

SOLUTION BRIEF

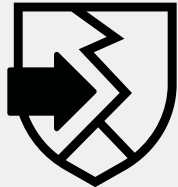
Quickly Respond to Attacks Across Your Network

Executive Summary

As attackers become more adept at hiding their activities in network traffic, security teams need a solution that analyzes and correlates network artifacts to spot potentially malicious activity. Network detection and response (NDR) technology fills that gap, providing security teams with intelligence, correlation, and identification of anomalous and malicious activity throughout complex hybrid networks and air-gapped, containerized, and cloud environments. Fortinet provides customers with two NDR deployment options, FortiNDR Cloud is SaaS-based while FortiNDR is designed for on-premises deployments.

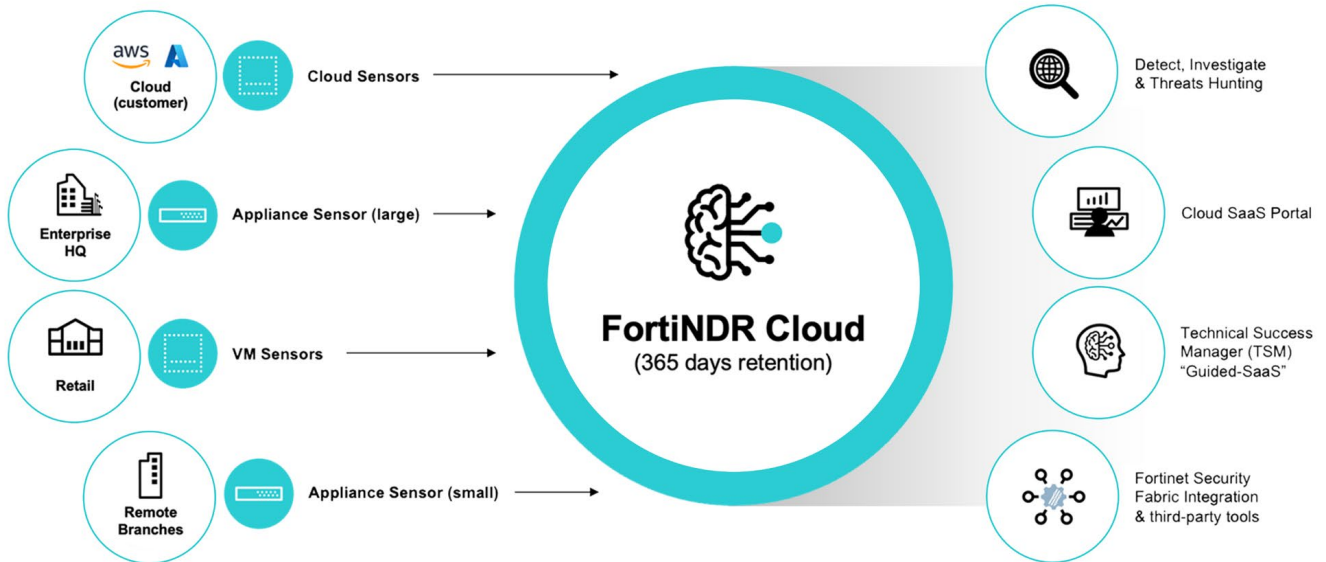
Detect and Stop Network Threats Faster with FortiNDR Cloud

SaaS-based FortiNDR Cloud leverages artificial intelligence (AI) and machine learning (ML), behavioral, and human analysis to inspect network traffic, including encrypted traffic, to detect malicious behavior early while reducing false positives. FortiNDR Cloud provides unified network traffic visibility across multi-cloud and hybrid environments, distributed workforces, and constrained, mission-critical environments.



Fortinet NDR solutions received the highest score possible in the Threat Detection and Detection Technologies criteria.¹

FortiNDR Cloud Architecture



Get expertise on demand

FortiNDR Cloud helps security teams overcome the skills gap challenge by providing in-person technical success manager (TSM) support. TSMs are trusted advisors who share findings, tune configurations, and help organizations optimize NDR deployments.



Combine AI and human analysis for effective response

By analyzing data attributes across Layer 2 through Layer 7, including Domain Name System (DNS), HTTP, Remote Desktop Protocol (RDP), Server Message Block (SMB), and encrypted traffic using AI and ML, FortiNDR Cloud automatically identifies anomalous and malicious behavior, provides risk scores, and shares relevant threat intelligence to assist security teams in prioritizing response efforts. FortiGuard Labs threat experts continually refine ML-driven models and update detections, resulting in high-fidelity alerts and out-of-the-box playbooks for faster investigations and threat hunting.

365-day data retention for retrospective analysis and threat hunting

Defenders need adequate data to effectively conduct in-depth analysis and prioritize response efforts. FortiNDR Cloud retains rich network metadata for 365 days, enabling a comprehensive investigation. This data ensures that newly discovered tools, tactics, and procedures can be retroactively investigated to discover if and when threats may have infiltrated the organization's network.

Globally crowdsourced threat intelligence

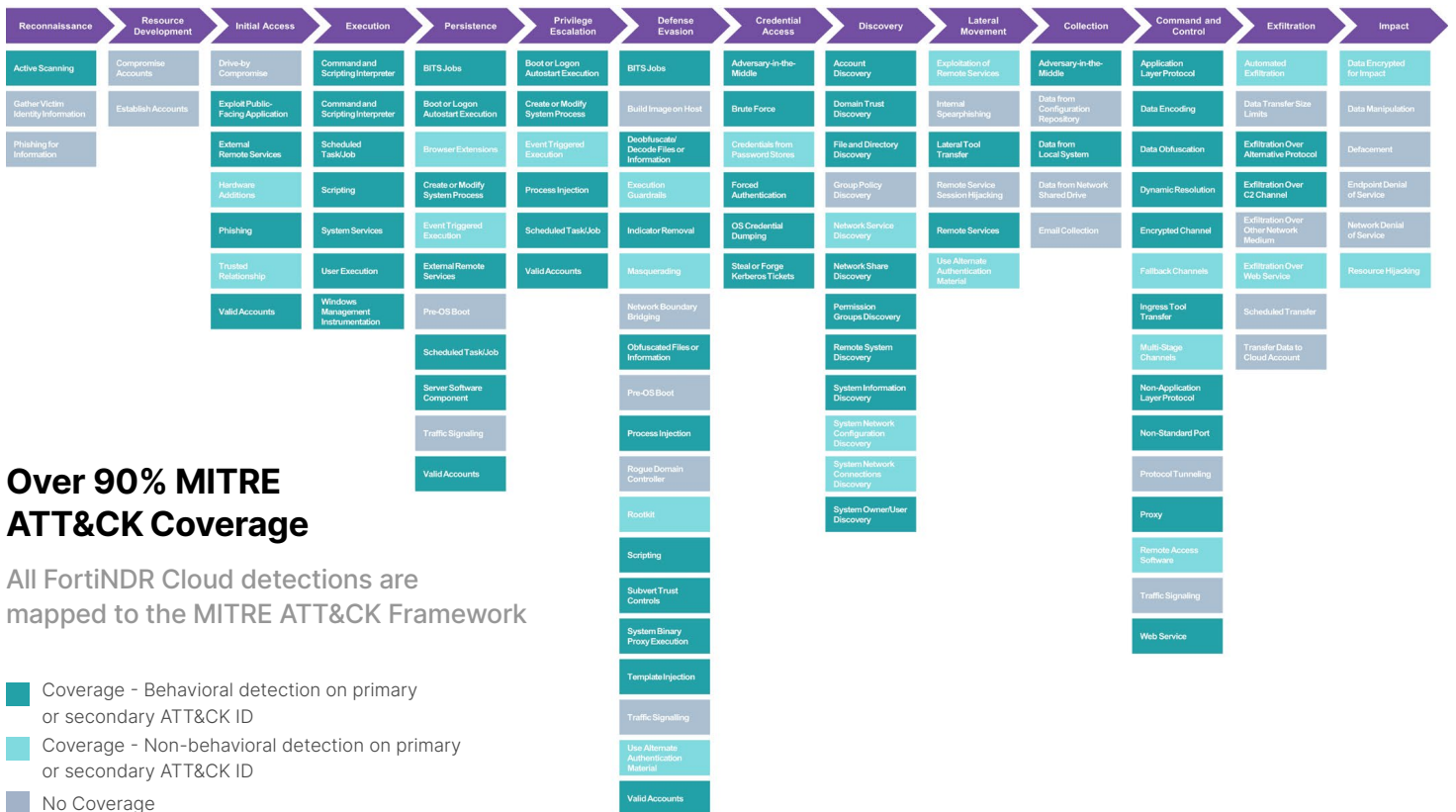
FortiNDR Cloud continually ingests network telemetry from numerous data sources, such as third-party feeds and proprietary sensors, to enhance detection capabilities, ensuring protection against advanced threat techniques, tactics, and procedures.

Orchestrated response

FortiNDR Cloud allows security teams to pivot from detection, to investigation, to threat hunting and response with a few clicks. It provides integrations with the Fortinet Security Fabric and numerous third-party solutions, such as EDR, SOAR, SIEM and XDR, ensuring you can automate investigations, triage, and remediation.

Comprehensive coverage of MITRE ATT&CK tactics, techniques, and procedures

Detections and observations from FortiNDR Cloud cover over 90% of MITRE ATT&CK techniques, ensuring analysts understand adversary tactics, techniques, and procedures (TTPs). These detections, and their associated MITRE ATT&CK mapping, extend into guided playbooks and associated next-step recommendations so that even entry-level analysts can understand what is happening and why it is important.



Over 90% MITRE ATT&CK Coverage

All FortiNDR Cloud detections are mapped to the MITRE ATT&CK Framework

- Coverage - Behavioral detection on primary or secondary ATT&CK ID
- Coverage - Non-behavioral detection on primary or secondary ATT&CK ID
- No Coverage



FortiNDR for Air-Gapped Environments

Mission-critical infrastructure and air-gapped environments must meet additional confidentiality, integrity, and availability requirements. FortiNDR operates in an isolated environment, ensuring secure operations while providing deep insight into IT and OT network traffic.

Non-intrusive, automated inventory discovery and analysis

Using a combination of NetFlow, Azure AD integration, and AI and ML to classify known and unknown devices communicating across the entire network, FortiNDR eliminates network blindspots. The technology identifies devices across your network and pinpoints malicious network activity and files.

Real-time detection

The FortiNDR Virtual Security Analyst leverages ML and artificial neural networks to detect malicious files and network anomalies, such as encrypted attacks via JA3 hashes, malware-based behaviors such as ransomware, downloaders, and coin miners, and attack origins such as worm infections.

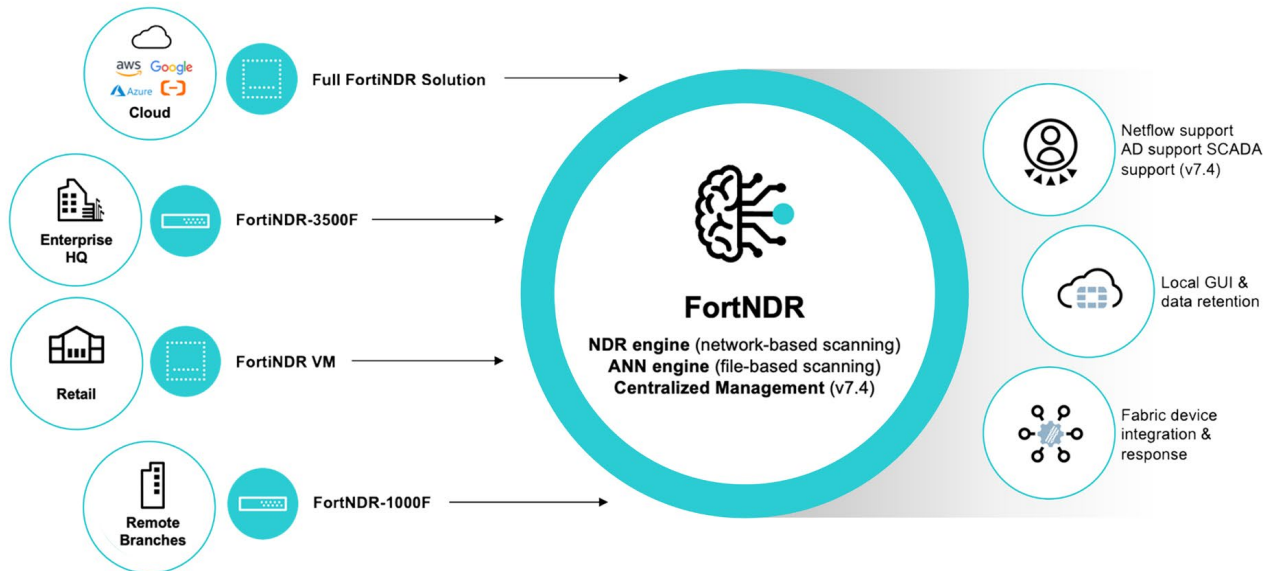
Enriched intelligence for orchestrated response

FortiNDR integrates with the Fortinet Security Fabric for fast response and attack isolation. The solution continually ingests FortiGuard Labs intelligence, providing up-to-date network detection capabilities based on hashes and similar variants in the network.



According to an Economic Validation report from TechTarget's Enterprise Strategy Group, it can take 168 hours or more, on average, to identify threats, while many threats are never detected.²

FortiNDR Architecture



Conclusion

As organizations evolve and the threat landscape grows increasingly complex, Fortinet NDR solutions help security teams simplify operations, gain efficiencies, and enhance risk management efforts. With Fortinet NDR solutions, teams get:

- **Improved threat visibility:** Real-time, automated investigation of network security incidents and extended historical network visibility enable a faster, more comprehensive response to threats. Because the impact of an intrusion increases over time, real-time response is the best way to minimize damage.
- **Virtual or human expertise when it matters most:** Virtual security analysts or TSMs ease high-pressure scenarios with on-call advice.
- **Fewer distractions from false positives and detection tuning:** With real-time threat analysis and detection tuning, organizations are less vulnerable while awaiting a vendor's application patch or anti-malware signature.

¹ ["Forrester Network Analysis and Visibility Wave Report, Q2 2023"](#)

² ["Enterprise Strategy Group Economic Validation, The Quantified Benefits of the Fortinet Automated SOC,"](#) June 2023.

