Solution Brief

THALES
Building a future we can all trust

CYBERSECURITY

Imperva WAF Gateway + Thales Luna HSM

cpl.thalesgroup.com

THALES
Building a future we can all trust

CYBERSECURITY

Enterprise Application Security with Hardware-Protected Keys

Complete web application protection and cryptographic key security from a single vendor

While Web Application Firewalls provide critical protection against external threats, many organizations still expose its TLS private keys in software keystores, creating a significant security gap at the application edge. Even with built-in safeguards, WAFs don't secure cryptographic keys at the same assurance level as dedicated hardware, leaving them vulnerable to insider threats and system compromises. Imperva WAF Gateway + Thales Luna HSM closes this gap by protecting private keys in FIPS 140-3 Level 3 validated hardware—strengthening application security, meeting compliance requirements, and improving overall security posture.

The Challenge

Organizations face an unprecedented convergence of threats and regulatory mandate. Bad bots now account for **37% of all internet traffic**—surpassing human activity for the first time in a decade. Meanwhile, data breach costs soared to an average of **$4.88 million in 2024**, creating extraordinary pressure on security teams.

The Challenge Becomes Acute

Organizations operating in highly regulated industries such as finance, government, and healthcare are increasingly challenged by an evolving data security compliance landscape, facing more regulations than ever before to ensure the protection of sensitive information. PCI DSS 4.0 Requirement 6.4.2 mandates an automated technical solution - typically a Web Application Firewall (WAF) to protect public-facing web applications, effective March 31, 2025. Combined with HIPAA, GDPR, and FedRAMP requirements for both application protection and provable cryptographic key governance, traditional approaches force organizations to choose between security and operational efficiency.

37%

of internet traffic is bad bots

$4.88M

average data breach cost in 2024

The Hidden Vulnerability

Most WAF deployments expose TLS private keys through vulnerable file-based keystores, creating a blind spot at the edge where encrypted traffic is terminated for inspection. While WAFs protect against application attacks, they typically store private keys in software—exposing the "crown jewels" of encryption to insider threats, malware, and system compromises. Adding Luna HSMs as a root of trusts helps reduce this vulnerability and ensure private keys always remain in the tamper-evident, secure environment of the HSM.

Organizations face a difficult choice: accept software-based key storage in their WAF deployments or add a separate HSM vendor that introduces integration headaches, dual vendor management, and operational friction. This trade-off between security and operational efficiency creates unnecessary compromises for enterprises that require both robust protection and streamlined architecture.

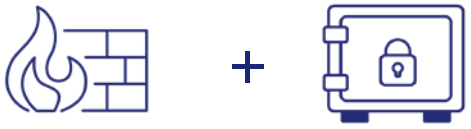
Key Security Challenges Addressed

- Unprotected TLS private keys at the edge
- Inability to prove TLS key governance
- Lack of integrated threat prevention
- Operational friction in certificate management
- Multi-vendor complexity and overhead

The Solution

Thales is the only vendor that owns and manufactures both enterprise-grade WAF technology and FIPS-validated HSM hardware. Together, these Thales solutions provide a comprehensive data security solution that controls the complete stack—eliminating integration risks and vendor finger-pointing.

Market-Proven Technologies



Web Application Firewall + **Hardware Security Module**

How This Solution Works

The Imperva WAF Gateway + Luna HSM solution combines real-time traffic protection with high-assurance key protection. This integration enhances the integrity of SSL/TLS termination, ensures cryptographic operations are anchored in certified hardware, and helps meet strict regulatory requirements.

Application Layer Defense

- Comprehensive protection against OWASP Top 10 threats
- Advanced bot attacks and API vulnerability protection
- Real-time threat intelligence and dynamic profiling
- Near-zero false positives in blocking mode with over 94% deploying from day one
- Keys protected by FIPS 140-3 Level 3 validated hardware
- Keys always remain protected inside the HSM
- Tamper-resistant protection
- Secure cryptographic boundary

Seamless SSL/TLS Integration

- WAF comes pre-installed with Luna HSM client software
- WAF terminates SSL/TLS using Luna HSM-stored keys
- Eliminates software-based keystore vulnerabilities
- End-to-end protection for encrypted traffic

Benefits

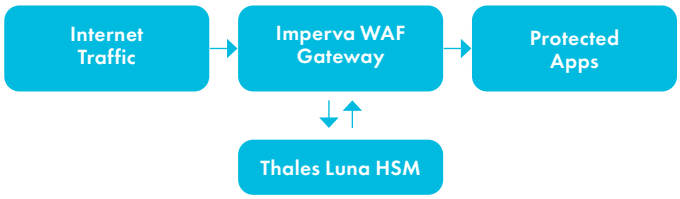
Seamless Integration: Luna HSM Client pre-installed - no additional software needed for HSM integration without application changes or architectural modifications.

Cryptographic Key Protection: TLS private keys remain within FIPS 140-3 Level 3 validated hardware throughout their entire lifecycle.

Operational Simplicity: No infrastructure changes required—just configure WAF to use HSM for TLS operations instead of software keystores.

For Organizations Seeking Complete Data Protection
Deploy enterprise-grade application security with built-in cryptographic key governance from day one. Imperva WAF Gateway provides industry-leading threat protection while Luna HSM ensures your encryption keys remain protected in tamper-resistant hardware.

Unified Architecture



Industry Recognition

KuppingerCole names Thales "Overall Leader" in Data Security Platforms for 2025, while Forrester positions Imperva, a Thales company, as a Leader in Web Application Firewall Solutions. Gartner Peer Insights rates Imperva 4.5 stars across 190+ customer reviews, and multiple FIPS 140-3 Level 3 certifications validate enterprise security architecture.

Elevate Your Application Security

Ready to complete your application security architecture?
Whether you're protecting web applications at scale or meeting stringent compliance requirements, hardware-backed key protection takes your defense to the next level. Join organizations maximizing their security investment with proven solutions.

Discover how Imperva Cloud WAF + Thales Luna HSM delivers FIPS-validated key storage, accelerated compliance, and robust application security.

About Thales

Thales is a global leader in cybersecurity, helping businesses, governments, and the most trusted organizations in the world protect critical applications, sensitive data, identities, and software anywhere, at scale — with the highest ROI. With more than 30,000 customers, including 58% of the Fortune Global 500, our solutions are deployed in 148 countries around the world. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us