Positive Technologies Application Firewall™

DATA SHEET

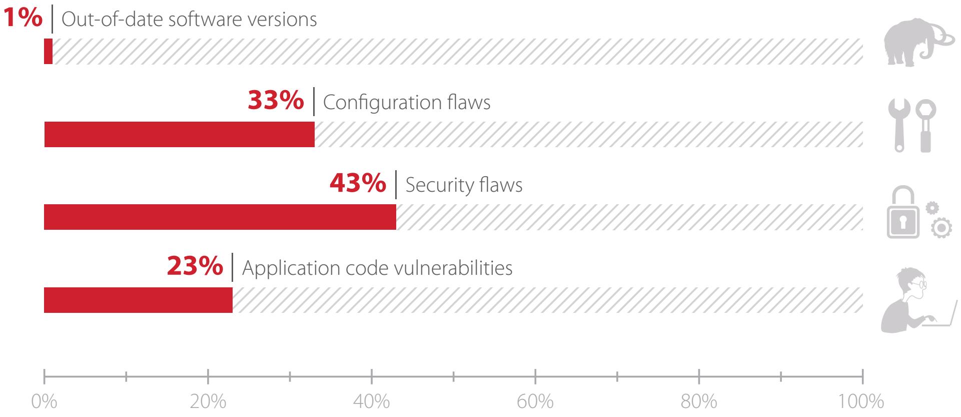
POSITIVE TECHNOLOGIES

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 volume of security vulnerabilities that could be exploited to damage your business.

The Verizon 2016 Data Breach Investigation Report (DBIR) found web application attacks are the #1 source of data breaches. It also revealed the percentage of data breaches caused by web app attacks in 2016 was 40 percent—up from around 9 percent in 2015.

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, IDSs or firewalls.



Types of security vulnerabilities

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, so 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 mechanisms to mitigate the risk of breaches while developers are fixing the code.

2. MEET PT APPLICATION FIREWALL™

PT Application Firewall™ (PT AF™), a smart protection solution 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 provides comprehensive protection against all common attack types 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). This is possible thanks to its powerful combination of innovative technologies and approaches:

- **Continuous, real-time protection.** Instead of applying the classical signature method, PT AF analyzes network traffic, logs and users' actions, creating and constantly maintaining a real-time statistical model of the application during normal operation. It uses this model to detect abnormal system behavior. Together with other protection mechanisms, this ensures zero-day attacks are blocked without any special adjustment needed within the client.
- **Focus on major threats.** PT AF automatically detects attack chains—from spying to data theft or backdoor setup. Instead of security specialists working through thousands of potential attacks, they receive alerts on only the most serious risks.
- **P-Code: Instant Blocking.** Our virtual patching technique (P-Code) allows you to protect an application, even before insecure code is fixed. While most WAFs require each patch to be created manually, PT AF combines our unique source code analysis technology with a secure exploit generation mechanism. This enables automated creation of virtual patches based on detected vulnerabilities.
- **Advanced L7 DDoS Protection.** Based on three application stress metrics (RPS, response time, and errors rate), PT AF not only detects L7 DDoS attacks but can also predict and prevent them. The product performs continuous behavior profiling using machine learning algorithms, dealing with all incoming HTTP requests and application health status. DDoS attacks are predicted and security engineers notified so they can proactively implement the action plan without any business disruption. Thanks to a high level of automation, minimal human involvement is required. PT AF's extended range of features eliminates the need for third-party DDoS L7 monitoring tools.
- **Bot Mitigation.** Automatic profiling of user behavior also allows you to quickly detect automated attacks (“crawlers”, “spammers”, and other intrusion tools). But because PT AF does not block search bots, it doesn’t prevent sites being indexed.
- **Data Leakage Prevention.** All outbound traffic is monitored and any sensitive data is blocked (masked) automatically, without any human intervention.
- **Maximum confidentiality for end-user data.** To enhance protection for application users, administrators can create special rules to detect sensitive data such as payment card numbers, passport information, insurance details, etc. Further rules can be used to mask this information from third parties or even from administrators using PT AF itself.

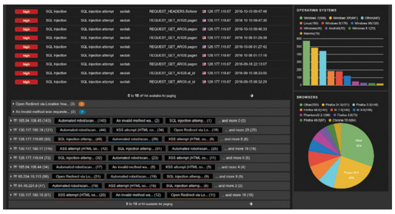
Positive Technologies has been positioned as a Visionary in Gartner Magic Quadrant for Web Application Firewalls 2017 for three years running.

ADDITIONAL CAPABILITIES:

- **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, as well as with the third-party solutions, such as Check Point, Arbor, etc., to provide advanced multilayer protection.
- **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 (HTTP Parameter Contamination), HPP (HTTP Parameter Pollution).
- **Compliance with PCI DSS** and other international, national, and corporate security standards.

3. USE CASES: SPECIAL CONDITIONS

With more than 15 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 leave 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 AF 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
- Ability to support normal app operations while minor defects are being fixed
- Enhanced protection for end-users' confidential data such as credit card numbers

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 by "hacktivists," rivals, and criminals.

- Automatic learning using application parameters
- Protection from application-level DDoS attacks
- Detection of site compromise and data leakage
- Signature-based and heuristic mechanisms as well as reputation services are used to detect clients' suspicious behavior

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 parts of the enterprise.
- Integration of simple mass services with payment systems raises the danger of fraud.

- Support of VAS/MMS model: protection of clients' applications
- Signature-based and heuristic mechanisms as well as reputation services are used to detect clients' suspicious behavior
- Protection from application-level DoS attacks
- Protection of mobile application versions

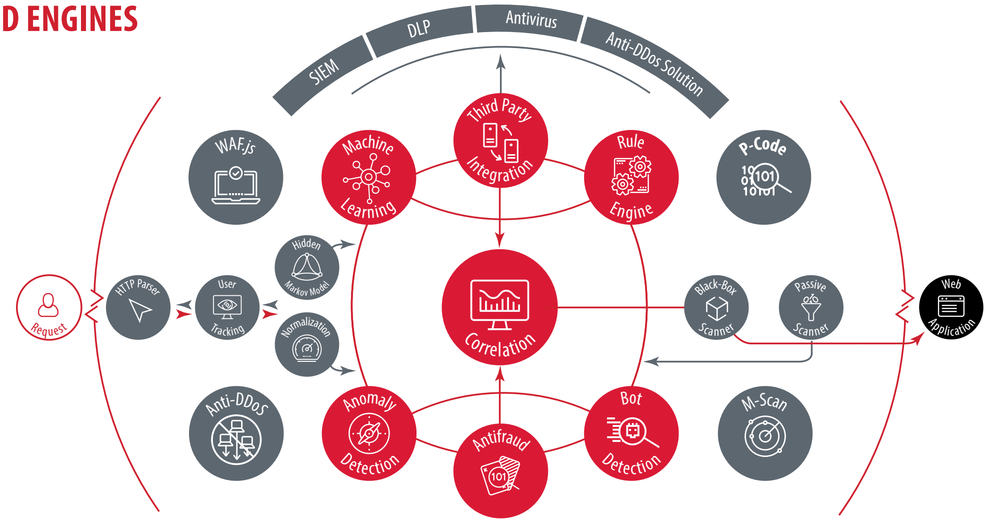
Utilities

Unique challenges:

- ERP systems control many processes including accounting, management, purchasing, etc., with internet access (like SRM, CRM, and HCM) through integration gateways.
- Systems often maintained and supported by integrator companies, requiring remote control.
- Security mechanisms may be weakened to simplify remote access.
- Developers of business applications are often more focused on functionality than security.
- Systems require regular modification.
- 24/7/365 operations leave little scope for developing and deploying vulnerability fixes.

- Pre-learned modules for portal SAP solutions
- Protection from XML-related attacks
- Virtual patching

4. HOW IT WORKS: MODULES AND ENGINES



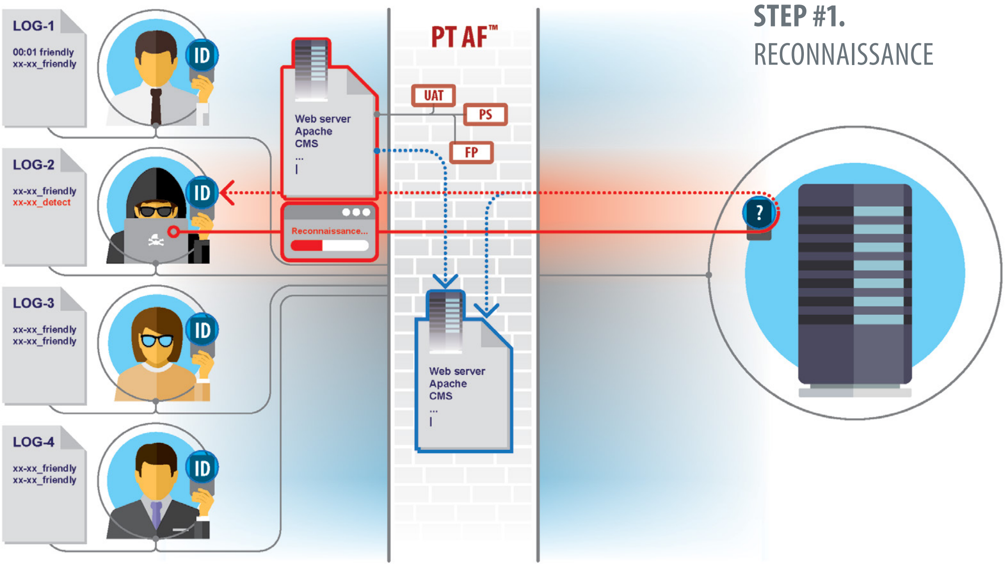
To provide precise and impenetrable protection of web, mobile, and ERP applications, PT Application Firewall™ uses a multilayer defense scheme with many specialized modules:

- **User Tracking** allows administrators to analyze session data, including the geolocation of the user account that is used to access the protected application. This enables the PT AF administrator to add blocking rules per user and/or user group, and manage access via Access Control Lists. In the case of suspicious activity, they can also identify security incidents to prevent web fraud. Additionally, PT AF™ can detect multiple unsuccessful login attempts and link such incidents together to quickly identify and block brute-force attacks.
- **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 be used for rapid verification of vulnerabilities probed by attackers.
- **Passive Scan** passively fingerprints application components (CMS, Framework, Libraries, etc.) and detects 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.
- **Third-party Integration.** PT AF uses built-in AV engine and sensitive data detection rules but can also be integrated with external antivirus and DLP solutions for industrial protection. To fight massive DDoS attacks, PT AF can report the bots' IP-addresses to external anti-DDoS solutions, such as Arbor.
- **Rule engine** allows the creation of custom rules, including for all known CVE vulnerabilities. Additional geolocation tuning supports the creation of blocking rules and exclusions based on particular geolocations, providing targeted protection against attacks from specific regions.
- **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.
- **Heuristics.** Based on self-learning artificial intelligence algorithms, PT AF constantly tracks request attributes to detect known and unknown (0-day) attacks.
- **Correlation** helps to reduce the number of alerts and to highlight important incidents based on application fingerprints, vulnerabilities, user tracking, and attack history. It also builds attack chain metrics to simplify forensics.
- **Data masking** ensures the confidentiality of end-user data such as payment card numbers, passport data, insurance details, etc. It also supports web applications to continue functioning normally until any minor defects detected in them have been fixed.

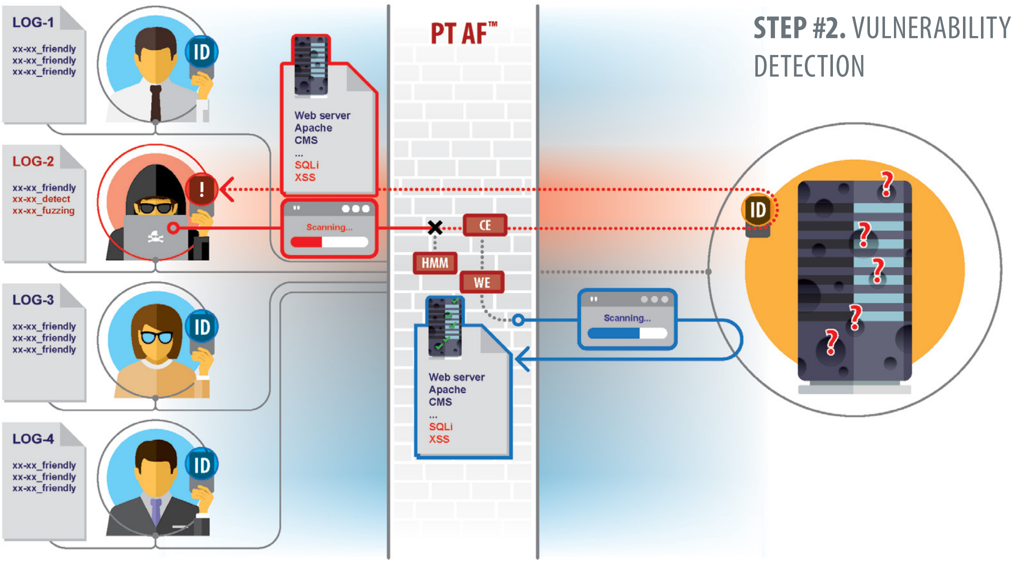
The unique P-Code Module detects source code vulnerabilities and automatically creates blocking rules (virtual patches) to provide instant protection for the application. This buys time for developers to fix the insecure code.

5. ATTACK-AND-DEFENSE SCENARIOS

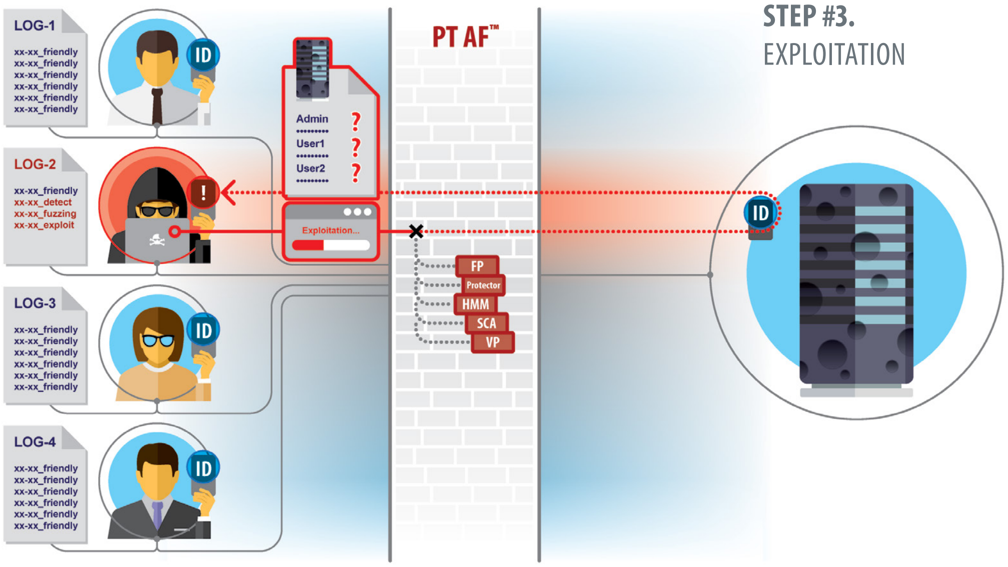
Typical attacks consist of several stages. Let us see how PT Application Firewall reacts to each element of the intruder's activity to protect the application in real time.



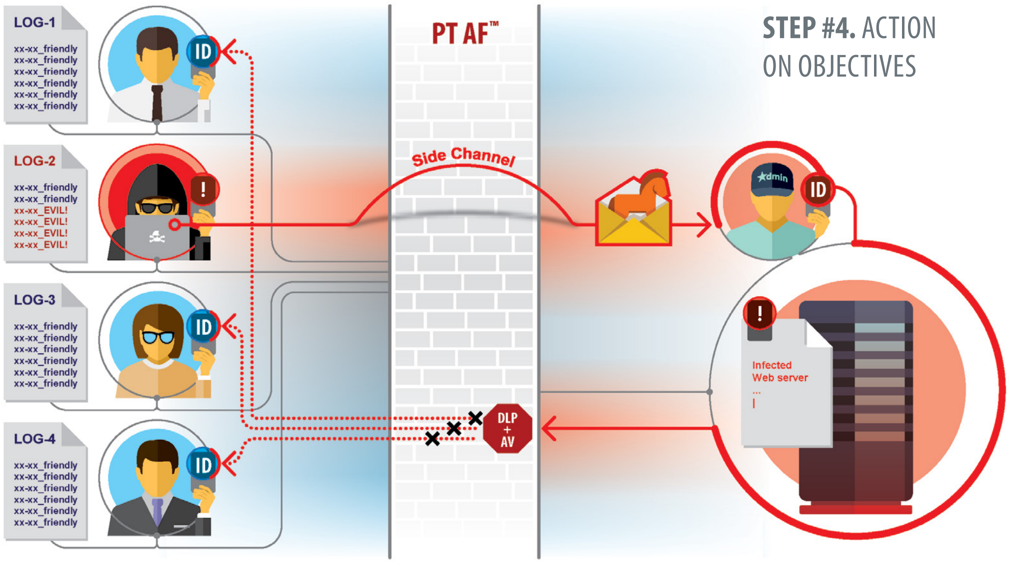
Step #1. Reconnaissance. An intruder studies the application's logic and architecture and learns what kind of services, software components, and frameworks are used. PT Application Firewall Normalization and Protection engines can be configured according to the specific behavior of the protected application. This allows PT AF to maximize detection rates and prevent potential bypassing.



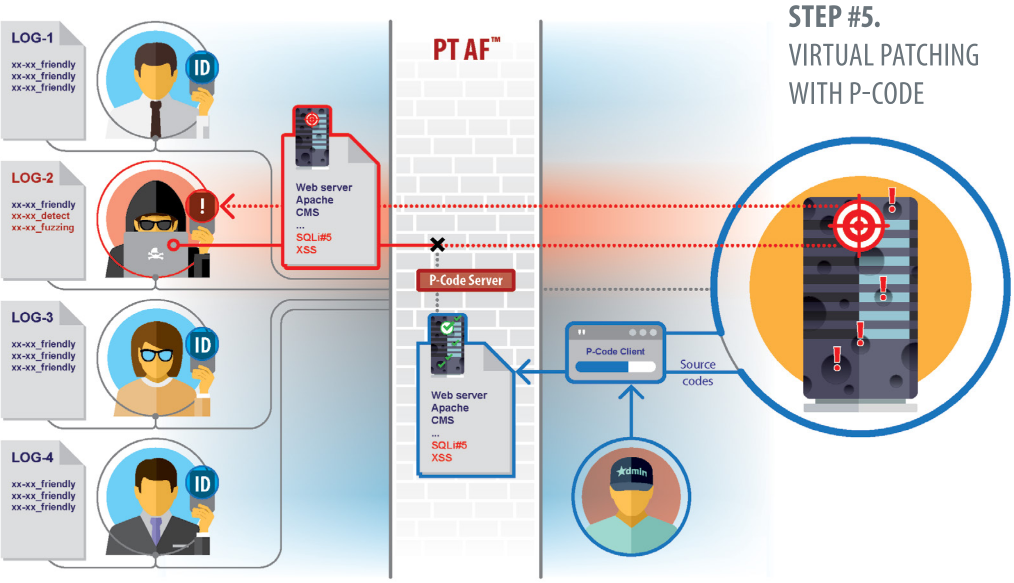
Step #2. Vulnerability Detection. While an attacker is trying to actively detect a vulnerability, PT AF uses its built-in DAST Web Engine to confirm the presence of the targeted flaw. The Self-Learning Hidden Markov Model (HMM) module can alert (or optionally block) an attack even in its earliest stages.



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.



Step #4. Action on objectives. If the system is breached via side channels (trojans, insiders, physical intrusions, etc.), 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 the PT AF flexible integration API.



STEP #5.
VIRTUAL PATCHING
WITH P-CODE

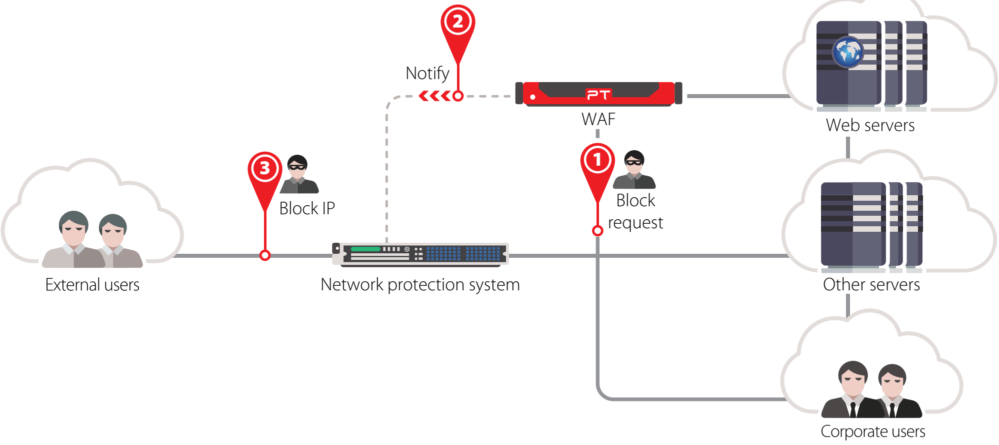
Step #5. Virtual Patching with P-Code technology. The latest WAF solutions assign custom blocking rules to protect insecure code that is hard, or impossible, to patch. However, most WAFs require manual patching and manual application analysis. Third-party dynamic scanners allow you to detect only a limited 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 reducing manual efforts.

6. MULTILAYER PROTECTION SCENARIO

PT AF is a flexible solution that can be integrated with other Positive Technologies and third-party systems aimed at protecting network communication layers (e.g., Check Point, Arbor). The result of this integration is a combined protection mechanism that can accurately detect attacks based on fully synchronized and smart correlation of security incidents from all systems. This provides comprehensive protection from most common network and web attacks.

PT AF detects a suspicious request, blocks it, and immediately notifies the network protection system about the suspicious IP address. The network protection system immediately blocks the source of the threat throughout the organization.

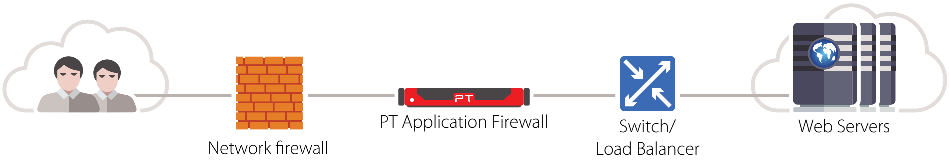


7. DEPLOYMENT OPTIONS

PT Application Firewall can be deployed as a virtual appliance, hardware appliance or as Software as a Service (SaaS), and is available in public cloud (Microsoft Azure).

PT Application Firewall can be deployed in one of the following modes:

1



In-line Mode

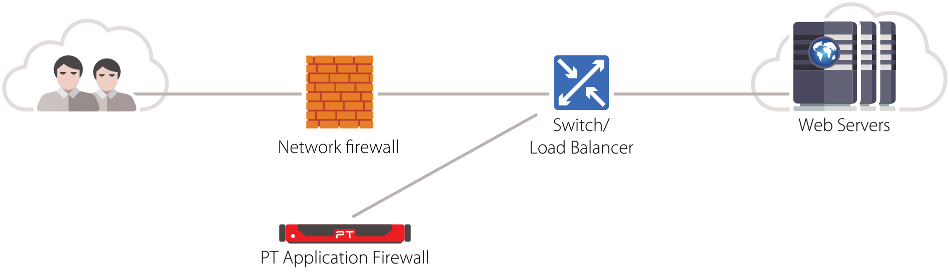
Three deployment schemes are available:

- Reverse Proxy
- Transparent Proxy
- L2 Bridge (detection mode only)

Traffic is routed through PT Application Firewall, which actively detects and prevents attacks.

Administrators can easily and quickly switch between Transparent Proxy and L2 Bridge via the PT AF web interface.

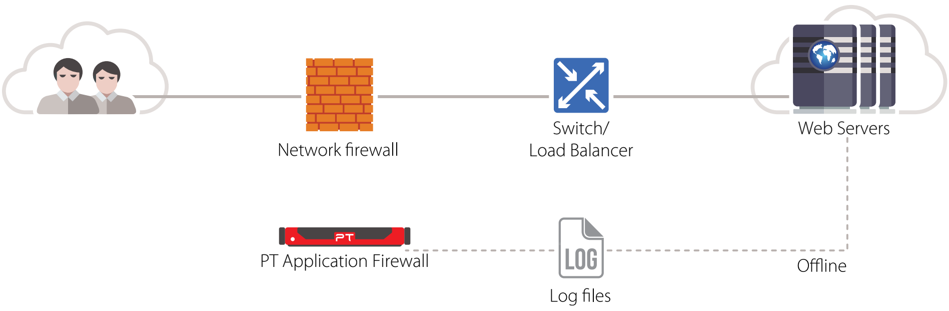
2



Mirror Mode

A router mirrors traffic to PT Application Firewall, which then detects potential threats and alerts your existing security systems.

3



Offline Mode

PT Application Firewall examines logs for evidence of previous attacks for forensic analysis.

8. SETUP AND CONFIGURATION

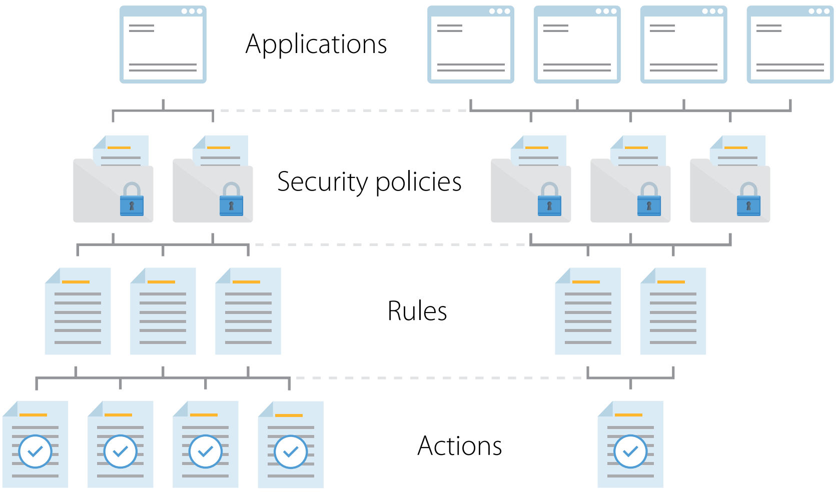
PT AF requires little setup and configuration time thanks to following capabilities:

- **Standard WSC wizards and convenient interface.** Administrators can use standard CLI scenarios and PT AF's intuitive web interface to rapidly finalize deployment settings.
- **Automatic detection of protected resources.** While utilizing Transparent Proxy, Bridge, and Mirror deployment modes there is no need for administrators to remember all protected resources as they are detected automatically. After the preliminary product setup is complete, the UI displays information about all protected applications. A range of flexible management options are supported including filter, sort, add, remove, etc.
- **Flexible security policies.** PT AF includes pre-defined security templates. This means administrators can quickly set up required security policies that can be defined:
  - **By level of security** (high, middle, low)
  - **By hierarchy** (for example: a general policy for multiple apps or individual policies for each separate app)
  - **By function** (allowing different policies to be applied to each part of an app such as the public-facing elements, personal account, administration interface, etc.)
- **Flexible settings within security policies.** PT AF includes a unified base of rules that is automatically applied to all security policies. So there is no need to create separate rules for each security policy. Administrators can also apply different system actions like blocking or logging to each rule, depending on the criticality of the protected application. This does not require any changes to be applied to the security policies themselves. This means administrators can control the level of PT AF protection at a granular level while significantly reducing the time and effort required for such fine-tuning. This is especially important when working with a large number of apps.

ADDITIONAL CAPABILITIES:

- **Auto-restore for system configuration.** If the system configuration fails, previously saved settings can be automatically restored. This reduces manual effort and is particularly useful for administrators working remotely from the PT AF appliance.
- **Ability to specify stored data length.** There is no need to store all data, if certain parameters are of little long-term value. Administrators can specify which parts of lengthy data (Request POST Data, Matched arguments value, Request / Response headers, etc.) should be stored. This reduces the risk of database overload and speeds up searches by reducing the size of the stored data set.

PT AF configuration flexibility



PT AF offers in-depth fine-tuning capabilities to meet the needs of any kind of security hierarchy:

- Each app or set of apps can be protected by one or many policies
- Each policy or set of policies can be regulated by one or many rules
- Each rule or set of rules can trigger one or many actions

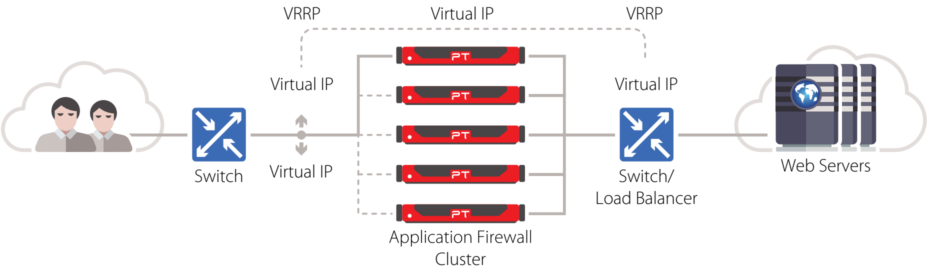
Once settings are configured, they can be saved as a template for future use, eliminating repetitive configuration tasks.

9. 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.

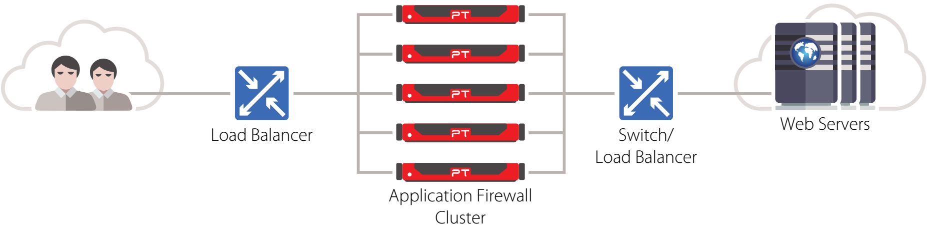
1

Active—Active High Availability:
Built-in load balancing, caching and Active—Active cluster create a highly-performant and reliable application.



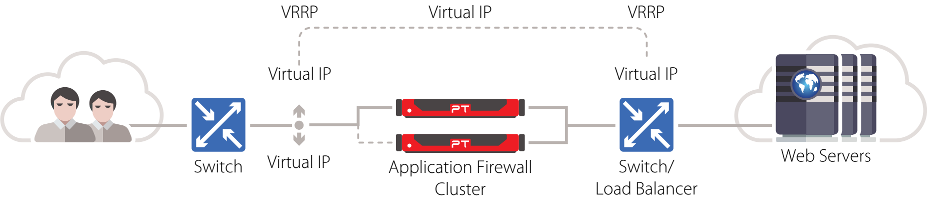
2

Active—Active High Availability:
Active—Active cluster can be integrated with external load balancers.



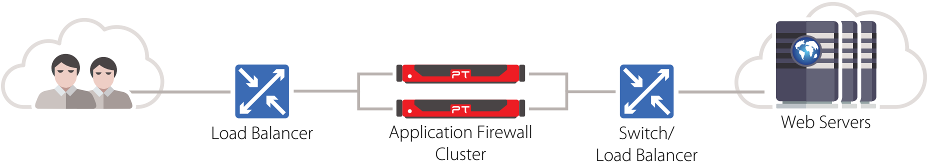
3

Active—Passive High Availability:
Active—Passive cluster supports two-node operations with built-in load balancing.



4

Active—Passive High Availability:
Active—Passive cluster can be integrated with external load balancers.



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