IMPERVA®

Federal Government Overview

Fallout from Data Breaches is Growing for U.S. Government Agencies

Fallout from Data Breaches is Growing for U.S. Government Agencies

Cyber security attacks targeting U.S. Federal Government data continue to grow in number and sophistication, creating substantial risks to critical government functions. Security incidents reported by government agencies grew by 10% from 2014 to 2015.[1] Well-funded adversaries remain a major concern, and – with their knowledge and access to sensitive data – insider threats change the playing field.

Significant Risk to Mission-specific Data

Despite continued, significant investments in endpoint, perimeter and network controls, breaches of U.S. Government data continue to occur. When adversaries gain access to the network or a privileged user's credentials, they can breach internal resources containing sensitive information. In addition, recent incidents of confidential information leakage (i.e. WikiLeaks, IRS and FBI) and fraudulent activity show that even trusted insiders can pose a serious risk to data. Federal agencies need to adopt a security model where they assume that the adversary is already inside the network, and complement traditional endpoint, perimeter and network security controls with solutions that directly monitor and control access to data and applications.

The need to control the threat from within is reflected in federal regulations such as FISMA/NIST 800-53, ICD 503, HIPAA, DITSCAP/DIACAP and NISPOM 2006. All require implementation of information security policies, procedures and technical controls to protect sensitive data, prevent unauthorized access and ultimately detect and contain data breaches. This creates technical challenges to security organizations in the Federal Government.

Stop Cyber Criminals from Exploiting Web Applications

Hacktivists and cyber-criminals know vulnerable web applications bypass federal perimeter defenses and provide a direct path to back-end data stores such as databases, file servers, or Sharepoint portals. Network firewalls that are used to lock down the organization's perimeter, continue to allow passage of HTTP and SSL traffic via ports 80 and 443, leaving an open door for hackers to exploit application-layer vulnerabilities. Intrusion Prevention Systems (IPS) which identify known attack patterns via signatures and apply packet restrictions are unable to address vulnerabilities unique to the behavior of a targeted application and its logic.

[1] Cyberwar.news, "Report: Number of Cyber 'Incidents' Up at Federal Agencies." March 28, 2016

Protect Information Systems from Unauthorized Access and Improper Usage

Imperva application and data security solutions map directly to NIST 800-53 controls that focus on protecting information systems from unauthorized access and improper usage. NIST SP 800-53 specifications supported by Imperva include:

- Access Controls
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Identification and Authentication
- Incident Response
- Risk Assessment
- Systems and Services Acquisition
- System and Communications Protection
- System and Information Integrity

Source: Gartner (July 2015)[5]

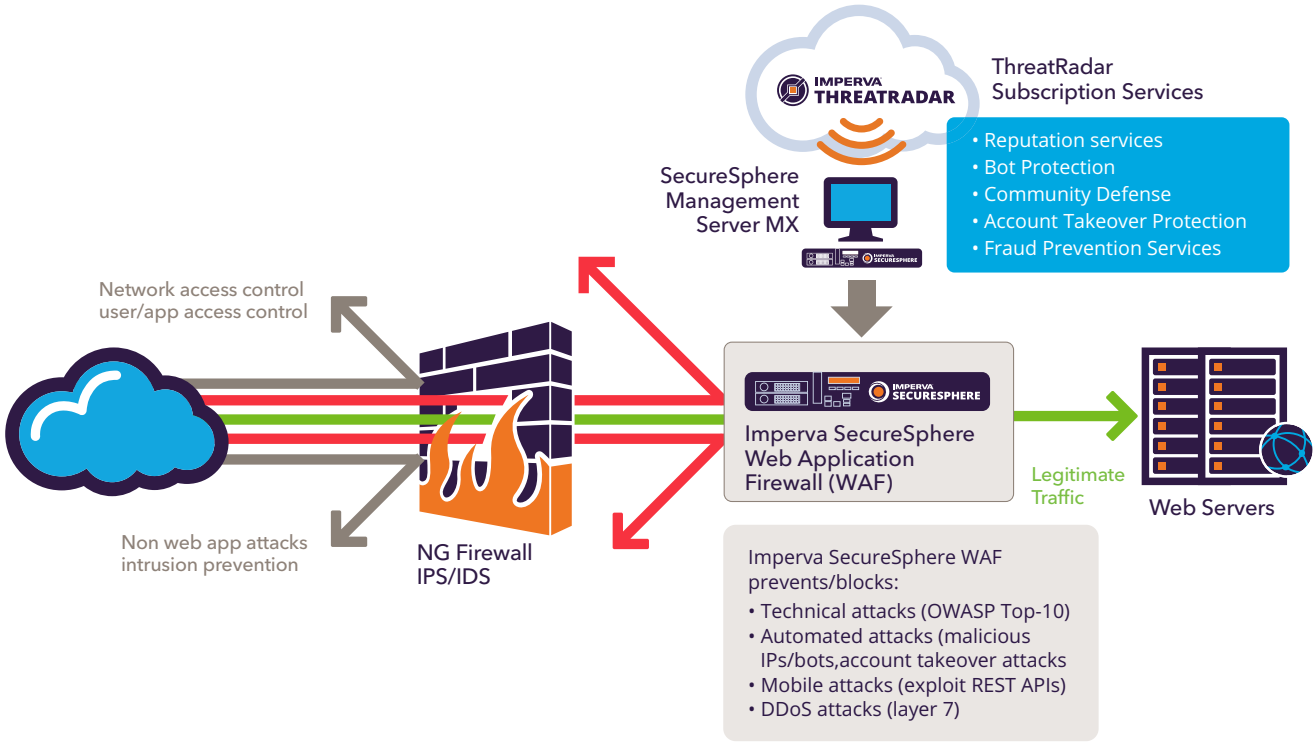
The Web Application Firewall Leader[2]

Imperva is the only vendor ranked in the Leaders Quadrant for two years running for the Gartner Magic Quadrant for Web Application Firewalls.

Imperva SecureSphere Web Application Firewall (WAF) analyzes all user access to your mission-critical web applications and protects your applications and data from cyber-attacks. It dynamically learns your applications' "normal" behavior and correlates this with global threat intelligence updated in real time. Imperva was recognized as the only leader in Gartner's Magic Quadrant for Web Application Firewalls[2] in both 2014 and 2015 based on completeness of vision and ability to execute. The SecureSphere WAF identifies and acts upon network anomalies that appear as innocent-looking website traffic to block attacks from:

- SQL injection, cross-site scripting and remote file inclusion that exploit vulnerabilities in web applications
- Business logic attacks such as site scraping and comment spam
- Botnets and DDoS / DNS attacks
- Account takeover attempts, before fraudulent transactions occur

Imperva Threat Radar is an advance-warning system that stops emerging threats by collecting, comparing and analyzing attack data from a variety of trusted sources, and providing SecureSphere web and database firewalls with real time data on bad IPs, signatures, worms and viruses. Global threat research from Imperva Defense Center security experts and community feeds from Imperva customers, comprise the global threat intelligence updates that feed Imperva solutions.



[2] Gartner Magic Quadrant for Web Application Firewalls, Jeremy D'Hoinne, Adam Hils, Greg Young, 15 July, 2015

The Roadmap to Better Security – CDM Initiative

Continuous Diagnostics and Mitigation (CDM) is a $6 billion funded program by, Department of Homeland Security (DHS) to secure the cyber infrastructure of the .gov network environment. Imperva supports this initiative by providing industry leading cyber security solutions to protect the data, applications and cyber infrastructure of government agencies.

To participate in the program, the General Services Administration (GSA) and DHS have used the GSA IT Schedule 70 as a contract vehicle. The Continuous Monitoring as a Service (CMaaS) contract provides CDM tools and integration services to all federal agencies under a blanket purchase agreement.

DHS will pay for the cost of CDM tools and integration if a civilian government agency participates via CMaaS task orders. In fiscal year 2014 alone, DHS allocated $185 million to spend on CDM tools and services.

Directly Protect Sensitive Data

The people on the payroll present the greatest threat to your data security. To do their jobs, employees, contractors, consultants and vendors must have legitimate access to sensitive and valuable data stored in databases, file shares and cloud applications. However, some insiders are careless with data and others don't realize their accounts have been compromised, leaving data exposed. To detect and contain data breaches, federal agencies need to have visibility into who is accessing the data, understand if that access is legitimate and be able to respond immediately if it's not. Imperva provides industry-leading cyber security solutions that pinpoint critical anomalies indicating misuse of sensitive data in databases, file servers and cloud apps.

The industry leading Imperva SecureSphere Database Activity Monitoring solution addresses all aspects of database security and compliance with best-in-the-industry database auditing and real-time protection that does not impact performance or availability.

Imperva CounterBreach protects federal data from theft and loss caused by insiders. Machine learning technology proactively alerts security teams to dangerous data access behavior and noninvasive deception technology identifies compromised end-point devices. CounterBreach monitors user behavior, reports anomalies and enables security personnel to set up decoy systems to catch hacktivists and malicious insiders.

See the following resources to learn more about preventing data breaches with Imperva cyber security and the CDM program:

Federal@Imperva.com

Meeting NIST SP-800-53 Guidelines White Paper

www.us-cert.gov/cdm/home

www.gsa.gov/portal/category/105583

For all acquisition-related technical program questions, eligibility requirements, and ordering guide requests contact: cdm@imperva.com