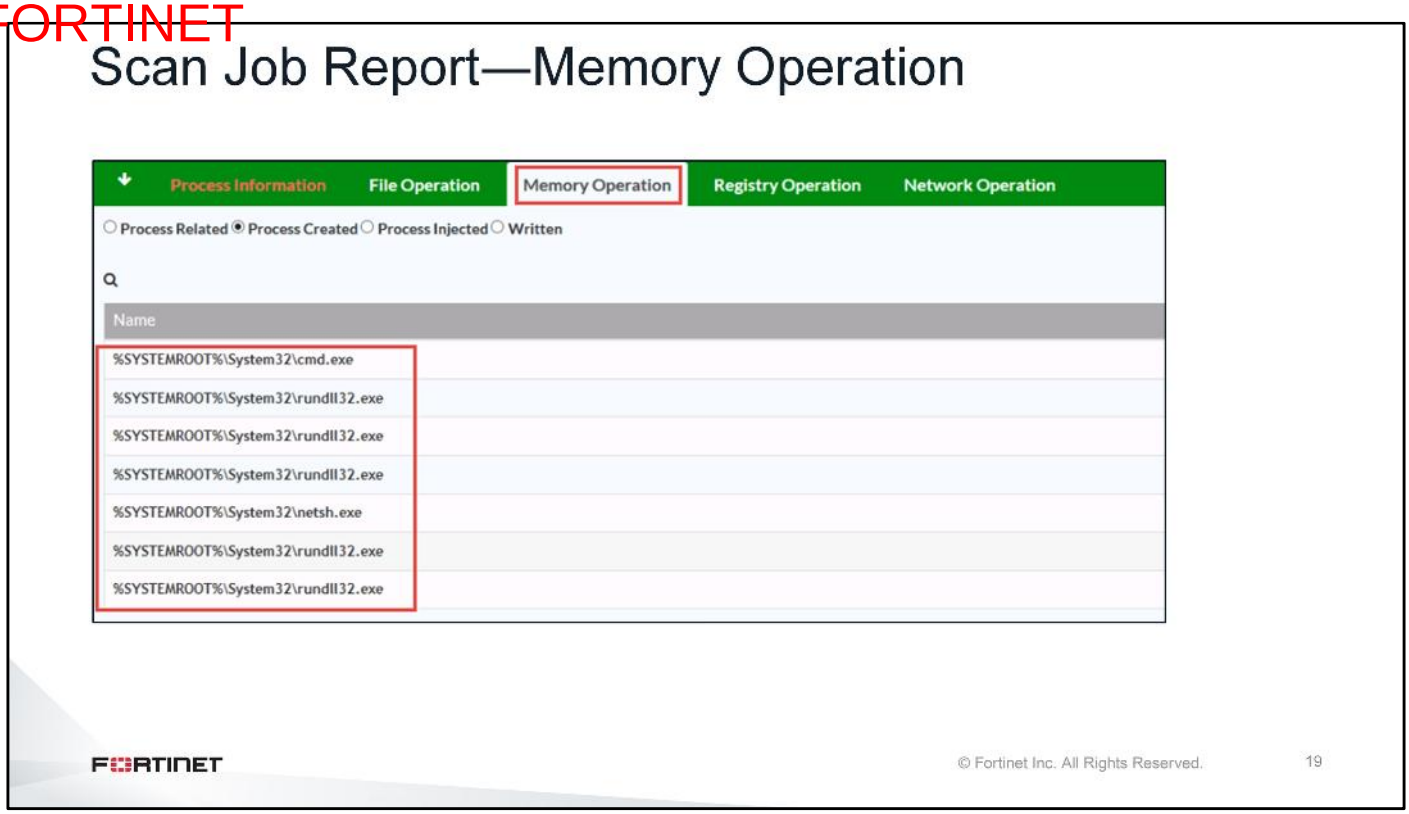


Click the executable root node to open more information in tab format. In the lower table, there are five tabs, which allow you to see information about the process, file, memory, registry, and network operations related to the execution of this sample.

Examine the **Process Information** tab. Here you can see all the processes picked up by FortiSandbox when the sample was running. The processes that are indicators are highlighted in color with a risk score.

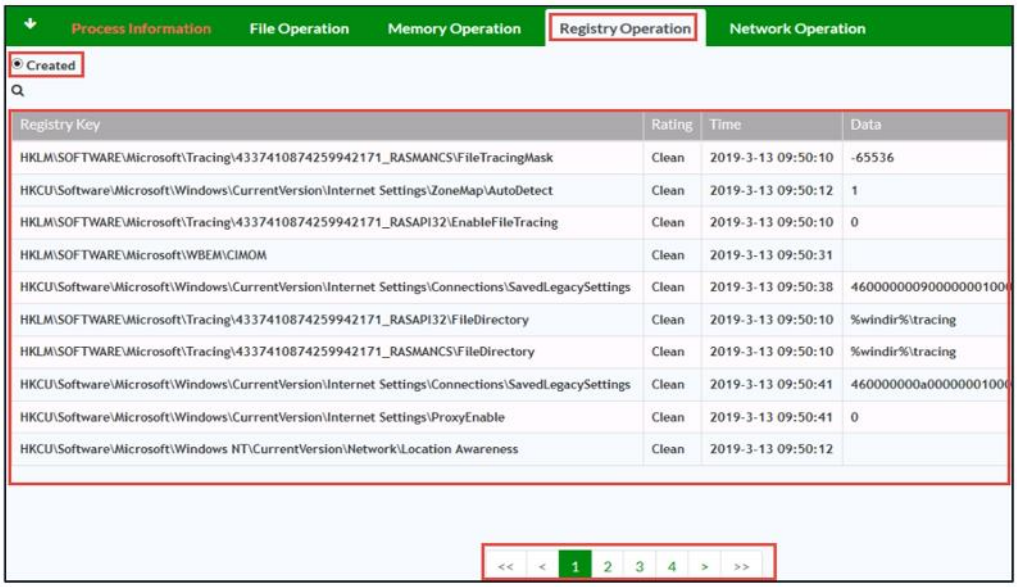


Now, you will learn about the **File Operation** tab. On this tab, you can see the files created, deleted, and modified when the executable was running. You will notice that a copy of the malicious file was created in the **SYSTEMDRIVE** and it matches the MD5 hash value of the original file.

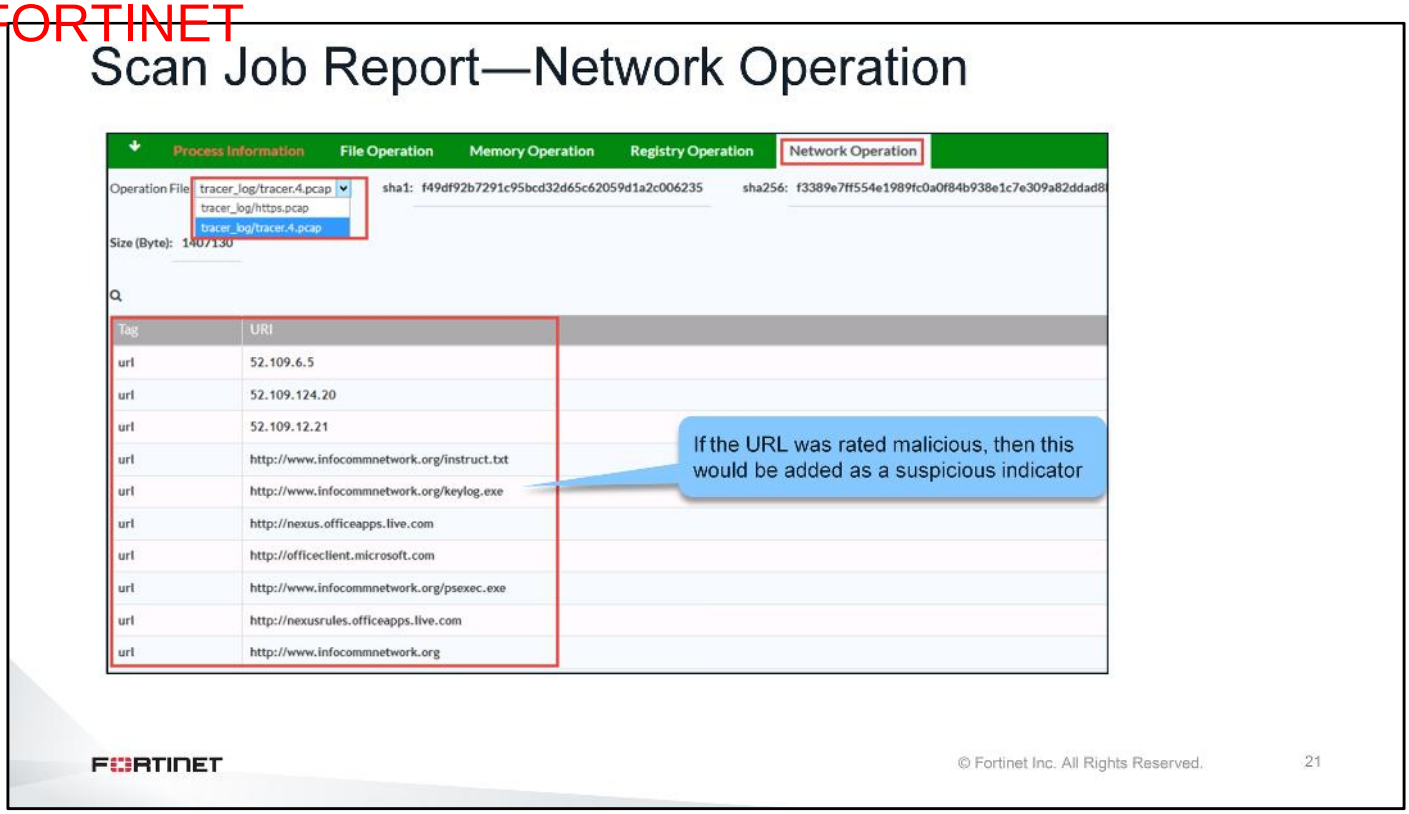


Now, look at the **Memory Operation** tab. Here you can see the processes created, injected, or written when the executable was running.

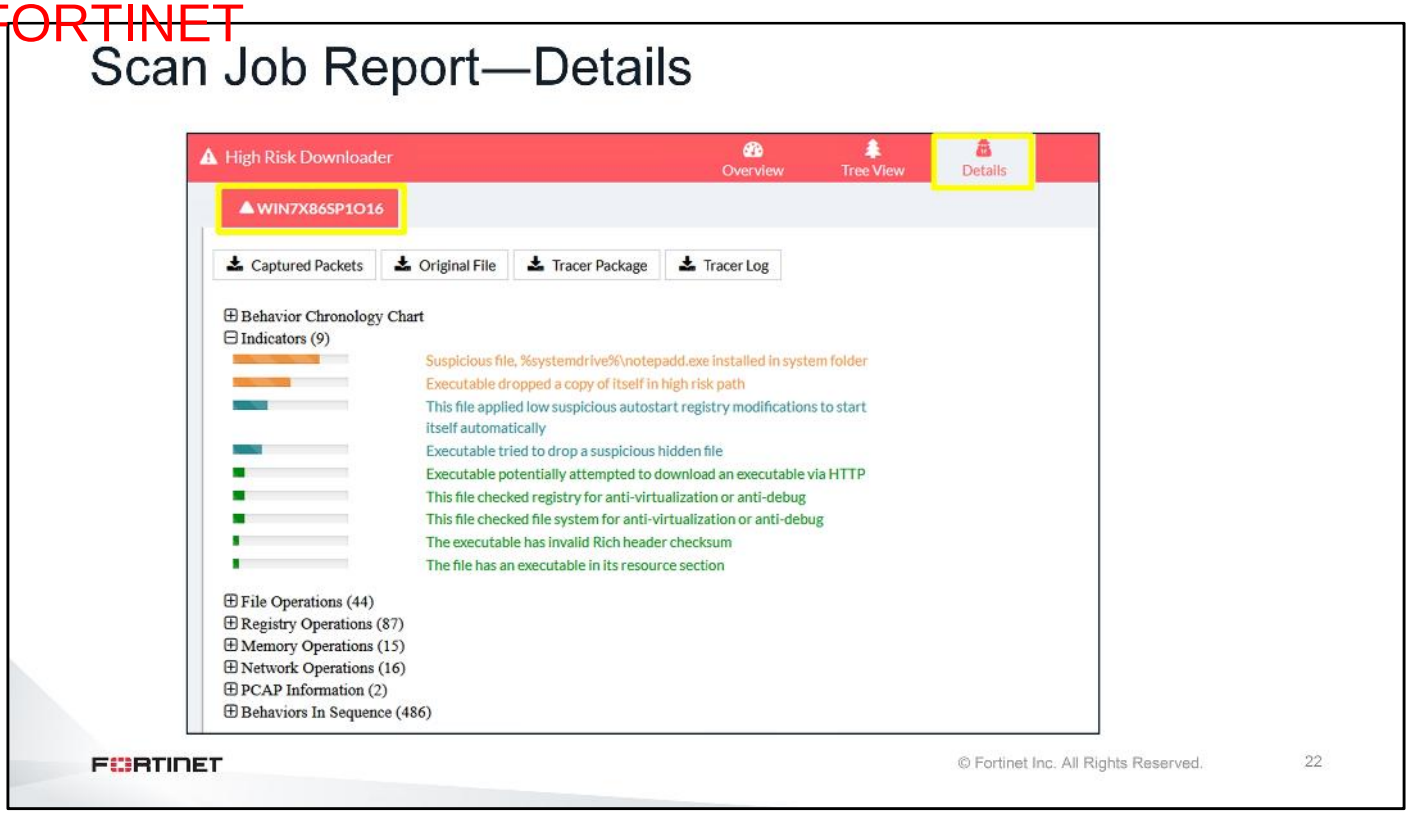
Scan Job Report—Registry Operation



Now, look at the **Registry Operation** tab. Here you can see the registry changes that occur when the process was running.



Now, you will examine the **Network Operation** tab. Here you can see the URLs that were requested when the sample ran. Each tab has a search feature that allows you to filter for specific information.



The **Details** view shows analysis details for each detection OS that is launched during the scan. The details of each detection OS will be shown on a separate tab. The infected OS will have an infected VM icon in its tab title. If the malware is detected by a non-sandboxing scan, such as FortiGuard static scan, the tab title is displayed as N/A.

Analysis Details—Download Options

- You have the ability to download all the information that was captured when the file was analyzed
- This is useful if you want to analyze the file further, outside of FortiSandbox
- The information that is available depends on the analysis
  - If the sample doesn't make any network connections, the **Captured Packets** button is not displayed

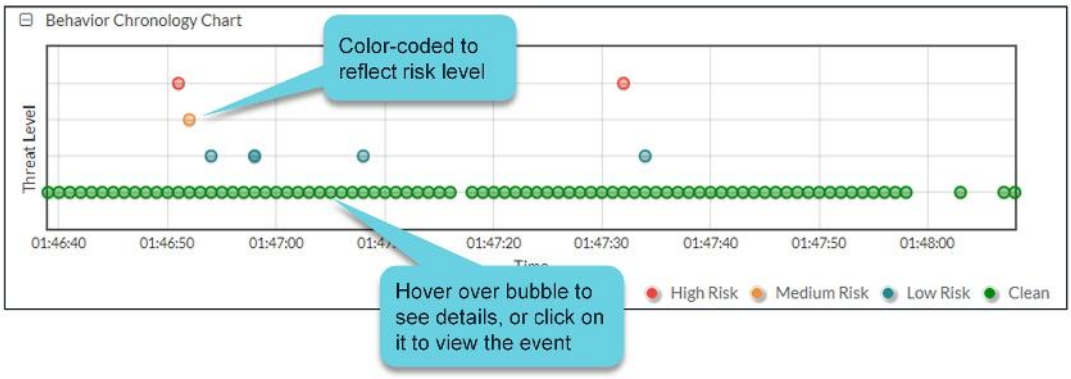
23

The options available for download will depend on the analysis.

- **Captured Packets**: This is the network traffic that was captured when the sample was running. This is in standard pcap format, which can be opened with WireShark or other packet analysis software.
- **Original File**: This is the file that was analyzed
- **Tracer Package**: This is the tracer log, dropped files, and other information.
- **Tracer Log**: These are the logs containing detailed information collected inside the guest VM.

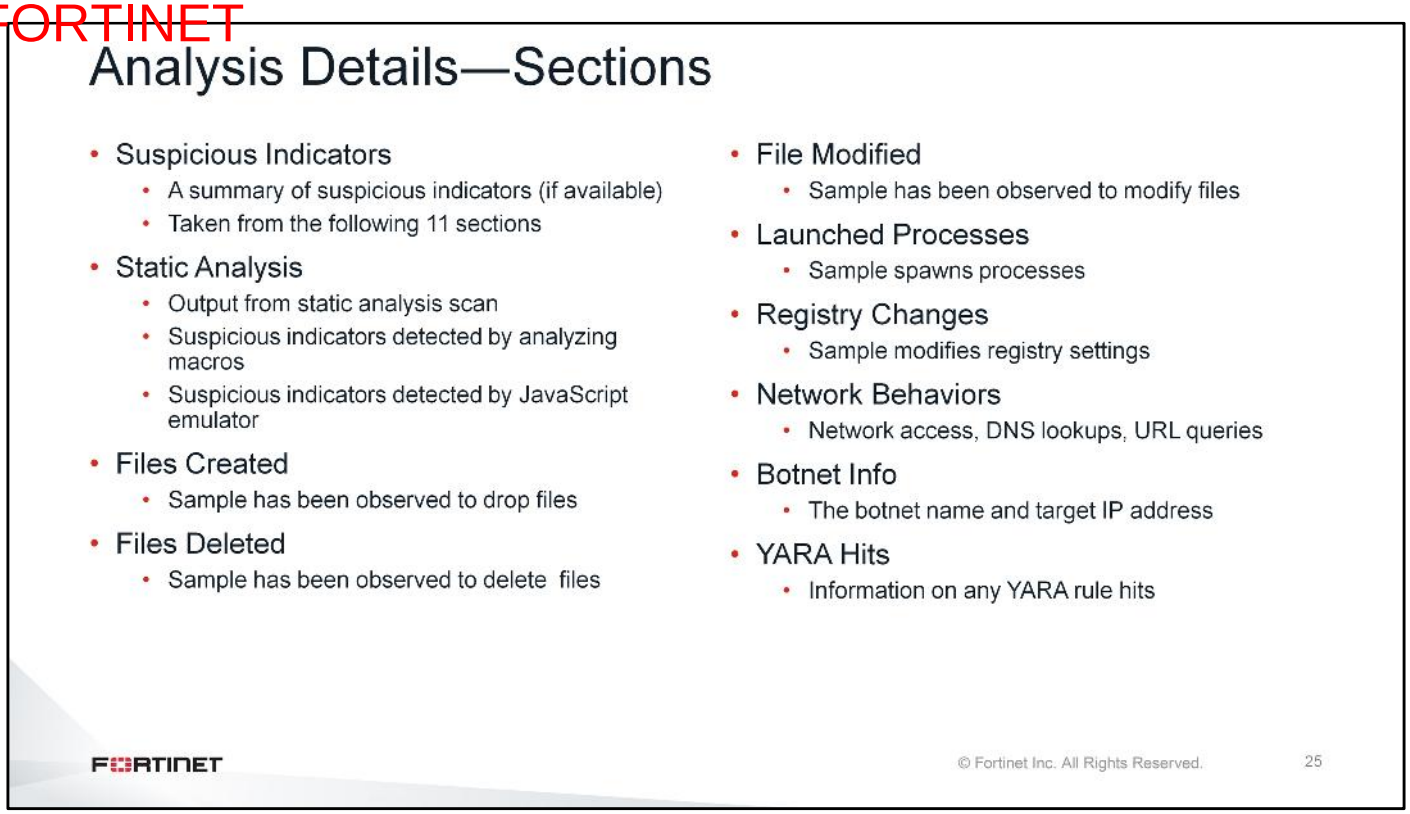
Analysis Details—Behavior Chronology Chart

- The **Behavior Chronology Chart** shows the file's behavior over time during the execution



24

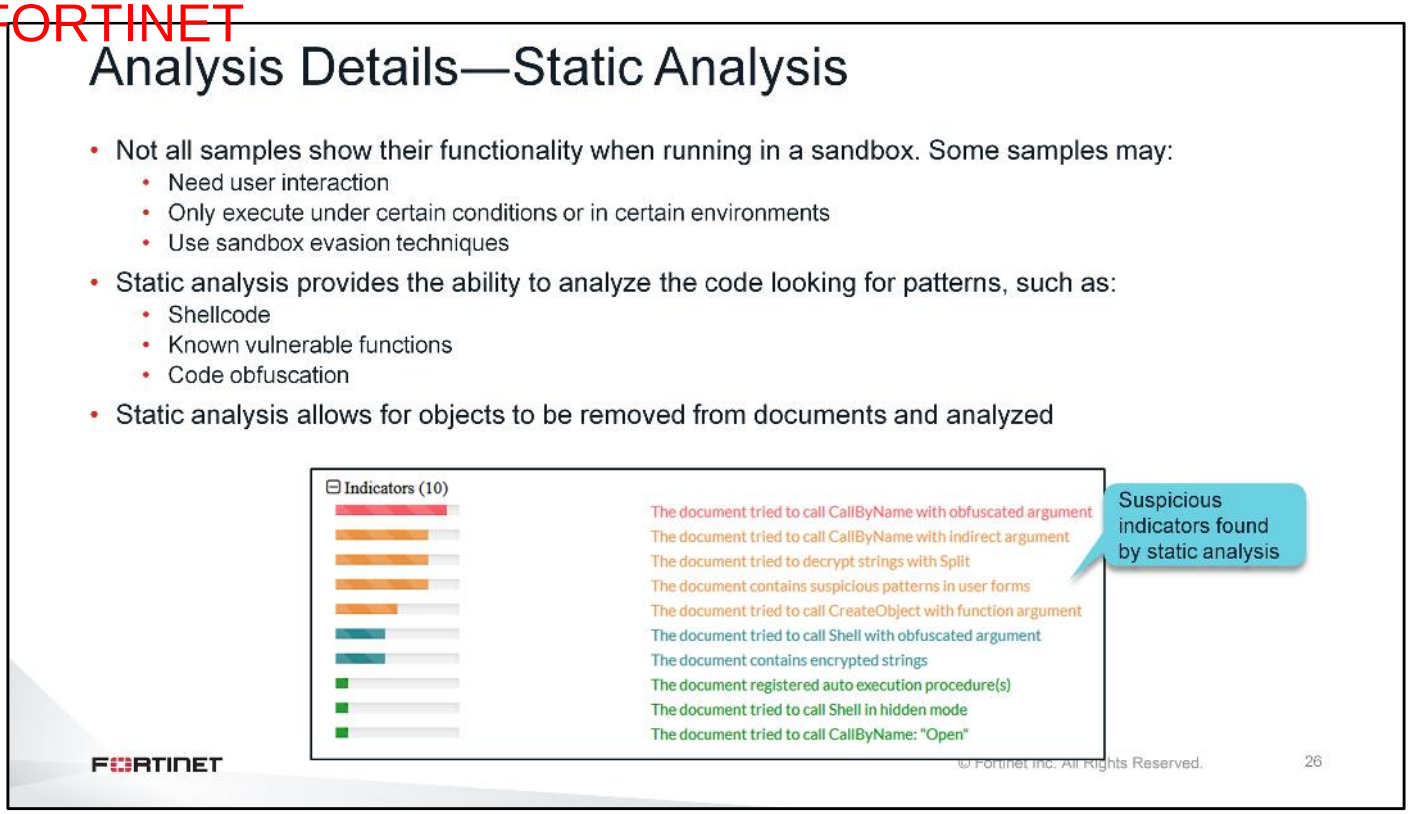
The **Behavior Chronology Chart** shows the file's behavior during the time it was executed. Clean behaviors are represented by a green bubble, and suspicious behaviors are represented by red (high risk), orange (medium risk), or blue (low risk) bubbles. The higher the bubble, the more serious the event is. Hover your mouse over the bubble to view the event details.



After the **Behavior Chronology** chart, there are other possible sections.

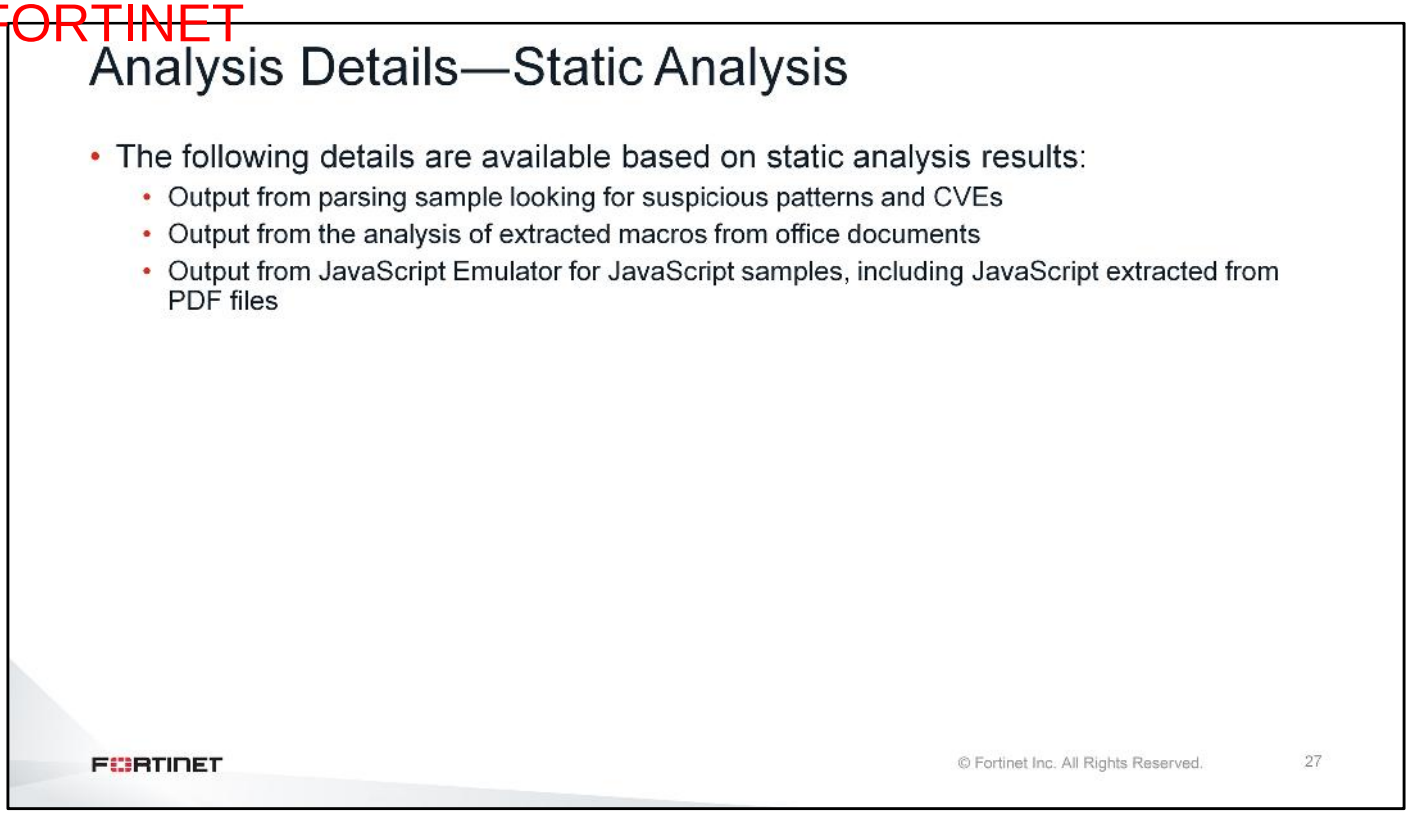
If a sample doesn't exhibit behaviors included in a section, that section is not included. For example, if FortiSandbox did not detect any registry changes, the scan job report will not include a section for registry changes.

This slide shows the common sections that are available, based on the behaviors seen when analyzing a sample. Expanding each section shows the behaviors observed for that section.



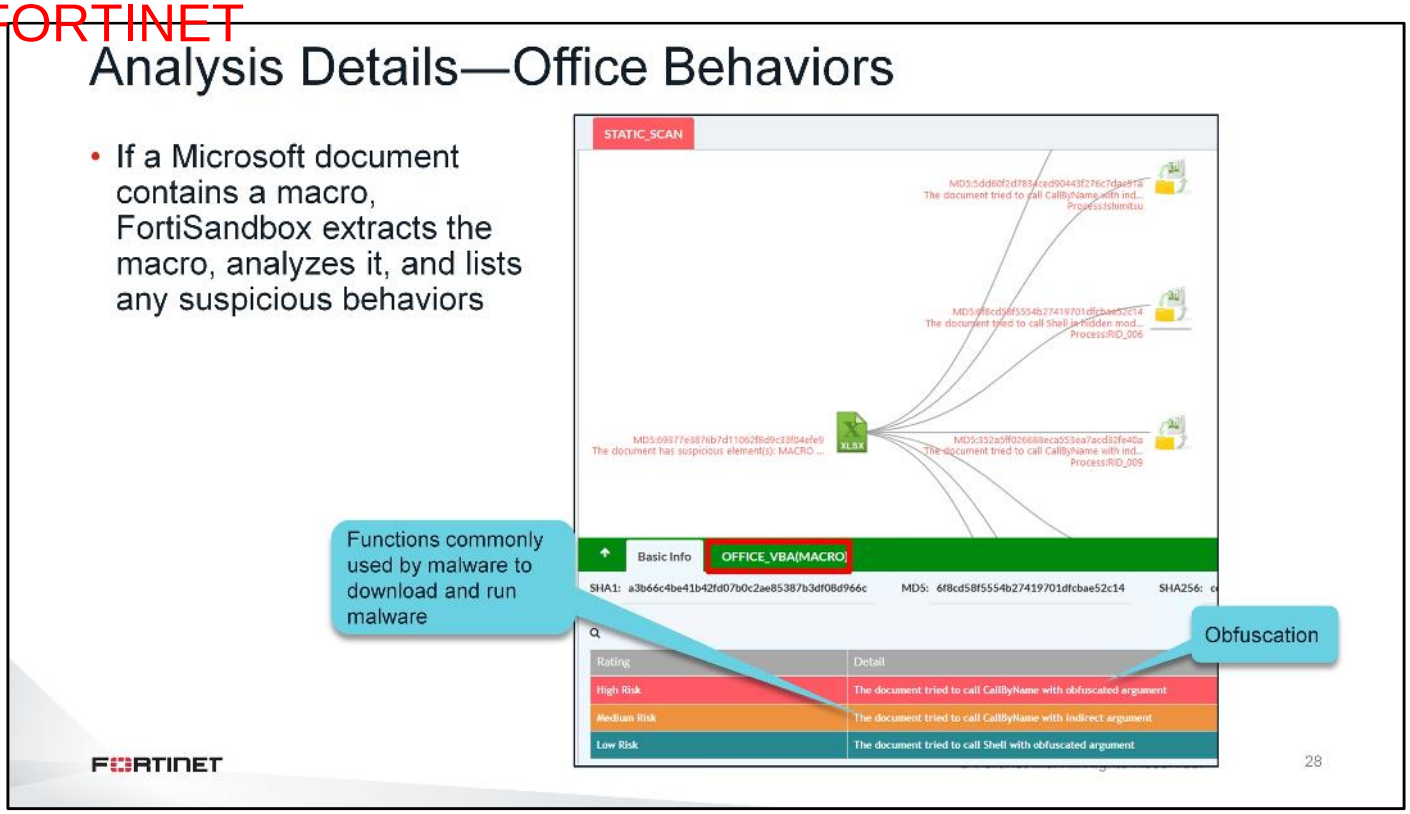
The goal of both static and dynamic analysis is to figure out if the sample is malicious. Searching through the code can be a simple way to learn more about the functionality of a program. For example, if the program accesses a URL, then you will see the URL stored as a string in the code. For executables, static analysis can look for strings, and whether or not it contains additional binaries.

The static analysis scan encompasses a few features, one of which is to statically scan samples looking for patterns. In this example, you can see a JavaScript file where the static analysis has detected shell code patterns, as well as exploit code for known vulnerable functions. Shell code is what will be executed after exploiting a vulnerability.



The static analysis section displays results based on:
- Parsing sample for malicious patterns and CVEs
- Analysis of extracted macros from office documents
- The JavaScript Emulator for JavaScript samples or JavaScript extracted from PDF files

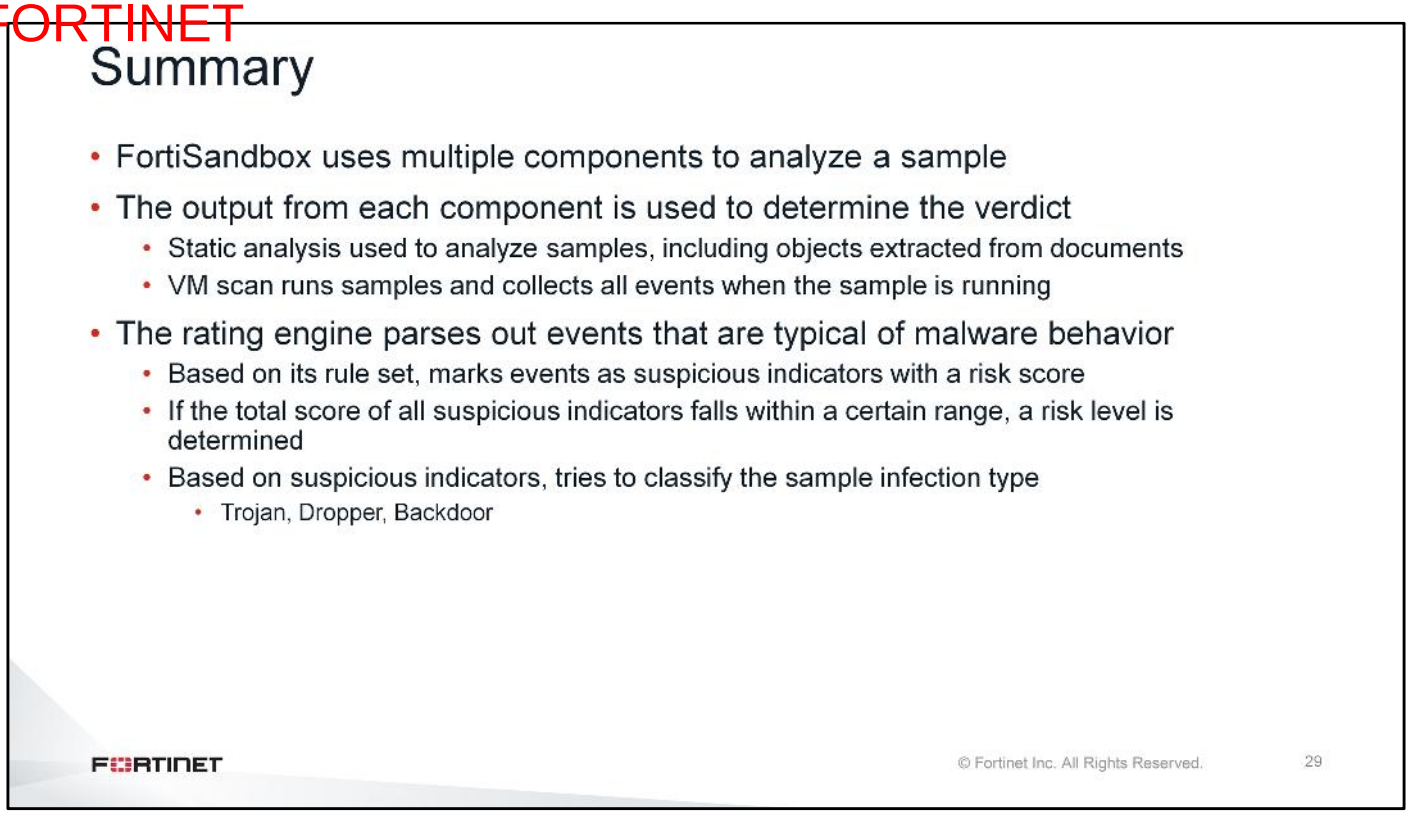
The rest of the sections are populated by results from the VM scan.



If a Microsoft document contains a macro, FortiSandbox extracts the macro, analyzes it, and lists any suspicious behaviors.

The example on this slide shows some of the ActiveX functions that you learned about earlier in this lesson. The macro automatically executes when the document is opened. Once executed, it has access to the file system and the windows shell. The macro can use this access to run a program locally or perform other functions, such as manipulate registry contents.

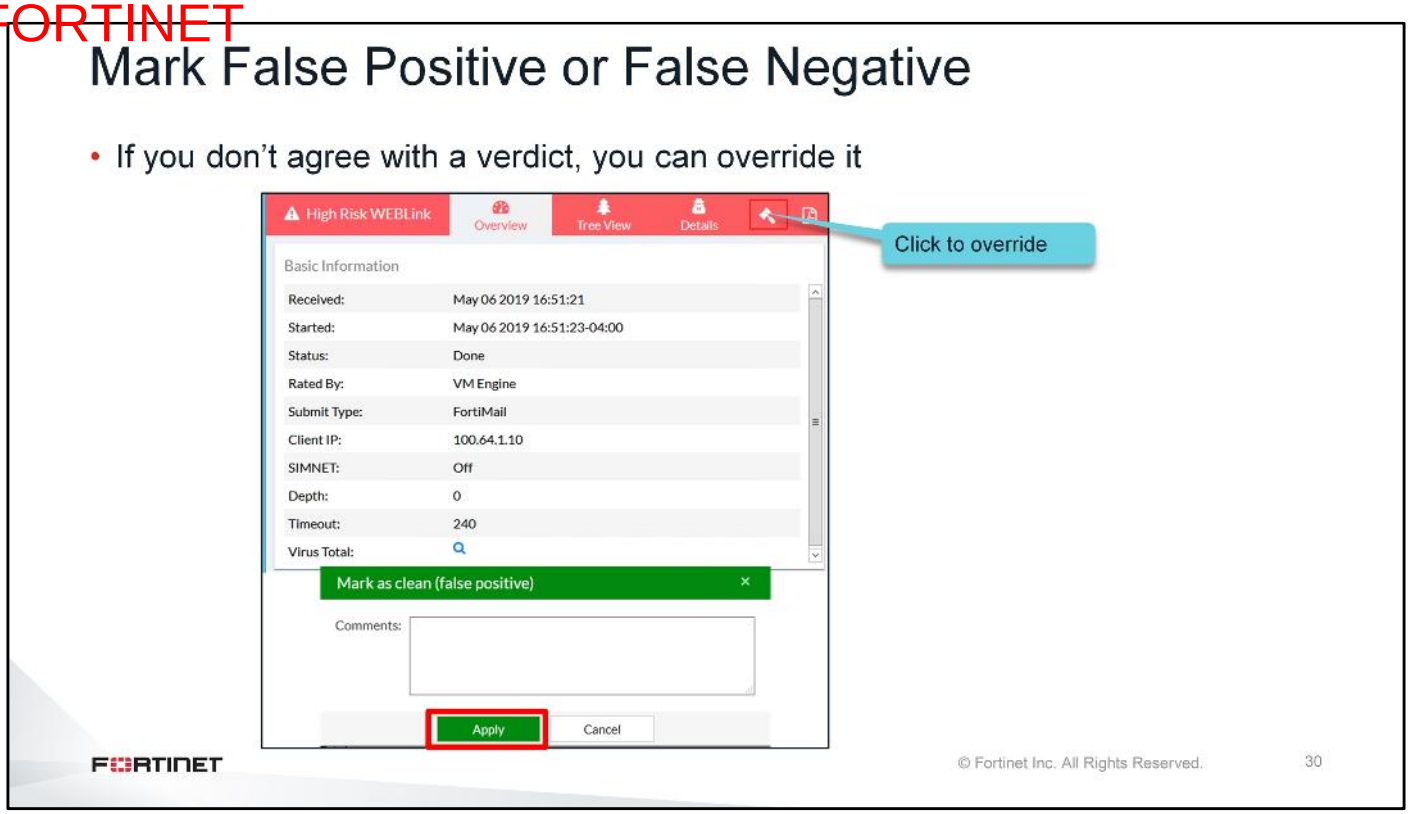
Note that FortiSandbox has detected that the macro is also using some obfuscation.



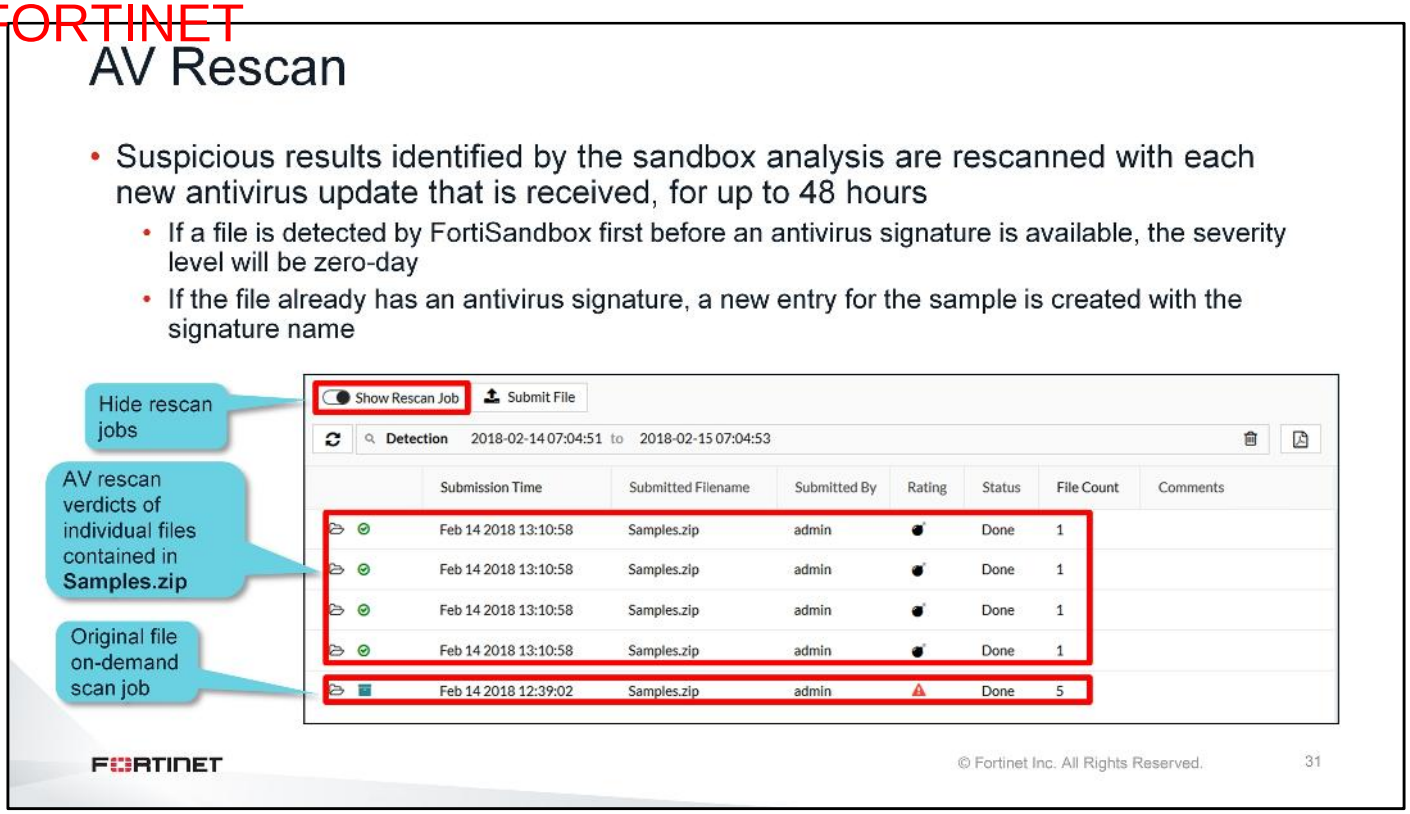
FortiSandbox uses multiple components to analyze a sample. The output from each component is used to determine the verdict.

Static analysis is used to analyze samples, including objects extracted from documents. VM scan runs samples and collects all events when the sample is running.

The rating engine parses out events that are typical of malware behavior and marks events as suspicious indicators with a risk score. If the total score of all suspicious indicators falls within a certain range, a risk level is determined. The rating engine also tries to classify the sample infection type based on those suspicious indicators.

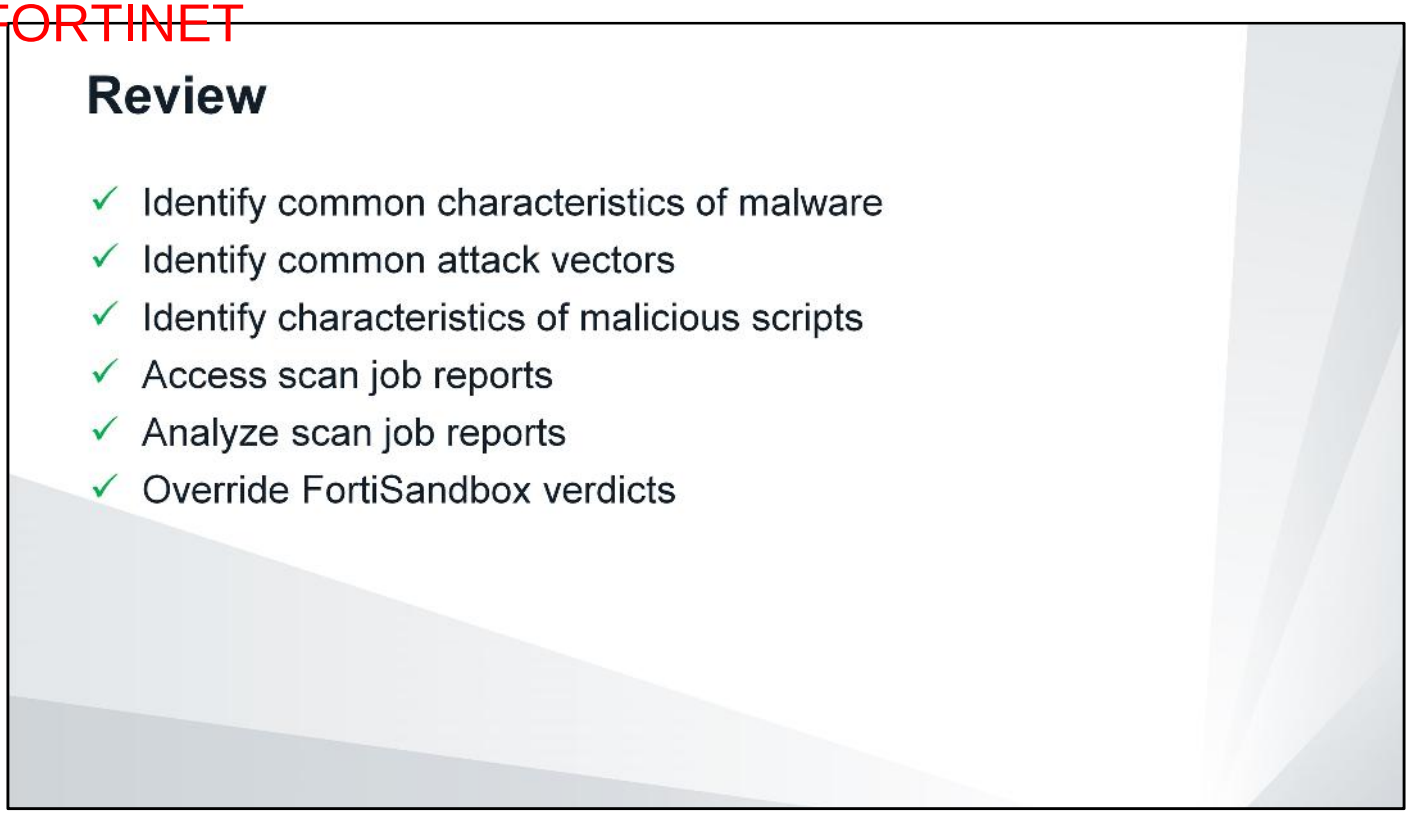


If you don't agree with a verdict, you can mark it as either false positive or false negative. Note that you also have the option to send the feedback to the FortiSandbox cloud community. For example, if you override a suspicious file rating by FortiSandbox as clean, and if the sample is found to be clean by the FortiGuard team, any other user submitting the same sample will get a clean rating from the cloud community.



When a new antivirus update is received, FortiSandbox will recheck all samples that were not detected by the previous database version, and update their ratings. This will create multiple entries of the same files, as shown on this slide.

The original entry is marked by the suspicious rating. The AV rescan jobs are marked with a malicious rating.



By mastering the objectives covered in this lesson, you learned how FortiSandbox generates verdicts for samples.