insightIDR

From compromise to containment. Fast.

Product Brief

Say goodbye to sleepless nights and the sinking feeling that the bad guys are still inside your environment. InsightIDR is the only fully integrated detection and investigation solution that lets you identify a compromise as it occurs and complete an investigation before things get out of control.

Cut Through the Noise to Detect Attacks

Getting too many worthless alerts?

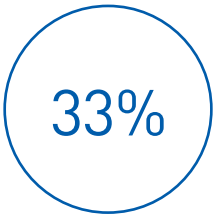
Rapid7 InsightIDR leverages attacker analytics to detect intruder activity, cutting down false positives and days' worth of work for your security professionals. It hunts for actions indicative of compromised credentials, spots lateral movement across assets, detects malware, and sets traps for intruders.

Adapt to evolving threats. InsightIDR leverages machine learning, allowing the solution to continuously evolve, as attacker behaviors do.

Expose attackers' hiding spots. InsightIDR monitors and tracks to detect local account abuses, malicious processes, and log manipulations.

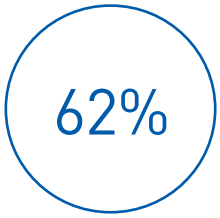
Trip intruders with deception. InsightIDR makes it easy to set traps to detect intruders when they initially explore the network, before they do damage.

Eliminate alert fatigue. InsightIDR's intruder analytics, based on years of learnings from our incident response, penetration testing, and Metasploit teams, quickly discern likely attacker behavior.



33% of all reported incidents take more than a month and up to a year to discover.

-Verizon Data Breach Investigations Report 2014/15



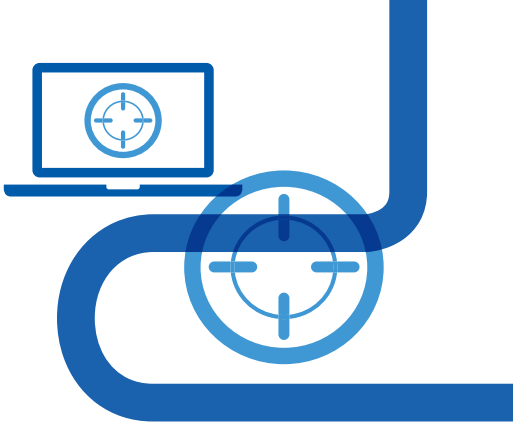
62% of organizations are receiving more alerts than they can handle.*

90% of organizations are worried about attacks using compromised credentials.*

* Data from the Rapid7 2015 Incident Detection and Response Survey

"[With InsightIDR] all of the information I need to understand and solve a problem is at my fingertips."

Jordan Schroeder, Security Architect, Visier



Investigate Incidents Faster

Incident investigations taking hours of tedious work?

Before an investigation even begins, InsightIDR devours data from across the network and attributes events to the specific user and asset involved. This allows security professionals to quickly look throughout the entire environment for all evidence of a discovered compromise.

Find missing puzzle pieces with notable behaviors. InsightIDR generates a timeline of notable events, empowering security teams to dig deeply to validate an incident.

Pull endpoint data into context without user disruption. InsightIDR enables you to pull contextual endpoint data on-demand without disrupting a user's work— even while the user is traveling and not on the company network.

Determine the scope of an attack. Attackers rarely pick one spot. InsightIDR's advanced search enables security analysts to pivot from validating an incident to quickly determining its scope, so they are poised to contain it quickly.

End the Drudgery of Security Data Management

Spending too much time managing data and tons of rules?

InsightIDR is a single solution with vast data coverage and visibility. Unlike most SIEMs and technologies designed primarily for compliance, InsightIDR extends data collection and detection to endpoints, as well as popular cloud applications.

Get value in days, not weeks or months. There's no need to wait weeks to get your security data and analytics platform set up. InsightIDR's cloud-based solution connects with your internal data sources, reducing the time and effort to set up and maintain the tasks of collecting, updating, and managing data sets.

View security data in a single, correlated context. InsightIDR brings together asset, user, and behavioral data into a single view, keeping analysts from jumping between tools, saving them time, and helping to analyze incidents faster.

Check the Compliance Box. PCI DSS requires that you log all events, review security alerts, and document the results of security investigations. InsightIDR fulfills all of these requirements without requiring a SIEM.

Gain comprehensive visibility across the network. InsightIDR provides security teams with immediate visibility across the network and into potential compromises, without waiting for the security team to write and validate complex rules.

Learn more about InsightIDR at www.rapid7.com/products/insightidr