API Fortress: Next-Gen Secure Integration

A Project Overview & Lessons Learned

Business Need

- Growing adoption of Service Oriented Architectures (SOA) and Microservices.
- Heavy reliance on APIs for communication and integration.

Challenges:

- Lack of standardization
- Inconsistent governance
- Vulnerable service security controls

Project Overview

Objectives

- Enhance API security and efficiency for robust controls and governance.

Focus Areas

- Services authorization
- Inter-services communications
- Services traffic analysis

Implementation Tools

Uniform Services Authorization

- Styra DAS
- Permit.io
- Aserto
- Warrant

Secure Network and Access Control for Kubernetes

- Calico SaaS
- Cilium

Services Traffic Analysis and Response

- Traceable.ai
- Salt Security
- Noname Security

Project Status and Milestones

- Redesigned on January 1, 2022
- Current Status:
  - Authorization Controls: PoC/Pilot – Implementation Q1 2024
  - Inter-Service Controls: PoC – Implementation Q3 2024
  - Traffic Analysis Controls: Design/Evaluation – Implementation 2025
- Expected Full Rollout: 2025

Innovation & Approach

- Shifted services security paradigm: security as policy, segmentation & isolation, behavioral analysis.
- Decoupled: deployment without changing application code.
- Transparency: policy testing without downtime.

Measurable Business Results

- Faster Time to Market: Streamlined development process.
- Improved Compliance: Better adherence to regulations.
- Decreased Operational Overhead: Simplified policy management.
- Adoption: Reduced complexity, standardization, and decoupling lead to adoption.

Key Takeaway 1

Stakeholder Education & Involvement is Paramount

The Challenge: Change, especially in deeply technical areas like API security, can be daunting for stakeholders. Initial hesitations or resistance aren't just about a reluctance to adopt new methods. Often, it's a reflection of uncertainties, concerns about potential disruptions, or simply a lack of clarity about the benefits of the proposed changes.

The Takeaway: Investing in stakeholder education is not a mere side task; it's central to the successful transformation of API security measures. Regular design reviews, comprehensive documentation, and hands-on training sessions can demystify the new processes. When stakeholders, whether they are from development, operations, or even non-technical teams, understand the tangible benefits and the operational logic of the new system, they're more likely to become its champions. Their buy-in can significantly smoothen the transition and ensure that the new security measures are integrated seamlessly and effectively.

Key Takeaway 2

Embracing Decoupled Security Frameworks

The Challenge: Traditionally, security and application functionalities were tightly interwoven. While this might seem like a practical approach, it can lead to significant bottlenecks, especially as systems grow and evolve. Moreover, the tight coupling can make system-wide upgrades or changes a herculean task, potentially jeopardizing security in the rapidly shifting landscape of threats.

The Takeaway: Adopting a decoupled security framework can be transformative. By separating security functionalities from core application logic, businesses can achieve enhanced flexibility. This approach allows for seamless security updates without disrupting application functionalities. Moreover, it enables developers to focus on core application development without the constant need to adjust for changing security protocols.

The Team

Thomas Baltis
Vice President and Chief Information Security Officer

Maurice Schilder
Manager of Cyber Risk Management Architecture

Chad Lomax
Director of Cyber Risk Management Solutions

Eric Cardinal
Expert Cyber Risk Management Architect

Medium Multi-Part Series