Positive Technologies
Application Firewall™

DATA SHEET
Almost every modern enterprise uses hundreds of Web, mobile or ERP applications to help run their operations. But as your number of applications grows, so does the number of security vulnerabilities that could be exploited to damage your business.

The Verizon 2014 Data Breach Investigation Report (DBIR) shows that last year 35% of security breaches involved attacks against web applications, up by 14% since 2012. Moreover, Web app attacks were the most common cause of data breaches, followed by cyber-espionage, POS intrusion and insider misuse.

1. APPLICATION SECURITY: KEY CHALLENGES

What kind of application vulnerabilities are used by attackers? According to Positive Technologies research on enterprise apps for financial institutions, only one third of problems are due to bad patch management and configuration flaws. Most threats are caused by developers’ mistakes that cannot be addressed with traditional security scanners, IDS or firewalls.

As a result, the average security level of corporate infrastructures has considerably decreased in recent years. Here are the main challenges faced by modern AppSec systems:

+ The implementation of a Secure SDL should dramatically reduce the cost of code errors as long as they are found and fixed at the early stages of coding, but it’s hard to find effective automated solutions for code analysis.

+ Modern corporate applications use different languages, protocols and technologies, as well as customized solutions and third party code. Protection of such applications requires thorough analysis of the application structure, user interaction patterns and usage context.

+ Attackers often exploit zero-day vulnerabilities, making signature analysis obsolete and confirming the need for adaptive solutions, self-learning and behavioral analysis techniques.

+ Modern firewalls deal with thousands of suspicious incidents. There is no time for security specialists to check them all manually to identify the real threats. There is an urgent need for automatic sorting, ranking and smart visualization of security events.

+ Even well-known vulnerabilities cannot be fixed immediately; patching of ERP or e-banking systems can take months. An application security system should have a mechanism to mitigate breaches while developers are fixing the code.
2. MEET PT AF™: GENERAL FEATURES AND CAPABILITIES

PT Application Firewall™, a smart protection system developed by Positive Technologies, is a serious response to the security challenges created by today's range of web portals, ERP and mobile applications. PT AF™ can block 30% more network attacks than other firewalls thanks to several innovative security technologies:

- **Fast adaptation to your system.** Instead of applying the classical signature method, PT AF™ analyzes network traffic, logs and users’ actions, constantly creating and maintaining a real-time statistical model of the application during normal operation. It then uses this model to detect abnormal system behavior. Together with other protection mechanisms, it ensures 80% of zero-day attacks are blocked without any special adjustment needed within the client.

- **Focus on major threats.** PT AF™ weeds out irrelevant attack attempts, groups similar incidents and detects the attack chains — from spying to data theft or backdoor setup. Instead of security specialists working through thousands of potential attacks, they just receive the messages that appear most serious.

- **P-Code: Instant Blocking.** Our virtual patching technique allows you to protect an application, even before insecure code is fixed. However, most WAFs require manual work for every virtual patch creation. The unique PT technology for source code analysis with exploit generation mechanism (P-Code) provides automated vulnerability detection and a virtual patch creation for PT Application Firewall™. The same P-Code module provides developers with exact information about incorrect code, greatly reducing the costs of correction and testing.

- **Protection against security bypass.** PT AF™ handles data with regard to a protected server technology stack, analyzes XML, JSON and other protocols typically used in modern portals and mobile applications. It ensures protection from the majority of firewall bypass methods including HPC, HPP and Verb Tampering.

- **Behavioral analysis against robots.** The mechanisms used against automated malware include protection from brute-force attacks, fraud, DDoS attacks, botnets, uncontrolled indexing, and data leakage.

* Positive Technologies is rated as a Visionary because of its unique, leading-edge security features. Organizations that are looking for high security first should consider adding Positive Technologies to their shortlists .

(Gartner Magic Quadrant for Web Application Firewalls 2015)

**ADDITIONAL CAPABILITIES:**

- Protection against all common vulnerabilities recognized by OWASP and WASC, including SQLi, XSS and XXE, as well as against HTTP Request Splitting, Clickjacking and complicated client-side attacks (DOM-based XSS).

- Proactive defense of queries, data and cookies allows you to block attacks such as CSRF, even if developers have overlooked the necessary security tools.

- Effective integration into your company’s information security management system: integration with antiviruses and DLP, anti-DDoS and SIEM.

- Anti-fraud and anti-bot mechanisms include reputation and profiling services, which detect client’s abnormal behavior (e.g., login from an unusual address).

- Compliance with PCI DSS and other international, national and corporative security standards.
3. USE CASES: SPECIAL CONDITIONS

With more than 10 years of security research and a huge knowledge base of vulnerabilities, the experts at Positive Technologies have amassed extensive experience in protecting enterprises of all sizes across a wide range of industries. Each industry has its own unique features and requirements that are crucial to its practical security. Every deployment of PT Application Firewall™ includes configuration to meet the specific needs of each client.

Banks and Financial Institutions

Unique Challenges: Many critical applications used both by clients and partners including: Internet Banking, Core Banking Systems, CRM, Trading, etc. Many third-party applications in which banks cannot fix the vulnerabilities themselves. 24/7/365 operations leaves little scope for developing and deploying vulnerability fixes. Usage of legacy systems, which have poor or no protection. Attention focused on malicious users; manual and automated attacks. Requirements of PCI DSS and other regulatory authorities.

PT Solutions:
- Detection of backdoors, sensitive information and clear-text data flows
- Self-learning mechanisms based on hidden Markov models
- Monitoring and fingerprinting of users, web fraud detection
- Virtual patching

Media

Unique Challenges: Applications are available to any Internet user. Frequently refreshing content and integration with a wide range of other sites (advertising, social media, partners, etc.) Online streaming and XML gateways for data communication. Attacks of “hacktivists”, rivals and criminals.

PT Solutions:
- Automatic learning using application parameters
- Protection from application-level DoS attacks
- Protection of XML applications
- Detection of site compromises and data leakages
- Behavioral analysis: detection of abnormal activity, particularly caused by robots

Telecoms

Unique Challenges: Lots of different applications including self-service portals, VAS/ MSS portals for clients, mobile and cloud applications. Convergence and close integrations lead to “avalanche” reactions, where a failure in one element creates issues in all elements of the enterprise. Integration of simple mass services with payment systems raises the danger of fraud.

PT Solutions:
- Support of VAS/MSS model protection of clients’ applications
- Behavioral analysis: detection of abnormal activity, robots, protection from fraud
- Protection from application-level DoS attacks
- Protection of mobile application versions

Utilities

Specific problems: An ERP system is the heart of the modern enterprise: accounting, management, purchasing and many other processes are implemented here. Today, these systems often have Internet access (like SRM, CRM, and HCM) and are connected through integration gateways. Such systems are often maintained and supported by integrator companies, which means they’re controlled remotely and security mechanisms are weakened for simplicity. The developers of business-application code tend to be more concerned with functionality rather than security. The systems are often modified. 24/7/365 operations leave little scope for developing and deploying vulnerability fixes.

PT Solutions:
- Pre-learned modules for portal SAP solutions
- Protection from XML-related attacks
- Virtual patching
To provide precise and impenetrable protection of Web, Mobile and ERP applications, PT Application Firewall™ uses a multi-layer defense scheme with many specialized modules:

**User Activity Tracking** – helps to fingerprint user, browser and related activity to detect bots and automated tools, manage access via Access Control Lists and prevent web-fraud.

**Web Engine** – is a built-in Dynamic Application Security Testing (DAST) module for active fingerprinting of application components (CMS, Frameworks, Libraries), training the self-learning engine and detecting vulnerabilities in the application. The web engine can work in “on-access” mode for quick verification of vulnerabilities probed by attackers.

**Passive Scan** – passively fingerprints application components (CMS, Framework, Libraries, etc.) to tune Normalization module and to detect known (CVE-based) vulnerabilities and data leakage.

**Normalization** – rebuilds HTTP data and headers according to backend Web-application fingerprints (Web server, Language, Frameworks) to prevent protection bypass by HPP, HPC and other data manipulation attacks.

**3rd party Integration** – PT AF™ uses built-in AV engine and sensitive data detection rules but can be integrated with external Antivirus and DLP solution for industrial protection. To fight massive DDoS attacks, the firewall can report the bots’ IP-addresses to external AntiDDoS solutions such as Arbor.

**Black and White Lists** – traditional signature-based protection rules can be created automatically by integration with static and dynamic Application Security Testing tools or Anomaly Detection engines.

**Heuristics** – based on self-learning artificial intelligence algorithms PT AF™ constantly tracks application structure and parameters to detect traditional and 0-day attacks.

**Anomaly, AntiFraud and Bot Detection** – work together to protect against web fraud, automated crawling and URL brute force. These modules help to identify abnormal user and server activity such as slow responses during application-level DDoS attacks.

**Correlation** – helps to reduce number of alerts and to highlight important incidents based on application fingerprints, vulnerabilities, user tracking and attack history. Builds attack chain metrics to simplify forensics.

**P-Code Module**: detects source code vulnerabilities and automatically creates the blocking rules (virtual patches) providing the instant protection of the application, before the insecure code is fixed.
5. ATTACK-AND-DEFENSE SCENARIOS

Typical attacks consist of several stages. Let us see how PT Application Firewall™ reacts to each element of the intruder’s activity to protect the application in real time.

**Step #1. Reconnaissance.** An intruder studies the application’s logic and architecture and learns what kind of services, software components and frameworks are used. PT Application Firewall™ passively fingerprints the application’s components with its Passive Scanner Module and tunes the Normalization and Protection engines according to specific system behavior and vulnerabilities. This allows PT AF™ to maximize detection rates and prevent potential bypassing. PT AF’s™ UAT Module tracks user activity. Massive scanning attempts will be detected by the Bot Detection Module.

**Step #2: Vulnerability Detection.** While an attacker is trying to actively detect a vulnerability, PT AF™ uses its built-in DAST Web Engine to confirm the presence of the targeted flaw. If a weakness is confirmed, all related attacks will get the highest priority. The Self-learning Hidden Markov Model (HMM) module can alert (or optionally block) an attack even in its earliest stages.
Step #3. Exploitation. Once an intruder has identified vulnerabilities in the application, they try to exploit them to crash the system or to get access to sensitive data. PT Application Firewall™ blocks the attack thanks to machine learning algorithms that can detect anomalies in data structure as well as in user behavior.

Step #4: Action on objectives. If the system is breached via side channels (trojans, insiders, physical intrusions), PT AF™ allows you to detect and block attacks that use the infected server for information exfiltration (theft) or to spread malware. PT AF’s™ built-in Anti-Malware and Data Control engines can be supplemented with your existing external antivirus or DLP solution via PT AF’s™ flexible integration API.
Step #5. Virtual Patching with P-Code technology. The latest WAF solutions assign custom blocking rules to protect insecure code that is hard, or impossible, to patch. However, most WAF’s require manual patching and manual application analysis. Third-party dynamic scanners allow you to detect a limited number of vulnerabilities due to the lack of source code analysis.

With PT Application Firewall™, clients can enable the P-Code module, which combines the advantages of static, dynamic, and interactive code analysis (SAST, DAST, IAST), for automated virtual patching. For each detected vulnerability, P-Code calculates a specific set of insecure parameters and their values (exploit), and automatically generates a blocking rule without requiring any human intervention. This automated process results in a reduction in hands-on maintenance resource requirements and therefore a reduction in personnel costs whilst developers get the detailed vulnerability data (i.e. exploits and exact launch parameters) sufficient for fixing the insecure code.
6. DEPLOYMENT MODELS

PT Application Firewall™ can be deployed as a virtual appliance, hardware appliance or as Software as a Service (SaaS). It can also be configured in one of the following three modes:

1. **In-line Mode**
   - Traffic is routed through Application Firewall, which actively detects and prevents attacks.

2. **Mirror Mode**
   - A router mirrors traffic to Application Firewall, which then detects potential threats and alerts your existing security systems.

3. **Off-line Mode**
   - Application Firewall examines logs for evidence of previous attacks for forensic analysis.
7. HIGH PERFORMANCE AND AVAILABILITY

PT AF™ is designed with high availability in mind. It can be deployed either in active-active or active-passive mode. Enterprises can benefit from the kernel load balancing built-in to PT AF™ as well as using an external load balancer.

**Active-Active High Availability:**

Built-in load balancing, caching and Active-Active cluster creates a highly-performant and reliable application.

**Active-Active High Availability:**

Active-Active cluster can be integrated with external load balancers.

**Active-Passive High Availability:**

Active-Passive cluster supports two-node operations with built-in load balancing.

**Active-Passive High Availability:**

Active-Passive cluster can be integrated with external load balancers.
# 8. PT AF™: HARDWARE SPECIFICATIONS

<table>
<thead>
<tr>
<th>Platform</th>
<th>Cisco UCS E-Series</th>
<th>PTAF-CH100</th>
<th>PTAF-CH200</th>
<th>PTAF-CH300</th>
<th>VAF</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>PTAF-H1K-S(HA)</td>
<td>PTAF-H100K-S(HA)</td>
<td>PTAF-H5K-S(HA)</td>
<td>PTAF-H10K-S(HA)</td>
</tr>
<tr>
<td>Requests per second</td>
<td>Up to 1,000</td>
<td>1,000</td>
<td>10,000</td>
<td>Up to 100,000</td>
<td>Up to 10,000</td>
</tr>
<tr>
<td>Concurrent Connection</td>
<td>N/A</td>
<td>25,000</td>
<td>150,000</td>
<td>300,000</td>
<td>N/A</td>
</tr>
<tr>
<td>Connection Per Second</td>
<td>N/A</td>
<td>3,000</td>
<td>30,000</td>
<td>70,000</td>
<td>N/A</td>
</tr>
<tr>
<td>Transaction Per Second</td>
<td>N/A</td>
<td>5,000</td>
<td>45,000</td>
<td>100,000</td>
<td>N/A</td>
</tr>
<tr>
<td>HTTP Throughput</td>
<td>N/A</td>
<td>100 Mbps</td>
<td>500 Mbps</td>
<td>1 Gbps</td>
<td>2 Gbps</td>
</tr>
<tr>
<td>Network Bypass ports</td>
<td>Unsupported</td>
<td>1 bypass network card</td>
<td>4 ports 1Gb RJ-45 (Copper)</td>
<td>4 ports 1Gb Fiber SR (MMF)</td>
<td>Up to 2 bypass network cards:</td>
</tr>
<tr>
<td>Network ports</td>
<td>2 x 1Gb internal 1 x 1Gb RJ-45 external</td>
<td>4 x 1Gb RJ-45</td>
<td>4 x 1Gb RJ-45</td>
<td>4 x 1Gb RJ-45</td>
<td>N/A</td>
</tr>
<tr>
<td>SSL HW Acceleration</td>
<td>Unsupported</td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
<td>N/A</td>
</tr>
<tr>
<td>CPU</td>
<td>Intel® Xeon® E3-1105C v2</td>
<td>2 x Intel® Xeon® ES-2420 v2</td>
<td>2 x Intel® Xeon® ES-2650 v2</td>
<td>4 x Intel® Xeon® ES-4640 v2</td>
<td>N/A</td>
</tr>
<tr>
<td>Memory</td>
<td>8 GB RAM</td>
<td>32 GB RAM</td>
<td>64 GB RAM</td>
<td>128 GB RAM</td>
<td>min 8 GB RAM</td>
</tr>
<tr>
<td>HDD</td>
<td>2 x 1 TB 7.2K SATA (RAID 1)</td>
<td>2 x 600 GB 10K SAS (RAID 1)</td>
<td>4 x 10K SAS (RAID 1)</td>
<td>min 500 GB</td>
<td></td>
</tr>
<tr>
<td>Power</td>
<td>Internal power</td>
<td>Dual, Hot-plug, Redundant Power Supply (1+1), 350W</td>
<td>Dual, Hot-plug, Redundant Power Supply (1+1), 780W</td>
<td>Dual, Hot-plug, Redundant Power Supply (1+1), 1100W</td>
<td>N/A</td>
</tr>
<tr>
<td>Size (W x D x H)</td>
<td>Blade form factor 18.9 x 19.1 x 4 cm (7.44 x 7.5 x 1.58 in)</td>
<td>1RU 48.24 x 60.7 x 4.28 cm (19 x 23.9 x 1.7 in)</td>
<td>1RU 48.24 x 70.05 x 4.28 cm (19 x 27.58 x 1.7 in)</td>
<td>2RU 48.24 x 77.76 x 8.68 cm (19 x 30.61 x 3.42 in)</td>
<td>N/A</td>
</tr>
<tr>
<td>Weight</td>
<td>11 kg (2.5 lb)</td>
<td>14.8 kg (32.63 lb)</td>
<td>15.6 kg (34.6 lb)</td>
<td>21.5 kg (47.4 lb)</td>
<td>N/A</td>
</tr>
<tr>
<td>Warranty</td>
<td>3Yr NBD support</td>
<td>3Yr NBD support</td>
<td>3Yr NBD support</td>
<td>3Yr NBD support</td>
<td>3Yr NBD support</td>
</tr>
</tbody>
</table>
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.

© 2016 Positive Technologies. Positive Technologies and the Positive Technologies logo are trademarks or registered trademarks of Positive Technologies. All other trademarks mentioned herein are the property of their respective owners.

info@ptsecurity.com  ptsecurity.com