Magic Quadrant for Hybrid Mesh Firewall

25 August 2025 - ID G00824307 - 42 min read

By Rajpreet Kaur, Adam Hils, and 4 more

This Magic Quadrant analyzes hybrid mesh firewalls, which offer unified cloud-based management across hardware, virtual and cloud deployments. Vendors can use this research to learn about HMFs that support hybrid environments with advanced CI/CD integration, native cloud features and strong threat prevention.

Market Definition/Description

A hybrid mesh firewall (HMF) is a multideployment mode firewall, including hardware, virtual appliance and cloud-based options, with a unified cloud-based management plane. HMF's are designed to support hybrid environments and evolving use cases by offering mature continuous integration/continuous delivery (CI/CD) pipeline integration, native cloud integration, and advanced threat prevention capabilities extending to Internet of Things (IoT) devices and DNS-based attacks.

With the adoption of hybrid environments, clients prefer the same firewall vendor with centralized management and visibility of firewall policies across environments to ease administration and reduce operational complexity. As a result, the demand and adoption of cloud firewalls from the same on-premises firewall vendor is growing. Hybrid mesh firewalls support this use case through hardware, virtual and dedicated cloud firewall deployment types, along with cloud-based centralized visibility and management capability.

Hybrid mesh firewalls provide support for multicloud and hybrid environment firewall use cases along with data center, enterprise perimeter and branch offices use cases. They offer advanced threat prevention, such as DNS security and IoT security. Features such as CI/CD integration and integration with native cloud controls support cloud firewall deployment use cases. The cloud-based centralized manager offers visibility and control across these firewalls deployed in hybrid environments through different deployment forms (hardware/virtual/cloud).

Mandatory Features

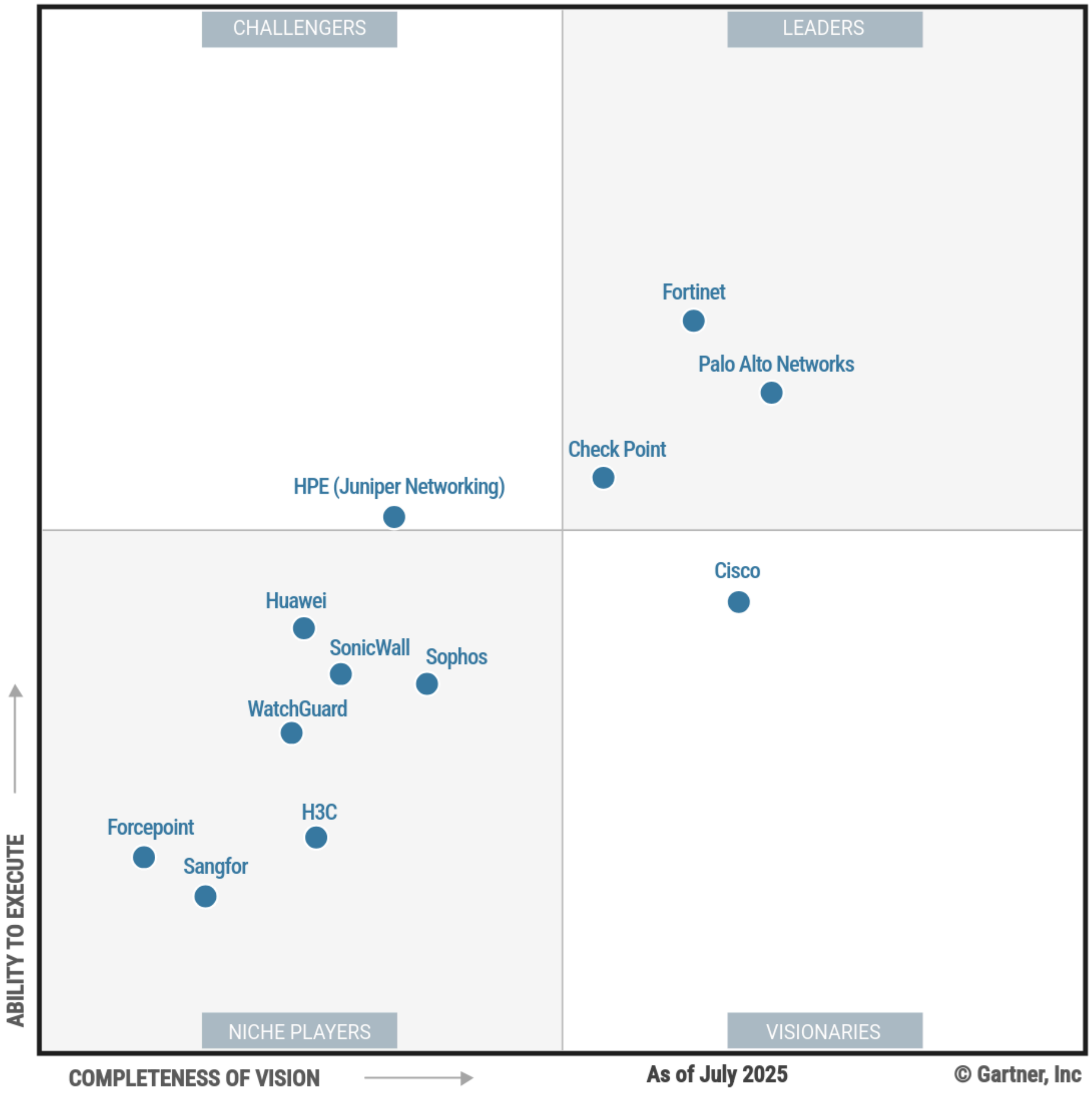
- Hardware/virtual and dedicated cloud firewall deployment forms managed by a single management interface.
- A cloud-based centralized manager with autotuning and policy recommendation capability.
- Firewall capabilities (stateful inspection, Secure Sockets Layer [SSL] decryption, URL filtering, app control, threat prevention).
- Advanced threat prevention for IoT- and DNS-based attacks.
- Secure remote access (e.g., SSL VPN, IPsec VPN, zero-trust network access [ZTNA]).
- CI/CD integration.
- Integration with cloud-native infrastructure.

Common Features

- Centralized visibility into cloud-native network security controls
- Zero-touch home office firewall appliances
- Centralized visibility into cloud-native microsegmentation controls
- Centralized visibility and microsegmentation third-party integration
- Optional ability to orchestrate firewall as a service (FWaaS) from central management platform

Magic Quadrant

Figure 1: Magic Quadrant for Hybrid Mesh Firewall



Gartner.

Vendor Strengths and Cautions

Check Point

Check Point Software Technologies is a Leader in this Magic Quadrant. Check Point, headquartered in Tel Aviv, Israel, offers hybrid mesh firewall capabilities through its Infinity Platform managed via a centralized cloud-based console. The vendor provides hardware, virtual, managed firewall-as-a-service and cloud-native deployment options through product lines such as Quantum Network Security, CloudGuard and Harmony SASE. Clients can license HMF offerings through flexible consumption models that support a range of deployment types alongside the cloud manager.

Check Point has a global presence across all geographies, utilizing both direct and partner-based sales channels. The vendor serves clients of all sizes and maintains a strong presence across various industry verticals.

Strengths

- **Sales execution:** Check Point has a strong track record of delivering transparent product pricing for many years. It is the only vendor offering a publicly available pricing portal for all its hybrid mesh firewall products and other product lines. The vendor also offers a flexible subscription-based licensing model covering hardware appliances.

- **Market responsiveness:** Check Point offers open API playbooks with prebuilt automation workflows for common use cases and utilization of a GenAI-based natural language converter to create or modify playbooks.

- **Vertical strategy:** Check Point has a strong vertical focus, with financial services, telecom, OT/ICS being the key verticals. The vendor shows strong OEM and integration partnerships along with a focus on different regulations and standards specific to these verticals.

- **Product:** Check Point offers advanced 5G support and security. Check Point supports quantum-safe encryption. It also offers partnerships and features to protect digital assets against blockchain and Web3 attacks.

Cautions

- **Marketing execution:** The visibility of Check Point in newer HMF deals is low compared to direct competitors. Clients are often not aware of new offerings and product enhancements, creating a market gap.

- **Client feedback:** Check Point scores low in ease of administration, with surveyed clients and client inquiries reporting complexities around initial setup and operational complexity when using the tool for troubleshooting incidents.

- **Offering:** Check Point does not offer containerized firewalls. The vendor lacks remote browser isolation and advanced SD-WAN capabilities compared to direct market competitors.

- **Market responsiveness:** Check Point introduced its SASE offering later than direct market competitors, reducing its appeal for those looking for a centralized cloud-based manager for HMF and SASE implementations.

Cisco

Cisco is a Visionary in this Magic Quadrant. Cisco, headquartered in San Jose, California, U.S., is a large vendor with an extensive product portfolio. Cisco offers HMF through its centralized cloud-based manager Cisco Security Cloud Control (SCC). The vendor offers hardware, virtual, FWaaS, cloud-native and containers deployment types through multiple product lines, namely Cisco Secure Firewall, Cisco Secure Access, Cisco Multicloud Defense, Cisco Secure Workload and Cisco Hypershield. The vendor offers HMF licensing through Cisco's Cloud Protection Suite, allowing clients to consume different firewall deployment types along with the cloud manager.

Cisco has a strong global presence through direct and channel sales. The vendor serves clients of all sizes and has a presence across various verticals.

Strengths

- **Product strategy:** The vendor offers multiple flexible firewall deployment types to support hybrid environments compared to direct competitors. Cisco Hypershield offers advanced distributed deployment for cloud. Cisco is the only HMF vendor with agent-based microsegmentation, which is offered through Cisco Secure Workload.

- **Geographic and vertical strategy:** Cisco offers technical support in the greatest number of regional languages. The vendor has strong partnerships with CPS vendors as a strategy aligned with the manufacturing vertical.

- **Market responsiveness:** Cisco shows a strong focus by responding to the growing demand for cloud firewall use cases. The vendor offers advanced cloud firewall orchestration capabilities through Cisco Security Cloud Control and Cisco Multicloud Defense.

- **Product:** Gartner scores Cisco high in secure remote access features. The vendor offers VPN posture management, a single interface to manage ZTNA, IPsec and SSL VPN through Cisco Security Cloud Control with extensive third-party MFA authentication support.

Cautions

- **Marketing execution:** Cisco continues to sell multiple product lines for similar deployment types, creating confusion around product positioning. Clients often indicate that these overlapping products are confusing and are a factor in moving away from the vendor.

- **Customer experience:** Clients rate Cisco low in ease of management compared to its direct competitors. The vendor lacks single policy creation through a single screen and requires multiple steps to create an end-to-end firewall rule.

- **Sales execution:** Cisco is rarely seen in stand-alone HMF and cloud firewall shortlists despite a mature offering. The vendor displays one of the lowest new customer acquisition volumes in this market.

- **Marketing strategy:** A large part of Cisco's network security value proposition is focused on Cisco infrastructure as a fabric, including switching, targeting network and data center teams. This creates a disconnect with the chief information security officer teams as the primary buyers and negatively impacts the network security brand.

Forcepoint

Forcepoint is a Niche Player in this Magic Quadrant. Forcepoint, headquartered in Austin, Texas, U.S., offers hybrid mesh firewall capabilities via the Forcepoint ONE platform and centralized Security Management Center (SMC). Forcepoint supports diverse deployment models, including hardware appliances, virtual firewalls and firewall-as-a-service. HMF licensing is modular and available through subscriptions like Forcepoint Next-Generation Firewall (NGFW) security suite.

Forcepoint has a presence in both enterprise and government sectors, primarily in Europe.

Strengths

- **Product:** Forcepoint offers advanced VPN orchestration capabilities, rated highly by users. The centralized manager offers centralized real-time visibility and management of VPN connections through a single click, making it easy to manage. The vendor also offers API-based CI/CD pipeline integration.

- **Sales strategy:** Forcepoint's growth is in multiyear enterprise agreements (EA) in regulated industries and government sectors. Gartner observes Forcepoint HMF offerings bundled within comprehensive enterprise licensing agreements (ELA).

- **Product strategy:** The focus is on flexible deployments, including clustering for high availability and scalability. The product emphasizes user and data-centric security, with deep user activity monitoring and DLP integration.

- **Geographic strategy:** Forcepoint offers multilingual support and has a strong focus in EMEA, government and the OT vertical. As a result, the vendor offers regional compliance support and local language support for the region. It collaborates with system integrators and technology partners to meet diverse security needs.

Cautions

- **Marketing execution:** The vendor primarily focuses on perimeter firewall and distributed office use cases. Gartner does not see adoption of Forcepoint in cloud firewall use cases in client inquiries, making it less likely to be shortlisted as an HMF vendor compared to other competitors.

- **Offering:** The vendor lacks a SASE offering, reducing its appeal for those looking for centralized cloud-based management of HMF and SASE implementations.

- **Customer experience:** Forcepoint scores low in cloud management capabilities. Some advanced configuration and troubleshooting features still require local console access despite Forcepoint's push toward full-featured cloud management.

- **Vertical strategy:** Forcepoint's focus on regulated and government sectors can limit visibility and adoption in the commercial midmarket.

Fortinet

Fortinet is a Leader in this Magic Quadrant. Headquartered at Sunnyvale, California, U.S., Fortinet offers HMF through its centralized cloud-based manager FortiManager Cloud. The vendor offers hardware (FortiGate), virtual (FortiGate VM), FWaaS (in its FortiSASE service and its dedicated firewall-as-a-service), cloud-native (FortiGate CNF) and container firewalls (cFOS). FortiManager Cloud allows customers to orchestrate different firewall deployment types along with the cloud manager.

Fortinet has a global footprint in all geographies through distributed channel sales and support presence. The vendor serves clients of all sizes with a presence across various verticals.

Strengths

- **Market understanding:** Fortinet offers its FortiOS fabric as part of its HMF, extending integrations to other product lines, including FortiSASE managed through FortiManager Cloud. Advanced reporting is available through FortiAnalyzer.

- **Market responsiveness:** Fortinet has introduced PQC support for IPsec key exchange, enabling FortiGate devices to use quantum-resistant algorithms to secure VPN tunnels in FortiOS version 7.6.1. This provides protection against "harvest now" and "decrypts later" threats against IPsec VPN traffic.

- **Product offering:** Fortinet offers on-FortiGate AI processing for FortiAI-Assist as an agentic AI assistant, which can autonomously analyze security events, triage alerts, conduct threat hunting and perform root-cause analysis at the FortiManager Cloud.

- **Sales execution:** Fortinet's points-based licensing, called FortiFlex, helps make HMF an operationally flexible solution after initial setup, allowing customers to change form factors over time as their use-case-driven needs change.

Cautions

- **Customer experience:** Fortinet disclosed vulnerabilities in its products, and Gartner clients and surveyed customers have expressed concern over the number and severity of bugs and exploitable vulnerabilities. The vendor has made some VPN-related announcements impacting end users, such as phasing out SSL VPN tunnel mode for IPsec VPN and discontinuing support for agentless VPN on certain models.

- **Product execution:** The demo went through several different UIs to meet the requirements: The number of steps required to complete one end-to-end task requires multiple tabs, interfaces and back and forth as per Gartner's analysis and client feedback. In addition, clients mention limited logging visibility within the firewall.

- **Sales strategy:** Some surveyed customers express frustration with the lack of visibility into Fortinet's HMF roadmap, making it difficult to evaluate short- and medium-term product vision versus competition.

- **Marketing execution:** Fortinet is more desirable as an appliance-based vendor. Although the vendor offers a mature cloud firewall with orchestration capabilities, visibility of FortiGate for cloud firewall use cases is lower compared to direct competitors.

H3C

H3C is a Niche Player in this Magic Quadrant. Headquartered in Beijing and Hangzhou, China, H3C is a vendor with a large product portfolio not only in cybersecurity but also in network, server, storage, among other offerings. The vendor offers HMF through different deployment types like hardware, virtual, cloud and container deployment under various product lines, namely H3C SecPath and H3C SecPath Virtual Firewalls (vFWs). H3C offers HMF licensing through the centralized manager, H3C SecCloud OMP, which can be delivered both in the cloud and on-premises.

H3C has its majority business in China, with some presence in the rest of Asia, Latin America, the Middle East and Africa. Geographies are served through direct and channel presence.

The vendor serves clients of all sizes with presence across various verticals.

Strengths

- **Product:** H3C's product supports flexible deployment both in the cloud and on-premises. The vendor offers containerized firewalls with AI runtime security features and focuses on CPS security, offering NetFlow analysis for advanced threat detection.

- **Product strategy:** H3C has a large security portfolio as well as network, servers and other offerings. It is chosen by many enterprises seeking vendor consolidation. H3C offers products such as SecCenter CSAP-iSOC for security operations, making it a desirable vendor for consolidation in China.

- **Sales execution:** H3C offers affordable products compared to other vendors. Product pricing has been stable over the past few years, which is an advantage for clients who are experiencing budget constraints.

- **Customer experience:** Surveyed clients highlighted technical support as very responsive. Clients also appreciated cost-effective pricing and easy licensing.

Cautions

- **Product strategy:** Some of H3C's product interfaces are only available in Chinese, like the LLM-powered AI assistant.

- **Product execution:** H3C lacks a unified cloud manager for its overlapping security products. The cloud manager lacks maturity and often redirects users to different management consoles, increasing operational complexity. Additionally, H3C doesn't have a clear plan to consolidate.

- **Geographic strategy:** As a regional vendor, H3C has a heavy focus on domestic cloud platforms (e.g., AliCloud, Tencent Cloud) and lacks support for global cloud platforms, limiting its international competitiveness for cloud firewall use cases.

- **Sales strategy:** The majority of H3C's sales are to the Chinese market and a few parts of Asia, Latin America, the Middle East and Africa. It lacks sales presence in other regions, especially North America and Europe.

HPE (Juniper Networking)

Hewlett Packard Enterprise (HPE) Juniper Networking is a Challenger in this Magic Quadrant. Headquartered in Spring, Texas, U.S., HPE Juniper Networking delivers hybrid mesh firewall capabilities via its Security Director Cloud platform. The vendor offers a broad range of deployment options, including SRX Series Firewalls (hardware, vSRX, cSRX) and Juniper Secure Edge (FWaaS, SWG and CASB). They provide a range of licensing models to support various deployments, which can be per device, per feature, or subscription-based depending on the specific product and service.

On 2 July 2025, HPE closed its acquisition of Juniper Networks. HPE's network security offering is outside the scope of this research.

HPE has a global presence across all geographies, leveraging both direct and channel sales strategies.

Strengths

- **Product:** HPE Juniper Networking offers a mature cloud-based manager. The Security Director can integrate with Juniper security analytics to provide advanced threat correlation. The security director offers visibility of VPCs and advanced cloud-native policy orchestration.

- **Product execution:** Security director offers an easy-to-manage interface. It offers mature orchestration capabilities for cloud firewall use cases. It also offers advanced IoT tagging and categorization information, enabling IoT device posture management capability.

- **Market understanding:** HPE Juniper Networking has a focus on cloud use cases and offers a mature containerized firewall that can be fully managed by the security director. The company's approach includes simplifying licensing by bundling hardware, software and management into a single SKU.

- **Geographical strategy:** The company has a global presence with a diverse industrial and vertical focus. The vendor offers multilingual technical support. It offers a network of regional partners across the globe, focusing on regional customer support.

Cautions

- **Overall viability:** There has been a constant decline in Juniper's firewall market share due to factors such as constrained past investments and uncertainty of future investments following the HPE acquisition. This has led to its decline in the HMF shortlist compared to the direct competitors.
- **Marketing strategy:** The vendor lacks dedicated security branding and marketing. Overall marketing is directed more toward integrated infrastructure promoting convergence between HPE Juniper Networking products, making it more desirable for network and infrastructure teams than security teams.
- **Marketing execution:** Gartner has very low visibility of HPE Juniper Networking firewalls being shortlisted for stand-alone HMF use cases. Despite a mature cloud firewall offering, Gartner does not see its cloud firewall shortlisted for cloud use cases.
- **Offering:** At the time of assessment, HPE Juniper Networking does not have a SASE offering as per Gartner SASE market definition. This makes it less appealing to HMF customers who desire a centralized cloud-based manager for managing HMF and SASE.

Huawei

Huawei is a Niche Player in this Magic Quadrant. Headquartered in Shenzhen, Guangdong Province, China, Huawei is a large vendor with a broad product portfolio. Huawei offers HMF through the centralized cloud-based manager iMaster NCE-Campus. The vendor offers hardware, virtualHardware, virtual, cloud-native and container firewall deployment types through multiple product lines, namely Huawei HiSecEngine USG series firewalls and Eudemon series firewalls, Host Security Service and Cloud Firewall. Huawei provides flexible licensing options and support for customers converting licenses between platforms.

Huawei has a global presence in many geographies through direct and channel presence. The vendor has presence across various verticals including, a high number of government, healthcare, financial and manufacturing customers.

Strengths

- **Product:** Huawei offers orchestration for branch deployment, security policy modification, one-click configuration in Huawei Cloud, support for multiple enforcement types, MFA authentication, IPsec and SSL VPN connectivity, as well as advanced risk scoring for enhanced security management.

- **Sales execution:** The vendor has a strong focus on high-throughput appliances with competitive pricing for large enterprises. The vendor has maintained its list price for a few years, providing pricing stability.

- **Product strategy:** The vendor supports multiple firewall enforcement types, including cloud firewall out-of-box deployment, one-click purchase, automatic route synchronization and fine-grained permission configuration. The platform includes an intelligent policy recommendation feature with policy self-learning to refine original policies without manual intervention.

- **Vertical strategy:** Huawei offers technical support in various regional languages to its customers globally. It has a strong vertical presence in manufacturing, government and carrier in China. The vendor also has a large MSSP presence.

Cautions

- **Product strategy:** Huawei scores low in public cloud use cases as its support is limited to Huawei Cloud only. The vendor lacks a mature SASE offering, limiting its appeal for those looking to extend HFM to SASE through a centralized cloud management.

- **Customer experience:** Huawei offers multiple firewall product lines with dedicated managers. There are differences in features between Huawei's cloud-based manager and its on-premises/virtual firewall centralized managers, resulting in a lack of centralized management experience.

- **Marketing execution:** Huawei firewalls are generally shortlisted as a part of larger infrastructure Huawei EA deals involving multiple products. Gartner does not see Huawei firewalls shortlisted for stand-alone HMF use cases.

- **Geographic strategy:** Due to geopolitical constraints, Huawei has a limited global presence with no sales in some key countries, restricting its customer base. This also impacts its product strategy, partnerships and support for regional compliances.

Palo Alto Networks

Palo Alto Networks is a Leader in this Magic Quadrant. Palo Alto Networks is headquartered in Santa Clara, California, U.S. The vendor offers its HMF through its centralized cloud-based manager, Strata Cloud Manager. The vendor offers hardware (PA-Series), virtual (VM-Series and Prisma AIRS), FWaaS (in its SASE service and dedicated firewall-as-a-service), cloud-native (Cloud NGFW), and container firewalls (CN-Series). Palo Alto Networks offers HMF licensing through Strata Cloud Manager, allowing customers to orchestrate different firewall deployment types along with the cloud manager.

Palo Alto Networks has a global footprint in all geographies through channel sales and support presence.

The vendor serves clients of all sizes with a presence across various verticals.

Strengths

- **Product strategy:** Palo Alto Networks' HMF security services leverage AI methods, such as deep learning and GenAI, to continuously train on a wide range of data sources. AI/ML models assess the severity of threats based on the risk and policy enforcement decisions are made based on the severity levels.
- **Marketing execution:** Palo Alto Networks is the most visible vendor for HMF use cases in inquiries. The vendor is a desirable choice for HMF clients seeking unified cloud management along with SASE and SSE through its Strata Cloud Manager.
- **Product:** The vendor offers advanced IoT posture management capabilities within Strata Cloud Management compared to competitors. The vendor's IoT approach uses continuous traffic monitoring and crowdsourced intelligence to identify and baseline normal behaviors of IoT devices.
- **Market responsiveness:** The vendor has a strong focus on AI runtime security and the 5G security use case. Strata Cloud Manager offers advanced orchestration capabilities such as predictive analysis and policy recommendation. The vendor supports visibility and control over PQC usage in encrypted traffic.

Cautions

- **Sales execution:** Gartner clients often highlight frustration and concern over higher renewal costs, forcing them to sign short-term contracts rather than multiyear deals. The total cost of ownership of Palo Alto Networks HMF is relatively higher than direct competition and is one of the key reasons clients tend to migrate away.
- **Pricing:** Gartner finds Palo Alto Networks ELAs and ESAs complex and lacking clarity. Gartner clients often struggle to understand these proposals and describe them as complex and time-consuming.

- **Offering:** At present, there is a feature disparity between Strata Cloud Manager and Panorama. As a result, Gartner clients cite that they will have to run both Panorama and Strata Cloud Manager for at least a year before they can fully move to Strata Cloud Manager. The CN-Series is not managed through Strata Cloud Manager either, but it is supported via Panorama.

- **Customer feedback:** Gartner clients and surveyed customers mention that the hardware firewalls can have performance-related issues, such as slow boot times and high resource requirements. Customer support around such issues can be inconsistent.

Sangfor

Sangfor is a Niche Player in this Magic Quadrant. Sangfor, headquartered in Shenzhen, China, offers hybrid mesh firewall capabilities through its Sangfor Network Secure platform. Sangfor supports multiple deployment types, including hardware appliances, virtual firewalls, cloud-native firewalls and firewall-as-a-service. These are managed through the Sangfor Platform-X cloud-based manager.

Sangfor has a regional presence in Asia/Pacific and is expanding into the Middle East and Africa through a mix of direct and channel sales. Its customer base includes small-to-midsize enterprises, government agencies and educational institutions.

Strengths

- **Product:** Sangfor offers cloud deception as a feature that enables Sangfor Network Secure/NGAF to integrate with cloud decoys without any third-party product deployment. The vendor also offers AI-based phishing detection using LLMs.

- **Sales execution:** Sangfor has maintained its list pricing for a few years, making it a cost-effective offering that highlights its strong SMB and upper-midsize enterprise focus.

- **Product strategy:** Sangfor’s product strategy centers on ease of use and cost-effective pricing, delivering an intuitive and user-friendly interface that streamlines deployment and management for organizations of all sizes. The vendor emphasizes flexible deployment across hardware, virtual and cloud environments, ensuring scalability and high availability.

- **Geographic strategy:** Sangfor maintains a strong focus on China and emerging markets. As a result, the vendor offers multilingual technical support for these regions and a growing network of local channel partners.

Cautions

- **Sales execution:** Gartner clients have reported the vendor's strong focus on selling bundled security suites, sometimes creating complexity in conducting focused product evaluations and licensing purchases for stand-alone HMF use cases.
- **Product strategy:** Sangfor has less focus than the Leaders on dedicated HMF-based use cases and targets a wider product stack, including NGAF, IAM and cloud-based security services.
- **Product execution:** At present, the Chinese version and English version of centralized cloud manager have feature disparity. Some advanced configurations and troubleshooting are dependent on direct access to local consoles or on-premises interfaces and other product interfaces.
- **Market responsiveness:** Sangfor lacks advanced SASE and IoT management capabilities compared to the leaders. As a result, it lacks visibility in client shortlists seeking HMF and advanced SASE from the same vendor.

SonicWall

SonicWall is a Niche Player in this Magic Quadrant. Headquartered in Milpitas, California, U.S., SonicWall delivers hybrid mesh firewall capabilities through its cloud-native SonicWall Unified Management (SonicPlatform). The vendor offers a broad range of deployment options, including multiple hardware appliance series (SOHO, TZ, NSa, NSsp), virtual appliances, firewall-as-a-service and secure SD-WAN. HMF licensing is available through offerings such as the Managed Protection Security Suite (MPSS), Advanced Protection Security Suite (APSS) and Essential Protection Service Suite (EPSS), allowing clients to select flexible protection bundles.

SonicWall maintains a global presence in all geographies through direct and channel sales.

Strengths

- **Product:** SonicWall emphasizes DNS security features such as domain categorization, threat intelligence, DNS tunneling detection and sinkhole services. The platform provides unified management for firewalls, switches, access points, endpoint threat detection and secure service edge. The system supports autopolicy generation for low-scoring devices.
- **Sales execution:** SonicWall offers easy-to-consume and cost-effective pricing models that are highly desirable for MSSPs and SMBs. The company continues to offer hardware,

software subscriptions and management as a bundled solution, with cloud management included at no extra cost.

- **Marketing strategy:** SonicWall's sales strategy emphasizes bundled offerings, such as free secure internet access and ZTNA licenses with three-year HMF bundles. It also offers new bundled subscriptions for CASB, ZTNA, SWG and SD-WAN use cases. It also offers an inclusive cyber warranty program through a third-party cyber insurance provider.
- **Vertical strategy:** The vendor employs an MSP/MSSP-focused strategy, targeting education, healthcare, IT/service providers and retail sectors. It has a diverse global presence, offering technical support mainly in English, with other languages available regionally.

Cautions

- **Marketing execution:** SonicWall does not have direct end-user branding, as it is 100% MSP/MSS-focused. As a result, end users have limited awareness of SonicWall HMF, which limits marketing execution across all types of customers.
- **Market responsiveness:** The vendor has been slow to extend HMF to fully integrated and cloud-managed capabilities, such as ZTNA, FWaaS, SASE or cloud firewall, making it less appealing to buyers who value higher levels of integration of these products.
- **Product strategy:** SonicWall's product strategy is more focused on MSP/MSSP and SMB use cases and demands. The vendor's roadmap indicates closing product gaps and lacks innovation related to emerging HMF use cases.
- **Offering:** The offering has feature gaps, making it less desirable for cloud firewall use cases. The absence of public cloud CSPM capabilities, limited generative AI assistant functions, lack of IoT detection or tagging, no Kubernetes-specific policy support and no container firewall support are a few examples of such gaps.

Sophos

Sophos is a Niche Player in this Magic Quadrant. Sophos, headquartered in Abingdon, U.K., supports diverse deployments, including hardware appliances, virtual firewalls (VMware, Hyper-V, KVM, Citrix) and cloud-native firewalls (AWS, Azure, Nutanix). HMF licensing is integrated with the Sophos Central platform, which also manages endpoint, ZTNA, email and other security services for synchronized protection.

With a global presence, Sophos primarily targets SMBs through a strong channel network, focusing on sectors like education, healthcare and retail.

Strengths

- **Product:** Sophos offers integration of NDR with Sophos Central. The lightweight version of NDR directly integrates with Sophos XGS Firewalls and analyzes TLS metadata and DNS queries using AI. It also offers risk-based scoring detection.
- **Product strategy:** Sophos enables unified policy management across on-premises, virtual and cloud environments via its cloud-native Sophos Central platform, allowing centralized visibility and control of all firewall deployments.
- **Sales strategy:** Sophos maintains a strong global presence with multilingual technical support and an extensive channel partner network spanning North America, EMEA and Asia/Pacific.
- **Sales execution:** Sophos is one of the top-cited competitors in SMB because of its bundled pricing. The vendor focuses on a simplified and intuitive user interface, providing ease in deployment and management for organizations with limited resources.

Cautions

- **Marketing strategy:** Sophos lacks dedicated HMF-based positioning, with a primary focus on cloud firewall use cases. Sophos traditionally emphasized Synchronized Security, highlighting the integration between Firewall and EDR. Sophos now focuses on Active Threat Response, emphasizing the integration between Firewall and XDR or MDR services.
- **Marketing execution:** While Sophos offers a single firewall series, there are some overlapping capabilities between Sophos Firewall and Endpoint products. These overlapping offerings can leave clients uncertain about which product best fits their needs and can be a factor in clients considering alternative vendors with more streamlined portfolios.
- **Product offering:** Sophos Central provides unified cloud-based management; however, some advanced configuration, policy tuning and troubleshooting tasks require direct access to individual firewall appliances or on-premises interfaces. While this depth of management is not always needed, this limits the seamlessness of centralized management and may create operational inefficiencies for clients seeking fully cloud-native unified administration

- **Market responsiveness:** Sophos lacks FWaaS and lags market leaders in core and advanced features for ZTNA, IoT device detection and network segmentation.

WatchGuard

WatchGuard is a Niche Player in this Magic Quadrant. Headquartered in Seattle, Washington, U.S., WatchGuard operates with a 100% channel-focused business model, selling its products exclusively through the channel. The HMF product line includes Firebox, FireboxV, Firebox Cloud and FireCloud, supporting various deployment types such as hardware, virtual and firewall-as-a-service. WatchGuard offers a Unified Security Platform that integrates its Firebox appliances (hardware, virtual, and cloud) with advanced threat detection capabilities. The WatchGuard Cloud platform provides centralized, multitier, multitenant management for MSPs, offering ease of administration through policy templates and streamlined visibility across all connected security solutions.

Its partner-centric model prioritizes partners with a strong channel-focused business model. WatchGuard has a global presence with regional focus through channel presence in over 20 countries.

Strengths

- **Offering:** The unified cloud-based manager supports all hardware and software models, enabling scalable policy management with shared policies, templates, tags and device groups. WatchGuard offers integration of XDR with NDR, providing agentless telemetry, full network visibility and device monitoring.

- **Sales strategy:** The vendor offers large regional channels and scores high in global presence. Technical support ranks high, with support in multiple languages.

- **Sales execution:** WatchGuard offers a flexible licensing model, including FlexPay for MSP partners with options for monthly subscriptions and choices between one-year or multiyear terms. There is also a points system option for product allocation to tenants. It provides multiple security service packages from which to choose, with tools and quick reference guides available for partners to estimate pricing.

- **Customer experience:** Surveyed clients have scored WatchGuard high in ease of use and deployment. They have also highlighted that the licensing bundles are easy to consume and cost-effective.

Cautions

- **Product:** WatchGuard's offering lacks features, such as containerized firewalls, user-based dynamic risk scoring and comprehensive IoT tagging. Additionally, TLS decryption causes significant performance drops, even when used on high-performance appliances.

- **Product execution:** Connectivity for SSL VPN users can be slow, impacting user experience. There are feature gaps between on-premises and cloud managers, which may impact the adoption of cloud management.

- **Market execution:** WatchGuard's GTM is through resellers/MSPs/MSSPs. It prioritizes SMB requirements and is not often cited by Gartner clients for the cloud firewall use case.

- **Product execution:** Client feedback suggests that documentation for initial configurations could be improved because it lacks the necessary detail for inexperienced users.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

As this is a new Magic Quadrant, no vendors were added.

Dropped

As this is a new Magic Quadrant, no vendors were dropped.

Inclusion and Exclusion Criteria

To qualify for inclusion, the vendor's HMF offerings must:

- Have a dedicated hardware-based product line and a cloud firewall product line.

- Have a dedicated cloud-based firewall manager with centralized hardware and cloud firewall enforcement management.
- Have a proven track record of not being a regional-only player and shown evidence that their offering generates more than 15% of the total revenue outside the home region.
- Gartner must have strong evidence that the vendor meets the HMF market definition as defined by Gartner.

A vendor is excluded if it does not meet any of the following as of February 2025:

- If it does not qualify as a hybrid mesh firewall as per Gartner's market definition.
- If a vendor does not sell a dedicated hardware firewall and cloud firewall product line.
- If a vendor does not offer a cloud-based unified firewall manager.
- If the vendor does not qualify as a global player, because of revenue split as per different geographies.
- If the vendor only offers FWaaS, as a part of their firewall offering.
- If the vendor only offers cloud firewall, as a part of their firewall offering.
- If the vendor offers only hardware/virtual appliances, as part of their firewall offering.
- If the cloud-based manager of the firewall doesn't support both hardware and cloud firewall enforcement types.

Evaluation Criteria

Ability to Execute

Product/Service: The key capabilities focused for this market are, but not limited to, platform, cloud-based manager, product integration, advanced threat detection and prevention, secure connectivity, use-case-specific capabilities, core firewall features and URL filtering/application control.

Overall Viability: We assess the health of the vendor, the business unit, and whether they will continue to grow and invest across multiple areas related to this market and overlapping technologies related to this market.

Sales Execution/Pricing: Key areas evaluated include growth of the business, how pricing and licensing is offered to customers and its relative consumability, evidence of the ability to build and maintain strong relationships with end customers, and the value of the product for its cost. End-user feedback is critical to this section and provides strong evidence to understand the consumability of the vendor's sales execution for this market.

Market Responsiveness and Track Record: This assesses the vendor's track record compared to competitors of delivering effective and customer-aligned capabilities in the platform. The historical evidence of leading the market and timely introduction of features and other offerings completely aligned with customer demand as per Gartner's analysis is evaluated.

Marketing Execution: We address the clarity of messaging and its efficiency, as well as whether it is clearly differentiated and aligned with their product capabilities. We also assess investments in marketing and whether these investments are delivering results in how prominently clients consider the vendor. Clarity of messaging as it resonates with customers is critical as per Gartner's analysis.

Customer Experience: We assess and consider all aspects of the customer experience, including presales and postsales experience, availability and quality of documentation, technical support and end-user satisfaction with the product. This includes customer feedback as directly gathered by Gartner.

Ability to Execute Evaluation Criteria

Evaluation Criteria	*Weighting*
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	High
Market Responsiveness/Record	High

Evaluation Criteria	*Weighting*
Marketing Execution	Medium
Customer Experience	High
Operations	NotRated

Source: Gartner (August 2025)

Completeness of Vision

Market Understanding: This includes the ability to understand and address client needs, likely competitors for the vendor’s product now and in the future, and self-awareness and clear understanding of their own strengths and weaknesses in the market.

Marketing Strategy: The vendor shows novel and effective approaches to communicating and differentiating, as well as forward-looking investments in their marketing program and messaging.

Sales Strategy: This includes partnerships that extend the scope and depth of a provider’s market reach, expertise, technologies, services and their customer base. Vendors demonstrate their vision of sales with market evolution and the evolution of customer demands.

Offering (Product) Strategy: This includes delivering new features that are relevant to the market as Gartner sees the market, to end-users’ current and emerging needs, and delivering them in a timely fashion. Gartner will evaluate vendors’ vision for developing their offering for this market and the top use cases as identified by Gartner.

Vertical/Industry Strategy: Vendors’ ability to identify top verticals and ability to meet their use cases.

Innovation: Marshaling of resources, expertise or capital for competitive advantage, investment, consolidation or defense against acquisition. Vendors’ ability to identify the emerging use cases and innovate. This is not just confined to the technical product capabilities but overall offering innovation.

Geographic Strategy: The ability to focus on different geographies and support them through multiple regional strategies.

Completeness of Vision Evaluation Criteria

Evaluation Criteria	*Weighting*
Market Understanding	High
Marketing Strategy	Low
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	NotRated
Vertical/Industry Strategy	Low
Innovation	Medium
Geographic Strategy	Low

Source: Gartner (August 2025)

Quadrant Descriptions

Leaders

A Leader can address both current and future end-user requirements in the market. Leaders have strong offerings that address multiple use cases, typically via a unified platform that provides a single cloud-based manager with multiple deployment types to support a hybrid environment. Further, a Leader's strategy is well-aligned with emerging user needs and has the potential to drive, shape and transform the market going forward. They lead the market with innovation and strong execution. A Leader typically has strong visibility in the market, solid networking and security features, a large installed base of customers and maintains positive relationships with its customers and partners on a global basis. Additionally, they possess a product strategy that aligns with the market trend for providing easy-to-use, advanced features and making business investments for the future. Leaders have effective sales and distribution channels for all of their product portfolios, a well-diversified vertical and geographic strategy, and a vision for how HMF is placed within the broader network security platform approach.

Challengers

A Challenger has a proven ability to address current end-user requirements in the market. A Challenger typically has good visibility, a sizable installed base of customers and products that are above average for most enterprises across multiple use cases. However, a Challenger's strategy and roadmap are less likely to transform the enterprise market going forward. They may compensate for this with a strong sales channel (possibly in adjacent security areas) and strategic relationships or extensive visibility in the market. They are often late to introduce new features and lack a complete, unified product strategy. Challengers appeal largely to clients that have established strategic relationships with them.

Visionaries

Visionaries stand out for their strong technical or product strategies and vision, but may lack the proven execution, visibility, or corporate resources, such as robust sales channels and strategic partnerships, of Leaders. Visionaries often help transform the market — from driving new ideas and innovations, including new business models, to solving enterprise challenges. While Visionaries often have a solid strategy going forward, they often lack a consistent, proven ability to address customer challenges in a scalable manner to date.

Niche Players

Niche Players are often focused on specific portions of the market, such as a specific use case, geography, vertical or technological specialty. They have a viable technology but have not shown the ability to drive the broader market or sustain execution in the broad enterprise market. A Niche Player has a mature network firewall offering but still has gaps per the HMF offering, with some limitations that manifest outside of their core focus areas. These limitations often include feature depth, usability, geographic reach, market visibility and installed base.

Context

While the firewall market has existed for years, it still lacks the level of automation and integration required in the product to meet the changing and evolving networks and threat landscape. Organizations are moving beyond traditional use cases to more innovative use cases involving hybrid environments, hybrid workforces and hybrid teams. The HMF market offers features and functionalities to support the evolution toward these use cases. HMFs offer mature, cloud-based, unified management with automation and orchestration capabilities. Features such as application connectivity mapping, visibility into cloud-native network security policies, policy fine-tuning and recommendations facilitate the administration of all firewall components across hybrid environments. The HMF, with its platform approach, offers an integration of firewall mesh with centralized management, support for multiple deployment forms and better integration of tools from multiple vendors. The HMF also supports the evolving use cases and threat landscape. The market will continue to evolve to support traditional and emerging firewall use cases to offer microsegmentation, centralized visibility and control management across hybrid environments.

The network firewall market has become mature and commoditized. Vendors are offering similar features around threat inspection, URL filtering, App-ID and VPN along with stateful inspection. Clients seeking network firewall solutions for use cases like on-premises perimeter protection and internal segmentation should choose a vendor that meets their specific criteria, including throughput and concurrent session requirements, low total cost of ownership (TCO), competitive price-to-performance ratio, strong local support and affordable renewal costs.

The HMF market is rapidly evolving, driven by the need for unified firewall and threat prevention controls across hybrid environments — spanning on-premises, cloud and edge. This Magic Quadrant evaluates 12 vendors across the hybrid mesh firewall capabilities and market.

Market Overview

Market Drivers

Expansion of hybrid environments: As infrastructure environments become more complex and distributed, network security teams struggle to manage these environments effectively. Enterprises continue to move toward the cloud, but the landscape remains predominantly hybrid. While enterprises are adopting cloud, the majority have to maintain on-premises infrastructure. This increasing diversity is leading to greater management complexity and widening skill gaps for teams trying to keep pace.

Centralized management and visibility: SRM leaders focus on providing centralized management and visibility across hybrid environments, helping to minimize the administrative burden of daily operations and streamline investigation and reporting processes.

Platform approach: Vendors have integrated their stand-alone products into modular security platforms that address common use cases. They are emphasizing these platforms to clients as a way to tackle current challenges related to complexity and skill gaps.

Expanding attack surface: The attack surface is expanding due to AI-driven threats, increased use of SaaS applications, supply chain integrations, containers, and IoT devices. Organizations are finding it more difficult to manage this growth as their environments become more complex and distributed across on-premises and cloud systems.

Need for open API framework: The increasing need for interoperability of multiple tools in the network and demand of running security as code requires a Cybersecurity Mesh Architecture approach. These offerings support outbound APIs for integration with other security platforms and nonsecurity tools such as ticketing, unified endpoint management, threat intel, and communications tools. Tools are required to offer bidirectional APIs to allow for the platform to integrate with other security tools, platforms and automation.

Simplified licensing: CFOs and sourcing teams are struggling to manage the growing complexity of cybersecurity tool licensing and renewals. They seek strategic vendor partnerships to simplify licensing while maintaining effective security.

End-User Adoption Trends

Adoption of Multiple Deployment Types

An increasing number of hardware renewal proposals include cloud firewall part numbers. As clients adopt multicloud while maintaining on-premises systems, they prefer firewalls from a single vendor for centralized management and advanced security across all environments.

Higher Renewal Costs

Clients are increasingly concerned about rising firewall renewal costs and have found that vendor consolidation does not always reduce expenses. As a result, they are rethinking their convergence strategies and carefully evaluating the total cost of ownership before purchasing advanced software subscriptions.

On-premises vs. Cloud-Based Managers

Clients are interested in cloud-based HMF managers, but feature gaps compared to on-premises options make running both unappealing with an unnecessary cost. As a result, most vendors now include basic cloud manager versions at no extra cost.

Role of AI with HMF operations

AI’s greatest impact will be automating daily firewall tasks, such as change management and routine policy assessments. The majority of HMF vendors are offering AI-based chat assistants to simplify operations. Although these AI assistants are at different stages of maturity, some offer basic documentation search, while others offer more granular capabilities. AI-based operations can offer real-time traffic flow, connections analysis, and assistance around tagging and labeling. Gartner regularly receives inquiries where customers are still using older/nonsupported firmware versions, as they feel that the upgrade cycle might break their connectivity and impact business continuity, exposing themselves to the risk of unpatched vulnerabilities. AI can automate this process and be utilized to provide a realistic risk assessment and impact analysis, and securely test the latest firmware.

Key Observations

Cloud-based manager: The maturity of HMF cloud managers varies greatly between the vendors. Most cloud managers still use different platforms or work as a single sign-on interface for other screens and portals. Many clients are open to migrating on-premises managers to the cloud but are waiting for vendors to address feature gaps before fully making the switch.

Advanced threat detection: Support for IoT and DNS-based attacks, CPS device discovery and posture management is becoming standard. Few vendors offer dedicated IoT and DNS security features under different part numbers. Vendors are already developing and providing granular features for CPS device discovery and classification, behavioral anomaly detection, posture management and risk scoring, and microsegmentation through third-party integrations.

Secure connectivity: All surveyed HMF vendors support IPsec, SSL VPN and ZTNA. Few offer universal ZTNA with posture validation and integration with SASE/SSE platforms. Vendors are providing a single unified agent with ZTNA, VPN (IPsec/SSL), posture validation, threat detection and response, DNS security and DLP capabilities.

Orchestration and automation: Since the maturity of cloud-based centralized managers is the primary feature of HMF, vendors are focusing on enhanced orchestration and automation capabilities. The participating vendors have highlighted features such as zero-touch deployment, dynamic policy orchestration, multicloud policy sync, AI-driven configuration and troubleshooting-based features and enhancements.

LLM chat assistant: The LLM chat assistant is continuously developing and vendors are at different phases of maturity, providing basic or enhanced features. A limited number of vendors offer a mature solution with impactful features related to orchestration and policy recommendations. The top features include natural language interface for querying firewall configurations, logs, policies, guided troubleshooting and policy optimization, and context-aware recommendations for rule creation and remediation.

API integration: Although all vendors claim to support API-based third-party integration, many HMF vendors lack mature APIs for leading third-party tools and primarily support their own product lines.

AI-based threat correlation and prevention: HMF vendors are leveraging agentic AI capabilities to improve threat correlation and provide predictive analysis and policy recommendations to improve threat detection and prevention.

Prevention of AI application workloads: HMF vendors are building features to secure AI application workloads and environments, primarily in VM and container deployments. These include monitoring AI model interactions and protecting LLMs and AI workloads from prompt injection, data leakage, and misuse. Few vendors offer partial AI runtime security, while Palo Alto Networks provides a dedicated AI runtime security firewall with its containerized firewall solution.

⊕ Evaluation Criteria Definitions