EVOLUTION OF WEB APPLICATION FIREWALLS: FROM SERVER PROTECTION TO DEFENSE-IN-DEPTH

Internet-based network attacks have become increasingly sophisticated over the last 20 years. Once-useful Intrusion Detection System/Intrusion Protection System (IDS/IPS) solutions show their age as the diversity and interactivity of today's web applications open up vectors for invisible, destructive cyberattacks. Most corporate network breaches are the result of vulnerabilities in web applications, even at companies that use the traditional security tools. Security-conscious companies are meeting this challenge by supplanting IDS/IPS and classic firewalls with the new technologies found in Web Application Firewall solutions.

WAF 1.0

The first generation of web application protection featured two main advances over IDS/IPS: utilization of HTTP attributes (method, address, parameters) and conversion of data prior to analysis (urlencode, base64). These solutions used a signature-based approach and were oriented at protection from server attacks (RCE, Path Traversal, SQL Injection).

WAF 2.0

The Web 2.0 technology stack, including AJAX, and explosive growth in the number of critical web applications drove development of WAF 2.0. The incredible number and complexity of web applications made classic signature-based approaches obsolete – the number of false-positive detections became too great to handle.

In response, dynamic profiling methods were introduced. Supervised machine learning optimized signature lists, although the process was time-intensive due to requiring extensive human intervention.

Methods for protecting users from attacks (XSS and CSRF) appeared in the second generation of WAF solutions as well.

WAF 3.0

To evade signature analysis, hackers shifted their attention to zero-day vulnerabilities. Defenders were forced to build a model of normal application functioning in order to detect anomalies while keeping false positives to a low level. Fully automated methods came up short due to the absence of "clean" traffic as source material for machine learning. Since real-world traffic contains legitimate queries mixed in with malicious ones, most WAF software is incapable of using this traffic to learn how to sort good traffic from bad traffic.

By building user behavior models with the help of Hidden Markov Models, PT Application Firewall can use this mixed traffic for learning, protect from zero-days, and prevent bypass attempts.

EMERGENT RISKS

Modern applications are massively complex undertakings, integrating a large number of client–server interactions in a single window. Securing the application "storefront" is not enough: it is essential that the connections between all the application systems and components be safeguarded as well. Applications for retailers, industrial control systems, online banking, and e-government typically rely on XML or JSON for such communication. Therefore, the WAF must identify unauthorized and malicious data in XML messages, and validate and profile SOA calls.

PROACTIVE PROTECTION

Instead of waiting for attacks, defenders can proactively increase the security of a web application by using a protection system to pinpoint and address vulnerabilities. But traditional firewalls – which simply compare traffic against a defined list of signatures – are incapable of this. Experience with penetration testing and other techniques enabled the experts at Positive Technologies to implement two important anti-vulnerability tools in PT Application Firewall: dynamic scanning for verifying attack success in real time, and automated virtual patching, based on test exploits generated by PT Application Inspector.

Third-generation WAF solutions emphasize protection from attacks on business logic (fraud and application-level DDoS) and implement user tracking, which tracks and reconstructs the chain of events in a particular user session.

INCIDENT DAMAGES TOP USD 162 MILLION

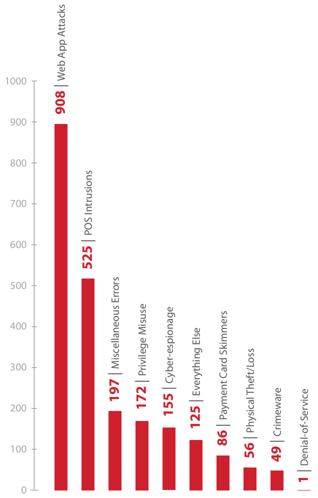
A massive 2013 hack infected payment systems at Target stores running on out-of-date versions of Windows. The attackers used a vulnerable web service, which allowed uploading arbitrary executables, to obtain access to POS terminals. Over 19 days, hackers made away with 40 million credit and debit card numbers in addition to personal information for 70 million customers. The company's direct expenses exceeded $162 million.

MORE THAN GBP 100 MILLION LOST DUE TO A SINGLE VULNERABILITY

In October 2015, U.K.-based TalkTalk fell victim to a hacking attack that stole bank card and personal information for over 150,000 clients. Launched through a vulnerable web application, the attack cost £42 million for the company and caused £60 million in shareholder losses. Approximately 100,000 clients took their business elsewhere.

THREAT #1: WEB APP VULNERABILITIES

According to Verizon DBIR, web application vulnerabilities were the single largest vector for breaches in 2015.



POSITIVE TECHNOLOGIES

Solna, Sweden
London, UK
Moscow, Russia
Rome, Italy
Boston, USA
Dubai, UAE
Seoul, Korea
Tunis, Tunisia
Mumbai, India

Established in: 2002

Offices in: 9 countries

Employees: over 600

Analysts: over 200 experts in protection of ERP, SCADA, banks, telecom companies, and web and mobile apps

Business partners: over 100 IT and infosecurity integrators

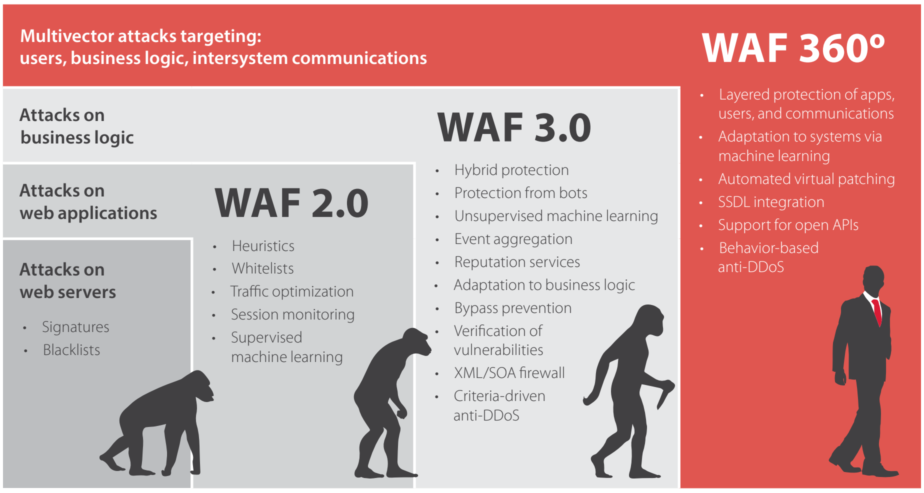
Technology partners: over 50 world-leading software and hardware manufacturers, including Check Point, Cisco, HP, Microsoft, Oracle, and SAP

WAF 360º

Most WAF solutions concentrate on protecting web applications from outside attacks. But on today's distributed infrastructures, a more holistic approach is required.

Comprehensive tools protect users and intersystem communications, and also use smart data analysis technologies to minimize the amount of manual work by IT security staff. WAF products can extend the secure software development lifecycle and close vulnerabilities that may be the result of the operating environment – after a web server is updated, for example. Support of orchestration for large numbers of WAFs (such as via Cisco ACI) and open APIs reduces the expenses required for data centers and cloud services. By integrating with anti-fraud systems to prevent data leaks and user fraud, WAF 360º helps companies and governments to manage client-related risks, without needing to make changes to the code of their web applications.

Drawing upon these advanced technologies, PT Application Firewall addresses all the weak links in the corporate security stance to make application protection truly comprehensive and complete.



Multivector attacks targeting:
users, business logic, intersystem communications

WAF 360º

- Layered protection of apps, users, and communications
- Adaptation to systems via machine learning
- Automated virtual patching
- SSDL integration
- Support for open APIs
- Behavior-based anti-DDoS

Attacks on business logic

WAF 3.0

- Hybrid protection
- Protection from bots
- Unsupervised machine learning
- Event aggregation
- Reputation services
- Adaptation to business logic
- Bypass prevention
- Verification of vulnerabilities
- XML/SOA firewall
- Criteria-driven anti-DDoS

Attacks on web applications

WAF 2.0

- Heuristics
- Whitelists
- Traffic optimization
- Session monitoring
- Supervised machine learning

Attacks on web servers

- Signatures
- Blacklists

INDUSTRY RECOGNITION

In 2015 and 2016, Gartner placed Positive Technologies as a Visionary in the Gartner Magic Quadrant for Web Application Firewalls because of its completeness of vision and ability to execute*. PT Application Firewall secures the web services of major banks, telecom operators, retailers, oil and gas companies, medical institutions, and media organizations. Learn more at af.ptsecurity.com.

* Gartner, Magic Quadrant for Web Application Firewalls, Jeremy D'Hoinne, Adam Hils, Claudio Neiva, 19 July 2016.

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.

info@ptsecurity.com ptsecurity.com