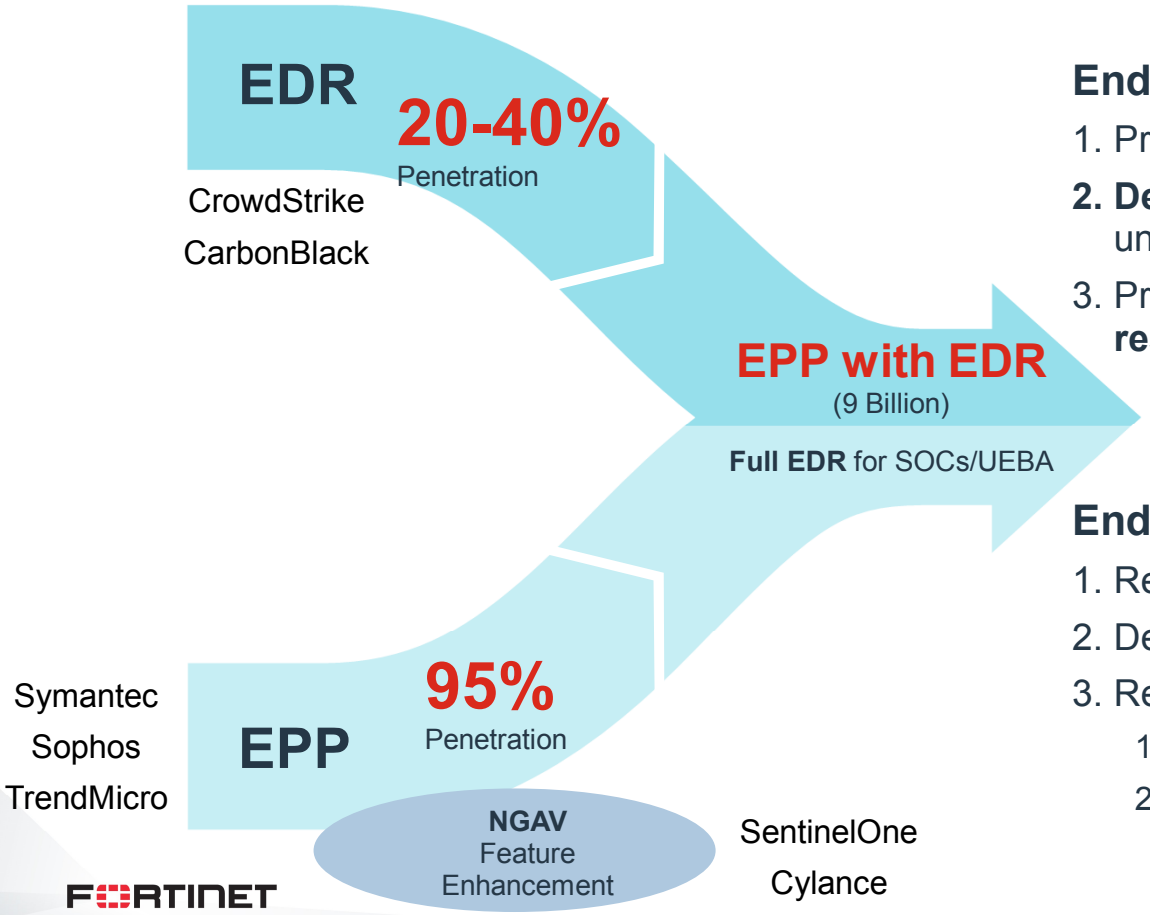
FortiEDR
Real Time Endpoint Protection

Tsailing Merrem

Anthony Giandomenico

Evolution of EPP

Advanced Endpoint Protection Platform (EPP) with Automated Detection and Response Capabilities



Endpoint Protection Platform (EPP)

1. Prevent file-based malware
2. **Detect** and block malicious activities from *trusted* and untrusted applications
3. Provide the investigation and remediation capabilities to **respond** to security incidents and alerts

Endpoint Detection and Response (EDR)

1. Record and store endpoint behaviors and events
2. Detect security incidents
3. Response
    1. Containment and remediate
    2. Forensic—investigate security incidents, root cause analysis

FORTINET

Pain Points

Compromised endpoints

- There is no 100% prevention
- Threat landscape - Ransomware, data theft, business disruption
- Need better detection. Reduce time to contain, time to remediate

Incident response – cost, pain and business disruption

- **We all want to stop the breach, but at what cost?**
- Alert fatigue, false positive
- Blunt tools and Manual response
- Business disruption, machine off-line, lost of productivity, user complaint

Not enough security expertise in house, other resource constrains

- Need to accelerate SOC maturity,
- Need to scale SOC capacity
- Don’t have time to patch, can’t upgrade all machines

Complex security eco system, too many point solutions

- Need Integrated solution

To Automate or Not to Automate?

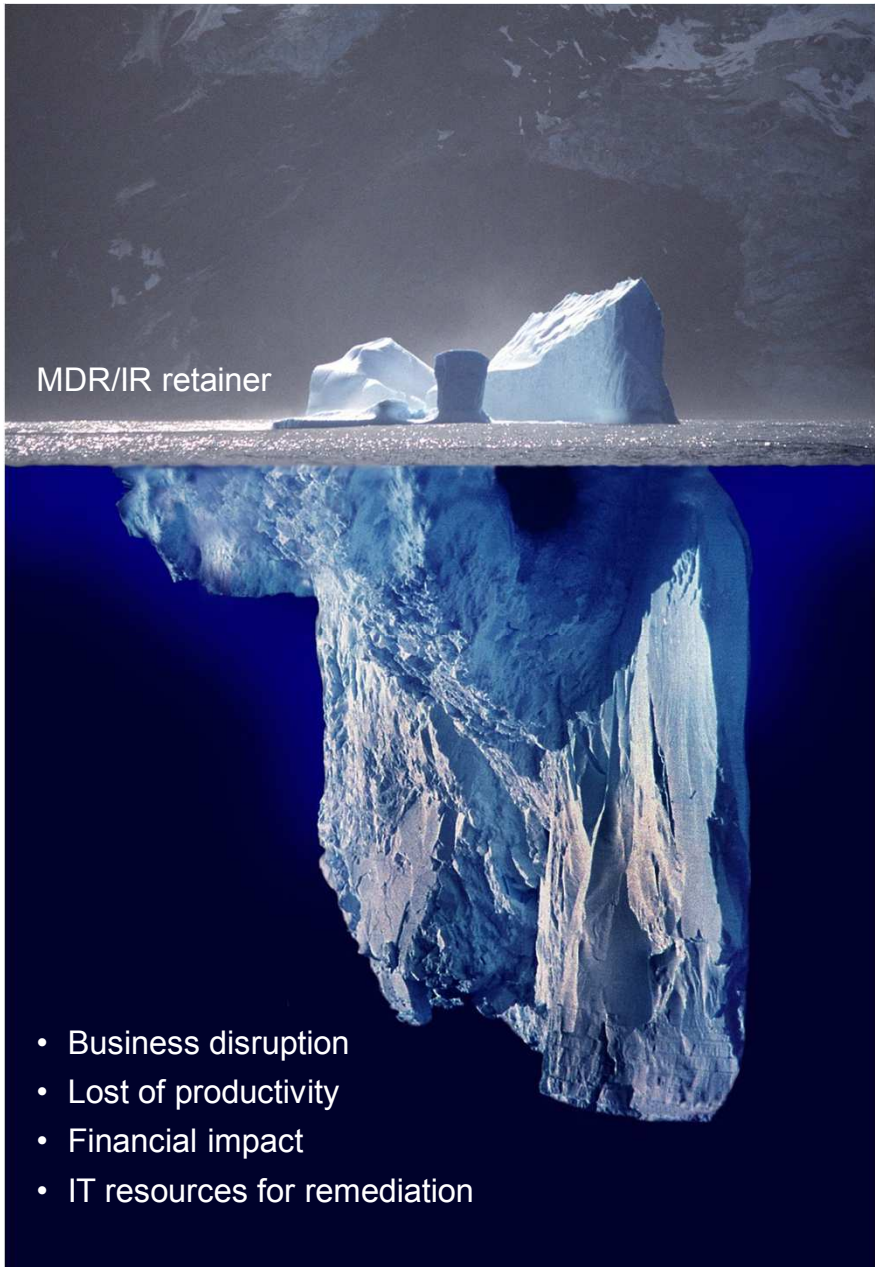
Manual Process – by First Generate EDR

- Time to respond?
- Manual remediation
- Re-image?
- Alert fatigue

vs.

Automated but Blunt

- False positive?
- Blunt tools – endpoint quarantine
- Business disruption
- Machine offline?



FortiEDR – Real-time Endpoint Protection at Pre- and Post-Infection

Pre-Infection

Discover & Predict

Proactive risk mitigation

- Discover rogue devices & IoT
- Application and reputation
- Vulnerabilities
- Risk-based policies reduces attack surface
- Virtual patching

Prevent

Pre-execution protection

- Kernel-level
- Machine learning & Signature-less
- Application communication control
- Eliminate data tempering and exfiltration

Post-Infection

Detect

Detect threats in real time

- No alert fatigue
- Provide malware classification
- Display IOC's
- Deliver full attack chain

Defuse

Stop Breach and data loss

- First and only real-time post infection blocking
- Block outbound communication
- Prevent data exfiltration
- Prevent data tempering and ransomware encryption

Respond & Investigate

Full attack visibility

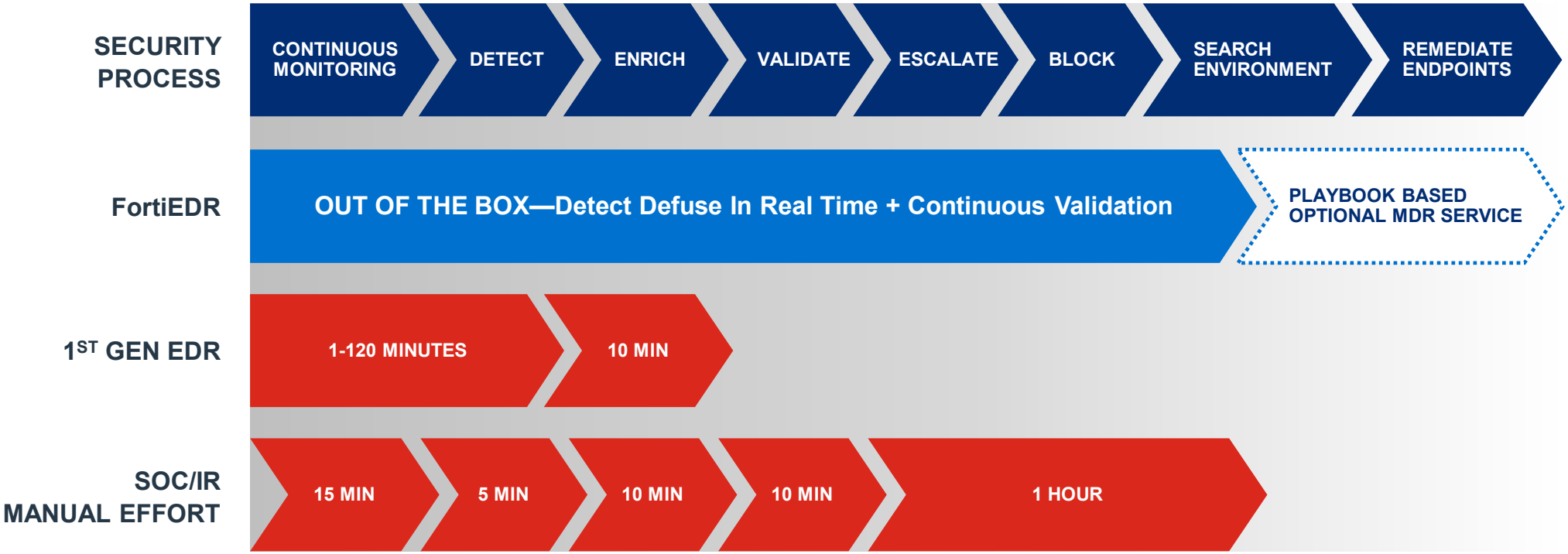
- Customizable incident response playbooks
- Eliminate dwell time
- Capturing forensic data
- Memory snapshot for file less attack
- Conduct threat hunting in your time

Remediate & Roll back

Dis-infection

- Rollback malicious changes
- Remove bad files
- Clean up persistency
- Eliminate re-image/rebuild
- Ensure business continuity
- REST API output for external remediation tools

FortiEDR Automated vs. Manual EDR

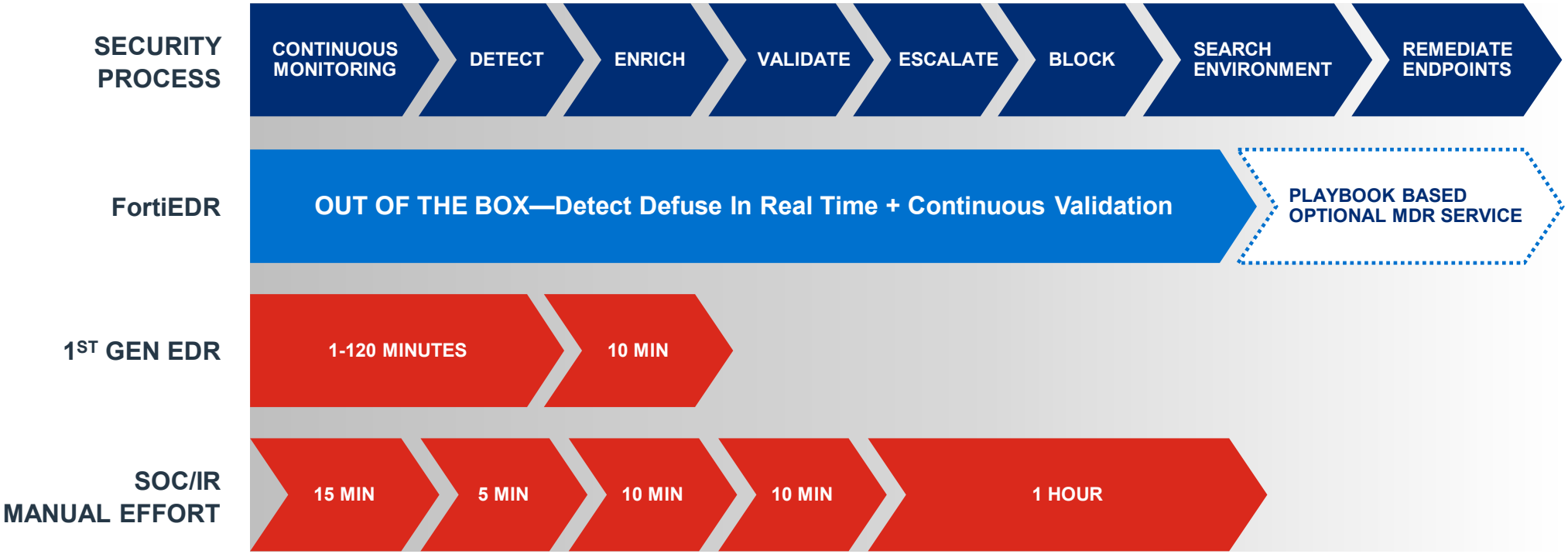


Advanced Endpoint Protection, Detection and Response

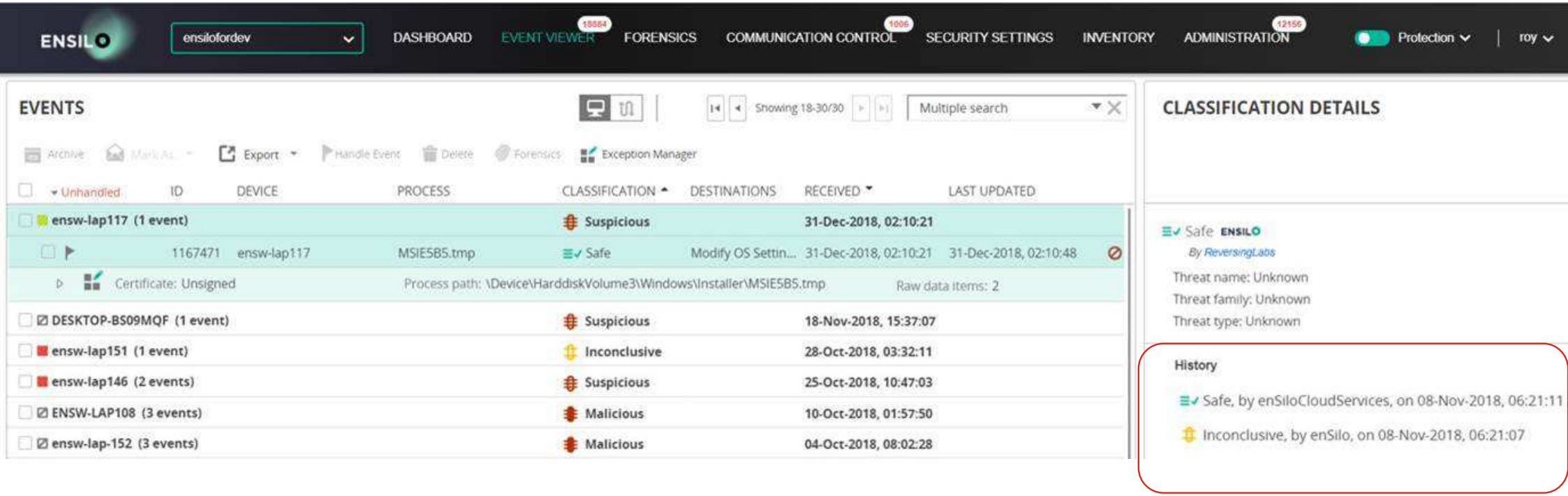
Table stakes vs. extra mile

Prevent	Detect	Respond	Predict/attack surface reduction
File based malware Signatureless Pre-executive protection Detect and block exploits	Behavioral based detection for File-less attacks/ living off the land attacks	**Respond** to security incidents Alert Triage Containment Remediate Investigate Optional MDR services	Discovery Visibility Vulnerabilities
• Pre- and ***post-infection*** protection	• ***Defuse*** potential threats automatically • Stop ransomware damage • Continuous validation • No business interruption	• Automated Response & Remediation • Playbook Orchestrated • Memory snapshot for forensic investigation	***Attack Surface reduction*** Discover Applications Rogue devices and IoT **Virtual patching**

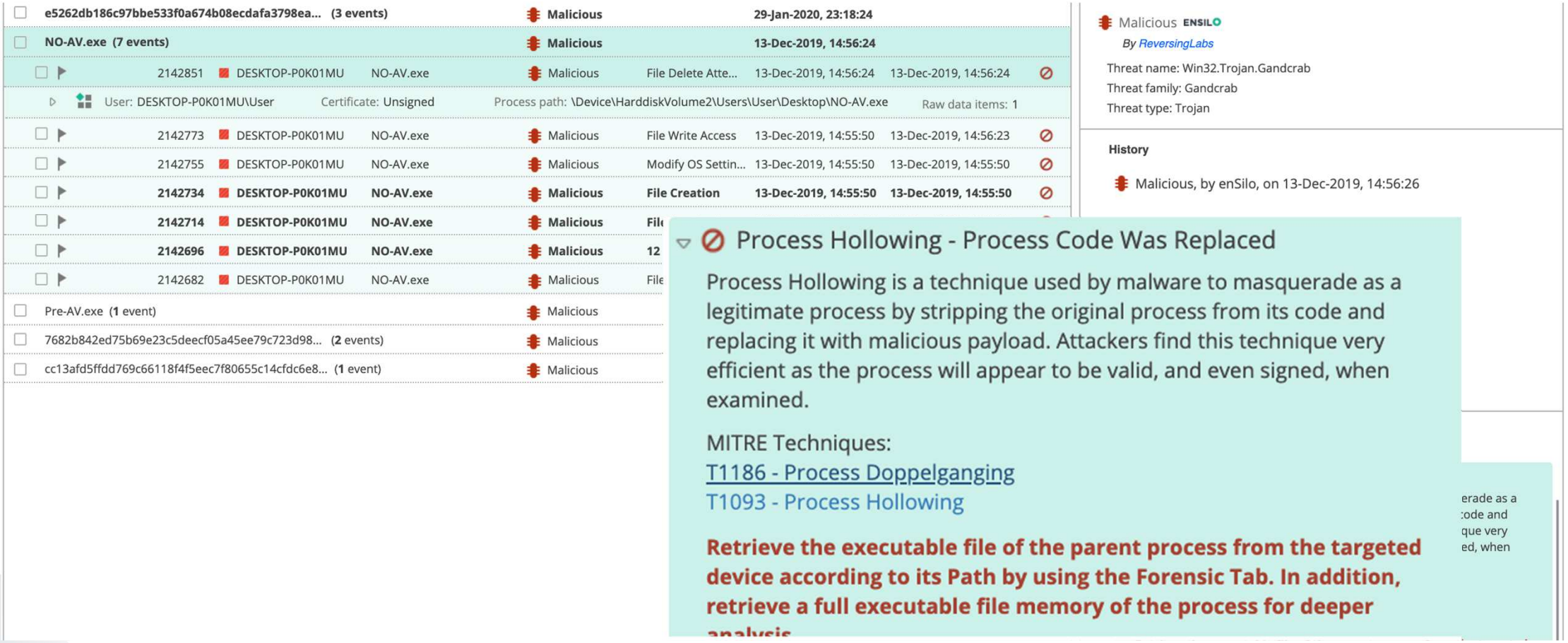
Automated vs. Manual



Reduce Noise, Boost SOC maturity



Guided Interface



Customer Reviews

"EnSilo Is The First Product In My 15 Year Career That Makes Me Think We Have A Chance."

CISO in a financial industry

"EnSilo is efficient in all aspects. The agent has almost no overhead, the management interface provides detail without needing to dig, and most importantly, blocking occurs with minimal user impact."

"Successfully Regain Advantage Over Malicious Actors"

Sr. Security Analyst from manufacturing

"The zero-day capabilities are outstanding. Changes the table on suspicious activity from "Opt out" to "Opt In" -- suspicious activity is stopped and only allowed after activity analysis."

Source: Gartner (December 2019)

FortiResponder Services

Managed Detection and Response
Incident Response Services

Our Team is comprised of individuals with strong knowledge in:

- Malware Hunting/Analysis Reverse Engineering
- Multiple Scripting Languages
- Forensics
- Incident Response Processes
- Threat Actors TTPs
- Chinese and Russian

Customers

32 Customers/600,000+ Devices


Team Focus
Preparation
Planning
Process
Technology
People
Testing
& Training
Deploy
?
Detection &
Analysis
Response
FortiResponder Services
Recover
Reporting and Lessons Learned…
No
Yes
No
Recovery?

FortiResponder Managed Detection and Response

24x7 Monitoring and Response

Continuous
Monitoring

FortiResponder MDR provides organizations with 24x7 continuous threat monitoring, alert triage, and incident handling by experienced analysts and the FortiEDR platform

Available as an add-on subscription or as part of:

- *FortiEDR premium bundle for servers*
- *FortiEDR ultimate bundle for endpoints*

Incident Response Workflow

Detect & Block

FortiEDR agent detects and blocks malicious activities at the endpoint

Cloud Analysis

Related events and files are submitted to FortiEDR Cloud for analysis and further inspection

Classification & Confirmation

Upon analysis a final verdict is made on the event

Automated Response

If malicious disposition is made, automated playbooks are executed:

- Notify user
- Open ticket
- Remediate, etc.

Investigate

Events may require further inspection, FortiResponder teams are there to assist

Managed Detection and Response Task List

- Review & analyze FortiEDR alerts on a 24 x 7 basis with a 24-hour response time SLA
- Validate and (re)classify threats (Malware Analysis)
- Investigate and report on previously unknown malware and PUPs (Malware Analysis)
- Investigate and report on potential vulnerable applications
- Set micro exceptions for clean applications
- Make recommendations for review and remediation
- Quarterly Environment Reviews

Investigate

Events may require further inspection, FortiResponder teams are there to assist

Trusted Advisor (TA)

Planting a team of TAs 24/7 365 to help drive "PULL THROUGH REVENUE."

TRUSTED

ADVISOR

FORTINET

SECURITY FABRIC

FortiResponder Incident Response

Additional IR Hour SKU

Per Incident

Forensics and Incident Response

SOW-based remote forensic analysis and incident response

Ideal for customers running FortiEDR who do not already have continuous monitoring subscriptions

Assists clients with the analysis, response, containment and remediation of security incidents to decrease the time to resolution limiting the overall impact to an organization.

Benefits

FortiResponder Service

Accelerate SOC Maturity

24/7 - Scale the Existing SOC

Reduce Analyst Burnout

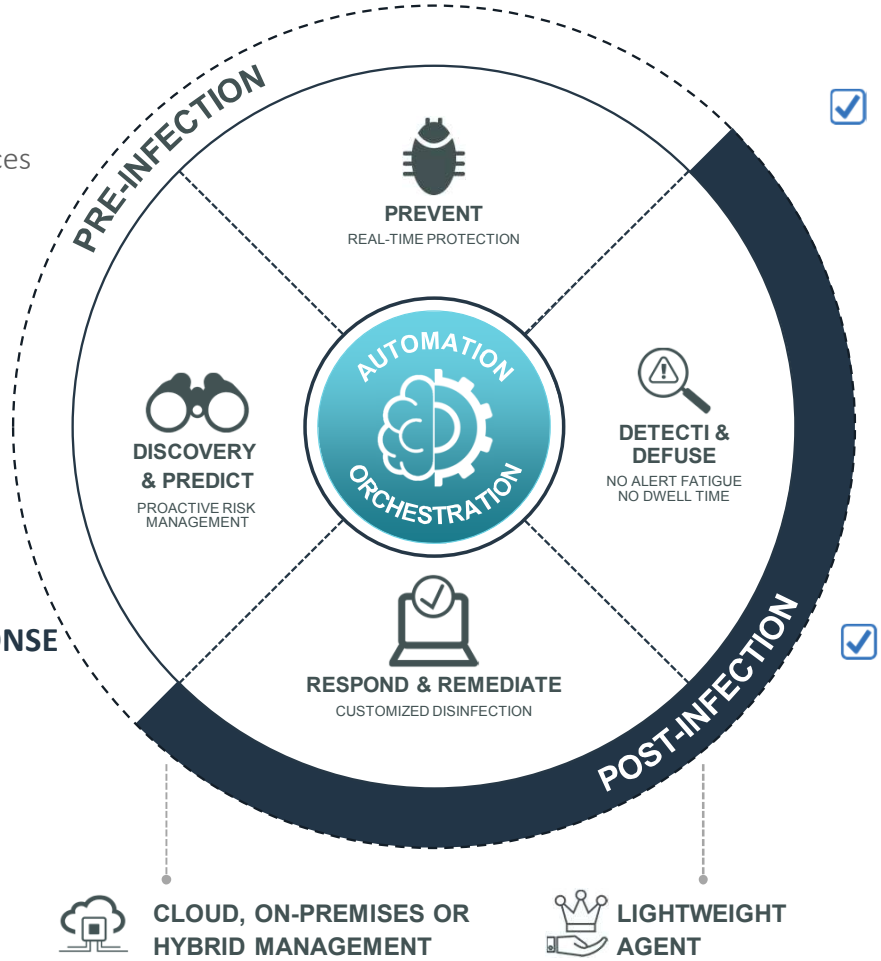
Real-time Automated Security with Orchestrated Incident Response

REAL-TIME PROACTIVE RISK MITIGATION

- Discover and track applications and IoT devices
- CVE and application rating data enrichment
- Risk based proactive policies enabling attack surface reduction

REAL-TIME ORCHESTRATED INCIDENT RESPONSE

- Automated event classification
- Automated remediation (notify users, isolate device, remediate device, open ticket)
- Automated investigation with minimal interruption for user



REAL-TIME PREVENTION

- Machine learning, Kernel-based Next Generation AV
- Feeds from a continuously updated cloud database
- Real-time automated prevention of ransomware encryption

REAL-TIME DETECTION AND DEFUSION

- Automated post-infection detection and blocking
- OS-centric technology
- Analysis of entire log history
- Surgical containment


FORTINET

FortiEDR vs. Competitors

FortiEDR delivers comprehensive, fully automated protection, detection and response

	Fortinet FortiEDR	Crowdstrike	CarbonBlack	Sentinel One	Symantec
AUTOMATED PROTECTION					
Vulnerability scanning and virtual patching	●	◑ Requires add-on, no remediation options	◑ Requires LiveResponse	◑ no remediation options	◑ Requires add-on and Windows 10 only
Real-Time, **Pre-Execution** Blocking (AV)	●	●	●	●	●
Real-Time, **Post-infection** protection	●	No, detect only and no real-time blocking	No, detect only and no real-time blocking	No, detect only and no real-time blocking	No, detect only and no real-time blocking
AUTOMATED EVENT MANAGEMENT					
Orchestrated & Automated Response	●	○ Manual	○ Manual	◑ Limited, not orchestrated	○ Manual
Remediation in **real time**	●	○	○	○	○
Eliminate Dwell Time and Alert Fatigue	●	○	○	○	○
Available **on-premises** or in the **Cloud**	●	Cloud-only	◑	◑	◑

Electronic Manufacturer

Challenges

- Threat bypass the existing AV solution
- Under continuously state of attacks - 3% infection rate
- Ransomware attacks cause disruption of production
- Vulnerable systems with legacy manufacturing applications

Requirements

- Effective endpoint protection, detect and block ransomware
- Support legacy platforms
- Business continuity, system availability

Business outcome

- Immediately identified pre-existing infection
- Insure business continuity.
  - Blocked malicious activity from spreading or corrupting the manufacturing line
  - Allowed the infected devices to continue manufacturing without any service interruptions.
- Protects Legacy systems/Slimline laptops on the manufacturing floor

OT System environment

Windows legacy systems

Balance high availability and Security

Deployment size – 7,000 endpoints

Financial Services

Challenges

- The financial services industry is a constant target
- Security is perimeter-focused, and prevention only with Endpoint security focus on static file analysis at pre-execution prevention
- Fileless malware undetected for extended periods of time.
- Ransomware interrupting business continuity.

Requirements

- Upgrade security posture. Move from perimeter-focused and prevention to include detection and response capabilities.
- Ability to detect fileless malware and ransomware attacks
- Identify pre-existing infection, Isolates malware and prevent data exfiltration from stealing data.

Business outcome

- Deliver comprehensive defense that includes a first line (pre-execution prevention) and last line of defense. Protects endpoints and data even during active infection states
- Behavioral-based detection identify suspicious processes and prevents malicious activity from calling home, exfiltration of data and stem lateral movement.
- Complete visibility of attacks. enSilo provides a precise view of where the actions are initiated from, the path to the process root, and the attempted destination.
- Provide remediation and automatic roll back

Financial Services

Deployment size – 9,000 end points