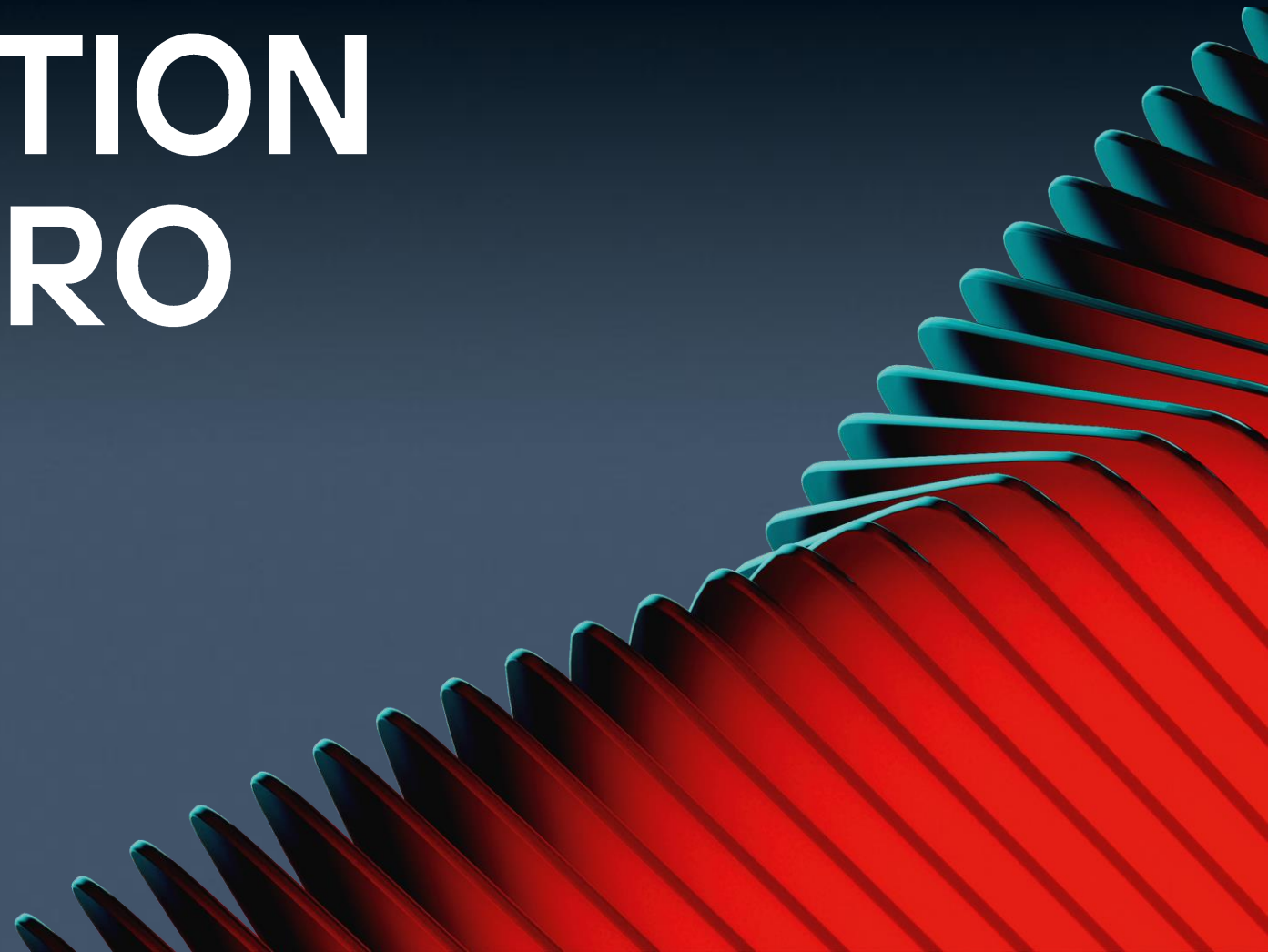
positive technologies

PT APPLICATION FIREWALL PRO

Zero-day threat protection



POSITIVE TECHNOLOGIES

PROTECTING THE WORLD FROM NON-TOLERABLE EVENTS*
WITH THE LATEST TECHNOLOGY

1

Positive Technologies is an industry leader in result-driven cybersecurity and a major global provider of information security products and solutions.

Our mission is to safeguard businesses and entire industries against the threat of cyberattacks.

Who we protect

2

Positive Technologies' **global experience and expertise** covers almost all continents and regions, including MENA, LATAM, South- East Asia, India, China, and Africa.

3

Global Events

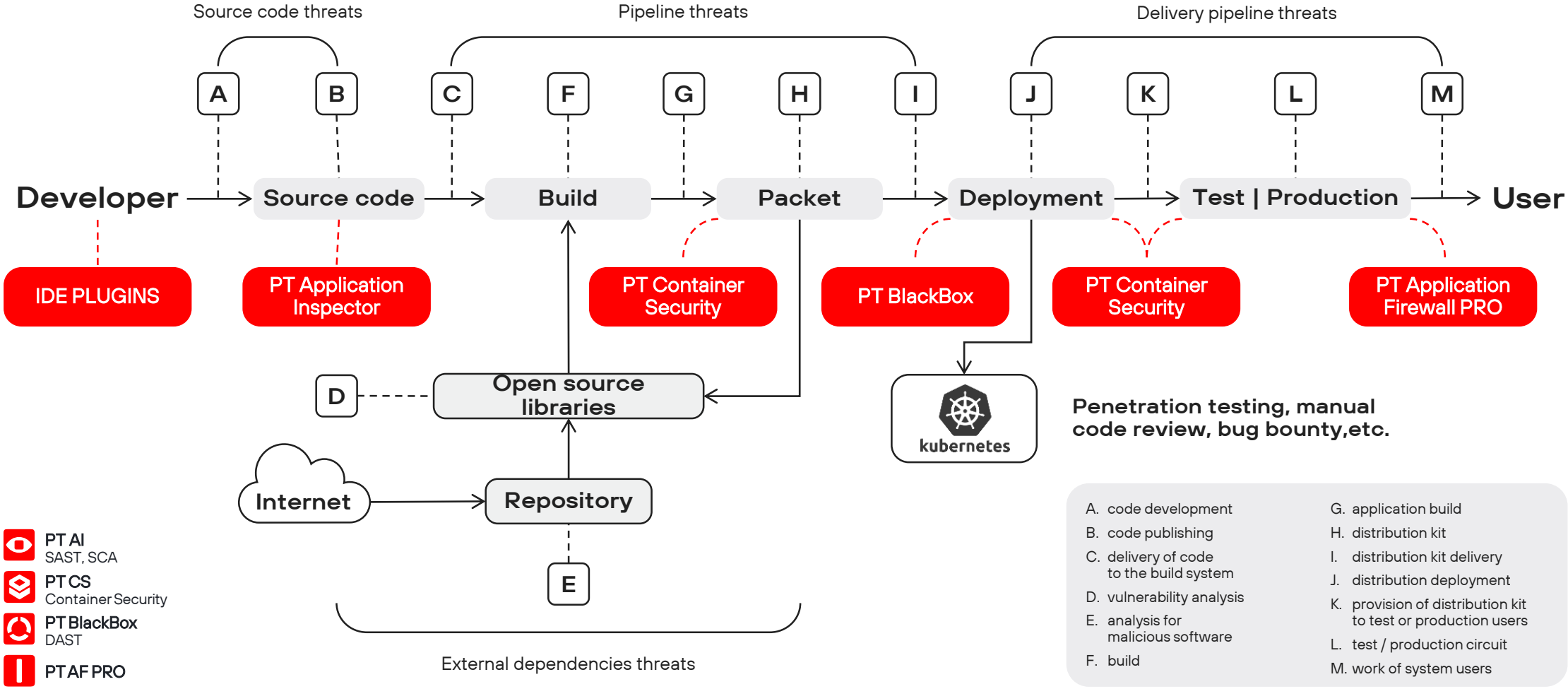
- Sochi Olympic Games
- FIFA World Cup
- Phygital Games of the Future

*Non-tolerable event – an event resulting from a cyber attack that makes it impossible to achieve an organization's operational and/or strategic goals or that results in significant disruption to its core business

Publicly traded **MOEX: POSI**

R&D in cyber security, years	22+
Customer Count, worldwide	4k
Creative environment, specialists and experts	2.8k
Leading integrators as partners	300+

PRODUCT SUITE



PT APPLICATION FIREWALL PRO

ZERO-DAY THREAT PROTECTION

PRODUCT OVERVIEW

High-performance Web Application Firewall (WAF). Protects web applications — from simple landing pages to high-load enterprise portals — and their APIs from external cyber threats.

Our web application firewall is an innovative protection system that detects and blocks attacks including the OWASP Top 10, WASC, layer 7 DDoS, and zero-day attacks with pinpoint accuracy. It ensures continuous security for applications, APIs, users, and infrastructure while supporting compliance with security standards including PCI DSS.

ADVANTAGES

1 Adaptable architecture	Microservice-based design enables deployment in diverse network environments, allowing components to integrate directly into application segments.
2 Cost-efficient deployment	Supports lightweight modules for Kubernetes-based or nginx servers, minimizing deployment and support costs.
3 Advanced attack protection	Safeguards against OWASP Top 10 threats, malicious bots with Google reCAPTCHA, and unauthorized web application access.

Protection against
OWASP Top 10
and OWASP API Security Top 10*

KEY BENEFITS

150k RPS
Stable performance

Defends against
5k+
known vulnerabilities

2k+
clients over 10+ years

* The exact list of threats is available upon request

Why PT AF PRO

Multi-tenancy Support

Isolated environments (tenants) enable independent configuration and access for multiple applications within the same platform. Each tenant has its own traffic processors, with physical cluster separation — offering stronger isolation than just logical separation.

Full HTTP/2 Proxy Support

End-to-end support for modern HTTP/2 protocol significantly improves data transfer speed, minimizing latency and maintaining high application performance.

Auto-scaling Capabilities

Handles traffic spikes (e.g., during DDoS attacks or Black Friday sales) by automatically spinning up additional traffic processors. The container-based architecture allows dynamic scaling of cluster nodes based on available resources.

Flexible Deployment Options

Choose from several deployment scenarios:

- On-premises — full data control without internet connection.
- Multi-site — via agents or additional traffic processing servers.
- Hybrid/cloud — lightweight module communicating with the cloud version of PT AF to reduce infrastructure costs.

Use Cases

1

Proactive DDoS defense

Profiling with behavioral analysis improves application security - and even allows predicting how an attack will unfold

2

Automatic blocking of zero-day attacks

Multiple techniques, based on ML algorithms, combine to flag anomalies and automatically stop never-seen-before threats

3

Targeted protection

Built-in security scanners, plus PT Application Inspector integration, detect vulnerabilities in application source code and block attack attempts

4

Stopping attacks on users

Application users stay safe thanks to data masking, and granular access settings

5

Pinpoint protection from bot attacks

Modeling of user behavior makes it easy to identify bots and thwart automated attacks without slowing legitimate traffic

6

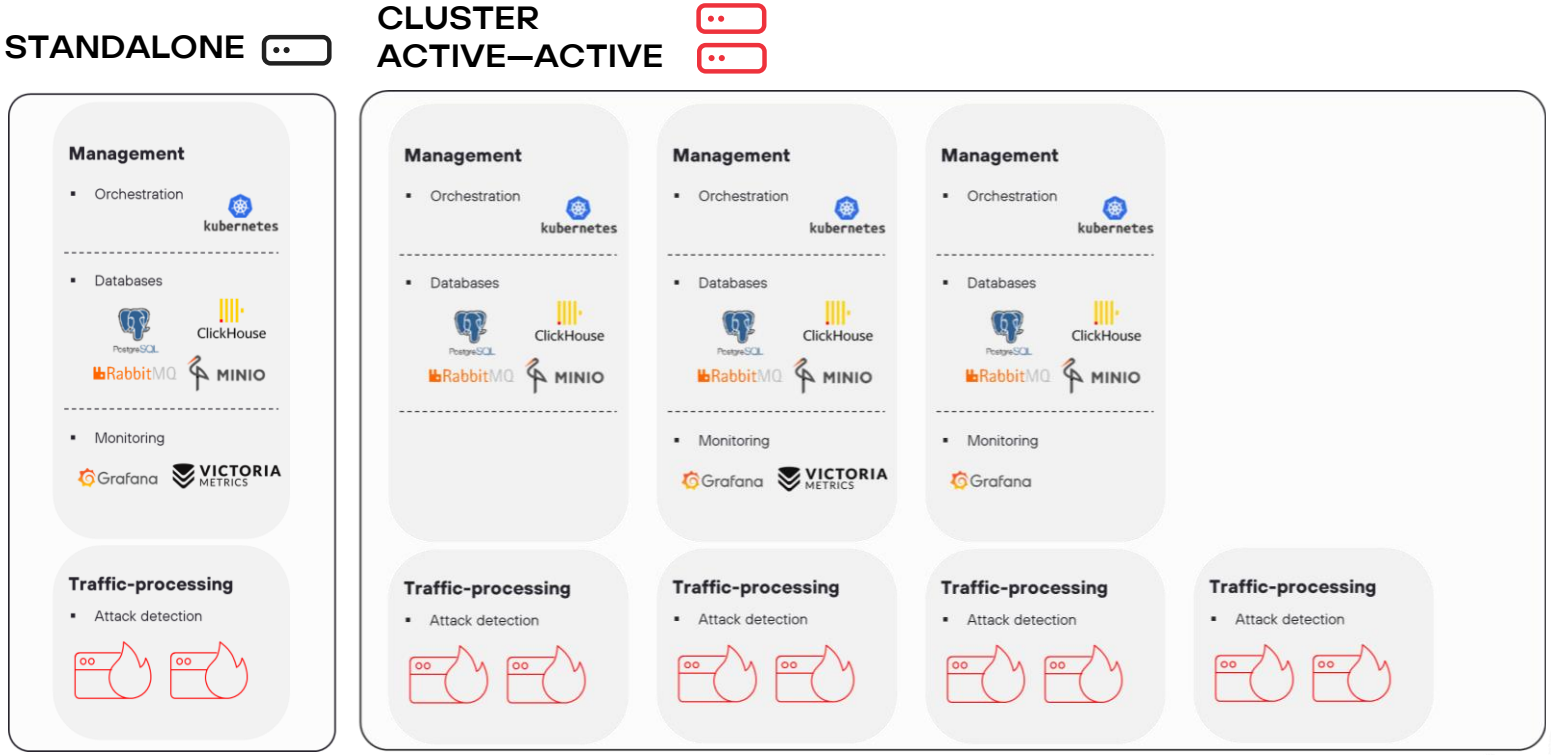
Full security for web and mobile APIs

Threats to web and mobile APIs are stopped by analysis of JSON and XML data

Flexibility and scalability

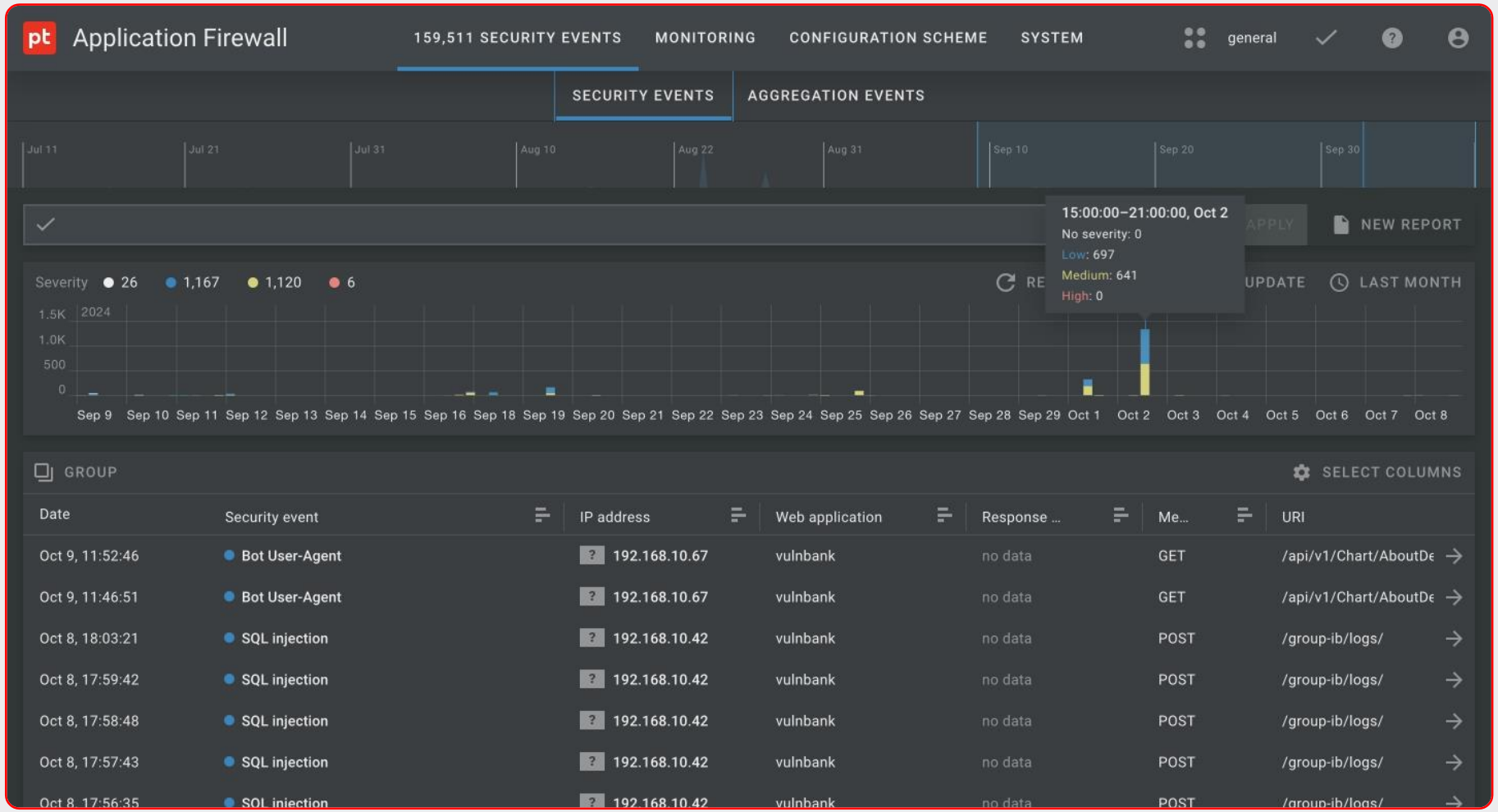
STANDALONE

CLUSTER
ACTIVE—ACTIVE



- Flexible deployment: software and hardware appliance, virtual appliance
- Ability to build scalable high-availability active-active configuration with no loss in efficiency and service interruption
- Multitenancy at the basis of the product architecture
- Ability to connect multiple locations using agents or additional traffic-processing servers

Monitoring a vulnerable web application



What you get

Expertise Inside

PT Application Firewall PRO is powered by Positive Technologies' extensive offensive security experience, including real-world penetration testing and threat intelligence from the Positive Research team and our Security Operations Center (SOC).

Machine Learning Technologies

Our ML-powered modules detect: suspicious user behavior, Malicious web shells and hidden threats in uploaded files

Unlike signature-based detection that only identifies known threats, our behavior-based models detect unknown and evolving threats — a capability proven effective during international cyber drills like Standoff.

HOW CAN WE START

WE ARE READY TO HOLD A MEETING
AND SHARE OUR CASE STUDIES

LET'S GET
IN TOUCH

1

ASSESSMENT

Analyze the current application development security posture

2

STRATEGY

Create a strategy for a secure application development process

3

PILOT

Pilot scanning solutions and tools for secure development

positive technologies

More about

PT Application Firewall PRO

global.ptsecurity.com
info@ptsecurity.com