InsightIDR

The Security Information and Event Management (SIEM) solution purpose-built to detect threats

Challenge

Customers want to enrich GuardDuty findings and monitor infrastructure using a SIEM, but complex deployments, endless maintenance, and high costs stand in their way

A SIEM is supposed to give a security team the ability to quickly detect if their organization's IT infrastructure has been compromised by collecting and analyzing log and event data from all of the organization's IT systems. Unfortunately, traditional SIEMs are so difficult to set up that many companies spend years trying to make due with a half-deployed product. Legacy SIEMs also require a large team just to keep up with maintenance. Worst of all, many SIEM vendors only include log aggregation features in their base product, charging extra for threat detection capabilities.

The Rapid7 Solution:

InsightIDR is a fast-to-deploy SIEM and XDR solution designed to quickly detect sophisticated attacks against hybrid environments

InsightIDR is a SaaS SIEM built on Rapid7's deep knowledge of how attackers successfully breach networks. With deployment times that can be measured in hours instead of months and low maintenance requirements, it makes it easy for organizations to ditch their clunky legacy threat detection tools. InsightIDR aggregates data from AWS sources like GuardDuty and CloudTrail with on-prem networks, remote endpoints, cloud-based services, and honeypots. InsightIDR detects threats in this aggregated data by leveraging multiple strategies, including User Behavior Analytics to detect suspicious behavior and Rapid7's renowned threat intelligence library to spot indicators of an attack. Threat investigations are also drastically sped up, thanks to all relevant data being available in one place.

Benefits

InsightIDR is fast to deploy, easy to use and manage, and provides a complete workbench for threat detection and response.

Time to Value

On average, it takes less than four days for prospects who start a free trial with InsightIDR to launch their first investigation..

Log Management & Compliance

Any data sent to IDR is normalized, attributed, and enriched to offer a single console for fast log search, reporting, and regulatory compliance.

Built-In Threat Detection

The base InsightIDR offering includes comprehensive threat detection capabilities such as User Behavior Analytics (UBA), threat intelligence libraries, and deployable honeypots.

Respond to Threats Faster

Visual timelines and aggregated data dramatically accelerate threat investigations: *"[InsightIDR] has decreased our average amount of time to investigate and remediate any incident from days[...] to an average time of 22 minutes."*
- Gartner Peer Insights Review

Rapid7 on AWS

Security concerns are often a central reason why an organization hasn't started or expanded their migration to the cloud. Rapid7 helps organizations migrate to AWS with confidence. Our products are built to secure hybrid environments. Not only do they offer an array of features addressing the unique challenges of securing on-prem and cloud environments, they also integrate with AWS' native security services. Joint Rapid7/AWS customers enjoy the best of all worlds: the convenience and deep integration of AWS security solutions as well as the ability to monitor, detect, and react to threats across their entire hybrid environment using Rapid7's Insight family of products.

Features

One Solution for SIEM and Threat Detection

InsightIDR customers easily collect data from AWS, endpoints, on-prem networks, other cloud providers and SaaS applications. Lightweight collectors, APIs and the Insight Agent make it easy for the customer to get up and running. From there, all data is aggregated and analyzed for suspicious user behavior and known attacker behavior. Machine learning and out of the box Rapid7 threat detections mean incidents can be detected the instant InsightIDR is setup - no rule configurations needed. *Please note that Active Directory/AWS Directory Service, LDAP, and DHCP are required data sources to unlock all functionality.*

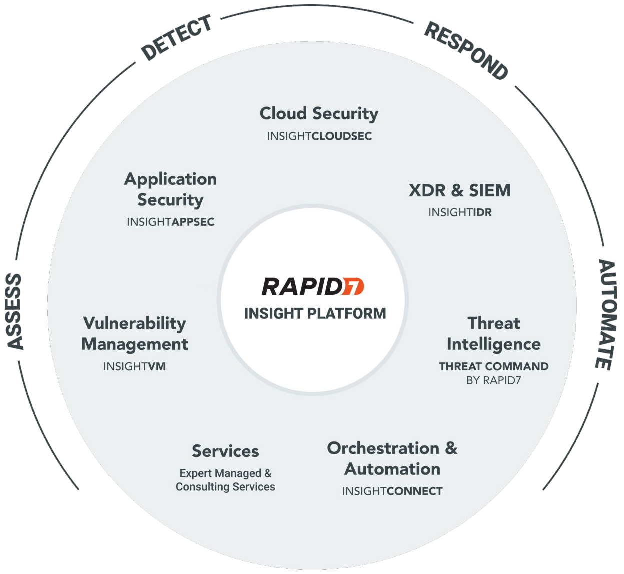
Native Support for Monitoring AWS Assets and Services

AWS CloudTrail and GuardDuty integrations offer detailed visibility into AWS environments. InsightIDR combines these logs with endpoint, user, and network data for complete visibility across the customer environment. As customers migrate to the cloud, they can use InsightIDR as a single console to centralize logs, detect threats, and respond with confidence.

Part of the Rapid7 Insight Platform

Rapid7's Insight platform offers an array of solutions to address different cybersecurity needs. The products on the Insight Platform exchange data with one another out of the box, reducing both setup and maintenance for the security team. The Rapid7 Insight Agent is also shared between multiple products, reducing agent fatigue and making it easy to start using additional Rapid7 products in the future.

Beyond the Platform's technical capabilities, Rapid7 also offers managed services for several products, including InsightIDR. Let our veteran security analysts run InsightIDR on your behalf out of our worldwide network of SOCs. Even better, you'll still get direct access to InsightIDR as well.



Get started with Rapid7 InsightIDR

To learn more about InsightIDR or to start a free trial, speak to your AWS Account Manager or contact the Rapid7 sales team.

Available on aws marketplace