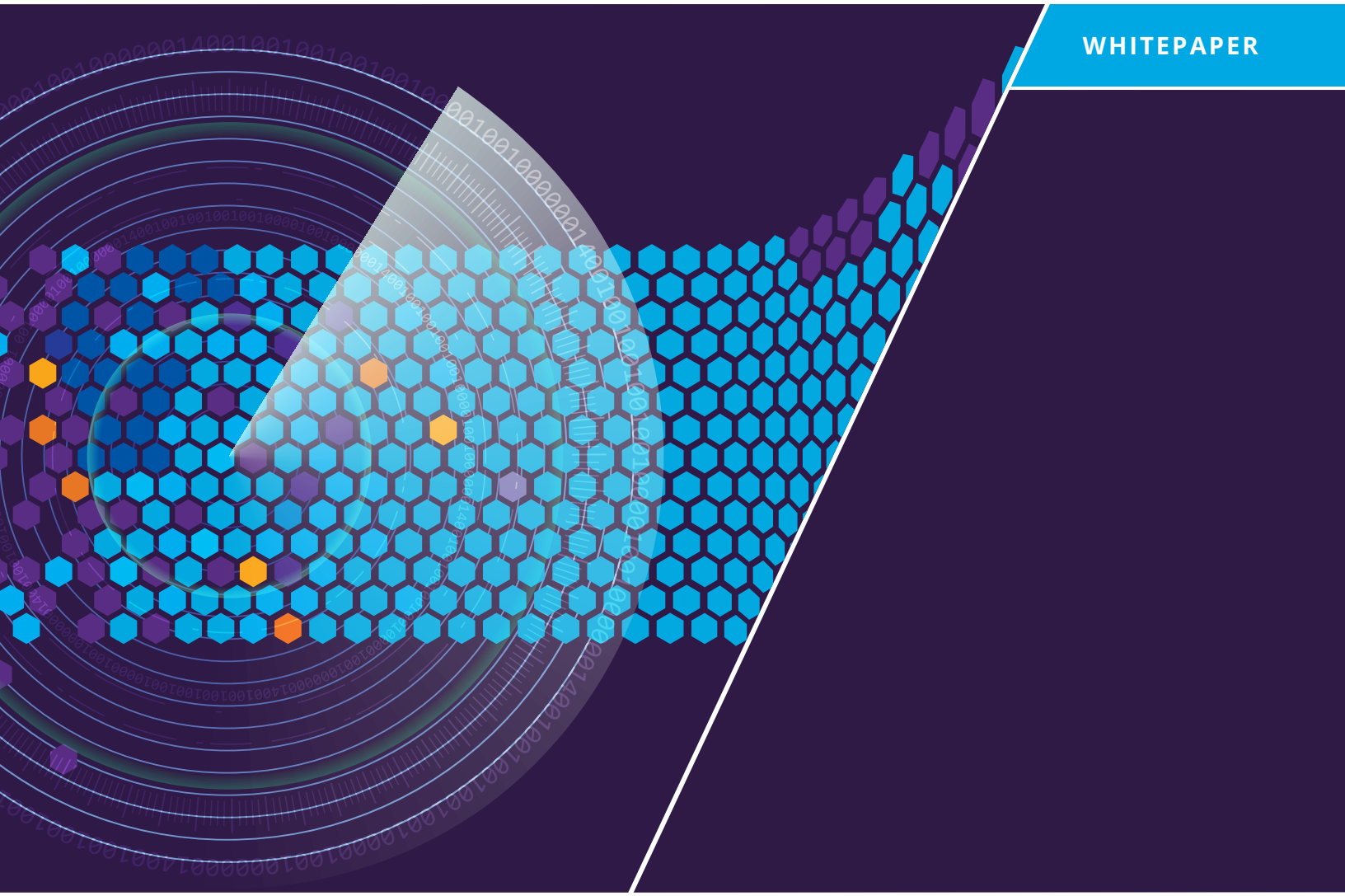
IMPERVA®

Five Key Capabilities Required for an Effective Web Application Firewall



WHITEPAPER

Executive Summary

Web application firewalls have become an essential component of the modern organization's security infrastructure, providing scalable high-fidelity protection of business-critical web applications from a broad spectrum of cyber threats. As with any must-have enterprise security solution, there is considerable variation in available offerings. To help IT security and application defense teams navigate the evaluation process, this paper examines five ways that Imperva SecureSphere Web Application Firewall surpasses the competition.

With Imperva – positioned by Gartner for three years in a row as the only Leader in the Magic Quadrant for Web Application Firewalls[1] – enterprises obtain a web application security solution that sets itself apart by delivering:

- Highest accuracy of detection with dynamic profiling and correlation;
- Comprehensive protection in one integrated application and data security platform;
- Broadest deployment options to meet a variety of business requirements;
- Extensive out-of-the-box integrations for simplified security operations; and
- Enterprise scale management for globally distributed deployment.

The State of Web Application Security

The fact that web applications are a prime target for data thieves, hacktivists, and cybercriminals is practically a foregone conclusion. After all, web applications are:

- Pervasive – as they are used in support of countless customer, partner, and employee-facing business processes;
- Valuable – as they expose material business functionality and often serve as a conduit to numerous types of sensitive data, including personally identifiable and proprietary information; and,
- Vulnerable – as they often incorporate multiple third-party components and cutting edge technologies, and typically sacrifice security in favor of functionality, ease of use, and time-to-market.

Making matters worse for the IT teams charged with defending these critically important assets are changes occurring on the threat side of the ledger. In particular, no longer is it sufficient to be able to thwart technical attacks such as SQL injection, cross-site scripting, and remote file inclusion that exploit application vulnerabilities. Web application defenses today must also be capable of handling business logic attacks that work by exploiting flawed logic encoded into applications or abusing standard functionality, for example to create unauthorized accounts, "game" the checkout process for a retail application, or deposit a ton of comment spam. On the rise too are highly automated account takeover attacks and similar threats responsible for fraudulent transactions – not to mention botnet-driven, application-layer DDoS attacks capable of evading volumetric defenses.

[1] Gartner, Inc., Magic Quadrant for Web Application Firewalls, Jeremy D'Hoinne, Adam Hils, Claudio Neiva, 19 July 2016
Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

To adequately address this ever-growing set of fully automated attacks, organizations are finding it necessary to place increasingly greater emphasis on proactive security measures. In other words, security technologies and solutions that proactively work to stop web application threats outright and prevent organizations from ever being compromised in the first place are now at a premium relative to those that reactively detect the occurrence of a breach after the fact. Due to the potentially substantial impact of successful attacks – ranging from application downtime, theft of data, and brand damage to financial costs in the millions of dollars per incident – we also see the elevation of web application security from a check-box item for compliance purposes to a board-level concern for many organizations.

Why Web Application Firewalls Are a Must-Have Countermeasure

The unique capabilities and comprehensive coverage that web application firewalls provide make them an indispensable component of an organization's security infrastructure. Before getting into these significant differentiators, let us "set the record straight" on what some see as the alternatives to a web application firewall.

Traditional Network Defenses: Application Awareness is Not the Same as Application Fluency

What sets next generation firewalls apart from earlier network defenses is the ability to identify the type or even particular application associated with a given stream of network traffic. The result is a powerful way to tighten access control rules previously dependent solely on IP addresses, ports, and protocols for enforcing security policies. However, this basic level of application awareness is nowhere near the same as having the application fluency required to thoroughly protect web applications. Besides not having the means to establish how each web application is intended to be used, solutions limited to application awareness also lack the ability to validate application inputs, correlate multiple attributes, provide cookie and session protection, and prevent automated attacks that abuse business functionality.

Emerging Technologies: Immature, Intrusive, and Difficult to Scale

Another technology receiving attention of late is runtime application self-protection, or RASP. RASP works by dynamically inserting security checks into an application or its runtime environment to control execution and detect and prevent real-time attacks. However, it too has a number of limitations. In particular, RASP is:

- Intrusive – it changes application behavior in unpredictable ways, adds performance overhead, and complicates change management processes.
- Incomplete – protection is typically provided solely for technical web attacks (leaving business logic, account takeover, and other fraud-oriented attacks to continue to wreak havoc).
- Immature – coverage is currently limited to applications using a handful of common runtime environments, such as JVM, PHP, and .NET (leaving applications built on Python, Ruby, ASP and other popular frameworks exposed).
- Inefficient – it places extra load on application servers and is unable to prevent unwanted traffic (e.g., from sources with bad reputations or botnets) from getting through in the first place.

The net result is a solution that is best suited as an interactive application security testing (IAST) tool for diagnostics in pre-production or staging environments, to detect and report on application vulnerabilities.

Web Application Firewalls: A Unique Blend of Capabilities and Coverage

Compared to the available alternatives, leading web application firewalls deliver a more comprehensive and completely non-intrusive solution for web application security that is at once efficient, effective, and easy to scale. Such solutions leverage an in-depth understanding of the applications being protected as a foundation for identifying abnormalities associated with otherwise elusive threats and attacks. Depending on the solution, additional strengths can include the ability to:

- Dynamic application profiling to account for changes and upgrades made to protected applications
- Stop unwanted traffic before it can make its way “inside” and consume valuable computing resources
- Stay ahead of attackers by incorporating superior threat intelligence into detection, enforcement, and response policies
- Detect bots and prevent the rising tide of fully automated threats
- Reliably thwart evasion techniques and minimize false positives
- Mitigate account takeover attacks and other fraud-focused threats
- Proactively detect security breaches by tracking users accessing sensitive data through internet facing web applications
- Provide out-of-the-box coverage for any web application that logically resides behind it
- Automate and scale web application security and compliance operations

The net result is a strategic solution for protecting all of an organization’s essential web properties, now and in the future.

5 Critical Differences that Set Imperva SecureSphere Web Application Firewall Apart

Acknowledging the need for and value of a web application firewall is only a starting point. Organizations must still select the best solution for meeting their needs from a variety of available options. To help with this challenge, the following sections disclose five significant ways SecureSphere Web Application Firewall surpasses its competition.

Imperva Difference #1 – Highest accuracy of detection with dynamic profiling and correlation

Modern organizations require protection for tens to hundreds of web applications, most of which are custom built. Similarly, they must contend with thousands to millions of cyber threats, a growing percentage of which are exploiting a combination vulnerabilities and business logic attacks in applications. Given the scope of the problem space, automation is a much-needed ingredient for any solution.

SecureSphere Web Application Firewall addresses the need for automation in numerous ways, including the following:

Dynamic application profiling. Patented Dynamic Profiling technology automates the process of learning the structure, elements, business logic, acceptable inputs, and expected user behavior for protected applications – as well as changes that are made to applications over time. It eliminates the biggest drawback of other web application firewall solutions that require manual rule creation and maintenance of constantly changing variables including URLs, parameters, cookies, XML elements, and form fields, which can be major drain on operational overhead.

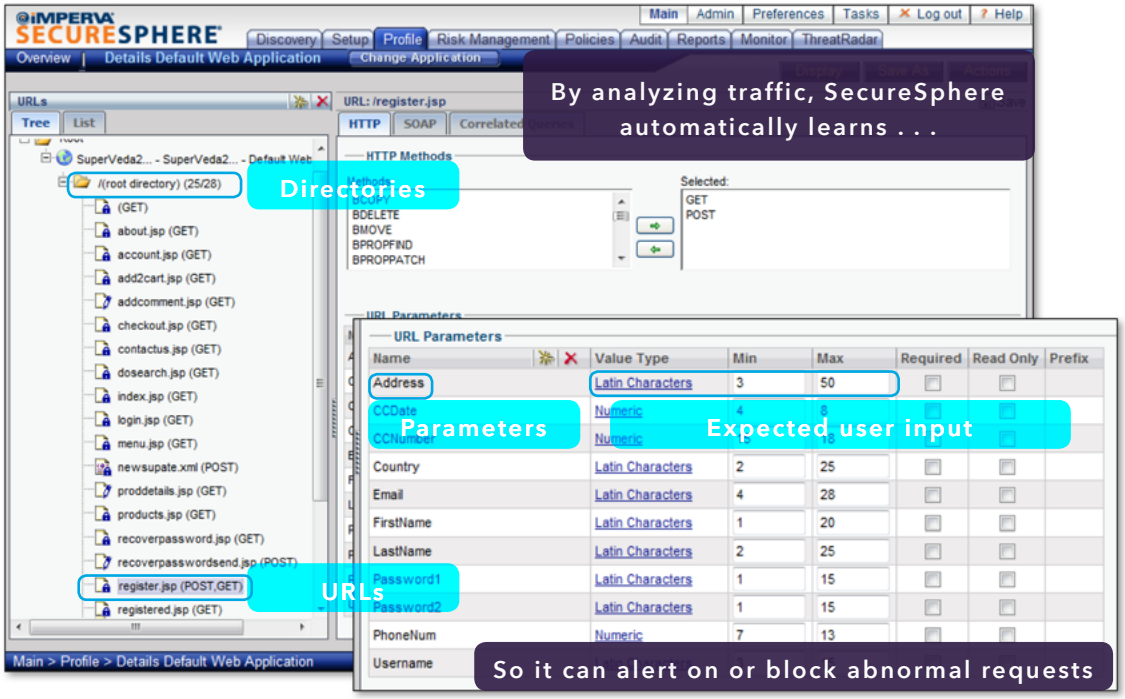


Figure 1: Dynamic Profiling Screens in SecureSphere Web Application Firewall

Granular correlation policies. SecureSphere further boosts both the efficacy and accuracy of detection by enabling detailed correlation between all available sources of information to establish a clearer picture of what is going on in any given situation. A straightforward example is one where an SQL injection attack is originating from a malicious bot sitting behind a TOR (The Onion Router network), which can evade IP-address based detection techniques that other web application firewalls typically use.

In addition to activating numerous pre-defined correlation policies, SecureSphere administrators can craft custom policies to account for other pieces of contextual threat intelligence to minimize the occurrence of resource-sapping false positives.

Automated content updates. Regular content feeds from the Imperva Defense Center, an internationally recognized security research team, ensure that SecureSphere is always armed with the latest defenses against advanced application attacks, along with best-practice protection policies and up-to-date reports for maintaining regulatory compliance.

Compared to the competition, not only is dynamic application profiling relatively unique, but so too is the customizable correlation policies that is included in content updates from the Imperva research team . This valuable combination enables customers to proactively detect evolving cyber attacks with the highest accuracy and least number of false positives or false negatives.

Imperva Difference #2 – Comprehensive protection in one integrated application and data security platform

Hand-in-hand with the requirement for automation is the need for protection that not only spans the broad spectrum of application attack vectors organizations are likely to encounter, but also secures the related data stores accessed by the web application with one integrated SecureSphere security platform. For example, ability to "track" and provide audit details for users end-to-end from both the application and data perspective. Strengths of SecureSphere in this area include:

Comprehensive threat coverage. With SecureSphere, organizations obtain coverage for a broad range of threats and attack types. Where many other solutions do little more than counteract common technical attacks, SecureSphere protection extends to account not only for the full OWASP Top 10[2], but also the twenty classes of automated threats identified by OWASP[3] and a wide range of business logic attacks. Specialized protection is also available to prevent account takeover attempts in real-time, before fraud events can be perpetrated.

Deep threat intelligence. Unlike most competing solutions, SecureSphere directly incorporates comprehensive threat intelligence to further enhance its protection capabilities and better account for constantly evolving threats.

[2] OWASP Top Ten Project

[3] OWASP Automated Threat Handbook, July 2015

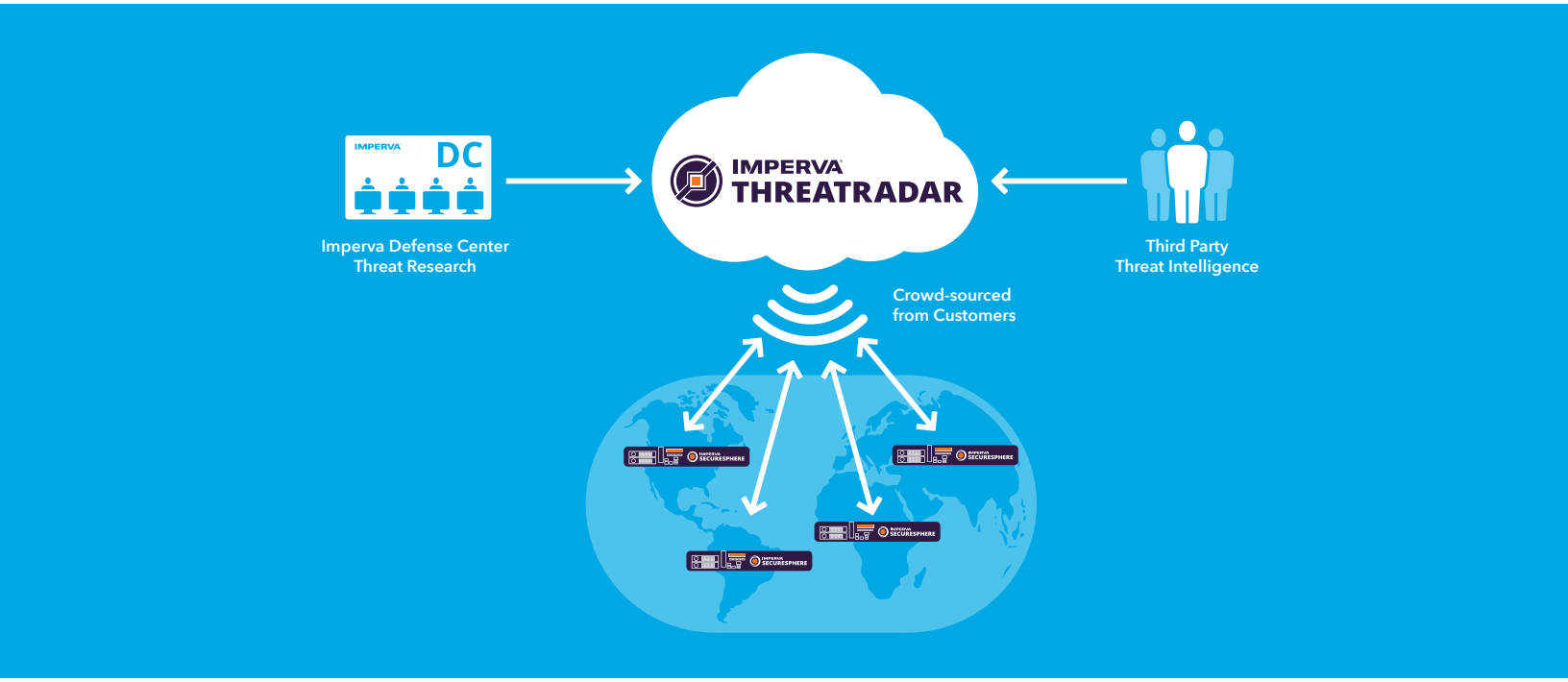


Figure 2: ThreatRadar crowd-sourced threat intelligence for SecureSphere Web App. Firewall

Imperva ThreatRadar – a powerful combination of crowd-sourced intelligence from the SecureSphere worldwide customer community and threat data feeds from best-of-breed, third- party providers that is curated by the Imperva research tean – arms SecureSphere Web Application Firewall with the following proactive intelligence-driven protection services:

- ThreatRadar Reputation Services – identifies known malicious and otherwise troublesome source IPs, such as those associated with anonymous proxies, TOR networks, phishing attacks, and comment spammers
- ThreatRadar Community Defense – includes anonymized attack data that SecureSphere customers have opted-in to share with Imperva. So, when one customer sees an attack from a new source, all other Imperva customers get protected from attacks originating from those sources.
- ThreatRadar Bot Protection – accurately distinguishes between human and bot sources of incoming traffic, good and bad types of bots, and "imitation" browsers used by bots to fool detection mechanisms into concluding they are human users
- ThreatRadar Account Takeover Protection – leverages a combination of credential intelligence and over 2.5 billion device intelligence entries to detect unauthorized attempts at gaining access to both ordinary and privileged web application accounts

Web to database user tracking[4]: enables organizations to simultaneously monitor web and database activity to identify which web users performed which SQL transactions, by linking web user session identity with backend SQL queries. It requires no changes to the existing infrastructure: no application recoding, no agent installation. Web to database user tracking offers a unique way to audit database transactions originating from internet facing web applications, which no other no other vendor provides.

Imperva Difference #3 – Broadest Deployment Options to Meet a Variety of Business Requirements

Application architectures, delivery options, and protection preferences are as diverse and rapidly evolving as application threats. Accordingly, web application firewalls need to have flexible deployment and configuration options to satisfy every organizations' unique requirements, now and in the future.

With SecureSphere Web Application Firewall, enterprises get the flexibility and adaptability they need a number of key features, including:

A broad set of deployment options. SecureSphere can be deployed on-premises as a physical or virtual appliance. In addition, a variety of deployment modes - transparent in-line bridge, transparent proxy, reverse proxy, and out-of-band span/tap mode are supported. Some of the deployment modes require no changes to network configuration or application changes. In all cases, customizable detection, enforcement, and response policies further ensure the ability to match an organization's unique preferences and requirements.

Secure Multiple Cloud Infrastructures. SecureSphere virtual machine images are available for Infrastructure-as-a-Service providers such as Amazon AWS and Microsoft Azure. It enables customers to automatically expand their applications and data footprint into cloud infrastructure, and auto-scale based on customer demand. SecureSphere leverages the load-balancing and high-availability capabilities natively provided by AWS and Azure, to provide robust deployment options to customers.

An extended solution portfolio. As their needs dictate, customers can build on the foundation of web application security achieved with the SecureSphere Web Application Firewall in a sensible and coordinated manner. Progressively adding SecureSphere data security solutions (for database and big data protection), Incapsula cloud-based DDoS protection services, and Imperva Skyfence Cloud Gateway provides unparalleled protection of data and applications wherever they reside – on-premises or in the cloud.

Our laser focus on protecting business critical data and applications, is what sets Imperva apart. Unlike competing solutions, ours are not a secondary, add-on component to another offering, such as a content delivery network (CDN). Or tied to a unified threat management (UTM) or application delivery controller (ADC) platform, where they compete with five or ten other components for research, development, and maintenance resources. The result with SecureSphere Web Application Firewall – and the rest of the Imperva portfolio – is a best-of-breed solution with the flexibility and adaptability organizations require to achieve and maintain a maximally effective implementation.

[4] Technical Brief: Universal User Tracking

Imperva Difference #4 – Out-of-the-Box Integration for Simplified Operations

There are no silver bullets when it comes to information security. Defense-in-depth is not an option, but a necessity. Accordingly, a web application firewall needs to provide seamless integration with other essential components of an organization's security infrastructure.

Out-of-the-box integrations available with SecureSphere that enhance web application defenses and accelerate related operations include those with:

Security Information, Event, and log Management (SIEM/Log) tools – including CA Enterprise Log Manager, HP ArcSight, IBM QRadar, McAfee Enterprise Security Manager, RSA enVision, Splunk Enterprise, and more – for enhancing visibility, incident response, and detailed forensic investigations

Vulnerability scanners – SecureSphere integrates with the leading vulnerability scanners to automate the process of generating vulnerability-based signatures, thereby reducing the need for costly out-of-cycle application fixes. It integrates with HP WebInspect, IBM, AppScan, Qualys, and WhiteHat Sentinel – for enabling instant virtual patching of custom web applications.

Automation APIs – SecureSphere provides RESTful application program interfaces (APIs) to automate IT/Security operations for deployment, configuration, and on-going maintenance of security policies on multiple web app firewall instances. It provides additional API's and template scripts to simplify provisioning of proof-of-concept environments and large scale deployments in cloud infrastructure environments (AWS/Azure).

Imperva Difference #5 – Enterprise Scale Management for a globally distributed deployment

Any multi-national company typically operates hundreds of web applications to conduct business worldwide, and these applications may be located in different geographically distributed data centers. Such companies must be able to centrally manage application security policies, monitor events, and investigate security incidents at a global level. SecureSphere provides the following capabilities to simplify enterprise-scale management across web application firewalls are located in separate data centers or continents.

Provider scale management. A single SecureSphere Management Server can manage up to 25 SecureSphere gateways. To manage larger distributed deployments of SecureSphere, Imperva provides tiered management with SecureSphere Operations Manager (SOM). A SOM helps overcome the "disconnected islands" problem that plagues some solutions. Maintaining consistent web application security policies and creating unified, enterprise-wide compliance reports remains straightforward even for large implementations.

Real-time visibility. An intentional by-product of SecureSphere's scalable, multi-tier architecture is that administrators obtain real-time access to monitoring and event data, along with associated reports. In comparison, solutions with legacy architectures are often limited to batching and periodically aggregating information gleaned across multi-site deployments, resulting in significant delays before administrators can view, analyze, and respond to detected issues and threats.

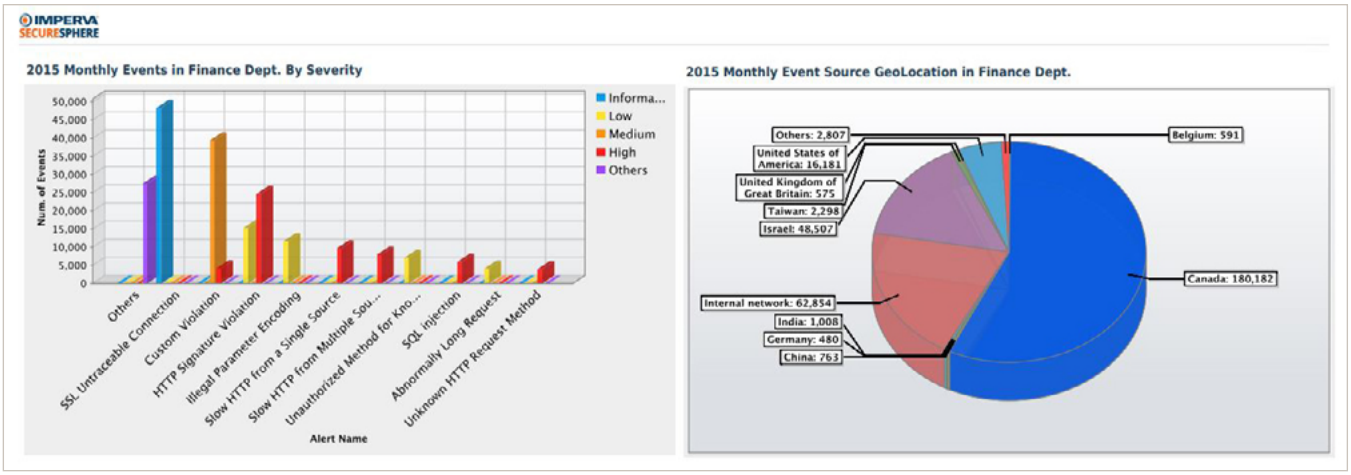


Figure 3: Customizable Reporting in SecureSphere Web Application Firewall

Robust reporting. An extensive set of pre-defined reports enable customers to easily understand web application security and compliance status, while full customization capabilities allow complete alignment with organization-specific policies, processes, and practices.

Most competitors do not provide centralized management of security policies, application profiles, or logging, and fundamentally can't scale to manage hundreds or thousands of applications. A key proof point is the Imperva significant footprint for web application firewall in the hosting environments, which also use network infrastructure solutions from competitors. From a business perspective, most hosters would have preferred a single vendor, but found the competitive solution to be unable to meet their management scale requirements.

Conclusion

Web applications drive businesses more today than at any other time in history. To adequately protect these business-critical resources, organizations need a web application firewall. However, not just any solution will do. Effectively defending against increasingly automated and sophisticated web attacks depends on selecting a web application firewall that, as described in this paper, delivers unparalleled levels of situational awareness, threat protection, flexibility, automation, and scalability.

IMPERVA SECURESPHERE

To learn more about SecureSphere Web Application Firewall and other Imperva solutions for protecting your organization's data, applications, and reputation, please visit http://www.imperva.com/Products/WebApplicationFirewall and http://www.imperva.com/Products/ThreatRadarSubscriptions.