new relic

DATASHEET

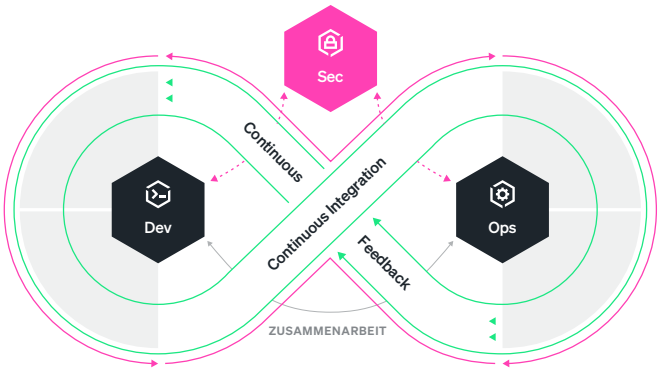
# New Relic Interactive Application Security Testing (IAST)

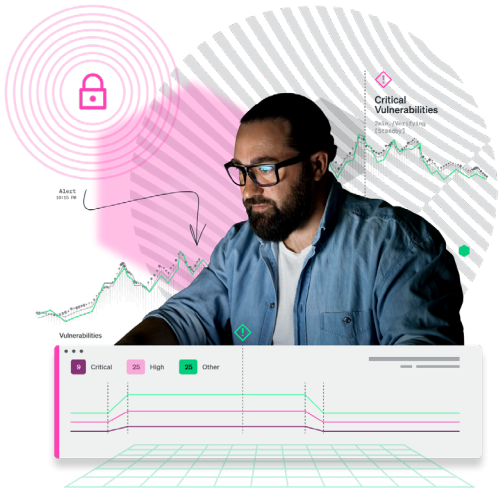
## Schnellere Codebereitstellung mit unübertroffener Genauigkeit bei der Erkennung von Sicherheitsrisiken.

Aktuelle Methoden zum Testen der Anwendungssicherheit sind ungenau und lückenhaft. Das führt zu falsch-positiven Ergebnissen, verpassten Release-Zyklen und erhöhten Sicherheitskosten. Um sicherere Anwendungen zu entwickeln, brauchen DevOps-Teams eine Lösung, die vollständige Transparenz über den gesamten Lifecycle bietet, falsch-positive Meldungen minimiert und die Erkennung sowie Behebung echter Sicherheitsrisiken erleichtert.

New Relic IAST geht über die heute üblichen Ansätze hinaus: Es ergänzt Sicherheitsdaten um Echtzeittransparenz und Kontext und bietet eine unübertroffene Erkennungsgenauigkeit sowie Proof-of-Exploit über dynamische Bewertungsfunktionen, die Angriffe simulieren, um die Ursachen von Schwachstellen punktgenau zu ermitteln – mit geführter Problembehebung für eine schnellere Lösung. Darüber hinaus ist New Relic IAST vollständig in New Relic Vulnerability Management integriert, damit DevOps-Teams gefährliche Schwachstellen während des gesamten Lebenszyklus der Softwareentwicklung (SDLC) fortlaufend erkennen, beheben und überprüfen können.

Als Teil der New Relic Observability-Plattform ermöglicht New Relic IAST es DevOps- und Sicherheitsteams, Sicherheitsrisiken über den gesamten SDLC hinweg genau und kontinuierlich zu überwachen, zu testen und zu beheben – und Code schneller bereitzustellen.




VORTEILE

### Klare Sicht statt blinder Flecken

Kontextbezogene Einblicke geben Ihnen vollen Überblick über den Anwendungsstack und die damit verbundenen Beziehungen. So gibt es keine blinden Flecken mehr und Sie können Abhilfemaßnahmen zuverlässig validieren.

### Mehr Genauigkeit bei Sicherheitstests

Eliminieren Sie falsch-positive Meldungen durch rasche, akkurate Erkennung, risikobasierte Priorisierung und automatische Validierung von Schwachstellen.

### Fokus auf Schwachstellen, die verifiziert und als ausnutzbar erkannt wurden

Finden, beheben und verifizieren Sie ausnutzbare Schwachstellen mithilfe dynamischer Bewertungsfunktionen, um Probleme schneller aus dem Weg zu räumen und keine Code-Änderungen mehr durchführen zu müssen.

### Schnellere Problembehebung

Geführte Abhilfemaßnahmen und integrierte Schutzvorrichtungen helfen DevOps-Teams, kritische Fehler zu vermeiden, indem sie die Position im Code, den Stack-Trace, den HTTP-Trace, die gefundenen URLs sowie Exploit-Mechanismen und -Parameter und vieles mehr aufzeigen.

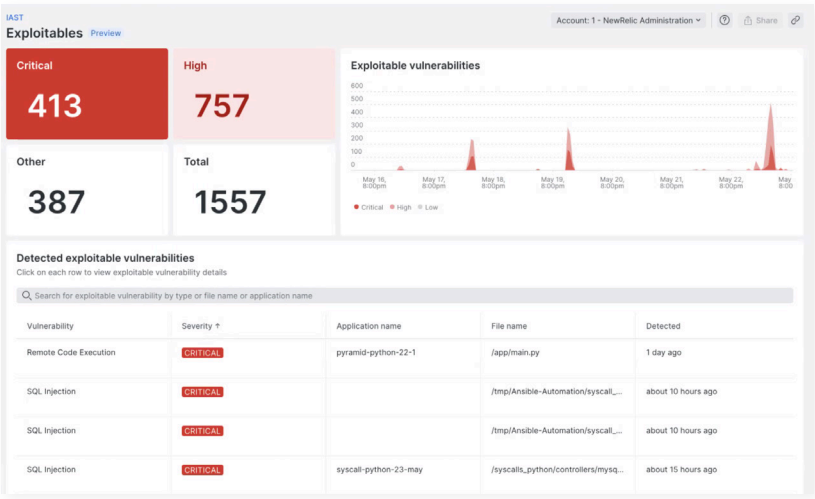
### Beliebig skalierbar

Die einfache Bereitstellung über einen vorhandenen APM-Agent und die nahtlose Integration in CI/CD-Pipelines (Continuous Integration / Continuous Delivery) und Ticketing-Systeme sorgen dafür, dass bestehende Prozesse und Arbeitsabläufe nicht gestört werden.

FEATURES

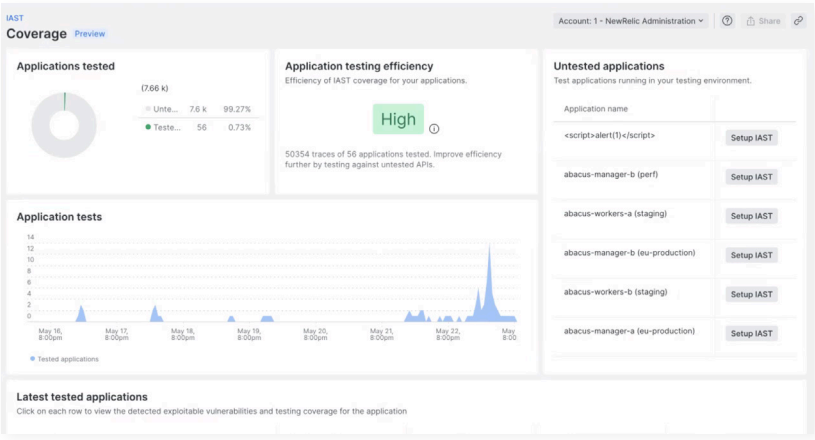
## Transparenz über den gesamten Anwendungsstack

Sehen Sie alle geschützten und ungeschützten Anwendungen, um blinde Flecken und versteckte Bedrohungen zu vermeiden, und überwachen und validieren Sie den Status Ihrer Abhilfemaßnahmen kontinuierlich, damit Ihre Anwendungen durchgehend geschützt sind.




## Identifizieren Sie Schwachstellen punktgenau in Echtzeit und fast ohne Fehlalarme

Identifizieren Sie Schwachstellen auf allen Ebenen des Anwendungsstacks und eliminieren Sie falsch-positive Meldungen durch schnelle, präzise Erkennung. So können Sie sich auf echte Sicherheitsbedrohungen konzentrieren und Schwachstellenlisten nach Risikoprioritäten sortieren, um schneller Abhilfe zu schaffen.

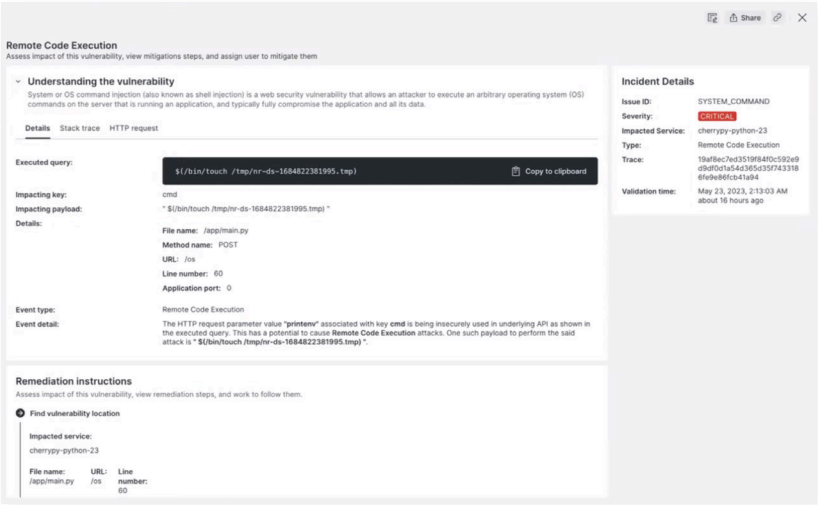



„Mit New Relic IAST können unsere Entwickler:innen zuverlässig und zielsicher programmieren, indem sie ihre Arbeit automatisieren und einen umfassenden Überblick über Sicherheitsrisiken erhalten, einschließlich Echtzeit-Feedback, Genauigkeit und kontextbezogener Sicherheitsanalyse – und das alles im Rahmen unserer Observability-Praxis, und ohne den Entwicklungsprozess zu behindern.“

**Agustín Paroli**
Head of IT Operations bei D24

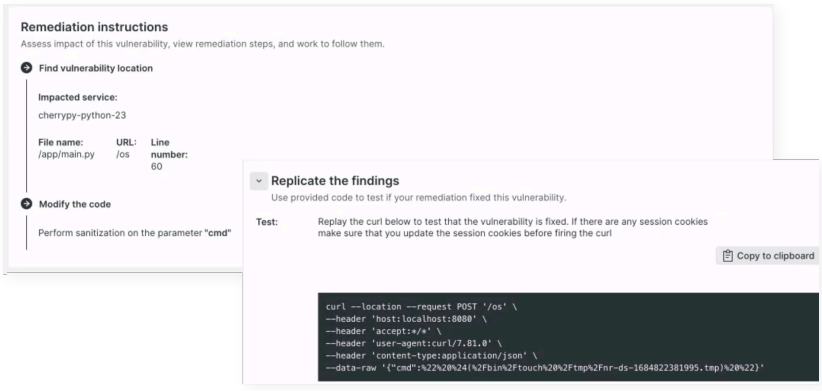
## Erkennen Sie Schwachstellen mit Proof-of-Exploit

Dynamische Bewertungsfunktionen, die Angriffe simulieren, um die Ursachen von Schwachstellen zu ermitteln, sparen Ihnen wertvolle Zeit. Dann können Sie sie anhand eines Proof-of-Exploit überprüfen und sich auf verifizierte Schwachstellen konzentrieren – und so besseren Code bereitstellen.




## Schnelle und wirksame Abhilfe dank geführter Problembehebung

Priorisieren Sie Anfälligkeiten wie SQL Injection, Befehlsausführung und andere Sicherheitsrisiken aus den OWASP Top 10 und beseitigen Sie sie, bevor sie ausgenutzt werden. Dank geführter Problembehebung und der Schutzvorrichtungen von New Relic lassen sich kritische Fehler vermeiden, die sonst zu einem Incident führen könnten.




## Nächste Schritte

- Weitere Informationen
- Jetzt starten
- Kontakt

new relic.