FortiWeb Webinar
17. & 22. März 2022

FORTINET

AVANTEC
Competence. Security. Trust.

Webinar
Web Applikationen und APIs schützen mit FortiWeb

Gabriel Kälin
Systems Engineer and FortiWeb Subject Matter Expert
Fortinet Schweiz

Web Applications are under attack

Threat actors are actively seeking to exploit vulnerable web applications

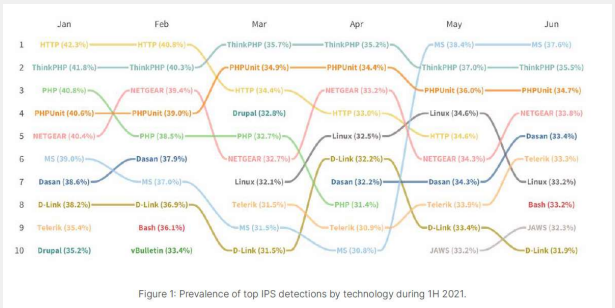


Figure 1: Prevalence of top IPS detections by technology during 1H 2021.

Overall the IPS detections shown reflect several general trends we've seen for some time now: web servers, content management systems (CMS), and Internet of Things (IoT) devices.
-FortiGuard Labs Global Threat Landscape Report, 1H 2021

"… the IPS triggers racking up the highest volume were HTTP.Server.Authorization.Buffer.Overflow and HTTP.URI.Java.Code.Injection, while HTTP.Header.SQL.Injection and HTTP.URI.SQL.injection were detected by the largest number of organizations."

AVANTEC
Competence. Security. Trust.

FortiWeb Webinar
17. & 22. März 2022

The application attack surface keeps growing and changing

48%
of the organizations have 100 or more unique applications in their environment

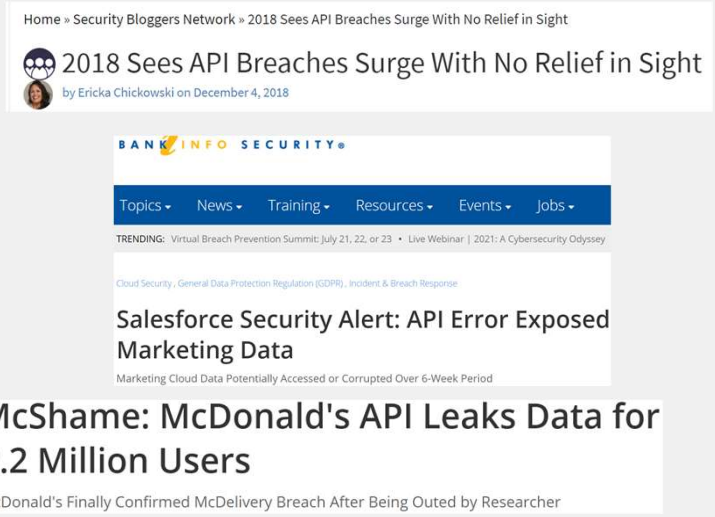
On average, companies publish **25** software updates into production on a monthly basis

For the full report, go to https://go.fortinet.com/global-lp/aws-app-security-report

State of APIs – API Breaches

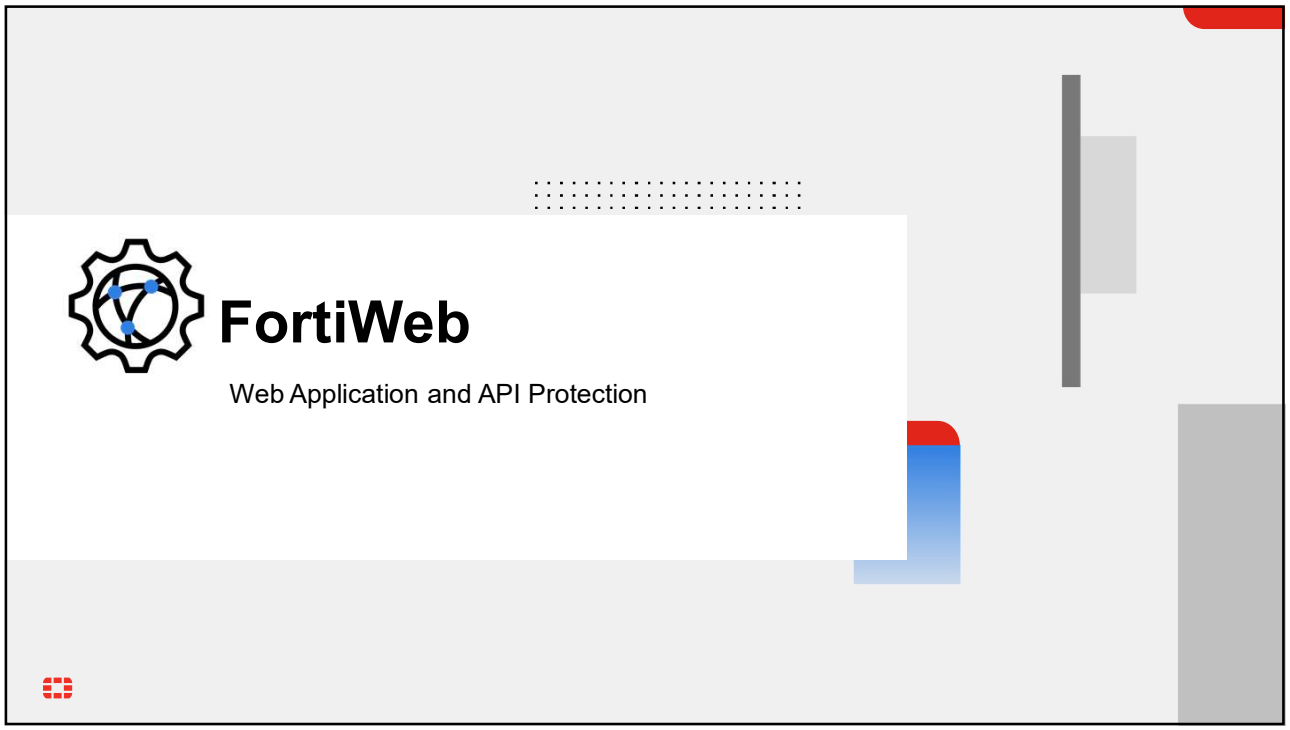
Gartner:

- By 2021, 90% of web-enabled applications will have more surface area for attack in the form of exposed APIs rather than the UI, up from 40% in 2019
- By 2022, API abuses will move from an infrequent to the most-frequent attack vector, resulting in data breaches for enterprise web applications.



AVANTEC
Competence. Security. Trust.

FortiWeb Webinar
17. & 22. März 2022



Primary Web Application & API Security Use Cases

APPLICATION SECURITY

FORTIWEB

1. Web Application Security

Protect from OWASP top 10 and other known threats as well as unknown threats.

ML Optimized Business Application Security

2. Bot Defense

Block the full range of malicious bot activity (for example content scraping, denial of service, data harvesting, transaction fraud).

Advanced ML Powered Bot Detection

3. Regulatory Compliance

Address regulatory compliance requirements related to public-facing applications.

Meet Compliance Requirements

4. Protect Internet-facing APIs

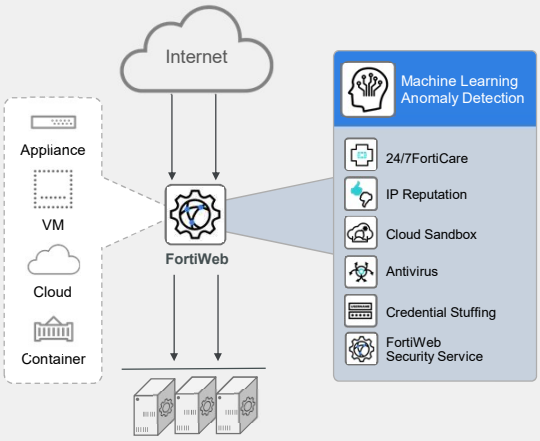
Protect the APIs that enable B2B communication and support your mobile applications.

Leverage ML to Protect APIs That Support Critical Line-of-Business Capabilities

AVANTEC
Competence. Security. Trust.

FortiWeb Webinar
17. & 22. März 2022

Web Application Security



1. Web Application Security

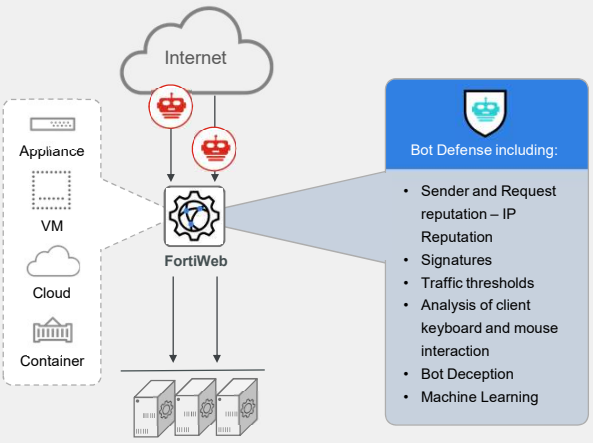
Protect from OWASP top 10 and other known threats as well as unknown threats.

ML Optimized Business Application Security

Protects against threats to web-based applications:

- Protect against known risks, including the OWASP Top 10
- Protection against unknown and zero-day threats
- Reduces administrative overhead by reducing false positives with machine learning

Bot Defense



2. Bot Defense

Block the full range of malicious bot activity (e.g., content scraping, denial of service, data harvesting, transaction fraud).

Advanced ML Powered Bot Detection

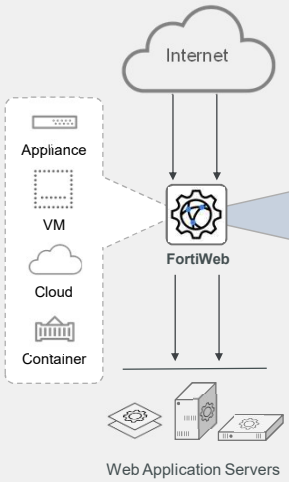
Protection of applications from bots

- Blocks malicious bots without blocking users or interfering with legitimate bot activity such as search engines
- Reduce or eliminate reliance on user verification techniques that degrade the user experience such as ReCaptcha

AVANTEC
Competence. Security. Trust.

FortiWeb Webinar
17. & 22. März 2022

Regulatory Compliance



Address Compliance Requirements, including WAF-specific require-ments outlined in the Payment Card Industry Data Security Standard (PCI-DSS) and elements of GDPR, HIPAA, and others

Addresses PCI DSS 6.6:
"Installing an automated technical solution that detects and prevents web based attacks (for example, a web application firewall) in front of public facing web applications, to continually check all traffic."

3. Regulatory Compliance

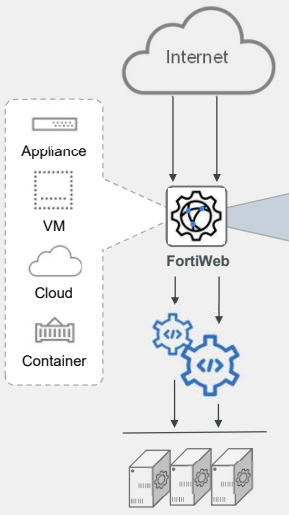
Address regulatory compliance requirements related to public-facing applications.

Meet Compliance Requirements

Address specific compliance controls for protection of web-based applications:

- Protect against known risks, including common web threats such as those listed in the OWASP Top 10
- Address PCI-DSS 6.6 requirements
  - PCI DSS is mandated by credit card companies and applies to all entities that store, process or transmit cardholder data

Protect Internet-Facing APIs



API Defense Includes:

Schema validation
Attack signatures
Protocol limits
API gateway capabilities:
- API user management
- API key verification
- API access control
- Rate limit control
- API call rewriting

4. Protect Internet-Facing APIs

Protect the APIs that enable B2B communication and support your mobile applications.

Leverage ML to protect that APIs that support critical line-of-business capabilities

Advanced protection for APIs

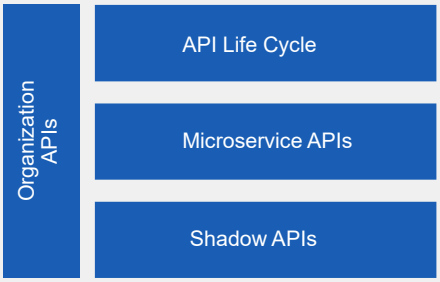
- Single point of access to APIs
- Hides internal API structure from potential attackers
- Delivers improved user experience for users on a wide range of devices without sacrificing security

AVANTEC
Competence. Security. Trust.

FortiWeb Webinar
17. & 22. März 2022

Securing APIs

- APIs are developed and managed differently than standard web applications
- Shadow APIs – developed as part of the app implementation, not known publicly
- Microservices introduce many internal APIs
- API lifecycle – API evolution/deprecation/temporality
- You can't secure what you don't know. API visibility is key – **API Discovery**
- Achieving a strong level of protection requires layered security



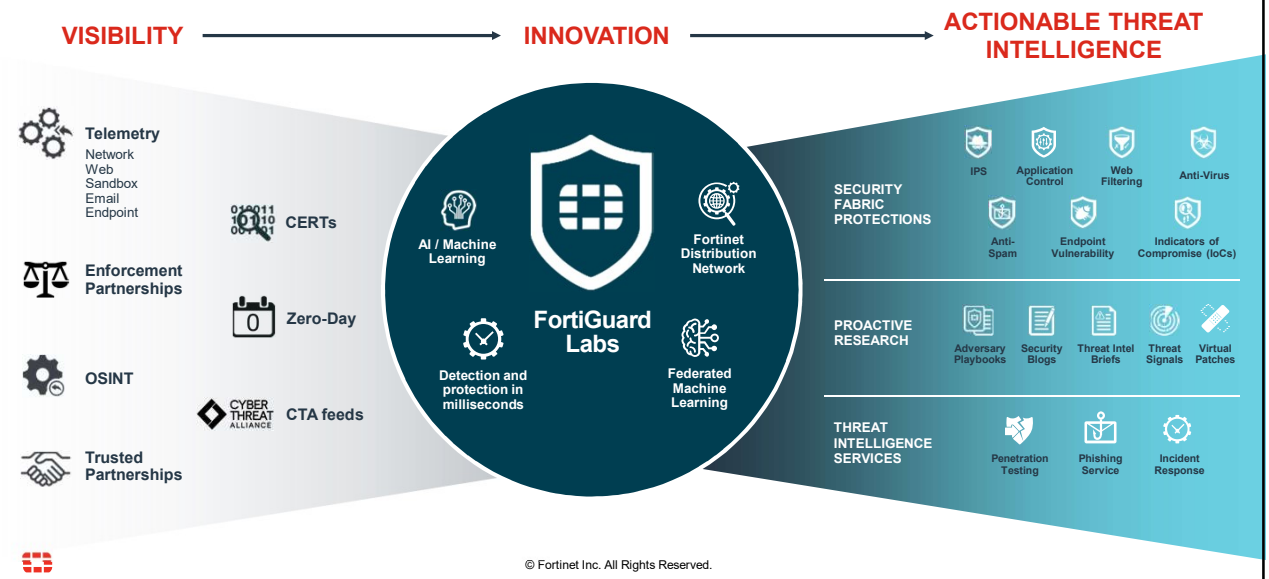
Comprehensive WAF Security

A multi-layer approach to protection web applications

AVANTEC
Competence. Security. Trust.

FortiWeb Webinar
17. & 22. März 2022

Actionable Threat Intel from FortiGuard Labs



Threat Intelligence Lays the Foundation

ATTACKS/THREATS	
BOTNETS, MALICIOUS HOSTS, ANONYMOUS PROXIES, DDOS SOURCES	IP REPUTATION
APPLICATION LEVEL DDOS ATTACKS	DDOS PROTECTION
IMPROPER HTTP RFC	PROTOCOL VALIDATION
KNOWN APPLICATION ATTACK TYPES	ATTACK SIGNATURES
VIRUSES, MALWARE, LOSS OF DATA	ANTIVIRUS/DLP

FortiWeb leverages threat intel from FortiGuard Labs to create signatures and block known malicious sources.

AVANTEC
Competence. Security. Trust.

FortiWeb Webinar
17. & 22. März 2022

Fortinet Security Fabric Integration

ATTACKS/THREATS	
BOTNETS, MALICIOUS HOSTS, ANONYMOUS PROXIES, DDOS SOURCES	IP REPUTATION
APPLICATION LEVEL DDOS ATTACKS	DDOS PROTECTION
IMPROPER HTTP RFC	PROTOCOL VALIDATION
KNOWN APPLICATION ATTACK TYPES	ATTACK SIGNATURES
VIRUSES, MALWARE, LOSS OF DATA	ANTIVIRUS/DLP
FORTIGATE AND FORTISANDBOX ATP DETECTION	FABRIC INTEGRATION

Integration with Fortinet Security Fabric components

- **FortiGate for Fabric Visibility and Redirection**
- **FortiAnalyzer for Logging and Reporting**
- **FortiSandbox for enhanced malware detection**

Bot Management and API Protection

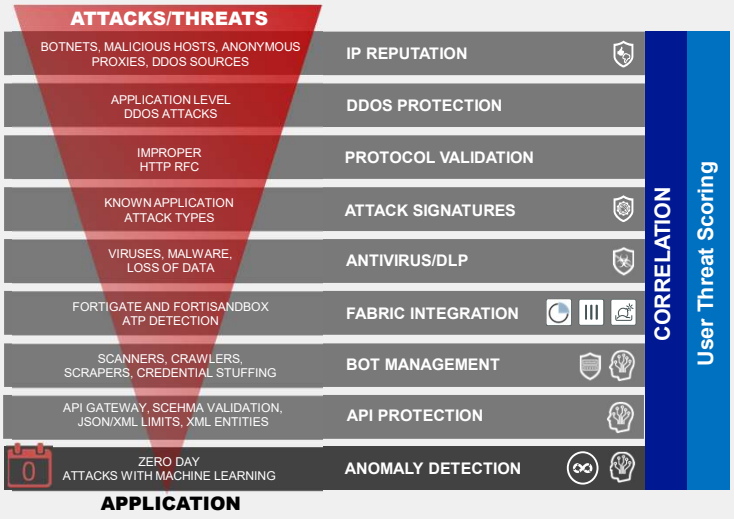
ATTACKS/THREATS	
BOTNETS, MALICIOUS HOSTS, ANONYMOUS PROXIES, DDOS SOURCES	IP REPUTATION
APPLICATION LEVEL DDOS ATTACKS	DDOS PROTECTION
IMPROPER HTTP RFC	PROTOCOL VALIDATION
KNOWN APPLICATION ATTACK TYPES	ATTACK SIGNATURES
VIRUSES, MALWARE, LOSS OF DATA	ANTIVIRUS/DLP
FORTIGATE AND FORTISANDBOX ATP DETECTION	FABRIC INTEGRATION
SCANNERS, CRAWLERS, SCRAPERS, CREDENTIAL STUFFING	BOT MANAGEMENT
API GATEWAY, SCEHMA VALIDATION, JSON/XML LIMITS, XML ENTITIES	API PROTECTION

FortWeb adds additional Bot Management and API Protection capabilities to deliver a full Web Application and API Protection (WAAP) solution.

AVANTEC
Competence. Security. Trust.

FortiWeb Webinar
17. & 22. März 2022

Machine Learning for Anomaly Detection



Machine Learning based anomaly detection learns how your users interact with your application, delivering both improved threat detection and reducing the false positives that drive administrative overhead.

Deployment Flexibility

AVANTEC
Competence. Security. Trust.

FortiWeb Webinar
17. & 22. März 2022

Maximum Deployment Flexibility

Delivering a full range of deployment options to support on-premise, hybrid, and pure cloud application deployments

Appliances
- 7 models
- 50 Mbps to **70** Gbps
- Support for 10/40GE

Virtual Machines
- 5 VM models
- CPU-based
- Perpetual and subscription 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 on data consumption or throughput
- Hosted by Fortinet

Container
- 4 virtual appliances
- 25 Mbps to 2 Gbps
- Docker support

Partner Rules
- 5 packages
- Add on to AWS WAF
- Basic to complete OWASP Top 10 protection

FortiWeb Appliances and Virtual Machines

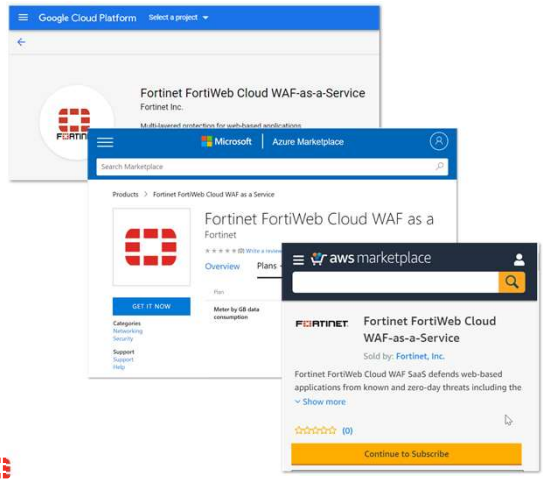
- **7 HW appliances and 5 VM models (50 Mbps to 70 Gbps)**
- **Virtual Machines available BYOL or PAYG for deployment in Public Cloud**

AVANTEC
Competence. Security. Trust.

FortiWeb Webinar
17. & 22. März 2022

FortiWeb Cloud

- **Available on AWS, Azure, GCP, and OCI**
- **Purchase with annual contracts or from the public cloud marketplaces**



- Subscription based based on data consumed and number of sites
- Hosted by Fortinet
- Delivered on AWS, Azure, GCP, and OCI
- CDN available at no additional cost
- Purchase with annual contracts or from the public cloud marketplaces

Summary: Web Application and API Security

Automate and Simplify Protection for Web Applications and APIs everywhere you deploy them

Your applications and APIs

Deployed in the cloud or on-premise

Delivering Line of Business Capabilities

To your users, anywhere, from any device

Protected by FortiWeb's unique AI-powered detection engine, that minimizes false positives and reduces administrative overhead

Extending the protection of Fortinet's Security Fabric across your application attack surface.

AVANTEC
Competence. Security. Trust.

FortiWeb Webinar
17. & 22. März 2022

FORTINET

2
3

Case Studies

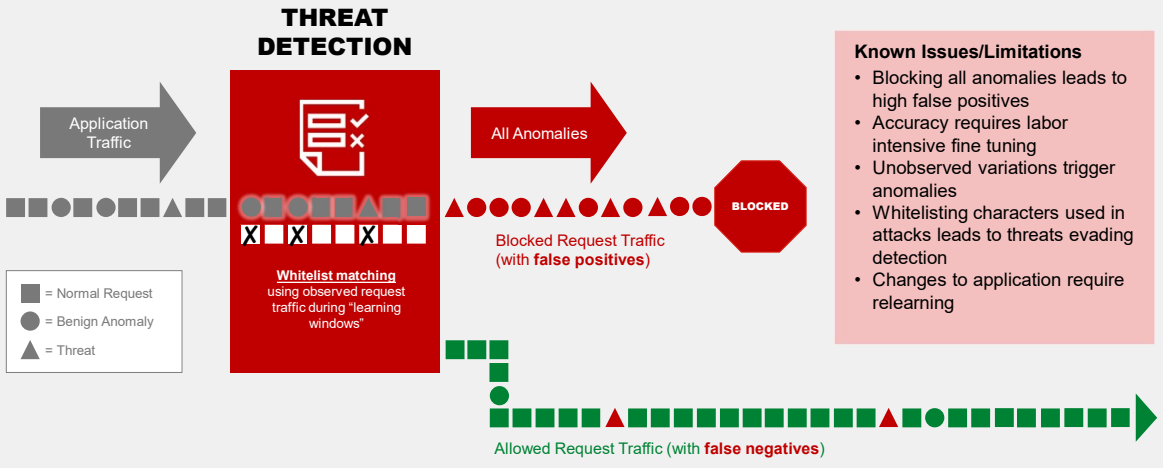
Learn how Fortinet uses FortiWeb Cloud to protect our web applications. . .

AVANTEC
Competence. Security. Trust.

FortiWeb Webinar
17. & 22. März 2022

Why Machine Learning?

Traditional WAF Application Learning Detection



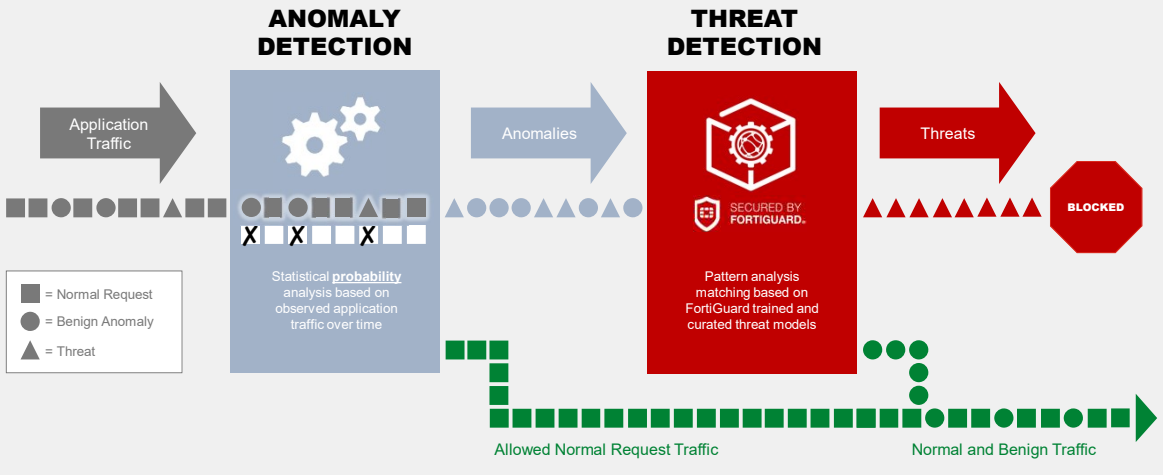
Known Issues/Limitations

- Blocking all anomalies leads to high false positives
- Accuracy requires labor intensive fine tuning
- Unobserved variations trigger anomalies
- Whitelisting characters used in attacks leads to threats evading detection
- Changes to application require relearning

AVANTEC
Competence. Security. Trust.

FortiWeb Webinar
17. & 22. März 2022

FortiWeb Employs 2 Layers of Machine Learning



Reduce friction when deploying web applications!

Why Machine Learning for Web Application Protection Matters for Customers

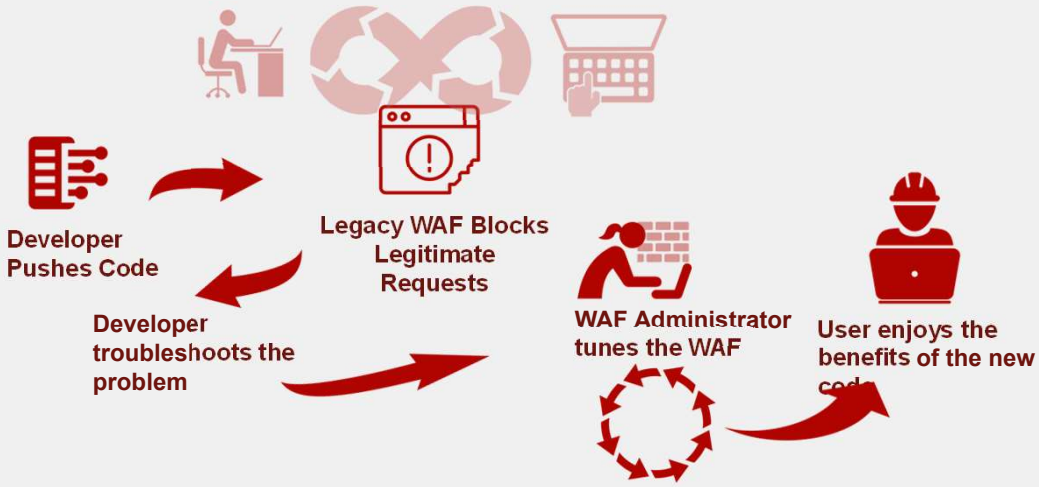
Reduce friction when deploying web applications

continuous integration and continuous deployment (CI/CD)

AVANTEC
Competence. Security. Trust.

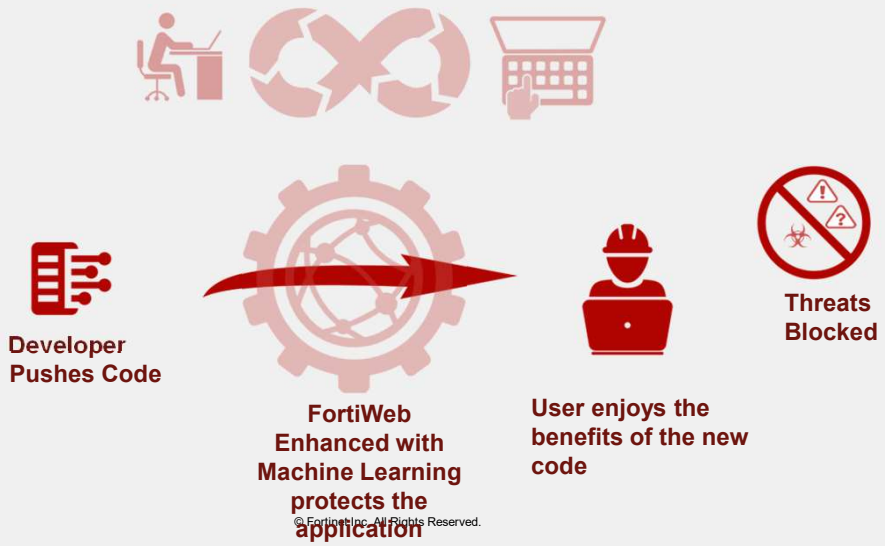
FortiWeb Webinar
17. & 22. März 2022

Old Fashioned WAFs add friction



Machine Learning for Web Application Protection

FortiWeb with Machine Learning Secures your Application without slowing you down



AVANTEC
Competence. Security. Trust.

FortiWeb Webinar
17. & 22. März 2022

Referenzen

- https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/massnahmen-schutz-cms.html
- https://global.fortinet.com/lp-en-aws-app-security-report

AVANTEC
Competence. Security. Trust.