



Обеспечение безопасности web-ресурсов

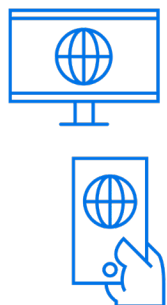
Гордеев Вячеслав



FortiWeb Web Application и защита API

Защита веб-приложений и API везде, где вы их развёртываете

Ваши
приложения
и APIs



Развернуты
в облаке и
on-premise



Представляют
бизнес-
возможности



Вашим
пользователям
в любом месте,
с любого устройства



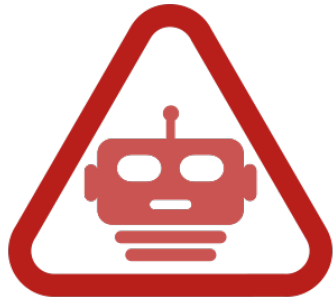
С защитой на базе
искусственного интеллекта
FortiWeb, который сводит к
минимуму ложные
срабатывания и сокращает
административные
издержки



С защитой от
Fortinet Security
Fabric с покрытием
поверхности атак
ваших приложений



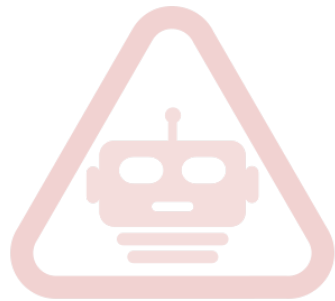
Web Application и защита API



FortiWeb решает основные проблемы, с которыми сталкиваются организации при развертывании web-приложений для публикации в Интернет:

- Защита web-приложений
- Bot Mitigation
- API Protection

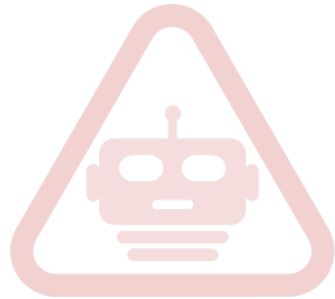
FortiWeb Web App Protection



The Web Application Firewall (WAF) сложность:

Блокировка угроз в режиме реального времени, не блокируя легитимных пользователей и не создавая ложных срабатываний, вызывающих административные издержки

FortiWeb Web App Protection

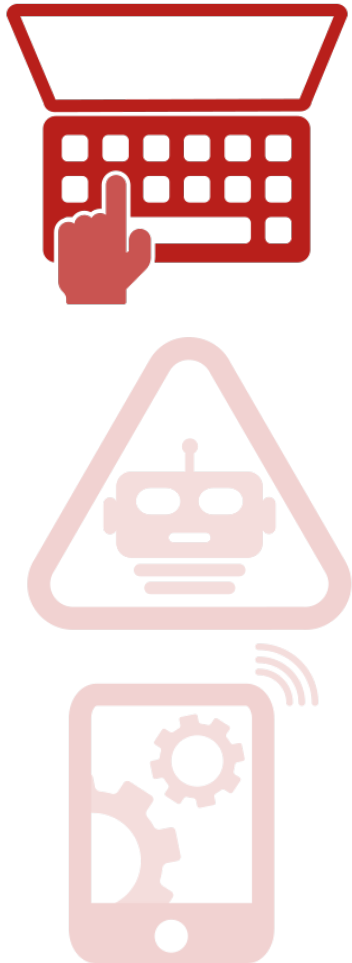


Примеры запросов, начинающиеся с:

- &==; – Python Django между параметрами!
- FooBar==POST verb – Apache с PHP
- <%I%M%u011e>== – IIS ASP Classic
- ;/path1;foo/path2;bar/;==/path1/path2/ – Apache Tomcat
- Transfer-Encoding: chunked

Ã–•£...•£`Ä%00¢—¢%00£%00–•z@•◆?”

FortiWeb Web App Protection



Решение:

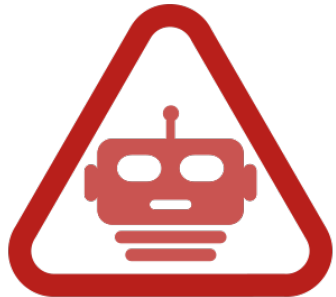
FortiWeb выявляет и блокирует угрозы с помощью комбинации:

- Машинное обучение, создающее шаблон вашего приложения для обнаружения вредоносных аномалий
- Постоянно обновляемая информация об угрозах и аналитика от FortiGuard Labs, включая обновление сигнатур атак и алгоритмов обнаружения

Преимущества:

- Защита от известных угроз, в том числе OWASP Top 10
- Защита от неизвестных угроз и угроз нулевого дня
- Снижает административные издержки за счет уменьшения количества ложных срабатываний с помощью машинного обучения
- Выполнение требований стандарта PCI-DSS 6.6.

FortiWeb Bot Mitigation



Сложности с ботами:

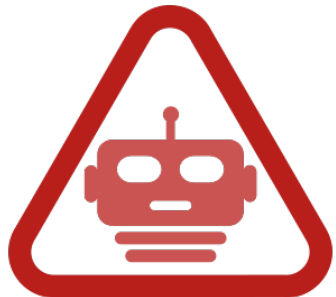
Приложения взаимодействуют как с «добрыми», так и с вредоносными ботами, и им необходимо блокировать вредоносных ботов, предоставляя управляемый доступ безобидным ботам

FortiWeb Bot Mitigation



**«Хорошим» ботам
может быть разрешено
взаимодействовать с
вашим приложением, в
том числе с:**

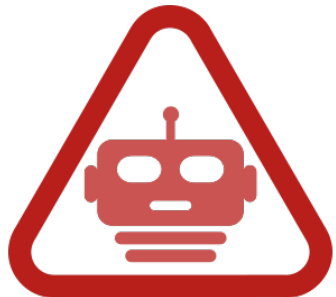
- search engines
- virtual assistants
- Chatbots
- Content aggregators
(e.g. price comparison
sites)



**Действия вредоносных
ботов могут включать :**

- web scraping
- competitive data mining
- personal and financial data
harvesting
- account takeover
- digital ad fraud
- transaction fraud

FortiWeb Bot Mitigation



Решение:

- FortiWeb выявляет и блокирует вредоносную активность ботов с помощью комбинации:
 - Sender and Request reputation – IP Reputation
 - Signatures
 - Traffic thresholds
 - Analysis of client keyboard and mouse interaction
 - Bot Deception
 - **Machine Learning**

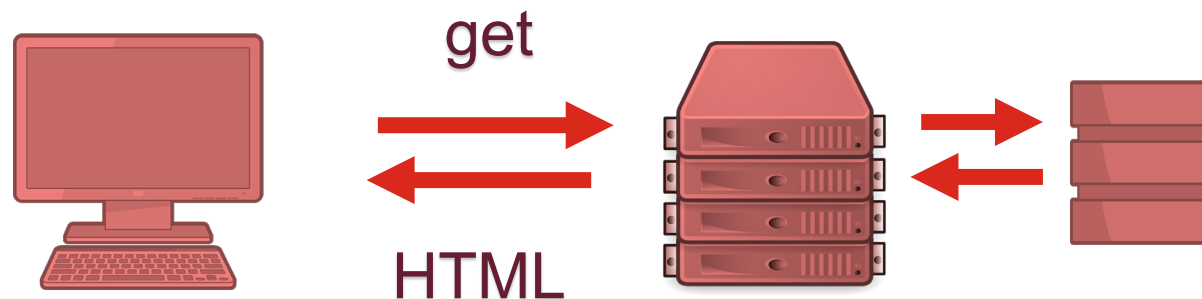
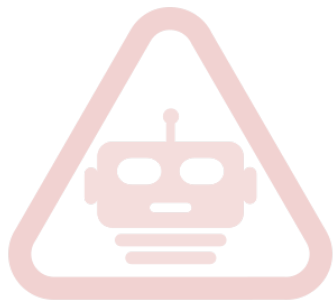
Преимущества:

- Блокирует вредоносных ботов, не блокируя пользователей и не мешая легитимной активности ботов (например, поисковые системы)
- Уменьшите или устраните зависимость от методов проверки пользователей, которые ухудшают взаимодействие с пользователем (например, ReCaptcha, формы и т. д.)

FortiWeb API Protection

Сложности с API:

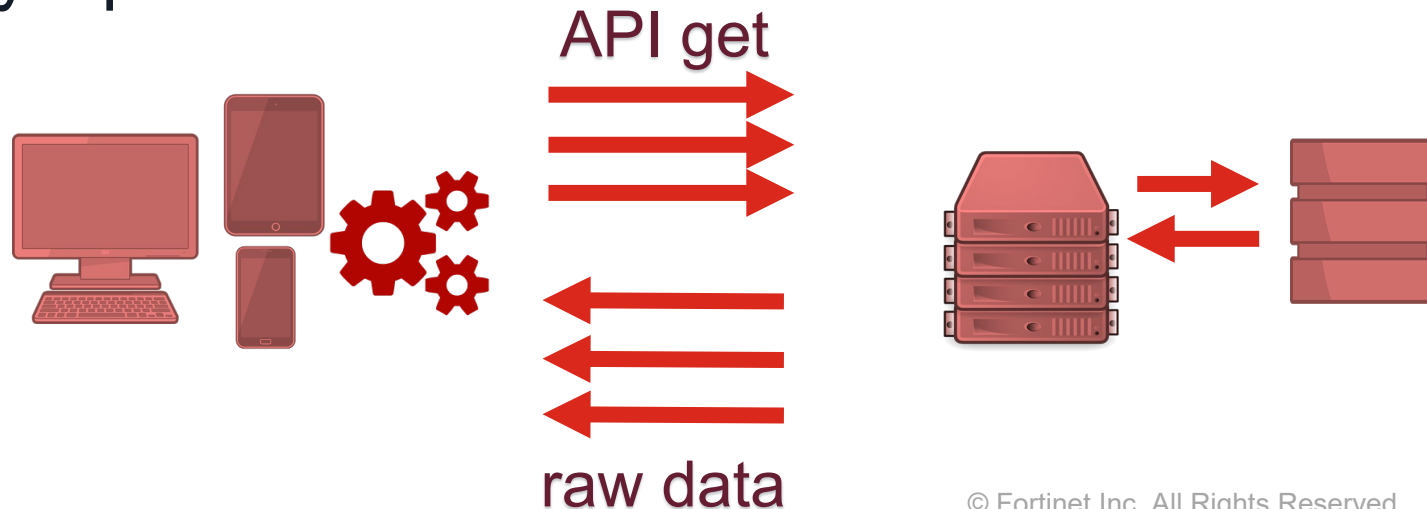
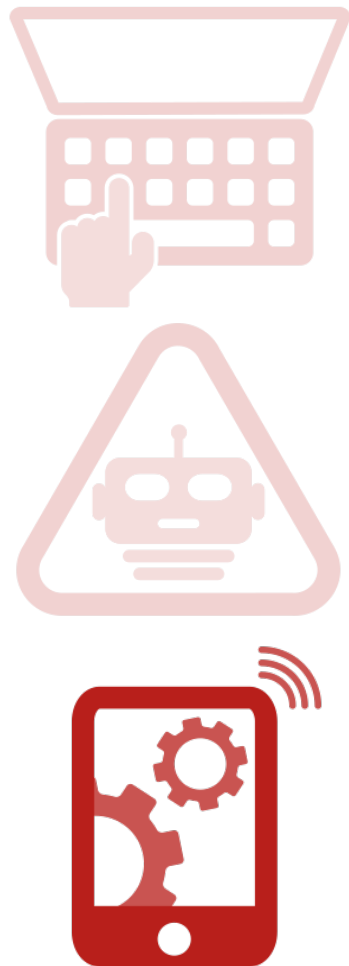
Использование традиционных веб-приложений сокращается.



FortiWeb API Protection

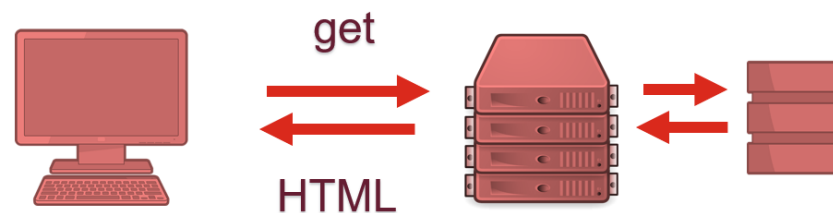
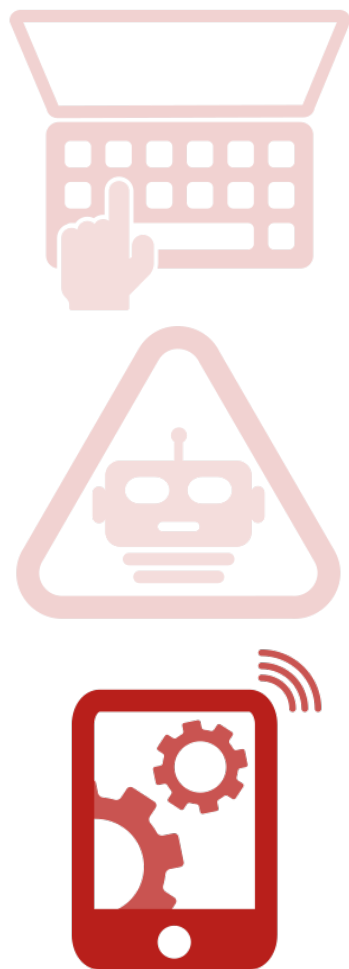
Сложности с API:

... заменены приложениями на основе API, которые могут обеспечить более богатый и отзывчивый пользовательский интерфейс, особенно для пользователей мобильных устройств.



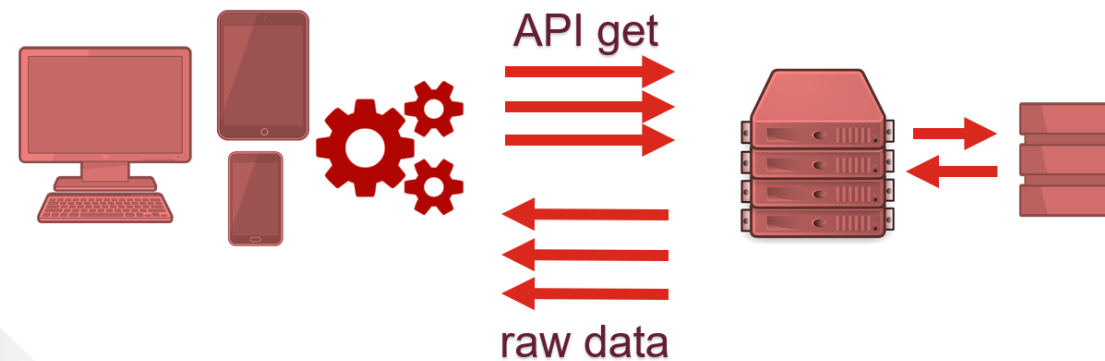
FortiWeb API Protection

Сложности с API:



Traditional Web Applications

- Most processing takes place on the server
- Browser renders the HTML



API Based Applications

- Relies on more powerful clients to process raw data
- Better performance
- Better user experience for mobile devices.

FortiWeb API Protection

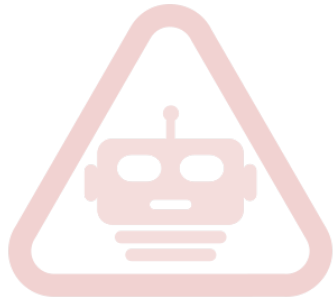
Решения:

FortiWeb предоставляет шлюз API, который обеспечивает единую точку входа для доступа к API, который включает:

- schema validation
- attack signatures
- protocol limits
- API gateway that provides:
 - API user management
 - API key verification
 - API access control
 - Rate limit control
 - API call rewriting

Преимущества:

- Единая точка входа API
- Скрывает внутреннюю структуру API от потенциальных злоумышленников
- Обеспечьте улучшенный пользовательский интерфейс для пользователей на широком спектре устройств без ущерба безопасности



Machine Learning for Web Application Protection

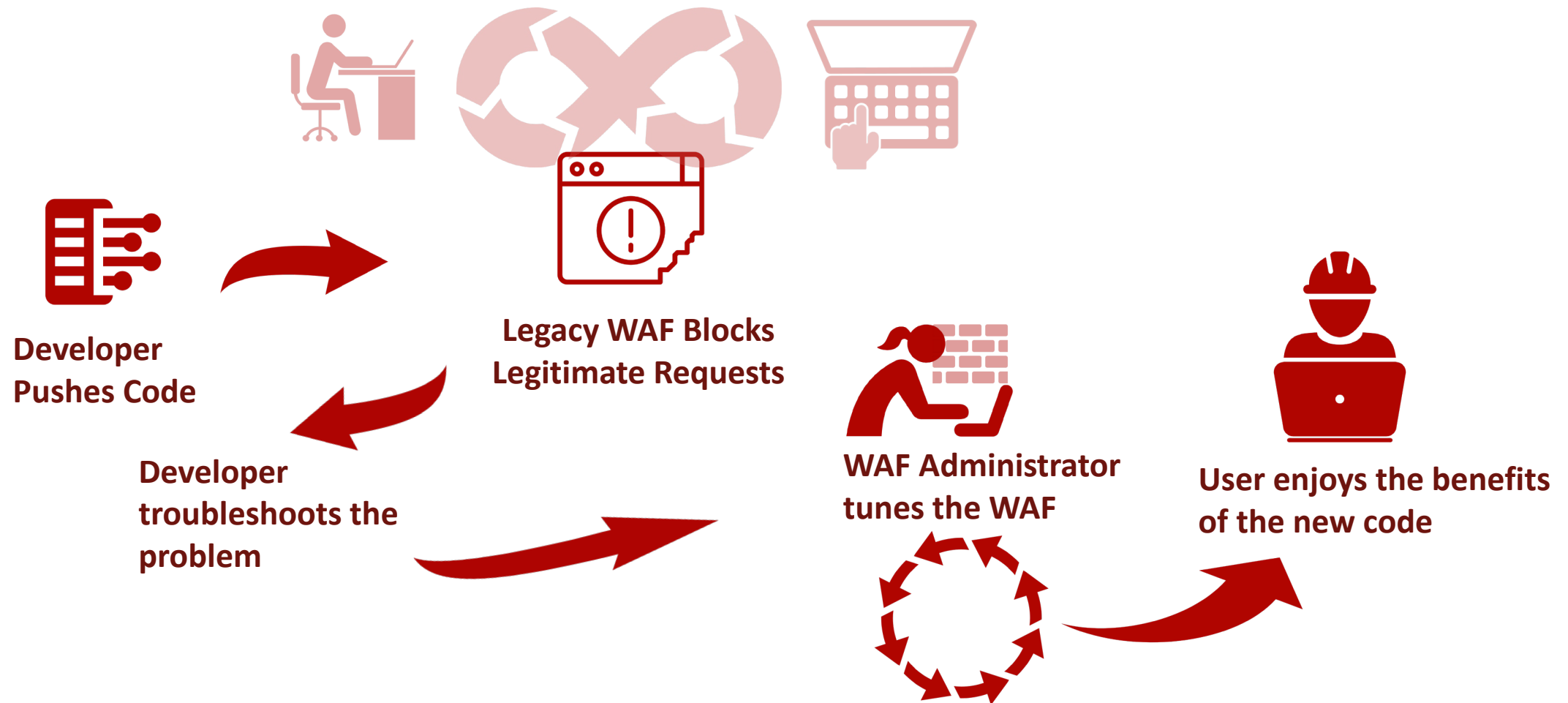
Уменьшите временные потери при развертывании веб-приложений



непрерывная интеграция и непрерывное развертывание (CI/CD)

Machine Learning for Web Application Protection

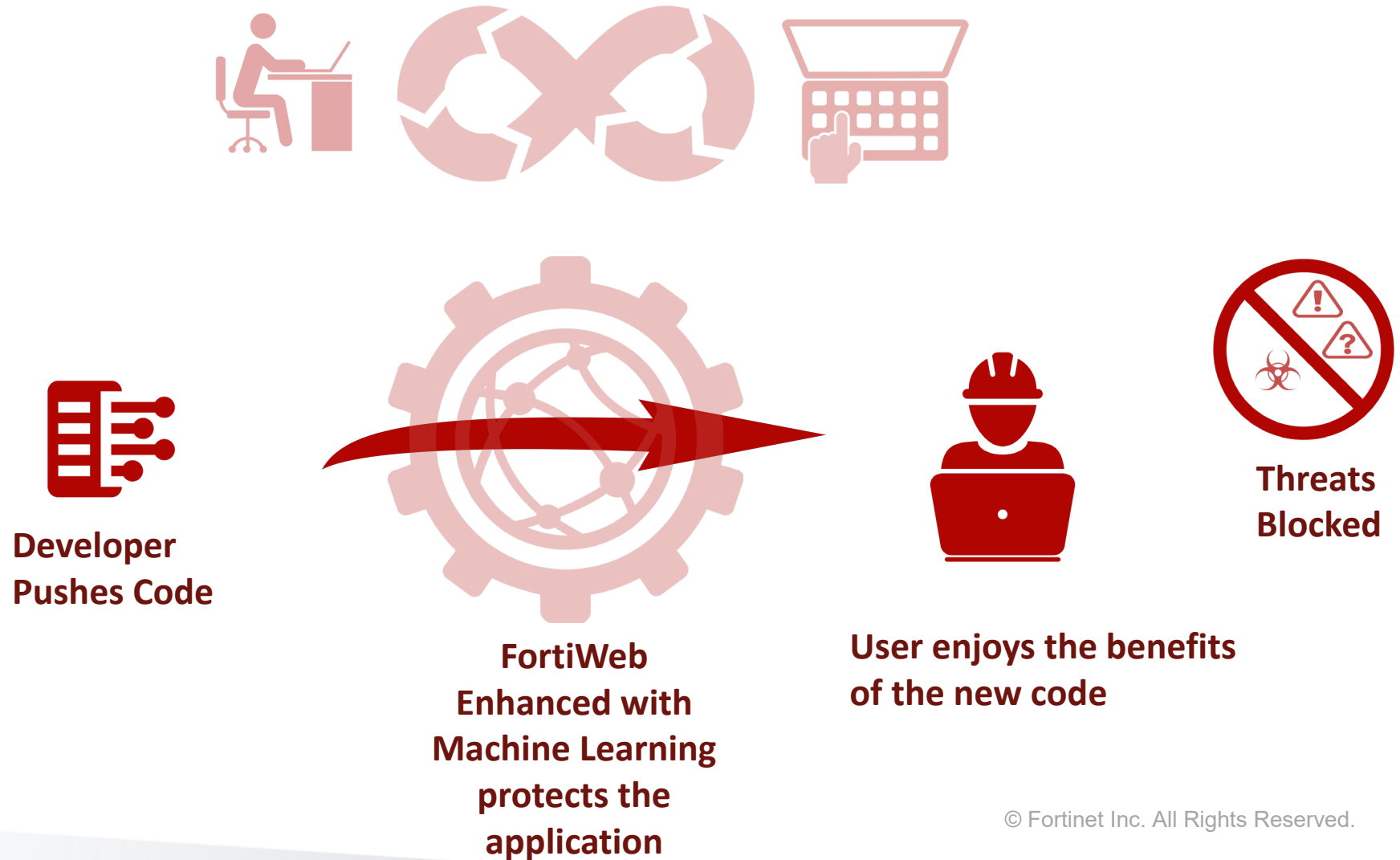
Старомодные WAF добавляют проблем



Существует лучший способ. . .

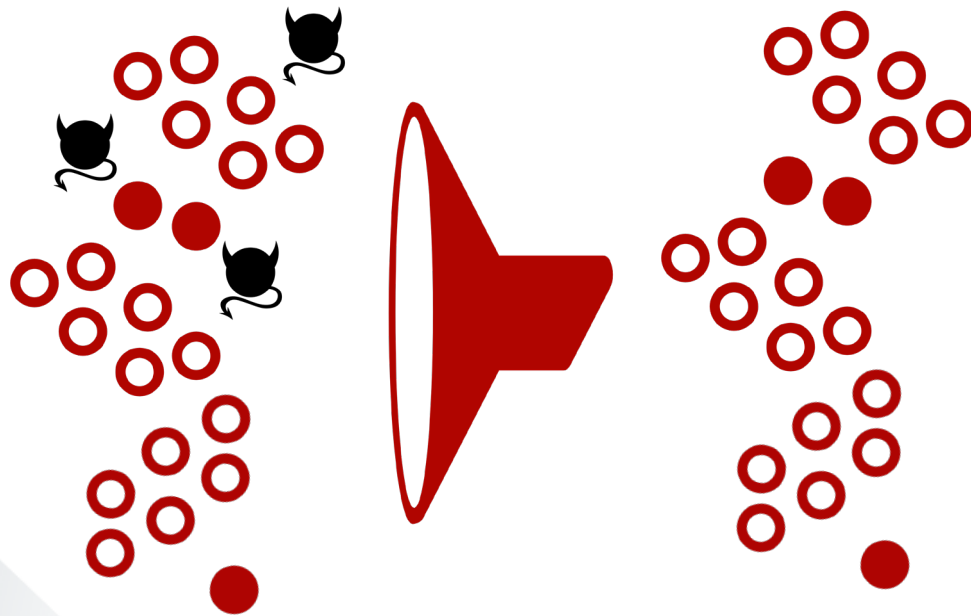
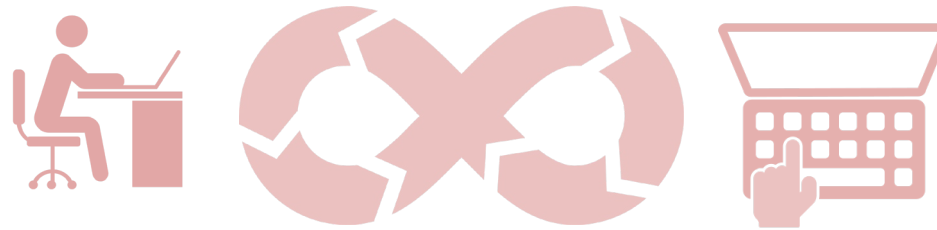
Machine Learning for Web Application Protection

FortiWeb с машинным обучением защищает ваше приложение, не замедляя его работу



Machine Learning for Web Application Protection

Традиционные методы WAF блокируют вредоносный трафик. . .

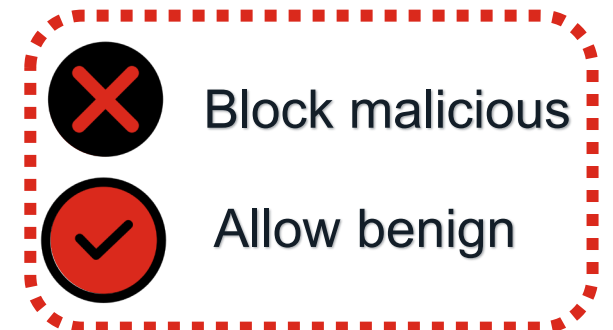
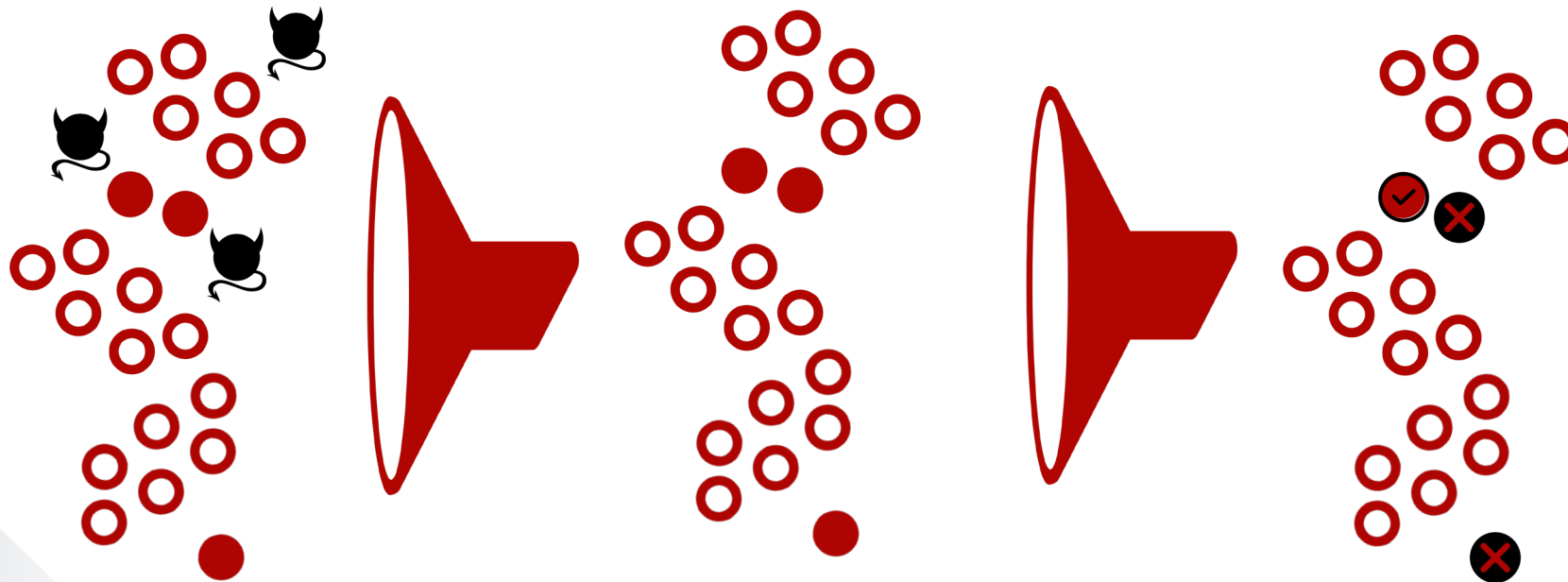
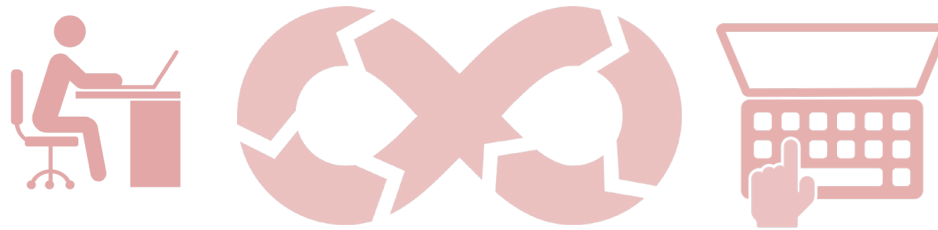


FortiWeb блокирует угрозы с помощью комбинации:

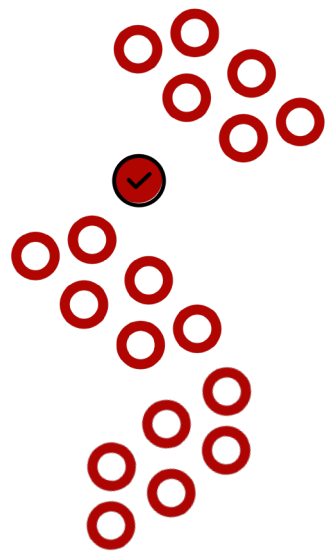
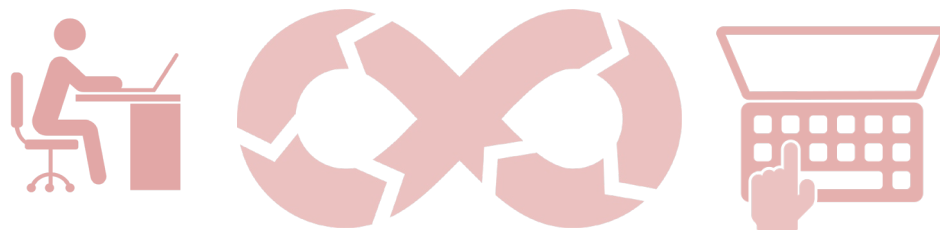
- IP Reputation
- DDOS Protection
- Protocol Validation
- Attack Signatures
- Antivirus / DLP

Machine Learning for Web Application Protection

Дополнительный уровень анализа на основе машинного обучения различает вредоносные и «добрые» аномалии



FortiWeb Machine Learning Benefits



Меньше ложных срабатываний
Меньше административных
накладных расходов

Тенденции продолжают стимулировать инновации WAF . . .



Cloud Adoption

Applications deployed in the cloud require new WAF capabilities:

- Flexible deployment options (VMs, containers, SaaS)
- Multi-cloud support (including private cloud)
- New consumption models (e.g. Pay as you go)



Digital Transformation (DX)

DX is “a fundamental change in the way a company does business using digital technology.”

- Journey, not a destination
- Not just deploying technology
- Customer-focused
- Ongoing rapid changes
- Convergence of technologies (e.g. Web, mobile, APIs, AI)



SaaS

Organizations are increasing adoption of SaaS solutions for mission-critical capabilities, and want to consume WAF capabilities as a service.

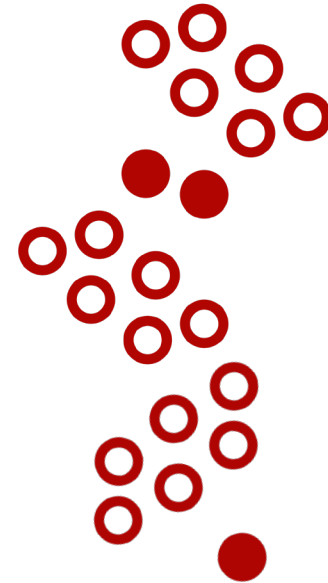
WAF-as-a-Service must provide

- Multitenancy
- Scalability
- Easy deployment
- Streamlined management

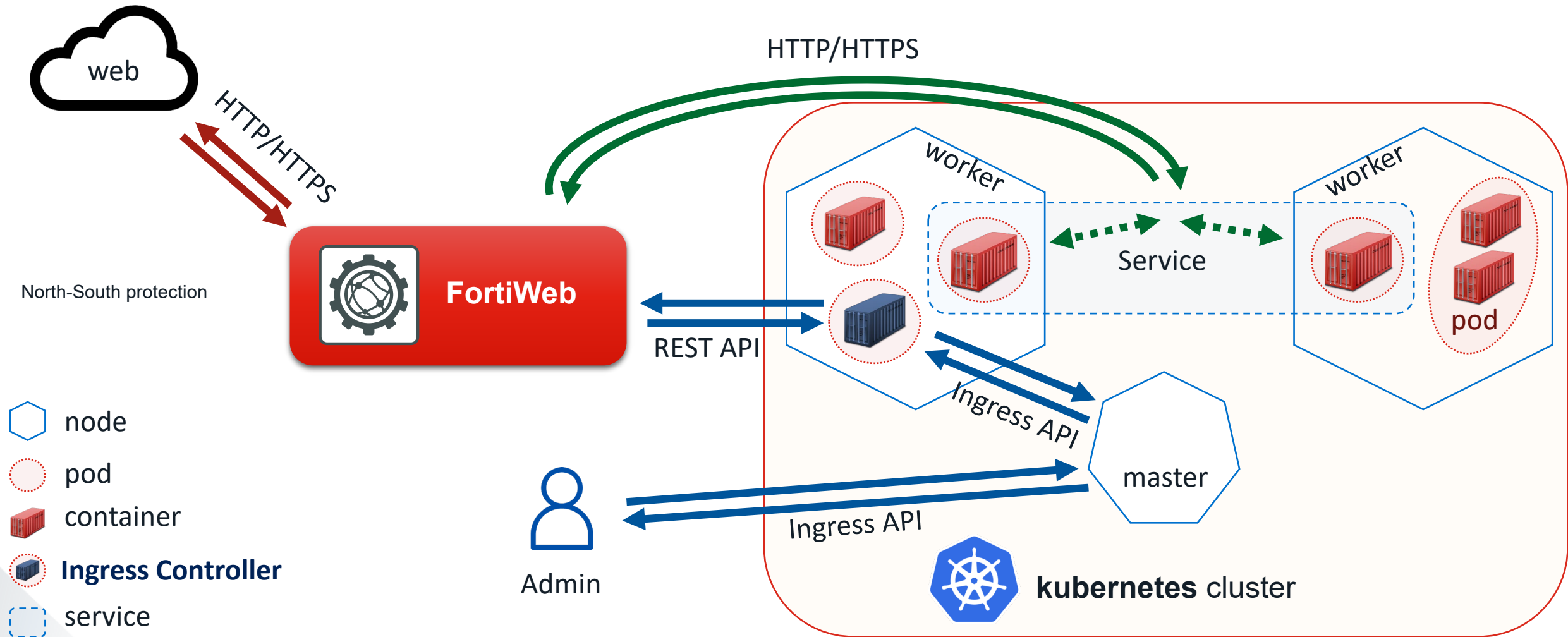
FortiWeb Container



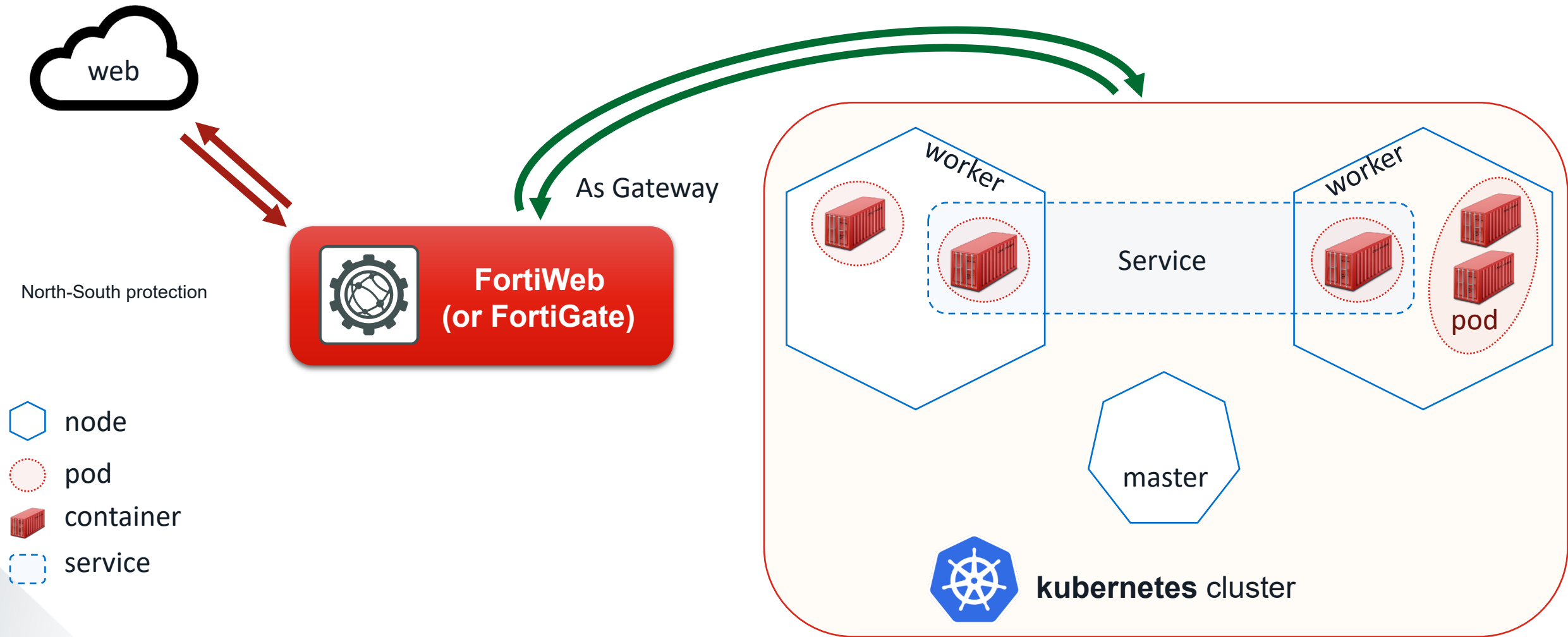
Kubernetes



I - FortiWeb and Ingress Controller

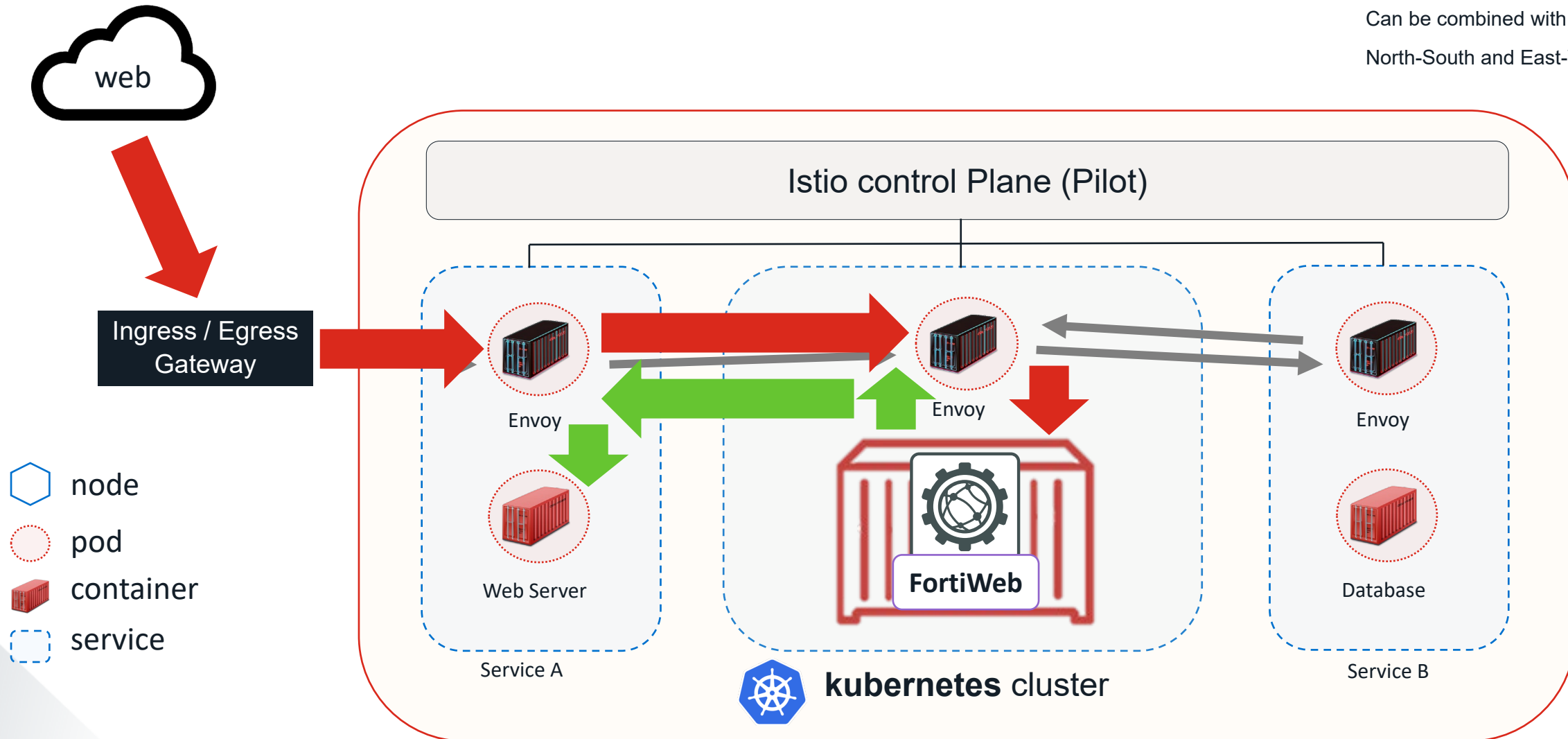


II - FortiWeb / FortiGate (no Ingress Controller)

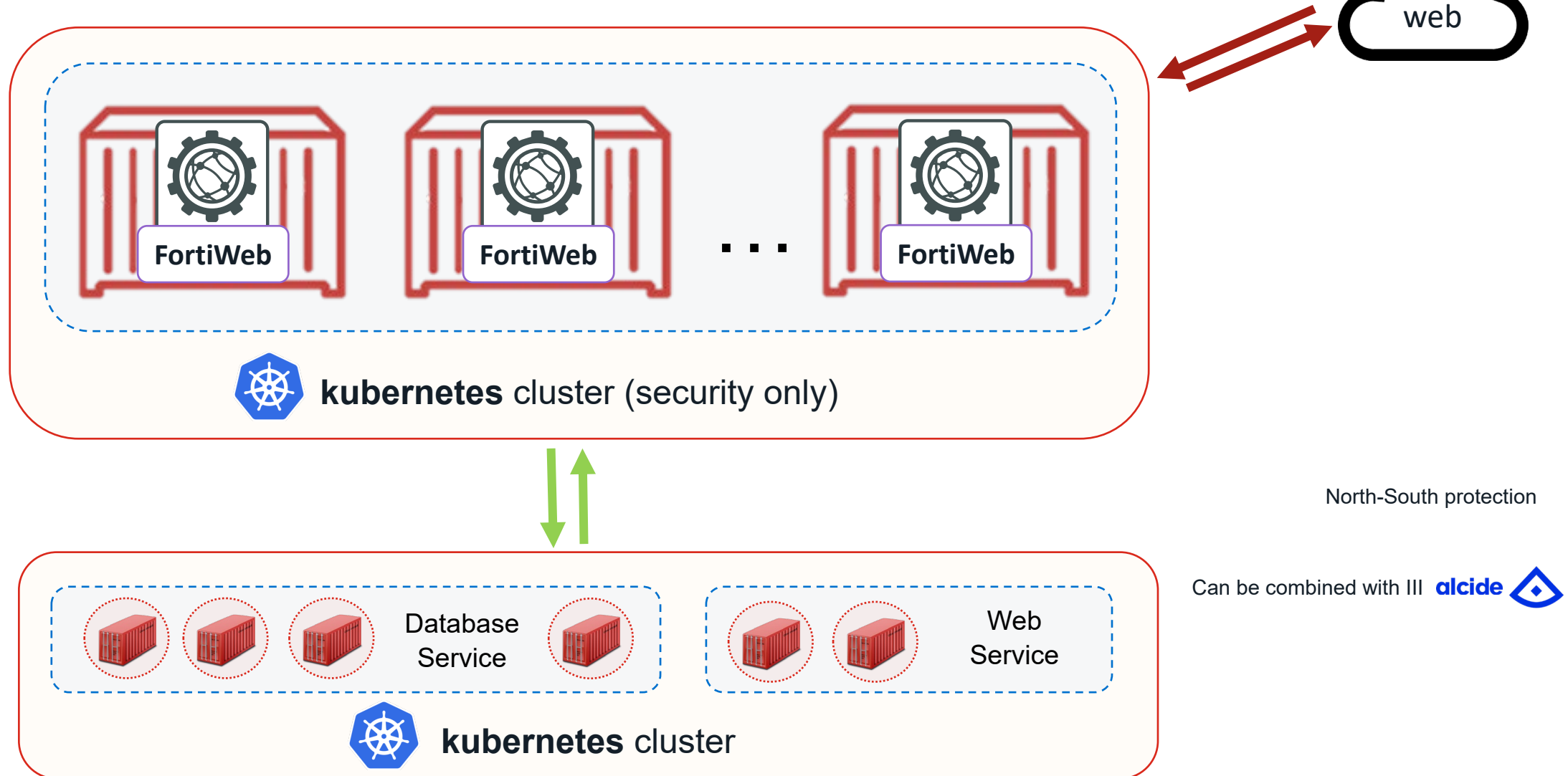


III – FortiWeb as Container

Can be combined with III **alcide** 
North-South and East-West protection

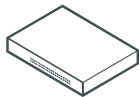
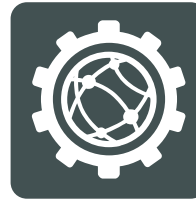


IV – Using a cluster only for security appliances



FortiWeb форм факторы

Несколько вариантов для максимальной гибкости развертывания



Appliances

- 7 models
- 25 Mbps to 20 Gbps
- Support for 10GE



Virtual Machines

- 5 VM models
- CPU-based
- Perpetual licensing
- VMware, Hyper-V, Xen, Citrix Xenserver, KVM, VirtualBox



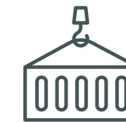
Public Cloud

- 4 VM models
- BYOL and On-demand
- AWS, Azure, Google Cloud, Oracle Cloud



SaaS

- Subscription based
- Based on data consumed and number of sites
- Hosted by Fortinet
- Delivered on AWS, Azure, and GCP
- Purchase with annual contracts or from the public cloud marketplaces



Container

- 4 virtual appliances
- 25 Mbps to 2 Gbps
- Docker support
- AWS ECS

FORTINET®