

WEB APPLICATION SECURITY FROM IMPERVA

BENEFITS:

- Automatically learns Web Application structure and user behavior
- Helps address PCI Data Security Standards compliance requirements
- Successfully identifies traffic originating from malicious sources

THE PROTECTION OF WEB APPLICATIONS

In the past few years, web applications have become the leading target from malicious attacks. This is due to the accessibility of high value data such as personable identifiable information (PII). Web-based applications must be protected while not affecting performance or uptime.

AUTOMATED LEARNING OF WEB APPLICATION STRUCTURE AND USER BEHAVIOR

Unlike traditional firewalls, Web Application Firewalls (WAF) must be able to interpret and understand application structure and expected user behavior. As more business applications are moved to the web, or into the cloud, WAF technologies are becoming a critical application in the network security infrastructure. Imperva's patent-pending Dynamic Profiling technology can help organizations profile protected applications, while building a list of acceptable use behaviors.

ADDRESS PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS COMPLIANCE

No single security application is capable of addressing all of the Payment Card Industry's (PCI) Data Security Standards (DSS). It is through utilizing a combination of best-in-class security applications, that PCI compliance can be achieved. Imperva's SecureSphere WAF satisfies the security requirements for auditing and user access controls (PCI DSS 6.6). By design provides continuous and automated protection that can meet the needs of enterprises with minimal configuration. From an auditing perspective, SecureSphere offers pre-defined, as well as, custom reporting capabilities that can help streamline compliance.

SUCCESSFULLY IDENTIFY MALICIOUS TRAFFIC

Attacks on corporate networks are becoming so complex that often times, multiple applications are required to work together to help identify malicious traffic and activity. The Imperva SecureSphere solution incorporates WAF, Database Firewall, and File security to help defend networks from unwanted activity. The WAF component is one of the most important security technologies in today's security network, as web-based applications are most vulnerable. Imperva helps identify and protect from unwanted traffic using multiple automated and customizable features:

- Research driven security policies powered by the Imperva Application Defense Center;
- Adaptable protection that mitigates large-scale automated attacks by integrating credible information on known attack sources;
- Import assessment results from multiple best-in-class vulnerability assessment organizations through the use of virtual patching;
- Fortifies all application layers against online threats by continuously updating web application signatures;
- Reduces false positives by correlating web requests across security layers over time.

With Imperva's market-leading protection of web applications, and Crossbeam's high performing and flexible architecture, enterprise organizations are able to safeguard web applications in high performing networks without adding latency or administrative overhead.

ABOUT CROSSBEAM

We improve the sophisticated networks of enterprises, government agencies, and service providers by architecting platforms that are more adaptable, high-performing, reliable, and secure.

