Solution Brief

THALES
Building a future we can all trust

CYBERSECURITY

API Threat Defense + Secrets Management

cpl.thalesgroup.com

THALES
Building a future we can all trust

CYBERSECURITY

Comprehensive API Ecosystem Protection

Securing the Complete API Lifecycle: From Credentials to Traffic

Modern digital architectures rely heavily on APIs to connect services, applications, and data across cloud environments. However, this API proliferation creates two serious security challenges: managing the credentials that authenticate API access and protecting the APIs themselves from sophisticated threats. By combining CipherTrust Secrets Management and Imperva API Security, enterprises gain comprehensive protection that secures both the credentials powering API access and the API traffic itself—delivering a unified defense strategy that strengthens security posture while streamlining DevSecOps workflows.

Credential Sprawl Meets API Proliferation

Today's development teams face **mounting pressure to deliver applications faster while maintaining security**. APIs are created rapidly to support microservices architectures, third-party integrations, and cloud-native applications. Each API requires authentication credentials - API keys, OAuth tokens, service account passwords - that are often scattered across repositories, CI/CD tools, and cloud environments.

44%

of advanced bot traffic now targets APIs

(2025 Imperva Bad Bot Report)

61%

cite secrets management as top DevOps challenge

(2024 Thales Data Threat Report)

DevSecOps teams grapple with secrets management across their toolchain: hard-coded API keys in configuration files, unmanaged tokens in CI/CD pipelines, and static credentials buried in container images and Kubernetes secrets. Meanwhile, APIs are created faster than they can be inventoried, leading to shadow APIs with inadequate authentication, missing rate limiting, or misconfigured access controls.

Compliance and Audit Complexity

Regulatory frameworks such as PCI DSS, GDPR, HIPAA, NIS2, and DORA demand comprehensive security controls across both credential management and API protection. Organizations face challenges to provide unified audit trails or demonstrate strong controls across their entire API ecosystem without significant manual effort, creating compliance gaps and operational overhead that can result in failed audits and potential penalties.

API Ecosystem Security

End-to-End Protection Strategy

CipherTrust Secrets Management and Imperva API Security work together to provide comprehensive protection across your entire API ecosystem. While Imperva API Security discovers, monitors, and protects your APIs from runtime threats including OWASP API Top 10 risks and business logic abuse, CSM ensures that the credentials powering those APIs are securely managed, rotated, and controlled through centralized policy enforcement.

Bridge API traffic protection and credential security. While Imperva API Security discovers and protects APIs from runtime threats, CipherTrust Secrets Management powered by Akeyless (CSM) ensures the API keys, tokens, and credentials powering those APIs are centrally managed and securely rotated—eliminating credential sprawl across DevOps pipelines.

Seamless Integration for DevSecOps

This solution eliminates the friction between security and development velocity. CSM integrates natively with DevOps tools like GitHub, Kubernetes, and OpenShift, enabling policy-driven secret injection without disrupting development workflows. Imperva API Security provides agentless API protection that deploys in minutes, automatically discovering APIs and protecting them without code changes.

The combination of the two Thales solutions addresses the core challenge of developers bypassing security controls to maintain delivery speed—with automated secret injection and agentless API protection, security becomes transparent to development teams while maintaining comprehensive protection. Both solutions provide enhanced visibility when deployed together. CSM logs all credential access patterns while Imperva monitors API traffic behavior.

Enhanced Security Posture

CipherTrust Secrets Management and Imperva API Security deliver automated secret lifecycle management and real-time

API threat protection across development, staging, and production environments.

Eliminate Credential Sprawl

CSM centralizes secrets management with policy-based

access controls and automated rotation, preventing hard-coded credentials in repositories and CI/CD pipelines. Dynamic secrets and just-in-time credential provisioning replace static secrets that create long-term exposure risks.

Complete API Visibility and Protection

Imperva automatically discovers all APIs across your environment, including shadow APIs and deprecated endpoints, and provides real-time protection against sophisticated threats. This includes business logic abuse detection, bot protection, and data leakage prevention that traditional security tools lack.

Unified Compliance Management

The joint solution provides comprehensive audit trails across both credential usage and API access patterns. Organizations can demonstrate strong controls for regulated data and API exposure with automated logging and policy enforcement that aligns with regulatory requirements across multiple frameworks.

Enhanced Security Posture

Developer Productivity Enhancement

Enable developers to move fast without compromising security. Policy-driven secret injection eliminates manual credential management, while agentless API protection works behind the scenes without requiring code changes. This approach eliminates security bottlenecks that typically slow development cycles.

Automated Risk Reduction

Both solutions automate capabilities that reduce human error and enforce security policies. CSM automates credential lifecycle management, while Imperva automates threat detection and response, reducing operational burden.

Single Vendor Simplicity

Reduce vendor management complexity and procurement overhead by consolidating your API security and secrets management under one trusted provider. Eliminate vendor finger-pointing and streamline support relationships.

Regulatory Alignment

Organizations across industries face similar compliance challenges that benefit from both API protection and secrets management:

PCI DSS 4.0, SOX

Secure authentication + financial system audit trails

HIPAA

ePHI protection + auditable credential access

GDPR

Breach detection + data encryption controls

NIS2, DORA

ICT security measures + incident classification

Real-World Impact

DevSecOps teams eliminate hardcoded secrets in CI/CD pipelines through automated secret injection while gaining instant API visibility across all environments without agents or code changes.

Security architects implement Zero Trust principles with fine-grained access controls for both secrets and API endpoints, reducing attack surface through centralized secrets governance and real-time API threat detection.

Compliance officers demonstrate strong controls for sensitive data protection with comprehensive audit trails from both credential usage and API access, streamlining audit processes with detailed logging that supports regulatory requirements.

Platform engineers standardize security controls across hybrid and multi-cloud environments, integrate with existing Kubernetes and API gateway infrastructure, and scale security automatically as deployments grow while maintaining operational simplicity through consistent policy frameworks.

Deployment Scenarios

Current Imperva API Security customers often identify weak authentication tokens as a major factor contributing to risk. By utilizing CSM, organizations can seamlessly add secrets management capabilities, including secure token management to existing deployments, immediately enhancing credential security across their API ecosystem. Imperva API Security covers audit and assessment, while CSM provides the API token management solution.

Current CSM customers can extend protection to API traffic, completing their comprehensive data security strategy with runtime API protection.

Organizations benefit from complete API lifecycle security from day one, avoiding the complexity of integrating point solutions.

Engage our Security Specialists

Ready to secure your complete API ecosystem? Contact your Thales representative to discuss how our integrated approach can strengthen your security posture while accelerating your DevSecOps initiatives.

Transform your API security strategy with a solution that eliminates credential sprawl while protecting against sophisticated threats across your entire digital infrastructure.

Discover how combining CipherTrust Secrets Management + Imperva API Security delivers comprehensive protection, accelerated compliance, and measurable business value.

About Thales

Thales is a global leader in cybersecurity, helping the most trusted organizations protect critical applications, data, identities, and software anywhere, at scale. Through Thales' integrated platforms, customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

cpl.thalesgroup.com

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