SOLUTION BRIEF

FortiNDR Proactively Identifies and Responds to Network Intrusions

Executive Summary

Getting insights from “big data” has been a growing trend in many industries, including cybersecurity. By harnessing this information using artificial intelligence (AI), cybersecurity leaders can perform thorough analyses of cyberattacker behaviors and identify those that may have evaded traditional detection methods.

FortiNDR applies AI—including machine learning (ML) and deep learning (DL)—as well as other analytics to an organization’s network traffic metadata to improve security operations center (SOC) efficiency while also providing high-fidelity adversary detections for a rapid and informed response. By blending the latest AI/ML-driven breach protection technology with historical visibility into network data and human expertise, FortiNDR is redefining how network detection and response are delivered.

The evolution of AI, ML, and DL in cybersecurity

Harvesting insights from big data has been a growing trend in many industries, including cybersecurity. Many technology vendors have been using various forms of AI in the fight against cybercriminals for years (at Fortinet, it’s been more than a decade)—most notably in threat detection. Training algorithms use ML/DL to enable increasingly accurate identification of malicious network activity and files, resulting in the real-time identification of advanced threats, including zero-day attacks. For security teams seeking a proactive security posture, leveraging these security technologies is becoming a requirement to stop advanced attacks.

In 2022, security teams needed 277 days, on average, to identify and contain a data breach. Historical visibility into network data is essential for effective response.[1]

However, better threat detection alone does little to make security operations teams feel less overwhelmed. If anything, better detection means an even higher volume of alerts that must be addressed manually. The answer is a balanced approach to threat detection that combines AI/ML with behavioral and human analysis to ensure alerts are high-fidelity and true positives.

Closing the SOC visibility gap

By applying a range of general purpose as well as purpose-specific AI and other analytics, FortiNDR offers unique detection and observations based on the MITRE ATT&CK framework. This allows for the breaking down of the tactics, techniques, and procedures (TTPs) of adversaries into easy to understand format for SOC teams to act upon.

FortiNDR provides:

- Historical visibility and recording of near packet-level metadata on any device, any network, and any traffic, including N | S | E | W and encrypted
- High-fidelity adversary detections that blend machine learning, artificial and crowdsourced intelligence, and behavioral analysis to drive down false positive rates
- Analysts with out-of-the-box triage and investigation tools and 365 days of enriched network metadata for historical investigations
- Integration with the Fortinet Security Fabric and other third-party SIEM solutions by providing detections and observations to threat hunters and incident responders

Cybersecurity Analysts on Your Side

Cybersecurity teams are in a race against time to protect their organizations. With limited knowledge of—or time to learn—the adversary's latest intent, tactics, techniques, or procedures and working without external guidance, the security team must often go it alone. FortiNDR offers the option of virtual or in-person expertise to ensure customers are best positioned to thwart adversaries. Let Fortinet experts do the work to keep you current on the evolving threat landscape.

FortiGuard Applied Threat Research (ATR)

Our seasoned advanced threat researchers monitor cybercriminal activity, perform reverse engineering, and handle detection engineering of adversary behavior with high accuracy. The first-hand knowledge from FortiGuard ATR empowers both the AI and the on-demand technical success managers (TSMs) in advance of and during high-pressure incidents.

Virtual Security Analyst

Operating in unsupervised mode, the FortiNDR Virtual Security Analyst helps SOC teams analyze and investigate new threats while continuously adapting to new and emerging threats.

Eliminating Distractions

Purchasing a security solution should enable security professionals to focus on protecting their organization. However, all too often, security solutions create unnecessary distractions rather than positive results. Many NDR solutions have hidden costs and time tied to providing care and feeding, solution proficiency, addressing false positives, and performing detection tuning—all negating their intended value. FortiNDR includes expertise, virtual or in-person, from product and threat experts to remove distractions.

Zero tuning

FortiGuard Labs performs ongoing detection tuning and QA of all machine learning, behavioral analysis, and threat intelligence detection engines.

Minimal maintenance

The Fortinet TSMs and SaaS Ops teams provide sensor and traffic diagnostics, a fully managed FortiNDR Cloud web portal, and automatic software updates.

Speeding Response

Remediating the often wide-ranging spread of multi-stage cyber campaigns throughout today's digital organizations for a return to safe operation, requires the coordination of actions across multiple security controls and infrastructures.

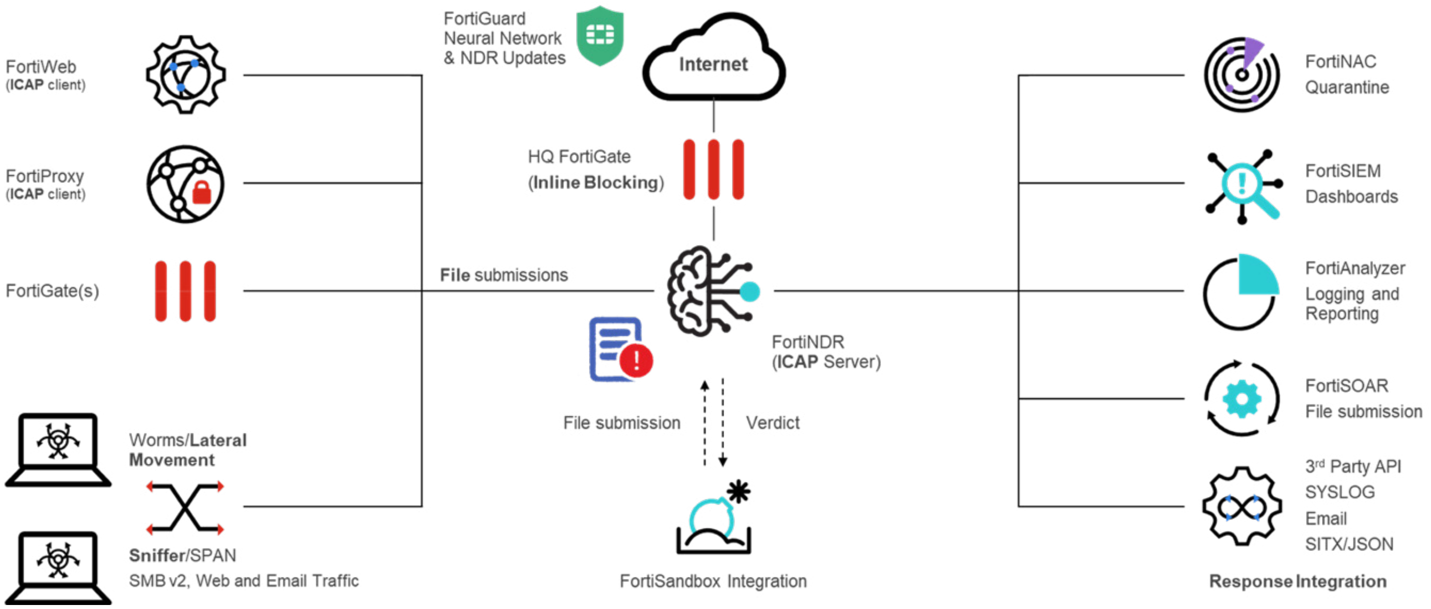
The Fortinet Security Fabric

Designed as a component of a single cybersecurity platform, FortiNDR natively integrates with the Fortinet Security Fabric and other products—from network to email to endpoint security. This facilitates automated response.

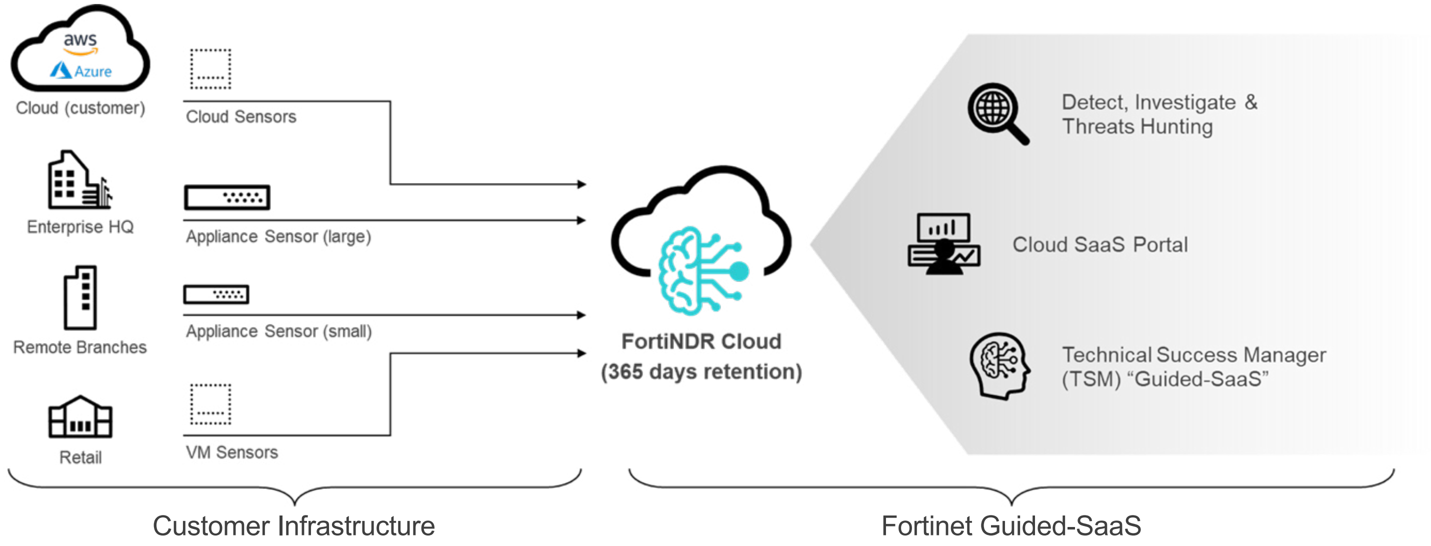
Third-party technologies

Although 75% of organizations report consolidating cybersecurity vendors[2], security infrastructures often maintain some multi-vendor elements. APIs enable additional integration beyond the Fortinet Security Fabric.

FortiNDR (on premises) Architecture and Integration



FortiNDR Cloud Architecture and Deployment



Conclusion

For today's overburdened cybersecurity professionals, FortiNDR helps cybersecurity operations teams move from a reactive to a proactive security posture, while increasing their efficiency and remediating threats faster. FortiNDR delivers these key benefits:

- **Improved visibility of threats.** Real-time, automated investigation of network security incidents and extended historical network visibility enable a faster, more comprehensive response to threats. Since 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 technical success managers ease high-pressure scenarios on your cybersecurity analysts with expertise on your side.
- **Fewer distractions from false positives and detection tuning.** With threat analysis and detection tuning provided in real-time, organizations are less vulnerable while awaiting a vendor's application patch or anti-malware signature.

84% of SOC analysts rank "minimization of false positives" (detection tuning) as the most important SOC activity. Reducing false positives should be the vendor's responsibility.[3]

[1] Cost of a Data Breach Report 2022, IBM Security

[2] Second Annual Study on the Economics of Security Operations Centers: What is the True Cost for Effective Results? 2021 – Ponemon Institute

[3] Ibid