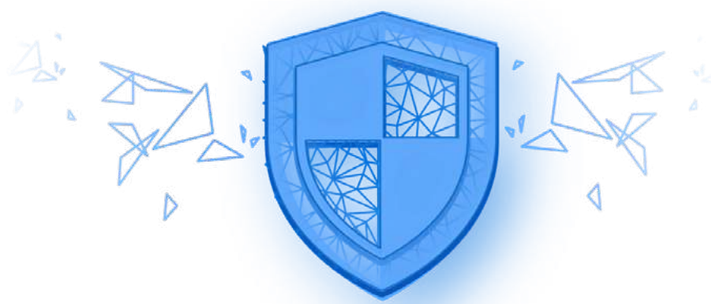
OpsMx

eBook

AppSecurity That Pays for Itself

Case Studies on Enhancing Application Security While Reducing Cybersecurity Expenses



Limitations of Current AppSec Models

Today, organizations face increased pressure to reduce costs and optimize investments while also confronting a growing list of security risks and compliance requirements. This case study book explains how leading enterprises have dealt with these challenges using OpsMx Delivery Shield. These companies have seen first-hand improved efficiency, better risk management, improved security posture, automated governance, and simplified DevSecOps all while reducing their security spending.

Who Should Read This?

This case study collection is designed for:

- **AppSec** and **DevSecOps** teams looking for automated processes to enable efficient security management while reducing costs.
- **Security** and **Compliance** leaders intending to strengthen their organization's security posture, meet various regulations, and optimize security spending.
- **Engineering** and **Platform managers** hoping to shift security left without impeding application development or increasing operational overhead.

What You'll Learn

- Efficiencies gained across industries by automating security and compliance along with cost reduction.
- First-hand experiences and recommendations from industry professionals.

Securing Cryptocurrency Transactions with DevSecOps Automation

Investment: $47,000/year

Savings: $600K/year

ROI: 6x within the first year, with consistent improvements in subsequent years as the platform continues to optimize workflows and security practices.

Customer Overview

A global crypto trading platform provides secure transactions, trading, and portfolio management services, operating under strict regulations. Their business prioritizes efficiency, security, and compliance while addressing challenges like rapid releases and scalable operations.

Objective

- Reduce operational overhead and improve collaboration among development, security, and operations teams.
- Simplify compliance management to streamline regulatory requirements.
- Enhance security posture through proactive threat detection.
- Automate vulnerability assessments to reduce manual effort.
- Achieve effortless software delivery with integrated security and compliance workflows.

Challenges

- **Time Spent on Diagnosis and Manual Effort:** Excessive time spent on diagnosing issues manually thereby reducing efficiency.
- **Security Controls Across SDLC:** Needs end-to-end security controls throughout the development lifecycle to ensure end-to-end protection.
- **Audit Report Preparation:** Compliance reporting is manual, time-consuming and thereby requires automation.
- **Shift-Left Approach:** Aims to reduce security costs by detecting vulnerabilities earlier in SDLC.
- **Hyperautomation with DevSecOps:** Wants to automate security processes and minimize manual effort by integrating DevSecOps practices.

Solution: Comprehensive DevSecOps Platform

- **Unified Security Dashboard with RBAC:** A centralized dashboard with role base access that provides end-to-end visibility of security, operations, and compliance activities.
- **Security Controls across SDLC:** Integrated security checks at each stage of the SDLC, ensuring a comprehensive security posture for every application.
- **Shift-Left Security Implementation:** Early detection and remediation of vulnerabilities in the development process before they become costly problems.
- **Automated Artifact Scans and Container Security:** Automated artifact scanning, container scanning, and DAST to enforce security controls across all applications.
- **Hyperautomation for DevSecOps:** Seamless DevSecOps workflow by automating security testing, vulnerability management, and compliance activities.

Results

- **Reduced Operational Costs:** Automation lowered manual effort, reducing security and compliance costs by 40%.
- **Faster and More Reliable Software Releases:** Automated security checks improved release velocity and reduced issues by 30%.
- **Streamlined Audit and Compliance Processes:** Automated reporting reduced audit preparation time by 70%.
- **Shift-Left Security Implementation:** Early vulnerability fixes lowered operational costs and improved efficiency.
- **Unified Visibility for Multiple Teams:** The RBAC dashboard provided real-time insights and role-based access.

Enhancing Application Security with a Centralized Security Platform

Investment: $2,00,000/year

Savings: $920K/year

ROI: 4.6x within the first year, with consistent improvements in subsequent years.

Customer Overview

A global conglomerate with diverse businesses across industries, employing over 100,000 people. Operating in multiple sectors, the organisation focuses on innovation, scalability, and efficient cybersecurity and application security practices.

Objective

- Establish centralized and standardized security practices for all applications.
- Unify security visibility across teams for better risk management.
- Improve developer productivity by integrating security early in SDLC.
- Ensure scalable, secure, and efficient operations across all business units.

Challenges

- **Fragmented Security Visibility:** Lack of centralized visibility made identifying risks and vulnerabilities cumbersome.
- **Inconsistent Toolsets Across Business Units:** Usage of diverse tools and technologies leading to inefficiencies and skill gaps.
- **Reactive Security Posture:** Security issues were often detected late in the development cycle, leading to higher costs and effort to resolve.
- **Complex Compliance Management:** Significant Manual effort in meeting compliance requirements across different geographies.
- **Developer Productivity Challenges:** Challenges in deploying secure code efficiently, with vulnerabilities often causing delays in production releases.

Solution: Centralized Security Platform

- **Unified Security Dashboard with RBAC:** Unified view across all business units with drill-down capabilities for detailed analysis by enterprise, team, or application.
- **Standardized Tools and Practices:** Streamlined security tools and technologies across the conglomerate to reduce inconsistencies.
- **Shift-Left Security Approach:** Integrated security into the earliest stages of the SDLC, to identify and fix vulnerabilities during development.
- **Secure Application Deployment:** Process Implementation to ensure vulnerable deployments were blocked, enhancing the overall security posture.
- **Compliance Automation and Reporting:** Automated compliance checks for industry-specific and regulatory standards.

Results

- **Improved Efficiency:** Standardization reduced tool-related training costs by 30%.
- **Enhanced Security Posture:** Shift-left approach reduced late-stage vulnerabilities by 40%.
- **Faster Software Releases:** CI/CD automation minimized security bottlenecks, improving developer productivity by 20%.
- **Simplified Compliance Management:** Automated compliance reduced audit preparation time by 50%.
- **High ROI:** $2.3M annual savings with a 10x ROI in the first year.

Optimizing Vulnerability Management with Automated Security & Compliance

Investment: $40K/year

Savings: $100K/year

ROI: 2.5x within the first year, with consistent improvement in subsequent years

Customer Overview

The organisation specializes in real-time data integration and streaming analytics. Its platform helps businesses harness live data for better decision-making, operational efficiency, and smooth cloud migrations. By enabling real-time data processing and distribution, the company empowers organizations to achieve data-driven results.

Objective

- Automate vulnerability detection to enhance security and efficiency.
- Streamline security workflows for faster issue resolution and tracking.
- Reduce false positives to improve accuracy in threat identification.
- Provide pre-release security assessments to prevent potential risks.
- Ensure a secure, efficient, and transparent software development process.

Challenges

- **Lack of Transparency:** Difficulty proving shipped product versions and generating detailed vulnerability audit reports.
- **High False Positives:** High number of false positives leading to increased security workload and slow vulnerability resolution times.
- **Pre-Release Risk Management:** Needed to detect vulnerabilities before release without interrupting the rapid deployment cycle.
- **Manual Tracking:** Time-consuming and inefficient vulnerability management process leading to higher costs.
- **Tracking & Closure Gaps:** Inconsistent logging, tracking and resolution of vulnerabilities leading to risk of missed security issues.

Solution: Automated Vulnerability Management

- **SAST Security Assessment:** Identifying vulnerabilities early in the development lifecycle to ensure more secure code.
- **Vulnerability Analysis and Prioritization:** Prioritization based on severity, business impact, and exploitability, allowing to focus on high-risk issues first.
- **Seamless Workflow Integration:** Automated Jira ticket generation for streamlined tracking and resolution of vulnerabilities.
- **Source Code Management and Security:** Continuous security assessments for source code management system, ensuring ongoing security throughout the development process.
- **Built-In Reporting:** Built-in reporting tools to trend and report Common Vulnerabilities and Exposures (CVEs), enabling the generation of clear, actionable audit reports.

Results

- **Improved Efficiency:** Automated workflows reduced manual tracking efforts.
- **Enhanced Security Posture:** Proactive risk detection ensured secure releases.
- **Faster Software Releases: Vulnerability detection without deployment delays.**
- **Simplified Compliance:** Accurate, transparent audit reports improved regulatory adherence.
- **Operational Cost Savings:** Reduced false positives and inefficiencies, cutting security overhead.

Strengthening Cybersecurity for Global Enterprises with Automated Security

Investment: $200K/year

Savings: $900K/year

ROI: 4.5x within the first year, with consistent returns in subsequent years

Customer Overview

A European multinational engineering and technology company with over 200,000 employees and close to 100 billion euros in annual revenue. The organization operates on a global scale and is committed to innovation and operational excellence.

Objective

- Bridge the gap between security knowledge and development practices.
- Train developers to improve cybersecurity awareness and skills.
- Automate security processes to enhance efficiency and accuracy.
- Fix vulnerabilities early in the SDLC to reduce costs.
- Enhance productivity by integrating security into development workflows.

Challenges

- **High Cost of Vulnerabilities in Production:** Missed vulnerabilities led to costly fixes, with an estimated cost of $5,000 per issue.
- **Manual Efforts in Security Assessment:** Security teams manually classified issues, causing productivity loss and communication delays.
- **Knowledge Gap Between Security and Development:** Developers lacked cybersecurity expertise, increasing the security team's workload.
- **Scalability Issues:** Installing security tools and infrastructure was time-consuming, requiring a centralized security platform.
- **Compliance Challenges:** Manual compliance checks were resource-intensive, with limited access to compliance scorecards.

Solution: Centralized Security Platform

- **On-Demand Security Coverage:** Automated scans (SAST, DAST, container, IAC, etc.) for code and cloud security.
- **AI-Driven Insights:** Integrated AI/ML for real-time vulnerability insights, automating aggregation and prioritization.
- **Automated Compliance Management:** Auto-generated compliance scorecards and policy tagging for easy identification of relevant compliance measures.
- **Developer Training & Knowledge Transfer:** Security training and tools to help address vulnerabilities during development.
- **Centralized and Scalable Platform:** Eliminated redundant tool installations and provided detailed visibility with Role-Based Access Controls (RBAC).

Results

- **Cost Savings:** Early vulnerability fixes saved $5,000 per issue, exceeding $1.3M in annual savings.
- **Productivity Gains:** Automation saved 20,000+ hours annually; developers resolved issues 30% faster.
- **Enhanced Compliance:** Automated compliance checks cut audit prep time by 40%.
- **Improved Scalability:** ecurity tools enabled cross-team scalability, reducing project timelines by 25%.
- **Strengthened Security Posture:** AI insights improved risk management and reduced exposure.

Empowering a Health Tech Innovator with Streamlined Security & DevSecOps

Investment: $50K/year

Savings: $650K/year

ROI: 13x within the first year, with continual growth in subsequent years as security practices mature.

Customer Overview

A fast-growing health tech startup committed to innovative healthcare solutions for providers and patients. Operating in a highly regulated environment, it prioritizes data privacy and security while complying with stringent certifications like ISO 27001, SOC2, and HIPAA. The company uses GCP cloud and hybrid applications but lacks a formal DevSecOps process.

Objective

- Establish a robust DevSecOps process for enhanced security.
- Ensure compliance with ISO 27001, SOC2, and HIPAA standards.
- Automate security workflows to improve efficiency and accuracy.
- Enhance overall security posture across all development stages.
- Accelerate development cycles while maintaining strong security.
- Reduce operational costs by streamlining security processes.

Challenges

- **Regulatory Compliance:** Needed to meet ISO 27001, SOC2, and HIPAA requirements to protect sensitive data like PII and PHI.
- **Security Automation:** Required automated SAST, secret scanning, and artifact security to eliminate manual effort and prevent sensitive data exposure.
- **Vulnerability Management:** Needed a system to trace and address zero-day vulnerabilities in production environments.
- **Audit and Reporting:** Lacked automated audit report generation for compliance and real-time tracking of security posture.
- **Lack of DevSecOps Practices:** Security vulnerabilities were addressed too late in the development lifecycle, increasing costs and risks.

Solution: OpsMx Secure Software Delivery Platform

- **Automated Security Controls:** Integrated SAST, secrets scanning, and build artifact security into the CI/CD pipeline.
- **Vulnerability Management:** Provided real-time insights and actionable intelligence, categorizing vulnerabilities by risk level along with remediation suggestions.
- **Zero-Day Management:** Enabled real-time detection, isolation, and tracing of zero-day vulnerabilities in production.
- **Compliance Automation:** Automated compliance checks for HIPAA, ISO 27001, and SOC2 requirements, simplified audit preparation and reporting through pre-built compliance templates.
- **Real-Time Dashboards:** Provided real-time insights into the security posture across applications, microservices, and infrastructure through dashboards and notifications.

Results

- **Regulatory Readiness:** Streamlined compliance processes, ensuring ISO 27001, SOC2, and HIPAA adherence.
- **Security Automation:** Accelerated development while maintaining high-security standards with automated workflows.
- **Improved Productivity:** Enabled developers to address vulnerabilities earlier, reducing costs and improving efficiency.
- **Enhanced Security Posture:** Dashboards and alerts ensured rapid response to threats, strengthening security overall.
- **Cost Savings:** Reduced manual effort in security and compliance processes, saving time and operational costs.

Ready to Strengthen and Reduce the Cost of Your Application Security with OpsMx?

Application security shouldn't slow you down—or drain your budget. Staying ahead of evolving threats requires **smarter security,** not just more tools. As seen in these case studies, leading organizations have eliminated inefficiencies, **reduced security costs by up to 50%,** and accelerated compliance by leveraging **OpsMx Delivery Shield.**

Why Choose OpsMx?

OpsMx delivers **cost-efficient, automated application security** by integrating risk-based vulnerability management, compliance automation, and AI-driven threat prioritization directly into your SDLC. With OpsMx, enterprises can:

- **Reduce security costs by eliminating redundant tools** and leveraging open-source integrations
- **Cut manual effort by up to 70%** with hyperautomation in SBOM generation and risk assessment
- **Accelerate vulnerability detection and remediation** to prevent costly security breaches
- **Avoid compliance penalties** with automated reporting and audit-ready documentation

Security doesn't have to be expensive—**OpsMx makes it smarter, faster, and more cost-effective.**

Let's Transform Your Security Strategy

The cybersecurity landscape is evolving—**OpsMx can help you stay ahead.** Whether your goal is **compliance, DevSecOps maturity,** or **security cost reduction,** our solutions are designed to fit your needs.

Let's talk about how OpsMx can help your organization achieve these results.
[Talk to Application Security Expert]

About OpsMx

OpsMx simplifies and accelerates comprehensive application security from developer to deployment building on AI-driven automation, open source security tools, and a deep understanding of the software delivery process. OpsMx enables tens of thousands of developers at both fast moving innovators and global enterprises to deliver more secure software faster.

For More Information, Contact Us:

OPSMX, INC | 350 OAKMEAD PKWY, SUNNYVALE, CA 94085
INFO@OPSMX.COM
WWW.OPSMX.COM/SECURE SOFTWARE DELIVERY

OpsMx