Case Study

Armis Centrix™ Enables a Salesforce DevOps Platform to Shift Into a More Proactive Application Security Management Strategy

The Challenge

- Scaling High Standards: Maintaining the rigorous security posture required for FedRAMP Moderate ATO while managing rapid growth.
- Operational Noise: High-fidelity security controls generated a volume of alerts that required more efficient triaging to maintain developer velocity.
- Evolving Threat Landscapes: Proactively managing the security implications of AI-generated code at scale.
- Orchestrating Visibility: Integrating visibility across a complex multi-cloud environment (AWS and GCP GovCloud) into a single, unified source of truth.
- Optimizing Remediation: Moving from manual tracking to automated, risk-based prioritization to consistently exceed SLAs.

The Solution

- Deployed Armis Centrix™ for Application Security as part of a comprehensive Continuous Exposure Management (CEM) program
- Configured Armis Centrix™ for VIPR Pro - Prioritization and Remediation to deduplicate, contextualize, prioritize and mitigate risk and exposures
- Identified security champions within each department
- Sorted and assigned assets to specific owners

The Results

- Prevented scalable risk exposure by detecting vulnerabilities in application code before production
- Aligned security alerts with the right teams, reducing friction and shortening remediation time
- Cut alert noise by up to 70%, boosting developer productivity and focus
- Shifted to a platform security strategy focused on Infrastructure-as-Code (IaC) hardening
- Gained contextual visibility into applications so they are seen as part of a holistic attack surface
- Instituted risk benchmarking to help clear 17,000 vulnerabilities in one month
- Reduced the average remediation time to seven days

Industry: Software

Location: Chicago, Illinois

Size: 490

Armis Centrix™ for Application Security

Armis Centrix™ for VIPR Pro - Prioritization and Remediation

Background

Copado, headquartered in Chicago, Illinois, is an enterprise software company providing a comprehensive end-to-end DevOps platform that streamlines application coding, testing, and deployment for the Salesforce cloud. Its platform, Copado Org Intelligence™, maps every dependency, relationship, and hidden risk to give organizations the ability to deploy new code with confidence and speed. Copado operates globally in North America, Europe, and Japan, with a workforce of 490 people.

Security Applications Lead Engineer Robert Roldan Notario is responsible for driving the strategy and implementation of security controls across the software development lifecycle, ensuring applications are secure from design to deployment. Part of that responsibility includes ensuring that Copado meets its service level agreements (SLAs) to customers.

"While our previous security stack provided broad coverage, it lacked the cross-layer context needed for high-speed triage. Armis Centrix™ allows us to contextualize code-level bugs with infrastructure reality, enabling us to focus our elite engineering talent on the risks that actually matter."

Robert Roldan Notario,
Security Applications Lead Engineer, Copado

The Challenge

Copado operates a sophisticated, multi-cloud environment spanning AWS and GCP, designed to meet the highest industry standards. Having already achieved FedRAMP Moderate ATO, the team had established a robust security foundation. However, as the organization scaled, the challenge shifted from establishing security to optimizing operational efficiency. The legacy security stack, while effective at identifying risks, consisted of siloed point solutions. As the environment grew, these tools generated thousands of alerts daily. While these reflected a high-coverage security net, the volume of data created "noise" that made it labor-intensive to isolate the most critical risks. The goal wasn't to find security—it was to streamline it.

As Copado embraced AI-driven development, the sheer speed of code generation introduced a new scale of vulnerabilities. Even with an ATO in place, the security team found themselves spending excessive time manually correlating data across environments, including AWS and GCP GovCloud.

Before integrating Armis, prioritization was often driven by the volume of findings rather than a unified, context-aware risk score. To maintain their commitment to customer SLAs and regulatory frameworks, Copado sought a way to move beyond manual tracking. They needed a "single pane of glass" to transform their existing high-security standards into a proactive, automated, and sustainable risk-management engine.

"Maintaining a FedRAMP-standard security posture across a modern attack surface requires deep integration, not just more tools. Armis Centrix™'s ability to categorize risk across cloud, code, and container surfaces in a single view was the catalyst we needed to move from siloed security to a unified orchestration strategy."

Robert Roldan Notario,
Security Applications Lead Engineer, Copado

The Solution

To build upon their FedRAMP-certified foundation, Copado implemented Armis Centrix™ for Application Security and Armis Centrix™ for VIPR Pro - Prioritization and Remediation. Rather than just adding another layer of software, we used this as an opportunity to push security ownership back to the squads, making high-standard risk management part of our daily workflow.

Central to this strategy was the appointment of Security Champions within Copado's engineering squads. By assigning clear ownership and accountability, Copado shifted security "left," ensuring that risk management became a core part of the development lifecycle rather than a final hurdle. Notario's vision was clear: "We moved from fragmented, cloud-specific views to a unified, 360-degree visibility of our entire application estate, including our most sensitive GovCloud environments."

The deployment followed a structured, departmental rollout across Copado's five core groups. A critical phase of the implementation focused on intelligent noise reduction. By leveraging Armis Centrix™ to automatically filter false positives—specifically for internal or deprecated tools—Copado restored the engineering team's trust in security data. This allowed developers to focus exclusively on high-impact, verified risks, significantly improving the Mean Time to Remediation (MTTR).

Today, Armis Centrix™ acts as the "source of truth" for Copado's application code, while Armis Centrix™ for VIPR Pro - Prioritization and Remediation module enables proactive SLA governance. Security leaders now distribute high-fidelity reports directly to Security Champions, fostering a culture of continuous risk management and compliance enforcement.

17,000

findings remediated in a 30-day window

40,000%

increase in remediation progress

7-day

average remediation time across the enterprise

To ensure the long-term success of this ecosystem, Copado has dedicated two specialized team members to lead the Armis integration, working in close partnership with the Armis team to continually refine their security posture.

By implementing Armis as a unified orchestration layer, Copado has transformed its FedRAMP-certified foundation into a high-velocity security engine. The most significant outcome has been the shift from manual oversight to automated, context-aware governance, allowing the team to maintain its rigorous security posture at the speed of modern DevOps.

The transition to a Continuous Threat Exposure Management (CTEM) lifecycle yielded immediate, record-breaking results. By automating the prioritization of high-fidelity risks, Copado achieved:

40,000% Increase in Remediation Throughput: The team cleared a significant volume of vulnerabilities in just the first month.

Rapid MTTR: Average remediation time dropped to just seven days, comfortably exceeding customer and regulatory SLAs.

Elimination of Manual Toil: The security team reclaimed hundreds of hours previously spent on manual spreadsheet reconciliation, pivoting that energy toward strategic architecture and framework design.

The visibility provided by Armis Centrix™ enabled a strategic shift toward a Platform Security strategy. By hardening Infrastructure-as-Code (IaC), security policies are now embedded directly into the CI/CD pipeline. This “secure-by-design” approach ensures that misconfigurations in storage (such as unencrypted buckets) or sensitive credential exposures are identified and blocked before they ever reach production.

With a “single pane of glass” view across AWS and GCP GovCloud, the “fire-drill” culture has been replaced by a proactive, data-driven program. “Armis’s ability to categorize risk across cloud, code, and host surfaces in one view was a major shift,” Notario explained. “By providing the high-fidelity value that siloed tools lacked, Armis has become our primary platform for orchestration.”

Today, Copado’s security department is viewed not as a bottleneck, but as a business accelerator. Leadership now has the real-time metrics and confidence needed to scale new AI initiatives and cloud expansions, knowing their security posture is both elite and infinitely scalable.