RAPID7 PRODUCT BRIEF

InsightIDR

From compromise to containment. Fast.

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 both User and Attacker Behavior Analytics to detect intruder activity, cutting down false positives and days' worth of work for your security professionals. It hunts all of the top attack vectors behind breaches: the use of stolen credentials, malware, and phishing, and alerts on stealthy intruder behavior as early as possible in the attack chain.

Adapt to evolving threats.

Our global security analysts and threat intelligence teams directly contribute expertise into InsightIDR. As we identify attacker techniques, new behavior detections are pushed out to automatically match against your data. InsightIDR doesn't just highlight point-in-time malicious behavior; it provides full context on affected users and assets, as well as threat intel around adversaries using these techniques.

Trip intruders with deception.

Between Metasploit, pen tests, and our SOCs, Rapid7 understands the attacker—and the traces they leave behind. InsightIDR includes deception technology to trick attackers, making it easy to deploy multiple traps to expose intruders early in their attack chain.

INVESTIGATE INCIDENTS FASTER

Incident investigations taking hours of tedious work? Before an investigation even begins, InsightIDR devours data from across your network and attributes events to the specific users and assets involved. This allows security professionals to quickly look throughout the entire environment for all evidence of a discovered compromise.

In 2017, the use of stolen credentials was the top action behind confirmed breaches.

-Verizon 2018 Data Breach Investigations Report

38% of companies are not equipped to detect a breach without third-party assistance.*

Attackers lurk undetected on networks a median of 101 days before discovery.*

* Data from 2018 Mandiant M-Trends

Find missing puzzle pieces with notable behaviors.

InsightIDR generates a timeline of notable events, empowering security teams to dig deeply to validate an incident.

Real-time endpoint detection and investigation.

InsightIDR natively collects data off the endpoint with the Insight Agent and Endpoint Scan. This gives you real-time detection for malware, fileless attacks, and the use of stolen credentials even on assets off the corporate 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 monitoring to include endpoints, logs, and cloud services, leaving attackers nowhere to hide.

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, whether you are augmenting an existing log deployment or as your full 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.

"[InsightIDR] is absolutely fantastic, easy to use, and provides comprehensive data to manage all aspects of our security posture."

-IT Security Analyst,
via Gartner Peer Insights

GET STARTED TODAY

Deploying a SIEM shouldn't be hard. Most customers deploy in hours, and we'll guide you each step of the way.

Start your 30-day free trial:
www.rapid7.com/products/insightidr