

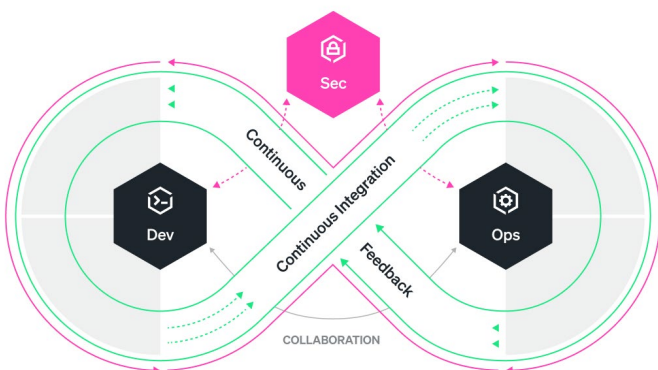
New Relic Interactive Application Security Testing (IAST)

Accurate, fast IAST. Ship code faster with unmatched detection accuracy of security risks.

Today's application security testing practices are inaccurate and disjointed, resulting in false positives, missed release cycles, and increased security costs. To build more secure applications DevOps teams need a solution that provides complete visibility across the application lifecycle, eliminates false positives, and makes it easy to detect and fix real security risks.

New Relic IAST goes beyond current approaches, providing visibility and context to security findings, unmatched detection accuracy, and proof of exploit via dynamic assessment capabilities that pinpoint the source of vulnerabilities by simulating real-world attacks—with guided remediation for faster resolution. In addition, New Relic IAST is fully integrated with New Relic Vulnerability Management, enabling DevOps teams to continuously find, fix, and verify high-risk vulnerabilities across the software developer lifecycle (SDLC).

As part of the New Relic observability platform, New Relic IAST enables DevOps and security teams to accurately and continuously monitor, test, and remediate security risks across the SDLC at scale, and ship code faster.



BENEFITS

See everything and eliminate blind spots

Gain visibility into the entire application stack and associated relationships with context-driven insights to eliminate blind spots, and validate the status of remediation efforts.

Enhance security testing accuracy

Eliminate false positives with fast, accurate detection, risk-based prioritization, and automated vulnerability validation.

Focus on what matters with proof-based exploit validation

Find, fix, and verify exploitable vulnerabilities for faster remediation with dynamic assessment capabilities that eliminate the need for code changes.

Accelerate remediation efforts

Guided remediation and guardrails enable developers to avoid critical mistakes by pinpointing code location, stack trace, HTTP trace, encountered URLs, and exploit mechanism and parameters, and more.

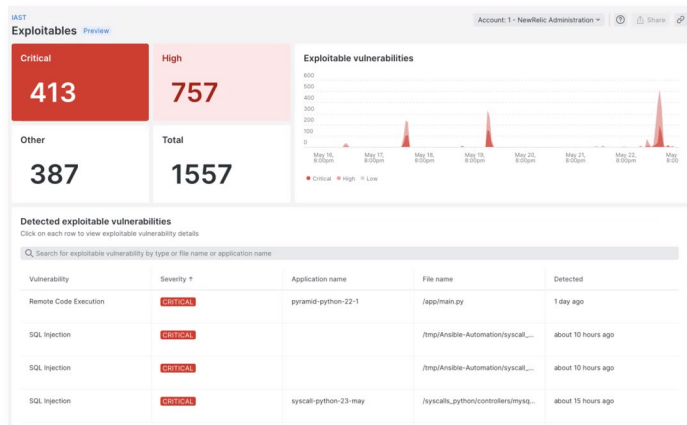
Scale at will

Easy deployment via existing APM agent and seamless integration with CI/CD pipelines and ticketing systems helps prevent disruption of existing processes and workflows.

CAPABILITIES

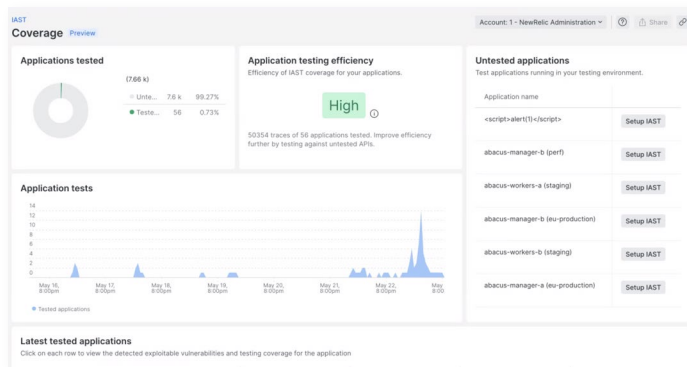
Gain visibility into the entire application stack

See all protected and unprotected applications to eliminate blind spots and pinpoint hidden threats, and continuously monitor and validate the status of remediation efforts to ensure applications are always protected.



Pinpoint exactly where vulnerabilities exist in real time with near zero false positives

Identify vulnerabilities across all layers of the application stack and reduce false positives with fast, accurate detection, enabling developers to focus on real security threats with risk-prioritized vulnerability lists for faster remediation.

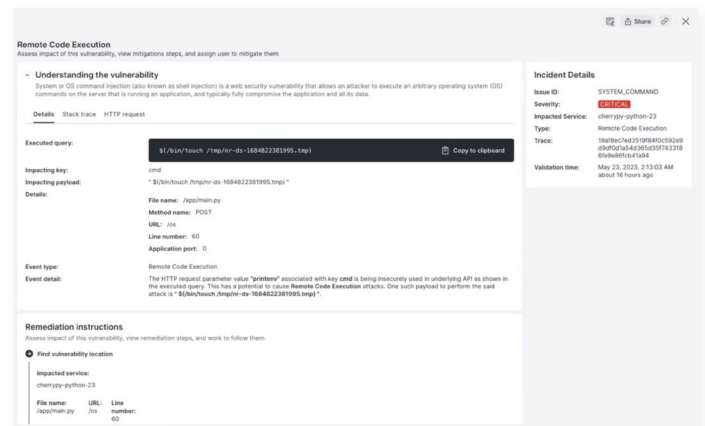


Next Steps:

[Read More](#) | [Get Started](#) | [Contact Us](#)

Identify vulnerabilities with proof of exploit

Save time with dynamic assessment capabilities that identify the source of vulnerabilities by simulating real-world attacks. Then validate them with proof of exploit so that developers can focus on verified vulnerabilities and ship more secure code.



Guided remediation for fast, effective elimination of security risks

Automatically prioritize software flaws like SQL injection, command execution, and other OWASP Top 10 standards, and then eliminate them before they can be exploited. With guided remediation and guardrails from New Relic experts, developers can avoid critical mistakes that could lead to a potential security incident.

