SOLUTION BRIEF

FortiNDR

Helping Security Operations Teams Move from Reactive to Proactive

Executive Summary

Security leaders know that by harnessing "big data," organizations can perform more thorough security analyses and identify attacker behaviors that may have evaded other protection methods. It took 277 days to identify and contain a data breach in 2022, and 69% of security operations center (SOC) analysts cite a lack of visibility into network traffic as the top reason for SOC ineffectiveness.

FortiNDR applies artificial intelligence (AI), including machine learning (ML) and deep learning as well as other analytics to an organization's network traffic "metadata" to gain more insight into attacker behavior. It improves SOC efficiency while providing high-fidelity adversary detections enabling rapid, informed responses. FortiNDR redefines how network detection and response are delivered by blending the latest AI/ML-driven breach protection technology, historical visibility into network data, and human expertise.

In 2022, security teams needed 277 days, on average, to identify and contain a data breach.[1]

The Evolution of Artificial Intelligence, Machine Learning, and Deep Learning 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/deep learning (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.

But 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 and purpose-specific AI and other analytics, FortiNDR offers unique detections and observations based on the MITRE ATT&CK framework, which breaks down tactics, techniques, and procedures (TTPs) of adversaries into an easy-to-understand format for SOC teams to act upon.

Specifically, FortiNDR:

- Provides historical visibility and recording of near packet-level metadata from any device, network, and traffic, including N-S, E-W and encrypted data
- Delivers high-fidelity adversary detections that blend ML, artificial and crowdsourced intelligence, and behavioral analysis to drive down false positive rate.
- Provides analysts with out-of-the-box triage and investigation tools and up to 365 days of enriched network metadata for historical investigations
- Integrates with the Fortinet Security Fabric and other third-party solutions, providing detections and observations to your threat hunters and incident responders

Security Analysts on Your Side

Security 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, 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 our experts do the work to keep up with the evolving threat landscape and keep your teams up to speed.

84% of SOC analysts rank "minimization of false positives" (detection tuning) as the most critical SOC activity.[2]

FortiGuard Threat Experts

Seasoned advanced threat researchers monitor cybercriminal activity, perform reverse engineering, and handle detection engineering of adversary behavior with high accuracy. This first-hand knowledge of FortiGuard empowers both the AI and the on-demand Technical Support Managers (TSMs) of FortiNDR in advance of and during high-pressure incidents.

A Virtual Security Analyst

Operating in unsupervised mode, the FortiNDR Virtual Security Analyst helps SOC teams analyze and investigate new attacks 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, negating their intended value. As mentioned, FortiNDR includes virtual or in-person expertise from product and threat experts to remove distractions.

Zero tuning

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

Minimal maintenance

Fortinet's 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 other Fortinet products from network to email to endpoint security. This facilitates automated response.

Third-party technologies

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

Using AI to learn about specific orgs

To accelerate threat intelligence to machine speed and keep pace with the advanced threat landscape, FortiNDR learns and adapts to new attacks on a specific organization over time, continually improving and optimizing the threat protection life cycle. The result is that FortiNDR supports security operations staff by identifying and analyzing network anomalies in fileless and file-based malware and identifies compromised systems across the organization with 100% certainty—all in less than a second. To do so, FortiNDR uses AI technology to make the decisions that a security analyst would make when manually investigating attacks, including:

- Detecting network anomalies by processing large amounts of north-south and east-west traffic at the perimeter and data center. Using ML to profile, traffic, and detect anomalies and attacks, such as encrypted attacks, malicious web campaigns, botnet-based attacks, intrusions, and more, FortiNDR finds the needle in the haystack for malicious activities on your network.
- Investigation and classification of the attack by tracking the source of the infection with a time stamp and providing complete visibility of the lateral spread from patient zero to all subsequent compromised systems.
- Malware analysis determines the type of malware by features observed by the FortiNDR DNN (Deep Neural Network) and provides an event timeline for each infection event. This is akin to a miniature kill-chain model that describes in scientific terms what the threat tried to do step-by-step, including techniques employed. For example, at "time zero," a download of an HTML file occurred; at "time one," a malicious code exploit took place in a browser; at "time two," a Trojan was downloaded to a user or temp directory. FortiNDR comes prebuilt with over 6 million malware features and learns additional ones over time. As FortiNDR performs these layers of analysis, its full integration with the FortiGate Next-Generation Firewall (NGFW) enables it to identify and block threats. Security operations staff can then apply the intelligence to security controls across the network and other elements of the Fortinet Security Fabric.

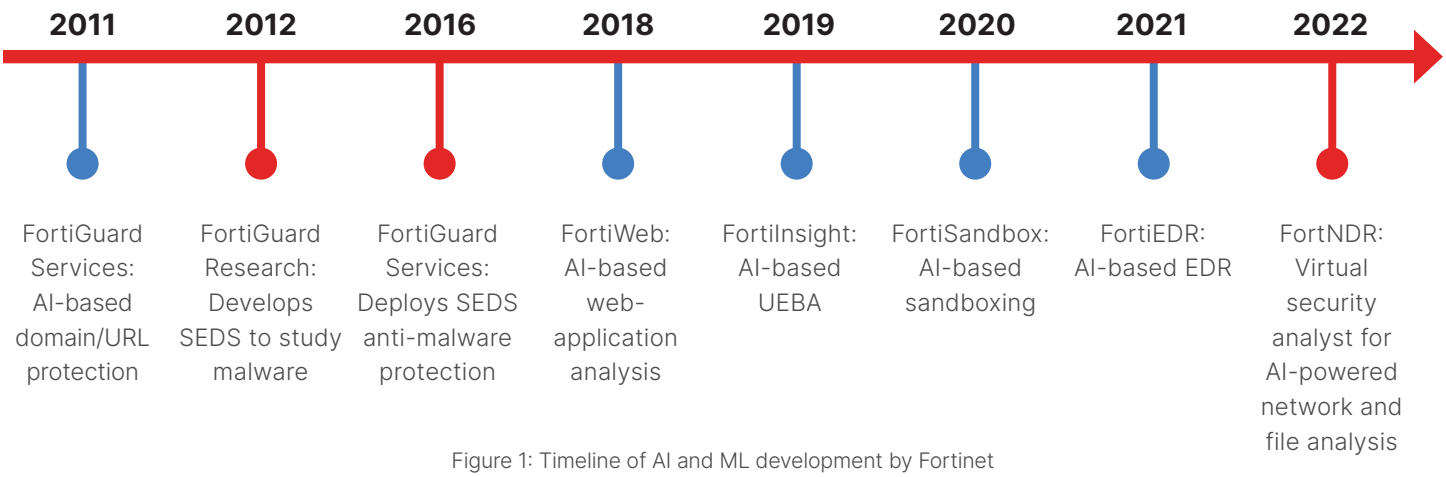

Figure 1: Timeline of AI and ML development by Fortinet

Benefits of FortiNDR

For today's overwhelmed security professionals, FortiNDR helps security operations teams move from a reactive to a proactive security posture while increasing efficiency and remediating threats faster. It delivers key benefits that include:

1. Improved visibility into today's threats. Real-time, automated investigation of network security incidents and extended historical network visibility enable faster, more comprehensive responses to threats. Since the impact of an intrusion increases over time, real-time response is the best way to minimize damage.
2. Virtual or human expertise when it matters most. Virtual Security Analysts or Technical Success Managers ease the high-pressure scenarios your security analysts face with expertise on your side.
3. Fewer distractions from false positives and detection tuning. With threat analysis and detection tuning provided in real-time, organizations are less vulnerable while waiting for a vendor's application patch or anti-malware signature.

[1] IBM, "Cost of a Data Breach 2022."

[2] Bassam Khan, Gigamon, "Introducing Guided-SaaS NDR," June 9, 2021.

March 10, 2023 12:34 PM
594577-B-0-EN