SOLUTION BRIEF

Find and Stop Threats with the Fortinet Network Detection Security Solution

Executive Summary

Attackers must continuously evolve their techniques to avoid detection. They often combine malicious activity with network traffic and use encrypted channels to exfiltrate data, so it can be challenging to discover and distinguish between genuine and malicious activities. By analyzing suspicious activity from multiple sources, including network metadata and deployed decoy devices, security teams can get high-fidelity detections of unknown attacks and weak indicators of malicious activity and stop evolving threats more quickly.

The Fortinet Network Detection Security solution combines advanced analytics, machine learning, behavioral analysis, and decoy deployment to detect unusual and malicious activities within network traffic. The solution helps overburdened security teams find and stop advanced threats that may bypass traditional security solutions like firewalls and antivirus.

According to an Economic Validation report from the TechTarget Enterprise Strategy Group, it can take an average of 168 hours or more to identify threats, and many are never detected.[1]

Improve Threat Visibility Across Complex Network Architectures

Organizations with large, complex networks inevitably have blind spots, which means high volumes of network traffic may not be monitored. This traffic often includes unmonitored devices that are connected to the network but do not support endpoint detection and response (EDR) agents, such as operational technology (OT), Internet of Things (IoT), and bring your device (BYOD) technology. Attackers can use network blind spots to hide and use common administrative tools that may go unnoticed by agent-based detection techniques.

Security operations center (SOC) teams also face an overwhelming number of alerts from various security tools. Many alerts are false positives, leading to alert fatigue, so potentially critical threats are overlooked or never investigated.

The Fortinet Network Detection Security Solution

The Fortinet Network Detection Security solution combines the power of network detection and response with deception technology. This combination provides behavior-based metadata analysis on known and unknown threats while expanding visibility across complex networks and improving response capabilities.

FortiNDR Cloud network detection and response

FortiNDR Cloud leverages artificial intelligence (AI), machine learning (ML), and behavioral and human analysis to analyze network metadata, detecting malicious behavior and anomalies across multi-cloud and hybrid environments. It collects and analyzes network traffic metadata across Layer 2 through Layer 7, including domain name system (DNS), IPs, HTTP, remote desktop protocol (RDP), server message block (SMB), and encrypted traffic. Metadata is retained for 365 days for retrospective analysis and threat hunting.

FortiNDR Cloud analyzes metadata because network metadata cannot be manipulated by an attacker, making it a reliable “source of truth” for analysts looking to discover evidence of a sophisticated attack.

FortiDeceptor deception technology

FortiDeceptor lures attackers into revealing themselves early in the reconnaissance stage by engaging with a wide range of deception assets distributed throughout the network environment. The platform generates high-fidelity alerts based on real-time engagement with attackers and malware, providing attack activity analysis and attack isolation.

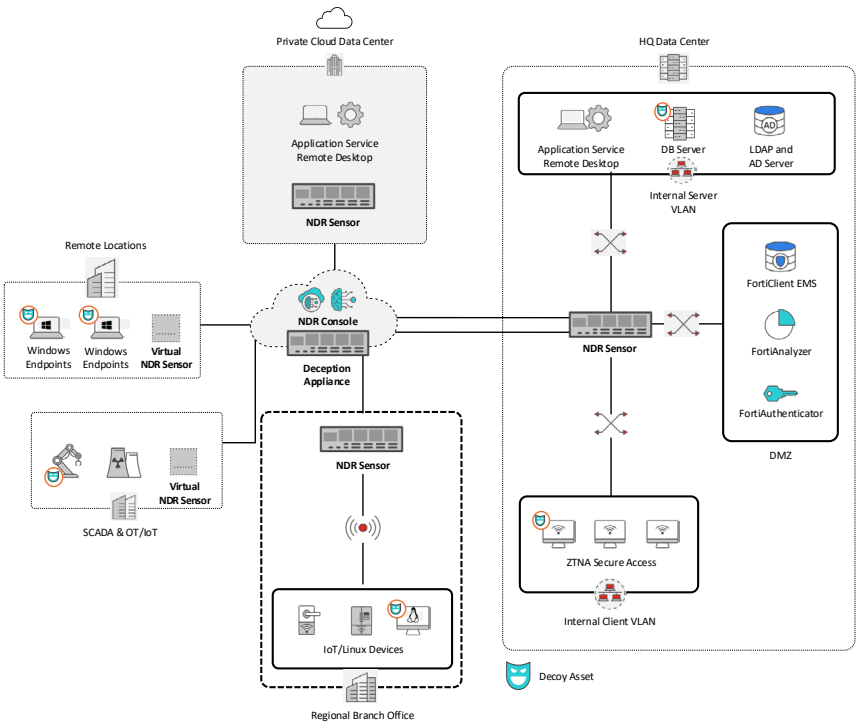

Figure 1: The Fortinet Network Detection Security solution

Streamline Detection and Response Across Complex Networks

The Fortinet Network Detection Security solution provides tangible benefits to resource-constrained security teams. It enhances visibility across complex networks and offers these benefits:

Enhanced threat detection: The solution uses advanced analytics, ML, behavioral analysis, and decoy deployment to detect unusual and malicious activities within network traffic. It helps identify threats that may bypass traditional security solutions like firewalls and antivirus.

Visibility across the network: The solution offers comprehensive visibility into internal and external network traffic, including encrypted traffic. It helps identify hidden threats and maintain security across diverse environments.

Integration across the Fortinet Security Fabric: The solution integrates with the Fortinet Security Fabric and other third-party security tools, such as security information and event management (SIEM), EDR solutions, and security orchestration, automation, and response (SOAR) to streamline response efforts.

Expedite Investigation and Response

The Fortinet Network Detection Security solution brings network detection, response, and deception technology together, offering unparalleled visibility and high-fidelity detection of unknown threats and weak indicators of malicious activity across network domains.

Combining AI-based behavioral network traffic analysis with decoy device context gives security teams an end-to-end view of an attacker's actions. The Network Detection Security solution identifies unmonitored endpoints and obtains contextual, enriched threat intelligence with endpoint data to give security teams unparalleled response capabilities.

[1] Enterprise Strategy Group Economic Validation, The Quantified Benefits of Fortinet Security Operations Solutions, January 2025.

Copyright © 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

March 26, 2025 10:34 AM
MKTG-1147-0-0-EN