## KEY BENEFITS

### Continuous proactive protection

- **Automated protection from 0-day attacks.** Advanced machine learning enables PT AF to proactively and accurately detect both known and unknown attacks, including 0-days. It also delivers a high level of automation.
- **Rapid identification of major threats.** Smart correlation techniques significantly reduce false positives, allowing you to focus on the most important incidents. Detailed attack chain metrics make forensic investigations more efficient.
- **Instant targeted protection.** PT AF's unique built-in source code analysis module (P-Code) detects vulnerabilities and creates instant "virtual patches."These block attempts to exploit the specific flaws in your code. PT AF can be also integrated with our application security testing (AST) tool PT Application Inspector™ to promote secure development processes.
- **Advanced L7 DDoS Protection.** Based on three application stress metrics (RPS, response time, and error rate), PT AF's continuous behavior profiling not only detects but also predicts L7 DDoS attacks. Early warning enables your security team to proactively prevent business disruption.
- **Essential help to ensure compliance with PCI DSS** and other international, national, and corporate standards.

### Quick and easy start

- **Deployment and configuration in a few clicks.** PT AF can be rapidly deployed in several modes (L2 Bridge, Transparent Proxy, etc.). Set-up time is also reduced thanks to standard WSC wizards, pre-defined security templates, automatic detection of protected apps, and other automated features available via the intuitive interface.
- **Pre-integrated with existing systems.** PT AF has plug-and-play support for many market-leading solutions such as antivirus, DLP, anti-DDoS, SIEM, and IPS, as well as Positive Technologies' advanced solutions such as PT Application Inspector™, PT MultiScanner™, and PT SIEM™. Third-party integrations include CheckPoint Security Gateway, Arbor Peakflow, Qrator, Array Networks, HP ArcSight, IBM QRadar, Zecurion Zgate, and other devices on request.
- **Automatic integration into existing infrastructure.** Support for Cisco ACI means PT AF™ can be rapidly added to networks of any size.

# PT APPLICATION FIREWALL™: PROACTIVELY PROTECT YOUR BUSINESS

## MARKET PROBLEMS AND CHALLENGES

In every enterprise—from finance, industry, telecom, IT, and media to government—the internet is reaching deeper into business than ever before. Previously time-consuming tasks are automated with websites, online storefronts, document management systems, inventory, e-banking, and other applications that streamline workflows. But these same technologies also create new opportunities for cybercriminals.

*Research by Positive Technologies in 2016 revealed at least medium-severity vulnerabilities in all the applications tested. 70% had one or more critical vulnerability, and the percentage of web applications with this level of flaw has grown consistently over the last three years.*

Most vulnerabilities in web applications result from developer errors. Traditional scanners, intrusion detection/prevention systems (IDS/IPS), and firewalls can't always detect these because:

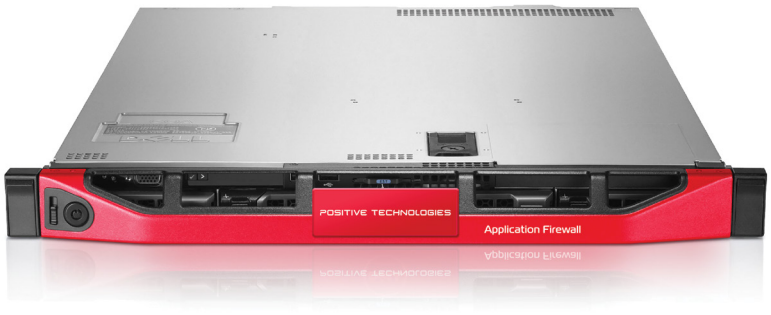
- Attackers often exploit 0-day vulnerabilities, making traditional signature analysis obsolete.
- Standard IDS and IPS generate thousands of alerts about suspicious events, which must be processed manually to identify actual threats.
- Many corporate sites and online services use customized solutions, including third-party modules, with unique vulnerabilities. Defending these applications requires advanced technologies that can thoroughly analyze the application structure, user interaction model, and usage context.
- Even well-known vulnerabilities cannot be fixed immediately. Patching code requires time and money, and sometimes even interrupts critical business processes. In the meantime, hackers can take advantage of the vulnerability.
- To protect critical applications and distinguish real attacks from normal operations, the application's business logic must also be considered.

## INTRODUCING PT APPLICATION FIREWALL

Positive Technologies Application Firewall™ (PT AF™) is a modern response to the evolving challenges of securing web portals, ERP systems, and mobile apps. Thanks to powerful technologies and innovative approaches, PT AF continuously and proactively protects apps from established attack techniques, including OWASP Top 10, client-side attacks, and automated attacks such as scraping, but also from unknown or emerging attacks (0-days).

PT AF is continuously updated based on our ongoing application security research, ensuring it maintains the highest levels of protection, usability, and interoperability.

Positive Technologies has been positioned as a Visionary in Gartner Magic Quadrant for Web Application Firewalls 2017 for three years running.



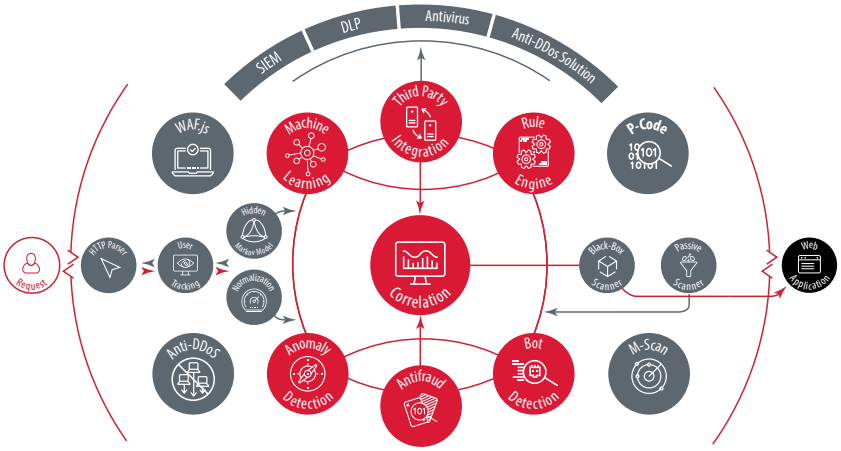
## ADDITIONAL CAPABILITIES

- **Supports multilayer protection.** PT AF can be deeply integrated with network layer security systems (Check Point, Arbor) enabling comprehensive protection of the organization's entire infrastructure against network and web attacks.
- **Promotes administrative efficiency.** PT AF's automation saves you time and money on set up and day-to-day administration. From one-click switching between deployment modes, to the granular management of security policies that can be saved and reused).
- **Utilizes business logic to identify attacks.** PT AF analyzes common application data protocols such as XML, JSON, and more. It then interprets and "sanity-checks" this data based on the application's business logic to differentiate attacks from normal operations.
- **Maximizes confidentiality for end-user data.** PT AF can identify and hide (mask) private data such as payment card numbers, passport information and insurance details from any third parties and even from the PT AF administrators.
- **Available everywhere.** PT AF can be deployed as a hardware appliance or virtual appliance, depending on your IT policy. It is fully cloud-ready (SaaS, VAS, MSS) and a great choice for secure application hosting. PT AF is also available in the public cloud (Microsoft Azure).

# HOW IT WORKS: MODULES AND MECHANISMS

PT Application Firewall provides comprehensive 360° protection with a wide range of specialized modules and mechanisms:

- **Hidden Markov Model (HMM)**, a self-learning module that blocks 0-day attacks and ensures advanced level of automation.
- **WAF.js** is a JavaScript module for protection against client-side attacks (XSS, DOM XSS, DOM Clobbering, CSRF) that runs in the user's browser every time a protected page is opened. The module also protects against robot programs of varying degrees of complexity, even those that can execute JavaScript by emulating the browser. WAF.js also detects hacking tools that are launched by clients when accessing the protected application.
- **P-Code module** identifies vulnerabilities in application source code and automatically generates rules (virtual patches) to block attacks based on those flaws.
- **Bot Mitigation** provides advanced bot detection based on a smart combination of signature-based and heuristic analysis. It blocks bot attacks without impacting on the activities of good bots.
- **M-Scan module** automatically scans user-uploaded and downloaded files using antivirus engines.
- **Passive Scanner** identifies application components (CMS, frameworks, libraries) passively in order to configure the normalization module, as well as detecting data leaks and known CVE vulnerabilities.
- **BlackBox Scanner** performs dynamic application security testing (DAST) and identifies application components, as well as assisting the self-learning engine and detecting application vulnerabilities.
- **Rule Engine** allows the creation of custom rules, including for all known CVE vulnerabilities.
- **SOA Firewall**, an XML analysis module that thwarts attacks on distributed web services. The normalization mechanism sanitizes data and headers of HTTP requests, taking the server context into account. This prevents most firewall bypass methods (such as HPC, HPP, and Verb Tampering).




## TAKE PT APPLICATION FIREWALL™ FOR A TEST DRIVE

Want to try a free pilot of PT Application Firewall™ at your organization? Get in touch at af.ptsecurity.com

## About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.



POSITIVE TECHNOLOGIES

info@ptsecurity.com ptsecurity.com