wallarm

# API Security for Financial Services

www.wallarm.com
(415) 940-7077
188 King St. Unit 508, San Francisco, CA 94107

wallarm

# API Security for Financial Services

## The State of API Security in Finance

As financial institutions and fintech companies undergo rapid digital transformation, APIs have emerged as both a critical business enabler and a growing risk. These organizations rely heavily on APIs to power online banking, mobile apps, payment systems, and partnerships with third-party providers. While APIs unlock innovation and improve customer experiences, they also expose the enterprise to new and evolving threats.

The sheer volume and complexity of APIs in the financial sector is staggering. A single institution may operate hundreds or even thousands of APIs, spanning internal systems, external partners, and customer-facing applications. This sprawl makes it difficult to maintain visibility and control, particularly as APIs are developed and deployed across diverse teams and business units.

At the same time, APIs have become a primary target for attackers. Cybercriminals exploit vulnerabilities to scrape sensitive data, take over customer accounts, and abuse business logic for financial gain. High-profile breaches have shown how weaknesses in API security can lead to regulatory penalties, reputational damage, and financial losses.

Compounding the risk is a complex web of compliance obligations. Regulatory bodies scrutinize financial APIs closely, requiring organizations to demonstrate strong controls over access, authentication, and data protection. Meeting these expectations demands a proactive, continuous approach to API security, one that spans discovery, risk assessment, protection, and monitoring.

## Regulatory Requirements for Financial APIs

In response to the growing threat landscape and the increasing reliance on APIs in digital financial services, U.S. regulatory bodies have implemented a range of requirements that govern how APIs must be secured. These regulations are not only aimed at mitigating cyber risk but also at ensuring customer data protection, operational resilience, and effective oversight of third-party relationships. Financial institutions and fintechs must navigate a complex matrix of compliance frameworks, each with expectations around API inventory, risk assessments, continuous monitoring, and data protection. Below is a summary of the most relevant regulations and their implications for API security.

### FFIEC IT Examination Handbook

The Federal Financial Institutions Examination Council (FFIEC) outlines clear expectations for information security, including requirements that directly apply to APIs, within its IT Examination Handbook. While APIs are not explicitly named, their inclusion is required through controls over application security, interconnectivity, and asset classification. For example, Section II.C.5 requires institutions to maintain a current inventory of technology assets, including software and interconnections, which encompasses APIs. Section II.C.17 mandates secure application development, including testing for vulnerabilities and controls like authentication, access control, and encryption—all critical for API security. Additionally, Section II.C.6 requires controls over interconnected systems, including third-party APIs, and Section II.C.22 emphasizes log management for anomaly detection, which applies directly to API activity.

## OCC and Interagency Guidance

The Office of the Comptroller of the Currency (OCC), along with other regulatory agencies, emphasizes third-party risk management in guidance such as OCC Bulletin 2023-17 and Bulletin 2013-29. These require banks to conduct due diligence and continuous oversight of third-party relationships, including APIs exposed to fintech partners. In the OCC's Payment Systems Handbook, the agency explicitly states that 'API protocols must be current' and that poor API security design may expose data to compromise. This guidance establishes expectations for monitoring third-party API behavior, securing data flows, and validating partner integration against current standards.

## GLBA Safeguards Rule

Under the Gramm-Leach-Bliley Act (GLBA), financial institutions must implement a written information security program to protect customer data. The Interagency Guidelines (12 CFR 364 Appendix B) include requirements that encompass API traffic and exposure. These include periodic risk assessments (§III.B), adoption of access controls (§III.C.1), employee training (§III.C.2), and vulnerability testing (§III.C.3). APIs that handle customer information—such as login, transaction, or account detail services—must be monitored and protected with the same rigor as other customer-facing systems.

## NIST RMF / FISMA

Though originally designed for federal systems, the NIST Risk Management Framework (SP 800-37) and FISMA are widely adopted in the financial sector. The NIST RMF requires organizations to categorize systems (including APIs), implement security controls (SP 800-53), assess and authorize them, and continuously monitor operations. NIST SP 800-53 rev 5 includes specific controls applicable to APIs such as AC-4 (information flow enforcement), SI-10 (information input validation), and AU-12 (audit generation). These controls establish requirements for API access enforcement, schema validation, anomaly monitoring, and secure development.

## PCI Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS v4.0) applies to any API that stores, processes, or transmits cardholder data. It mandates the use of secure coding techniques (Req. 6), strong authentication and access control (Req. 7–8), and logging and monitoring (Req. 10). Specifically, Req. 6.4.3 requires vulnerability detection and management for APIs, and Req. 6.2 mandates that all system components, including APIs, are kept up to date with security patches. APIs exposing payment data must be regularly tested for flaws like broken object level authorization, formerly called insecure direct object reference (IDOR).

# How Wallarm Helps Meet These Requirements

## API Discovery & Inventory

Wallarm's platform automatically discovers and catalogs all APIs across an organization's environment, including internal, external, and third-party APIs. The system provides a risk rating for APIs based on sensitivity, exposure, and complexity, providing the complete visibility needed to comply with FFIEC, GLBA, and NIST requirements for API inventory.

## Risk Assessment & Vulnerability Testing

Wallarm continuously scans APIs for vulnerabilities such as those in the OWASP API Security Top 10. It detects misconfigurations, weak authentication, and logic flaws. Risk scores are generated for each API and integrated into compliance-aligned reporting, helping institutions perform ongoing assessments as mandated by FFIEC, GLBA, and PCI DSS.

## Continuous Protection & Monitoring

Wallarm provides machine learning–driven attack detection to identify credential stuffing, API abuse, account takeover, and more. Its enforcement capabilities include blocking, specification enforcement, and rate limiting to secure traffic in real time. These features ensure continuous protection aligned with the requirements of NIST, FFIEC, and PCI DSS.

## API Security Testing

Wallarm provides API security testing for pre-production and production APIs, supporting shift-left security practices in addition to finding risk in production. Vulnerabilities can be identified and remediated during development to reduce risk. In production, Wallarm delivers API-specific telemetry that supports incident response, enabling organizations to quickly detect, analyze, and respond to threats in accordance with GLBA and OCC expectations.

## Compliance Reporting & Dashboards

Wallarm provides detailed reporting on attacks and vulnerabilities, supporting evidence collection for compliance requirements. Users can sort and filter data for reports, ensuring the right data is collected to support specific regulatory requirements.

# Wallarm Coverage of Key Regulations

| Regulation | Requirement | Wallarm Capability |
|---|---|---|
| FFIEC IT Handbook | API inventory, risk analysis, monitoring | Automated discovery, risk scoring, behavior detection |
| OCC Third-Party Oversight | Fintech API monitoring, data protection | Partner API telemetry, anomaly alerts |
| GLBA Safeguards Rule | Risk analysis, safeguard audits | Vulnerability testing, attack surface mapping |
| NIST RMF | Continuous monitoring, risk mitigation | API traffic inspection, continuous protection |
| PCI DSS | Secure coding, access control | Web Application and API Protection (WAAP), specification enforcement, API security testing |

# Conclusion

Regulations are clear: APIs in finance must be cataloged, assessed for risk, continuously protected, and auditable. Wallarm delivers a comprehensive API security platform that fulfills these requirements, empowering security and compliance teams to:

- Maintain a real-time API inventory
- Continuously detect vulnerabilities and behavioral anomalies
- Enforce protective controls and threat detection
- Generate audit-ready compliance reports

Wallarm makes financial API security easier, faster, and more effective—supporting both regulatory compliance and customer trust.

BOOK A DEMO