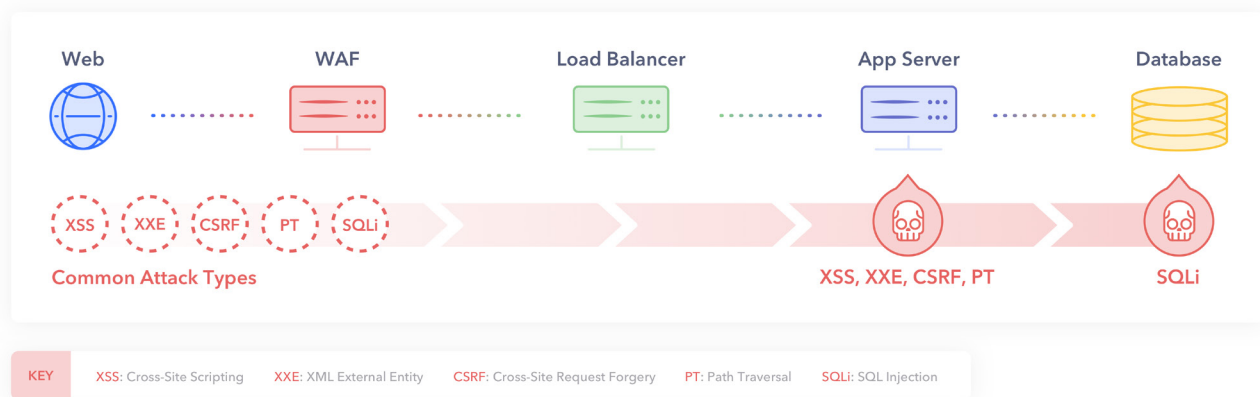# PREVOTY
WHITEPAPER

THE EVOLUTION OF APPSEC: FROM WAFS TO AUTONOMOUS APPLICATION PROTECTION

October 2017

Web application firewalls (WAFs) entered the security market at the turn of the century as web apps became increasingly complex and critical to digital life. Technologists modeled the WAF after network firewalls to act as a security policy enforcement point positioned between the app and the client endpoint. A WAF is configured with rules and policies that are meant to protect apps from exploitation leveraging signatures and patterns that are known threats.

The troves of personally identifiable, financial and critical data that live in web applications have attracted throngs of nefarious actors. As app-targeted attacks have become more common and sophisticated, WAFs have failed in much the same way that other firewalls, rule-based security measures, and legacy security solutions have: defenses that rely on past signatures and patterns always lose. Like so many outdated security technologies, WAFs lack the real-time context and situational awareness required to fend off zero-day attacks and suffer from high false positive and negative rates. With the acceleration of DevOps application development, WAFs consistently fall behind because they must learn new application behaviors each time the app is updated.

WAF Architecture

| Web | WAF | Load Balancer | App Server | Database |

Common Attack Types — XSS, XXE, CSRF, PT, SQLi

XSS, XXE, CSRF, PT

SQLi

KEY   **XSS:** Cross-Site Scripting   **XXE:** XML External Entity   **CSRF:** Cross-Site Request Forgery   **PT:** Path Traversal   **SQLi:** SQL Injection
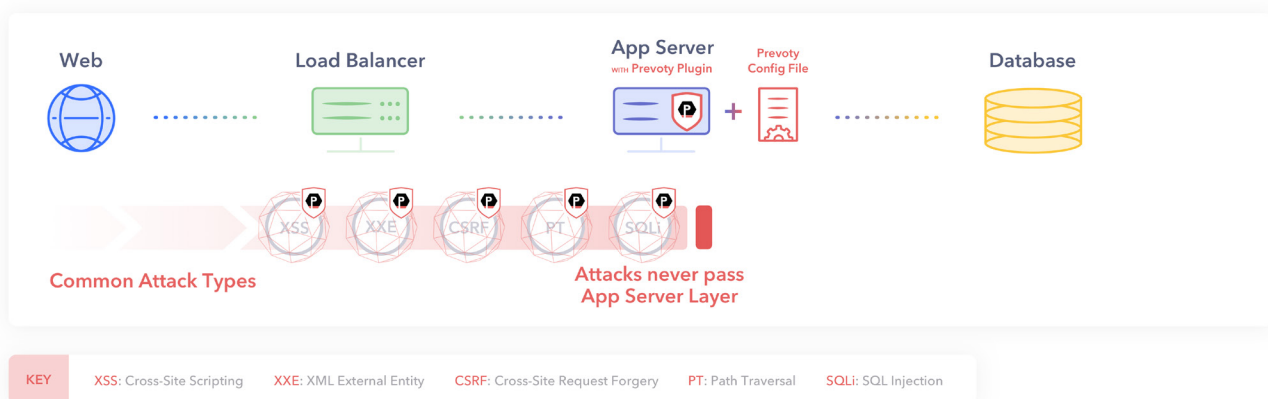
Securing applications requires radical thinking… Applications must defend themselves.

Prevoty has developed an autonomous application protection solution that enables applications to defend themselves from known and zero-day attacks in real-time, in production.

Prevoty Autonomous Application Protection employs a lightning-fast, attack detection technique called Language Theoretic Security (LangSec). LangSec is the formal process of understanding how data such as content payloads, database queries, operating system commands and more will execute in an environment. Prevoty employs LangSec to condition applications to the safe handling of data. Prevoty deploys via autonomous plugins that can be attached to applications at any point in the software development life cycle, and travel with the apps wherever they are deployed. Prevoty inspects all incoming payloads, understands contextually how payloads will execute, and neutralize threats in real-time.

Prevoty Autonomous Plugin Architecture

Web   Load Balancer   App Server
                                     with Prevoty Plugin   Prevoty
                                                                  Config File   Database

Common Attack Types   Attacks never pass
                             App Server Layer

KEY   XSS: Cross-Site Scripting   XXE: XML External Entity   CSRF: Cross-Site Request Forgery   PT: Path Traversal   SQLi: SQL Injection

WAF v. Prevoty Autonomous Application Protection

Threat Detection

Prevoty inspects data in the context of how the application will use it. This enables more accurate threat detection, protection against a broader range of threats, and a significant reduction in false positives.

✓ Prevoty is tightly coupled with application code that is susceptible to malicious exploit. Unlike a WAF, Prevoty uses contextual awareness – not rules and signatures – to detect threats.

✗ WAFs depend on rules and signatures – blindly guessing if a payload is nefarious before the data is sent to the application.

Scaling with DevOps

Modern enterprise application development is shifting to a continuous integration and deployment model. DevOps cycles are rapid, aggressive, and applications are often deployed without sufficient security. It is the latent vulnerabilities within organization's own application software that are the most commonly exploited attack vector.

✓ Prevoty was built to scale with DevOps. Prevoty protected applications are secure from malicious payloads, regardless of any latent vulnerabilities within the software. That means developers can push new or updated applications into production with the confidence that they are **secure by default**.

✗ WAFs can't keep up with DevOps using a signature and usage-pattern or RegEx approach; their learning curve is too steep for rapid development cycles with frequent updates. WAFs were not built to defend apps from unknown vulnerabilities in their own code, or zero-day attacks.

Ease of Deployment

Security tools should solve problems, not create new ones. Large-scale, disruptive deployments are a headache security teams don't need.

Prevoty deploys via autonomous plugins that can be dropped into applications no matter where they are in the software development life cycle, live inside the applications themselves, and protect them no matter where they are deployed – whether on-prem, in the cloud, in containers, virtual environments, or micro-services. Deployment is quick and quiet, allowing business to go on as usual without disrupting user experience.

WAFs are positioned between the app and the endpoint. WAF deployments are big and heavy, requiring a team of dedicated personnel. They are obstructive to DevOps cycles, application performance and, often, user experience.

Cost Efficiency

When estimating the ROI of a security tool, buyers must consider the upfront investment, time, and resources that the deployment and maintenance will require, and the value of its potential to reduce risk.

Prevoty saves organizations time and money. Its total cost of ownership is slashed by a quick and easy deployment and simple upgrades. According to David Nolan, Director of Information Security at Aaron's Inc., "A WAF requires two full-time staff members dedicated to deployment and support. Prevoty requires two hours a week from one staff member, and it delivers better protection."

WAFs are expensive upfront. Not only that, they require extensive ongoing resources to deploy, maintain and tune.

Real-Time, Analytical Insights

Many organizations integrate their appsec solutions with a log management tool, SIEM, or other analytical platform where data can be collected, analyzed, visualized and interpreted into valuable security and risk insights.

✓ Prevoty delivers a completely new perspective on application security. Because it lives inside the application itself, Prevoty's visibility into network, application, operating system and database activity is thorough and extensive. The data Prevoty generates can be fed into SIEMs, log management, or analytical solutions, enabling security teams to make faster, smarter, data-driven security decisions.

✗ WAFs have unilateral visibility into application activity. The data they generate is limited to network-level activity. Most have the capability to integrate with analytical platforms, but as the saying goes: bad data in, bad data out.

These are just some of the critical differences between a WAF and Prevoty Autonomous Application Protection. If you're wondering whether to invest in a WAF or frustrated with the one your organization already has in place, reach out to our team of application security experts at prevoty.com. They'll be happy to provide a complimentary demo that illustrates how Prevoty outperforms WAF in every category.

About Prevoty

Prevoty protected applications are secure by default. Prevoty delivers powerful Autonomous Application Protection via its runtime application self-protection (RASP) technology. It enables fast, efficient and secure software development life cycles, monitors and protects applications at runtime, and neutralizes known and zero-day attacks.

For more information, visit prevoty.com