FORTINET | **WINDSTREAM ENTERPRISE**

POINT OF VIEW

The Need for AI-Powered Threat Protection, Scalability, and Efficiency

Boost Protection While Reducing Complexity and Operational Overhead

Executive Summary

In cybersecurity, the use of artificial intelligence (AI) makes it easier and faster for cybercriminals to develop new, more capable, and compelling threats, including zero-day threats. But the flip side is that many cybersecurity vendors have taken advantage of AI technologies for years. As already overloaded security and IT teams face emerging AI-based threats, their cybersecurity solutions must incorporate AI while being efficient and scalable to meet these new demands.
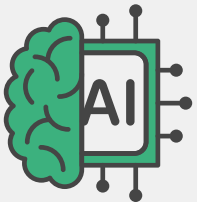
The Balancing Act

Today, the use of AI by bad actors amplifies the urgency for security and IT teams to secure their digital infrastructures from these new AI-based cyberthreats. However, adding more technology also means that staff must learn how to use more consoles and manage additional alert streams for triage and investigation. Unfortunately for overworked teams, adding more security doesn't necessarily improve efficiency. And that's a problem.

Artificial intelligence will almost certainly increase the volume and heighten the impact of cyberattacks over the next two years.[1]

With heightened and hardened security must also come heightened efficiency. Today's cybersecurity solutions must help security and IT teams secure their organizations effectively while simultaneously helping them scale their efforts. Going forward, this change in perspective and requirements needs to come from two vantage points:

- Organizations should converge separate roadmaps to integrate their security efforts.
- Cybersecurity vendors must offer holistic solutions that defend against emerging AI-based threats and improve efficiency so organizations can do more with their existing resources.

An Example of Scaling Efficiency

Hybrid mesh firewalls (HMFs) are an excellent example of a security approach that combines AI-powered security features while improving efficiency through a coordinated approach to security. An HMF is a centralized and unified management solution that simplifies cybersecurity operations; it is a logical step in the evolution of the next-generation firewall.

An HMF optimizes security policies, simplifies deployment, improves scalability, and enhances threat visibility. An HMF unifies network management and security policies for all firewall deployments, protecting the entire expanding network attack surface, including IT and OT environments, on-premises, and cloud, or across disparate physical locations. Ultimately, using an HMF boosts network protection while reducing complexity and operational overhead.
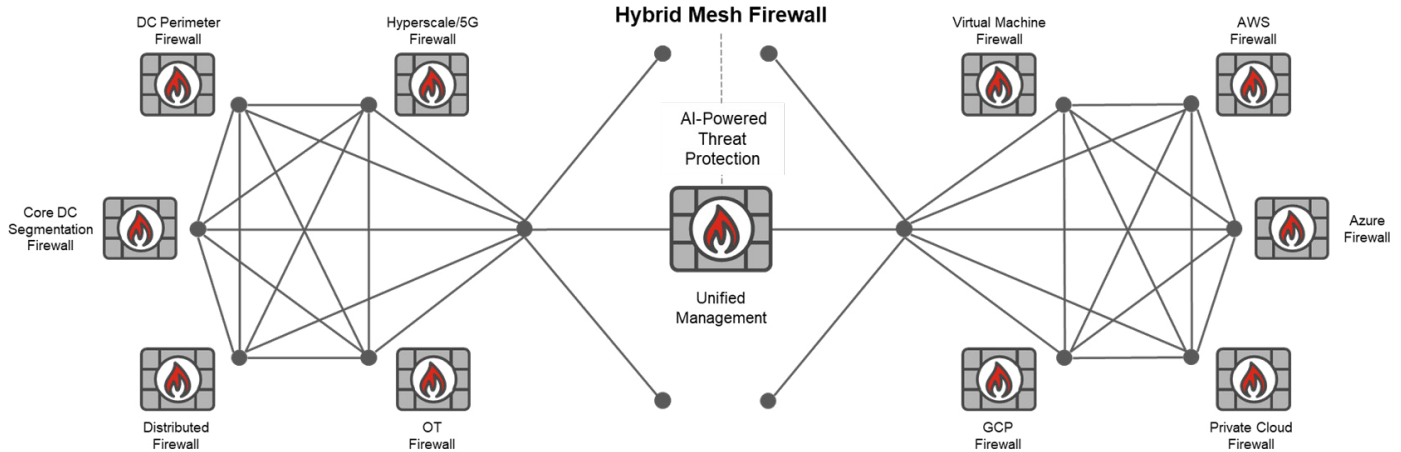

Figure 1: How a hybrid mesh firewall works

AI-Powered Threat Protection

Enhancing threat intelligence is one of the best uses for AI in cybersecurity. AI technologies are critical to data collection, analysis, correlation, and, ultimately, formulation of that data into actionable intelligence. And visibility absolutely matters. The more visibility AI has into the data, the more AI models can learn.

This intelligence can then be channeled through specialized capabilities to address a wide set of threat vectors and all manner of threats.
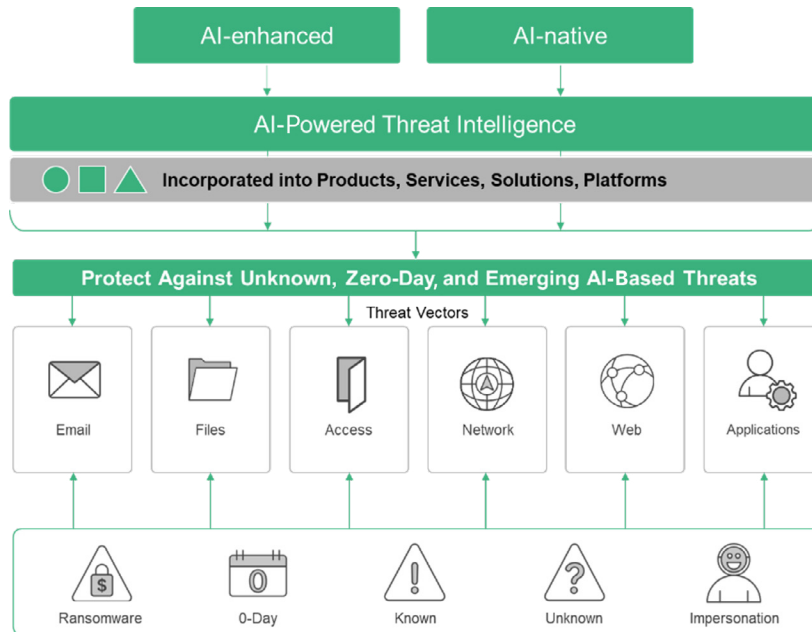

Figure 2: AI-enhanced and AI-native capabilities as part of threat intelligence formulation

HMFs include specialized capabilities, such as intrusion prevention, antivirus, web security capabilities such as DNS and URL filtering, and inline sandboxing. And each of these capabilities should use the latest AI-powered threat intelligence and take advantage of AI technologies directly to protect against cyberthreats. HMFs offer these key security capabilities:

Network and file security

- **Intrusion prevention:** Intrusion prevention performs deep-packet inspection of network traffic, including encrypted traffic, to detect and block the latest stealthy network-level threats and intrusions.

- **Antivirus:** Antivirus protects against the latest polymorphic threats, including ransomware, viruses, spyware, and other content-level threats.

- **Application control:** Application control lets you quickly create policies to allow, deny, or restrict access to applications or entire categories of applications.

Web and DNS security

- **DNS filtering:** DNS filtering provides consistent protection against sophisticated DNS-based threats. It provides complete visibility into DNS traffic while blocking high-risk domains, including malicious newly registered domains and parked domains.

- **URL filtering:** URL filtering identifies and blocks access to malicious URLs by users and applications.

- **Anti-botnet and command and control (C2):** Anti-botnet and C2 capabilities block unauthorized attempts to communicate with compromised remote servers to receive malicious C2 information or send out extracted information.

Software-as-a-Service (SaaS) and data security

- **Cloud access security broker (CASB):** A CASB secures SaaS applications in use, providing broad visibility and granular control over SaaS access, usage, and data.

- **Attack surface management:** Attack surface management works to identify, assess, and monitor network assets and associated security infrastructure to provide an overall evaluation of the organization's security posture.

Zero-day security

- **File sandboxing:** In a safe environment, file sandboxing performs advanced analysis of unknown files to determine if the files represent a threat.

All types of cyberthreat actors—state and non-state, skilled and less skilled—already use AI to varying degrees.[2]

Improving Scalability and Efficiency through Centralized and Unified Management

Because the use of AI by bad actors is increasing, security and IT leaders and practitioners must evaluate their future security initiatives and related spending in a broader context. In addition to evaluating how an AI-enabled security solution meets their cybersecurity goals, they must also look at how it improves efficiency.

The AI-powered threat protection along with the productivity and efficiency improvements in HMFs is a good example of how security and IT teams need to approach security going forward. With HMFs, security and IT teams can automate numerous protection capabilities without duplicating efforts, re-creating policies, or investing needless manual hours.

Our managed connectivity, communications and security solutions are innovative. Your business outcomes are imperative.

Windstream Enterprise drives business transformation through the convergence of our proprietary software solutions and cloud-optimized network to unlock our clients' revenue and profitability potential. Our end-to-end IT managed services modernize technology infrastructure, optimize operations, eliminate resource constraints and elevate the experience of our clients and their end users, while securing their critical data and brand reputation. Analysts recognize Windstream Enterprise as a market leader for our product innovation, and clients rely on our best-in-class management portal. Businesses trust Windstream Enterprise as their single-source for a high-performance network and award-winning suite of connectivity, collaboration, and security solutions— delivered by a team of technology experts whose success is directly tied to our clients' complete satisfaction.

[1] National Cyber Security Centre, The near-term impact of AI on the cyber threat, January 24, 2024.
[2] Ibid.

FORTINET

www.fortinet.com

May 2, 2024 11:58 PM

2615339-A-0-EN