Enhanced Endpoint Telemetry in InsightIDR

Detect, investigate, and respond more effectively with extended visibility into your endpoint data

With comprehensive coverage across the modern environment, InsightIDR goes beyond the scope of traditional SIEMs to provide highly reliable threat detection out of the box and advanced environment visibility when teams need it. Critical to InsightIDR's holistic coverage is real-time endpoint detection and response, which is necessary for identifying the early signs of an attack.

Broader and More Effective Investigations

InsightIDR is the only SIEM with powerful endpoint detection and response (EDR), Network Traffic Analysis, and behavioral analytics built in, enabling customers to detect and investigate threats on their endpoints without any integrations or additional configurations. With InsightIDR, customers can leverage Rapid7's universal Insight Agent to access real-time endpoint scanning and threat detection alerts out of the box.

But our endpoint capabilities don't stop at threat detections: With Enhanced Endpoint Telemetry (EET), InsightIDR customers see a historical archive of process start endpoint data to accelerate detections, investigations, and remediation.

Accelerate Alert Investigations and Unlock Custom Use Cases

EET provides context to what happened before and after any action on an endpoint, allowing teams to tell the full story around what actions triggered a particular detection. Now, security teams can accurately decipher between what was an attack and what was a normal command that happened to look suspicious—without jumping in and out of multiple tools.

This full archive of process start data also allows customers to create custom detections based on this data. This is incredibly useful to recognize potential indicators of compromise that may be unique to your organization's specific policies and/or your specific industry or market sector.

For example, if a customer only uses Slack for internal communications and suddenly Skype is being run on an endpoint, their analyst would want to be able to kick off an incident response process to contain this threat as soon as possible; with EET's start process data, they can now create an alert to trigger any time another chat application, like Skype, is run.

With EET, InsightIDR customers can see the full scope of an attack, including what led up to the attack, what occurred during it, and what happened after. For example, if the attack started from an employee opening a phishing link, and the stolen credentials were used to perform malicious actions on the endpoint, you can review that endpoint activity and choose to disable the user account to avoid future compromise. If after an attack, they went on to change administrative settings on any endpoint, you may want to go back and revert those changes.

Drive Effective and Complete Detection and Response with InsightIDR

There are a lot of technologies out there today that security teams have access to—and very much need access to—to build a successful detection and response program. However, as teams adopt more and more tools, what is meant to help with detection can actually create friction in the process, with complicated integrations, time jumping between tools, and needing to learn the ins and outs of multiple security platforms.

At Rapid7, we've looked at detection and response holistically and identified all of the key pieces of technology that help drive visibility and make sure our customers are protected. The best part? We deliver it all in one solution.

InsightIDR analyzes endpoint data alongside user behavior analytics logs and network traffic data to give customers a full picture of their security threat landscape. These datasets provide critical activity data and contain the earliest indicators of potential compromise, forming the three pillars of Gartner's Security Operations Center (SOC) Visibility Triad—SIEM/UEBA, Network Detection and Response, and Endpoint Detection and Response. By leveraging the SOC Visibility Triad, InsightIDR accelerates detection and response by providing fast, accurate alerting, and giving customers the tools and context needed to respond quickly and confidently to threats.

About InsightIDR

InsightIDR cuts through complexity and noise to accelerate detection and response with reliable alerts, high-context investigations, and automation. Powered by insights from our MDR, research, and threat intelligence teams, InsightIDR aggregates and analyzes data sources across logs, users, endpoints, and the network to notify teams at the first signs of attack. With lightweight cloud hosting, InsightIDR avoids many burdens faced by traditional on-premises SIEMs. Customers report the fastest deployment times in the industry, seeing return on investment from day one.

To learn more about Rapid7 or get involved in our threat research, visit www.rapid7.com.

Support

call +1.866.380.8113

Customer Portal

> "In our team's opinion, this is one of the greatest tool they have ever used as an IDS/IPS solution and feel like the tool's packed with assortment of features (Report Logging, Intuitive Dashboard, Process Automation, Network Monitoring, etc.) that makes it way better than all of its competitors."
>
> — Gartner Peer Insights