seemplicity

Unified Application Security Posture Management

Integrated, end-to-end visibility and management of application risks with the Seemplicity Remediation Operations platform.

SOLUTION BRIEF

60%

Reduction In Mean Time To Respond (MTTR)

80%

Decrease in Manual Operations

75%

Increase in SLA Compliance

Trusted by

SoFi · fiverr. · Graphic Packaging International · OpenWeb · Paramount · NTT · Carlsberg Group

Centralized Visibility & Management of Application Risk

As organizations rapidly adopt DevOps, CI/CD, and cloud-native environments, application security grows increasingly complex. Prioritizing vulnerabilities, consolidating fragmented data, and orchestrating remediation across teams and the software development lifecycle (SDLC) requires advanced solutions.

The Seemplicity platform simplifies ASPM, providing seamless, end-to-end visibility and management of remediation across the SDLC. By consolidating and correlating findings from disparate tools into actionable, prioritized remediation plans, the platform empowers organizations to proactively reduce risk, drive operational efficiency, and achieve stronger governance.

Key Business Challenges for Security Teams

Fragmented Tooling and Data Silos

Disconnected tools limit end-to-end visibility, creating inefficiencies and impeding collaboration across development, security, and operations teams.

Overwhelming Security Noise

Although adding multiple application security testing tools into the DevSecOps pipeline is best practice, high volumes of uncorrelated findings make it challenging to prioritize and address critical vulnerabilities.

Manual Processes and Complexity

Manual, ad-hoc triage and remediation processes are too error-prone and time consuming to keep up with application vulnerabilities in modern development environments.

How the Seemplicity Platform Helps

Accelerate Risk Reduction

The Seemplicity platform consolidates, normalizes, and enriches findings from security tools with additional context using AI-powered correlation and scoring. This allows teams to prioritize critical vulnerabilities and automate workflows across their existing ticketing systems such as Jira and GitHub.

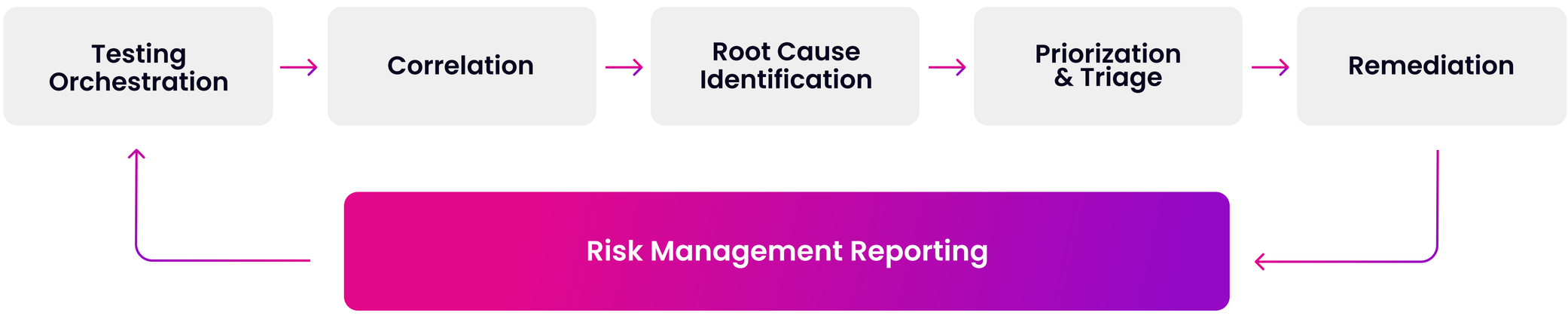
Context-Driven Automation

The platform dynamically updates remediation priorities by continuously ingesting findings and enriching them with contextual data. This ensures effective collaboration and compliance across security, development, and operations teams while enabling faster, more precise action on risks.

Build Scalable and Reliable Processes

Seemplicity eliminates error-prone, manual workflows with customizable no-code automation. Triage is done efficiently and remediation tasks are routed with precision, for consistent, scalable remediation that aligns with organizational objectives without disrupting development timelines.

Application Security Posture Management (ASPM)



ASPM is the continuous process of evaluating and remediating vulnerabilities from development to production. The Seemplicity Remediation Operations platform facilitates and optimizes this process by correlating findings across security testing tools to actionable remediation that can be executed at scale. The Seemplicity platform's robust reporting capabilities help teams fuel process improvements, SLA compliance, and more.

Business Benefits Achieved with the Seemplicity Platform

FASTER RISK REDUCTION

Automate workflows, streamline prioritization, and address vulnerabilities more quickly. Centralizing findings into actionable fixes reduces time-to-remediate and improves overall security outcomes.

MAXIMIZE OPERATIONAL EFFICIENCY

Integrate with existing application security testing tools (SAST, DAST, SCA, etc.) and ticketing systems to transform raw data into actionable insights. This enhances collaboration and optimizes the value of your existing tech stack.

KEY CAPABILITIES

How the Seemplicity Platform Transforms Your Application Security Posture

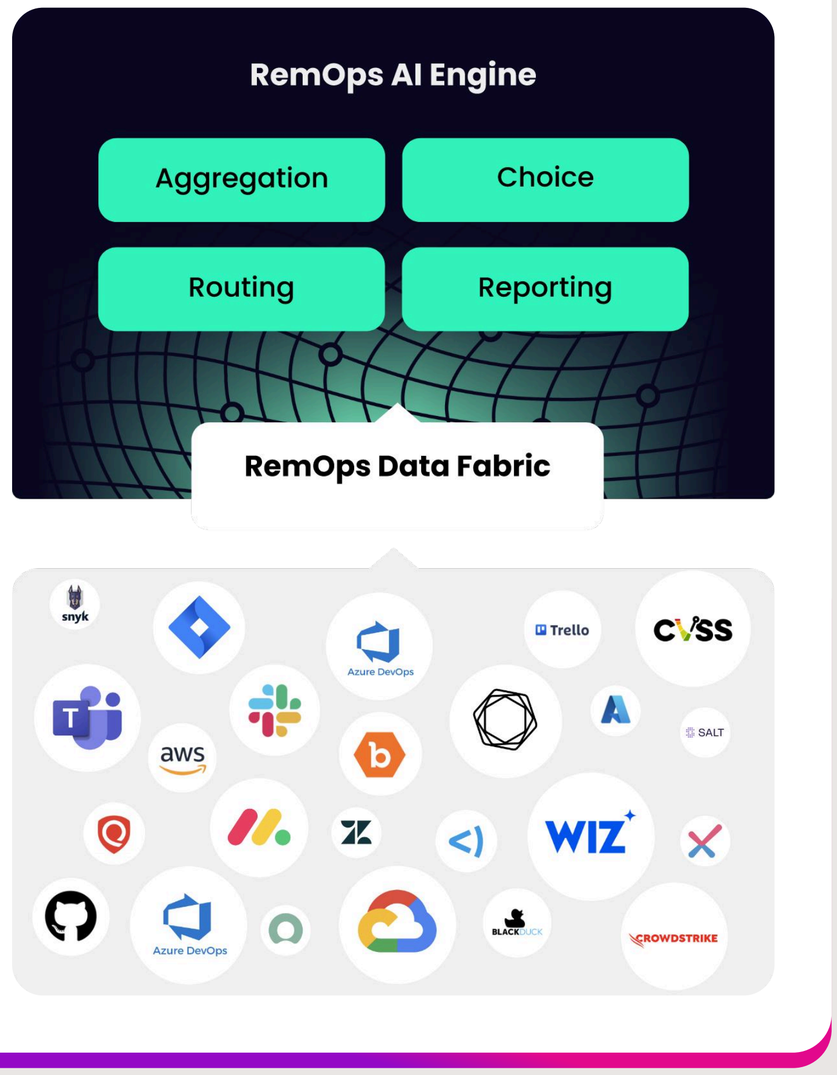
The Seemplicity platform is designed to fit into every step of your SDLC to help you proactively spot and remediate vulnerabilities before they become incidents.

SEEMPLICITY REMOPS AI ENGINE

The Seemplicity RemOps AI Engine combines AI, machine learning (ML), and large language models (LLMs) to analyze vulnerabilities, identify root causes, and prioritize risks. It helps teams focus on the most critical issues and provides clear, actionable guidance to streamline remediation efforts.

SEEMPLICITY REMOPS DATA FABRIC

By normalizing and consolidating findings across application security, infrastructure as code (IaC), and cloud platform testing tools, the Seemplicity RemOps Data Fabric creates a centralized, context-rich view of application security. This unified backlog empowers teams to make informed decisions and address vulnerabilities efficiently.



TAILORED REMEDIATION PLANS

Custom remediation plans prioritize tasks by identifying who needs to act, what to address, and how to resolve issues. These plans dynamically align with team workflows, ensuring targeted and efficient remediation.

SLA TRACKING AND MANAGEMENT

Monitor critical metrics, such as open vs. closed findings, SLA compliance, and ticket status across teams. Real-time tracking supports streamlined governance and ensures adherence to compliance standards.

NO-CODE REMEDIATION WORKFLOWS

Automates the management of remediation processes with customizable, no-code workflows that adapt to your organization's requirements. These workflows eliminate complexity, accelerate task execution, and support scalable operations.

BI-DIRECTIONAL COLLABORATION

Integrates seamlessly with popular ticketing systems like GitHub and Jira, enabling real-time synchronization and effortless collaboration. Teams can update tickets, add notes, and track progress directly within their preferred tools, ensuring smooth task transitions, cross-functional alignment, and efficient workflows.

VALIDATE REMEDIATION TEAM FIXES

Confirm remediation effectiveness with retesting of vulnerabilities, boosting confidence that risks are fully resolved. This process reinforces the application's security posture and reduces manual overhead.

REMEDIATION WORKFLOW ORCHESTRATION AND PROCESS COMPLIANCE

Automates and streamlines workflows throughout the SDLC, ensuring consistent execution and alignment with organizational policies. Customizable tracking and reporting provide real-time insights into SLA performance, process adherence, and risk reduction progress.

Improve Your Application Security with the Seemplicity Platform

VISIT SITE

Seemplicity simplifies ASPM by integrating unified visibility, intelligent automation, and actionable insights into a single platform. The result is faster remediation, enhanced governance, and seamless collaboration across the SDLC.

Discover how Seemplicity can transform your application security posture and help you effectively reduce risk at your organization.

Visit **seemplicity.io** to learn more.