RAPID7

PRODUCT BRIEF

InsightIDR Network Traffic Analysis

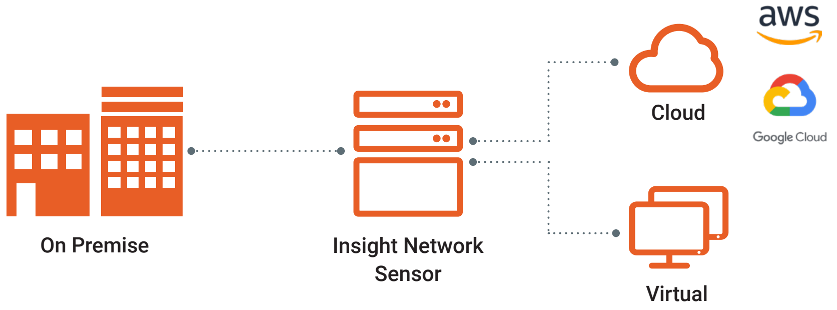
Eliminate Blind Spots and Unlock Maximum Visibility

InsightIDR—Rapid7's cloud-native SIEM and XDR—delivers highly efficient, accelerated detection and response with no blind spots, even on the edge and perimeter. Network Traffic Analysis (NTA) in InsightIDR helps teams detect threats early and follow attacker movement across the network. Work smarter and faster with frictionless SaaS deployment experience, hyper intuitive interface, robust out-of-the-box detections, and actionable automation.

Insight Network Sensor is Easy to Download and Deploy

You can deploy the Insight Network Sensor on-premises, virtually, or in the cloud (via AWS). The sensor collects all network traffic metadata for analysis and observation on the central management portal, without interacting with other devices or impacting network performance. This network traffic data is passed to InsightIDR and aggregated with other critical data sources.

Deployment options with the Insight Network Sensor



A 24/7/365 Record of Activity

Every user and device on a network leaves a trail of traffic data that's incredibly valuable for investigations and forensics. The trail is nearly impossible for malicious actors to tamper with, and it can reveal the steps (or even location) of attackers in real time.

Key SOC Challenges

- **Traditional network solutions are noisy and low ROI.** With tons of data and little context, it's difficult for teams to get a full picture of their environment
- **Bespoke NTA solutions create data silos and disjointed telemetry.** They're separate products to maintain and update, with data isolated rather than integrated alongside other critical security data
- **Unactionable, non-intuitive packet capture data** means more time combing through data, and less time spent detecting real threats

The Insight Network Sensor collects human-readable network metadata, attributed to specific users and devices which can then be used for detections and for building context around new and existing investigations. This gives you a complete record of both east-west and north-south activity on your network.

Detect Threats Early and Reliably

Network traffic offers a new axis for attacker detection. This happens through a combination of Intrusion Detection System (IDS) events and alerting around known bad attacker activity, as well as suspicious and malicious behaviors. For example:

- Network based IDS which is run directly on the sensor. This uses signature and rules that require direct access to network packets
- Platform based detections which use network metadata. This includes DNS query analysis and suspicious IP information contained within network flows.
- Behavioral type detections such as Anomalous Data Transfer (ADT), which identify data exfiltration attempts on a network for easier monitoring of data transfers and unusual behavior.

Traditional IDS tools can be noisy. Rapid7's Threat Intelligence and Detection Engineering (TIDE) team has carefully analyzed thousands of IDS events to curate a list of only the most critical and actionable events. This means when malware, botnets, or other compromises are detected, teams won't have to go through tedious cycles to determine their validity. Like our IDS events, these ADT detections are expertly curated by Rapid7 so your team's analysts can take action confidently, on reliable, expertly vetted detections.

Do More Without Doing More

With the data transformation, attribution, analysis, and detection in InsightIDR, customers get comprehensive coverage across their environment to find threats early—without creating more work for security teams.

All InsightIDR and MDR customers have full, free access to the Insight Network Sensor, IDS events, and DNS and DHCP data captured by the Sensor included in their subscription. With InsightIDR's other lightweight collection methods—including the Insight Agent, Collectors, and APIs—users have their network traffic data alongside user activity, logs, cloud, endpoints all in one place, ending tab-hopping and multi-tasking and accelerating detection and response.

> **Rapid7 InsightIDR vastly improved the visibility of our network, endpoints, and weak spots. We now have the ability to respond to threats we didn't see before we had InsightIDR.**
>
> Robert Middleton, Network Administrator, CU4SD via TechValidate

InsightIDR Ultimate customers have access to an advanced dataset, Enhanced Network Traffic Analysis, which provides the advanced visibility and monitoring capabilities that flow data unlocks, as well as Anomalous Data Transfer (ADT) data exfiltration detections. Learn more about all InsightIDR has to offer here.