

Stop Vulnerabilities from Reaching the Production Environment, Accelerate Compliance Certification Process for a Health-Tech Enterprise

Customer Overview

A fast-growing health tech startup focused on providing innovative solutions for healthcare providers and patients. Operating in a highly regulated industry, the company is dedicated to ensuring data privacy and security while meeting stringent compliance standards such as ISO 27001, SOC2, and HIPAA certifications. The company operates on the GCP cloud platform and has a hybrid application environment, including both VM-based and containerized microservices (Kubernetes), but it lacks a formal DevSecOps process.

Challenges

Regulatory Compliance:

The company needs to comply with critical certifications (ISO 27001, SOC2, HIPAA) which require a robust security framework to protect Personally Identifiable Information (PII) and Protected Health Information (PHI).

Security Automation:

The company requires automation for security controls like Static Application Security Testing (SAST), secret scanning, and building artifact security to prevent exposure of sensitive data. Manual security checks are too time-consuming, and workflow automation is necessary.

Vulnerability Management:

The company needs a system to trace and manage zero-day vulnerabilities and isolate issues as they arise in production environments.

Audit and Reporting:

Generating automated audit reports for compliance and tracking security posture in real-time is essential for maintaining regulatory readiness and reducing manual reporting overhead.

Lack of DevSecOps Practices:

The company lacks a formal DevSecOps pipeline, which means security is not integrated early in the development lifecycle. Without this integration, security vulnerabilities are discovered too late, increasing remediation costs.

Solution: OpsMx Secure Software Delivery Platform





OpsMx provided a comprehensive DevSecOps solution to address all of the company's requirements:

Automated Security Controls:



Integrated SAST, secrets scanning, and build artifact security into the CI/CD pipeline, ensuring sensitive patient and doctor information was protected from exposure through code.

Actionable Intelligence for Vulnerability Management:

The platform provided real-time insights and actionable intelligence, categorizing vulnerabilities by risk level (low, medium, high) and provide remediation suggestions to the development team.


-  **Zero-Day Vulnerability Management:**
Enabled the detection and isolation of zero-day vulnerabilities, including the ability to trace vulnerabilities in production and take immediate action.
-  **Compliance Automation:**
Automated compliance checks for HIPAA, ISO 27001, and SOC2 requirements, simplify audit preparation and reporting through pre-built compliance templates and on-demand audit reports.
-  **Real-Time Dashboards:**
Provided real-time insights into the security posture across applications, microservices, and infrastructure through dashboards and notifications, ensuring that the security team could quickly react to emerging threats.
-  **Modular and Scalable Solution:**
The platform offered a modular approach, allowing the company to start small with essential security and compliance features and scale up as needed.


Results

-  **Regulatory Readiness:**
Compliance management became streamlined and automated, significantly reducing the time and effort needed for audit preparation and ensuring adherence to ISO 27001, SOC2, and HIPAA standards.
-  **Security Automation:**
Automation of security checks, vulnerability scanning, and remediation suggestions reduced reliance on manual interventions, speeding up the development lifecycle while maintaining high-security standards.
-  **Enhanced Developer Productivity:**
With actionable intelligence and risk categorization, developers were empowered to fix vulnerabilities earlier in the development cycle, reducing late-stage remediation costs and accelerating feature delivery.
-  **Improved Security Posture:**
The platform's real-time monitoring and dashboard alerts helped security teams identify and address vulnerabilities more effectively, enhancing the overall security posture.
-  **Efficient Vulnerability Management:**
Real-time insights allowed the engineering team to trace vulnerabilities, isolate them in production, and take action immediately, reducing potential security breaches.
-  **Cost Savings:**
By automating vulnerability management and compliance processes, the company reduced the manual effort involved, leading to significant savings in both operational costs and time spent on security activities.

Net Annual ROI:

 **Savings:** \$1.3M/year.

 **Investment:** \$50,000/year.

 **ROI: 2,500% within the first year**, with continual growth in subsequent years as security practices mature.

Conclusion

By implementing the OpsMx Secure Software Delivery Platform, the company was able to streamline its security and compliance practices, automate critical security controls, and ensure regulatory readiness for ISO 27001, SOC2, and HIPAA certifications. This enabled the company to accelerate development cycles, improve security posture, and gain actionable insights into vulnerabilities, ultimately resulting in a substantial return on investment.

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)