Solution Brief

THALES
Building a future we can all trust

CYBERSECURITY

Cloud Web Application Firewall + CipherTrust Data Security Platform

cpl.thalesgroup.com

THALES
Building a future we can all trust

CYBERSECURITY

Modern Layered Security Architecture for Applications

Elevate your organization's security posture by combining robust web application defenses with advanced data protection, ensuring both the pathways to your critical assets and the data itself remain secure. Thales Cyber Security Products empower you to contain threats swiftly when security incidents arise, minimizing risk and disruption. As web applications are continuously targeted by sophisticated adversaries seeking access to sensitive business information, deploying Cloud Web Application Firewalls (WAFs) helps safeguard against threats like SQL injection, cross-site scripting, and other OWASP Top 10 vulnerabilities at the application layer. Yet, today's attackers employ a variety of tactics—including exploiting compromised credentials, abusing insider privileges, and targeting backend systems—to bypass traditional defenses. The CipherTrust Data Security Platform is an integrated suite of Thales solutions that unifies data discovery, protection, and access management under a single centralized console. It helps organizations discover sensitive data across environments, protect it with encryption and tokenization, control access through centralized key and policy management, and continuously monitor data activity to maintain compliance and reduce risk.

WAF + CDSP Architecture Makes Sense

Modern attackers use multiple techniques to reach your data. While Cloud WAF effectively blocks application-layer threats like SQL injection, XSS, and other web-based attacks, determined attackers will explore alternative pathways. They may attempt to exploit compromised user accounts, leverage insider access, target backup systems, or find vulnerabilities in APIs and services that bypass your web application entirely.

CDSP data protection transforms your sensitive data into ciphertext or tokens. Regardless of how attackers attempt to access your databases and file systems, data remains unreadable without the appropriate keys and access permissions. This approach transforms your data into a protected asset that maintains its security even when other defenses are circumvented.

Implementation Approaches

Expanding Existing Web Security: Organizations with Cloud WAF can add CipherTrust database protection to create comprehensive coverage. CipherTrust integrates seamlessly with existing infrastructure without requiring changes to current WAF configurations or application code.

Enhancing Data Protection: Companies using CDSP for database encryption can implement Cloud WAF to prevent threats from reaching protected databases, creating complete application-to-data security coverage. Existing native database encryption can be enhanced by adding CipherTrust Cloud Key Management for robust, centralized, and automated key lifecycle management.

Comprehensive Security Strategy: New implementations can deploy both technologies to achieve application layer protection and database layer security through proven, enterprise-grade solutions.

45%

of real-world intrusions contain lateral movement events with attackers moving through multiple hosts

Strategic Advantages

Multi-Layered Threat Prevention: Cloud WAF stops SQL injection and known threats at the perimeter, while CDSP secures data with encryption and access controls, protecting against insider threats and zero-day attacks.

Defense-in-Depth: Together, they provide end-to-end protection from application layer detection to backend data security, ensuring comprehensive coverage across multiple attack surfaces.

Proactive Risk Reduction: This combination helps prevent breaches reducing the likelihood of data loss, regulatory fines, and costly incident response.

Compliance Coverage: By integrating edge threat detection (which sends encryption logs to an SIEM for reporting, with data protection (which encrypts the data), the solution supports compliance (GDPR, HIPAA, PCI DSS) and is ideal for highly regulated sectors like finance, healthcare, and government.

Complete Security Visibility

Security teams gain unprecedented insight when combining Cloud WAF and CDSP. WAF logs provide detailed information about application-layer attacks, including the types of SQL injection attempts, attack frequency, and source patterns. CDSP logs show exactly who accesses encrypted data and when, including legitimate users and applications.

Together, these logs enable security teams to correlate attack attempts with data access patterns, providing complete forensic traceability from initial attack vector through final data interaction. This comprehensive visibility accelerates incident response and enables faster threat containment when security events occur.

Web Application Firewall

+

CipherTrust Data Security Platform

$1 million

saved on average when breaches are detected internally versus disclosed by attackers, with 61 days shorter breach lifecycle

Technical Architecture & Capabilities

Cloud WAF Protection Layer

- Best-in-class, PCI-certified web application firewall
- Automated protection against OWASP Top 10 threats
- Real-time threat intelligence with daily signature updates
- Terraform integration for DevOps automation
- 24/7 security operations and support team

CDSP Data Protection Layer

- Transparent column-level database encryption
- FIPS 140-2 validated encryption algorithms
- Centralized key management across multiple environments
- Granular access controls by user, group, and application
- Support for Oracle, Microsoft SQL Server, IBM DB2, Teradata

CDSP Products	Description
CipherTrust RESTful Data Protection (CRDP)	Data security controls in your app without installing an SDK/client on our app server.
CipherTrust Application Data Protection (CADP)	Fastest possible response time to return protected data to one or more apps.
CipherTrust Data Protection Gateway (DPG)	Data security controls without modifying existing browser-based web apps.

Compliance Framework Coverage

Every major regulation requires both application protection and data security, creating natural synergy between these capabilities:

HIPAA

PHI protection + web application security

PCI DSS

Cardholder data protection + injection attack prevention

GDPR

Personal data encryption + application security controls

SOX, GLBA

Financial data controls + web threat detection

Solution Benefits

Audit Readiness: Correlated attack and access logs from WAF and CipherTrust speed up forensics, response, and insider threat detection while accelerating audit processes.

Operational Efficiency: Defense-in-depth approach from a unified vendor partnership reduces complexity and vendor sprawl while providing comprehensive coverage from edge-layer threat detection to data protection.

Flexible Deployment Options: Scalable to provide high availability and performance. Cloud WAF's global network can be combined with CDSP as a service or on-premises deployment.

Fast Time to Value: Proactive breach prevention reduces risk of data loss and compliance violations. Even when attackers bypass perimeter protections, CDSP ensures encrypted data remains inaccessible without authorization.

Business Impact

Faster deployment timelines result from cloud-friendly technologies that integrate with existing infrastructure without requiring application changes or extensive reconfiguration, accelerating your security transformation initiatives.

Reduced audit scope becomes possible when a single architectural approach satisfies multiple compliance mandates simultaneously, streamlining regulatory assessments across PCI DSS, GDPR, HIPAA, and other frameworks.

Comprehensive platform growth allows organizations to expand beyond initial encryption use cases, leveraging the full CDSP for data discovery, data protection, data control, and data monitoring as business requirements evolve.

Enhanced incident response capabilities emerge through correlated logging that provides complete forensic traceability from initial web application attacks through final data access attempts.

Improved efficiency through vendor consolidation and reduced management overhead compared to maintaining separate point solutions for web application security and data encryption.

Business Impact

Healthcare organizations leverage this architecture to protect patient records and medical applications from both web-based attacks and unauthorized database access, meeting HIPAA technical safeguards while ensuring PHI remains encrypted against unauthorized users, including system administrators who can manage IT infrastructure without accessing sensitive patient data.

Financial services firms deploy the combined solution to secure online banking platforms and customer data repositories, addressing PCI DSS requirements for both application security and cardholder data encryption while enabling rapid breach detection through correlated logging.

Retail and e-commerce companies protect customer transaction systems and payment processing applications, securing both the web application layer and backend databases storing payment card and customer personal data.

Manufacturing enterprises safeguard industrial applications and intellectual property databases, preventing web application attacks while protecting trade secrets from unauthorized access by database administrators and other privileged users.

Government agencies implement layered protection for citizen-facing web portals and sensitive data repositories, meeting federal security requirements while ensuring classified information remains encrypted against unauthorized database access.

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.

Engage our Security Specialists

Ready to close your data security gaps? Whether you're protecting applications without data encryption or encrypting data without application security, complete coverage is within reach.

Discover how Cloud WAF + CipherTrust Data Security Platform delivers comprehensive protection, accelerated compliance, and measurable business value.

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