Detection and Response for the Remote Workforce

How we help you secure remote employees and monitor disparate environments

Threat detection and response is a critical piece in an ongoing journey to improve your security program, but feeling confident in your coverage can seem challenging with a remote workforce. When users are remote, they may be operating assets like laptops in potentially hostile networks outside of IT and security's control. And to do their jobs effectively, your remote employees still need access to company data and key applications.

To combat these challenges, we've developed a comprehensive approach to detection and response, to help you enable business continuity, keep your organization protected (no matter where they are), and build a foundation for success across your entire environment.

Scale a remote workforce

When the demand for remote working spikes, the last thing you want to do is re-architect your detection and response solutions to scale to these new demands. With its cloud-native architecture and built-in expertise, InsightIDR is designed to get you up and running faster than any other SIEM in the space, while continuously up-leveling your capabilities and providing context into threats. As your demand shifts, there's no need to provision additional hardware or reconfigure settings; InsightIDR automatically scales with your environment—even as that environment moves beyond the four walls of your headquarters.

For any new threats that emerge focused on remote users, InsightIDR automatically stays on the bleeding edge. Using insights from our global Managed Detection and Response (MDR) team and Rapid7's threat intelligence network (including Metasploit users, Project Sonar internet scanning, Project Heisenberg global honeypot network, and more), our SOC experts curate new detections for these threats, which are then added to InsightIDR and automatically rolled out for customers via our SaaS delivery (no need for manual updates).

Get instant visibility across your environment

Remote users

When employees move off campus, establishing what a new normal looks like can be a challenge for security teams. Is this a valid user working somewhere else, or malicious use of credentials? InsightIDR has a deep heritage around User Behavior Analytics and leverages finely tuned analytics and machine learning to quickly establish a baseline and recognize anomalous activity. We also include valuable reporting, such as our Ingress Locations dashboard, to provide vital information for your analysts to confidently investigate. By recording and displaying historical activity on remote user location (including authentications from outside the US), failed login attempts, and more, you and your team can easily identify malicious vs. normal user activity.

When users are remote, you may also use more cloud applications and services, such as Office 365, Azure, and AWS. InsightIDR can aggregate Security Center alerts from Microsoft Event Hubs, and recognize user or environment changes in AWS and alert teams on these changes right away.

Remote endpoints

Our lightweight, cloud-hosted Insight Agent provides critical, real-time visibility across your Windows, Mac, and Linux assets—no matter where they are in the world. The agent collects user activity and, for InsightVM customers, asset vulnerability data. You'll marry real-time endpoint data with user activity and log search for comprehensive incident detection across the entire attack chain. With the ability to search assets by username, InsightIDR allows you to quickly and accurately track which assets your users log on to most frequently and expedite the process of granting remote access to those devices.

The Insight Agent provides context to anomalous behaviors by analyzing:

- Running processes
- Security events
- System event codes
- Registry data
- Intruder traps
- Asset and user data
- File audit logs
- File and package data

Remote network access

With the Insight Network Sensor, you'll monitor, capture, and assess the end-to-end network traffic moving throughout your physical and virtual environment, including remote workers when deployed alongside your VPN solution.

Our approach to Network Traffic Analysis (NTA) is unique in that our MDR team has curated a library of the most critical Intrusion Detection System (IDS) alerts for teams to focus on, helping cut down on noise and increase analysts' confidence in taking action. We also leverage a proprietary Deep Packet Inspection (DPI) engine to capture all raw network traffic flows, extracting rich metadata. This information is enriched with our UBA attribution engine, so you can quickly identify which user and what asset is associated with a network flow.

Respond faster to keep attackers away

Response plans and procedures can't be shelved during a work-from-home scenario. With a SaaS detection and response solution, you can know for certain that your security team has access to the same information and views, even when they aren't together in the office.

When you have a remote workforce operating on potentially insecure networks, security teams have to be able to respond quickly to contain a threat. By providing rich forensic context with our alerts and powerful search and reporting tools, analysts can feel confident taking action on threats right away. InsightIDR customers have access to automation functionality to accelerate response across a variety of use cases, including suspending users, containing threats on an endpoint, or integrating with ticketing systems. As the need for efficiency increases in a remote working spike, InsightIDR connects seamlessly to InsightConnect, Rapid7's SOAR solution, for customers looking for more ways to orchestrate and automate response processes across their tools.

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 network to notify teams at the first signs of attack.

To see how InsightIDR aggregates diverse data sources and leverages expertly curated detections to secure a remote workforce, visit rapid7.com/insightidr

Support

call +1.866.380.8113

Customer Portal

See why Gartner named Rapid7 a leader in the 2020 Magic Quadrant for SIEM. Visit rapid7.com/siem-leader