RAPID7 | insightIDR

PRODUCT BRIEF

Detect faster, respond smarter, secure everywhere.

InsightIDR delivers the freedom to focus on what matters most.

InsightIDR is Rapid7's cloud-native SIEM and XDR provides complete coverage with a native endpoint agent, network sensors, collectors and APIs. Lightweight software-based collection technology and integrations go beyond unifying data to correlate, attribute, and enrich diverse datasets into a single, harmonious picture.

UNIFY: With leading next-gen SIEM at the core, it's big data collection without big work

Today's sprawling environments need data ingestion, scale, and computing power to keep pace. As a two-time leader in the Gartner Magic Quadrant for SIEM, this core simultaneously streamlines security operations and levels up outcomes.

- **Fast, flexible log search**
  Analysts of any skill-level can quickly visualize and process complex data
- **13-month data retention**
  Normalized and readily searchable data is at your fingertips
- **Actionable reporting**
  Be audit-ready always with pre-built dashboards and intuitive, custom report builders
- **Intuitive rule creation**
  Zero in on policy violations and unique threats with wizard-style UIs that guide you through custom log parsers and rule creation

DETECT: Unique intelligence plus expert vetting mean early threat detection you can trust

InsightIDR has a robust library of high-fidelity detections spanning attacker behavior-based detections as well UEBA detections, covering both known and unknown threats.

- **Embedded threat intelligence**
  Get high-signal, low-noise from intelligence across Rapid7's open-source community, service engagements, and detailed attack surface mapping
- **Emergent threat coverage**
  InsightIDR is SaaS-delivered, giving you immediate access to new detections with detailed guides to hunting for new adversaries
- **MITRE ATT&CK mapping**
  Users have a full matrix view and searchability, with filters on tactic, technique, and advanced persistent threat (APT) group
- **Expertly vetted**
  Rapid7's global MDR SOC experts use InsightIDR, giving us a rare feedback loop and deep understanding of the user experience

A Leader in the Gartner Magic Quadrant

See why we were named a leader in the Gartner 2020 Magic Quadrant for SIEM. Visit rapid7.com/siem-leader

RESPOND: Analysts respond faster and more confidently with playbooks and automation

When an attack is underway, every second counts. InsightIDR eliminates distractions and context switching, and drives fast, automated responses to stop attackers cold.

- **Detailed events and investigations**
  The InsightIDR attribution engine tracks users and assets as they move around the network, auto-enriching every log line
- **Correlation across diverse telemetry**
  Get a single investigation timeline for each alert, streamlining workflow with all the details of an attack in one place
- **Expert response recommendations**
  Each alert comes with recommended actions from our global MDR SOC and Rapid7 Velociraptor's digital forensics and incident response playbooks
- **One-click response and automation**
  With embedded containment workflows or seamless integration with Rapid7 InsightConnect SOAR workflows, orchestrated response just a click

> ***Whenever you log into InsightIDR, it's simple. It maps to the kill chain. It allows me to prioritize. That visualization just makes my job easier.***
>
> **Brett Deroche**
> Director of Security Operations,
> Amedisys

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.

Learn More:
www.rapid7.com/products/insightidr

aws marketplace

Support

call +1.866.380.8113

Customer Portal