TRACEABLE

COMPLIANCE AND SECURITY POSITION WHITEPAPER

Meeting Regulatory and Industry Standards for API Security

New whitepaper examines the regulatory requirements and standards that are shaping the demand for API security measures and implementation strategies.

Regulations and Standards Covered:

- FFIEC: Authentication and Access to Financial Institution Services and Systems
- OCC: Model Risk Management Booklet
- FS-ISAC FDX API
- CFPB: Open Banking and General-Use Digital Consumer Payment Rule
- Federal Reserve: FedNow
- PCI DSS 4.0
- FTC Safeguards Rule
- ISO 20022 (SWIFT replacement)
- White House Executive Order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

Introduction

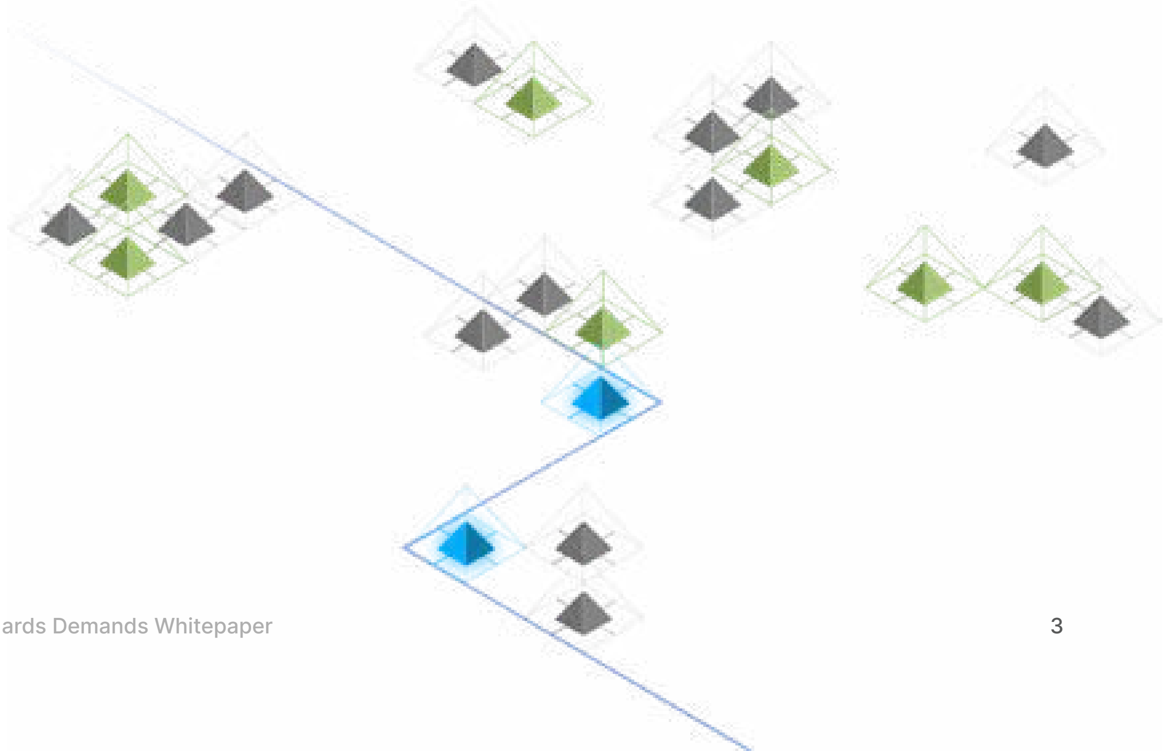
The demands for API security in the banking sector are becoming increasingly prescriptive, driven by the evolving landscape of cybersecurity threats and regulatory requirements. As financial institutions rely more on APIs to enable digital services, the vulnerabilities associated with these interfaces have come under intense scrutiny. Regulatory bodies worldwide are now mandating stricter API security measures to safeguard sensitive financial data and ensure the integrity of banking operations

One of the primary catalysts for these enhanced regulatory demands is the rising number of API-related breaches. APIs, which facilitate the seamless exchange of data between different software systems, have become attractive targets for cybercriminals. These attackers exploit weaknesses in API security to gain unauthorized access to sensitive information, execute fraudulent transactions, and disrupt financial services. The trend of API exploitation by malicious actors continues to grow, necessitating a proactive approach to securing these digital assets.

In response to these threats, regulatory frameworks have evolved to include specific guidelines for API security. For instance, the Financial Stability Board (FSB) and the European Banking Authority (EBA) have introduced directives that require financial institutions to implement robust API security measures. These include stringent authentication and authorization protocols, continuous monitoring for anomalies, and regular security assessments. Additionally, the Federal Financial Institutions Examination Council (FFIEC) in the United States has emphasized the need for comprehensive API security strategies as part of their broader cybersecurity guidance. The shift towards more prescriptive regulations reflects a broader understanding that API security is not just a technical issue but a critical component of overall financial stability and consumer trust. As financial services become more digitized, the protection of API endpoints becomes paramount.

Institutions are now required to adopt a security-first mindset, integrating API security into their development lifecycles and ensuring that all APIs comply with regulatory standards.

The increasing prescriptiveness of API security demands in banking regulations underscores the critical role APIs play in modern financial ecosystems. By adhering to these evolving standards and predicting the operational implications of future regulatory directives, financial institutions can better protect themselves against emerging threats, maintain regulatory compliance, and uphold the trust of their customers in an increasingly digital world.



Current Regulations and Standards and their API Security Implications

ENTITY:

FFIEC

SOURCE DOCUMENT:

Authentication and Access to Financial Institution Services and Systems August 11, 2021

Requirements

- **Comprehensive API Inventory:** The FFIEC guidelines mandate that financial institutions maintain a detailed inventory of all APIs. This inventory should include information about the APIs' functions, the data they access or manipulate, and the systems they connect to. By cataloging all APIs, institutions can better understand their digital landscape and identify potential vulnerabilities. This inventory serves as a foundational element in managing API security, enabling institutions to monitor and control their API usage more effectively.
- **Risk Assessment:** Alongside maintaining an API inventory, the FFIEC requires financial institutions to conduct thorough risk assessments for each API. These assessments must evaluate the potential security risks associated with each API, considering factors such as data sensitivity, exposure to external threats, and the potential impact of a security breach. The risk assessment process should be continuous, reflecting the dynamic nature of API usage and the evolving threat landscape. This ongoing evaluation helps institutions prioritize their security efforts and allocate resources to the most critical areas.

ENTITY:

Office of the Comptroller of the Currency

SOURCE DOCUMENT:

OCC Model Risk Management Booklet
August 18, 2021

Requirements

- The OCC mandates that institutions must identify and evaluate each API's potential impact on the integrity and reliability of financial data. This includes assessing the APIs for vulnerabilities that could lead to unauthorized access or data manipulation, which could compromise financial reporting accuracy.

ENTITY:

FS-ISAC FDX API

SOURCE DOCUMENT:

FS-ISAC Website FDX API Description

Requirements

- The Financial Data Exchange (FDX) was established on the idea that consumers and businesses should have easier, more secure access to their financial data. Through its FDX API and technical frameworks, FDX is unifying leading financial institutions, fintechs and others around a common standard for data sharing across the entire financial industry.
- Security requirements aren't specified publicly and would only be available to FS-ISAC member banks. However, given that the FDX API is a published standard, API security and monitoring will be an absolute necessity to insure the integrity of the API payment scheme.

ENTITY:

CFPB (Consumer Finance Protection Bureau)

SOURCE DOCUMENT:

Multiple CFPB Rule Making Announcements since December 2023

Requirements

Open Banking

- Under the proposed Personal Financial Data Rights rule, people would have the power to share data about their use of checking and prepaid accounts, credit cards, and digital wallets. The CFPB's Open Banking requirements leverage APIs to enhance transparency and facilitate secure data sharing between financial institutions and third-party providers. By mandating the use of standardized APIs, the CFPB aims to promote interoperability and ensure that consumers have greater control over their financial data. This approach allows for seamless integration of various financial services, enabling consumers to access a wide range of banking products and services through a single platform. APIs also support real-time data exchange, which improves the accuracy and efficiency of financial transactions and reporting, thereby enhancing the overall consumer experience in the financial ecosystem.

General-Use Digital Consumer Payment Rule

- The CFPB's general-use digital consumer payment rule focuses on ensuring transparency, security, and consumer control over digital transactions. The rule mandates that digital payment providers offer clear, concise information about fees, transaction details, and consumer rights. It also emphasizes the necessity of secure authentication methods and data protection to prevent unauthorized access and fraud. Additionally, the rule requires that consumers have easy access to their transaction history and the ability to dispute unauthorized transactions efficiently. By setting these standards, the CFPB aims to foster a trustworthy digital payment environment that prioritizes consumer protection and financial transparency.

AGENCY/ENTITY:

Federal Reserve

SOURCE DOCUMENT:

Multiple directives and communications from the Cleveland Federal Reserve, Federal Reserve Bank of St. Louis

Requirements

FedNow

- The Federal Reserve has announced that the FedNow service, which initially launched in July 2023, will expand to include consumer payments. This development is part of a broader effort to modernize the U.S. payment system by enabling real-time payments. The FedNow service aims to provide individuals and businesses with the ability to send and receive payments instantly, 24/7, thereby enhancing the speed and convenience of financial transactions
- The expansion to consumer payments is expected to significantly impact the way people handle everyday financial transactions, offering immediate access to funds and improving the efficiency of payment processes across various sectors,
- The FedNow service relies on APIs to facilitate real-time payments. The Federal Reserve designed FedNow with a strong emphasis on API integration to enable financial institutions to seamlessly connect their systems and offer instant payment services. These APIs allow for the secure and efficient transmission of payment data between different financial entities, ensuring that transactions can be processed instantly, 24/7.
- APIs are crucial for FedNow's functionality as they support interoperability and standardization across various banking platforms. This integration ensures that financial institutions can offer their customers immediate access to funds, enhanced payment tracking, and reduced transaction times, thereby modernizing the U.S. payment infrastructure.

ENTITY:

Payment Card Industry (PCI-DSS) Security Standards Council

SOURCE DOCUMENT:

PCI DSS 4.0 Specification

Requirements

PCI DSS 4.0

- The PCI DSS 4.0 standard includes several significant implications for API security to ensure the protection of payment card data. Key requirements include:
- **Comprehensive API Inventory:** Organizations must maintain an up-to-date inventory of all APIs, including bespoke and custom software. This inventory is crucial for risk assessment, security testing, and incident response.
- **Secure Development Practices (Requirement 6):** PCI DSS 4.0 emphasizes the importance of embedding security throughout the Software Development Lifecycle (SDLC). This involves secure coding practices, regular code reviews, and addressing common vulnerabilities such as injection flaws and buffer overflows. Developers must receive annual training on these practices to stay current with evolving threats.
- **Authentication and Access Controls (Requirements 7 and 8):** The standard mandates robust authentication mechanisms, including multifactor authentication (MFA) and strict access controls to ensure that only authorized individuals can access sensitive API endpoints. This helps prevent unauthorized access and ensures that APIs are securely managed.
- **Encryption and Secure Protocols:** All data transmitted via APIs must be encrypted using robust cryptographic protocols like TLS. This ensures the confidentiality and integrity of sensitive information, reducing the risk of interception and unauthorized access during data transmission.
- **Logging and Monitoring:** Organizations are required to log all API activities and conduct regular reviews to detect and respond to unauthorized access attempts or excessive privileges. This continuous monitoring helps in maintaining a secure environment for API operations.
- By adhering to these requirements, organizations can better protect their APIs from common security threats, ensuring compliance with PCI DSS 4.0 and safeguarding sensitive payment card information.

ENTITY:

Federal Trade Commission

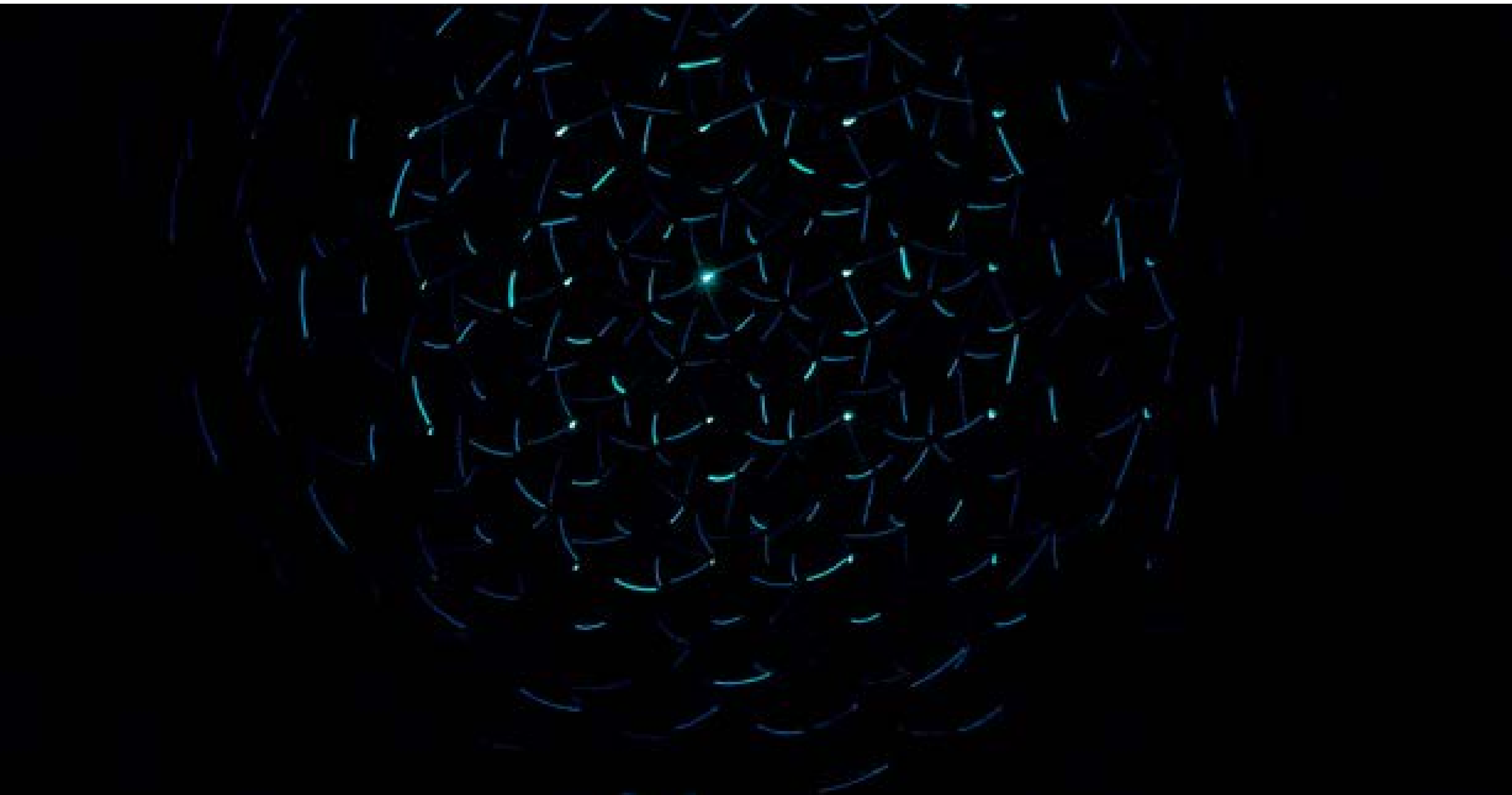
SOURCE DOCUMENT:

FTC Website

Requirements

FTC Safeguards Rule

- In May 2024 the FTC updated the Safeguards Rule, including more stringent breach notification requirements (in line with the SEC's recent breach notification change) and places a strong emphasis on encryption and proactive, not reactive, security measures.
- The FTC has expanded the Safeguards Rule to include non-bank financial companies. This amendment to the Gramm-Leach-Bliley Act (GLBA) mandates that non-bank financial institutions, such as mortgage brokers, motor vehicle dealers, payday lenders, and other similar entities, develop and maintain comprehensive security programs. Additionally, these institutions are now required to report data breaches to the FTC if the breach involves unauthorized access to unencrypted customer information affecting 500 or more consumers. The report must be submitted within 30 days of discovering the breach.



ENTITY:

International Standards Organization

SOURCE DOCUMENT:

ISO 20022 Design Documentation (credit - Finextra Research)

Requirements

ISO 20022 (SWIFT replacement)

- ISO 20022, a global standard for financial messaging, includes specific requirements for API security to ensure the secure exchange of financial data. The standard outlines several key aspects:
- **Data Encryption:** ISO 20022 mandates encryption of data both in transit and at rest to protect sensitive financial information from unauthorized access and breaches.
- **Secure Authentication:** APIs must implement robust authentication mechanisms, including OAuth 2.0 and other secure token-based methods, to verify the identity of users and systems accessing the financial data.
- **Data Integrity and Validation:** Ensuring the integrity of data is crucial. ISO 20022 specifies that financial institutions must implement measures to validate data accuracy and consistency throughout the transaction lifecycle. This includes technical and business validations to prevent errors and fraud.
- **Standardized Messaging Format:** ISO 20022 promotes the use of standardized messaging formats such as JSON and XML for API communications. This standardization facilitates interoperability and reduces the complexity of integrating different systems.
- **Comprehensive Documentation:** Detailed documentation of APIs, including their functions, endpoints, and security protocols, is required. This documentation supports transparency and ensures that developers and users understand the security measures in place.
- **Access Controls:** Implementing strict access controls to restrict API access to authorized users and systems is essential. This helps prevent unauthorized access and potential breaches.
- By adhering to these requirements, financial institutions can ensure that their API implementations are secure, compliant with regulatory standards, and capable of facilitating safe and efficient financial transactions.

ENTITY:

White House Executive Office

SOURCE DOCUMENT:

Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (credit - Harvard Belfer Center Research and Center for Center for a New American Security research referenced). October 30, 2023

Requirements

Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

- The Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, issued by President Biden, has several implications for API security. This order, which seeks to ensure the responsible development and deployment of AI, emphasizes the importance of securing APIs, especially those used in critical infrastructure and sensitive applications.

Key API security implications include:

- **Enhanced Reporting Requirements:** Entities developing or utilizing large-scale AI models must report their activities, including the security measures used to protect these models. This includes reporting on the physical and cybersecurity measures in place to safeguard API endpoints involved in AI model training and deployment.
- **Identity Verification and Record-Keeping:** The order mandates the Secretary of Commerce to draft regulations requiring Infrastructure as a Service (IaaS) providers to verify the identities of foreign entities using their services for AI training. This includes establishing minimum standards for verification and ensuring comprehensive record-keeping, which impacts how APIs handle authentication and data logging.
- **Integration with National Security Protocols:** Agencies are directed to assess AI's potential risks within critical infrastructure and report findings. This includes evaluating how APIs are used to facilitate AI integrations and ensuring they adhere to stringent security protocols to prevent vulnerabilities.
- **Development of AI Safety and Security Board:** The creation of an AI Safety and Security Board to offer recommendations on improving AI security also impacts API management. This board will likely influence best practices for securing APIs that interface with AI systems, ensuring they are robust against cyber threats.

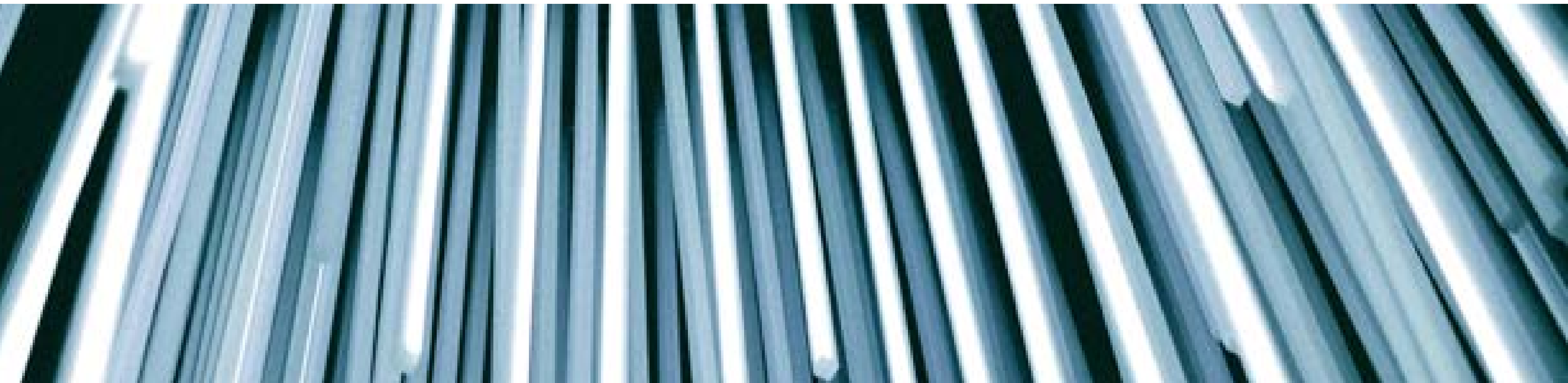
- **International Cooperation and Standards:** The order emphasizes global coordination, which includes developing international frameworks for the secure use of AI. This will likely result in standardized API security practices across borders, ensuring consistent protection measures.
- **By enforcing these measures, the Executive Order aims to strengthen the security of APIs used in AI applications**, thereby protecting sensitive data and critical systems from potential cyber threats. For more detailed information, you can refer to sources such as the Belfer Center for Science and International Affairs, Lawfare, and the Center for a New American Security.

The Bottom Line

The regulatory landscape has placed a significant emphasis on the security of APIs, recognizing their critical role in modern financial ecosystems. Regulatory bodies worldwide have introduced stringent guidelines and mandates that require financial institutions to implement robust API security measures to safeguard sensitive data, ensure operational integrity, and maintain consumer trust.

This whitepaper has examined the key regulatory requirements and industry standards that are shaping the demand for comprehensive API security practices. The analysis covers directives from entities such as the FFIEC, OCC, CFPB, Federal Reserve, PCI Security Standards Council, FTC, and the White House Executive Office, among others.

By adhering to these regulatory and standards-based requirements, financial institutions can better protect their APIs from emerging threats, maintain compliance, and position themselves to adapt to the evolving digital landscape. Implementing effective API security controls, continuously monitoring for anomalies, and aligning with industry best practices are crucial steps in building a resilient and compliant API infrastructure.



About Traceable

Traceable is the industry's leading API Security company that helps organizations achieve API visibility and attack protection in a cloud-first, API-driven world. Traceable is the only intelligent and context-aware solution that powers complete API security – API discovery and posture management, API security testing, and attack detection and protection, anywhere your APIs live. Traceable enables organizations to minimize risk and maximize the value that APIs bring their customers.

www.traceable.ai