

Imperva Cloud WAF + CipherTrust Cloud Key Management

Application Threat Defense

Application Threat Defense & Cloud Key Control

Enterprise Security from Edge to Encryption

Modern organizations face a growing security paradox: while **Imperva Cloud WAF protects applications from external threats**, many organizations still rely on cloud provider-managed keys for their data encryption. With **83% of organizations expressing data sovereignty concerns** and cloud security breaches rising significantly, the gap between application protection and cryptographic control has become a business-critical opportunity. **Combining Imperva Cloud WAF with CipherTrust Cloud Key Management** closes this gap by delivering comprehensive cloud security from applications to data by monitoring, filtering, and blocking malicious traffic while also applying industry-leading cryptography in a unified Thales solution.

The Missing Link in Cloud Security

Organizations cannot achieve comprehensive cloud security with application protection alone. While Cloud WAF defends against OWASP Top 10 threats, bot attacks and more, it provides limited control over the encryption keys protecting data stored in cloud environments.

Traditional approaches create strategic limitations: cloud provider-managed keys limit customer control over cryptographic custody and data sovereignty, while restricting the cloud-agnostic flexibility organizations need for multi-cloud strategies.

83%

of organization have data
sovereignty concerns (1)

35%

increase in cloud security
breaches in 2024 (2)

Market Forces Driving Change

Multi-Cloud Reality: 69% of organizations use three or more cloud providers, yet only 8% encrypt 80% or more of their sensitive cloud data.

Vendor Independence: 89% of IT leaders say companies shouldn't rely on just one cloud provider, driving demand for cloud-agnostic solutions.

Compliance Deadlines: PCI DSS 4.0 mandates automated web application protection (effective March 2025) while requiring comprehensive key management.

Rising Breach Costs: Cloud security incidents now cost multiple millions on average, with 78% of organizations reporting at least one incident.

Address the critical gap between application protection and cryptographic control. While Cloud WAF defends applications from external threats, CipherTrust Cloud Key Management ensures those applications operate with trusted, customer-controlled encryption keys—reducing reliance on cloud provider-managed key services.

Comprehensive Security Benefits

By combining Thales Imperva's industry-leading WAF with CipherTrust Cloud Key Management, organizations achieve:

Layered Defense Strategy

Real-time application protection combined with customer-controlled encryption keys creates comprehensive security from edge to data layer.

Centralized Multi-Cloud Key Control

CipherTrust Cloud Key Management provides unified control across AWS, Azure, Google Cloud, and Oracle Cloud with support for Native, BYOK, and HYOK deployment models.

Cryptographic Sovereignty

Maintain complete custody and control over encryption keys while Cloud WAF protects applications, ensuring data remains inaccessible even if cloud providers face external pressures.

Operational Excellence

Manage native, BYOK, and HYOK keys across all clouds without learning multiple cloud KMS interfaces. Automated key rotation and policy synchronization reduce management overhead.



**Web Application
Firewall**



**Cloud Key
Management**

Industry-Leading Application Protection

Imperva Cloud WAF delivers enterprise-class protection with near-zero false positives, enabling organizations to deploy in blocking mode from day one.

OWASP Top 10 Defense: Real-time blocking of SQL injection, XSS, and remote file inclusion attacks

Advanced Bot Protection: Machine learning-based detection of sophisticated automated threats

API Security: Comprehensive protection for REST and GraphQL APIs

DDoS Mitigation: Integrated protection against volumetric and application-layer attacks

Broad Compliance Coverage

Simultaneously addresses PCI DSS, HIPAA, GDPR, and NIS2 requirements for both application protection and encryption key governance.

Multi-Cloud Freedom

Cloud-agnostic key management preserves flexibility regardless of where applications run—eliminating vendor lock-in while maintaining consistent security policies across all environments.

Organizations can achieve significant reduction in vendor management overhead through single-vendor approach, while reducing potential breach costs by addressing both external application attacks and centralized key governance challenges.

94%

of customers deploy in blocking mode from day one

Near-Zero

false positive enable immediate protection

Ready to Get Started?

Whether you're protecting applications without cryptographic control or managing keys without application visibility, this layered solution delivers comprehensive coverage through proven technologies.

Contact our security specialists to discover how Imperva Cloud WAF + CipherTrust Cloud Key Management addresses your specific compliance requirements and security objectives.

cpl.thalesgroup.com



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

Regulatory Alignment

Organizations across industries face similar compliance challenges that benefit from both application protection and encryption key governance:

PCI DSS 4.0

Automated web attack prevention + key management processes

HIPAA

Technical safeguards for ePHI + encryption when deemed appropriate

GDPR

System resilience against incidents + encryption of personal data

NIS2

Risk-appropriate security measures + cryptography policies and encryption

Implementation Value

Organizations with existing Cloud WAF deployments can seamlessly extend their security investment by adding centralized key management across multi-cloud environments, leveraging established Thales relationships to accelerate deployment while achieving cryptographic sovereignty. **Current CipherTrust users** gain comprehensive application layer defense that complements existing encryption controls, providing visibility across both application threats and key management operations. **For organizations seeking complete cloud security** from the ground up, deploying both solutions together delivers end-to-end protection through a single vendor strategy, reducing operational complexity while ensuring consistent security policies from applications to data encryption across all cloud environments.

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.

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.