FORTINET

AI-Powered Threat Protection with Next-Generation Firewall Buyer's Guide

Combining Artificial Intelligence, Security, and Scalability

The Threat Landscape

The use of artificial intelligence (AI) technologies by bad actors has been amplifying the challenges IT and security teams have in securing their organizations. From new exploits to deep fakes to advanced phishing emails and other tactics, cybercriminals are using AI to penetrate defenses faster and more decisively than ever before. This means that already stressed IT and security teams will only feel further pressure to keep up with an already daunting threat landscape.

However, adding more technology also means that staff must learn to use more consoles and manage alert streams for triage and investigation. Unfortunately for overworked teams, adding more security doesn't necessarily improve efficiency. And that's a problem.

Operations at Capacity

As organizations continue to pursue digital initiatives to support strategic objectives and improve efficiency, attack surfaces inevitably expand. Whether cloud adoption, the breaking down of air gaps between IT and OT, the proliferation of Internet-of-Things (IoT) devices connecting to the network, or supporting a hybrid workforce, these activities push the limits of already overburdened security and IT teams.

Security, Scalability, and Efficiency

With heightened or hardened security must also come heightened efficiency. Today's cybersecurity solutions must help security and IT teams secure their organizations effectively against various threats, including emerging AI-based threats.

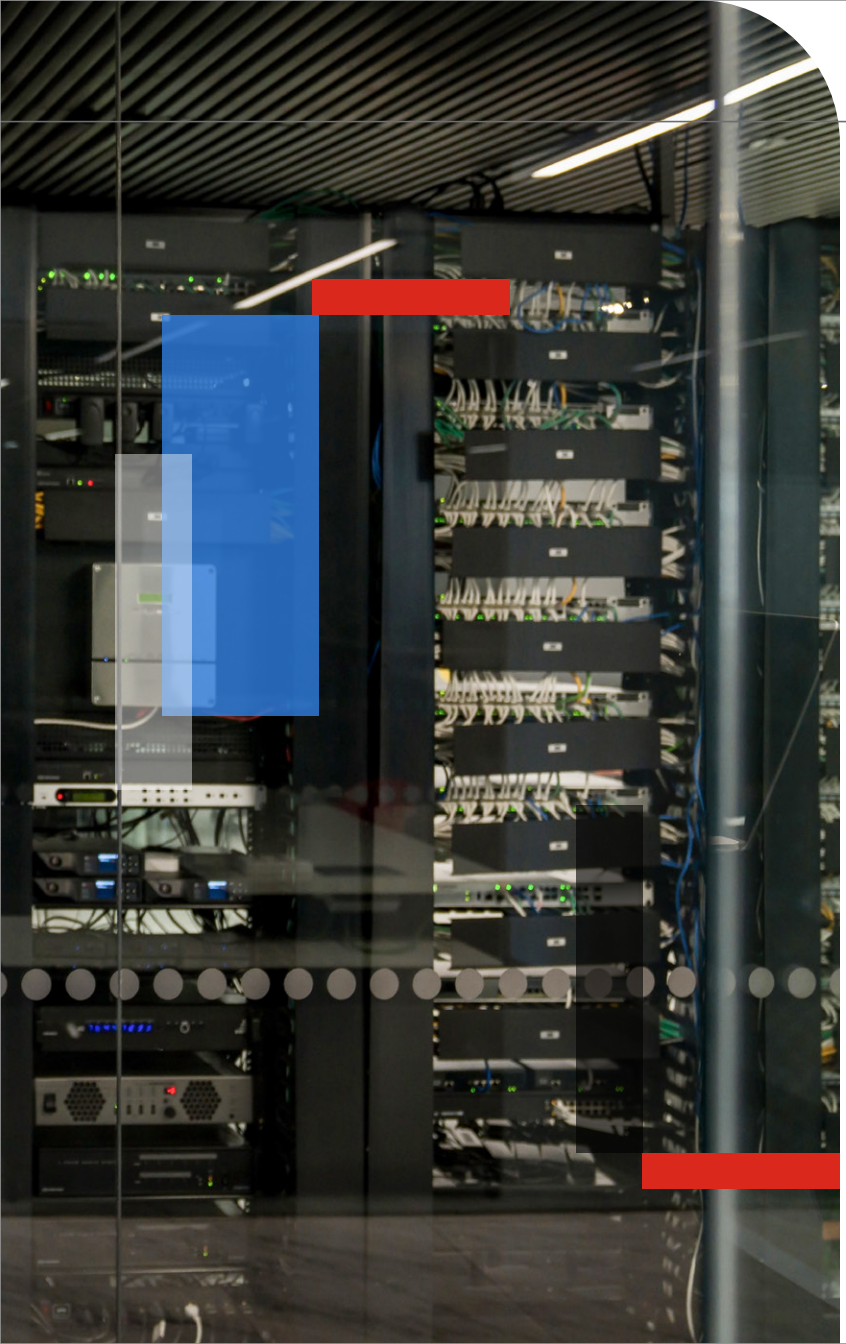
At the same time, solutions should help teams scale their efforts. Going forward, this change in perspective and requirements needs to come from two vantage points:

- IT and security teams 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.

Hybrid mesh firewalls (HMFs) are an excellent example of an opportunity to combine AI-powered security features while improving efficiency through a centralized and coordinated approach to security. This hybrid solution includes AI-powered threat protection and security features to help organizations effectively fight AI with AI. They also offer a centralized and coordinated approach to protecting the expanding network attack surface, including IT and OT environments, on-premises, and cloud, or across disparate physical locations.

What Is a Hybrid Mesh Firewall Solution?

An HMF solution is a centralized and unified management solution that simplifies cybersecurity operations; it is a logical step in the evolution of the next-generation firewall. In a hybrid environment, organizations can deploy firewalls on-premises or in the cloud with a single operating system for communication and threat intelligence updates across all deployments.



Implementing Unified and Centralized Management

- **Simplified management:** Consolidates security management into a single platform to eliminate the complexity of managing multiple firewalls from different vendors
- **Consistent security posture:** Reduces the risk of security gaps and vulnerabilities by enforcing a single security policy across the entire network that helps organizations comply with data privacy and regulatory guidelines
- **Enhanced security:** Allows faster and more precise responses to security incidents by leveraging automation, AI, and machine learning to analyze network traffic and identify potential threats more effectively
- **Improved scalability:** Add new security enforcement points as needed, eliminating management headaches and easily accommodating growth in the network or cloud deployments
- **Better visibility:** Provides a holistic view of the entire network's security posture to better identify and troubleshoot issues more efficiently

Why AI-Powered Threat Intelligence Matters

In cybersecurity, one of the best uses for AI is in enhancing threat intelligence. The applied use of AI technologies is critical to data collection, analysis, correlation, and, ultimately, the formulation of that data into actionable intelligence. This AI-powered threat intelligence can be channeled through integrations to address a wide set of threat vectors and threats, whether AI-enabled or not. A vendor's application of AI and breadth of data sources and data matter. The more visibility a vendor has into the data, the more that AI models can learn from that visibility.

Threat Protection Powered by AI

The use of AI in cybersecurity isn't just a technological upgrade. It's an increasingly urgent evolution that can help organizations elevate their defenses against emerging threats. Combining AI-powered security features with the improvements in efficiency inherent in NGFW solutions helps organizations create a more resilient security posture. NGFWs 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/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:** File sandboxing performs advanced analysis of unknown files in a safe environment to determine if the files represent a threat.

FORTINET

Key Considerations for Unified and Centralized Management

When securing a complex hybrid environment, start with the main line of defense: firewalls. Before purchasing a cybersecurity solution, such as an NGFW with AI-powered services, consider:

- **Network needs:** Carefully assess your network environment's specific needs, like the size and complexity of your network, the distribution of your workloads (on-premises vs. cloud), and your existing security posture.
- **Security features:** Evaluate the different features offered by various vendors, such as threat detection capabilities, data encryption, and integration with other security tools.
- **Management ease:** Ensure the cybersecurity solution offers a user-friendly and centralized management console to reduce the burden on your security team.
- **Scalability:** Consider how easily the cybersecurity solution can scale to accommodate future growth in your network or cloud deployments.
- **Cost:** Factor in licensing fees, ongoing subscription costs, and any required professional services for implementation and maintenance.
- **Vendor reputation:** Choose a reputable vendor with a proven track record verified by third-party sources.

By carefully considering these factors, you can choose an NGFW that meets your specific security needs and delivers the best value for your investment.

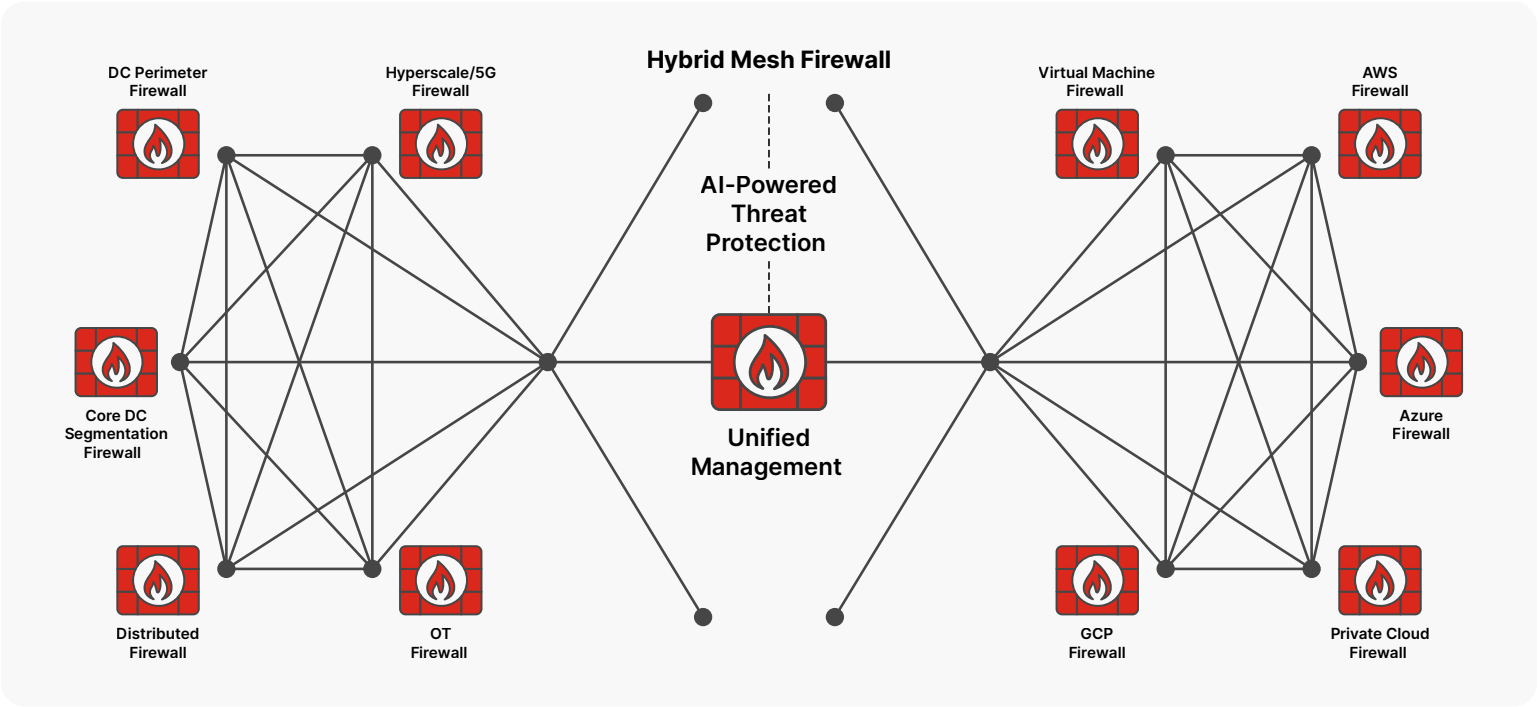


Figure 1: How HMFs with AI-powered threat protection work

Key Questions to Ask Your NGFW Vendor

1 Understanding the vendor's threat research capabilities

AI-based threat intelligence is critical. It starts with the dedicated group of individuals who make up the vendor's threat research team (if they have one).

- Does your organization have a threat research team, and if so, what is its composition and role?
- Is this team involved in adopting AI technologies at your company, and to what extent?

2 Understanding threat intelligence formulation

In cybersecurity, AI enhances threat intelligence, so you must understand the vendor's breadth of visibility. You need to know the extent of telemetry and information sources and the AI capabilities that help turn that telemetry and other data into actionable intelligence.

- What visibility into threats and related data sources does your organization use to formulate threat intelligence that powers your solution?
- How is AI used in the formulation of that threat intelligence?

3 Understanding the extent of AI use

You want to know how pervasive and committed a vendor is to use AI technologies and tools to enhance the offerings and related security outcomes.

- What is your organization's experience concerning the use of AI technologies in its products, services, and solutions?
- What specific AI technology or technologies are being applied to this particular solution, and what is the benefit of their use?
- Can you tell me what data sources the product, service, or solution uses to feed any AI technologies it uses?

4 Understanding the integrated security capabilities in a solution

For example, NGFWs should provide several key security features and integrations. You need to know what they are, what's included when buying a solution, and how they could benefit your organization.

- Which of the following security capabilities does your solution provide?
  - Intrusion prevention
  - Antivirus
  - Application control
  - Anti-phishing
  - Cloud access security broker
  - Data loss prevention
  - File sandboxing
  - Web security including DNS security
  - Attack surface management
  - OT security
  - IoT security
  - Other
- How is AI being applied to any of the services listed above?

5 What to look for in a hybrid environment

When choosing an NGFW, it's crucial to understand your specific security needs and network environment. Don't hesitate to ask vendors for demos and trials to ensure the solution meets your requirements. And, if you have a multivendor environment, look for an NGFW solution that can integrate with existing firewalls from different vendors.

Here are some key features to look for in an NGFW:

Security capabilities

- Advanced threat protection that utilizes AI technologies, including machine learning, to identify and block sophisticated cyberthreats
- Granular policy enforcement to define and enforce consistent security policies across all your IT infrastructure
- Threat intelligence feeds to stay updated on the latest vulnerabilities and attack methods

Management and scalability

- Centralized management with a single pane of glass to manage and monitor all your firewalls
- Automated deployment and provisioning that effortlessly deploys and configures all firewalls across your entire network
- Scalability to easily add or remove firewalls as your network grows or shrinks

Cost Savings and Business Benefits

"Fortinet is more than just a firewall. It converged several network and security components for improved network and security performance. The selling point for Fortinet is that it does more than just a firewall."

— Network and technical security manager, natural resources

318%
return on investment (ROI)

50%
reduction in network outages as a result of improved networking and security performance

6 months
payback is less than six months

50%[1]
increase in productivity of security and network teams

A New Way of Thinking

AI has moved to a new phase of innovation and the negative and positive impact it will have on organizations. In addition to evaluating how an AI-enabled security solution meets its cybersecurity goals, security and IT leaders must also consider how it improves efficiency.

NGFWs represent a compelling example of this new thinking. They provide AI-powered threat protection while centralizing visibility across your hybrid network, including coordinating and enforcing firewall policies. The result is a heightened security posture and corresponding increase in a team's ability to scale to meet the challenges posed by an evolving threat landscape.

If you are interested in deploying an NGFW at your organization, contact a Fortinet expert who can help you choose a solution that meets your specific security and network needs.

Call toll-free in the U.S.: **+1-866-868-3678**

U.S. federal government sales: **+1-833-386-8333**

Canada sales: **+1-833-308-3247**

[1] Forrester, The Total Economic Impact™ Of Fortinet NGFW for Data Center and AI-Powered FortiGuard Security Services Solution Cost Savings and Business Benefits Enabled by NGFW for Data Center and AI-Powered FortiGuard Security Services Solution, July 2023.

www.fortinet.com

April 12, 2024 12:19 PM

2627272-0-0-EN