POSITIVE TECHNOLOGIES

PT APPLICATION FIREWALL

Flexible and precise tool for protection against web attacks

ptsecurity.com

Why it is important to protect web applications

ptsecurity.com

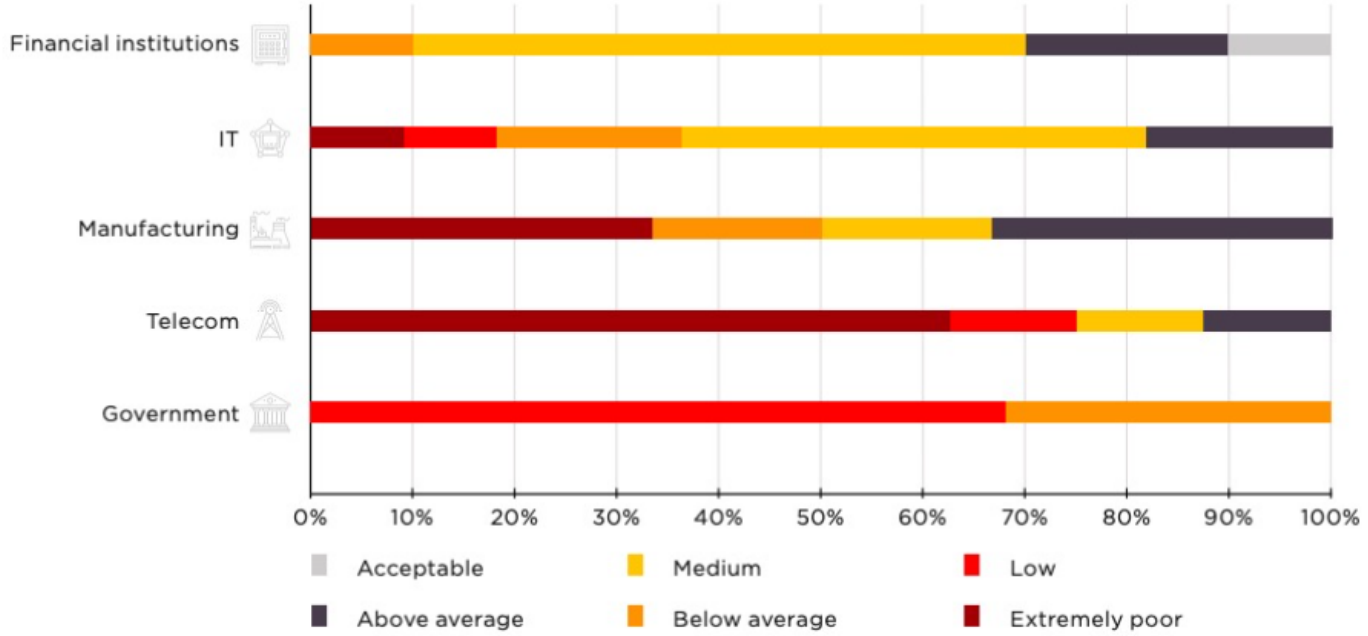
The web is not secure

50% of web applications
contain critical vulnerabilities.

One fifth of attacks
target web applications.

The average web application has
four critical vulnerabilities.

Secure and insecure applications: Distribution by sector



Web application vulnerabilities and threats: statistics for 2023, Positive Technologies

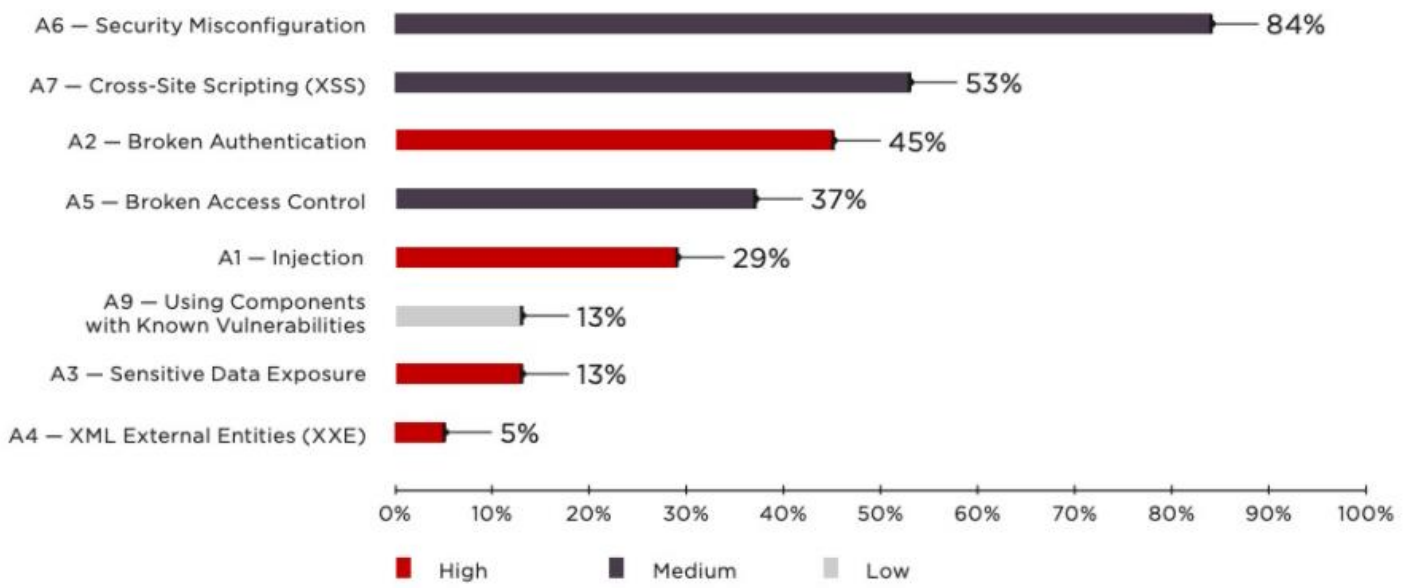
Most popular vulnerabilities

Almost a third
of applications are vulnerable to code injection.

Half
of applications have critical vulnerabilities.

Most applications
are configured incorrectly from a security standpoint.

The most common OWASP Top 10 vulnerabilities**
(by percentage of web applications)



Web Application Vulnerabilities and Threats: Statistics for 2023, Positive Technologies
** OWASP Top Ten, OWASP Foundation

Possible outcomes

UNAUTHORIZED ACCESS TO COMPANY INFRASTRUCTURE

- Remote code execution (RCE)
- Server-side request forgery (SSRF)

Consequences: theft of confidential data, failure of internal company infrastructure.

IMPORTANT INFORMATION LEAKAGE

- SQL Injection
- Access to application source code (Git, SVN)
- Unauthorized access to objects (JDOR)

Consequences: sale of personal information on the darknet, reputational damage due to media coverage, large regulatory fines (GDPR).

FAILURE OF CLIENT BUSINESS PROCESSES

- Distributed denial-of-service attack (DDoS)
- Web form abuse

Consequences: financial and reputational losses suffered by company, inaccessibility of critical infrastructure services.

HACKER GAINS ACCESS TO USER ACCOUNTS

- Cross-site scripting (XSS)
- Brute-force attack
- Credential stuffing

Consequence: financial losses suffered by compromised clients, reputational losses, exodus of service users.

How to protect web applications

ptsecurity.com

How to protect web applications

EXTERNAL SECURITY AUDIT

Black-box and white-box testing

- Perimeter inventory
- Confirmed vulnerability report
- Exploit risks

PT Blackbox

WEB APPLICATION FIREWALL

Web application firewall

- Timely remediation of detected vulnerabilities
- Proactive defense against zero-day attacks

PT WAF

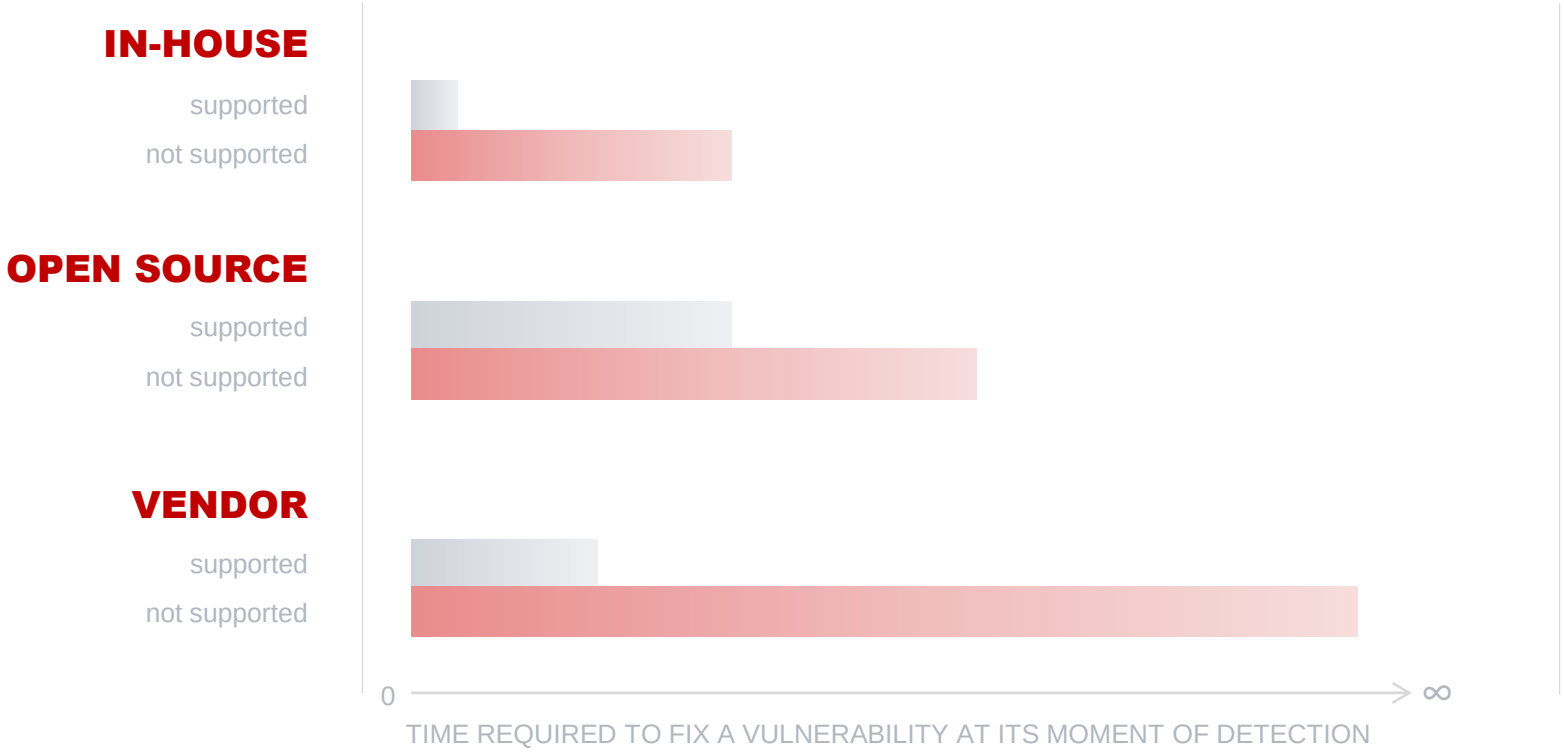
SECURE DEVELOPMENT LIFECYCLE

DevSecOps

- Early detection and remediation of vulnerabilities (when writing code and setting up the application)

PT Application Inspector

Why WAF is a must-have

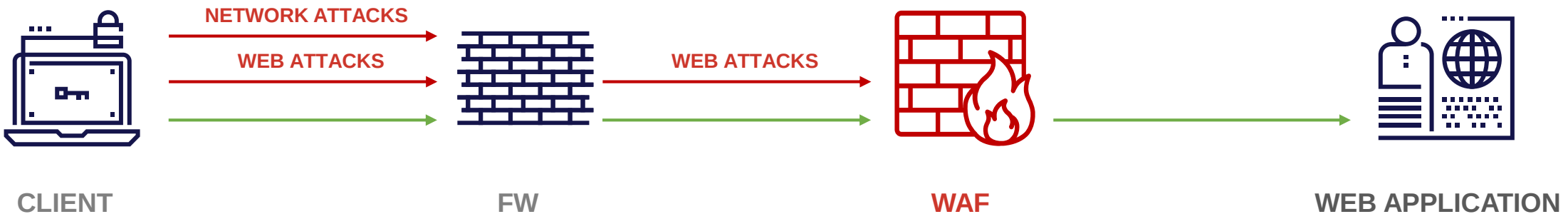


Application vulnerabilities may exist for several months (or years) before they are remediated via an official patch, or they may never be addressed at all.

Web Application Firewall makes it possible to defend a web application against exploits of existing vulnerability without making changes to the application itself.

Web application firewall (WAF)

- Analyzes network traffic in depth (up to L7), specializing in HTTP/HTTPS
- Accounts for the application's business logic
- Detects and prevents distribution during attacks
- Protects the web-application API



The Positive Technologies solution

ptsecurity.com

PT Application Firewall

WEB APPLICATION FIREWALL

A flexible and precise tool for total protection against web attacks

PT Application Firewall features

BLOCKS MASS AND ZERO-DAY ATTACKS

Thanks to a combination of security mechanisms and Positive Technologies expertise, PT Application Firewall ensures comprehensive protection both from known threats and zero-day attacks.

QUICKLY INTEGRATES WITH INFRASTRUCTURE

PT Application Firewall has a built-in configuration wizard and provides security policy templates, making it easy to install and use.

ADAPTS TO THE NEEDS OF EACH DEFENDED APPLICATION

PT Application Firewall combines out-of-the-box usability with finely tunable settings, allowing it to protect a large number of applications with varying degrees of complexity and importance simultaneously.

Benefits

MAINTAINS CONTINUITY OF BUSINESS PROCESSES.

PT Application Firewall defends against DDoS attacks at the application level (L7) and vulnerability exploits related to the business logic of the application.

MINIMIZING THE LIKELIHOOD OF A DATA LEAK

PT Application Firewall blocks the most cutting-edge attacks on web applications, including attacks from the OWASP Top 10 list and the WASC classification. It also automatically detects vulnerabilities in the application and protects against exploits that could target them.

EXPERTISE: FROM PRAXIS TO PRODUCT

Specialists from the application security analysis division make regular updates to the product's knowledge base, adding information about particular vulnerabilities discovered in real applications.

HELPING TO MEET STANDARDS

PT Application Firewall helps its users meet PCI DSS requirements and other international, federal, and corporate security standards.

Reverse proxy

Interception and decryption of traffic, attack blocking.
Most popular WAF integration scenario

PLUSES

- Attack blocking
- Traffic decryption
- Maximum protection provided via a full set of protectors

MINUSES

- Requires a change in network addressing and traffic routing
- Requires detailed calculation of the load on the application for correct sizing

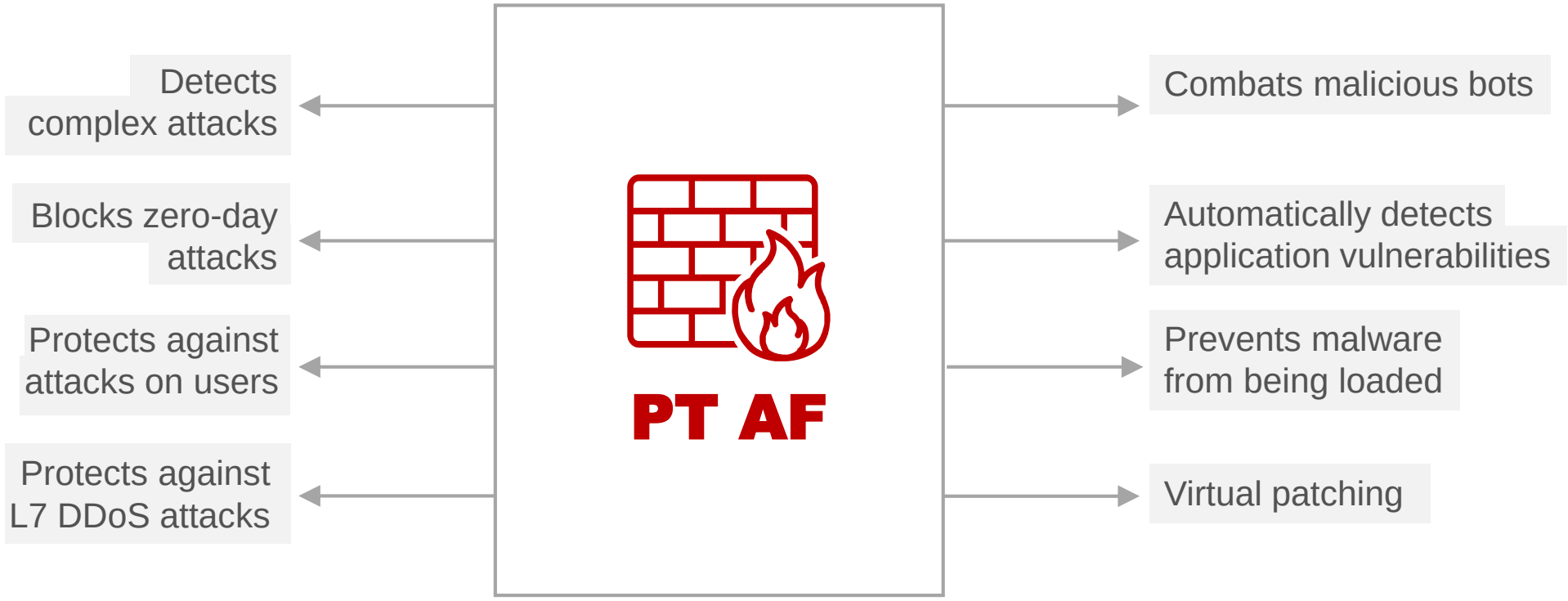
WHEN TO USE

- At the stage of industrial integration, if there are no apparent usage restrictions

Security mechanisms

ptsecurity.com

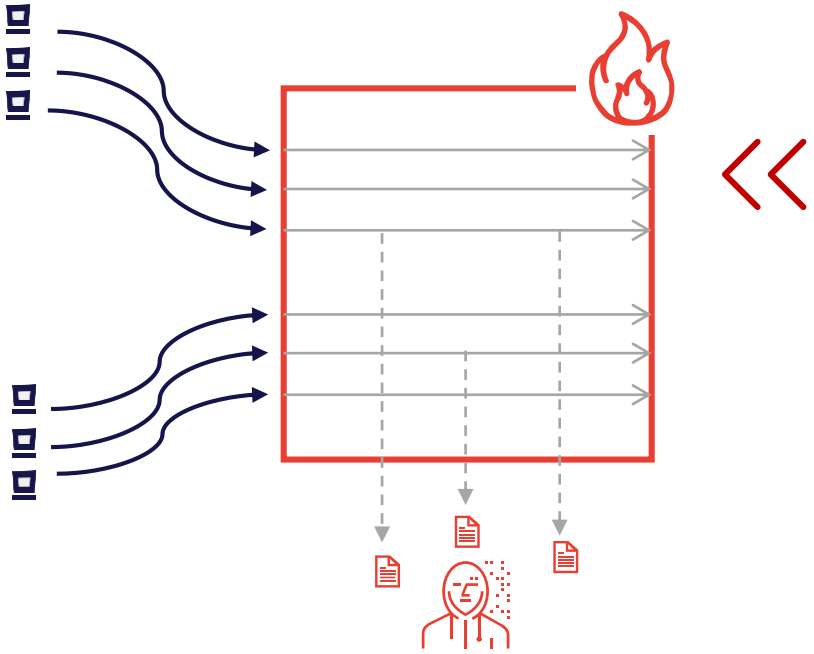
Security mechanisms



Detection of complex attacks

CORRELATION MECHANISM

links multiple logically related but temporally disparate events into a unified sequence.



USER-DEFINED RULES

configure audits of arbitrary application-user actions.

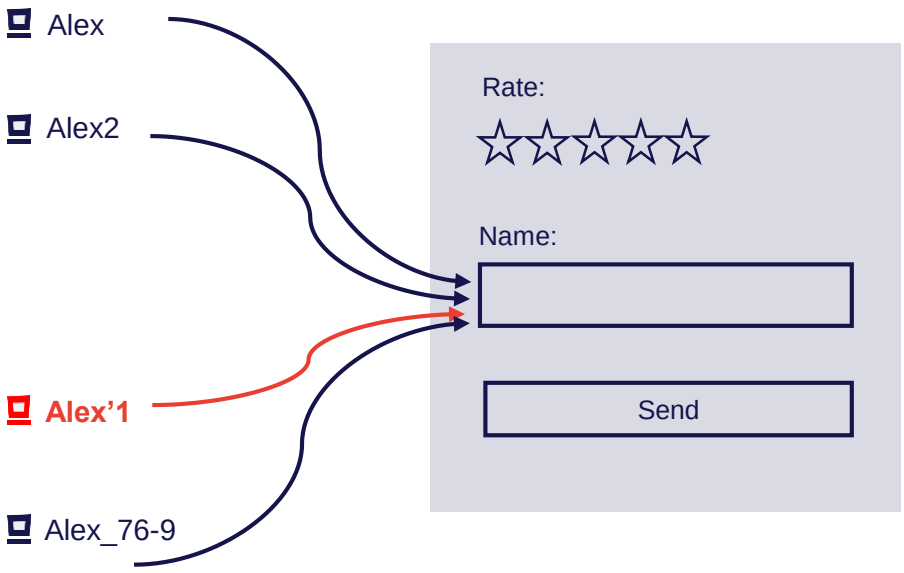
PT Application Firewall contains over 30 out-of-the-box correlation rules so you can quickly react to brute-force attacks, targeted discovery of your network perimeter.

Notifications about complex events significantly increase the efficiency of administration.

Machine learning

Application profiling
makes it possible to calculate anomalies in client requests, thereby blocking new attacks for which detection rules have yet to be defined.

User profiling via machine learning
makes it possible to track behavioral anomalies in users, including attempts to carry out L7 DDoS attacks.



Checking
the client environment

PROTECTION AGAINST CLIENT-SIDE ATTACKS

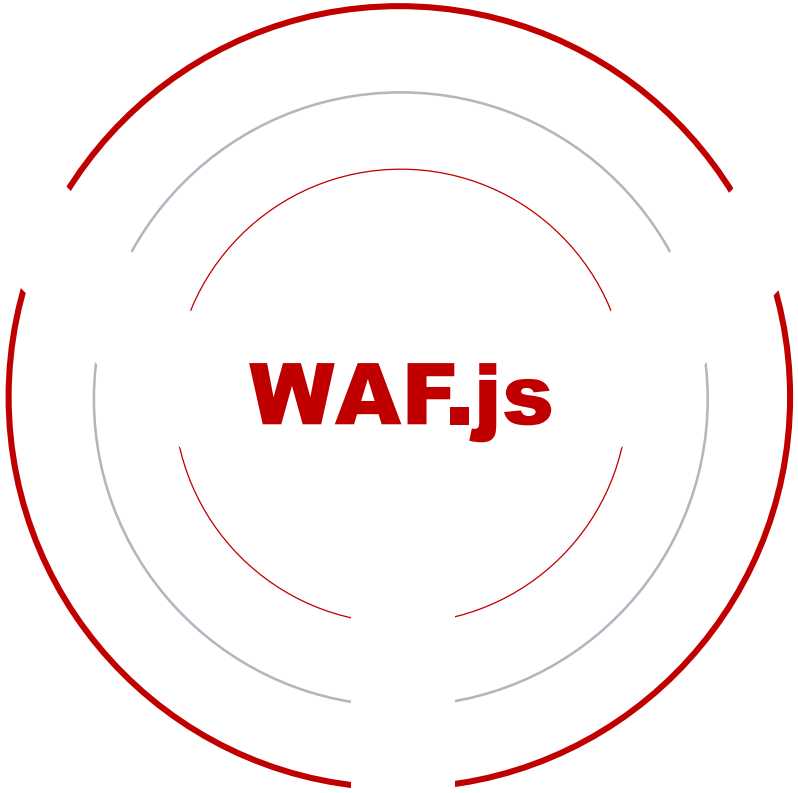
blocks XSS, DOM XSS, DOM clobbering, and CSRF attacks when opening the application page.

CLASSIFICATION AND DETECTION OF MALICIOUS BOTS

protects against bots of all levels of sophistication, including those that can use JavaScript to emulate a browser.

DETECTION OF HACKING TOOLS LAUNCHED BY THE CLIENT

detects hacking tools launched by the client while calling the defended application.



Integration options

POSITIVE TECHNOLOGIES PRODUCTS

MAXPATROL SIEM

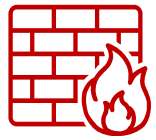
Passing of web-security events for further correlation

PT APPLICATION INSPECTOR

Formation of virtual patches for protection against exploits of current vulnerabilities

PT MULTISCANNER
PT SANDBOX

Protection of web portals against malware uploads



PT AF

OTHER SOLUTIONS

NGFW, SIEM (Syslog), DLP and AV systems (ICAP)

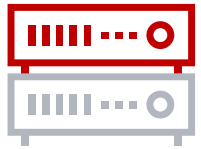
PT Application Firewall deployment

ptsecurity.com

Installation modes

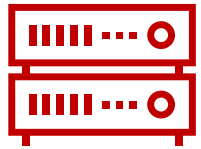
STANDALONE

- Product installation on one hardware or software platform
- Low cost
- Fail-safes not built in
- Ideal for applications of low to mid importance



ACTIVE—PASSIVE CLUSTER

- Product installation on two hardware or software platforms
- Includes fail-safe mode
- 50% of hardware is not working the majority of time
- Ideal for applications with heightened access requirements



ACTIVE—ACTIVE CLUSTER

- Product installation on two or more hardware or software platforms
- Even load distribution among nodes
- All licenses are active
- Ideal for high-load applications

How to get started with PT Application Firewall

ptsecurity.com

Form factors and licensing

APPLIANCES

Hardware Appliance

to be deployed on a physical server
Performance: up to 40,000 RPS

Virtual Appliance

to be deployed on a virtual machine
Performance: up to 10,000 RPS

ANNUAL LICENSE

Core license

Depending on number of requests per second (RPS)

Infrastructure licenses

Depending on number of cluster hosts

How to order a pilot

PT Application Firewall

01

Complete an application on the PT AF website

or **contact a Positive Technologies personal manager** or a partner company

02

Preparing

- survey, NDA
- goals, tasks
- report format

03

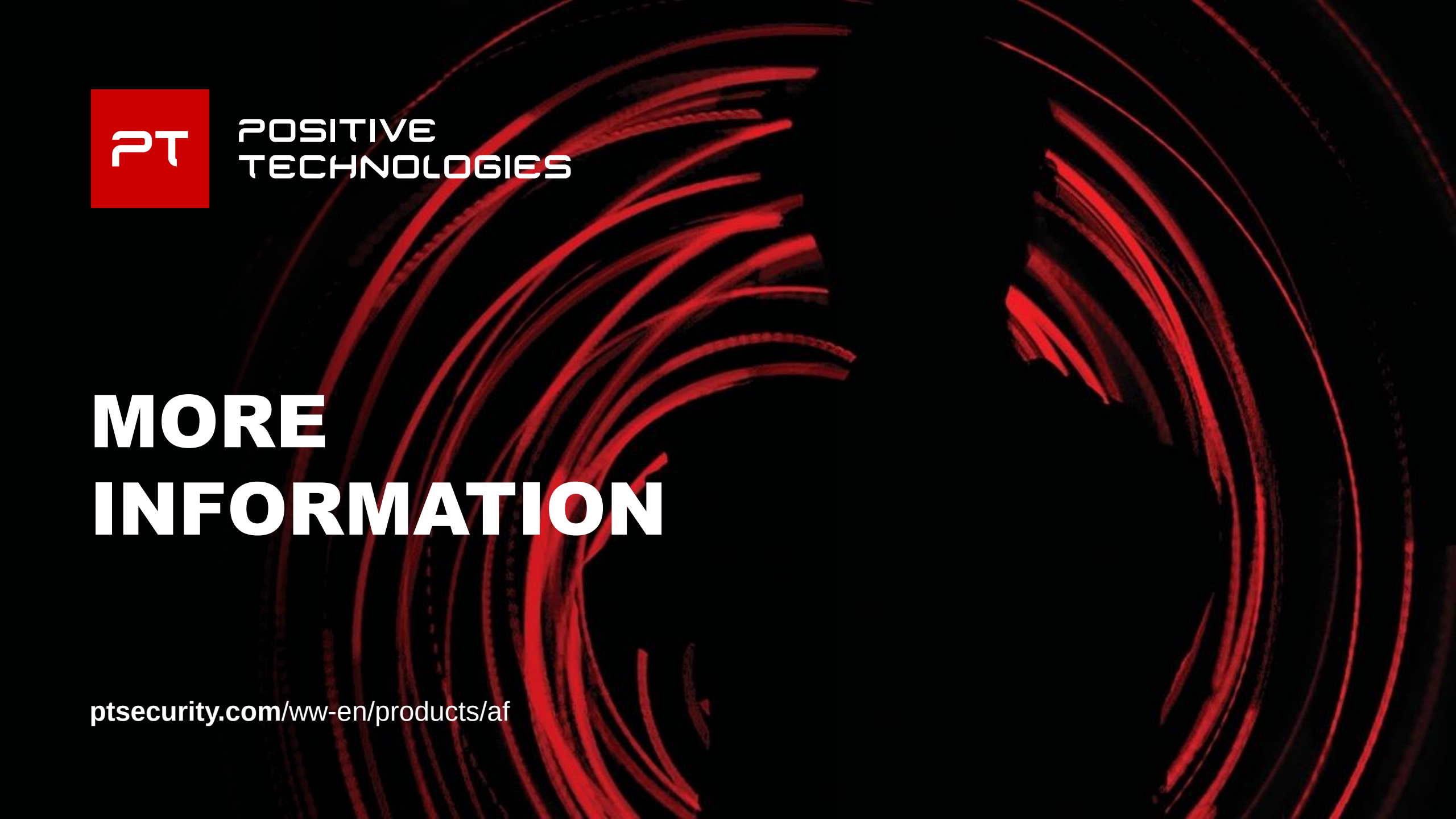
Testing and monitoring conducted by specialists from Positive Technologies or a partner company

04

Report on detected attacks

ptsecurity.com/ww-en/products/af/

3 – 4 WEEKS



MORE INFORMATION

ptsecurity.com/ww-en/products/af