SOLUTION BRIEF

Detect and Investigate Known and Unknown OT-Based Attacks with Fortinet NDR Solutions

Executive Summary

As organizations bring more IT, IoT, and OT devices online, security practitioners are tasked with safeguarding their expanding attack surfaces in the face of increasing intrusions. This explosive growth in intrusions underscores the complexities of securing these environments.

Network detection and response (NDR) is vital to any robust security strategy, particularly given the growing number of IoT and OT devices that teams must secure. Fortinet NDR solutions are built for hybrid, on-premises, air-gapped, and OT environments. The solutions use artificial intelligence (AI) and machine learning (ML) to analyze network traffic to identify known and unknown network attacks and provide full agentless visibility that spans IT/OT environments so analysts can detect, investigate, and respond to threats that evade perimeter defenses.

Fortinet NDR solutions collect network traffic from cloud, hybrid-cloud, IT, and OT infrastructures to identify malicious network activity and files. They use multiple network and OT protocols and numerous unique application control signatures for real-time identification of advanced threats, including insider threats and zero-day attacks, ultimately improving incident response capabilities.

Of those organizations that suffered a breach in 2023, nearly half of respondents indicated both IT and OT systems were impacted, up from 32% last year.[1]

Challenges Related to Securing Diverse OT Environments

Legacy OT systems are often vulnerable to attacks because they run outdated software and firmware that leaves systems open to attack. Standard security activities like vulnerability tracking and patching, sharing threat intelligence, and signature profiling are often unavailable in OT environments. Additionally, endpoint agents cannot be deployed, which can leave critical infrastructure unpatched or unmonitored. In a recent survey of OT organizations, nearly one-third of respondents had six or more intrusions, up from only 11% in 2023.[2] It was also notable that all types of intrusions increased, except malware.

NDR Solutions for Comprehensive Visibility across IT and OT Networks

Fortinet offers two NDR solutions: Software-as-a-Service (SaaS) and on-premises for hybrid, on-premises, air-gapped, or OT environments. The solutions provide intelligence, correlation, and identification of anomalous and malicious activity throughout complex hybrid networks so security teams can respond quickly to attacks in progress using network metadata analysis, AI, and ML across the Fortinet Security Fabric.

Fortinet NDR solutions analyze all traffic and activity to provide continuous detection, complete visibility, and file and malware analysis across complex OT environments. The solutions correlate network metadata, file, and malware analysis, as well as OT-specific vulnerability information, to provide security teams with a comprehensive, prioritized picture of current risks. It includes the existing paths to exploitation, which can help security teams identify and prioritize remediation needs.

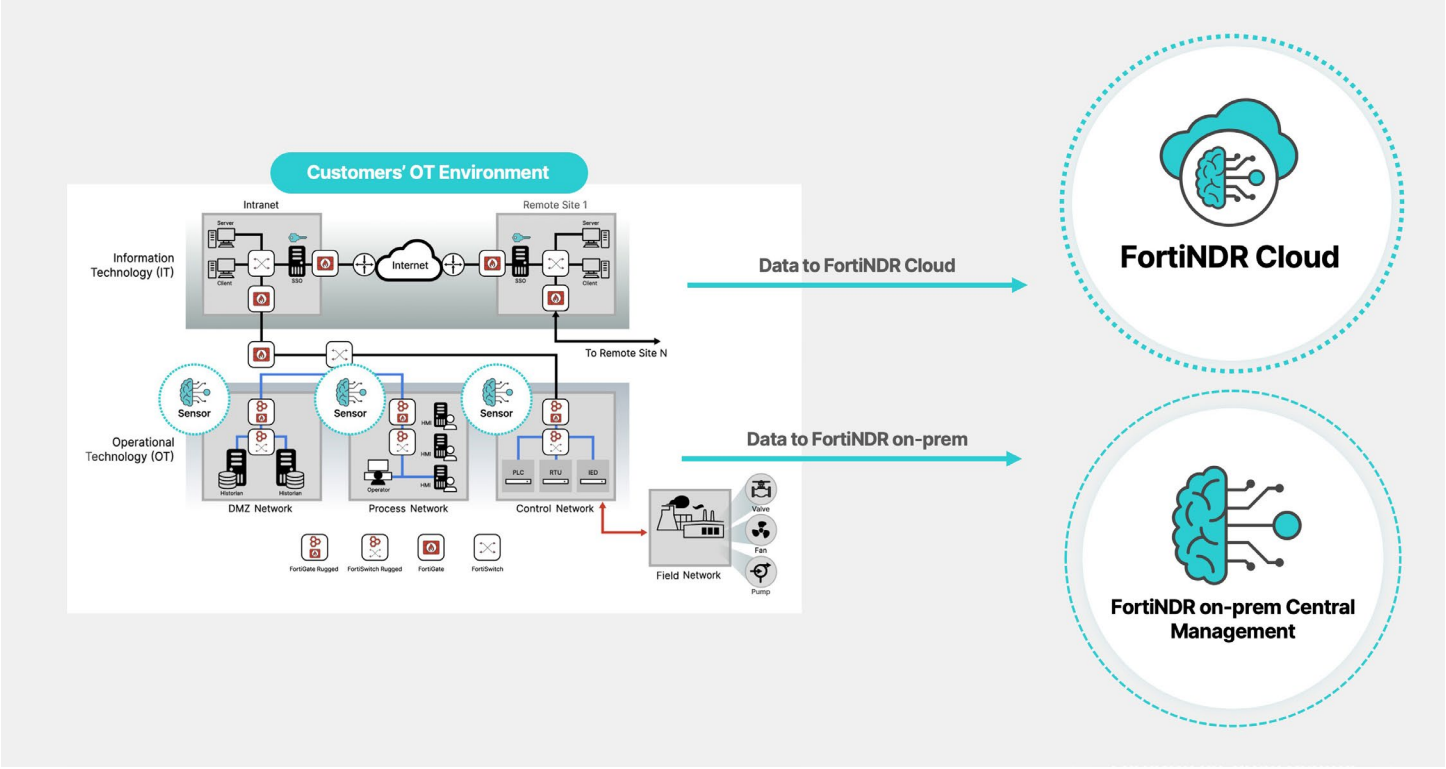

Figure 1: NDR sensors can be deployed across your OT environment at the DMZ, process network, or control network to provide continuous visibility.

Security teams using Fortinet NDR solutions benefit from:

- **AI-powered threat detection:** Fortinet NDR solutions leverage AI and ML to identify suspicious and anomalous network activity. The on-premises FortiNDR solutions use artificial neural networks trained to identify OT-specific malware to detect malicious network activity and files for real-time threat identification. Security teams can also use ML features to set baselines and profile traffic in both IT and OT networks to help detect anomalies and highlight suspicious traffic.
- **Integration with FortiGuard Labs threat intelligence**: The NDR solution capabilities are augmented with OT-specific threat intelligence from FortiGuard Labs to help security teams identify attacks faster. The intelligence is continuously updated from FortiGuard Labs to ensure all OT-related signatures and protocols are up to date and removing the need for tedious, manual updating.
- **An always-on device inventory mechanism**: When devices come online or go offline and are dynamically reassigned IP addresses, building an accurate device inventory is difficult. FortiNDR uses network metadata analysis to continuously monitor network traffic and create an accurate device inventory across IT and OT networks without the use of endpoint agents. For every discovered device, FortiNDR builds a profile that includes the device type, operating system, Active Directory hostname, and vendor, product, and firmware version. It also provides insights into the protocols that the devices may have used. Analysts can use the insights to identify policy violations, malicious activity, and potential threats.

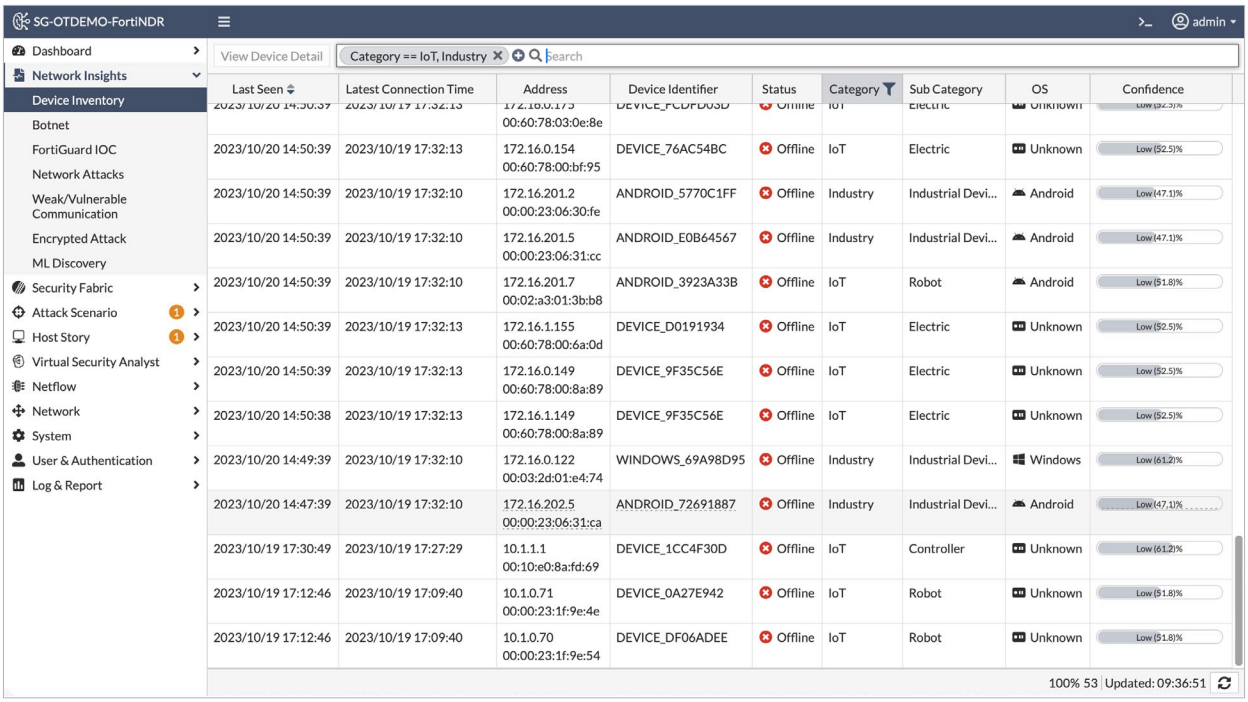

Figure 2: The FortiNDR on-premises solution provides a detailed device inventory with information including operating system, device type, and Active Directory hostname.

- **Application control and protocol support for OT networks:** FortiNDR combines application control and intrusion protection system (IPS) signatures that are developed specifically for OT, which speeds detection and protection against network-level threats. FortiNDR applies ML and AI to identify malicious activity across 18 different OT-specific network protocols, including Modbus TCP, BACnet, and OPC. The solution also monitors more than 1,850 unique application control signatures within these protocols for specific security policy rules that can be applied to the various OT systems communicating in the network.
- **OT environment rules and queries:** Security analysts can use Fortinet NDR solutions to investigate network data and hunt for evidence of attacker activity and create custom detection rules across 365 days of network events and common OT protocols.

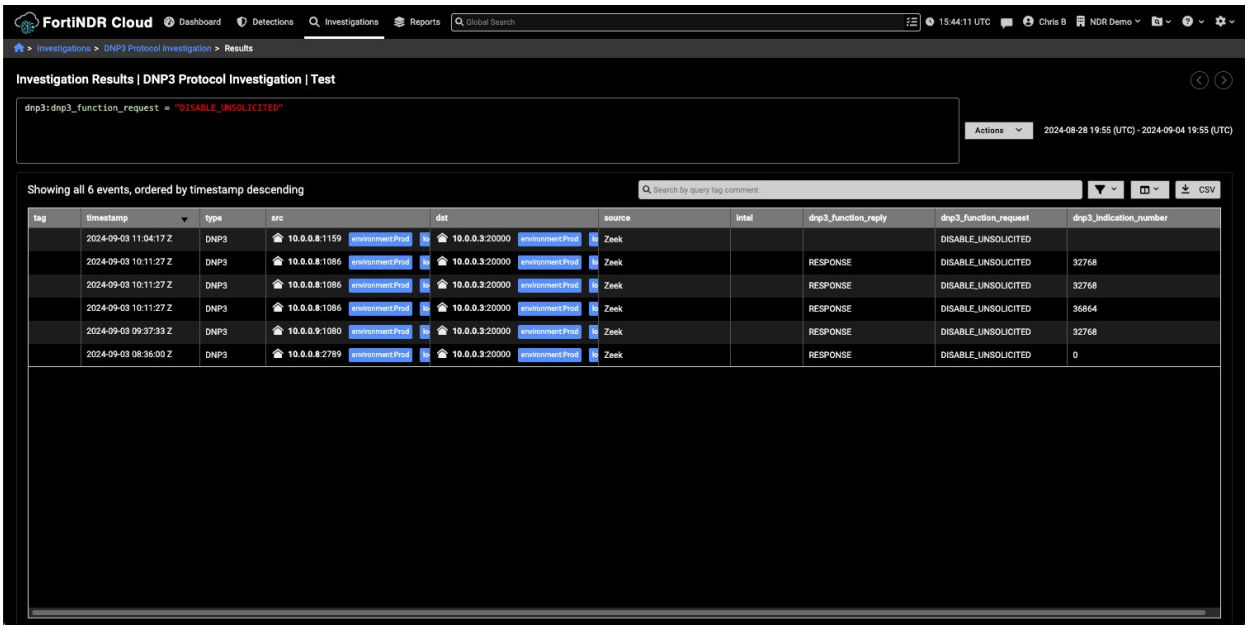

Figure 3: FortiNDR cloud OT investigation results with a list of events.

- **OT-specific malware detection**: Fortinet NDR solutions leverage AI, ML, and artificial neural networks to detect and analyze cyberthreats targeting industrial networks to find unknown threats across OT and IT environments without the need for endpoint agents.
- **Easy integrations to power rapid response**: Through integrations with Fortinet Security Fabric tools such as FortiGate Next-Generation Firewalls, FortiNAC network access control, FortiSIEM security information and event management, and FortiSOAR security orchestration, automation, and response, FortiNDR alerts can trigger automated mitigation actions on affected endpoints. In-depth reporting is also available using FortiAnalyzer.

Protocols

- BACNet
- CIP
- CoAP
- DNP3*
- ELCom
- ETHERNET_IP
- HART
- IEC104
- KNXnet_IP
- LONTALK
- PROFINET
- MMS(TSAP)
- MODBUS*
- NFP
- NMXSVC
- OPC
- S7(TSAP)
- Synchrophasor

Vendor Applications

- 3S-Smart
- 7 Technologies
- ABB
- Advantech
- AzeoTech
- B&R
- Beckhoff
- Broadwin
- CODESYS
- CirCarLife
- CitectSCADA
- Cogent
- DATAC
- Delta
- Dut
- Eaton
- Fuji
- GE
- Gemalto
- Guardzilla
- IBM
- Iconics
- Indusoft
- Intellicom
- KeySight
- KingScada
- KingView
- Korenix
- LAquis
- Measuresoft
- Microsys
- Mitsubishi
- Moxa
- Nordex
- OMRON
- PcVue
- QNX
- RSLogix
- RealFlex
- Rockwell
- Schneider
- SE
- Siemens
- Sunway
- TeeChart
- WECON
- WellinTech
- Yokogawa

*Investigation support

Figure 4: Supported vendor applications and protocols

Get Full Visibility and Centralized Management across Your Entire Network

FortiNDR provides centralized management with flexible deployment options. It can be deployed in a hub-and-spoke model with a single centralized management appliance and multiple sensors or as individually managed devices deployed across the environment. These deployment models ensure FortiNDR can monitor network traffic across the entire network infrastructure.

As the threat landscape expands and evolves, security teams need complete visibility into the types of network traffic reaching their IT and OT environments. FortiNDR solutions can help with rapid analysis and threat detection and improved visibility for faster response across OT and IT environments. To learn more about Fortinet solutions for OT, visit the Secure Operational Technology page on Fortinet.com.

[1] 2024 State of Operational Technology and Cybersecurity Report, Fortinet, June 12, 2024.

[2] Ibid.

FORTINET

www.fortinet.com

September 17, 2024 1:41 PM

2437799-0-0-EN