

Enhancing Application Security for a Large Multinational Conglomerate

Customer Overview

This case study highlights a global multinational conglomerate with diversified businesses across industries, employing over 100,000 individuals worldwide. With operations spanning multiple sectors, the organization prioritizes innovation, scalability, and operational efficiency in its cybersecurity and application security practices.

Objective

The objective was to standardize and centralize application security practices across all enterprises within the conglomerate. The focus was to provide a unified view of security performance across business units, standardize tools and practices, and enhance security posture while improving developer productivity.

Challenges

Fragmented Security Visibility

- Security leaders had to monitor multiple dashboards for insights into various business units, consuming significant time and effort.
- Lack of centralized visibility made identifying risks and vulnerabilities cumbersome.

Inconsistent Toolsets Across Business Units

- Diverse tools and technologies used by different enterprises created knowledge gaps and inefficiencies.
- Standardizing tools was critical to improve skillsets and reduce training overhead.

Reactive Security Posture

- Security issues were often detected late in the development cycle, leading to higher costs and effort to resolve.
- There was a need to adopt a “Shift Left” approach for early detection and correction of vulnerabilities.

Complex Compliance Management

- Meeting compliance requirements across industries and geographies required significant manual effort.
- Automating compliance checks and reporting was essential to reduce audit complexity.

Developer Productivity Challenges

- Developers faced challenges in deploying secure code efficiently, with vulnerabilities often causing delays in production releases.
- A balance was needed to improve security without overloading developers.

Solution: Centralized Security Platform

Unified Security Dashboard:

- Provided a single, consolidated view of security performance across all business units.
- Allowed drill-down capabilities to analyze specific enterprises, teams, or applications.

Standardized Tools and Practices:

- Streamlined the toolsets and technologies used across the conglomerate to reduce inconsistencies.
- Improved team skillsets and reduced knowledge gaps through focused training.

Shift Left Security:

- Integrated security into the earliest stages of the SDLC, enabling developers to identify and fix vulnerabilities during development.
- Reduced late-stage vulnerability remediation costs.

Secure Application Deployment:

- Implemented processes to ensure vulnerable deployments were blocked, enhancing the overall security posture.
- Simplified the developer experience by automating security checks during CI/CD pipelines.

Compliance Automation and Reporting:

- Automated compliance checks for industry-specific and regulatory standards.
- Simplified audit preparation through on-demand compliance reports.

Results

Centralized Visibility:

- Security leaders gained a unified view of risk and posture across all enterprises within the conglomerate.
- Reduced the need to log into multiple dashboards, saving an estimated 500+ hours annually.

Improved Efficiency:

- Standardizing tools across business units led to a 30% reduction in tool-related training costs.
- Increased productivity of both security and development teams by streamlining workflows.

Enhanced Security Posture:

- Shift Left practices reduced late-stage vulnerabilities by 40%, significantly lowering remediation costs.
- Vulnerable deployments were reduced by 30%, ensuring safer production environments.


Developer Productivity Gains:

- Automation and early vulnerability detection improved developer productivity by 20%, enabling faster deployment cycles.
- Reduced security bottlenecks during the CI/CD pipeline.

Simplified Compliance Management:

- Automated compliance reporting reduced audit preparation time by 50%.
- Ensured adherence to industry-specific standards across all business units.

Net Annual ROI:

 **Savings:** \$2.3M/year.

 **Investment:** \$200,000/year.

 **ROI:** 10x within the first year, with consistent improvements in subsequent years.

Conclusion

By adopting a centralized security platform, the conglomerate achieved significant improvements in its application security posture, operational efficiency, and developer productivity. The solution provided unified visibility, standardized practices, and automated compliance, ensuring that the organization remains secure and agile in an increasingly complex threat landscape.

ABOUT US

OpsMx secures and intelligently automates software delivery from developer to deployment, building on an Open Software Delivery architecture and AI/ML-powered DevSecOps. OpsMx products and services enable hundreds of thousands of developers at Google, Cisco, Western Union, and other leading global enterprises to ship better software faster.

FOR MORE INFORMATION, CONTACT US:

OPSMX, INC | 350 OAKMEAD PKWY, SUNNYVALE, CA 94085 | INFO@OPSMX.COM

[WWW.OPSMX.COM/SECURE SOFTWARE DELIVERY](http://WWW.OPSMX.COM/SECURE_SOFTWARE_DELIVERY)