Ovum

Ovum Market Radar: Next-Generation Firewall Platforms

Despite seismic shifts, NGFW market offers diverse set of vendors, each with unique strengths

Publication Date: 15 Jan 2020 | Product code: INT005-000072

Eric Parizo

Summary

Catalyst

In recent years, seismic shifts in the enterprise IT landscape have had an enormous impact on enterprise network security. Transformative capabilities such as mobility, cloud computing, and software-defined networking require network security architectures to provide more functionality in more places and in more form factors than ever before.

Despite these changes, the next-generation firewall (NGFW), a mainstay on network perimeters for more than a decade, remains the cornerstone of sound enterprise network security. Identifying and denying unwanted or malicious packet flows at the distributed network perimeter is a proven method for thwarting malicious actors and preventing breaches. Yet enterprises must understand that the NGFW is much more than a packet-filtering device or even an application traffic-control mechanism; it is the engine that will drive evolving enterprise network security architectures into the future, including into the cloud.

In this report, Ovum details the capabilities of a "new" generation of NGFW platforms, explains how enterprises can ultimately benefit from the NGFW technological and market evolution, and reviews the NGFW product landscape to delineate each vendor's strengths and weaknesses. Ovum can say with certainty that the NGFW market is diverse, each product offers unique capabilities, and buyers have a variety of strong options to meet their specific use cases.

Ovum view

NGFW technology remains critical to the success of enterprise cybersecurity programs, but CISOs, security architects, and other stakeholders must understand that the NGFW is becoming much more than a network security appliance. Increasingly, it will act as a critical sensor providing network security intelligence data to a wide variety of threat detection and prevention appliances, as well as third-party offerings and emerging security telemetry platforms; as a unified networking-enablement device, particularly in branch offices, where secure direct access to SaaS applications via the internet is a business imperative; as an integration hub enabling enterprises to interconnect disparate solutions to customize their own best-of-breed security architectures; and as an enforcement mechanism, not only in physical and virtual appliances, but also as a component of networking and other devices and as a cloud-delivered service.

NGFW platform vendors must recognize open architectures are the future. The increasing variety of network security capabilities and delivery mechanisms means that even in a time of solution consolidation, no single security offering or platform can be all things to all customers. Enterprises will increasingly prioritize how easily and successfully a firewall solution fits into (and enables integration of) a multivendor security architecture.

Vendor solution differentiation in the marketplace will hinge on easy-to-use, single-pane-of-glass cloud-based management; unified dynamic policy paradigms that employs machine learning to identify never-before-seen threats in traffic flows and other network activity; reliable detection of threats in encrypted traffic; and ease of use for a growing number of managed security services providers in the industry.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

Key messages

- An NGFW platform remains critical to enterprise network security, protecting against known and unknown threats.
- With increasingly heterogeneous, hybrid environments, over time, an NGFW is less likely to be deployed as a physical or virtual appliance.
- An NGFW platform aspires toward a single, easy-to-use cloud-based management system featuring a single, dynamically adaptable policy.
- Homogeneous platform integration enablement and interconnection among third-party components within best-of-breed security architectures will become key NGFW capabilities.

Recommendations

Recommendations for enterprises

- Intense vendor competition and commoditization of "speeds and feeds" features has driven down NGFW prices, but enterprises should spend more, if needed, to invest in a solution and vendor that aligns with their long-term security architecture objectives.
- No two vendors' NGFWs are the same. Each vendor competes on a unique set of strengths that align with its product portfolio and business strategy. Understanding these strengths, and in turn weaknesses, is critical to making a successful NGFW purchase.
- Integration is of rising importance because of the need for orchestration and automation among multivendor security architectures. Enterprises should ensure a NGFW not only directly integrates with other key security solutions, but also enables broader integration.
- Built-in SD-WAN features are increasingly popular for branch deployments, but these capabilities vary widely, sometimes sacrificing security efficacy. Emerging cloud-delivered NGFW services may eventually negate the need for branch NGFWs.

Recommendations for vendors

- The firewall appliance market has never been larger more diverse, but vendors must prepare for its impending decline. Alternative NGFW delivery modes – within routers, as SaaS applications and via cloud-delivered services – will chip away at appliance revenue. Vendors able to also deliver virtual, cloud-native and containerized offerings will thrive.
- The NGFW is often the beachhead to sell broad security architecture platforms, but customers don't want vision alone. Product roadmaps driven by agile development should highlight when incremental improvements will come, and how customers will benefit.
- Enterprises are less tolerant of vendors that fail to invest in integrating their own ecosystems, whether built, bought, or both. The NGFW and other directly integrated solutions should offer a single platform, using a single policy set, with a single cloud-based management system.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

Defining and exploring NGFWs

Definition and characteristics

The next-generation firewall market segment is one of the largest enterprise cybersecurity IT product segments by revenue. Despite specious industry claims that "the perimeter is dead," enterprise network perimeters still exist, though they have evolved and expanded over time to meet usage requirements created by distributed network perimeters. Hence next-generation firewalls have expanded to conduct a variety of important security functions related to network traffic, including bouncing away unwanted traffic, filtering out malware and other malicious flows before they can reach devices, not to mention identifying, categorizing, and applying policy to application traffic. And that's just for starters.

Key capabilities

While next-generation firewall features are numerous and specific, Ovum has identified six primary categories against which to evaluate NGFW vendor technology and the vendors supplying it.

- **Performance**: NGFW performance can be measured in a variety of ways. To positively position their performance capabilities, most vendors highlight their "monitoring" throughput, the top megabit- or gigabit-per-second speed of traffic that can traverse the device when the firewall is essentially only watching traffic pass by. However, for its evaluation of NGFW performance, Ovum primarily examines what it terms "full-inspection" throughput, or the performance of a NGFW appliance when most or all of its various security and traffic-analysis capabilities have been enabled, a common and ideal use case for many enterprise deployments. Also of growing importance is an appliance's performance when decrypting encrypted traffic for inspection, a computationally intensive process that commonly reduces performance to one-tenth of an appliance's monitoring throughput. This feature is increasingly critical because more than 70% of inbound enterprise network traffic is now typically encrypted. Ovum also examines uptime, reliability, depth of performance-related features, and innovation related to performance.
- **Threat detection and mitigation**: Ultimately a NGFW is of little use if it is unable to detect, categorize, and address malicious and suspicious traffic flows. However, in a mature market segment, many features such as intrusion detection and network antimalware have become mandatory and largely lack innovation. When evaluating threat detection and mitigation capabilities, Ovum has therefore prioritized anomalous threat detection covering malicious never-before-seen traffic patterns and evasions that attempt to "hack" or trick the device itself into malfunctioning, as well as application traffic analysis specifically covering malicious flows involving on-premises and SaaS applications; support for automated remediation of malicious or suspicious events as dictated by policy; and across-the-board innovations related to threat detection and mitigation.
- **Manageability**: NGFW administrators typically devote many hours each workday to using the system's management graphical user interface to deploy and configure instances, investigate events, and conduct remediation actions. It should therefore be no surprise that the functionality of the management system is nearly as critical as the NGFW itself. In its review, Ovum prioritizes policy management, particularly dynamic, adaptive policies based on

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

business rules rather than specific ports and protocols, as well as feature granularity versus ease of use for administrators, and a product's ability to strike an effective balance between the two. Ovum also examines the functionality and capabilities built into the underlying operating system software and the ease with which customers can update and customize the OS, as well as across-the-board innovations related to manageability, most notably including fully featured cloud-based SaaS management as an alternative to on-premises appliances.

- **Integration**: An NGFW, or for that matter any enterprise security product, does not work in isolation. Furthermore, to deliver desired outcomes for enterprises, real-world enterprise deployments require interoperability and integration with many different products from a range of vendors. Ovum has therefore prioritized integration as a key capability of NGFWs. This includes ecosystem integration, or the depth, breadth, and effectiveness of pre-built integrations between a NGFW and other cybersecurity products from the same vendor, as well as third-party integration including technology partnerships and security platform integration frameworks (SPIFs) the product supports. It also includes ease of integration, such as how much time and effort is required on the part of the customer to achieve integrations supported by the vendor, and depth of integration, which looks at the extent to which customers can customize existing capabilities, achieve integrations not formally supported by the vendor, and the reliability and usefulness of integrations.
- **Service and support**: Ovum evaluated several facets of NGFW service and support, including the frequency and quality of the vendor's ability to produce software and firmware updates and new features, as well as its technical support and other related support services; and across-the-board innovation related to service and support.
- **Pricing, licensing, and value**: The cost of a product is always a factor in a purchase, particularly in IT organizations when enterprise security often competes against other business priorities served by the overall IT organization. Here Ovum examines the price of a vendor's appliances and associated software and service licenses and agreements the ease of licensing, including the number of different licensing options offered and how appropriate they may be for each respective product, and the flexibility customers are afforded in managing, applying, and when necessary upgrading licenses, and ultimately the value that the entirety of the NGFW solution set provides customers when reviewed in context with its cost.

Ovum's research process involves a wide array of independent research processes, document reviews, strategic and technical briefings with NGFW vendors, and interviews with customers.

Business value and applications

Customers, stakeholders, partners, and regulators expect enterprises to protect their assets and ensure the uninterrupted operation of the business and its key functions. While cyberattacks and other negligent or mistaken activities inevitably result in threats to the business, the next-generation firewall remains a critical front-line security control to detect and mitigate network-borne threats, and ultimately ensure the value of the organization is maintained.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

Market landscape and participants

Market origin and dynamics

The next-generation firewall emerged in the mid-2000s, the result of a lengthy evolution. The commercial firewall market has existed for about 30 years, initially comprising a variety of packet-filtering devices to interrupt unwanted traffic at the network edge. Over time, firewalls evolved to add more features, including stateful inspection (contextual awareness of port-connection status), network address translation (IP address assignment), virtual private networking (encrypted connections to and from supported remote clients), intrusion detection and prevention, and many more.

It was the addition of application awareness that began the NGFW era, specifically in 2007 when Palo Alto Networks debuted a firewall that could identify and control TCP/IP packet flows between certain types of applications. With the widespread adoption of web browsers, email clients, and other internet-enabled applications, the ability to inspect, identify, and apply policy-based controls to application traffic became critical for providing sound enterprise network security.

Today, more than a dozen competitive vendors offer a variety of physical, virtual, and cloud-based NGFWs for service providers and telecommunications networks, large enterprises, branch offices, and/or small and midmarket firms.

Key trends in the NGFW market

The top trend in next-generation firewalls is the recent debut of numerous cloud-delivered firewall services, layering packet inspection and intrusion prevention along with add-on capabilities such as DNS filtering, dynamic malware analysis, secure web gateway, and data loss prevention. These NGFW-as-a-service (NGFWaaS) options are quickly coming to complement physical and virtual firewalls for use cases in which a firewall deployment is architecturally impractical and cost-prohibitive, as well as to protect remote devices outside the corporate network.

By the end of the decade, Ovum forecasts that yet another form factor will emerge when NGFW functions will be componentized in accordance with the growth of microservices and serverless application architectures. Specifically, it will be commonplace for firewall functions to exist both on the network edge and as segmentation mechanisms as is common today, but also within applications as individual application service functions that can be called on demand.

Future market development

Ovum believes history will come to show that the next-generation firewall market segment in 2020 was at or near its peak. Based on various industry estimates, the segment generates between $2.5bn and $4.5bn in revenue annually, with a compound annual growth rate (CAGR) in excess of 10%. However, it is expected that this growth will soon level off and eventually recede, as expensive physical NGFW appliances give way to virtual and cloud-native software firewall instances. By the end of the next decade, NGFW technology will commonly exist not as a standalone offering but as a commodity component of various application service offerings, including within what today are emerging microservices and serverless architectures. This evolution will, over time, reduce the number of expensive physical appliances that are purchased and deployed, in turn reducing the revenue derived from firewall technology.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

Vendor landscape

Ovum's next-generation firewall platform market heatmap is a revealing mosaic, painting a picture of a strong yet diverse group of vendors. Each has unique strengths and weaknesses, and no two vendors are the same.

While the NGFW market segment is relatively mature, Ovum's research revealed vendors with varied states of maturity. Numerous products have been in the market for a decade or longer, but are underdeveloped in categories such as performance, manageability, or integration. On the other end of the spectrum, several promising SMB vendors have carved out highly successful market niches, with more than one potentially laying important groundwork to move upmarket.

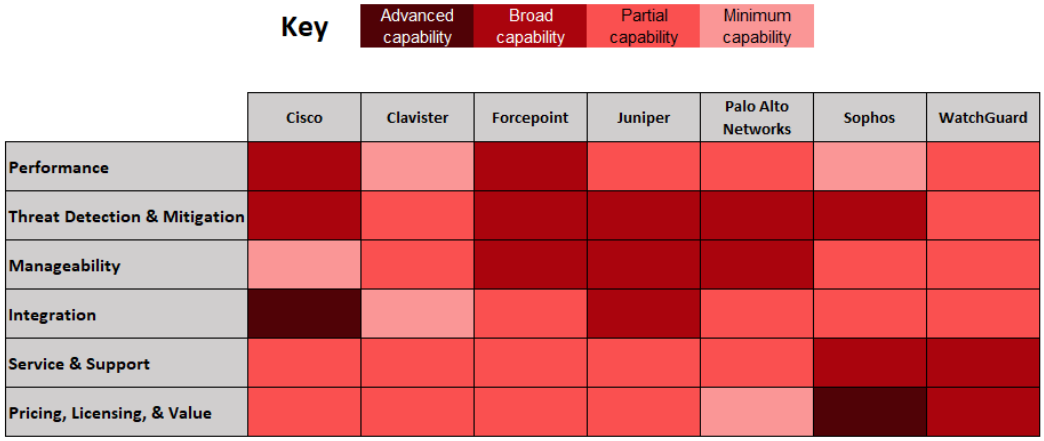
Increasingly, however, vendors are incorporating their NGFWs into broader solution sets, sometimes strengthening the value proposition of the firewall, in other instances to the detriment of the firewall's performance and evolution.

Still, the NGFW market segment is thriving, with nearly every vendor identifying ways to successfully differentiate, while buyers have plentiful options to meet their individual needs.

Vendors that participated in this research effort included Cisco Systems, Clavister, Forcepoint, Juniper Networks, Palo Alto Networks, Sophos, and WatchGuard Technologies.

Vendors that were invited but declined to participate included Barracuda Networks, Check Point Software Technologies, Fortinet, Huawei Technologies, and SonicWall.

Figure 1: Ovum heatmap for the next-generation firewall platform market



Source: Ovum

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

Vendors on the Ovum Market Radar in next-generation firewall platforms

On the radar: Cisco Systems Firepower Next-Generation Firewall

Ovum view

As a standalone product, Cisco Firepower lacks some of the bells and whistles of other contemporary enterprise firewalls, but when combined with other key elements of the Cisco Security ecosystem, it becomes much harder to pass up.

Anecdotally, Ovum has heard no other enterprise security solution praised more in 2019 than Cisco Umbrella, the networking giant's cloud-delivered DNS security service, recently upgraded to offer secure web gateway (and, by extension, firewalling) capabilities.

Firepower is a compelling solution when paired with Umbrella and other Cisco Security ecosystem options such as Threat Grid and Stealthwatch Cloud, not to mention industry-leading threat intelligence from Talos. And thanks to Cisco's newly simplified licensing paradigm, the cost and complexity of doing so is more attractive than ever before.

Key messages

- Cisco has made substantial progress on ease of management, especially for customers with a mix of legacy ASAs, new Firepower devices, and Meraki UTMs.
- Cisco's security efficacy, backed by threat intelligence from its renowned Talos research group, has consistently proven to be a strong differentiator.
- Cisco's recent licensing overhaul, including the Security Choice ELA program and its new license-management portal, have significantly eased acquiring and managing entitlements.
- Firepower's ease of use and feature depth fall short of key NGFW competitors. It is therefore best purchased alongside other offerings such as Umbrella and Stealthwatch.

Recommendations for enterprises

Why put Cisco Firepower on your radar?

In Ovum's view, Cisco boasts the industry's most accurate, future-focused vision of the technological and market segment evolution of the next-generation firewall. Tangible NGFW appliances, such as the network perimeter itself, aren't going away, but they will be supplemented by virtual and cloud-native firewalls as well as cloud-delivered NGFW-as-a-service, where additional security controls such as DNS and web gateway security can be layered in.

Cisco has already aligned its network security portfolio accordingly, with its Firepower physical and virtual appliances bolstered by cloud-native firewall support for all three major public cloud infrastructure providers, along with its widely lauded Umbrella cloud-delivered security services.

Cisco has also quietly become one of enterprise cybersecurity's standard-bearers with regard to third-party best-of-breed integration enablement, boasting what's believed to be the largest technology partner program in the industry, managing a variety of internal and external integration efforts, and fostering Snort and more than a dozen other free open source tools.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

Highlights

Firepower, which debuted in 2016, is based on technology from Cisco's venerable ASA line of stateful firewalls and next-generation intrusion prevention technology acquired via its purchase of Sourcefire, applying both signature- and anomaly-based techniques to identify likely threats in network traffic.

Firepower features four primary appliance lines: the small-office 1000 Series, the midrange 2100 Series, the enterprise-grade 4100 Series, and the carrier-grade Firepower 9300

Not traditionally seen as a performance leader, Cisco has upped its game with Firepower. Its top 1U model, the newly released 4145, offers 80Gbps of firewall throughput, 27Gbps of full-inspection throughput, and 10Gbps when decrypting traffic for inspection (TLS 1.2).

Beyond traditional firewalling and application traffic visibility and control, licensed security features available for Firepower include network antimalware, intrusion detection and prevention, VPN, and URL filtering. Cisco supplements its appliance features with a comprehensive set of integrated capabilities including dynamic malware analysis (AMP Threat Grid) and DNS controls (Umbrella).

Cisco accompanies its physical firewalls with its Firepower NGFWv virtual firewalls, available on Amazon Web Services and Microsoft Azure. It also offers cloud-native versions of Firepower on AWS, Azure, and Google Cloud Platform. In addition, Umbrella can work in tandem with Firepower, automatically forwarding network traffic to the Umbrella secure web gateway (SWG) for inspection.

Firepower Management Center serves as the central management appliance for all of Cisco's firewall and intrusion prevention appliances, supporting a maximum of 750 managed devices and up to 300 million IPS events in a single 1U appliance. Cisco now supplements FMC with Cisco Defense Orchestrator, a SaaS application offering a simplified configuration and management experience along with the ability to create and manage policies across ASA, Firepower and Meraki devices, Umbrella, and cloud-native firewall instances.

Cisco arguably leads the industry in NGFW integration enablement. The Threat Intelligence Director feature in Firepower Management Center can ingest and correlate threat intelligence with events, automatically enriching events and reducing the time spent by analysts. Via APIs Cisco has opened Firepower to allow third-party vendors to manage and audit configurations and identify gaps, as well as to assess compliance. A differentiator is its System Event Streamer (eStreamer) for narrowcasting detailed firewall events to third-party systems. Firepower also benefits from many dozens of other Cisco security ecosystem integration capabilities spanning pxGrid (ISE), AMP for Endpoints, Threat Grid, and Cisco Threat Response, among others.

Customers, however, have long derided Firepower's ease of use and stability. Many reports indicate frequent bugs in its underlying Firepower Threat Defense OS and FXOS chassis-management software, requiring frequent updates. Customers with whom Ovum spoke said usability was a top Firepower drawback.

Background

To paraphrase a well-worn saying among enterprise CIOs, "You never get fired for buying IBM or Cisco." This certainly speaks to the networking giant's long history of success.

The company, founded in the early 1980s to develop LAN technology, has since grown to dominate the global enterprise network equipment segment, earning nearly $50bn in revenue in fiscal 2018. In the mid-90s it released PIX, designed largely for network address translation, but it found success as a stateful traffic-inspection mechanism on the enterprise perimeter.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

In the 2000s the company sought to address the growing need for enhanced security on, and secure access into, enterprise networks. The result was the Adaptive Security Appliance or ASA, the first appliance that combined firewalling with virtual private networking and intrusion prevention. It was a huge success and remains widely deployed today.

Cisco's security efforts struggled to find consistent momentum with a string of leaders and strategies in the late 2000s and early 2010s. However, Check Point's failed acquisition of Sourcefire was an opportunity for Cisco, which snatched up the company, founded by Snort creator Martin Roesch, for $2.7bn. And it was the combination of technology from Cisco and Sourcefire that gave birth to its contemporary next-generation firewall platform, Firepower, in 2016. Since then, largely through a string of follow-on acquisitions, Cisco has greatly expanded its security portfolio, increasingly developing capabilities from and for the cloud.

In Cisco's overall revenue pie, security is still a tiny slice (only accounting for about 6% of its quarterly revenue), but its Security Business Group has been consistently meeting its stated goal of at least 10% annual revenue growth, with no signs of slowing.

Current position

Innovation is no doubt critical to Cisco's future in security, but integration is key to its present. Cisco recognizes that the network perimeter now extends into everything from third-party cloud environments and home workers' living rooms to factories, power plants, and cargo ships half a world away. It has therefore extended its strategy to provide world-class security controls in every place needed, offering detailed visibility and reliable threat detection and prevention efficacy managed with unified security policy.

Cisco is delivering on this strategy by providing network security via whatever delivery model makes sense for customers (on-premises physical or virtual appliances, cloud-native firewalls, or cloud-delivered firewall services) with unified policy management and incident response. While Cisco is probably several years away from fully realizing its strategy via new and enhanced products, it deserves credit for recognizing and tackling the ease-of-use problems customers have complained about for years.

Its next challenge will be to foster innovation at a pace that matches its key competitors. Cisco has yet to outline an approach to address the emerging cloud-native microservices-based and serverless architectures that will come to define the next decade. It also has yet to fully bring to bear the power of its copious cybersecurity telemetry datasets, which will be essential in the coming years not only for detecting in-progress attacks with greater speed and accuracy, but also for preventing future attacks before they strike.

Still, Cisco squarely resides in the top tier of enterprise network security competitors, and its trajectory is indicative of a vendor headed in the right direction.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

Data sheet

Key facts

Table 1: Data sheet: Cisco Systems

Product name	Cisco Firepower Next-Generation Firewalls	**Product classification**	NGFW
Product categories	Firepower 1000 Series (SMB/distributed), 2100 Series (midrange), 4100 Series (enterprise), 9000 Series (carrier/provider)	**Latest release date**	September 2019 (Firepower Threat Defense 6.5; Firepower Management Center 6.5)
Industries covered	All	**Geographies covered**	All
Relevant company sizes	All	**Licensing options**	Subscription (one-, three-, and five-year terms)
URL	https://www.cisco.com/c/en/us/products/security/firewalls/index.html	**Routes to market**	Direct, channel, two-tier distribution
Company headquarters	San Jose, CA, US	**Number of employees**	74,200

Source: Ovum

On the radar: Clavister NetWall next-generation firewall

Ovum view

Clavister has earned thousands of loyal customers that appreciate its modular network security portfolio, flexible deployment, and simple licensing options, but because it lacks the necessary scale and performance capabilities, it isn't globally competitive with top-tier NGFW vendors.

Key messages

- The vendor's Swedish origin and culture allow for positioning as the "independent alternative" to vendors with strong ties to the East or the West.
- Clavister offers its InCenter analytics system at no additional cost to customers.
- It places an emphasis on usability and reliability, providing granularity with a smooth, easy-to-navigate interface.
- Clavister's rapid revenue growth is indicative of a vendor on the rise.

Why put Clavister on your radar?

Clavister serves customers whose security maturity varies from highly sophisticated to little or no experience, and it has become a specialist in providing a multifaceted network security solution set that can meet the needs of its growing customer base.

Its tight focus on four specific regions means it can meet the needs of customers in these areas arguably better than its competitors, especially in focus verticals that include education, public sector, retail, critical infrastructure, transportation, and communication service providers.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

Clavister also positions its Swedish history and culture as a strength. Those values inspire its modular Ikea-like product portfolio that offers deployment flexibility, and its proud efforts to be perceived as the "independent alternative" to vendors with American or Chinese ties. It positions itself above the geopolitical fray with its commitment to never cede to the wishes of nation states by allowing back doors in its products, and invites customers to review the integrity of its source code.

Highlights

Clavister's enterprise firewall portfolio features two distinct product lines: NetShield and NetWall. It refers to NetShield as a services-based firewall designed for use in telco and service provider networks, and NetWall as a next-generation firewall for SMB and enterprise deployments.

While its throughput capabilities are somewhat limited (its top-end NetWall W50 Pro offers 55 Gbps of monitoring throughput and just 2 Gbps of full-inspection throughput), it offers all the standard NGFW capabilities, including stateful inspection, IDS/IPS, and application traffic classification and inspection, as well as network anti-malware including IP reputation services. It also offers SD-WAN features with on-box routing, load balancing, and traffic route optimization.

The vendor supports inspection of nearly 3,300 network and application protocols, and its True Application Control feature identifies, classifies, and develops a baseline of normal application traffic behavior, identifying deviations that are consistent with malicious activity.

Clavister offers an optional OEM add-on appliance or cloud service called NetEye for encrypted traffic inspection to offer flexible deployment options to customers. Similarly, it relies on third-party technology partners for a wide array of supporting capabilities, including antivirus (Kaspersky), endpoint security (BitDefender), IP Reputation (Webroot), URL filtering, and malware sandboxing, as well as SSL inspection (ContentKeeper).

The vendor's firewalls run its own proprietary operating system, cOS Core, which is not based on Linux but includes limited other open source components. The vendor claims this keeps its products from being affected by high-profile open source vulnerabilities such as Heartbleed and Shellshock/Bash. For consistent performance and cost savings, it has standardized on Intel x86 microprocessors. Meanwhile, it is updating its OS to also support Arm microprocessors, in part to support low-cost universal CPE platforms as part of its SD-WAN strategy.

Clavister offers a virtual firewall and supports VMware ESXi, Microsoft Hyper-V, and KVM. It supports OpenStack for private cloud deployments, but NetWall is not available via cloud provider marketplaces.

Similarly, the vendor avoids the popular OpenVPN protocol and uses its own proprietary SSL VPN engine and terminator in its firewalls, which in turn necessitates a highly customized SSL VPN client. Its IPsec VPN does not require an additional client.

Its InControl provisioning and configuration system requires deployment on-premises or in own-managed cloud hosted environments and provides zero-touch provisioning support. Its InCenter log management, analytics, and reporting system is available in a SaaS-based version.

Clavister’s W50 Pro 1U appliance priced at approximately $26,000, and discounts for multiple appliances and various software subscriptions can trigger incentive discounts of up to 40%. The company offers a basic subscription that includes software updates, 24x7 support, and hardware failure replacement. The advanced subscription adds signature and pattern updates for the NGFW features and includes cloud-hosted analytics with InCenter.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

Background

Clavister, based in Örnsköldsvik, Sweden, might not be a widely known name in enterprise network security, but it has 20 years of experience developing security technology.

For most of its history, the vendor built firewalls based on Intel x86 hardware, but expanded into virtual firewalls in 2008 and application-aware next-generation firewalls earlier this decade.

About three years ago, a change in the board of directors, including new chairman, Viktor Kovács, led to the implementation of a high-growth strategy that has seen the company diversify its product line beyond network security appliances into security software and cloud-delivered security solutions.

Today, the company is listed on Nasdaq First North (CLAV) and has more than 140 employees.

Current position

After two decades, Clavister has accumulated more than 22,000 customers around the world, with most of them located in its target geographies of the Nordics, Western Europe, Southeast Asia, and Japan.

Its annual revenue is in the low seven-figures, but the vendor highlights a conspicuous improvement in its growth trajectory, with an annual revenue increase in its fiscal 2018 of more than 50% year-over-year and between 80% and 150% growth in its four target regions.

Interestingly, while the vendor has no brand awareness to speak of in North America, it has had success with some multinationals, such as Nokia, which employs Clavister firewalls as part of its managed security services. Many enterprises in North America might not therefore realize they are being protected by Clavister firewalls.

Perhaps despite its potential, Clavister has work to do to mature its product, specifically its core offering, NetWall. Its appliance throughput is below rising industry standards. It suffers dramatic performance drops when full-inspection capabilities are enabled, and encrypted traffic analysis requires an add-on appliance. Its provisioning and log-analysis systems run separately, and only part of it is available as a SaaS offering.

While Clavister's long-term vision of pairing network security with secure connectivity, multifactor authentication, and single sign-on to cloud-based SaaS applications is compelling and in line with the direction of the market, to be broadly competitive it requires multicore appliances with greater throughput than it can currently provide, as well as tighter integration of its portfolio components, and a cloud-based single-pane-of-glass management system.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

Data sheet

Key facts

Table 1: Data sheet: Clavister

Product name	Clavister NetWall	**Product classification**	NGFW
Product Categories	SMB (E Series); midmarket/small enterprise (W Series)	**Latest release date**	November 2019 (cOS Core 13.00.00)
Industries covered	All	**Geographies covered**	All (150 countries)
Relevant company sizes	All	**Licensing options**	One-, three-, and five-year subscription terms. Optional advanced subscription provides full NGFW signature updates.
URL	https://www.clavister.com	**Routes to market**	Distributors, partners, direct sales, OEM
Company headquarters	Örnsköldsvik, Sweden	**Number of employees**	140

Source: Ovum

On the radar: Forcepoint Next Generation Firewall

Ovum view

Forcepoint NGFW is a strong choice for a variety of deployment scenarios, particularly distributed and high-availability environments. While the product is somewhat lost amid the vendor's high-risk, high-reward vision of human-centric cybersecurity, as a standalone offering it has too many strengths not to be on buyers' shortlists for most enterprise NGFW purchasing scenarios.

Key messages

- Forcepoint NGFW is a mature, proven product with innovative features such as evasion detection and high-availability clustering.
- Forcepoint offers arguably the industry's most mature built-in SD-WAN features for a NGFW, and it has offered this capability for more than 15 years.
- Forcepoint's NGFW is becoming a foundational element of its "human-centric security" paradigm that uses contextually adaptive controls to protect data, devices, and people.
- Forcepoint NGFW has lost significant momentum in the marketplace over the years due to brand awareness and its multiple ownership transitions.

Why put Forcepoint on your radar?

It is Forcepoint's ambition to usher in a new era of enterprise cybersecurity. This is a lofty goal but having one of the industry's most proven firewalls is a good place to start.

The Raytheon-owned vendor has assembled a portfolio of technologies, including NGFW, secure web gateway, DLP, and UEBA, to secure people, data, and devices by understanding and proactively adapting as risk changes. Specifically, it aims to offer a unified, dynamic policy across its portfolio that

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

collects data from all its products, uses machine learning to analyze the telemetry and detect when anomalous or risky activity may be occurring, then adjusts policy rules to increase security where appropriate.

It is a highly ambitious effort, three-plus years in the making. If it succeeds, it could set a new standard for enterprise cybersecurity platforms. In the meantime, Forcepoint must sell not only its future vision, but also the current value of its individual products and raise its brand awareness in a crowded market.

Highlights

Despite several names and several corporate homes, the enterprise network security technology known today as the Forcepoint Next Generation Firewall is among the industry's most capable offerings.

Forcepoint offers a broad line of physical appliances:

- 50 Series and 100 Series desktop models for small offices
- 300 Series for branch offices
- 1100 Series and 2100 Series for distributed and network edge deployments
- 3300 Series for campus environments
- 6200 Series for data center environments.

The Forcepoint NGFW line has a surprising number of strengths. In addition to standard stateful firewalling, routing, DHCP, VPN, deep-packet inspection, antimalware, URL filtering, and on-box SSL/TLS decryption, it can identify and apply policy on more than 7,400 unique network and application protocols. Its top 1U appliance, the N2105, offers a competitive 80 Gbps of network monitoring throughput, 15 Gbps of full-inspection throughput, and 4 Gbps of encrypted traffic inspection throughput.

The product line has long been known for its high availability. It reduces system downtime by supporting clusters of up to 16 physical and/or virtual appliances, enabling software upgrades or maintenance on individual devices without the need to take the cluster offline.

Unlike many enterprise firewalls that lack the ability to serve as standalone intrusion prevention appliances, Forcepoint NGFWs are effective in dedicated IPS use cases. The appliances can perform inline layer 2 traffic inspection, offering customers the flexibility to redeploy them for different purposes as their network security requirements evolve. Its IPS technology has excelled in independent third-party testing for its ability to prevent evasions (new and modified attack techniques designed to avoid detection).

Few realize that the SD-WAN technology built into Forcepoint's NGFW is more than 15 years old. Formerly called Multi-Link VPN, it combines secure networking and built-in load balancing with dynamic network availability, using broadband connections to supplement or displace MPLS and other expensive leased-line connections, particularly in distributed deployments. Forcepoint is aiming to develop market campaigns around its SD-WAN features for the first time in 2020.

Forcepoint complements its physical appliances with virtual appliances supporting the VMware ESXi and NSX, Microsoft Hyper-V, and KVM hypervisors. It also offers versions for Amazon Web Services and Microsoft Azure with on-demand licensing (via the respective marketplaces) as well as with bring-your-own-license models.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

The vendor recently debuted a cloud-delivered NGFW service called Dynamic Edge Protection, which integrates with its physical and virtual appliances to secure off-premises devices.

Forcepoint's Security Management Center (SMC) management system is deployed as a physical or virtual appliance on-premises or in the cloud. It offers fully integrated logging and reporting and supports more than 2,000 unique NGFW devices per SMC instance. Its device OS is a unified software image (hardened Linux-based) across all its network security devices.

Ovum research of Forcepoint customers revealed strong affinity for the product's versatility and broad array of features, its consistent performance, scalability, and reliability, and its feature development, specifically in support of its key verticals like retail and government. Customers also appreciate that while Forcepoint is incorporating the NGFW into its broader architecture strategy, standalone firewall purchases still yielded plenty of ROI. Ovum received customer feedback, however, that Forcepoint NGFW deployment is overly complex, often requiring an on-site technician and a significant amount of customization when integrating with third-party products.

Background

The Forcepoint brand might be relatively new, but its products include some of the industry's most proven in their respective segments.

Forcepoint's story began in 2015, when defense giant Raytheon sought to expand its capabilities in enterprise cybersecurity by acquiring secure web gateway vendor Websense for $1.9bn. A year later, Forcepoint was formed after Websense acquired the Stonesoft/StoneGate and Sidewinder firewall businesses from McAfee. Stonesoft was subsequently renamed Forcepoint NGFW. The technology found a home alongside Websense's top-tier Triton SWG line, as well as email security and DLP. The vendor supplemented these capabilities with security analytics and data warehousing technology from corporate parent Raytheon, as well as user and endpoint behavioral analytics (UEBA) intellectual property from its 2017 acquisition of RedOwl.

Because the acquisition of new technology and the realignment of its product portfolio represented such a significant turning point for Websense, its leaders decided a new identity and therefore a new name, Forcepoint, was necessary as it redefined itself as a multifaceted provider of enterprise security products.

Today the Austin-based vendor employs about 2,500 people with thousands of customers in more than 150 countries. It boasts strong penetration in verticals including federal government, retail, and manufacturing. The company, which operates as an independent subsidiary of majority owner Raytheon, is led by CEO Matthew Moynahan, a former Veracode CEO who also held executive roles at Arbor Networks and Symantec. Forcepoint reported $634m in revenue in its fiscal 2018, and slightly above break-even in profitability.

Current position

Historically Forcepoint has primarily competed for distributed and branch office deployments due to its scalability, ease of use, and uptime, and resiliency. It also continues to serve a number of US federal government customers. The product is more than capable of excelling beyond these areas in a wide array of deployment scenarios.

The Forcepoint brand however remains underrecognized, and the company has only recently fully rebuilt the product marketing organization that it lost to McAfee during the Stonesoft acquisition. In addition, industry speculation persists that Raytheon could sell some or all of Forcepoint in light of

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

Forcepoint's difficulty increasing profitability. The NGFW line has also lost about half of its customer base since separating from McAfee, although the vendor contends its per-customer NGFW spending has increased.

Complicating matters further is the fact that many of its legacy customers, particularly in government, still use its Sidewinder purpose-specific legacy proxy firewall. Sidewinder's features have recently been incorporated into the Forcepoint NGFW product, but the vendor has yet to demonstrate success upselling those customers on a much different product.

Ultimately, Forcepoint NGFW's success will be inextricably tied to the company's top-down strategy to human-centric cybersecurity, and whether it can present a compelling case that Forcepoint NGFW is uniquely capable of helping customers realize the vision of dynamic, risk-adaptive security.

Data sheet

Key facts

Table 1: Data sheet: Forcepoint

Product name	Forcepoint Next Generation Firewall	**Product classification**	NGFW
Product categories	50 Series/100 Series (desktop/SMB); 300 Series (branch offices); 1100 Series and 2100 Series (distributed /network edge) 3300 Series (data center)	**Latest release date**	November 2019 (Version 6.7)
Industries covered	All	**Geographies covered**	All
Relevant company sizes	All	**Licensing options**	Subscription
URL	https://www.forcepoint.com/product/ngfw-next-generation-firewall	**Routes to market**	Two-tier, direct
Company headquarters	Austin, TX, US	**Number of employees**	2,500

Source: Ovum

On the radar: Juniper Networks SRX Series Next-Generation Firewall

Ovum view

Juniper Networks' SRX Series NGFW is a strong choice for any organization committed to a Juniper-based network infrastructure, due in large part to its ease of management and tight integration enabling network-driven threat detection and isolation. Juniper's next challenge is to expand its sales motions and articulate its value when compared to its well-heeled rivals that offer larger product ecosystems and broader visions.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

Key messages

- Juniper Networks' SRX Series NGFWs are at the center of its "connected security" vision, offering superior visibility, automated enforcement and remediation, and streamlined security operations to improve efficiency and business outcomes.
- Juniper emphasizes its history by positioning itself as a security-centric network infrastructure player, but the rise of NFV, SD-WAN, and cloud-driven IT architectures requires a more future-focused vision.
- Juniper has an impressive slate of deep technology partnerships fostering useful integrations.
- Juniper's reliance on other vendors for offerings including CASB, DDoS mitigation, and endpoint security hinders its ability to offer its own tightly integrated ecosystem.

Why put Juniper SRX on your radar?

The Juniper Networks SRX Series NGFW has a lot of good things going for it, including router-level integration via a single operating system, several strong integrated features including URL filtering, network-level threat mitigation, and SSL/TLS decryption, not to mention the industry's first containerized firewall. In addition, Juniper has placed SRX at the heart of a network security solution set featuring its various advanced threat protection (ATP) technologies.

However, after a multiyear period in which it de-emphasized security, Juniper has a way to go to catch up to the market. It must prove that it can bolster its network security ecosystem with the supporting capabilities and future-focused vision that will compel enterprises to invest in a NGFW that previously suffered from a long, steady market share erosion, which Juniper is now working to reverse.

Highlights

Juniper’s network security ecosystem is headlined by its flagship SRX Series next-generation firewalls and supplemented by dynamic malware analysis on-premises (JATP Appliance) and in the cloud (ATP Cloud), threat intelligence from ATP Cloud, and the Security Director management appliance.

The SRX Series runs the gamut from 1U appliances for the branch all the way up to appliances for securing large enterprise data centers, hosted or co-located data centers, and service provider infrastructure. Its physical appliances are supplemented by a virtual appliance (vSRX) that supports VMware ESXi and KVM, as well as a containerized firewall (cSRX) for Kubernetes deployments.

Key features include routing support for IPv4/IPv6, OSPF, BGP, and multicast; IPsec and SSL (TLS) VPNs; stateful and application-aware firewalling; intrusion detection and prevention (IDS/IPS); and on-box and cloud-based antivirus, antispam, and web content (URL) filtering. Its Junos OS runs on all its firewalls. Instances can be managed via command-line interface (CLI), scripting capabilities, a web-based GUI, or the Junos Space Security Director, a centralized management appliance, and can be located on premises or in the cloud (with near feature parity).

Where Juniper shines brightest is in the tight integration between its routing and security solutions. Routing was part of SRX's earliest capabilities, and according to the vendor, many customers use the NGFW for routing as well, with nominal if any performance concerns. Also, unlike most NGFWs that require an endpoint agent to receive posture-related data and in turn trigger response actions when malicious activity is detected, Juniper instead relies on its MX Series routers (or nearly any other vendor's SNMP-compatible router) to gather data about network and endpoint activity, and when a threat is detected, use the network infrastructure to isolate the problem.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

While this might not be a differentiator to organizations that face no difficulties with installing endpoint agents, one government customer of Juniper told Ovum that political issues in his organization prevent the network security team from exerting visibility or control over endpoints. Yet if the endpoint protection solution fails, the network security team is blamed because malware, ransomware, and the like propagate over the network. With Juniper's solution, however, when threats are detected over the network, they can quickly be mitigated without any direct intervention on the endpoints.

This capability is powered by Juniper's Policy Enforcer. Policy Enforcer provides the correlation and analytics capabilities to automate endpoint quarantines and other network policy enforcement, and can also map network infrastructure to help with network visibility.

The SRX offers standard security features such as anti-malware, intrusion prevention, web filtering, application-layer visibility, and on-box decryption. Juniper's performance throughput, however, consistently falls short of rising industry standards, particularly in terms of SSL/TLS traffic decryption. Only in the past year has Juniper started to redesign its hardware appliances to offload decryption processing, something rivals have done for years. For a vendor that bills itself as an infrastructure specialist, this shortcoming is particularly glaring.

A notable differentiator for Juniper is the cSRX, a containerized firewall launched about 18 months ago. The Docker-based instance offers sub-second spin-up in an application platform environment in public, private, or hybrid clouds, using the same Juniper policy and management systems as the vendor’s physical and virtual NGFWs.

Background

A network infrastructure vendor with a proud history, Juniper Networks is seeking to reposition itself in an increasingly cloud-driven world. Founded in 1996, Sunnyvale, Calif.-based Juniper is an established supplier to enterprises, service providers, and telecommunications firms.

In the early 2000s Juniper experimented with its own security solutions, but in 2004 decided to accelerate its efforts by acquiring NetScreen, which resulted in the industry's first commercial firewall with integrated IDS/IPS. Much of this technology was used to create what has become today's SRX Series NGFWs.

After largely dominating the firewall market in the 2000s, Juniper's leadership position slowly eroded with the rise of application-aware NGFWs from vendors such as Fortinet and Palo Alto Networks.

For several years, the SRX line and security weren’t priorities for Juniper. It went so far as to sell off its VPN, NAC and ADC products in 2014 when these became the core products for a separate company called Pulse Secure. However, Juniper Networks has come to understand that networking and security are inextricably linked and has recently redoubled its commitment to its security portfolio. Its new "connected security" vision therefore involves offering superior visibility, automating enforcement and remediation, and streamlining security operations to improve efficiency and business outcomes.

Juniper employs 9,300 people in 117 offices in 47 countries. It is a public company (NYSE: JNPR) led by CEO Rami Rahim since 2014, with annual revenue of $4.648bn in 2018.

Current position

For the past two-plus years, Juniper has refocused on advancing its venerable NGFW technology, and has made steady progress. Its key challenge now is convincing prospective enterprise customers that it once again deserves a seat at the table.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

Juniper declined to provide data on its total number of SRX customers deployed globally or a breakdown of its customer base by size, but product line revenue for fiscal 2018 for the SRX line totaled only about 7% of Juniper's overall 2018 revenue. This supports Ovum's understanding that the vendor has seen significant erosion of its firewall customer base over a period of many years, and that it has struggled to win competitive engagements against top-tier enterprise vendors.

However, due in large part to its history in the market segment and its position as a well-known infrastructure player, Juniper remains competitive in very large enterprise engagements, as well as with service providers and telecommunications companies.

Juniper would be well served to highlight its little-known strengths, such as its unified application-based policy schema that enables users to write network security policies based on business constructs such as user groups and applications rather than ports and protocols; innovations like its cSRX containerized firewall and the former Cyphort technology; and scalability few rivals can match, supporting up to 25,000 firewall devices on a single instance of Security Director. It should also articulate a long-term security product portfolio vision for providing security solutions for and from the cloud, an area where rivals are already investing heavily.

Juniper sees its numerous technology partner integrations as a key strength, relying on best-of-breed vendor partners for various security capabilities such as DDoS mitigation (Corero), antimalware (Sophos), endpoint detection and response (Carbon Black/VMware), cloud security (Netskope), and SIEM (IBM QRadar), not to mention Pulse Secure. However, this plethora of partnerships increases integration complexity for Juniper customers and inhibits Juniper from creating its own full-featured portfolio of natively integrated solutions that key rivals are fostering as market differentiators.

Juniper customer research conducted by Ovum found positive reactions regarding Juniper’s uptime and service-level consistency, its ability to employ the SRX as a routing device with minimal performance impact, and its automated network-layer threat detection and mitigation.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

Data sheet

Key facts

Table 1: Data sheet: Juniper Networks

Product name	SRX Series	**Product classification**	NGFW
Product categories	SRX3xx (SMB), SRX5xx (branch offices), SRX1500 (mid-size branch/campus), SRX4x00 & SRX5x00 (large campus, data center, service provider)	**Latest release date**	Q3 2019 (Junos OS 19.3)
Industries covered	All	**Geographies covered**	All
Relevant company sizes	All	**Licensing options**	1,3, and 5-year subscription terms. Optional add-on subscriptions: IPS, IPS and Application Control, ATP, and various bundles
URL	https://www.juniper.net/	**Routes to market**	Direct, channel, and two-tier
Company headquarters	Sunnyvale, CA, US	**Number of employees**	9,300

Source: Ovum

On the radar: Palo Alto Networks PA-Series next-generation firewall

Ovum view

Palo Alto Networks' PA-Series essentially created the next-generation firewall market, and has championed ease of use, largely through unified business-driven policy management. Other highlights include its broad functionality, solid efficacy, and high customer satisfaction.

However, the product line isn't perfect. Throughput metrics now trail notable competitors, it doesn't share key performance indicators like VPN and decryption specs, and its pricing has risen to the point where PA-Series is usually more expensive than competing solutions.

Key messages

- PA-Series provides a unified, business-centric policy across all its physical, virtual, and cloud-native firewall instances, allowing easier, more efficient administration.
- The vendor's growing ecosystem of cloud-driven capabilities, particularly its cloud-based WildFire sandboxing and Prisma Access cloud-delivered firewalling, are key strengths.
- The vendor's throughput notably lags competitors with more recent hardware refresh cycles, and it lacks candor on key metrics such as decryption performance.
- PA-Series pricing is generally higher than competing products, particularly on subscription costs.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

Why put Palo Alto Networks on your radar?

Palo Alto Networks pioneered the next-generation firewall and cloud-based malware sandboxing and has developed a reputation for ease of use and effectiveness. Its next goal, an ambitious one, is to become the Amazon.com of enterprise cybersecurity.

The vendor has subtly transformed in the past few years. While appliances remain the largest portion of its business, its emerging identity is as a provider of cybersecurity software and services via the cloud.

Its Cortex line aims to gather customers' data into a massive cloud-based data lake, apply machine learning to identify new threats and attack patterns, and empower customers to unify threat detection and incident response across networks, endpoints, and cloud systems. In addition, the vendor's Prisma line of cloud-delivered security solutions offers enterprise-grade security without traditional hardware deployments.

Ultimately, Palo Alto Networks is aiming to redefine how enterprises purchase, deploy, and operate their cybersecurity architectures. Few other enterprise security vendors are as dramatically disruptive, and this disruption is urgently needed in an industry where malicious adversaries succeed far too often.

Highlights

Palo Alto Networks' PA-Series next-generation firewalls deliver a robust set of network security controls in an easy-to-manage way, enabling organizations to secure users and devices wherever they are, be it inside the corporate network, at a branch office, or in a coffee shop halfway around the world.

The PA-Series appliance line consists of:

- PA-220 desktop models
- PA-800 Series for branch offices and midsize businesses
- PA-3200 Series for enterprise gateway deployments
- PA-5200 Series for large enterprise data centers
- PA-7000 line for service provider and large data center use cases.

It also offers a rugged appliance, and a variety of customizations for use in specific vertical industries.

Palo Alto Networks has long stood out for its ability to glean context from application traffic, identifying and classifying traffic flows based on users, applications, and content. Furthermore, the vendor was the first to offer a unified application-centric policy-management paradigm that adopts a business-centric approach to firewall policy, increasing adaptability while no longer being dependent on specific ports and protocols.

Interestingly, while Palo Alto Networks has long been known for its FPGA-based hardware appliances with single-pass architectures that allow a lone inspection engine to process traffic flows one time while applying multiple security functions, its appliance throughput performance is now far below its competitors. Its top 1U appliance, the PA-850, offers throughput of only 2 Gbps of firewall inspection and 1 Gbps of full inspection. The company declined to provide decryption and SSL (TLS) VPN performance figures.

However, it does compensate with innovative capabilities such as granular policy-based decryption, enabling customers to only decrypt flows that meet certain criteria, and conversely never decrypt

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

others such as those traffic carrying banking or healthcare data. Its PAN-OS firewall software also includes an optional decryption broker feature, which shares decrypted traffic with other security tools, decreasing the firewall load and increasing network efficiency.

Its physical appliances are supplemented by its VM-Series of virtual NGFW appliances, which support platforms including VMware ESXi, Nutanix AHV, Microsoft Hyper-V, Cisco ACI and ENCS, KVM on CentOS/RHEL and Ubuntu, OpenStack, and Citrix Xen Server on SDX. It also offers cloud-native virtual firewalls supporting all three major public cloud infrastructure platforms along with Alibaba AliCloud, Oracle, and VMware vCloud, with on-demand and bring-your-own-license options. All versions run its PAN-OS operating system, with version 9.1 released in December 2019.

Features that span its various firewall form factors include stateful and application-aware firewalling, intrusion detection and prevention, antimalware/spyware, URL filtering, and DNS query analysis. Its newest software release also added full native SD-WAN features.

PA-Series is supported by a variety of supplemental offerings including WildFire dynamic malware analysis and the many and varied options offered by Cortex and Prisma Access and Prisma SaaS. A noteworthy new offering is its revamped Prisma Access data loss prevention (DLP) engine addressing both data in motion and data at rest. The vendor's long-term goal is synchronized single-policy DLP across its product portfolio, although this will take multiple years to come to fruition.

All its NGFWs are managed by the Panorama management system. Available as an on-premises appliance, virtual appliance (ESXi), and as a public cloud SaaS application (though lacking feature parity), Panorama can manage up to 5,000 NGFWs and 65,000 unique policies on a single management instance.

Ovum research of Palo Alto Networks PA-Series customers revealed strong affinity for the product, especially its business-focused policy management system, which works consistently even across dynamic networks in which port and protocol usage often changes. Customers appreciate the openness about product roadmaps and access to product managers. Feedback on customer support, however, was inconsistent, with increasing customer response times cited as an issue.

Background

Palo Alto Networks essentially created the next-generation firewall segment because the company's founder, Nir Zuk, wasn't satisfied with the status quo. Zuk founded the company in 2005 following his work developing the first commercial stateful-inspection firewall for Check Point in his native Israel, and later the first commercial intrusion prevention system for NetScreen Technologies (later acquired by Juniper).

But these and other enterprise network security appliances couldn't identify and classify application traffic, an increasing necessity amid what Zuk correctly foresaw as explosive growth in traffic to and from web- and cloud-based applications.

In 2007, Palo Alto Networks therefore released the first of what it called next-generation firewalls because they were capable of not only managing Layer 3 and 4 traffic, but also Layer 7 application traffic. It didn't take long for the revolutionary NGFW to become the industry standard in firewalls, and every other major vendor has since developed or acquired application-aware firewall capabilities.

In 2012, the same year the company went public on the NYSE, Palo Alto Networks debuted WildFire, a cloud-based dynamic malware analysis product that disrupted what to that point had been a segment dominated by a small number of appliance vendors. The combination of PA-Series NGFWs

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

and WildFire cloud-based sandboxing has subsequently produced billions of dollars in revenue, serving as the primary engine powering Palo Alto Networks' rapid growth.

Today, the company has 7,300 employees, 67,000 customers in more than 150 countries, and nearly $3bn in revenue in its fiscal 2019.

Current position

Built into the corporate DNA of Palo Alto Networks is the constant need to seek ways to disrupt rivals and market segments. Its next-generation (application-aware) firewall and cloud-based dynamic malware analysis solutions both triggered seismic shifts that are still having an impact on the industry.

Its next ambitious goal is to disrupt the entire enterprise cybersecurity market by redefining how enterprises purchase, deploy, and operate their cybersecurity architectures. Its Cortex line offers an integrated set of cloud-based security offerings to enable rapid threat detection and response using orchestration and automation, bolstered by pre-integrated third-party best-of-breed solutions and a growing data lake of security telemetry from its customers and partners. Meanwhile, its Prisma line seeks to provide a broad set of offerings to secure its customers' journey into the cloud. The innovation being brought to bear by Palo Alto Networks is unrivaled in the industry.

However, its NGFW line, despite being a huge revenue driver for the company, is becoming an area of concern. Its lagging throughput performance figures are indicative of the need for an across-the-board hardware refresh. It is at least two years behind key rivals in the maturity of its SD-WAN capabilities. When combined with concern about a variety of subscription options and rising price points, without corrective action, Ovum sees PA-Series potentially becoming less competitive as a point product purchase option for enterprises. However, it remains a strong choice for customers buying into the Palo Alto Networks ecosystem, which offers arguably the industry's most comprehensive and innovative enterprise security product portfolio.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

Data sheet

Key facts

Table 1: Data sheet: Palo Alto Networks

Product name	PA-Series next-generation firewalls	**Product classification**	NGFW
Product categories	PA-220 (desktop), PA-800 Series (branch/midsize), PA-3200 Series (enterprise), PA-5200 Series (large enterprise/data center), PA-7000 Series (service provider)	**Latest release date**	December 2019 (PAN-OS 9.1)
Industries covered	All	**Geographies covered**	All
Relevant company sizes	All	**Licensing options**	
URL	https://www.paloaltonetworks.com/products/secure-the-network/next-generation-firewall	**Routes to market**	Channel (two-tier)
Company headquarters	Santa Clara, CA, US	**Number of employees**	7,300

Source: Ovum

On the radar: Sophos XG Firewall

Ovum view

Sophos XG Firewall isn't technically an enterprise-grade offering, but its ease of use, tight integration with the vendor’s endpoint security technology, and affordable price have made it extremely popular not only with midmarket enterprises, but also with a surprising number of large organizations. Should its anticipated acquisition by Thoma Bravo be approved, Sophos could get the cash infusion it needs to push further upmarket.

Key messages

- Ease of use is the hallmark of Sophos XG Firewall, excelling in small and midmarket organizations with little or no cybersecurity expertise.
- Tight integration between XG Firewall and its Intercept X endpoint security product offers enterprise-caliber XDR features to SMBs.
- Sophos offers a cloud-based management system for nearly all its products, facilitating frictionless policy management, investigation, and remediation activities.
- Limited appliance performance and a lack of enterprise-grade features makes XG impractical for large organizations.

Why put Sophos on your radar?

Sophos aims to produce innovative, simple-to-use cybersecurity products for small and midsize companies. To its credit, it isn't taking any shortcuts.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

Many top-tier enterprise cybersecurity vendors emphasize business scale and customer growth over efficiency and ease of use. Sophos, however, has prudently balanced steady, consistent growth with careful product development that prioritizes functionality and usability, while tucking in relatively small acquisitions when these can add innovative capabilities.

A large number of Sophos deployments are managed by IT generalists that lack training or experience specific to cybersecurity. Sophos therefore endeavors to make its product easy to learn and manage, while laying the groundwork for an increasing amount of automation, paired with guidance to make informed decisions.

All this combined with high customer satisfaction and reasonable pricing, Sophos is an NGFW vendor to watch.

Highlights

The Sophos XG Firewall line might not yet compete for data center rack space, but with more than 90,000 active customers and nearly 200,000 deployed instances globally and growing, the product line is already one of the industry's most widely deployed NGFWs.

For an SMB-centric product, the XG Firewall offers a wide array of enterprise-caliber features, including:

- stateful firewall,
- intrusion detection and prevention
- IPsec and SSL (TLS) VPN
- synchronized application control for identifying and categorizing application traffic
- antimalware
- antispam
- email encryption support.

The product also offers advanced web threat protection features to ward off polymorphic and obfuscated web threats, including JavaScript emulation (attack prevention), behavioral analysis, and origin reputation.

XG Series features desktop, 1U, and 2U rack-mounted appliances. Its performance generally trails that of its competitors. Its top-performing 1U appliance, the XG 450, offers 50 Gbps of monitoring throughput, but only 9.2 Gbps of full-inspection performance and 3.6 Gbps of encrypted traffic inspection throughput. Sophos, however, asserts it is increasing these figures with its upcoming v18 firmware release, which will feature its new Xstream packet-processing architecture.

In addition to its physical appliances, Sophos offers x86-compatible virtual firewalls, supporting VMware ESXi, Microsoft Hyper-V, KVM, and Citrix XenApp. It also supports public cloud deployments in Microsoft Azure with on-demand or bring-your-own licenses. Sophos offers full feature parity between its physical and virtual appliances, with all features available on all models.

Interestingly, Sophos supports divergent branch office use cases. Its XG Firewall line includes some little-known SD-WAN capabilities, such as support for multiple WAN links with monitoring, balancing, and failover. Dynamic WAN management features are also slated for its v18 release. Conversely, Sophos also offers its VPN-only Remote Ethernet Device (RED) for secure traffic backhaul in branch offices where full firewall deployments are cost-prohibitive.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

Sophos offers two licensing bundles. Its EnterpriseProtect bundle includes all firewall, network, and web protection features; Sandstorm cloud-based dynamic malware analysis; software updates; and 24x7 support. The TotalProtect bundle includes all those features plus email protection, DLP support, web application firewall, and reverse-proxy support.

One of the top benefits of the XG Firewall line is its tight integration with the Intercept X client product, which among other capabilities offers endpoint protection and endpoint detection and response for endpoints and servers (supporting Windows 7-10, Windows Server 2008 R2 and up, and Mac OS X 10.12 and up). The vendor's Synchronized Security feature enables Sophos firewalls and endpoints to exchange information about user actions and application traffic, as well as conducting automatic endpoint isolation at the firewall level when a policy violation is detected.

According to Sophos, arguably the top reason why it wins against high-profile industry competitors is Sophos Central, its SaaS-based, single-pane-of-glass management system for overseeing deployment, management, policy, updates, and response, with optional log management and analytics. An on-premises management appliance option is also available.

Ovum research among Sophos customers highlighted the ease of management, the integration of the XG Firewall with Intercept X endpoints, and an affordable price point with simple license management.

Background

Sophos might still be perceived as a niche antimalware vendor, but the company has grown well beyond its humble beginnings.

Founded in Oxford, UK, in 1985, Sophos produced antivirus and encryption products primarily for UK customers during its first decade, but in the late 1990s began to set its sights beyond the UK. Its first big move was to acquire antispam vendor ActiveState in 2003, expanding into email protection.

Much of the intellectual property that eventually developed into the XG Firewall line came from its acquisitions of network security vendors Astaro and Cyberoam Technologies in 2011 and 2014, respectively.

Today, despite being formally based in Abington, UK, and listed on the London Stock Exchange (SOPH), Sophos CEO Kris Hagerman and most of its senior leaders are from the US. The company offers a broad suite of network, endpoint, web, and cloud security products for small and midmarket customers. It employs 3,500 people, counts more than 400,000 customers and 100 million users in 150 countries, and more than 50,000 channel partners worldwide.

In October 2019, US private equity firm Thoma Bravo offered to acquire Sophos for approximately $3.9bn. Sophos's board of directors has recommended the offer to the company's shareholders and the deal is expected to be completed in the first quarter 2020.

Current position

There is no doubt that Sophos is focused on the midmarket. Companies with fewer than 5,000 employees account for about 80% of its sales but it has also won several thousand large enterprise customers that appreciate its simplicity and flexibility. Its proven success with enterprises highlights future opportunities to increase revenue by courting large customers.

However, should it choose to actively court enterprises, the company must invest in more hardware and features specifically geared toward large enterprises. Most notably it must significantly increase

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

its investment in hardware because its 1U and 2U appliances lack the processing power to scale up to meet needs of large enterprise data centers. It also lacks large-scale clustering support and is behind competitors on public cloud platform support. It supports only Microsoft Azure, and unlike rivals large and small, it lacks an accompanying cloud-delivered firewall service.

These are good problems to have, however, because they can be solved with time and money. Should Sophos's acquisition by Thoma Bravo come to pass, an infusion of cash that enables Sophos to accelerate its move into the large enterprise NGFW market could be positive for investors and customers alike.

Data sheet

Key facts

Table 1: Data sheet: Sophos

Product name	Sophos XG Firewall	**Product classification**	NGFW
Product categories	SMB, branch office, small enterprise	**Latest release date**	August 2019 (SFOS 17.5 MR8)
Industries covered	All	**Geographies covered**	All
Relevant company sizes	Recommended for organizations with fewer than 5,000 employees	**Licensing options**	1/2/3-year subscriptions; monthly terms available for MSP partners
URL	https://www.sophos.com/en-us/products/next-gen-firewall.aspx	**Routes to market**	Two-tier channel only; regional sales teams for high touch enterprise customers; global sales team for MSP partners
Company headquarters	Abingdon, UK	**Number of employees**	3,500

Source: Ovum

On the radar: WatchGuard Technologies Firebox Next-Generation Firewall

Ovum view

WatchGuard might be the best-kept secret in next-generation firewalls. Its depth of features and ease of use rival that of any enterprise vendor, and its price points are significantly lower than well-known competing brands. Should it decide to move upmarket, it would need to expand its Firebox line to serve large-enterprise use cases, improve throughput and performance, bolster its channel, and prove the efficacy of the rest of its burgeoning product ecosystem.

Key messages

- With little fanfare over many years, WatchGuard Technologies has created a next-generation firewall that holds up against any rival on efficacy and breadth of features.
- WatchGuard differentiates on ease of deployment and management, and by offering a lower price point than nearly all its key competitors.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

- The vendor has all the key pieces to make a major push into large enterprises, but insists it is firmly committed to its focus on the midmarket.

Why put WatchGuard on your radar?

WatchGuard prides itself on delivering enterprise-grade network security to customers that would otherwise lack the budget and staff to manage it (small and midmarket organizations with fewer than 1,000 employees, often distributed). It has, however, been quietly building a vast product portfolio that is poised to rival top-tier enterprise cybersecurity vendors.

What sets WatchGuard apart is pricing, which is not only as much as 50% lower than that of its key rivals but is also provided in simple licensing terms with only two subscription options, with some offerings, such as its Dimension logging and analytics server, provided for free, and 24x7 support for all customers.

Highlights

The Firebox line is split into two tiers: T-Series desktop models serving up to 60 users, and M-Series 1U rack-mounted appliances.

Its top-of-the-line M5600 model, which offers up to 60 Gbps of stateful firewall monitoring and more than 12 million concurrent connections, can support deployments of up to several thousand users. The vendor also supports virtual deployments on KVM, Microsoft HyperV, and VMware ESXi, as well as public cloud offerings for AWS or Microsoft Azure in both pay-as-you-go and bring-your-own-license options.

Despite not being known for enterprise-grade networking features, the Firebox line offers multiple network address translation options and dynamic routing on-box, as well as SD-WAN features including dynamic path selection, WAN failover, and multi-WAN load balancing.

Its software licensing is split into two tiers. The Basic Security Suite includes intrusion detection and prevention (IDS/IPS), application control, URL and web content filtering, gateway antimalware, antispam, user reputation scoring/botnet detection, and visual network mapping. Total Security Suite includes all of the above and adds cloud-based malware sandboxing (via Lastline), data exfiltration prevention, XDR with its Threat Detection and Response product), DNS screening with its DNSWatch product), and other features.

Its Fireware operating system uses a streamlined, hardened Linux kernel to enhance packet filtering performance while reducing the potential for software vulnerabilities. Case in point: Firebox wasn't affected by the high-profile 2014 Shellshock vulnerability because unlike most Linux distributions it does not include the Bash command language interpreter. WatchGuard relies on microprocessors from Intel and NXP Semiconductor.

The vendor touts its WatchGuard Cloud as a full-featured SaaS management system for both its Firebox NGFWs and AuthPoint IAM technology (its other security offerings such as endpoint and Wi-Fi management are not yet supported). It also offers WatchGuard System Manager, a legacy PC-based software application, as an on-premises management option featuring a GUI, a web-UI for remote access, and command-line interface for advanced scripting.

The vendor's Dimension log-collection and analytics product, available since 2013, is a separate add-on to its Firebox line (at no additional cost), translating firewall logs into a variety of different data points and reports that can be searched in real time or saved indefinitely for conducting future network forensic analysis. While not integrated within Firebox, Dimension is offered to Firebox customers with

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

Total Security Suite licenses at no additional charge. Customers can alternatively store log data in a WatchGuard-managed cloud storage system, but this is only tenable with a Total Security Suite package. Basic provides for just 24 hours of storage.

WatchGuard supplements on-premises Firebox deployments with cloud-based network security, based largely on technology acquired from its recent purchase of DNS security specialist Percipient Networks, a top rival to Cisco's Umbrella offering. Designed to provide NGFW-grade security to off-network devices, DNSWatchGO offers DNS protection against known-bad locations, as well as phishing attack prevention, command-and-control connection blocking, web content filtering, all without a VPN connection, though the solution requires installation of an endpoint client.

Background

Founded in 1996, Seattle-based WatchGuard Technologies employs nearly 700 people. The privately owned firm has delivered slow but steady growth since its early days as an SMB unified threat management startup.

In 1999, the company produced the industry's first self-contained hardware appliance for enterprise security. After making its public debut on the Nasdaq the same year, the company was acquired in 2006 by private equity firms Francisco Partners and Vector Capital for $151m. The vendor consolidated its various firewall platforms in 2010, resulting in the unified Fireware OS that underlays all its firewall technology, and went on to launch its first NGFW in 2011.

In the past few years, CEO Prakash Panjwani, who joined WatchGuard in 2015, has nearly doubled the size of the company in terms of both employee numbers and revenue. A portion of this growth has been fueled by acquisitions. WatchGuard acquired endpoint detection and response (EDR) vendor HawkEye-G from Hexis Cyber Solutions (Sensage) in 2016, multifactor authentication vendor Datablink in 2017, and last year purchased DNS security specialist Percipient Networks.

Current position

WatchGuard prides itself in making security frictionless and easily consumable by organizations that don't have either the budget or the expertise to deploy other vendors' NGFWs, and in making its product work well for security service providers which serve many of the same types of customers.

The numbers prove its success. The vendor competes in more than 100 countries, boasts more than 100 distributors and 10,000 active MSPs and VARs, serves nearly 100,000 total customers, and supports more than 350,000 active appliance deployments. One out of every seven new units sold in 2018 were to displace a competing product, with Cisco Meraki among the solutions WatchGuard most commonly reports displacing.

High-profile independent testing has shown Firebox to be among the industry's most capable NGFW products at both detecting attacks and warding off evasion attempts in which an adversary conducts a targeted attack against the device. Performance of its low-end desktop models has been shown to consistently meet or exceed that of competitors.

Ovum customer research on WatchGuard reveals satisfaction with the easy deployment and minimal upkeep for the Firebox line, along with high uptime and reliability, with policy actions such as blocking traffic to specific geolocations completed in under a minute. Customers also laud Dimension, which is now part of WatchGuard Cloud. They feel it is of tremendous value to get a competitive network forensics product bundled into the cost of the Total Security Suite solution, when such a capability would otherwise cost tens of thousands of dollars.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

WatchGuard affirms it does not intend to focus on large enterprises. If it chose to do so, however, it would have to address some capability gaps. Today it struggles to serve customers with more than several thousand employees in a non-distributed context, primarily because it offers neither a hardware appliance larger than 1 rack unit, nor high-end scalability features such as advanced clustering support. Its full-inspection throughput and encrypted traffic inspection performance numbers also fall well short of contemporary large enterprise expectations. In addition, it lacks a professional services organization. Continued growth would require scaling up in a variety of ways to meet the needs of large enterprises.

There is also a growing market expectation that NGFWs will be part of a larger XDR ecosystem featuring native integration with top-tier endpoint security technology. WatchGuard's top midmarket NGFW rival, Sophos, also offers arguably the industry's top endpoint protection technology featuring native firewall integration, and other competitors aren't far behind. WatchGuard's XDR offering is nascent by comparison, and WatchGuard should prioritize advancing its XDR technology and its marketing narrative to keep pace.

Data sheet

Key facts

Table 1: Data sheet: WatchGuard

Product name	Firebox next-generation firewall	**Product classification**	NGFW
Product categories	T-Series (desktop; up to 10 users), M-Series (1U rack-mounted, midmarket/distributed enterprise)	**Latest release date**	December 2019 (Fireware 12.5.2)
Industries covered	All	**Geographies covered**	All
Relevant company sizes	5,000 employees and under (larger deployment based on use case, typically distributed enterprise)	**Licensing options**	Two-tier (Basic Security Suite, Total Security Suite), one-year and three-year subscription options or support-only option
URL	https://www.watchguard.com/	**Routes to market**	100% channel (global sales function supports partner recruitment/enablement)
Company headquarters	Seattle, WA, US	**Number of employees**	675

Source: Ovum

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. Although On the Radar vendors may not be ready for prime time,

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

they bear watching for their potential impact on markets and could be suitable for certain enterprise and public sector IT organizations.

Further reading

Fundamentals of Next-Generation Firewall Platforms, INT005-000036 (September 2019)

Platform Plays and the Future of Security Management, INT005-000023 (August 2019)

Author

Eric Parizo, Senior Analyst, Infrastructure Solutions

eric.parizo@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

The contents of this product are protected by international copyright laws, database rights and other intellectual property rights. The owner of these rights is Informa Telecoms and Media Limited, our affiliates or other third party licensors. All product and company names and logos contained within or appearing on this product are the trademarks, service marks or trading names of their respective owners, including Informa Telecoms and Media Limited. This product may not be copied, reproduced, distributed or transmitted in any form or by any means without the prior permission of Informa Telecoms and Media Limited.

Whilst reasonable efforts have been made to ensure that the information and content of this product was correct as at the date of first publication, neither Informa Telecoms and Media Limited nor any person engaged or employed by Informa Telecoms and Media Limited accepts any liability for any errors, omissions or other inaccuracies. Readers should independently verify any facts and figures as no liability can be accepted in this regard – readers assume full responsibility and risk accordingly for their use of such information and content.

Any views and/or opinions expressed in this product by individual authors or contributors are their personal views and/or opinions and do not necessarily reflect the views and/or opinions of Informa Telecoms and Media Limited.

CONTACT US

ovum.informa.com
askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing
Boston
Chicago
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
Paris
San Francisco
Sao Paulo
Shanghai
Singapore
Sydney
Tokyo