A Comprehensive Approach to API Security for Financial Services

Data Theorem Voice

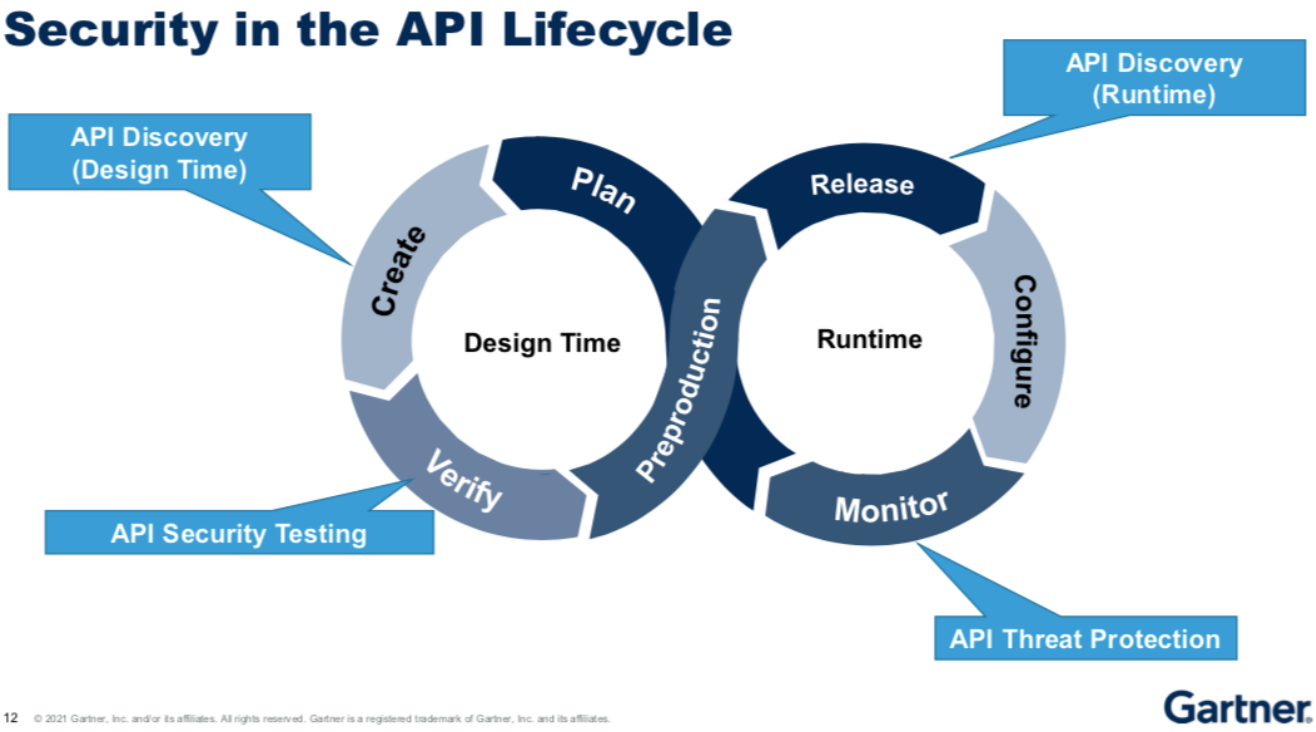
2024

Securing Your Digital Crown Jewels

A Comprehensive Approach to API Security for Financial Services

In the ever-evolving landscape of the digital economy, Application Programming Interfaces (APIs) have emerged as the fundamental building blocks facilitating seamless interaction between various systems and platforms. However, this proliferation of APIs has also escalated security risks, particularly within the financial services industry, where sensitive data and financial transactions are at stake. To effectively mitigate these risks, information security leaders must adopt a proactive and strategic approach towards API security.

This whitepaper outlines key considerations and best practices for establishing a robust API security program tailored to the unique needs of financial institutions.



Introduction

As the backbone of modern digital ecosystems, APIs play a pivotal role in enabling connectivity and driving innovation across industries. In the financial services sector, APIs facilitate secure data exchange, streamline processes, and enhance customer experiences. It's one of the very reasons why the FinTech industry, specifically, has exploded so much. However, the rapid adoption of APIs has introduced new vulnerabilities and threats, necessitating a comprehensive security framework to safeguard critical assets and maintain regulatory compliance.

API Security Risks in the Financial Industry

The financial services industry is witnessing a surge in API-related security incidents.

2019 First American Corporation

The 2019 data breach with First American Corporation truly highlights the havoc a misconfigured API can bring to an organization - an impact of 885 million credit card applications, one of the largest in the last 10 years. The event that caused this data breach was a data leak due to an unauthenticated API. In this specific case, the hacker used an IDOR attack, or Insecure Direct Object Reference Attack, one of the most common forms of API breach. A seemingly small oversight that essentially made history in cybersecurity.

2019 CapitalOne

That same year, CapitalOne also made cybersecurity history. Although the misconfiguration of certain cloud assets is often stated to be the primary culprit in CapitalOne's data breach, the reason why these cloud assets were able to be exploited was due to an API vulnerability. In this case, the vulnerability exploited is called SSRF or Server-Side Request Forgery. This happens when an API makes calls to other services. In this case, the malicious attacker can manipulate API requests and gain unauthorized access to internal network resources that are typically protected by a firewall (false sense of security). Here, the attacker leverages different cloud assets as a pivot point to gain access to more interesting things internally. When it comes to the role the API played, it was due to an API failing to properly validate user input. It assumed that because of where the input was coming from, everything was safe. Clearly, the concept of zero-trust couldn't ring any truer in this scenario. This is why it's critical to understand what data your APIs are touching to better prioritize the coverage and safeguards required.

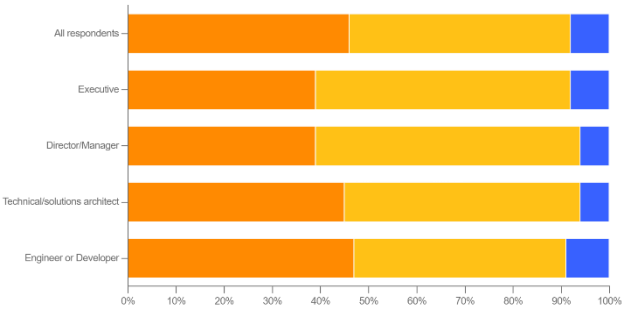
These examples are only some of the more buzz-worthy hits. The industry as a whole has seen significant increases in data breaches, cyberattacks, and fraudulent activities targeting APIs. This escalation underscores the urgency for organizations to fortify their API security defenses and mitigate potential risks associated with unauthorized access, data breaches, and service disruptions.

The Importance of API Inventory

Central to any effective API security strategy is the establishment of a clear inventory of all APIs within the organization's ecosystem. This inventory serves as the foundation for assessing security posture, identifying vulnerabilities, and prioritizing risk mitigation efforts. By maintaining an up-to-date inventory, organizations can gain visibility into their digital assets and effectively manage security risks across the API lifecycle.

According to a survey done by Postman, 92% of organizations' say their investment of time and resources into APIs will stay the same or increase. Over 50% of executives and director/management

level leads say that it will increase. The reasons for this are simple - connectivity. APIs truly make it simpler and easier to connect systems and information.



https://www.postman.com/state-of-api/api-global-growth/#api-global-growth

This growth makes it all the more critical to have a single source of truth so that your team has the visibility into what APIs require testing and which APIs to prioritize for the business. This brings us to our next point.

According to Gartner's most recent Market Guide on API Protection, API inventory falls under the recommended API discovery capabilities. Security leaders often mention how nefarious dormant ("zombie) and shadow ("rogue") APIs are to the business. But gaining visibility into all APIs in one place, leaders can now act accordingly.

Common Baseline Safeguards: API Posture Management (API Health)

Establishing a baseline security posture for APIs is paramount to mitigating common threats and vulnerabilities.

Key safeguards include robust authentication mechanisms, fine-grained authorization controls, availability visibility, and end-to-end encryption to protect data in transit and at rest. By implementing these foundational security measures, organizations can establish a strong security foundation and mitigate the risk of unauthorized access and data breaches.

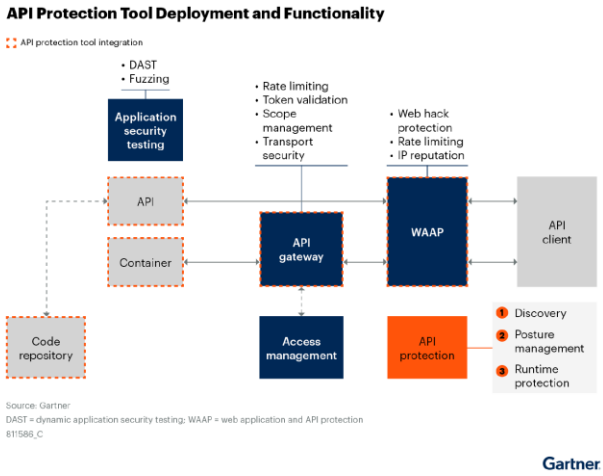
1. Authentication
2. Authorization
3. Availability
4. Encryption

Visibility and continuous monitoring and testing for these safeguards are a necessary Step 1 to get a proper handle on the various APIs that exist in your application and technical environment. In this case, we can call this API Posture Management - ensuring the configuration of your APIs are expected.

By taking this proactive approach towards API security and integrating a continuous approach into your security practices, organizations can identify and remediate common vulnerabilities in real-time. As a result, this minimizes the window of exposure to potential exploits and cyber threats. Once Inventory and API Posture Management have been achieved, security testing becomes much simpler to wrap your hands around and manage. Here, organizations should be leveraging automated scanning tools and penetration testing techniques, preferably automated, in a continuous fashion. This helps to ensure that your applications and cloud environments are always tested and monitored throughout the many changes it sees during development. Manual security testing is also advised in conjunction with the securing scanning and testing. The purpose of using the 2 techniques is not just to meet compliance requirements, but to narrow the manual security testing scope so that truly nefarious vulnerabilities are identified.

API Security Strategies

Gartner's most recent Market Guide for API Protection highlights the importance of taking a programmatic, big-picture approach to API security. While early adopters have been acquiring point solutions to address specific API security needs, it is clear that the industry is searching for something more holistic.



The following list the 3 main capabilities expected of an API security tool:

1. API Discovery
2. API security posture management
3. API runtime protection (or API detection & response)

One of the most eye-opening components to this is how the proliferation of APIs require integration to nearly every aspect of the application build.

- Code repository
- API
- Containers
- API Gateway
- WAAP

As a result, we recommend first focusing on homegrown (first-party APIs) that are public-facing and provide connectivity to critical applications, followed by third-party APIs that are both either open-source and/or provided by SaaS platforms.

Discovery & Inventory

API security begins with knowing what APIs your organization has. API Security programs should all begin by automatically discovering APIs in use, whether they are public or internal. It employs advanced crawling techniques to located APIs within web applications, mobile applications, and cloud services, to ensure that no API remains hidden. The discovery process needs to be continuous to provide organizations with an up-to-date inventory of their APIs as new services are deployed.

API Security Posture Management

Continuous monitoring of your APIs is a must-have to assess the inventoried APIs for misconfigurations or unsecure implementations. Even though an API may be configured correctly one day, it could very well be misconfigured the next due to testing reasons. Teams will want to look for solutions that can ingest description files like OAS/Swagger and GraphQL schemes that can then compare them to actual traffic with the absorbed schema during runtime. Better yet, the ability to ingest data during the API testing, such as that in Postman collections, will help to improve coverage.

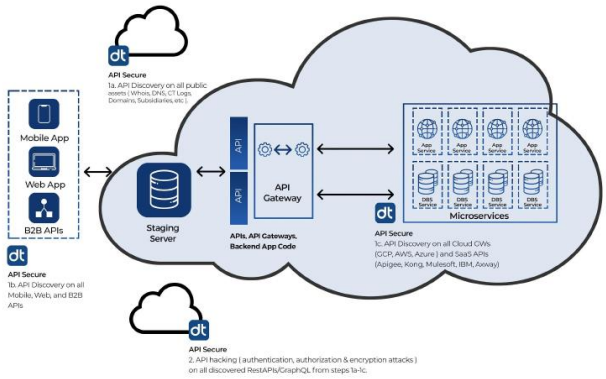
Security Testing is also a key component to API security posture management. By employing static analysis and dynamic analysis, teams will be able to identify issues earlier in the development cycle, so that teams can rectify them before they become exploitable weaknesses. Simulating real-world API interactions will uncover runtime vulnerabilities that represent the vulnerabilities that result in data breaches, as described earlier in this document.

Runtime Protection

Runtime protection monitors API interactions in the wild and can block malicious activity immediately. By providing organizations with a defense mechanism, teams will be able to react to threats as they occur, reducing the window of the vulnerability's accessibility.

Here, teams want to integrate with their Web Application Firewalls (WAFs) by sharing API threat intelligence. This enhances the WAF's ability to mitigate API-related attacks, ensuring comprehensive security coverage for organizations.

We caution security leaders when allowing AI to make active decisions for your team. Though AI can be a very powerful tool in helping to make decisions based on identified patterns, it is always recommended for humans to make the final call in whether certain activities should be blocked.



Compliance vs. Value Creation

While regulatory compliance is essential, security leaders must prioritize value creation and business enablement over a mere compliance checkbox. By aligning security initiatives with business objectives and demonstrating tangible value to stakeholders, information security becomes a strategic enabler rather than a regulatory burden.

Organizations that prioritize data protection and risk management gain a competitive edge in the marketplace and foster trust among customers and partners. In the financial industry, organizations who choose data protection and risk management over compliance always take the lead.

Conclusion

Financial Services organizations are typically on the leading edge of security due to compliance reasons and the inherent trust that is required to be in business. Leaders in this industry often have security thought leaders who are doubling down on the idea of API security – the new frontier of cybersecurity.

As technology continues to evolve and interconnectedness becomes the norm, we can say with certainty that APIs are here to stay. Having an API security program will put you in the driver's seat as security teams tackle the ever-evolving challenge of cybersecurity. By addressing the core aspects of an API security program: Discovery & Inventory, API Security Posture Management, and Runtime Protection, organizations can safeguard their APIs against a wide range of threats and vulnerabilities. As a result, teams are proactively reducing the business risk that comes with improving user accessibility and continued innovation.

About Data Theorem

Data Theorem is a SaaS-based solution for modern application security (CNAPP). Our cloud-based technology analyzes

- APIs (RESTful, SOAP, GraphQL, gRPC)
- Mobile Applications (iOS & Android)
- Web Applications (Web 2.0 & Single-Page WebApps)
- and Cloud (CSPM, IAM, CIEM, KSPM, & Serverless)

on a continuous basis in search of security flaws & data privacy gaps. By combining our extensive experience in information security/privacy with cloud-enabled scaling, we are able to provide customers a 365-day continuous security service for all layer-7 assets.

Founded in 2013 in the heart of Silicon Valley, Data Theorem is headquartered in Palo Alto, CA with offices in New York and Paris.

For more information, please visit us at https://www.datatheorem.com