coresecurity
by HelpSystems

DATASHEET *(Cybersecurity)*

Network Insight

Core Network Insight monitors and analyzes network traffic to reveal critical threats in real time on any device within your infrastructure. Multiple detection engines provide definitive evidence and pinpoint the specific location of an infection, enabling security teams to respond efficiently, rapidly reduce dwell time, and prevent loss.

Real-Time Actionable Detection

Network Insight uncovers hidden infections, identifying the type of threat and pinpointing the exact device on which it is located, facilitating swift recovery and remediation. Intuitive dashboards provide detailed data on currently infected assets, average infection age, riskiest infected assets, newly infected assets, and more.

The Case Analyzer, a unique context aware threat intelligence engine built on over a decade of research, confirms the infection, alleviating the need for analysts to spend valuable time on any additional threat investigation or research.

When an infection is verified, Network Insight ensures response teams can efficiently eliminate threats with instant alerts in their preferred platform, with notifications in SIEM, SYSLOG, or email, and automatic ticket creation in systems like Service Now or Jira Service Desk.

Multi-Faceted Intelligence

Most threat solutions rely on creating a single baseline of your environment, sending alerts of any potential threats solely based anomalies or changes. This often requires manual tuning and results in missing critical threats.

Core Security's threat intelligence database includes more than over 15 years of evidence collected from observing billions of DNS requests a day, thousands of malware samples, and nearly 100 billion domains. Additionally, Network Insight monitors many behaviors indicative of infected devices, including domain fluxing, DNS tunneling, sandboxing, and deep packet inspection.

Multiple detection engines continually capture and correlate evidence, applying this threat intelligence in the analysis of network traffic content, payload, and the behavior monitored by Network Insight. This multi-faceted approach to confirming infections provides an unmatched level of confidence in the alerts sent out.

PRODUCT SUMMARY

KEY FEATURES

- Real-time capture and correlation of evidence to detect APTs
- Automated Case Analyzer to confirm infections
- Agentless functionality to enable monitoring of every device, including high-end IoT
- Threat intelligence API to determine the risk status of domains
- Interactive, personalized dashboards with dark mode capability
- Searchable database with details on different threats
- Integrations with other solutions like Carbon Black or Event Manager
- Extensive reporting capabilities

SUPPORTED BROWSERS

- Microsoft® Edge
- Microsoft® Internet Explorer 11
- Firefox
- Chrome

HARDWARE REQUIREMENTS

- One or more sensor appliances for monitoring
- Management Console for analyzing both local and global intelligence

WORKFLOW INTEGRATIONS

Notify response teams using:

- SIEM solutions
- SYSLOG
- Email
- ServiceNow
- JIRA

No Device Left Behind

Most security products only protect a fraction of all endpoints or require an agent to be installed in order to monitor them. This leaves far too many high-end IoT and other devices unwatched, including security cameras, video conference units, MRIs, CT machines, SCADA systems, or even connected coffee makers and refrigerators. Network Insight is agentless, and OS and platform agnostic, covering any and every device in your network.