SOLUTION BRIEF

Detect Known and Unknown OT-Based Attacks with FortiNDR

Executive Summary

As organizations bring more IT, IoT, and OT devices online, security practitioners are tasked with safeguarding their expanding attack surfaces. Yet this explosive growth in devices underscores the complexities of securing these assets. Case in point: Nearly 80% of respondents in a recent survey reported having over 100 IP-enabled OT devices in their environments, and three-fourths of OT organizations reported suffering at least one breach in the past year.[1]

That's why 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. FortiNDR is built for on-premises, air-gapped, and OT environments, leveraging AI and ML to analyze network traffic to identify known and unknown network attacks. The solution gives security teams full agentless visibility, spanning IT/OT environments so that analysts can detect, investigate, and respond to threats evading perimeter defenses.

Of those organizations that suffered a breach in 2023, nearly one-third of respondents indicated both IT and OT systems were impacted, up from 21% last year.[2]

FortiNDR collects network traffic from the cloud, hybrid-cloud, IT, and OT infrastructures to identify malicious network activity and files using multiple network and OT protocols and numerous unique application control signatures within these protocols. This results in the real-time identification of advanced threats, including insider threats and zero-day attacks, which ultimately improves incident response capabilities.

Challenges Related to Securing Diverse OT Environments

Legacy OT systems are often vulnerable to attacks, typically running outdated software and firmware that leaves systems open to attack.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, leaving critical infrastructure unpatched or unmonitored.

Security professionals need a reliable way to detect and stop attacks across OT and IT environments without using endpoint agents early in the attack life cycle.

FortiNDR for Comprehensive Visibility Across IT and OT Networks

FortiNDR is a purpose-built NDR solution for on-premises, air-gapped, and OT environments. It provides security teams with intelligence, correlation, and identification of anomalous and malicious activity throughout complex hybrid networks. FortiNDR allows security teams to respond quickly to attacks in progress using network metadata analysis, AI and ML, and integrations across the Fortinet Security Fabric.

FortiNDR provides continuous detection, complete visibility, and file and malware analysis across complex OT environments by analyzing all traffic and activity. FortiNDR then correlates network metadata, file and malware analysis, and OT-specific vulnerability information to provide security teams with a comprehensive, prioritized picture of current risks—including existing paths to exploitation—which ultimately helps practitioners identify and prioritize remediation needs.

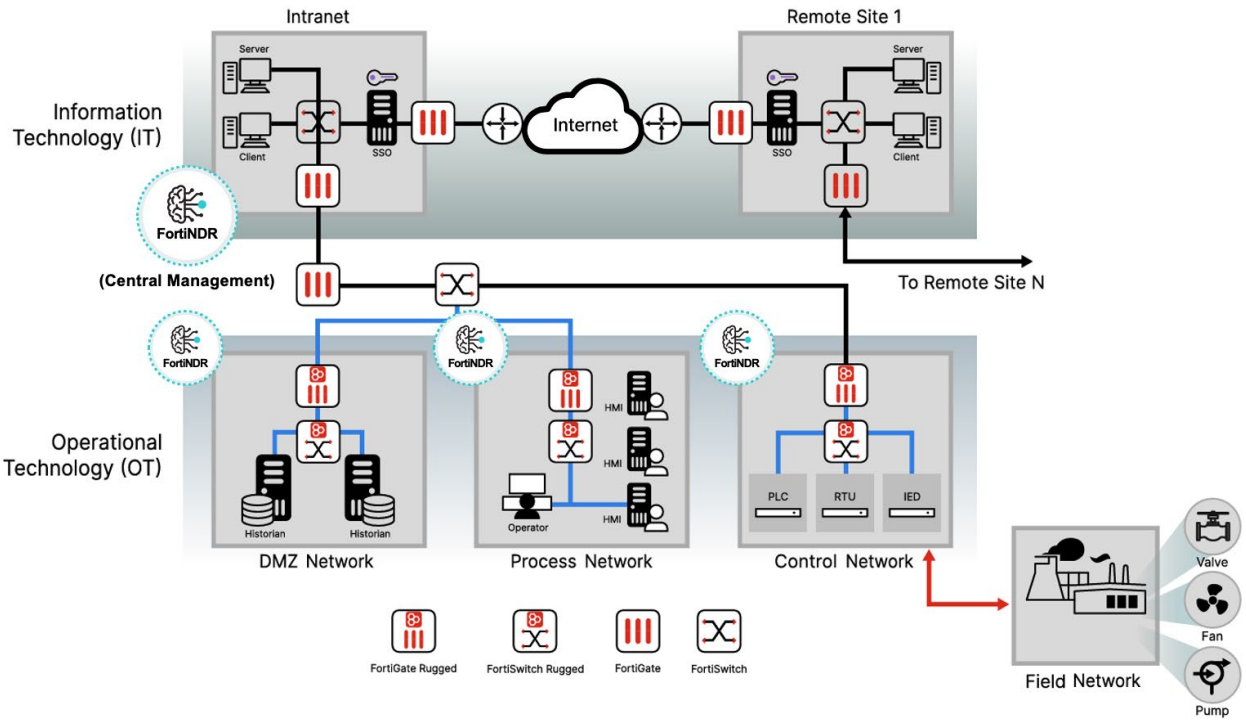

Figure 1: FortiNDR sensors can be deployed across your OT environment at the DMZ, process network, or control network to provide continuous visibility.

When security teams choose FortiNDR, they benefit from:

- **AI-powered threat detection:** FortiNDR uses Artificial Neural Networks (ANN), trained to identify OT specific malware, to detect malicious network activity and files, resulting in real-time advanced threat identification, including insider threats and zero-day attacks, improving incident response capabilities. Security teams can also use ML features to baseline and profile traffic in both IT and OT networks and detect anomalies, highlighting suspicious traffic.
- **Integration with FortiGuard Labs threat intelligence:** By augmenting FortiNDR capabilities with OT-specific threat intelligence from FortiGuard Labs, security teams can identify attacks faster. Using continuously updated intelligence from FortiGuard Labs, FortiNDR ensures all OT-related signatures and protocols are up to date, removing the need for tedious, manual detection updating.
- **An "always-on" device inventory mechanism:** As new devices come online or go offline and are dynamically reassigned IP addresses, building an accurate device inventory becomes increasingly difficult. FortiNDR uses network metadata analysis to continuously monitor network traffic and create an accurate device inventory across IT and OT networks without endpoint agents. For every discovered device, FortiNDR builds a profile that includes, for example, the device OS, type, and Active Directory hostname, and provides insights into protocols that those devices may have used. Analysts can use FortiNDR insights to identify policy violations, malicious activity, and potential threats for quick remediation.

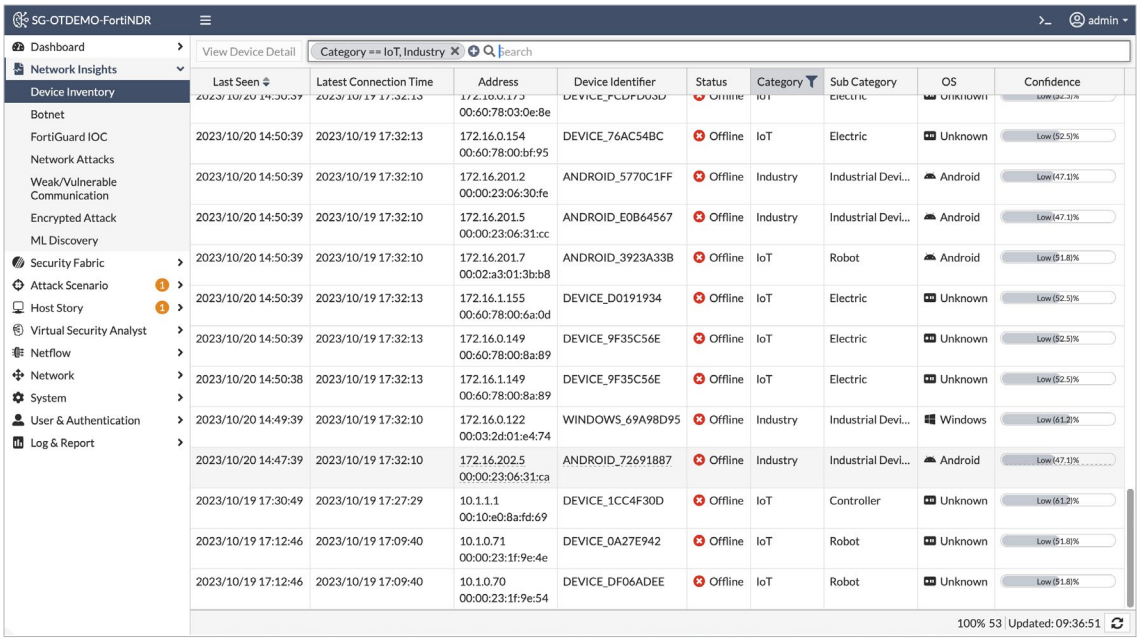

Figure 2: FortiNDR provides a detailed device inventory, providing information such as OS, device type, and AD hostname.

- **Application control and protocol support for OT networks:** FortiNDR combines application control and IPS signatures that are developed specifically for OT, enabling rapid 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-specific malware detection with the FortiNDR Virtual Security Analyst™ (VSA):** The FortiNDR VSA™ leverages AI, ML, and artificial neural networks to detect and analyze cyberthreats targeting industrial networks. The VSA™ speeds the analysis of known and 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 via 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

Figure 3: Vendor applications and protocols supported by FortiNDR

Get Full Visibility and Centralized Management Across Your Entire Network

FortiNDR offers security teams centralized management with flexible deployment options. FortiNDR 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.

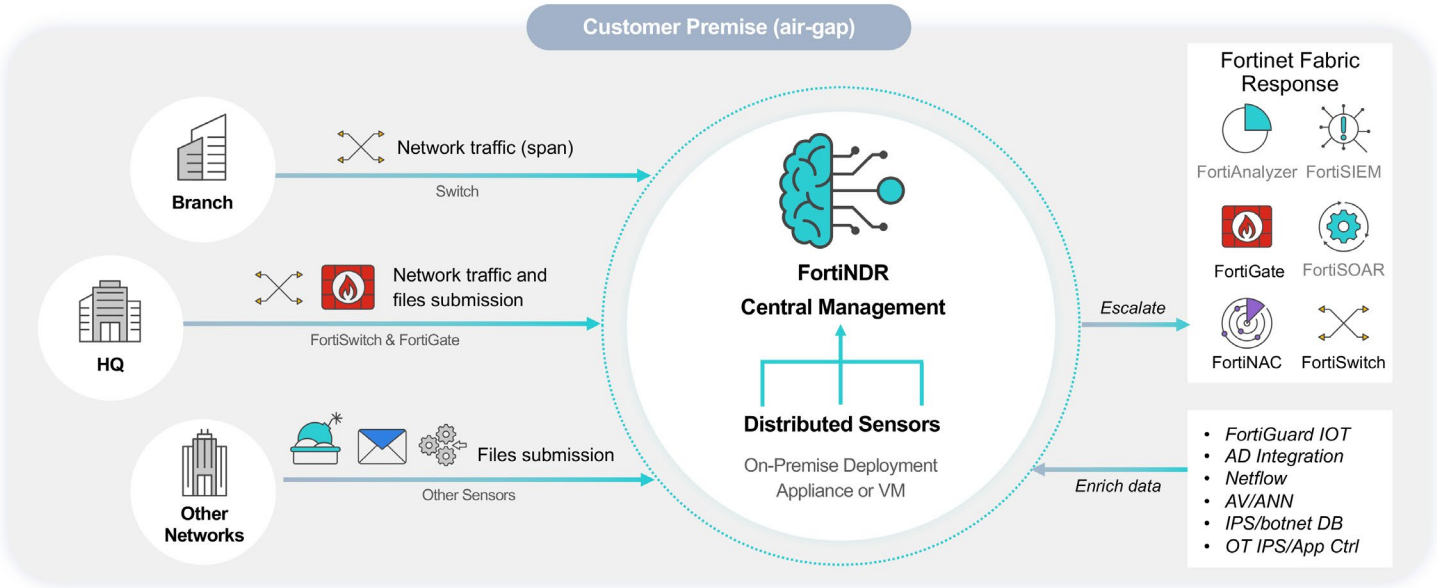

Figure 4: The hub-and-spoke FortiNDR deployment

Conclusion

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 provides:

- **Rapid analysis and threat detection:** Harness the FortiNDR VSA to assist with identifying attacks, using neural networks to classify OT-based malware to improve threat identification and understand the scope of an attack.
- **Improved visibility across OT and IT environments:** FortiNDR uses network traffic analysis, AI, and ML to identify malicious network activity across your entire network without endpoint agents.
- **Faster response:** FortiNDR provides AI-powered traffic analysis and integrations across the Fortinet Security Fabric and various third-party tools. These easy integrations simplify configuring, monitoring, and stopping attacks spanning IT and OT environments and enable an automated, orchestrated response.

[1] 2023 State of Operational Technology and Cybersecurity Report, Fortinet, May 24, 2023.

[2] Ibid.

FORTINET

www.fortinet.com

January 4, 2024 4:48 PM
2437799-0-0-EN