WHITE PAPER

Threat Hunting with NDR and Deception Technology

Stop Threats Earlier in the Attack Life Cycle

Executive Summary

Organizations with large, complex networks often run into challenges in establishing proactive network security. Security teams must contend with blind spots, siloed, non-integrated security products, a high volume of network traffic, and false positives, making it difficult to respond to advanced cyberattacks.

Through a combination of network detection and response capabilities and deception technology, security teams can put proactive threat hunting capabilities in place to stop threats earlier in the attack life cycle and reduce organizational risk.

Fortinet early detection and prevention technologies helped accelerate the time to identify threats from 168 hours to under an hour. The time to triage threats was reduced from 8 hours to 10 minutes, and the time to contain threats dropped from 4.2 hours to 1 minute.[1]

The Changing Network Landscape

Data traversing today's networks is growing exponentially. All that data crisscrossing networks across the globe can overwhelm legacy security systems, creating many opportunities for cybercriminals to exploit any vulnerability or temporary weakness in an enterprise data center's security.

A successful cyberattack may damage productivity, consumer confidence, and brand reputation, which may take years to recover from. While CIOs and IT leaders are certainly focused on risk management and protecting data stored on-premises and distributed across the network, the protections in place are often isolated and disjointed, inadvertently adding complexity and risk to the enterprise.

Enabling Efficient Response

Security teams that support complex network environments can use the combination of network detection and response and deception technology to gain visibility across the network, reduce false positives, and deter attacks in progress.

Defining Threat Hunting

Unlike traditional passive threat detection methods, threat hunting solutions are active with the ability to identify potential threats that may bypass traditional defenses. These solutions continuously look for indicators of compromise (IOCs) and can uncover any attacker activity that is in progress. Manual threat hunting is often performed by security teams that must scour log data or analyze network metadata. Solutions such as network detection and response (NDR) tools use artificial intelligence (AI) or machine learning (ML) to facilitate analysis and locate indicators of attacker activity in otherwise normal traffic.

By supplementing manual and NDR analysis with deception technology, teams can proactively look for attackers and use a network of decoy devices and tokens to lure attackers to specific assets across the network.

Leveraging Deception Technology

Much like conventional hunters use decoys that mimic natural behavior to lure or trap their quarry, security teams use deception technology to attract cybercriminals away from an enterprise's true assets and divert them to a decoy or trap. This decoy simulates legitimate organizational assets, applications, and data so the criminal is tricked into believing that they have infiltrated and gained access to important assets when they have not. Deception technology is especially useful in situations where endpoint visibility may be lacking such as operational technology (OT), industrial control system (ICS) or Internet of Things (IoT) environments. Although the use of decoys may seem more passive than traditional, hypothesis-driven hunting, deception technology can be particularly effective at detecting:

- **Account hijacking attacks:** These attacks involve an attacker that is trying to take over a legitimate user's account using stolen credentials.
- **Credential theft:** This type of theft centers around an attacker gaining access to a list of credentials and using them in a future hack.

- **IoT attacks:** These happen when a hacker targets IoT devices using weaker access credentials such as default passwords to gain access to an organization's network.
- **Lateral movement attacks:** These attacks involve a hacker trying to move laterally (east to west) through a network. The attacker first gains access to one system and then attempts to spread the attack to other systems the computer is connected to so they can take advantage of the interconnected assets within the organization.

With deception technology, when an attacker engages with deception assets such as fake files on an endpoint, or if malware tries to encrypt a fake file, the deception technology neutralizes the attack by isolating the compromised decoy. It prevents the attack from spreading and potentially halting communications with a command-and-control (C2) server.

Fortinet early detection and prevention tools provided zero false positive detection. Timely and prioritized insight to security teams helped to reduce the number of hours required to fully investigate and remediate threats, making security teams up to 86% more operationally efficient.[2]

Threat Hunting with Network Detection and Response

NDR solutions rely on network sensors to collect network metadata and continuously monitor network traffic. These solutions use behavioral analytics, ML, and AI to detect cyberthreats and anomalous behavior. Because the technology is not signature-based, it adapts to changes in attack techniques so security teams can keep up with and outmaneuver adversaries. NDR solutions typically follow these steps to detect threats:

1. Analyze north-south and east-west network traffic and build a baseline of normal traffic patterns.
2. Deploy ML, behavioral analysis, and threat databases to detect threats and anomalies.
3. Monitor every device on the network passively, without impacting performance or availability.
4. Integrate with complementary endpoint detection and response (EDR) and security information and event management (SIEM) solutions to provide greater telemetry.
5. Allow for in-depth investigations across the entire network, without the use of endpoint agents.

Security analysts can use NDR to query network traffic metadata and search for patterns or anomalies that could indicate suspicious or malicious activity. While conducting an investigation, analysts often write custom queries or use built-in search functions to look for specific behaviors, such as:

- Traffic to unusual domains
- Irregular file-sharing activity
- Unusual protocols, payloads, or destination IP addresses

Analysts also can use NDR to reconstruct network sessions to identify how a threat actor may have moved through the network, what data was exfiltrated, or how the actor established persistence.

NDR and Deception Technology in Action

Combining NDR with deception technology gives threat hunters unparalleled visibility into the entire network, including on-premises, hybrid, and cloud environments. It provides high-fidelity detections of unknown, weak indicators of malicious activity by correlating the NDR AI-based behavioral network traffic analysis with decoy device context. Using this data, SOC analysts have an end-to-end view of an attacker's actions. They also can monitor endpoints without endpoint agents and obtain contextual, enriched threat intelligence to streamline their investigations.

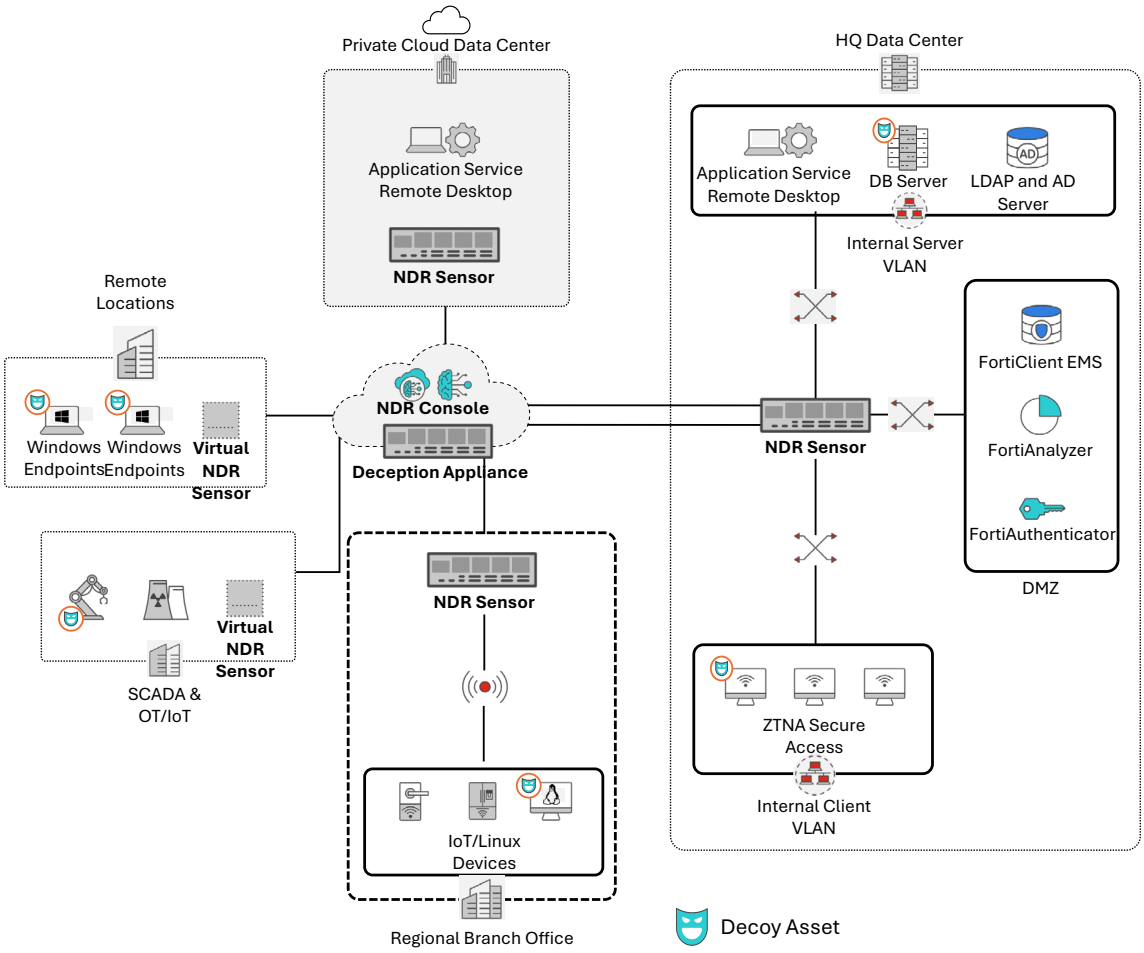

Figure 1: NDR and deception technology deployed in a complex environment

Identifying the Right Solution

Security teams must ensure that their combined NDR and deception solution provides these benefits:

- **Enhanced threat detection:** The solution should use advanced analytics, ML, behavioral analysis, and decoy deployment to detect unusual and malicious activities within network traffic. These capabilities help identify threats that may have bypassed traditional security solutions such as firewalls and antivirus.
- **Visibility across the network:** A solution should provide comprehensive visibility into both internal and external network traffic, including encrypted traffic to help identify hidden threats and maintain security across diverse environments.
- **Integration across the security stack:** The solution should integrate across the security stack and work with other third-party security tools, such as SIEM, EDR, and security orchestration, automation, and response (SOAR) solutions to streamline response efforts.
- **Reduced false positives:** The solution should help reduce security team alert fatigue by proactively reducing false positives. Analysts should only receive actionable detections that can be reasonably investigated while minimizing nuisance alerts and extraneous detections.

Fortinet Helps Stop Attacks Earlier

Using a combination of NDR and deception technologies can help overburdened security teams because it proactively searches for attackers and lures them to specific assets across the network. An effective solution provides better visibility, fewer false positives, and advanced threat detection.

The network detection security solution from Fortinet combines NDR and deception technology to streamline response and lower the workload for security teams by stopping attacks earlier in the attack life cycle.

[1] Enterprise Strategy Group, The Quantified Benefits of Fortinet Security Operations Solutions: Improved Security Team Operational Efficiency and Reduced Risk to the Organization, Each by Up to 99%, January 2025.

[2] Ibid.

April 4, 2025 9:00 PM / MKTG-1148-0-0-EN