Critical Capabilities for Network Firewalls

Published 17 January 2022 - ID G00740373 - 27 min read

By Analyst(s): Adam Hils, Rajpreet Kaur

Initiatives: Infrastructure Security

Network firewalls are key network security controls, and they are evolving to cover expanded use cases, such as the public cloud, firewall as a service and distributed edge security. SRM leaders must evaluate network firewall capabilities against the most relevant use cases for their organizations.

This Critical Capabilities is related to other research:

Magic Quadrant for Network Firewalls

View All Magic Quadrants and Critical Capabilities

Overview

Key Findings

- Firewall vendors are expanding their product offerings, but these new offerings are rarely tightly integrated with their platforms. New products often require multiple management consoles and multiple agents, and sometimes lack deep integrations between components.
- With the shift toward working from home, firewall vendors offering cloud-based security services with strong cloud security strategies are becoming more desirable to buyers.
- Cloud-first enterprises prefer firewall vendors that support the integrated management of cloud-native firewalls.
- With the shift toward a hybrid workforce, end users are finding less value in on-premises firewalls, and are instead seeking hybrid cloud security from their existing vendors.

Recommendations

Security and risk management (SRM) leaders responsible for infrastructure security and looking to evaluate firewall vendors should:

- Compare vendor products based on the business needs of the organization, rather than attempting to consolidate to a single vendor, given the wide range of offerings available. For example, a data-center-centric organization with many branches may find that pairing a best-of-breed data-center firewall vendor's offering with that of a separate strong firewall as a service (FWaaS) vendor would maximize overall value to the organization.
- Conduct an in-depth evaluation of offerings on the basis of integration and quality of centralized management capabilities, if vendor consolidation is deemed in scope.
- If the organization's primary goal is to migrate security capabilities in the cloud, focus on FWaaS vendors, cloud access security brokers and cloud workload protection platforms.

Strategic Planning Assumptions

By 2025, 30% of refresh opportunities of distributed branch-office firewalls will switch to firewall as a service, up from less than 10% in 2021.

By the end of 2025, 35% of end-user spending on network firewalls will be within larger security deals delivered by enterprise license agreement from a single vendor, up from less than 10% in 2021.

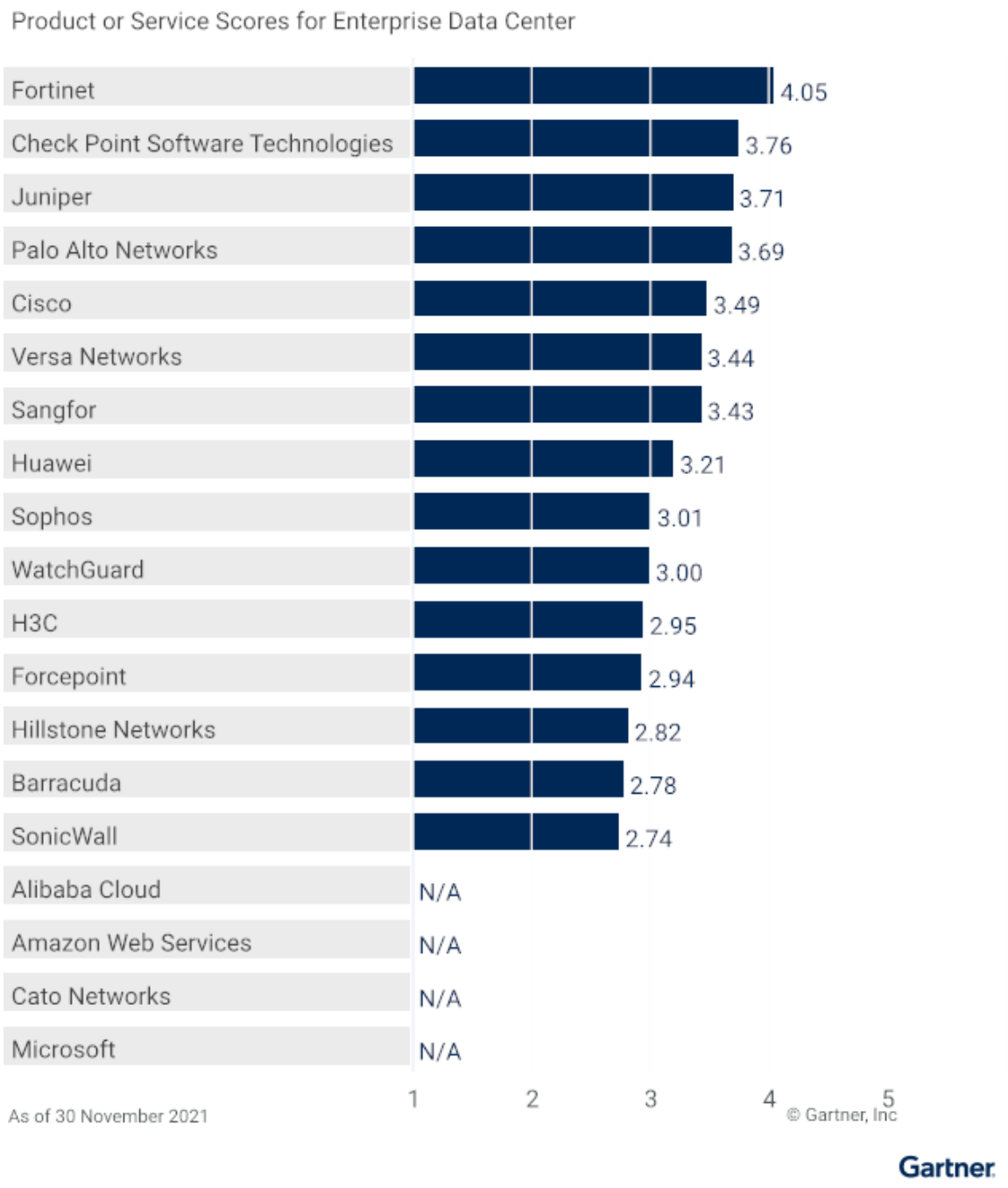
What You Need to Know

Firewall vendors are currently focusing on enhancing advanced threat detection and response capabilities, Internet of Things (IoT) security, integration with the public cloud and ransomware detection and response. In response to the increasing number of hybrid workers at customer organizations, vendors are also focusing on maturing FWaaS capabilities to offer more flexible and location-independent network security controls. The firewall market has recently seen several major acquisitions, especially in the public cloud use case, which includes FWaaS, secure software-defined WAN (SD-WAN) and identity-based segmentation, also known as microsegmentation. Some vendors that provide these capabilities are being acquired by firewall vendors. Network firewall vendors are expanding their product portfolios to meet the demands of organizations that are trying to consolidate their security solutions under a single vendor.

Analysis

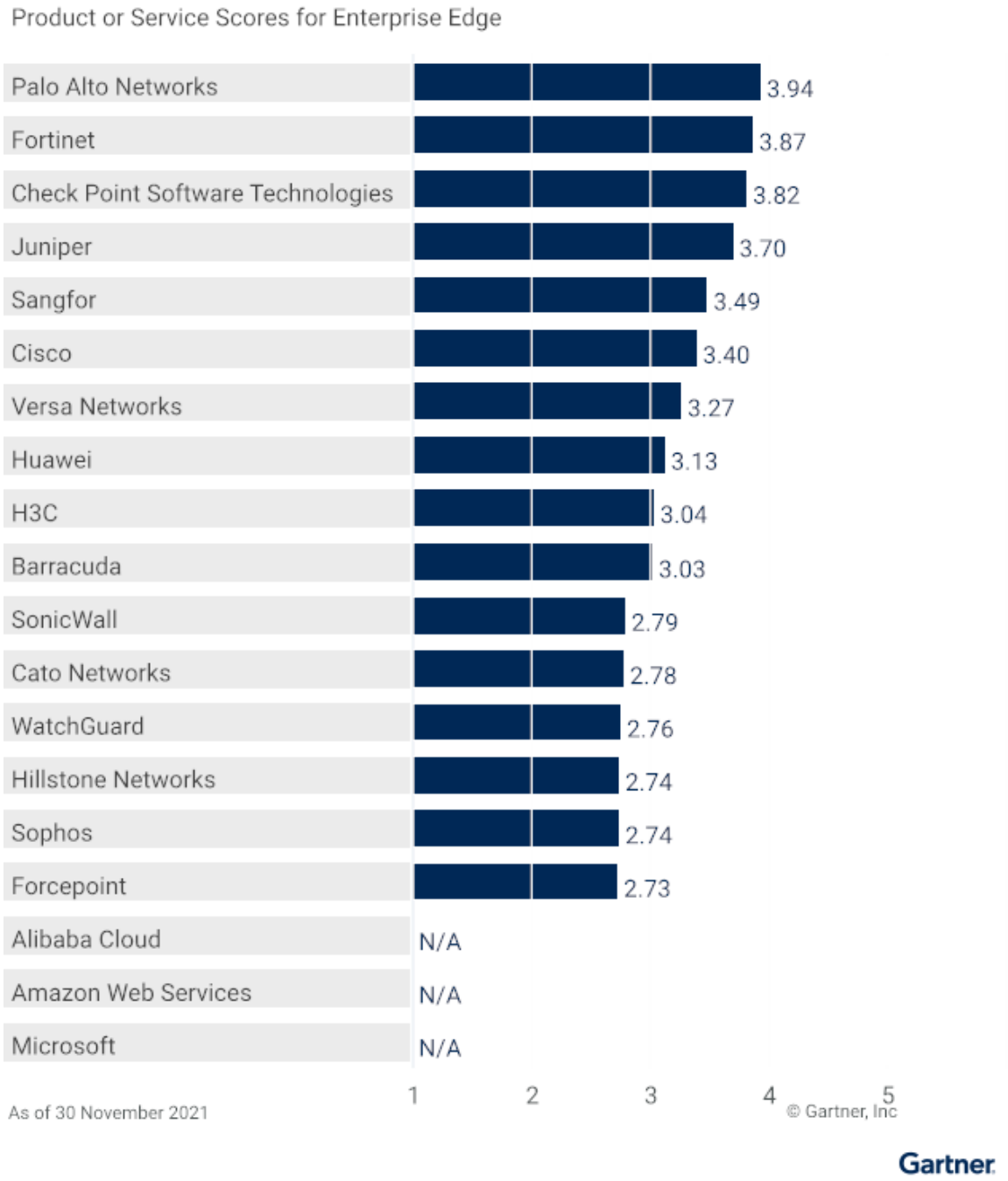
Critical Capabilities Use-Case Graphics

Vendors' Product Scores for Enterprise Data Center Use Case



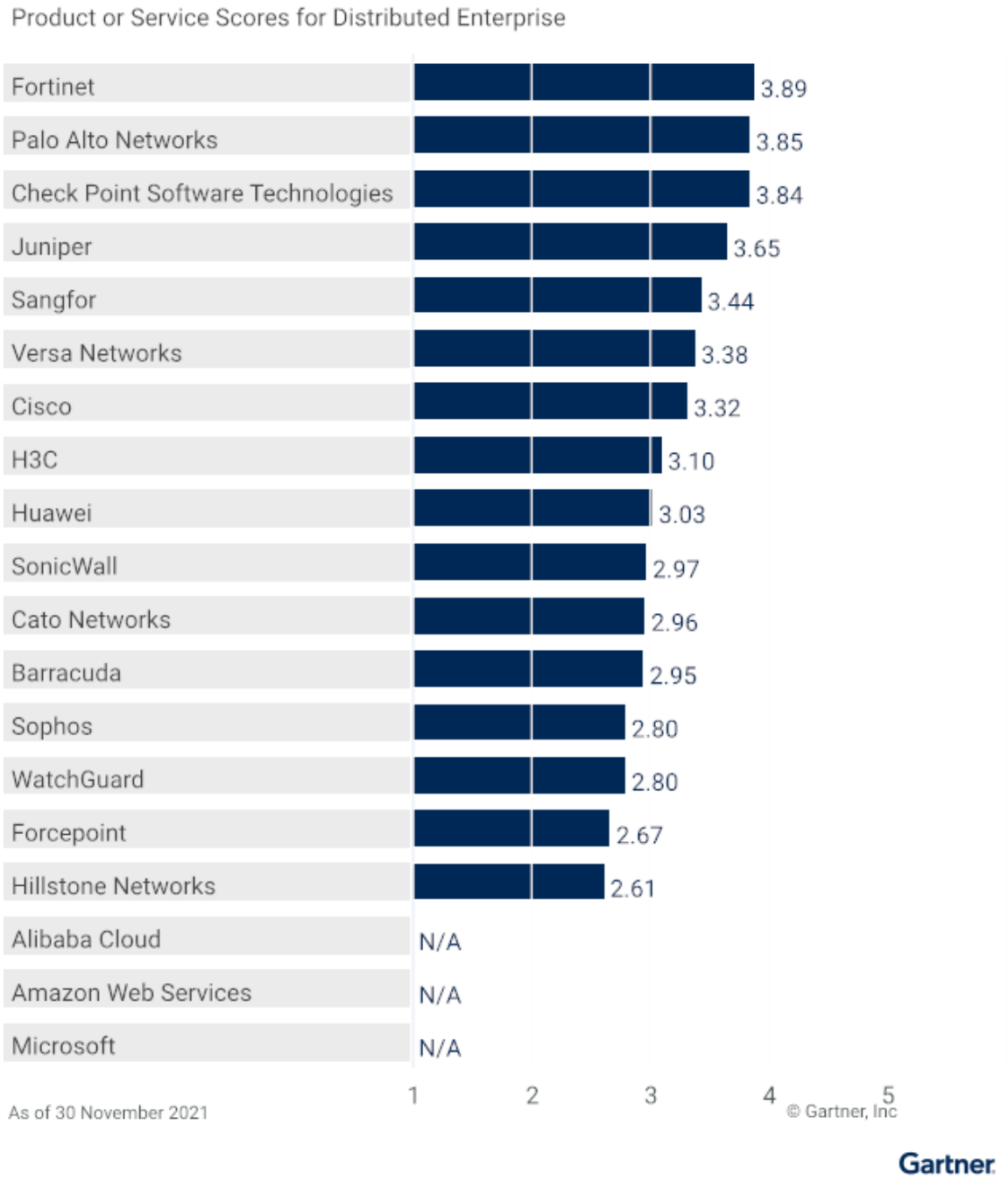
Source: Gartner (January 2022)

Vendors' Product Scores for Enterprise Edge Use Case



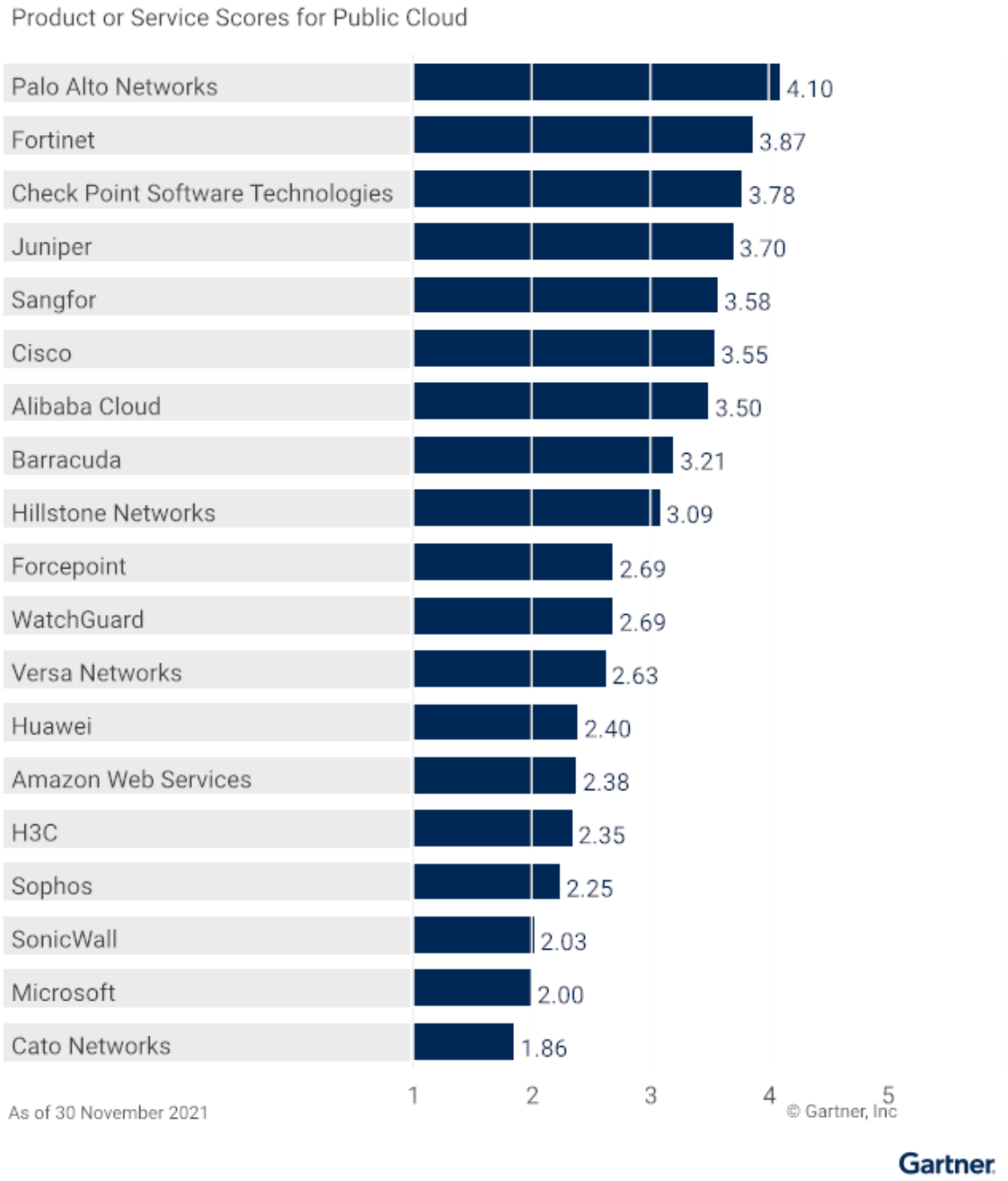
Source: Gartner (January 2022)

Vendors' Product Scores for Distributed Enterprise Use Case



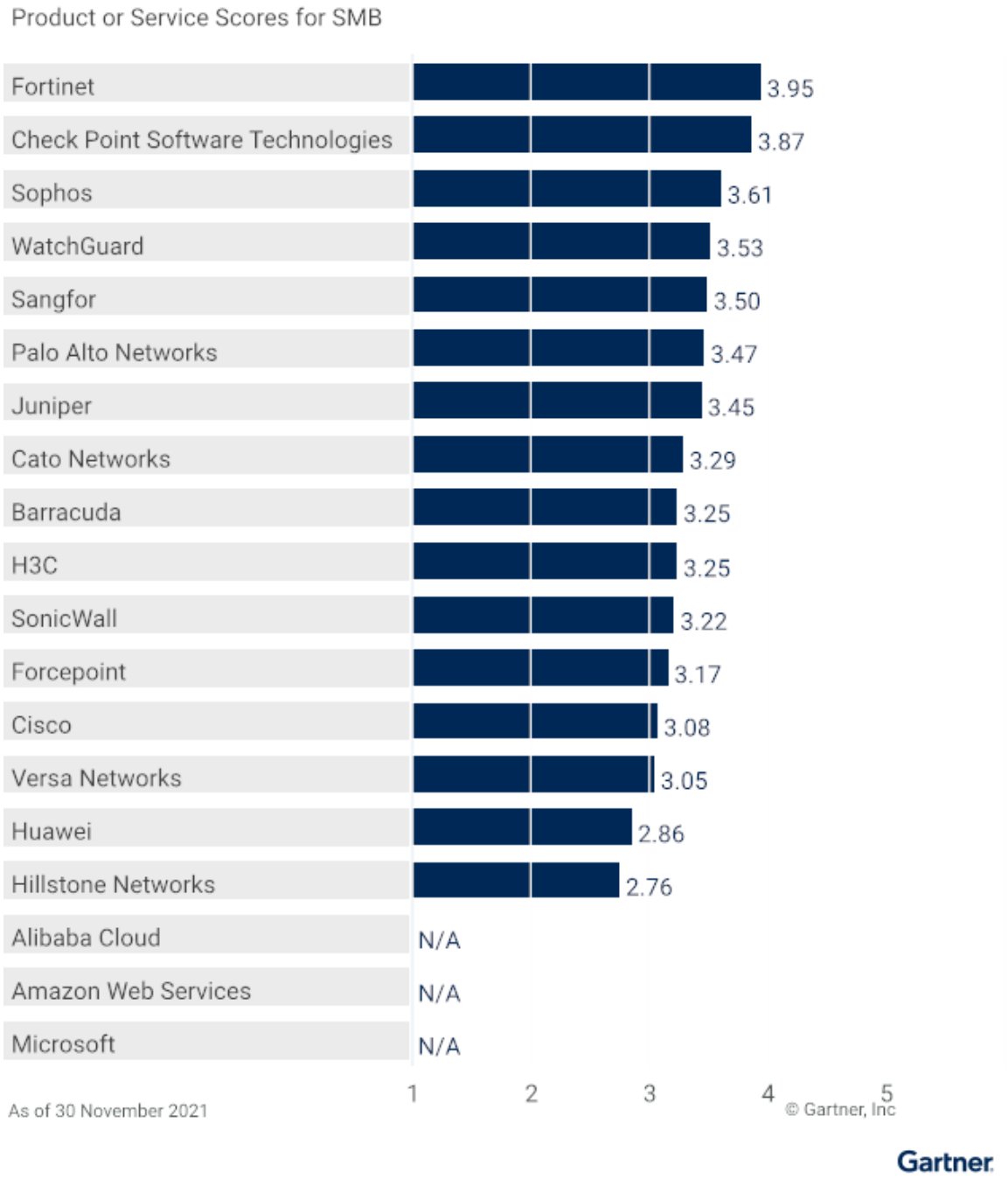
Source: Gartner (January 2022)

Vendors' Product Scores for Public Cloud Use Case



Source: Gartner (January 2022)

Vendors' Product Scores for SMB Use Case



Source: Gartner (January 2022)

Vendors

Alibaba Cloud

Alibaba Cloud offers a public cloud firewall called Alibaba Cloud Firewall, FWaaS and identity-based segmentation only for Alibaba Cloud customers. Alibaba Cloud Security Center enables the centralized management of the firewall and other products offered by this vendor. Furthermore, the Ultimate edition of Alibaba Cloud Firewall has its own centralized manager. In addition to firewalls, Alibaba Cloud offers multiple security offerings, including, for example, distributed denial of service (DDoS) mitigation, a web application firewall, data protection and encryption, and managed security services.

Recent updates have included the introduction of network services and multiple network-security-related features. Key highlights include the introduction of the Cloud Security Access Service (CSAS), with application access control, URL control, zero trust network access (ZTNA) intranet access control and logging capabilities, a container firewall and virtual patching.

Alibaba Cloud has received higher scores than other infrastructure as a service (IaaS)-based security vendors due to its broader support for third-party clouds, as well as its superior central management capabilities. However, although Alibaba Cloud is ahead of other IaaS vendors in advanced security capabilities (including non-IaaS solutions such as advanced threat detection and intrusion prevention), it does lag behind the market as a whole in this area.

Amazon Web Services

Amazon Web Services (AWS) is a global public cloud provider. It offers a number of network security controls for its public cloud customers, including Amazon Virtual Private Clouds (VPC) security groups and an Amazon VPC network access control list. The offering evaluated here is AWS Network Firewall, which was released in November 2020. AWS Firewall Manager centralizes the management of all of AWS's firewall-related offerings, including its web application firewall and DNS firewall.

In the last 12 months, AWS has extended the availability of the AWS Network Firewall to all 23 of its regions.

With its wide geographical coverage and ability to scale firewall capacity on demand, AWS has scored well for scalability. It has also outscored many vendors for ease of use, particularly within infrastructures based mostly on AWS. However, AWS has received lower scores in other categories, such as application control, intrusion prevention and advanced threat detection. While AWS provides seamless firewall integration with the AWS platform, it does not offer network firewall capabilities to secure other cloud environments.

Barracuda

Barracuda offers a firewall primarily for distributed offices and the public cloud use case within the CloudGen Firewall product line. It also offers FWaaS through its secure access service edge (SASE) offering, CloudGen WAN. Firewall Control Center is the centralized firewall manager, and Firewall Insights is the reporting tool.

Recent updates include Internet of Things (IoT), operational technology (OT) and cloud security features. Highlights include the integration of ZTNA (CloudGuard Access) and the addition of security features to CloudGen WAN. Barracuda has also announced a partnership with Crosser to manage firewall configuration changes for OT environments.

Barracuda is suitable for distributed offices and infrastructure as a service (IaaS) firewall use cases. Its solution integrates well with native AWS and Microsoft Azure controls when compared with most of its competitors in the firewall market. However, Barracuda does not yet offer a container firewall or ID segmentation.

Barracuda does not offer a cloud-based centralized firewall manager, due to which it received low scores for ease of management.

Cato Networks

Cato Networks offers FWaaS through its Cato SASE Cloud product. Although there is a hardware component called Cato Socket for a software-defined wide-area network (SD-WAN), this component requires Cato's cloud components. No stand-alone firewall or virtual appliance firewall is offered. The Cato Management Application manages all of Cato's product offerings.

Recent updates focus on building SASE capabilities. ZTNA capabilities are now available in an agentless format, which increases the breadth of users that can be protected by Cato SASE Cloud beyond the SD-WAN use case.

Cato offers FWaaS, ZTNA and SD-WAN through its SASE offering only for the distributed offices and roaming users use cases. However, the vendor lacks the required appliances for the data center and very-high-bandwidth enterprise perimeter use cases.

Cato offers undifferentiated URL filtering features, but lacks the required granularity of application control for client-based applications and data loss prevention (DLP) capabilities.

Check Point Software Technologies

Check Point offers a comprehensive security portfolio that features Quantum-branded hardware appliances, such as the recently released Maestro Hyperscale product line. Check Point also offers virtual appliances and cloud security products under the CloudGuard brand, plus a FWaaS product that comes under the Harmony brand and is used for Check Point's SASE solutions. Check Point offers on-premises (Quantum Security Management) and cloud-hosted (Infinity portal) centralized management and monitoring products.

In the last 12 months, Check Point has released new Maestro appliances and container firewalls. Software features include autonomous threat prevention, which makes configuration easier, Transport Layer Security (TLS) 1.3 support with detection of fake server name identification (SNI), and various improvements to management and monitoring consoles.

Check Point scored highly for the performance of its hardware firewalls, particularly for the enterprise perimeter and data center use cases. Check Point also scored highly for advanced threat prevention and centralized firewall management.

Check Point does not offer the ability to import policies from on-premises or cloud-based DLP tools and does not support the tokenization or decryption of data in SaaS applications. The vendor does not offer a native SD-WAN offering, instead using partners' products. As a result, Check Point received a lower score for the distributed offices use case than many of its direct competitors.

While many firewall vendors are expanding toward cloud security use cases, Check Point lacks an agent-enabled identity-based segmentation offering, and was also late to introduce container firewalls.

Cisco

Cisco offers multiple firewall product lines, including Cisco Secure Firewall (formerly Firepower), Cisco Secure Workload (formerly Tetration) and the Meraki MX series. In addition, Cisco offers Umbrella Secure Internet Gateway (SIG) for FWaaS, and industrial firewalls (the Secure Firewall Industrial Security Appliance [ISA] series). Cisco Secure Firewall Management Center (on-premises) and Cisco Defense Orchestrator (cloud-based) are Cisco's centralized managers.

During the evaluation period for this Critical Capabilities report, Cisco released six Firepower Threat Defense (FTD) virtual appliances, a container firewall and Cisco Managed Remote Access, a managed VPN solution. Another important update is multicloud management and control with the integration of Secure Workload and Secure Firewall.

Cisco's wide range of firewall offerings helped it to score well in some specific use cases. However, this diversity also hurt Cisco's ease-of-use score.

Because Cisco offers integrated SD-WAN, especially through its Meraki product line, as well as being able to support multiple protocols, the vendor scored well for advanced networking.

Cisco's intrusion prevention system (IPS) and advanced threat detection capabilities, which are included in all of its firewall offerings, helped it to receive high scores in enterprise use cases. However, it scored lower for application control due to its comparatively low granularity (relative to other major vendors) at Layer 7.

Forcepoint

Forcepoint's firewall appliance has built-in SD-WAN capabilities. Forcepoint also has several virtual appliance models. In addition to network firewalls, Forcepoint offers DLP, CASB and SWG product lines.

During the evaluation period, Forcepoint introduced several new firewall models, notably the N60 and N120WL at the low end. Other updates included increased SD-WAN performance to enable faster SD-WAN firewall edge connectivity, further enhancements to AWS and Azure integrations, and an additional IPS engine to enable open-source signature compatibility with Snort.

Forcepoint firewalls are aimed primarily toward the distributed offices use case, where clients are looking for mature threat prevention capabilities. Forcepoint offers mature integration with AWS and Azure for public cloud firewall use cases. Despite its strong SWG offering, Forcepoint has yet to offer FWaaS or a cloud-based centralized manager.

Fortinet

Fortinet's FortiGate firewall product line is available for all firewall deployment use cases. FortiGate is also available in virtual appliances for public cloud platforms such as AWS, Microsoft Azure, Google Cloud Platform (GCP), VMware Cloud, Oracle Cloud Infrastructure (OCI), IBM Cloud and AliCloud. Fortinet recently released FortiGate FWaaS, following its acquisition of OPAQ, which has been rebranded as FortiSASE. FortiManager and FortiGate Cloud are Fortinet's centralized managers, and FortiAnalyzer and FortiCloud are its centralized reporting tools. In addition to firewall, Fortinet has a broad security portfolio, which, in addition to firewalls, includes capabilities such as endpoint detection and response (EDR), web application firewall/web application and API protection (WAF/WAAP), network access control (NAC), deception, and identity and access management (IAM). All of these capabilities are integrated with FortiGate, and many are controlled by the same management system.

Recent updates include the introduction of security operations center (SOC) as a service, SASE and ZTNA product offerings. Fortinet has also introduced enhancements to its URL filtering and advanced threat detection features. Additionally, it has introduced integration between network operations center (NOC) and SOC operations in the Fabric Management Center.

Due to its differentiated hardware approach, Fortinet is highly scalable, and it offers advanced SD-WAN integrated with its branch firewalls. Fortinet's security fabric also helped receive it a high score for ease of use. However, Fortinet has yet to integrate identity-based segmentation into its offering, and its FWaaS has not been fully integrated into FortiSASE, which leaves the vendor with two immature FWaaS offerings.

H3C

H3C offers a full range of hardware firewalls, known as SecPath, for small, midsize and large environments. SecPath is also available as a virtual appliance. H3C's FWaaS is SeerEngine-DC. Three central management solutions are available: iMC Security Service Manager, SecCenter Security Management Platform and SecCenter Cybersecurity Situational Awareness Platform.

H3C has continued to invest heavily in security and detection capabilities. Deception, user behavior analytics, workflows aligned with the Cyber Kill Chain and asset risk assessment are among the most recent additions. Incremental improvements include web and DNS detection, and flagging illegal content and weak passwords.

H3C has strong cloud support for its FWaaS relative to other regional vendors, which helped it score highly for the distributed enterprise use case. H3C also scored well for application control. However, it received a low score for public cloud support, as it lacks support for some major IaaS providers.

Hillstone Networks

Hillstone offers multiple firewall product lines to meet different deployment use cases. Its hardware firewalls are sold as A-Series NGFW, E-Series NGFW, T-Series NGFW and X-Series Data NGFW. Hillstone sells the CloudEdge virtual firewall, CloudHive identity-based segmentation, the hosted CloudPano FWaaS for service providers, and the containerized CloudArmour firewall. The Hillstone Security Management (HSM) platform is its centralized firewall manager, and Hillstone CloudView is its cloud-based security management system. Hillstone also offers dedicated advanced reporting tools, such as the Hillstone Security Audit (HSA) platform and the Hillstone iSource XDR platform. In addition to firewalls, Hillstone has a broad portfolio including network security, cloud security and security operations product lines.

Recent updates include a new firewall product line, a cloud data lake and a cloud threat analytics platform. In addition, Hillstone has made feature enhancements related to policy orchestration and improved its IP reputation database.

Hillstone's advanced reporting tools, such as HSA, helped it to score highly relative to its regional competitors. Hillstone also supports some global public clouds, which helped it score highly in the cloud support use case.

However, Hillstone lacks a direct FWaaS offering. CloudPano is a hosted FWaaS offering sold directly by managed security service providers and local carriers in China. Due to this, Hillstone did not score highly in the distributed enterprise use case.

Huawei

Huawei offers different firewall product lines for different use cases. USG and Eudemon are its hardware firewall product lines. The Huawei Cloud firewall is for virtual and cloud firewall use cases. Huawei offers different centralized managers: eSight, iMaster NCE and SecoManager. HiSec LogAuditor is its centralized reporting tool.

Recent updates have enhanced Huawei's advanced threat detection and SD-WAN capabilities. Highlights include improved hardware performance for higher USG firewall models and enhancements to Huawei Cloud firewall features.

Huawei's firewalls scored highly for its price/performance ratio in the high throughput data center hardware appliances and enterprise perimeter use cases. However, Huawei did not score highly for cloud security use cases, as its offerings are primarily for Huawei Cloud and do not support international public clouds such as AWS and Azure.

Huawei also lacks an FWaaS offering, which reduced its score for the distributed offices use case. Huawei also needs to improve its firewalls' application control support to cover more applications from outside China.

Juniper

Juniper's firewall product line is the SRX series of next-generation firewalls, which is available as hardware appliances, virtual appliances (vSRX) and containers (cSRX). vSRX can be hosted on the customer's own hypervisor or run on AWS, Microsoft Azure, GCP, IBM Cloud Platform or OCI. In addition to firewalls, Juniper offers security information and event management (SIEM), DDoS mitigation and threat intelligence (TI).

Recent updates include enhancements to advanced threat detection capabilities, IoT security, and partnerships for industrial control system (ICS) and supervisory control and data acquisition (SCADA) environments.

Juniper's Security Director management platform enabled it to score highly for central management and ease of use, increasing its suitability for the SMB and data center use cases. Its containerized firewall and broad support for global public clouds enhanced its score for cloud security support. However, Juniper vendor lacks advanced DLP, which negatively affected its overall application control score.

Microsoft

The Microsoft Azure Firewall offering is available as two subscriptions: Standard and Premium. It can be centrally managed by Azure Firewall Manager and monitored using Azure Monitor and Azure Sentinel.

Microsoft recently introduced the Firewall premium subscription. It has also added fully qualified domain name (FQDN) filtering to its network rules, and TLS decryption to its application rules.

Microsoft is currently adding a range of new security enhancements, many features of which are likely to enhance its overall security posture. Microsoft's FWaaS offering is easy to implement within Azure environments, and its central management scores well in those use cases. However, Microsoft's lack of application control, advanced intrusion prevention and threat detection hinder its ability to service best-of-breed security use cases. Microsoft also does not support multicloud use cases.

Palo Alto Networks

Palo Alto Networks offers different firewalls for different deployment use cases: hardware firewalls (PA-Series), virtual firewalls (VM-Series), FWaaS (Prisma Access) and containerized firewalls (CN-Series). It also offers identity-based segmentation (Prisma Cloud). Their firewall centralized manager is Panorama, which is offered both as hardware and as a virtual appliance. In addition to firewalls, Palo Alto Networks offers endpoint security, cloud security and security operations products.

Recent updates include new features and enhancements across the firewall offerings. Highlights include new security subscriptions, namely IoT security, enterprise DLP, SaaS security and advanced URL filtering in the latest firewall firmware. Other key feature updates include enhancements to the IoT security, IPS and DNS security features.

Palo Alto Networks scored highly in advanced threat detection because of the quality of its threat research and the large number of customers with Wildfire deployed. The vendor also offers mature FWaaS with wide geographic availability and features such as DLP and SD-WAN, which helped it score highly in the distributed offices use case. Palo Alto Networks' cloud firewall offering supports the majority of cloud platforms, and its dedicated identity segmentation and containerized firewall offerings scored highly for the cloud firewall use case.

However, Palo Alto Networks received a low score for its centralized management feature, as it currently only offers cloud-based centralized firewall management for Prisma Access. Prisma Cloud cannot be managed from Panorama without an additional plugin.

Although Palo Alto Networks has improved its price/performance ratio through its recent hardware releases, it still receives a low score in this area. This is due to its high total cost of ownership (TCO), which makes it the most expensive firewall vendor in the market.

Sangfor

Sangfor offers a broad range of hardware firewalls to suit the throughput requirements of small to large environments. Its Next-Generation Application Firewall (NGAF) offering is also available as a virtual appliance. Sangfor Cloud Fortress Access is its FWaaS solution, and Sangfor Access is its SASE solution. Sangfor CWPP is its container firewall and identity segmentation offering. Sangfor Central Manager is its on-premises central management offering, and Sangfor Platform-X is its cloud-based central management offering.

Recent additions to the Sangfor firewall focus on deeper security capabilities, including integrated deception and user and entity behavior analytics (UEBA) capabilities. Sangfor has also enhanced its threat detection capabilities.

Sangfor is much more Layer 7-oriented than its regional competitors, and scored highly in most advanced security categories. It also scored well for its FWaaS due to having both a regional and global cloud presence, and its containerized firewall enhances its cloud security rating. However, Sangfor's lack of central management control and visibility into cloud security and software-defined networking environments reduced its central management scores.

SonicWall

SonicWall markets three hardware appliance firewall product lines — the TZ, NSa and NSsp series — and a virtual appliance firewall product line, the NSv series. The NSv series can be hosted on the customer's own hypervisor or found in the marketplaces of AWS and Microsoft Azure. Network Security Manager is SonicWall's centralized management and reporting tool. In addition to firewalls, SonicWall sells integrated EDR, SEG, ZTNA, VPN and CASB capabilities, sandboxing technology, wireless access points (WAPs) and switches.

Recent updates include multiple enhancements to the centralized manager, including rule optimization and SD-WAN workflow to simplify branch onboarding. SonicWall also finished rolling out its Gen 7 firewall product line. The vendor has introduced centralized management for SonicWall Switch, SonicWall Access Point and SonicWall Next-Gen Endpoint.

SonicWall's strong built-in SD-WAN and quality of service (QoS) capabilities helped it score highly in advanced networking. It also has a competitive FWaaS offering. However, SonicWall lacks certification in most prominent public clouds aside from AWS, which hurt its public cloud support rating.

Sophos

Sophos's firewall product lines include Sophos Firewall (formerly XG). Sophos also continues to support its SG UTM product line for existing SMB customers. It also offers cloud security posture management (CSPM; Cloud Optix) and a centralized management portal (Sophos Central). InterceptX is the brand name for its endpoint and server protection (including for cloud workloads). Sophos also offers other security product lines, such as endpoint security, email protection and managed detection and response services.

Recent updates have included a hardware refresh (XGS Series and SD-RED). Sophos has also continued to improve its integration with IaaS platforms and its centralized management and monitoring portals. Other features include performance improvements for its VPN and high availability, and refined TLS certificate management.

Sophos offers a single management and threat correlation portal for its firewall and endpoint layers, which helped increase its ease-of-use rating. However, Sophos lacks a cloud-delivered FWaaS, so it received a low score for the FWaaS category. Sophos does not offer identity-based segmentation or container firewalls, which negatively impacted its public cloud support score.

Versa Networks

Versa Networks' primary firewall offering is a FWaaS, part of its SASE product line. As an established network vendor, Versa also offers on-premises firewalls within its Versa Secure SD-WAN appliances, which are available with tiered licenses (the Next Generation Firewall [NGFW] tier being a full network firewall subscription). Versa Concerto is the company's centralized management and reporting portal.

Recent updates include the introduction of CASB, DLP, advanced threat protection (ATP) and host information profile services to its SASE offering, Versa SASE.

Versa's ability to scale its firewall with minimal latency at a low cost per user raised its scalability score, while its multitenant FWaaS management portal helped raise its FWaaS capability score. However, Versa does not offer Kubernetes labeling or posture management capabilities for a cloud environment, which reduced its public cloud support score.

WatchGuard

WatchGuard offers firewalls to meet SMB and branch office use cases. The name of its firewall product line is WatchGuard Firebox. WatchGuard also offers virtual firewalls for AWS, Azure and virtualized environments. WatchGuard Cloud (cloud) and WatchGuard System Manager (on-premises/virtual) are the vendor's centralized firewall managers. WatchGuard Cloud Visibility (cloud) and Dimension (on-premises/virtual) are its centralized reporting tools.

Recent updates include enhancements to Firebox management and cloud management of SD-WANs and VPNs, direct integration with AuthPoint and an endpoint product, and endpoint integrity enforcement for mobile VPNs.

WatchGuard's threat detection integrates seamlessly with numerous endpoint protection offerings from third-party vendors, which positively affected WatchGuard's ease-of-use score. However, WatchGuard is present only in the AWS and Microsoft Azure public clouds, and does not hold any certifications for public clouds, which reduced its public cloud support score.

Context

With the growing hybrid networks, firewall vendors are adding new features/products to meet different firewall deployment use cases. This research evaluates the technical capabilities of firewall vendors for different deployment use cases.

Product/Service Class Definition

Network firewalls have the capability to support one or more firewall deployment use cases, such as perimeter, SMBs, data center, enterprise edge, cloud and distributed offices. This market is no longer restricted to appliance-only vendors. It extends to vendors offering virtual versions, FWaaS offered as native firewall controls or dedicated offerings by public and private cloud vendors.

Security and risk management (SRM) leaders must consider the best use case for which they want to procure the firewall and use the Critical Capabilities note to shortlist the vendor suited for their use case.

This Critical Capabilities research includes the following types of network firewalls:

- Purpose-built physical appliances
- Virtual appliances

- Embedded firewall modules
- Firewall controls delivered from IaaS platform providers
- Dedicated FWaaS, which is a service directly hosted and sold by the vendor; it is not a hosted firewall service offered by MSS, telcos or any other partner.

Critical Capabilities Definition

Central Management and Reporting

The ability to manage policy, dispense updates, capture event logs, display threats and maintain visibility for multiple separate firewall instances. This capability captures the availability of management form factors, including cloud-based management. It evaluates meaningful summaries of activities aimed to show security posture and meet compliance requirements.

Scalability

The capability to meet capacity needs, including throughput, concurrent connections, connections per second and connectivity. To achieve a high rating, vendors must show the ability to scale up and down to meet the needs of customers' environments. Clustering and other high-availability capabilities are also considered.

Ease of Use

The ease with which users can install, configure, manage and update network firewalls.

Advanced Networking

Networking features and functionality, such as integrated SD-WAN, that enable the organization to adapt to new trends in the marketplace.

Application Control

The ability to add fine-grained application awareness to traffic, adding application context to the inspection stream.

FWaaS

The ability to provide fully featured firewall inspection to support the branch office and remote worker use cases.

Intrusion Prevention and ATD

IPS is a system that monitors a network for malicious activities, such as security threats or policy violations. The main functions of an IPS are identifying, blocking and reporting suspicious activities and maintaining a log of information on such activities.

This capability also encompasses any functionality through which a product analyzes threats, such as network sandboxing and traffic analysis. Another factor is the ability to use internal and external TI.

Public Cloud Support

Support for various IaaS platforms using either virtual appliances or innovative integrated cloud-based technologies.

Pricing

The ability to provide firewall functionality at competitive price points, taking into account corresponding performance. Feature and support pricing are also evaluated.

Use Cases

Enterprise Data Center

The use of firewalls to protect the enterprise data center and to perform segmentation inside the enterprise data center. The ability to address both ingress and egress traffic at scale.

Enterprise Edge

The use of firewalls to protect the enterprise perimeter.

Distributed Enterprise

The deployment of virtual firewalls in IaaS environments, as well as the deployment of firewalls at multiple branches of an enterprise.

Public Cloud

The deployment of virtual firewalls in IaaS environments.

SMB

The use of firewalls designed for small and midsize businesses, taking into account pricing and functionality.

Vendors Added and Dropped

Added

- Alibaba Cloud
- Amazon Web Services
- Cato Networks
- Versa Networks

Dropped

- Stormshield
- Venustech

Inclusion Criteria

Table 1: Weighting for Critical Capabilities in Use Cases

(Enlarged table in Appendix)

Critical Capabilities	*Enterprise Data Center*	*Enterprise Edge*	*Distributed Enterprise*	*Public Cloud*	*SMB*
Central Management and Reporting	10%	10%	15%	10%	5%
Scalability	30%	10%	10%	5%	0%
Ease of Use	10%	5%	10%	10%	30%
Advanced Networking	15%	15%	15%	5%	10%
Application Control	5%	15%	10%	5%	10%
FWaaS	0%	10%	15%	0%	5%
Intrusion Prevention and ATD	15%	15%	10%	10%	10%
Public Cloud Support	5%	10%	5%	50%	0%
Pricing	10%	10%	10%	5%	30%
As of 30 November 2021					

Source: Gartner (January 2022)

This methodology requires analysts to identify the critical capabilities for a class of products/services. Each capability is then weighted in terms of its relative importance for specific product/service use cases.

Each of the products/services that meet our inclusion criteria has been evaluated on the critical capabilities on a scale from 1.0 to 5.0.

Critical Capabilities Rating

Table 2: Product/Service Rating on Critical Capabilities

(Enlarged table in Appendix)

Critical Capabilities	Alibaba Cloud	Amazon Web Services	Barracuda	Cato Networks	Check Point Software Technologies	Cisco	Forcepoint	Fortinet	H3C	Hillstone Networks	Huawei	Juniper	Microsoft	Palo Alto Networks	Sangfor	SonicWall	Sophos	Versa Networks	WatchGuard
Central Management and Reporting	3.0	1.9	2.0	2.1	4.2	3.5	2.5	3.8	1.9	1.6	1.9	4.0	2.3	3.7	2.4	2.7	3.0	3.1	3.1
Scalability	3.5	2.8	2.0	3.5	3.6	3.5	2.7	4.3	3.0	3.0	4.0	3.7	3.7	3.3	3.5	2.3	2.5	4.3	2.5
Ease of Use	3.0	2.7	3.0	2.5	4.2	2.2	3.3	4.1	2.7	2.0	1.5	3.2	1.7	3.0	3.3	3.3	4.2	2.7	4.0
Advanced Networking	3.4	1.8	3.6	3.2	3.3	3.9	3.3	4.2	3.9	3.1	3.7	4.0	1.2	4.1	3.7	4.0	3.1	3.8	3.3
Application Control	2.8	1.0	3.2	2.0	4.3	2.3	2.8	3.5	3.2	2.0	3.6	3.8	1.0	3.9	3.4	2.7	2.8	2.8	2.5
FWaaS	3.0	1.0	3.0	4.0	3.8	3.0	1.0	3.5	4.1	2.3	3.3	3.2	3.5	4.5	3.9	3.5	1.0	4.4	1.0
Intrusion Prevention and ATD	2.2	1.9	2.8	2.1	4.0	4.2	2.8	3.8	2.3	2.8	3.1	3.9	1.3	4.6	3.4	2.0	3.0	3.0	2.5
Public Cloud Support	4.0	2.5	3.6	1.0	3.6	3.8	2.4	3.8	1.9	3.7	2.0	3.7	2.0	4.5	3.9	1.2	1.2	2.1	2.2
Pricing	3.8	3.9	3.8	5.0	3.5	3.5	3.7	4.0	4.0	3.9	3.7	3.2	3.5	3.0	3.8	3.5	4.2	3.0	4.3
As of 30 November 2021																			

Source: Gartner (January 2022)

Table 3 shows the product/service scores for each use case. The scores, which are generated by multiplying the use-case weightings by the product/service ratings, summarize how well the critical capabilities are met for each use case.

Table 3: Product Score in Use Cases

(Enlarged table in Appendix)

Use Cases	Alibaba Cloud	Amazon Web Services	Barracuda	Cato Networks	Check Point Software Technologies	Cisco	Forcepoint	Fortinet	H3C	Hillstone Networks	Huawei	Juniper	Microsoft	Palo Alto Networks	Sangfor	SonicWall	Sophos	Versa Networks	WatchGuard
Enterprise Data Center	N/A	N/A	2.78	N/A	3.76	3.49	2.94	4.05	2.95	2.82	3.21	3.71	N/A	3.69	3.43	2.74	3.01	3.44	3.00
Enterprise Edge	N/A	N/A	3.03	2.78	3.82	3.40	2.73	3.87	3.04	2.74	3.13	3.70	N/A	3.94	3.49	2.79	2.74	3.27	2.76
Distributed Enterprise	N/A	N/A	2.95	2.96	3.84	3.32	2.67	3.89	3.10	2.61	3.03	3.65	N/A	3.85	3.44	2.97	2.80	3.38	2.80
Public Cloud	3.50	2.38	3.21	1.86	3.78	3.55	2.69	3.87	2.35	3.09	2.40	3.70	2.00	4.10	3.58	2.03	2.25	2.63	2.69
SMB	N/A	N/A	3.25	3.29	3.87	3.08	3.17	3.95	3.25	2.76	2.86	3.45	N/A	3.47	3.50	3.22	3.61	3.05	3.53
As of 30 November 2021																			

Source: Gartner (January 2022)

To determine an overall score for each product/service in the use cases, multiply the ratings in Table 2 by the weightings shown in Table 1.

Critical Capabilities Methodology

This methodology requires analysts to identify the critical capabilities for a class of products or services. Each capability is then weighted in terms of its relative importance for specific product or service use cases. Next, products/services are rated in terms of how well they achieve each of the critical capabilities. A score that summarizes how well they meet the critical capabilities for each use case is then calculated for each product/service.

"Critical capabilities" are attributes that differentiate products/services in a class in terms of their quality and performance. Gartner recommends that users consider the set of critical capabilities as some of the most important criteria for acquisition decisions.

In defining the product/service category for evaluation, the analyst first identifies the leading uses for the products/services in this market. What needs are end-users looking to fulfill, when considering products/services in this market? Use cases should match common client deployment scenarios. These distinct client scenarios define the Use Cases.

The analyst then identifies the critical capabilities. These capabilities are generalized groups of features commonly required by this class of products/services. Each capability is assigned a level of importance in fulfilling that particular need; some sets of features are more important than others, depending on the use case being evaluated.

Each vendor's product or service is evaluated in terms of how well it delivers each capability, on a five-point scale. These ratings are displayed side-by-side for all vendors, allowing easy comparisons between the different sets of features.

Ratings and summary scores range from 1.0 to 5.0:

1 = Poor or Absent: most or all defined requirements for a capability are not achieved

2 = Fair: some requirements are not achieved

3 = Good: meets requirements

4 = Excellent: meets or exceeds some requirements

5 = Outstanding: significantly exceeds requirements

To determine an overall score for each product in the use cases, the product ratings are multiplied by the weightings to come up with the product score in use cases.

The critical capabilities Gartner has selected do not represent all capabilities for any product; therefore, may not represent those most important for a specific use situation or business objective. Clients should use a critical capabilities analysis as one of several sources of input about a product before making a product/service decision.

Document Revision History

Critical Capabilities for Network Firewalls - 10 November 2020

Critical Capabilities for Network Firewalls - 11 December 2019

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Magic Quadrant for Network Firewalls

How Products and Services Are Evaluated in Gartner Critical Capabilities

Gartner Peer Insights 'Lessons Learned': Implementing Network Firewalls

Table 1: Weighting for Critical Capabilities in Use Cases

Critical Capabilities	*Enterprise Data Center*	*Enterprise Edge*	*Distributed Enterprise*	*Public Cloud*	*SMB*
Central Management and Reporting	10%	10%	15%	10%	5%
Scalability	30%	10%	10%	5%	0%
Ease of Use	10%	5%	10%	10%	30%
Advanced Networking	15%	15%	15%	5%	10%
Application Control	5%	15%	10%	5%	10%
FWaaS	0%	10%	15%	0%	5%
Intrusion Prevention and ATD	15%	15%	10%	10%	10%
Public Cloud Support	5%	10%	5%	50%	0%
Pricing	10%	10%	10%	5%	30%
As of 30 November 2021					

Source: Gartner (January 2022)

Table 2: Product/Service Rating on Critical Capabilities

Critical Capabilities	*Alibaba Cloud*	*Amazon Web Services*	*Barracuda*	*Cato Networks*	*Check Point Software Technologies*	*Cisco*	*Forcepoint*	*Fortinet*	*H3C*	*Hillstone Networks*	*Huawei*	*Juniper*	*Microsoft*	*Palo Alto Networks*	*Sangfor*	*SonicWall*	*Sophos*	*Versa Networks*	*WatchGuard*
Central Management and Reporting	3.0	1.9	2.0	2.1	4.2	3.5	2.5	3.8	1.9	1.6	1.9	4.0	2.3	3.7	2.4	2.7	3.0	3.1	3.1
Scalability	3.5	2.8	2.0	3.5	3.6	3.5	2.7	4.3	3.0	3.0	4.0	3.7	3.7	3.3	3.5	2.3	2.5	4.3	2.5
Ease of Use	3.0	2.7	3.0	2.5	4.2	2.2	3.3	4.1	2.7	2.0	1.5	3.2	1.7	3.0	3.3	3.3	4.2	2.7	4.0
Advanced Networking	3.4	1.8	3.6	3.2	3.3	3.9	3.3	4.2	3.9	3.1	3.7	4.0	1.2	4.1	3.7	4.0	3.1	3.8	3.3
Application Control	2.8	1.0	3.2	2.0	4.3	2.3	2.8	3.5	3.2	2.0	3.6	3.8	1.0	3.9	3.4	2.7	2.8	2.8	2.5

FWaaS	3.0	1.0	3.0	4.0	3.8	3.0	1.0	3.5	4.1	2.3	3.3	3.2	3.5	4.5	3.9	3.5	1.0	4.4	1.0
Intrusion Prevention and ATD	2.2	1.9	2.8	2.1	4.0	4.2	2.8	3.8	2.3	2.8	3.1	3.9	1.3	4.6	3.4	2.0	3.0	3.0	2.5
Public Cloud Support	4.0	2.5	3.6	1.0	3.6	3.8	2.4	3.8	1.9	3.7	2.0	3.7	2.0	4.5	3.9	1.2	1.2	2.1	2.2
Pricing	3.8	3.9	3.8	5.0	3.5	3.5	3.7	4.0	4.0	3.9	3.7	3.2	3.5	3.0	3.8	3.5	4.2	3.0	4.3
As of 30 November 2021																			

Source: Gartner (January 2022)

Table 3: Product Score in Use Cases

Use Cases	*Alibaba Cloud*	*Amazon Web Services*	*Barracuda*	*Cato Networks*	*Check Point Software Technologies*	*Cisco*	*Forcepoint*	*Fortinet*	*H3C*	*Hillstone Networks*	*Huawei*	*Juniper*	*Microsoft*	*Palo Alto Networks*	*Sangfor*	*SonicWall*	*Sophos*	*Versa Networks*	*WatchGuard*
Enterprise Data Center	N/A	N/A	2.78	N/A	3.76	3.49	2.94	4.05	2.95	2.82	3.21	3.71	N/A	3.69	3.43	2.74	3.01	3.44	3.00
Enterprise Edge	N/A	N/A	3.03	2.78	3.82	3.40	2.73	3.87	3.04	2.74	3.13	3.70	N/A	3.94	3.49	2.79	2.74	3.27	2.76
Distributed Enterprise	N/A	N/A	2.95	2.96	3.84	3.32	2.67	3.89	3.10	2.61	3.03	3.65	N/A	3.85	3.44	2.97	2.80	3.38	2.80
Public Cloud	3.50	2.38	3.21	1.86	3.78	3.55	2.69	3.87	2.35	3.09	2.40	3.70	2.00	4.10	3.58	2.03	2.25	2.63	2.69
SMB	N/A	N/A	3.25	3.29	3.87	3.08	3.17	3.95	3.25	2.76	2.86	3.45	N/A	3.47	3.50	3.22	3.61	3.05	3.53

As of 30 November 2021

Source: Gartner (January 2022)