

Accelerate Risk Reduction with the Seemplicity Remediation Operations Platform

Increase effectiveness, efficiency,
speed, and throughput

60%

REDUCED MEAN TIME TO
REMEDiation (MTTR)

80%

DECREASE IN MANUAL
OPERATIONS

75%

INCREASE IN SLA
COMPLIANCE

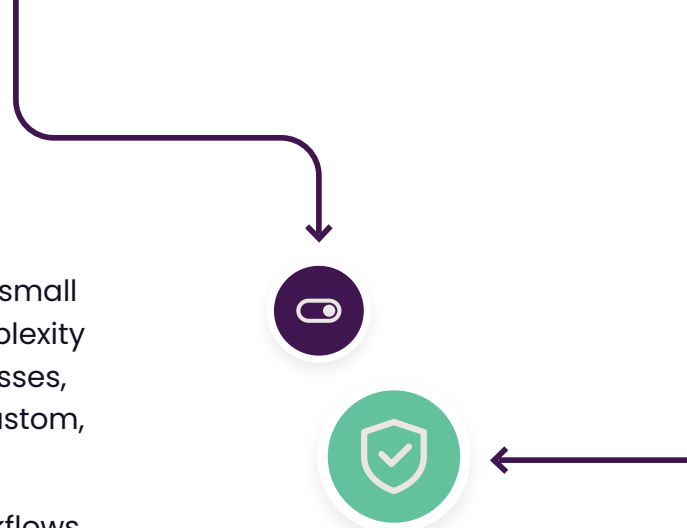
Trusted Around the Globe



How Seemplicity Tackles Gaps in the Remediation Process

Scalable, efficient risk and vulnerability remediation is no small feat – especially with the level of connectivity and IT complexity that digital transformation has introduced. Manual processes, spreadsheets and siloed information do not scale, and custom, home-grown solutions are too difficult to maintain.

Seemplicity's single, unified backlog and automated workflows accelerate the flow of information across teams, tools, domains, and processes in an efficient and impactful way.



Business Challenges for Security Teams

✘ Unmanageable Volume of Findings

Having multiple, disparate security testing tools and risk reporting workflows across thousands of IT assets can generate an overwhelming volume of findings.

✘ Process Scalability Challenges

Manual coordination and orchestration of findings-to-remediation teams causes unaddressed risk to accumulate, lowers morale and productivity, and leaves organizations open to threats and non-compliance. These problems are compounded by disparate security testing tools creating a fragmented view of risk, resulting in critical lapses in visibility.

✘ Tension, Fatigue & Inefficiency

A growing, evolving attack surface combined with the volume and velocity of findings as well as ad hoc processes can create confusion and fatigue that further slows remediation and security teams down as they try to reduce risk in a timely manner.

How Seemplicity's RemOps Solution Helps

✔ Accelerate Risk Reduction

Seemplicity aggregates, normalizes, deduplicates, and centralizes findings across technology layers and looks for common fixes so remediation teams can reduce risk at scale in bulk. End-to-end no-code workflows automatically open, adjust, and validate ticketing status – all using the work management software that these teams already use.

✔ Ensure Process Confidence & Compliance

Seemplicity empowers organizations to achieve consistent, quality results by continuously validating remediation effectiveness, enriching findings with risk (e.g., CISA-KEV and EPSS) and business context, and reporting on SLA compliance.

✔ Maximize Fixing Team Engagement, Productivity, & Morale

Seemplicity's Remediation Queues buffer the backlog based on team bandwidth and finding type, and are automatically updated as their relevance changes. Efficiency and process confidence further keep fixing teams engaged.

Business Benefits of Using Seemplicity

Accelerated Mean Time to Remediation (MTTR)

Seemplicity boosts your MTTR by 60% and eliminates time sinks and manual labor by automating the logistical parts of the remediation cycle and encouraging a flow of consolidated, consumable information.

Streamlined Risk Reduction

Seemplicity transforms lists of unorganized output from automated security testing tools into actionable tasks to eliminate ineffective, manual remediation process management and maximize efficiency.

Improved Team Morale

The risk of burnout and fatigue for security and remediation teams is high. Seemplicity reduces the costs associated with hiring and retaining cyber talent, a function that experiences around 20% turnover, by reducing the noise created by vulnerability scanners and chaotic processes, enabling efficiency, agility, and productivity throughout the risk remediation process.

How Seemplicity Transforms Your Remediation Efforts

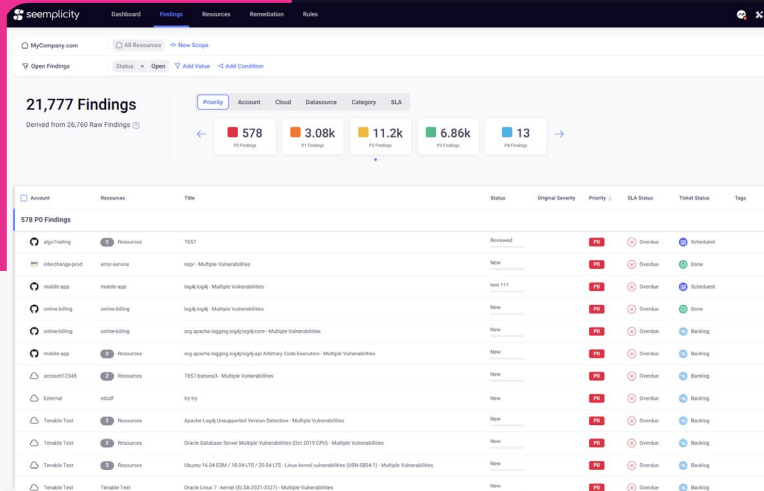
The Seemplicity platform is designed to fit into every step of your existing remediation process with intuitive yet innovative features.

Consolidated, Cross-Domain Backlog

Seemplicity connects with the tools you already have and provides users with a singular, consolidated, yet complete view of risk that allows teams to make consistent and efficient progress towards their remediation goals.

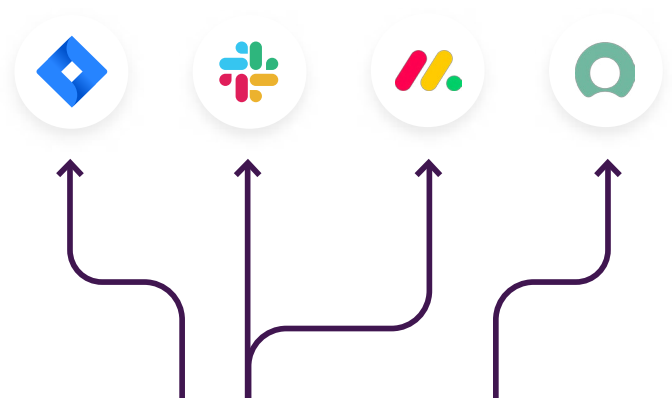
Seemplicity Remediation Choice Engine™

The Seemplicity Remediation Choice Engine™ enables efficiency by helping teams prioritize findings, identify remediation owners, define where remediation will be applied, and the guidance for how to remediate a vulnerability.



Seemplicity Intelligent Remediation Router

Seemplicity learns and locates the appropriate remediation owners in their native platforms by leveraging intelligent metadata correlations and resource integrations, even without a CMDB.

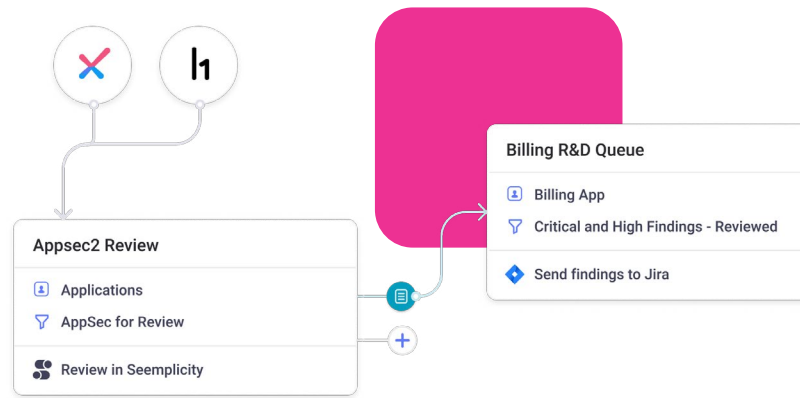


Bi-Directional and Multi-Fixer Queue Management

Bi-directional ticketing and real-time synchronization allow fixing teams to receive and respond to tickets in their native work management systems without security team coordination, making cross-functional collaboration easy. Fixers can accept, make notes, re-route, or reject requests, and security can track progress directly from Seemplicity.

SLA Tracker and Manager

Track and manage remediation performance metrics like open vs. closed findings, SLA compliance, and ticket status per team.

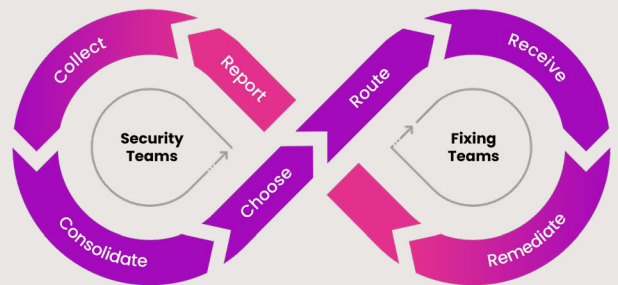


No-Code Workflow Remediation

Choose from out-of-the-box or custom automated workflows that segment backlogs into remediation queues and allow fixing teams to define severity and route vulnerability actions based on priority, ticket owners, and validation.

RemOps: Do More with Less

Remediation Operations (RemOps) is the collection of cybersecurity business processes that minimize risk by mobilizing the right teams with the data and context they need to eliminate, reduce, or accept risk findings. Seemplicity delivers cost savings in multiple areas that easily offset the investment, and you will be able to scale risk reduction far beyond its existing boundaries.



Cost savings include:



Time Returned to Security & Fixing Teams

Reduced time on manual processes



Process Compliance Cost Savings

Cost savings of automated tracking & reporting



Leverage on Security Investments

Improved ROI of existing scanner & testing tools



Increased Developer Value Delivery

Developer time returned



Accelerated Pace of Risk Reduction

Fewer incidents & associated IR costs

Where to Get Budget



SOC Modernization

Many organizations are reconsidering their entire SOC and logging architecture to support a more proactive approach. Seemplicity enables a reduction in events going to your SOC team by creating a workflow designed to maximize efficiency and remediation actions.

Vulnerability Management

Most organizations have multiple vulnerability scanners, but correlating and routing findings can waste time and resources. Seemplicity maximizes the ROI of existing vulnerability scanners and security tooling.

DevOps

Application code scanners also generate untenable volumes of findings and scattered vulnerability data, expanding the backlog even further. By centralizing findings across technology layers and creating an actionable plan, Seemplicity breaks silos and eliminates duplicate work.

**to get a tailored ROI, ask about our business justification model*

Getting Started with Seemplicity

Seemplicity is remediation, simplified. By enabling smooth integration, cross-team collaboration, and scalability, Seemplicity yields unmatched cost savings and risk reduction for any organization.

Visit seemplicity.io to learn more about transforming the way your organization handles risk.

