Magic Quadrant for Hybrid Mesh Firewall

7 September 2026 - ID G00840519 - 41 min read

By Rajpreet Kaur, Adam Hils, and 1 more

Hybrid mesh firewalls deliver the most critical preemptive security control in hybrid environments, providing centralized cloud-management across physical, virtual and cloud-native deployments. Select vendors that meet your security needs and provide effective protection across complex, distributed networks.

Market Definition/Description

Gartner defines hybrid mesh firewalls (HMFs) as a SaaS-based offering implementing in-line bidirectional stateful inspection through hardware (on-premises), virtual and dedicated cloud firewall enforcement types. HMFs are designed to support hybrid environments and related use cases by offering mature continuous integration/continuous delivery (CI/CD) pipeline integration, native cloud integration and advanced threat prevention capabilities.

With the adoption of hybrid environments, a centralized management and visibility toolset that enables users to oversee firewall policies across environments is preferable. This eases administration and reduces 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 SaaS-based centralized visibility and management capability. The SaaS-based offering comes with advanced orchestration features with AI assistant and predictive analysis and policy recommendations.

Hybrid mesh firewalls provide support for multicloud and hybrid environment firewall use cases such as hybrid networks, data center, multicloud, heavy branches, network segmentation and secure access. HMF supports open APIs to offer CI/CD and advanced integration with overlapping technologies such as SASE, SSE, NDR and microsegmentation to offer centralized management across the team and advanced threat correlation.

Mandatory Features

The mandatory features for this market include:

- A SaaS-based offering implementing in-line bidirectional stateful inspection through hardware (on-premises), virtual and dedicated cloud firewall enforcement types
- A single unified offering with dedicated licensing
- TLS decryption
- App control and URL filtering
- In-line advanced threat prevention such as intrusion prevention, network sandboxing, IoT security and DNS security
- Secure remote access (e.g., SSL VPN, IPsec VPN, zero-trust network access [ZTNA])
- DecSecOps automation for CI/CD pipeline integration to build security as code workflows
- Integration with cloud-native infrastructure such as Amazon Web Services (AWS), Azure and Google Cloud Platform (GCP) network security controls

Optional Features

The optional features for this market include:

- Discovery of AI application usage; logging of AI application usage; enforcement of controls, including prevention of data transfers; and reporting of risk at the network level
- Ability to insert a security policy between any two workloads in the same broadcast domain through an HMF platform
- Application-connectivity-based mapping visibility and traffic labeling
- Discovery and control of third-party AI application usage through API traffic analysis, including MCP, A2A and other integrations between agents and services

- Centralized visibility and control into cloud-native microsegmentation controls

Magic Quadrant

Figure 1: Magic Quadrant for Hybrid Mesh Firewall

Gartner

Vendor Strengths and Cautions

Check Point

Check Point is a Leader in this Magic Quadrant. Headquartered in Tel Aviv, Israel, the vendor offers hybrid mesh firewall (HMF) through its Hybrid Mesh Network Security offering.

Check Point's product development priorities include AI Defense Plane for specific AI platforms and end-to-end agentic security orchestration across its network security suite.

Check Point has a global presence spanning all regions and maintains a strong presence across various industry verticals.

Strengths

- **Sales execution:** Check Point targets AI data center and NeoClouds, addressing sovereignty, segmentation and protection of AI workloads and graphic processing unit (GPU) clusters at scale, including a partnership with NVIDIA.
- **Innovation:** Check Point demonstrates strong postquantum cryptography (PQC) readiness through early adoption. The vendor has added native support for ML-KEM/Kyber to its Transport Layer Security (TLS) inspection engine.
- **Feature:** Check Point integrates capabilities from its Lakera AI acquisition into its container, cloud and on-premises firewall, providing protection for prompts, Model Context Protocol (MCP) and Application-to-Application (A2A) communications.
- **Customer experience:** Check Point is the first vendor to introduce firewall appliance consumption-based subscriptions. Customers can deploy physical firewalls and capacity without fixed sizing or long-term commitments.

Cautions

- **Marketing execution:** Gartner does not see Check Point being shortlisted frequently for newer client deployments. Gartner attributes this to a lack of strong security branding across network security and cloud security use cases.
- **Client feedback:** Gartner clients report that deploying some security features in hardware firewalls introduces a heavier-than-normal performance tax, especially TLS decryption. As a result, they have to upgrade to a higher model for better performance, which impacts cost.
- **Feature:** The vendor lacks advanced SD-WAN capabilities compared with direct competitors. As a result, Gartner clients do not frequently shortlist it for heavy branch offices HMF use cases and integrated secure access service edge (SASE) use cases for unified management.

- **Market responsiveness:** Check Point is slower to address emerging cloud use cases, such as adding containerized firewalls and dedicated microsegmentation, compared with direct competitors.

Cisco

Cisco is a Visionary in this Magic Quadrant. Headquartered in San Jose, California, U.S., the company delivers Cisco Hybrid Mesh Firewall, which combines the HMF cloud-based manager Cisco Security Cloud Control with multiple enforcement options.

Cisco is focused on unified segmentation across hybrid mesh, layered protection for AI agents and applications delivered through the HMF, and preemptive security controls through kernel-level enforcement against critical vulnerabilities.

Cisco is a global vendor with a presence across all verticals.

Strengths

- **Product strategy:** Cisco's feature enhancements and roadmap support diverse HMF enforcement types across hybrid environments to meet advanced HMF use cases. With Cisco Cloud Protection licensing, the vendor offers flexibility to move between physical, virtual, cloud or container firewalls.
- **Market understanding:** Cisco demonstrates a strong market understanding by unifying microsegmentation orchestration capabilities through Cisco Security Cloud Control. The vendor continues to meet market demand by extending support to third-party firewalls (currently limited to a few vendors).
- **Feature:** Cisco offers AI Defense as a cloud-based security feature. AI Runtime Protection automatically configures guardrails for AI models to block prompt injection, extraction and denial of service in real time.
- **Innovation:** Cisco continues to emphasize PQC-related innovation through consistent feature development and roadmap execution, including support for NIST FIPS 203, 204 and 205 standards across HMF communications.

Cautions

- **Marketing execution**: Cybersecurity leaders do not view Cisco as a security vendor for best-of-breed security use cases such as cloud firewall or microsegmentation. Gartner

does not see Cisco HMF frequently shortlisted for newer customer deployments relative to direct competitors.

- **Customer feedback:** Gartner clients cite disclosure of exploited vulnerabilities as a concern to adopt the vendor as a brand. Some Gartner clients continue to report issues related to bugs, unstable firmware and frequent patching.
- **Sales execution:** Cisco channel network, continues to primarily promote and sell infrastructure offerings as compared to newer security offerings. Gartner clients cite that they are not aware of the vendor's newer security product lines and features.
- **Sales strategy:** Gartner clients continue to express confusion about Cisco's multiple product lines for the same or similar use cases — for example, Cisco Meraki MX and Cisco Secure Firewall for hardware enforcement — even when a unified management plane is available.

Forcepoint

Forcepoint is a Niche player in this Magic Quadrant. Headquartered in Austin, Texas, U.S., the vendor offers hybrid mesh firewall capabilities via the Forcepoint Network Security 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 such as the Forcepoint Next-Generation Firewall (NGFW) security suite. Forcepoint's major HMF product development initiatives include an AI gateway, zero-trust network access (ZTNA) enhancement and quantum-resistant cryptography support.

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

Strengths

- **Product:** Forcepoint offers advanced virtual private network (VPN) orchestration capabilities. Vendor also offers 16-node active-active clustering capabilities, making it useful for extreme, large-scale high-availability use cases.
- **Sales strategy:** Forcepoint bundles its HMF offerings within comprehensive enterprise licensing agreements (ELAs), making firewalls an easier and more cost-effective add-on for existing clients.

- **Features:** Forcepoint's product emphasizes user and data-centric security, with deep user activity monitoring and data leakage prevention (DLP) integration. Its Endpoint Context Agent (ECA) integrates with the firewall to provide advanced threat detection.
- **Geographic strategy:** Forcepoint offers regional compliance and local language support in EMEA for various countries/regions, making it a desirable vendor for regulated verticals in Europe.

Cautions

- **Product strategy:** The current features and roadmap show a lack of a strong HMF-focused product strategy. The vendor's focus is on limited use cases, and it lacks advanced capabilities for cloud firewall and data center use cases.
- **Innovation:** The vendor lacks a strong focus on innovation with basic PQC support, microsegmentation and container enforcement for cloud use cases.
- **Market responsiveness:** Forcepoint lags behind in cloud management capabilities compared with competitors. It offers basic automation and does not offer advanced configuration and troubleshooting features.
- **Sales execution:** Forcepoint's focus on regulated and government sectors limit its appeal to other industries.

Fortinet

Fortinet is a Leader in this Magic Quadrant. Headquartered in Sunnyvale, California, U.S., it offers HMF through FortiManager, its cloud-based centralized manager, with multiple firewall enforcement types.

Over the next 12 months, Fortinet plans to deliver a unified Model Context Protocol (MCP) framework for AI agent-based automation, workflow-based automation through a natural language interface, deception capabilities and additional detections for agentic AI threats.

Fortinet is a global vendor and serves enterprises of all sizes across all HMF use cases.

Strengths

- **Market execution:** The vendor leads in enterprise perimeter, heavy branches and data center use cases. Fortinet also offers dedicated carrier-grade scalable platforms that

support and secure 5G traffic and has a strong presence in managed security services (MSSs).

- **Product:** Fortinet leads in advanced routing and SD-WAN orchestration use cases. It offers advanced SD-WAN orchestration through FortiManager Cloud, enabling scalable, policy-driven WAN deployment across distributed enterprise sites.
- **Innovation:** Fortinet's current features and roadmap show strong innovation in AI-based automation, PQC and multicloud orchestration. FortiGate Cloud-Native NGFW Firewall (CNF) uses AWS Lambda to automatically ingest threat intelligence from services such as GuardDuty, enabling real-time, adaptive protection.
- **Feature:** The vendor introduced diverse advanced threat detection and response features over the past 12 months. Key features include Internet of Things (IoT) and cyber-physical systems (CPS) device detection, both passive and active, to categorize assets by manufacturer, firmware and industrial function. The vendor has also introduced real-time firewall file monitoring.

Cautions

- **Marketing strategy:** Vendor branding and marketing are still heavily focused on edge and perimeter use cases. As a result, Gartner does not frequently see Fortinet on client shortlists for the cloud firewall use cases compared with direct competitors.
- **Customer feedback:** Customers have reported firmware and bug-related issues with the vendor, as well as dissatisfaction with technical support. Some Gartner clients have also shared concerns regarding the disclosure of exploited vulnerabilities negatively impacting the Fortinet brand.
- **Pricing:** Gartner clients have expressed frustration with recent price increases and unexpected high costs. Clients have shared that Fortinet is more expensive than its direct competitors.
- **Sales strategy:** Fortinet HMF is frequently included in large EA deals with infrastructure line items and is less frequently shortlisted for best-of-breed network security use cases, such as HMF with security service edge (SSE), cloud firewall or microsegmentation use cases, compared with direct competitors.

H3C

H3C is a Niche Player in this Magic Quadrant. H3C is headquartered in both Beijing and Hangzhou, China. Its Boundary Security offering combines the HMF Security Cloud Management Platform with multiple enforcement types. All of these enforcement types can be managed through H3C SecCloud OMP.

Over the next year, H3C plans to focus on AI-driven security defense, unified data security, governance and compliance in multicloud and distributed environments. It also invested in securing AI agents and enhancing governance for AI-based dynamic permissions.

H3C is a regional vendor, and its largest client base is in China. The vendor has a regional presence mostly in carrier, enterprise and financial verticals.

Strengths

- **Product strategy:** H3C demonstrates an HMF-focused product strategy by consolidating various security functions into a single, unified platform, eliminating the need for multiple security appliances.
- **Product:** H3C's HMF is deployed as hardware and virtualized firewalls for implementation in cloud environments, branch locations and on-premises data centers. Its architecture enables simplified policy enforcement across these environments, ensuring consistent security operations.
- **Feature:** H3C's HMF utilizes AI and machine learning to enhance threat detection and response capabilities. It provides automated response capabilities that can sandbox, analyze and block malicious traffic.
- **Customer experience:** H3C offers mature orchestration features through policy templates and automated policy deployment. This helps streamline operations and reduce the risk of configuration errors.

Cautions

- **Geographic presence:** The vendor primarily sells in China and has a very limited presence in Europe. As a result, the vendor has limited sales channels across regions and provides limited language support.
- **Integration:** Integrating H3C's firewalls with non-H3C network infrastructure or third-party security platforms requires additional customization. The vendor lacks OEM partnerships with global third-party security vendors.

- **Feature:** Some parts of the web-based GUI for H3C's cloud management platform are in Chinese and require reauthentication for some modules.
- **Offering:** The vendor currently supports and integrates security policy enforcement and deployment for its firewall only on Alibaba Cloud. It is working with Microsoft Azure to expand deployment options.

HPE

Hewlett Packard Enterprise (HPE) is a Challenger in this Magic Quadrant. Headquartered in Spring, Texas, U.S., HPE offers HMF capabilities through its HPE Networking hybrid mesh security solution, delivered through the HPE Networking Security Director as a cloud-based manager.

Over the next 12 months, HPE plans to deliver hybrid mesh posture and assurance capabilities, providing a consolidated view of firewall topology and cloud workload health.

HPE has a global presence across all geographies, with limited regional language support, and leverages both direct and channel sales strategies.

Strengths

- **Feature:** Security Director offers persona-based dashboards customized for specific roles, such as security analysts and network administrators. The platform utilizes advanced visualizations, including Sankey diagrams, to map threat interconnectivity and improve response orchestration with granular drill-down reporting.
- **Market understanding:** HPE continues to focus on expanding cloud HMF use cases for perimeter protection. It offers integration with CI/CD pipelines and container network interface (CNI), along with advanced cloud routing features and dynamic tagging support.
- **Product:** HPE's Security Director leverages NETCONF as an open platform to offer native support for popular programming and scripting languages. This enables workflow-based automation with DevOps and NetOps.
- **Global presence:** HPE has a global direct and channel presence. This provides direct presence across different regions, with the potential to compete with other global and regional vendors.

Cautions

- **Product strategy:** The vendor lacks a strong product strategy for advanced HMF use cases such as microsegmentation for cloud environments. It also lacks a single integrated HMF and SASE offering for clients seeking a platform approach.
- **Client feedback:** Gartner clients cite product quality issues, reporting firmware-related bugs and the inability of technical support to provide faster resolution as primary reasons for moving away from the vendor.
- **Sales strategy:** HPE is rarely shortlisted by Gartner clients for new HMF deployment use cases. The vendor fails to gain traction with security teams for best-of-breed HMF use cases.
- **Market responsiveness:** The vendor offers basic support for PQC algorithms and lags behind competitors in support. The vendor also trails competitors in cloud firewall capabilities, as its cloud visibility and management features are currently supported only in AWS.

Huawei

Huawei is a Niche Player in this Magic Quadrant. Headquartered in Shenzhen, Guangdong Province, China, Huawei offers HMF through the centralized cloud-based manager iMaster NCE-Campus. The vendor offers hardware, virtual, cloud-native and container firewall deployment options.

Over the next year, Huawei is prioritizing automated optimization of security policy using an AI configuration assistant. In addition, the vendor is working on IoT asset and vulnerability management.

Huawei has a global footprint (outside North America) through direct and channel presence. Customers operate in verticals including government, healthcare, financial and manufacturing.

Strengths

- **Market responsiveness:** The vendor shows a focus on automation and orchestration capabilities as the primary feature of HMF to support hybrid use cases.
- **Product strategy:** The vendor has an HMF-focused product strategy through diverse enforcement options. In addition to native microsegmentation, the HMF offers hardware, virtual, cloud-native, container and firewall as a service (FWaaS) form factors.

- **Feature:** The vendor uses semantic analysis in-line AI algorithms to detect zero-day attacks such as remote code execution (RCE), cross-site scripting (XSS), SQL injection and web shell attacks. It can also define an interaccess matrix between resource groups to automatically orchestrate and recommend optimal firewall policies.
- **Market execution:** Huawei offers technical support in various regional languages to its customers. It has a strong vertical presence in the manufacturing, government and carrier sectors in China. The vendor also has a large MSSP and OT presence.

Cautions

- **Partnerships:** Huawei's cloud firewall support is limited to Huawei Cloud only. As a result, it cannot be adopted for cloud-based use cases by clients using other public cloud providers.
- **Product execution:** Customers and prospects find Huawei's multiple firewall product lines with dedicated managers confusing. Differences in features between Huawei's cloud-based manager and on-premises manager result in a lack of centralized management experience.
- **Sales execution:** Huawei HMF is almost always part of a Huawei "all-in" EA deal. As these deals are usually led by network infrastructure considerations, this limits HMF's appeal to cybersecurity-led investments.
- **Product strategy:** Huawei's offerings are unavailable in some western regions due to regulatory, legal and geopolitical restrictions. This also impacts its product strategy, partnerships and support for regional compliance regimes.

Palo Alto Networks

Palo Alto Networks is a Leader in this Magic Quadrant. Headquartered in Santa Clara, California, U.S., the vendor offers Strata Network Security Platform, which includes the HMF cloud-based manager Strata Cloud Manager (SCM) and multiple enforcement options.

Over the next year, the vendor plans to focus on intent-driven autonomous AI agent security, comprehensive agentic endpoint protection and vibe coding protection. These plans aim to ensure continuous network security health, simplify zero-trust deployments and automatically adapt to evolving security threats as part of the HMF offering's capabilities.

Palo Alto Networks is a global vendor with regional language technical support. Its customers operate across all verticals.

Strengths

- **Innovation:** Palo Alto Networks' Quantum Safe security app, part of Strata Cloud Manager, offers real-time discovery of vulnerable cryptographic assets and postquantum remediation across the enterprise.
- **Market responsiveness:** The vendor has shown early market responsiveness through a strong focus on real-time, adaptive AI runtime security through Prisma AIRS.
- **Product:** The vendor offers advanced automation through the Strata Network Security platform, which reduces complexity and the risk of misconfigurations. The built-in LLM assistant can perform complex administrative tasks through basic human language commands.
- **Feature:** The vendor offers advanced threat detection and protection capabilities. It provides automated incident response workflows, leveraging integrations with security orchestration, automation and response (SOAR) platforms (such as Cortex XSOAR) for rapid containment, investigation and remediation.

Cautions

- **Sales execution:** Gartner clients express frustration with higher total cost of ownership (TCO). Clients report that the vendor refuses to share list prices and that getting price transparency is a struggle.
- **Sales strategy:** Gartner small and midsize (SMB) business clients have reported a lack of proper account management by Palo Alto Networks. Clients often report that they struggle to get renewal quotations because of their smaller deal size and receive limited support for quotation-related queries.
- **Customer feedback:** Gartner clients report dissatisfaction with the vendor's premium support tier, especially with L1-related SLAs. They often report that, to get a better support experience, they are asked to adopt a higher-tier support model, which involves additional cost.
- **Customer experience:** Most new features are offered as add-on subscriptions rather than enhancements to existing features. In the past, the vendor has sold acquisition-based

products/features before they were fully integrated with the HMF offering, creating management complexity and dissatisfaction among Gartner clients.

Sangfor Technologies

Sangfor Technologies is a Niche player in this Magic Quadrant. Headquartered in Shenzhen, China, the vendor offers Sangfor Athena NGFW, which combines the HMF cloud-based manager Sangfor Platform-X with multiple enforcement types.

Over the next 12 months, the vendor plans to focus on AI governance and control, postquantum readiness and an LLM assistant.

Sangfor is a regional vendor with limited regional language technical support. The vendor's customers operate in a variety of verticals.

Strengths

- **Product:** Sangfor Platform-X delivers native microsegmentation capabilities to enforce granular security controls and isolate workloads. The platform's firewall is integrated with Sangfor's broader security suite, allowing for unified policy management and coordinated threat detection.
- **Feature:** Sangfor Platform-X leverages AI and ML for advanced threat detection, automated analysis and incident response. Its AI engine continuously analyzes network communication and user behavior to identify anomalies and respond to threats.
- **Product strategy:** The vendor demonstrates an HMF-focused product strategy through its platform approach. This integration streamlines workflows, improves visibility and reduces the complexity of managing multiple point offerings.
- **Sales strategy:** Sangfor offers competitive pricing with clear licensing compared with its direct global and regional competitors.

Cautions

- **Sales execution:** Sangfor has a significant market share in China and is expanding in the Middle East. While the vendor does not operate in North America, it has a limited sales presence in Europe and Africa.
- **Market responsiveness:** The vendor currently lacks a dedicated containerized firewall. It lags in native LLM assistant capabilities for human language interface automation.

- **Market execution:** The vendor has limited brand recognition and fewer large-scale reference customers outside of its core markets.
- **Customer experience:** Technical documentation is limited and support resources, particularly in languages other than Chinese, may be less comprehensive or difficult to access.

SonicWall

SonicWall is a Niche Player in this Magic Quadrant. Headquartered in Milpitas, California, U.S., the vendor offers HMF capabilities through SonicWall Unified Management, a cloud-based console that integrates Network Security Manager (NSM) Cloud to manage multiple enforcement types.

Over the next year, SonicWall's plans include automatic assessment of the security posture of firewalls using AI, predictive and proactive serviceability, and network traffic anomaly detection using AI related to its HMF offering.

SonicWall is a global vendor that offers regional language technical support. Its customers operate across a variety of verticals.

Strengths

- **Product:** SonicWall HMF provides centralized management, policy orchestration and visibility for security policies across on-premises, cloud and distributed branch environments.
- **Feature:** The platform integrates SonicWall's AI-based real-time deep memory inspection (RTDMI) and advanced threat protection (ATP) technologies to protect against zero-day threats, ransomware, encrypted attacks and advanced malware.
- **Sales strategy:** SonicWall offers simple, cost-effective pricing models that appeal to MSSPs and SMBs. The company continues to offer hardware, software subscriptions and management capabilities as a bundled offering.
- **Platform approach:** The vendor delivers integrated security services, including intrusion prevention, anti-malware, sandboxing, web filtering, ZTNA and cloud application security, within its unified platform to provide layered protection against threats.

Cautions

- **Product strategy:** The vendor lacks some advanced cloud-native features and integrations, and does not show a strong focus on cloud use cases.
- **Market execution:** SonicWall has a limited number of third-party OEM partnerships, making it less attractive to enterprise organizations that require integrations with a wider variety of vendors in their security stack.
- **Innovation:** The vendor lags behind competitors in PQC and advanced automation within cloud-based manager features.
- **Sales execution:** SonicWall does not offer advanced features to be adopted across all the HMF use cases and lacks a presence in data center, cloud and large-enterprise use cases.

Sophos

Sophos is a Niche Player in this Magic Quadrant. Headquartered in Abingdon, U.K., the vendor supports a variety of enforcement types, including hardware appliances, virtual firewalls and cloud-native firewalls managed through Sophos Fusion.

Over the next year, Sophos plans to use AI and integrated tooling to provide real-time visibility, governance-based reporting for CISO-level insights, centrally managed unified policies set and security controls across firewall, endpoint and workspace protection, and firewall REST APIs with token-based authentication to enhance API-based integration.

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

Strengths

- **Product:** Sophos offers an integrated platform approach. Its HMF and native product lines are managed centrally through Sophos Fusion (SaaS-based manager). It enables cross-domain visibility, facilitates telemetry sharing and supports automated response orchestration from a single interface.
- **Customer feedback:** Customers rate Sophos' simplified pricing and bundles highly. They have also cited technical support as a strength.
- **Product strategy:** With its platform approach and strong SMB-focused product strategy, Sophos is a strong option for SMBs. SMBs facing account management challenges with enterprise-focused vendors provide positive feedback on Sophos' channel and regional support.

- **Feature:** Sophos offers advanced integration between Sophos HMF, Network Detection and Response (NDR) and Extended Detection and Response (XDR), providing automated detection and response. It offers native network detection and response through Xstream Protection and XDR Linux sensors directly embedded in the HMF.

Cautions

- **Offering:** Sophos lacks a dedicated container firewall for cloud firewall use cases Gartner does not see Sophos HMF being adopted for cloud firewall use cases.
- **Market execution:** The vendor lacks mature integration with third-party detection and response and does not have a roadmap for enterprise-focused use cases. It also lacks higher-throughput appliances for data center and high-enterprise use cases.
- **Feature:** As more enterprises focus on compliance-based reports, Sophos lacks specific compliance reports for GDPR, FERPA, ISO 27701, ISO 27001 or NIST 800-53.
- **Sales strategy:** The vendor has a stronger MDR-focused sales strategy compared with their HMF offering. This limits its ability to grow faster in the HMF market compared with direct competitors.

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, where it exclusively sells its products. The vendor offers various deployment types such as hardware, virtual and firewall as a service.

WatchGuard is working to integrate Firebox with WatchGuard Cloud Directory and Identity Framework to support contemporary OpenID Connect (OIDC)-based authentication, develop shared configuration for security services and execute a planned broad hardware model upgrade.

Its partner-centric model prioritizes service providers with a channel-focused business model. WatchGuard has a global presence with a regional focus through channel presence, including growing representation in EMEA and APAC.

Strengths

- **Platform approach:** WatchGuard offers tight integration with its native product lines, which can be managed through WatchGuard Central. AuthPoint authentication services are

natively embedded with Firebox, enabling RADIUS-based authentication, multifactor authentication (MFA) enforcement and identity-aware policy control.

- **Feature:** Network telemetry from Firebox and other supported environments feeds into ThreatSync+ NDR, enhancing the platform with advanced anomaly detection. These insights are correlated back into ThreatSync Core, enabling unified investigation and orchestrated response across the entire security environment.
- **Sales execution:** WatchGuard offers a flexible licensing model, including FlexPay for managed service providers (MSPs), 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 offers multiple security service packages, with tools and quick reference guides available for partners to estimate pricing.
- **Customer feedback:** Gartner clients mention that WatchGuard is easy to use and deploy and that the GUI is intuitive. Clients also report that the licensing bundles are easy to consume and cost-effective.

Cautions

- **Feature:** WatchGuard lacks built-in, specific compliance reports for several major standards, including GDPR, FISMA, SOX, FERPA and ISO 27701, which most other vendors provide.
- **Sales strategy:** WatchGuard's go-to-market strategy is predominantly through MSPs/MSSPs, serving only the SMB market. This limits channel availability for non-SMB clients.
- **HMF uses:** The vendor lacks some advanced cloud-native features and integrations and does not show a strong focus on cloud use cases. Its offerings demonstrate limited effectiveness for high-performance data center requirements or large-scale enterprise perimeters.
- **Sales execution:** WatchGuard does not offer advanced features to be adopted across all the HMF use cases and lacks presence in data center, cloud and large-enterprise use cases. The vendor is more focused on lower SMBs.
- **Innovation:** The vendor offers basic policy orchestration features across hybrid environments. It lags behind enterprise-grade vendors in advanced policy orchestration features.

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

No vendors were added to this Magic Quadrant.

Dropped

No vendors were dropped from this Magic Quadrant.

Inclusion and Exclusion Criteria

To qualify for inclusion in this Magic Quadrant, 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 its offering generates more than 15% of the total revenue outside the home region
- Meet the HMF market definition as defined by Gartner

A vendor is excluded if any of the following are true:

- It does not qualify as hybrid mesh firewall as per Gartner’s market definition
- Vendor does not sell a dedicated hardware firewall and cloud firewall product line
- Vendor does not offer a cloud-based unified firewall manager
- Vendor does not qualify as a global player because of revenue split as per different geographies

- Vendor only offers FWaaS as a part of its firewall offering
- Vendor only offers cloud firewall as a part of its firewall offering
- Vendor only offers hardware/virtual appliances as part of its firewall offering
- 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 capabilities, features and overall quality of the core goods and services that compete in and/or serve the defined market. This includes current product/service capabilities, quality, feature sets and skills as defined in the market definition and features section.

Sales Execution/Pricing: The organization's capabilities in all presales activities and the structures that support these activities. This includes deal management, pricing and negotiation, presales support and the overall effectiveness of the sales channel. Key areas to be evaluated include growth of the business, how pricing and licensing are offered to customers and their 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 very critical to this section and provides strong evidence for understanding the consumability of the vendor's sales execution in this market.

Market Responsiveness and Track Record: The ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This includes the provider's history of responsiveness to changing market demands. This assesses the vendor's track record, relative to competitors, of delivering effective and customer-aligned capabilities in the platform. Historical evidence of leading the market and timely introduction of features and other offerings completely aligned with customer demand, as per Gartner's analysis, will be evaluated.

Marketing Execution: The ability to deliver clear, high-quality, creative and effective messaging via publicity, promotional activity, thought leadership, social media, referrals and

sales activities. This includes the organization's ability to influence the market, promote the brand, increase awareness of products and establish a positive reputation among customers. We will address the clarity of messaging and its efficiency, as well as whether it is clearly differentiated and aligned with its product capabilities. We also assess investments in marketing and whether these investments are delivering results in terms of how prominently clients consider the vendor. Clarity of messaging and its resonance with customers is critical, as per Gartner's analysis.

Customer Experience: The degree to which a vendor's products, services and programs enable customers to achieve their desired results. This includes the quality of supplier/buyer interactions, technical support or account support, as well as ancillary tools, customer support programs, availability of user groups and service-level agreements. We assess and consider all aspects of the customer experience, including pre- and postsales experience, availability and quality of documentation, technical support and end-user satisfaction with the product. This includes customer feedback directly gathered by Gartner.

Ability to Execute Evaluation Criteria

Evaluation Criteria	*Weighting*
Product or Service	High
Overall Viability	NotRated
Sales Execution/Pricing	High
Market Responsiveness/Record	Medium
Marketing Execution	Medium
Customer Experience	High
Operations	NotRated

Source: Gartner (September 2026)

Completeness of Vision

Market Understanding: The ability to understand customer needs and translate that understanding into products and services. Vendors with a clear vision of the market listen to and understand customer demands, and they can shape or enhance market changes with their vision. This includes the ability to understand and address client needs and identify current and future competitors, as well as possessing self-awareness and a clear understanding of its own strengths and weaknesses in the market.

Marketing Strategy: The ability to clearly communicate differentiated messaging, both internally and externally, through social media, advertising, customer programs and positioning statements. The vendor demonstrates novel and effective approaches to communication and differentiation, as well as forward-looking investments in its marketing program and messaging.

Sales Strategy: The ability to create a sound strategy for selling that uses the appropriate networks, including direct and indirect sales, marketing, service and communication. This includes partnerships that extend the scope and depth of a provider's market reach, expertise, technologies, services and customer base. Vendors demonstrate their vision of sales with the market evolution and changing customer demands.

Offering (Product) Strategy: The ability to approach product development and delivery in a way that meets current and future requirements, with an emphasis on market differentiation, functionality, methodology and features. This includes delivering new features that are relevant to the market as defined by Gartner, address end-users' current and emerging needs, and are delivered in a timely fashion. Gartner evaluates vendors' vision for developing their offerings for this market and the top use cases identified by Gartner.

Vertical/Industry Strategy: The ability to strategically direct resources (e.g., sales, product, development), skills and products to meet the specific needs of verticals and market segments. This includes vendors' ability to identify top verticals and meet their use cases.

Innovation: The ability to marshal resources, expertise or capital for competitive advantage, investment, consolidation or defense against acquisition. This includes vendors' ability to identify emerging use cases and innovate. This is not confined to the technical product capabilities but includes overall offering innovation.

Geographic Strategy: The ability to direct resources, skills and offerings to meet the specific needs of regions outside the provider's home region, either directly or through partners, channels and subsidiaries. This includes 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	High
Geographic Strategy	Low

Source: Gartner (September 2026)

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. Leaders drive 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 positive relationships with its customers and partners on a global basis. Additionally, Leaders possess a product strategy that aligns with market trends 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 fits within a broader network security platform approach.

Challengers

Challengers have a proven ability to address current end-user requirements in the market. Challengers typically have 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. Challengers 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 typically stand out for their strong technical or product strategies and vision, but may lack Leaders' proven execution, visibility or corporate resources, such as robust sales channels and strategic partnerships. 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 for the future, they often lack a consistent, proven ability to address customer challenges in a scalable manner.

Niche Players

Niche Players are often focused on specific portions of the market, such as a particular 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. Niche Players have mature network firewall offerings but still have gaps in their 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

Hybrid mesh firewalls continue to be the most essential security control for preemptive network security in hybrid environments. Enterprises implement HMF for in-line advanced threat prevention with support for high-throughput stateful inspection. Network and security leaders continue to utilize them for different use cases such as perimeter security, network segmentation, multicloud security, branch offices and data centers. This year, Gartner has seen a strong vendor focus on providing end-to-end automation around orchestration and policy management across hybrid environments. There is a growing focus on using AI-based threat detection and correlation to provide predictive analysis and upfront policy recommendations to enable preemptive controls.

End-user adoption trends show a clear shift toward cloud-based management platforms that match on-premises capabilities, as well as growing interest in SMB-focused vendors — a shift driven by cost pressures — and limited support from enterprise providers. Organizations increasingly seek to simplify operations by converging networking and firewall functions under HMFs and are adopting these solutions for branch security and advanced WAN routing use cases. However, adoption challenges remain, including low utilization of AI- and LLM-based automation in daily operations and ongoing complexity and frustration with licensing models.

Our observations indicate a clear market shift toward future-ready, automated and intelligence-driven security platforms. Vendors are prioritizing postquantum cryptography with NIST- and ETSI-aligned hybrid encryption approaches to ensure long-term resilience. Vendors are rapidly advancing cloud-based management platforms with unified control, zero-touch provisioning and telemetry-driven optimization.

The market is moving toward greater automation through LLM-based assistants for policy management and operations, though maturity levels remain uneven. Additionally, there is a strong push toward AI-driven threat prevention, with increasing reliance on predictive analytics and deeper integration with XDR, NDR and EDR ecosystems to deliver more comprehensive and proactive security outcomes.

This Magic Quadrant evaluates 12 vendors across the hybrid mesh firewall market.

Market Overview

Market Drivers

Continuous expansion of hybrid environments: As infrastructure environments become more complex and distributed, network security teams struggle to manage them effectively. Enterprises continue to move toward the cloud, but the landscape remains predominantly hybrid. Although cloud adoption continues to grow, most organizations must also maintain on-premises infrastructure. This diversity leads to greater management complexity and widening skill gaps for teams trying to keep pace.

In-line threat inspection is a critical part of security: HMFs are the first line of defense and can perform in-line inspection of varying volumes of traffic. With decryption capabilities, they can offer full TLS offloading of encrypted traffic, providing deep visibility and inspection.

Advanced threat prevention: Hybrid mesh firewalls deliver advanced threat prevention through a combination of AI/ML-driven detection, real-time zero-day protection and deeply integrated security intelligence across environments. HMFs provide in-line zero-day and advanced malware protection using techniques such as behavioral analysis, multiengine sandboxing and real-time memory inspection to block unknown and polymorphic threats. Beyond traditional IT, HMFs extend protection to IoT, OT and cyber-physical systems through device discovery, protocol-level inspection and risk-based policy recommendations. HMFs are now capable of delivering predictive analytics and recommendations based on enriched data, with integration into XDR, NDR and EDR tools.

Growing focus on preemptive security: HMFs are the core security controls for enforcing network segmentation, enabling preemptive security controls against lateral movement between network segments. With cloud-native and containerized enforcement types, this extends into east-west use cases with distributed firewalling use cases.

Growing multicloud adoption: HMFs directly enable secure multicloud adoption by delivering centralized, cloud-based management that simplifies operations through a unified policy interface and automation extending into a hybrid environment. They integrate with cloud-native environments (e.g., containers, microservices) and major platforms such as AWS, Azure and Google Cloud, supporting consistent security and governance across hybrid and multicloud deployments. Built-in advanced threat protection capabilities make them more trusted by cybersecurity teams.

End-User Adoption Trends

As vendors focus on HMF cloud managers as the primary managers, Gartner clients are evaluating feature parity with their on-premises firewall manager and preparing for smoother migration paths to cloud-based managers.

End users facing pricing and account-management challenges with enterprise-grade vendors want to move toward vendors focused on SMB HMF use cases. Gartner clients report rising costs and limited engagement from enterprise-grade vendors in supporting SMBs.

As multicloud adoption grows, Gartner clients want to converge cloud networking and firewall capabilities within HMF to simplify management and operations.

As enterprises rearchitect branch office segmentation and security use cases, heavy branches continue to see adoption of HMFs that offer advanced WAN routing capabilities and best-of-breed threat inspection.

Although adoption remains in its early stages, end users are not fully utilizing AI-based orchestration and LLM assistants for day-to-day administration, leading to a lack of policy optimization across HMF environments.

Licensing remains a pain point for Gartner clients that must manage different license types across multiple part numbers.

Key Observations

Focus on postquantum cryptography: HMF vendors are showing strong adoption of postquantum cryptography (PQC) capabilities to future-proof enterprise security against quantum threats, with a strong focus on crypto-agility, visibility and phased migration. While Leaders are at different stages of adoption, other vendors have also mentioned a strong roadmap for PQC. Common themes across vendors includes the adoption of NIST-aligned PQC algorithms (e.g., ML-KEM/Kyber and related standards) and support for quantum-safe encryption in VPNs, IPsec and SD-WAN tunnels, often using hybrid cryptography modes that combine classical and PQC algorithms to ensure backward compatibility during the transition.

Maturity of cloud-based manager: Vendors have significantly advanced their unified cloud-based management capabilities over the past year. Most vendors support zero-touch provisioning and offer dynamic policy management and intelligent scaling across hybrid and multicloud infrastructures. Vendors are using additional data enrichment for real-time context

with identities, tags and telemetry to enforce adaptive, intent-driven policies and continuously optimize configurations.

Automation using LLM chat assistant: While all the vendors in this Magic Quadrant offer LLM chat assistants, they still vary considerably in maturity. The key focus has been on natural language interfaces for policy management, threat prevention, operation efficiency and asset discovery. Features developed by the vendors include automated troubleshooting workflows, predictive monitoring, conflict detection and automated policy analysis.

AI-based advanced threat prevention: Vendors are delivering advanced threat prevention through a combination of AI/ML-driven detection, real-time zero-day protection and deeply integrated security intelligence across environments. Beyond traditional IT, they extend protection to IoT, OT and cyber-physical systems through device discovery, protocol-level inspection and risk-based policy recommendations. Vendors are offering predictive analytics and recommendations based on enriched data, with integration into XDR, NDR and EDR tools.

Security for AI: HMF vendors offer capabilities to address various use cases to secure AI. The three key use cases for which HMF vendors have developed capabilities and are showing a strong roadmap are: AI usage control, AI runtime security and AI workload security. Vendors are offering AI-specific App-ID and URL filtering, prompt injection and security controls for the underlying infrastructure (e.g., containers, VMs and clusters) where AI workloads are deployed.

⊕ Evaluation Criteria Definitions