Detect Threats Early and Follow Attacker Movement Across the Network

Leveraging Rapid7 Network Traffic Analysis (NTA) in InsightIDR

Get Up and Running Quickly with the Insight Network Sensor

InsightIDR boasts the best deployment times in the industry, and this commitment to immediate time to value continues with NTA. The Insight Network Sensor is easily downloaded and deployed, either on-premises or on a virtual VMware network. 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. These IDS events and DPI data are passed to InsightIDR and aggregated with other critical data sources.

Key Deployment Steps

1. Provision a Linux host (standalone or virtual machine)
2. Configure a network traffic source such as a SPAN or mirror port
3. Install sensor software and manage via Platform Data Collection Management

For more, visit our Help Docs

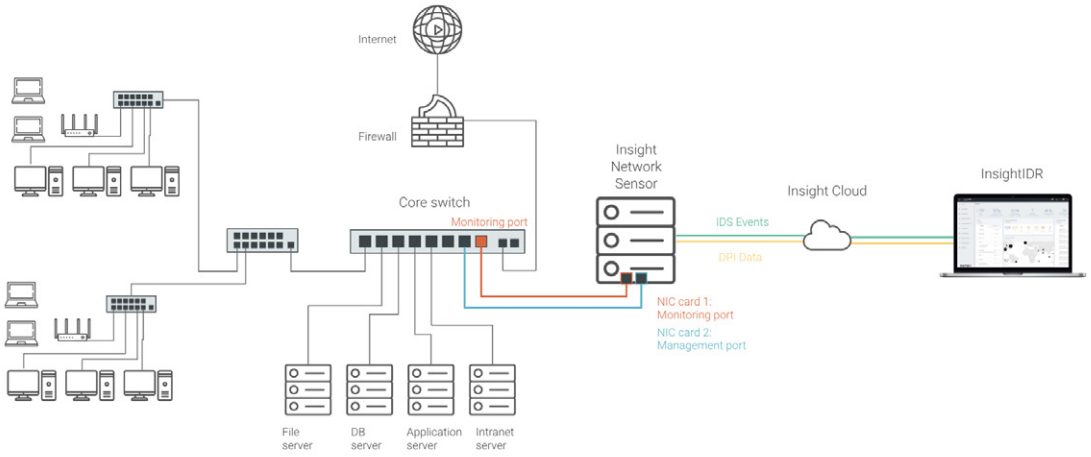

Figure 1: An example deployment of the Insight Network Sensor. A SPAN or mirror port is configured at the network core, which allows the capture of any traffic passing through (both north-south and east-west).

Discover Assets and Activity on Your Network

With NTA, get instant visibility into who is on your network and the sites and applications to which they are connecting. With this picture of the assets in your environment, you'll be able to establish a baseline of your landscape to monitor for unusual activity. This data can also supplement (or in some cases, replace) DNS or DHCP sources, to help drive further efficiencies for security teams.

Detect Threats Early and Reliably

Traditional Intrusion Detection System (IDS) tools can be incredibly noisy. The Rapid7 MDR team has carefully filtered IDS events to capture only the most critical and actionable detections. This means when malware, botnets, or other compromises are detected, teams won't have to go through tedious cycles to determine their validity. Analysts can take action confidently, on reliable, vetted alerts.

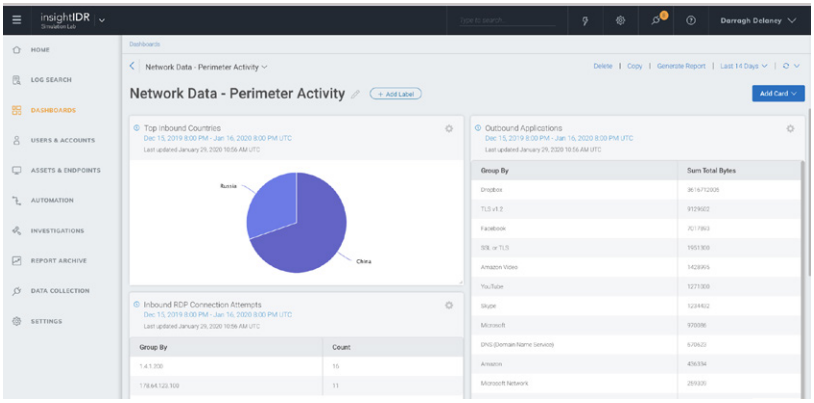

Figure 2: Cards that focus on north/south network activity leveraging data captured from the Insight Network Sensor.

Investigate Attacks More Effectively

Rapid7's proprietary DPI engine captures and analyzes traffic in readable, interpretable details, without the complexity and overhead of full packet capture. This passive analysis also means no performance impact to the network. With this rich flow data, teams have deep detail with which to track attacker entry and movement across the network. This can help accelerate investigations and inform response action.

Comply with Critical Regulations

The crux of most compliance regulation is protecting sensitive and personal information, and the first step in protection is visibility. In addition to a further step toward eliminating attacker success, network data is critical to achieve the visibility requirements for a number of compliance regulations. IDS, for example, is notably an explicit requirement for PCI-DSS compliance.

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 learn how InsightIDR aggregates diverse data sources and leverages expertly curated detections to find threats early—without creating more work for security teams—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