

Guided-SaaS NDR

Expertise on Your Side

Security leaders know that threats are evolving faster than ever before. As a result, security teams are on an uneven playing field. But what if you could even that playing field? Gigamon ThreatINSIGHT™ restores your advantage by giving your security teams more time, data and insight into attacker behavior. It improves SOC efficiency while providing high-fidelity adversary detection to enable rapid, informed response. ThreatINSIGHT Guided-SaaS NDR redefines how network detection and response is delivered, ensuring:

YOU AREN'T ALONE

Advisory guidance and out-of-the-box hunting tools during high-risk incidents helps improve staff retention.

YOU AREN'T DISTRACTED

Low maintenance and zero detection tuning improves SOC and IR efficiency and effectiveness.

YOU AREN'T IN THE DARK

Guided-SaaS closes the SOC visibility gap necessary to effectively identify cyber-adversaries across any network, device and traffic.

As a company's first responders to cyber adversaries, security operations and Incident Response (IR) teams are well-versed in tackling challenges. However, on an uneven playing field, mature security teams seek vendors that understand the SOC/IR workload and design solutions that focus not only on analyst effectiveness, but also burnout and staff retention. Specifically, an ideal network detection and response (NDR) solution should alleviate:

VISIBILITY GAPS LEAVING THE SOC IN THE DARK

Analysts are missing visibility they need to be effective:

- + SIEMs & EDRs have visibility gaps (devices, networks, and traffic).
- + Encrypted traffic is rapidly growing, making inspection difficult.
- + Analysts lack historical data to combat an adversary's extended dwell time.

UNNECESSARY TOOL DISTRACTIONS

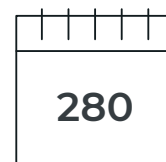
Analysts are overwhelmed because:

- + They face constant false-positive alerts and detection tuning.
- + Solutions require hidden care and feeding costs (maintenance, updates, visibility optimizations).

FIGHTING INCIDENTS ALONE

Analysts are facing high-pressure incidents on their own:

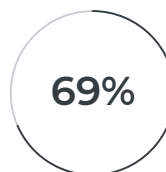
- + Alerts lack context or guidance for what to do next.
- + They lack out-of-the-box tools for thorough investigations and threat hunting.
- + Vendors charge for product expertise enablement, threat intelligence and investigation guidance.



Days to identify and contain a Data Breach¹ in 2021

280

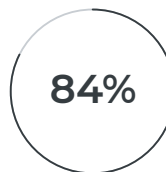
365-days of historical data is essential for effective response



Of SOC analysts cite lack of visibility into network traffic as the top reason for SOC ineffectiveness²

69%

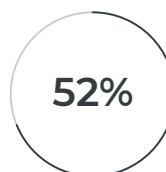
Visibility is a foundational need



Of SOC analysts report rank "Minimization of false positives" as the most important SOC activity (detection tuning)²

84%

Reducing false positives should be the vendor's responsibility



Of SOC analysts report they need access to more out-of-the-box content (i.e., rules, playbooks).²

52%

Guided Playbooks and parallel hunting are foundational for responders

The ThreatINSIGHT Difference

Gigamon ThreatINSIGHT Guided-SaaS NDR gives security teams the tools and visibility into historical network data that lets them quickly identify adversary activity, while improving incident response capabilities, removing tool maintenance distractions, and relieving analysts' burnout. The Gigamon Technical Success Management (TSM) team is staffed with field tested security analysts and incident responders who work alongside Gigamon Applied Threat Research (ATR) to ensure ThreatINSIGHT customers are best positioned to dismantle adversaries.

CLOSING THE SOC VISIBILITY GAP

While SIEMs and EDRs have increased a SOC/IR team's effectiveness in identifying active infections, visibility gaps to devices, networks and traffic remain. The result is analysts are left in the dark when trying to identify all adversary activity described across the MITRE ATT&CK framework. ThreatINSIGHT Guided-SaaS NDR solution:

- + Provides historical visibility and recording of near packet-level metadata**

Any device, any network, and any traffic, including N | S | E | W and encrypted

- + Delivers high-fidelity adversary detections**

Blending machine learning, behavioral analysis, and crowdsourced threat intelligence

- + Fast omnisearch powered triage and investigation capabilities**

365-day access to enriched network metadata

- + Guided Playbooks for rapid response and hunting**

Enable SOC teams to investigate attackers based on real-world behaviors at the click of a button

ELIMINATING DISTRACTIONS

Purchasing a security solution should enable security professionals to focus on protecting their organization. However, all too often, security vendors deliver solutions that create distractions rather than positive results. Many NDR solutions have hidden costs and time tied to providing care and feeding, solution proficiency, addressing false positives, and performing detection tuning—all negating their intended value. ThreatINSIGHT Guided-SaaS NDR includes expertise from product and threat experts to remove distractions and ensure:

- + Fast time to value**

TSMs provide deployment, configuration, and health check assistance along with ongoing product enablement to ensure continuous customer proficiency

- + Minimal maintenance**

Gigamon TSMs and SaaS Ops teams provide sensor and traffic diagnostics, fully managed ThreatINSIGHT web portal, and automatic software updates

- + Zero detection tuning with true-positive detections**

ATR performs ongoing detection tuning and QA of all machine learning, behavioral analysis, and threat intelligence detection engines

QQ You can't do big things if you're distracted by a thousand small things. — ANONYMOUS



Security incidents are high-pressure situations for SOC/IR analysts who are in a race against time to protect their networks. With little knowledge of the adversary's intent, tactics, techniques, or procedures and working without external guidance, the security team must often go it alone. External threat knowledge is often scarce, and security tools traditionally only offer generic recommendations. Most tools don't provide the necessary context, out-of-the-box tools, and search capabilities required to gain insight into what systems the attacker has compromised, the data they have accessed, or the identities and credentials they have obtained. These limitations make it difficult for the SOC/IR team to develop a comprehensive response plan.

ThreatINSIGHT Guided-SaaS NDR is backed by Gigamon ATR threat researchers and Gigamon TSMs, who are experienced security analysts and incident responders, both focused on ensuring customers are best positioned to dismantle adversaries.

+ ATR performs reverse engineering, tracking, and detailing of adversary behavior

Building first-hand knowledge on adversaries to empower both ThreatINSIGHT and the TSMs

+ TSMs work directly with customers to provide expert advisory guidance upon request

Sharing threat information and incident response best practices and guidance during high-pressure events

ThreatINSIGHT Guided-SaaS NDR



PURPOSE BUILT NDR TECHNOLOGY

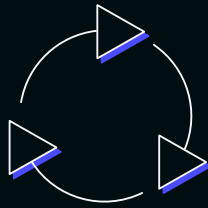
365-day historical visibility

+

High-fidelity adversary detection

+

Rapid, informed response



DISTRACTION FREE SaaS MANAGEMENT

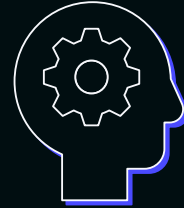
Minimal maintenance

+

Zero detection tuning

+

Automatic software updates



ADVISORY GUIDANCE WHEN IT MATTERS MOST

Threat/adversary knowledge

+

Incident management guidance

+

Out-of-the-box triage and
hunting tools

ThreatINSIGHT Guided-SaaS NDR

ThreatINSIGHT provides NDR as it should be. A solution built for responders, by responders that:

- + Augments your SIEM and EDRs with network detection and response to complete the SOC visibility triad, identifying threat actor behaviors not observable by other technologies across the ATT&CK framework so your team is not in the dark
- + Delivers NDR technology that requires no detection tuning and SaaS delivery that requires minimal solution management and maintenance so your team is not distracted
- + Eases high-pressure scenarios for security analysts with Guided-SaaS expertise on your side so your team is not alone

Learn more at gigamon.com/threatinsight.

REQUEST A DEMO AT GIGAMON.COM/DEMO.

¹ IBM Security: Cost of a Data Breach Report 2021, 2021

² Ponemon: Improving the Effectiveness of the SOC, 2020