FORRESTER®

WAVE REPORT

The Forrester Wave™: Enterprise Firewall Solutions, Q4 2024

The 10 Providers That Matter Most And How They Stack Up

October 3, 2024 • **16 min read**

Carlos Rivera
Senior Analyst

CP KC MB

With contributors: Joseph Blankenship, Caroline Provost, Kaitlyn Coalson, and Michael Belden

Summary

> In our 27-criterion evaluation of enterprise firewall providers, we identified the most significant ones and researched, analyzed, and scored them. This report shows how each provider measures up and helps network security professionals select the right one for their needs.

firewall buyers need solutions that can support microsegmentation strategies and secure virtual or cloud-hosted resources to maximize their initial enterprise firewall investments. Additionally, organizations are striving for more centralized policy management across diverse enforcement controls, including enterprise firewalls and components of Zero Trust edge/secure access service edge (ZTE/SASE) such as Zero Trust network access (ZTNA), software-defined WAN (SD-WAN), and firewall-as-a-service (FWaaS) instances. Enterprise firewall solution providers have made enhancements to meet these needs while pushing innovation to prepare organizations for postquantum and booming AI adoption.

As a result of these trends, enterprise firewall customers and their managed service providers (MSPs) should look for vendors that:

1. **Deliver a unified approach to streamline policy creation and orchestration.** Consistency and simplified management of policies within enterprise firewalls along with other network security controls helps organizations maintain greater visibility into policy enforcement and the security posture of their networks. This results in a more coordinated and faster incident response and enhanced operational efficiency. A unified approach also provides network

security teams with a single control plane to streamline policy changes or updates through automation and orchestration capabilities. Incorporating AI/ML capabilities further simplifies administrative tasks, enabling effective creation, implementation, and management of policies across various enforcement points.

2. **Enhance security and management of microsegmented networks.** Enterprise firewalls have traditionally been used to secure north-south traffic through their next-generation capabilities. Enterprise firewalls also support microsegmentation use cases; these solutions provide a granular and often more surgical means to apply policies that govern resource access beyond virtual LANs (VLANs). Policies can be applied by using tags, or labels, to ensure only authorized traffic is exchanged between segments, workloads, or applications and prevent unauthorized lateral movement. Delivering these next-generation capabilities at the workload level helps organizations mature their microsegmentation strategies while utilizing their existing enterprise firewall investments.
3. **Demonstrate efficacy to adapt and defend against modern threats.** Enterprise firewall providers are adopting and integrating innovative technologies to evolve their solutions to effectively address the challenges of the threat landscape of today — and tomorrow. Organizations in highly restricted and sensitive environments want solution providers to make more concentrated efforts to support their goals to adopt new technologies like postquantum cryptography (PQC) and AI as well as defend against threats enabled by these technologies. As a result, vendors have introduced modern capabilities, including support for QUIC and HTTP/3, beyond basic traffic management to allow organizations to

safely adopt these protocols. They also enhanced intrusion detection/response (IDS/IPS) and incident response with AI/ML to detect and defend against threats enabled by those capabilities, and enabled PQC VPNs for S2S connectivity that use NIST standards like CRYSTALS-Kyber for key establishment.

Evaluation Summary

The Forrester Wave™ evaluation highlights Leaders, Strong Performers, Contenders, and Challengers. It's an assessment of the top vendors in the market; it doesn't represent the entire vendor landscape. You'll find more information about this market in our report on The Enterprise Firewall Landscape, Q2 2024.

We intend this evaluation to be a starting point only and encourage clients to view product evaluations and adapt criteria weightings using the Excel-based vendor comparison tool (see Figures 1 and 2). Click the link at the beginning of this report on Forrester.com to download the tool.

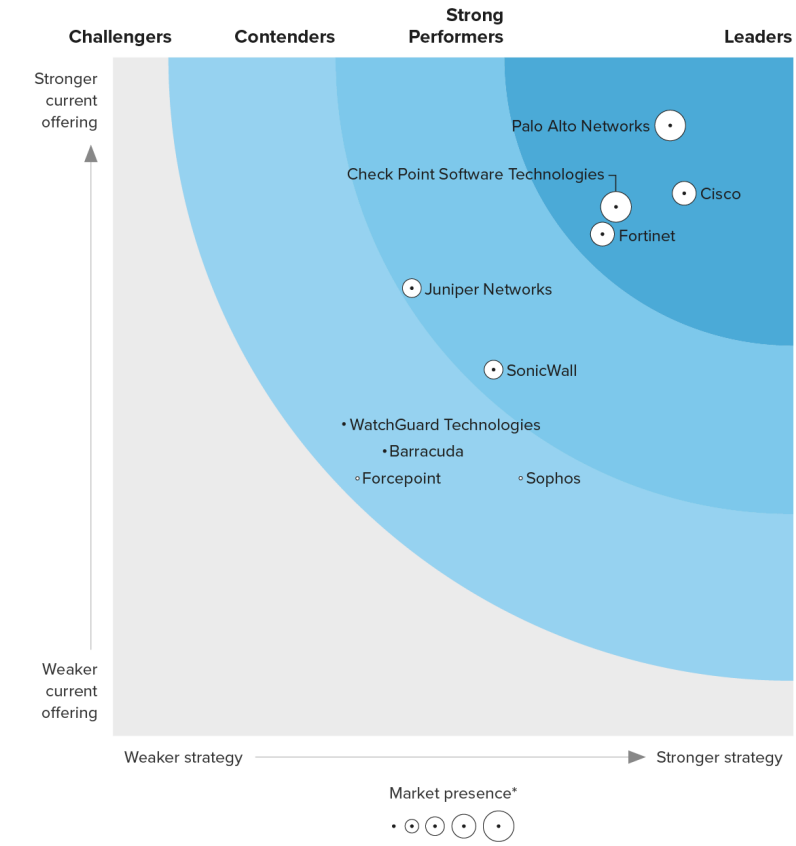

Figure 1 - Forrester Wave™: Enterprise Firewall Solutions, Q4 2024

	Forrester's weighting	Barracuda	Check Point Software Technologies	Cisco	Forcepoint*	Fortinet
Current offering		2.10	3.90	4.00	1.90	3.70
Policy creation and management	10%	3.00	3.00	5.00	1.00	3.00
Usability	5%	1.00	5.00	3.00	1.00	3.00
Traffic decryption	5%	3.00	3.00	5.00	3.00	5.00
Incident response	5%	3.00	5.00	3.00	1.00	3.00
Firewall-as-a-service	5%	1.00	5.00	3.00	3.00	3.00
Traffic encryption	5%	3.00	5.00	5.00	3.00	3.00
Software-defined WAN	5%	5.00	3.00	3.00	3.00	5.00
DNS security	5%	1.00	5.00	5.00	1.00	5.00
Threat intelligence	5%	1.00	5.00	5.00	1.00	3.00
IDS/IPS	5%	1.00	5.00	5.00	1.00	3.00
Malware analysis and mitigation	5%	3.00	3.00	3.00	1.00	3.00
OT and IoT	5%	3.00	3.00	5.00	3.00	3.00
Performance and optimization	5%	1.00	3.00	3.00	3.00	5.00
Automation efficacy	10%	1.00	5.00	3.00	1.00	5.00
Microperimeters	5%	1.00	3.00	5.00	3.00	3.00
Product security	5%	3.00	3.00	5.00	1.00	3.00
ZTE/SASE	5%	3.00	3.00	3.00	3.00	5.00
Zero Trust enablement	5%	1.00	3.00	3.00	3.00	3.00
Strategy		2.00	3.70	4.20	1.80	3.60
Vision	20%	1.00	5.00	5.00	1.00	3.00
Innovation	10%	1.00	5.00	5.00	3.00	3.00
Roadmap	25%	3.00	3.00	3.00	3.00	3.00
Partner ecosystem	15%	3.00	3.00	5.00	1.00	5.00
Adoption	15%	1.00	3.00	3.00	1.00	3.00
Pricing flexibility and transparency	5%	1.00	5.00	5.00	3.00	5.00
Supporting services and offerings	10%	3.00	3.00	5.00	1.00	5.00
Market presence		1.00	5.00	4.00	1.00	4.00
Revenue	50%	1.00	5.00	3.00	1.00	5.00
Number of customers	50%	1.00	5.00	5.00	1.00	3.00

	Forrester's weighting	Juniper Networks	Palo Alto Networks	SonicWall	Sophos*	WatchGuard Technologies
Current offering		3.30	4.50	2.70	1.90	2.30
Policy creation and management	10%	5.00	5.00	3.00	1.00	3.00
Usability	5%	3.00	3.00	3.00	3.00	5.00
Traffic decryption	5%	3.00	5.00	1.00	1.00	3.00
Incident response	5%	3.00	5.00	3.00	3.00	3.00
Firewall-as-a-service	5%	3.00	5.00	1.00	1.00	1.00
Traffic encryption	5%	3.00	5.00	3.00	1.00	1.00
Software-defined WAN	5%	3.00	5.00	3.00	1.00	3.00
DNS security	5%	3.00	5.00	1.00	1.00	3.00
Threat intelligence	5%	3.00	5.00	3.00	3.00	3.00
IDS/IPS	5%	5.00	3.00	3.00	3.00	1.00
Malware analysis and mitigation	5%	3.00	3.00	5.00	3.00	3.00
OT and IoT	5%	1.00	5.00	3.00	1.00	1.00
Performance and optimization	5%	5.00	5.00	3.00	1.00	1.00
Automation efficacy	10%	3.00	5.00	3.00	3.00	3.00
Microperimeters	5%	3.00	5.00	3.00	1.00	1.00
Product security	5%	3.00	3.00	3.00	3.00	3.00
ZTE/SASE	5%	3.00	5.00	1.00	1.00	1.00
Zero Trust enablement	5%	3.00	3.00	3.00	3.00	1.00
Strategy		2.20	4.10	2.80	3.00	1.70

Vision	20%	3.00	5.00	3.00	3.00	1.00
Innovation	10%	3.00	5.00	1.00	3.00	1.00
Roadmap	25%	1.00	5.00	3.00	3.00	1.00
Partner ecosystem	15%	3.00	3.00	3.00	3.00	1.00
Adoption	15%	1.00	3.00	3.00	3.00	3.00
Pricing flexibility and transparency	5%	3.00	3.00	3.00	3.00	5.00
Supporting services and offerings	10%	3.00	3.00	3.00	3.00	3.00
Market presence		3.00	5.00	3.00	1.00	1.00
Revenue	50%	3.00	5.00	3.00	1.00	1.00
Number of customers	50%	3.00	5.00	3.00	1.00	1.00

All scores are based on a scale of 0 (weak) to 5 (strong).
*Indicates a nonparticipating vendor

Figure 2 - Forrester Wave™: Enterprise Firewall Solutions Scorecard, Q4 2024

Vendor Offerings

Forrester evaluated the offerings listed below (see Figure 3).

Vendor	Product evaluated
Barracuda	CloudGen Firewalls
Check Point Software Technologies	Quantum Security Gateway
Cisco	Cisco Secure Firewall
Forcepoint	Next-Generation Firewall (NGFW)
Fortinet	FortiGate
Juniper Networks	SRX Firewalls
Palo Alto Networks	PA Series Firewalls
SonicWall	NS*sp* Series Next-Generation Firewall
Sophos	XGS Series Firewalls
WatchGuard Technologies	Firebox T Series, Firebox M Series, FireboxV, Firebox Cloud

Figure 3 - Evaluated Vendors And Product Information

Vendor Profiles

Our analysis uncovered the following strengths and weaknesses of individual vendors.

Leaders

1. **Palo Alto Networks differentiates with Strata Cloud Manager for centralized management.** Palo Alto Networks pioneered the next-generation firewall (NGFW) and continues to adapt in the evolving network security space. Precision AI, Palo Alto Networks' proprietary AI system, automates tasks with data from ML, deep learning, and AI models to enhance platform experience. Its ambitious roadmap, driven by customer feedback, highlights capabilities that align with its vision for a secure future in the quantum and AI era. Although Palo Alto Networks remains one of the pricier options in this evaluation, its "platformization" initiative aims to deliver greater value to customers by bundling and integrating its products, services, and features.

   Updates to PAN-OS position the vendor to support use cases for both AI readiness and postquantum. Its leading traffic decryption now intercepts and provides visibility into PQC traffic while blocking and downgrading QUIC sessions. Each firewall appliance is integrated with AI/ML technology to provide real-time IPS. The Strata Network Security Platform provides feature-rich and fully functional centralized management of PAN-OS firewalls — hardware and software — as well as Prisma SASE across a hybrid enterprise. Reference customers praise the vendor for centralized firewall management but express concern that limited feature parity between Strata Cloud Manager and Panorama leaves the latter absent of features for real-time status dashboards and policy optimization. Palo Alto Networks is well suited for existing clients transitioning from Panorama to cloud management and enterprises that are ready to invest in premium security features.

   View Palo Alto Networks' detailed scorecard.

2. **Cisco advances its Secure Firewall into the future with innovation and a strong vision.** Over the past decades, Cisco has balanced supporting its legacy firewall clients while promoting its Secure Firewall solution to help its customers address modern threats with advanced security. Cisco's vision aligns well with its networking strengths, leveraging these strengths to craft a security strategy that envisions the seamless integration of AI and security in the networking fabric. The vendor refined its Secure Firewall offering with persistent innovation including a shared and consistent UX/UI and enhanced IDS/IPS using a SnortML engine. The vendor's roadmap aligns with its vision, as it aims to enhance security efficacy with its newly announced Hypershield solution. Cisco, however, remains challenged in its migration from legacy firewall solutions.

   Cisco distinguishes itself with a multilayered approach to traffic inspection and decryption. Its Encrypted Visibility Engine (EVE) uses machine learning to identify traffic based on behavioral patterns, including PQC-encrypted traffic, without decryption. This enables the decryption of most encrypted traffic, such as TLS 1.3 and QUIC/HTTP3, when necessary, while adhering to industry standards. Its IDS/IPS, powered by Snort3 and SnortML, detects vulnerabilities and is enhanced with Talos threat intelligence for weekly updates. Reference customers praise Cisco's support, especially during migrations from legacy appliances. However, they also highlight the arduous implementation process and stress the need for the vendor to enhance its migration procedures. Organizations looking to replace legacy hardware or expand an existing Cisco ecosystem will find Cisco to be an ideal choice.

View Cisco's detailed scorecard.

3. **Check Point Software Technologies excels with collaborative tools.** Check Point Software Technologies has invested in its Infinity Platform, which includes Quantum, CloudGuard, and Harmony. The vendor's vision is practical and achievable, highlighting the importance of collaborative capabilities that enhance security functions through real-time telemetry — complementary to the Zero Trust Model. The vendor's Infinity ELA license streamlines product consumption, offering full-suite access with pay-as-you-go flexibility that has done well to address licensing issues noted by customers. Its innovations are progressive, driven by organic R&D and acquisitions that resulted in the development of native SD-WAN and improvements to Harmony SASE. The vendor's roadmap is generic and broadly focuses on AI, not offering significant enhancement to key components that clients rely on to maximize hardware investments for scaled hybrid architecture.

   Check Point's Infinity Platform excels in centralized management and UX, offering consistent UI and workflows across cloud and local consoles. The vendor supports collaborative administration with granular profiles, policy locking, change reports, and policy revisions. The vendor needs to refine its communication of the quantum gateway's effectiveness for creating microperimeters, as the focus is more on the Infinity platform rather than on leveraging quantum gateways to secure microsegmented networks beyond the network level. Reference customers like Check Point's strong incident response capabilities, thanks to robust integrations and automation with playbooks for

resolving incidents and creating tickets. Enterprises seeking advanced management and robust troubleshooting should consider Check Point.

View Check Point's detailed scorecard.

4. **Fortinet delivers competitive cost-to-performance united by FortiOS.** Over the years, Fortinet's enterprise firewall solution, FortiGate, has been celebrated for its market-leading cost-effectiveness. Today, the vendor provides greater flexibility through its FortiFlex program while still delivering a comprehensive solution, allowing for investment in complementary solutions including hardware and services. It has a robust reseller, service provider, and technology partner ecosystem but needs to improve integrations with third-party security orchestration, automation, and response (SOAR) tools. Fortinet's vision and roadmap emphasize a strategy focused on the convergence of network and security, revisiting familiar concepts that provide a consistent approach toward established ideas of AI integrations.

   Fortinet delivers a firewall appliance with top-tier performance, optimized by three dedicated ASIC processors to significantly reduce resource consumption. This gives organizations the confidence to decrypt and inspect traffic while performing TLS traffic decryption and inspection, including QUIC/HTTP3, with lower impact to performance. Fortinet delivers AI-powered security services through integrations with Fortinet solutions like FortiAnalyzer and other native capabilities to enhance incident response. While Fortinet delivers strong centralized management, it falls short on feature parity, with the FortiOS UI feeling more intuitive, sleek, and modern compared to the outdated appearance of the FortiManager interface.

Only one of Fortinet's reference customers responded to Forrester's outreach for this evaluation. Fortinet is ideal for budget-conscious organizations with more technical firewall skills that are content with leveraging native integrations for visibility and reporting.

View Fortinet's detailed scorecard.

Strong Performers

1. **Juniper Networks brings compelling AI capabilities, but its vision lacks depth.** Networking vendor Juniper is set to bolster its networking arsenal with enhanced security capabilities. However, its future is uncertain as its acquisition by Hewlett Packard Enterprise, announced in January 2024, is set to be finalized later in the year. The vendor's innovations include dedicated ASICs to improve hardware performance, integrations with cloud, and its AI-driven Juniper Mist. Juniper's overall vision emphasizes the mutual benefits of combined networking, security, and AI but lacks specificity on how the vendor will achieve its vision. Its roadmap emphasizes advancements in AI, large language models, and AI for IT operations (AIOps) but lacks transparency on product enhancements, migration plans, and microsegmentation support, with reference customers expressing the need for more information and improved ongoing support services. The vendor's conservative adoption approach leads to ineffective communication about the integration of its firewalls into the company's latest solution, Juniper Mist, which is becoming the new AI and cloud-powered network security solution.

Juniper delivers a consistent user experience across

its management interfaces — J-Web, Security Director, and Security Director Cloud. However, it lacks centralized policies since SD-WAN is managed separately through Juniper Mist. It's worth noting that the vendor's intuitive policy creation and management process enables administrators to configure both standard (traditional) and unified (dynamic and granular L7) policies including the ability to set groupings, user and device profiling, and time restrictions. Policy analysis is an embedded function during creation, allowing rules to be automatically reviewed for anomalies and placement within the firewall ruleset. Enterprises or telco providers seeking to simplify networking capabilities with AI-driven security on a single-vendor technology stack should consider Juniper.

View Juniper's detailed scorecard.

2. **SonicWall hits the mark for SMBs but lags in enterprise capabilities.** SonicWall released its first dedicated firewall appliance in 1997, targeting small and medium-size businesses (SMBs) with a secure, affordable, and easy-to-use solution. Today, its vision respects this legacy by adapting to a broader threat landscape and evolving network security needs. The vendor aims to move upmarket and serve enterprises. Strategic acquisitions like Banyan Security help to better position the vendor to deliver capabilities that meet enterprise hybrid architecture needs. SonicWall lags in its innovation as it is one of the last vendors in this evaluation to offer native FWaaS and ZTE/SASE. Its roadmap continues its MSP enablement but seeks to drive enterprise adoption by developing its cloud-native capabilities and integrating them to address hybrid use cases.

   SonicWall delivers formidable malware analysis and

mitigation capabilities with its Capture ATP. Capture ATP's sandbox is offered as a subscription service, incorporating the vendor's proprietary Real-Time Deep Memory Inspection (RTDMI) to protect against zero-day threats by blocking traffic with suspicious files at the gateway. With Capture ATP enabled, the firewall leverages both local sandboxing and ATP cloud for static and dynamic analysis, delivering verdicts in under a minute and automating the creation and deployment of new signatures. SonicWall's traffic decryption and DNS security trails others in this evaluation, as it has yet to demonstrate visibility and protection against advanced security protocols or provide standard protection for DoT and DGA. Only one of SonicWall's reference customers responded to Forrester's outreach for this evaluation. Enterprises with less complex environments should evaluate SonicWall.

View SonicWall's detailed scorecard.

Contenders

1. **Sophos meets SMBs' needs but misses on microperimeters.** Sophos entered the enterprise firewall space with its acquisition of Astaro in 2011. It now focuses largely on SMBs and its managed detection and response (MDR) service. Sophos' vision focuses on delivering cybersecurity as a service. This aligns well with its SMB customer base, which experiences skill shortages, complexity, and limited access to talent. Sophos' go-to-market approach focuses on MSPs. Its roadmap underscores a strong commitment to cybersecurity as a service, with a focus on enhancing its SASE solution through plans that include cloud-native FWaaS and cloud access security broker (CASB) components.

Sophos remains committed to delivering ease of use for its firewall solution. The UX and UI are consistent across the firewall control center and Sophos Central. However, the firewall solution lacks features like a policy analyzer, hit counts, and dynamic integrations that would streamline and simplify policy creation and management. The vendor now has built-in SD-WAN and a ZTNA gateway but lacks an FWaaS offering. It also lacks the ability to create robust microperimeters or support advanced microsegmentation strategies beyond the network level. The Xstream network processing unit is effective for offloading networking process but does little for security process. Small-office/home-office firms and enterprises without complex use cases or those looking for add-on MDR services should examine Sophos. Sophos declined to participate in the full Forrester Wave evaluation process.

View Sophos' detailed scorecard.

2. **Barracuda offers a cost-effective solution for SMBs but needs a more compelling vision.** Barracuda began as an email security vendor in the early 2000s and acquired firewall vendor Phion in 2009. Barracuda's vision is to create a unified cybersecurity platform, but it lacks depth beyond integrating its portfolio. The vendor is focused on organic growth and engineering, enhancing CloudGen Firewall and SecureEdge SASE with self-healing and a proprietary VPN protocol. However, reference customers note a need to further innovate and keep pace with competitors particularly around cloud integrations. Roadmap items include agentless ZTNA and transitioning ZTNA agents to a single agent to simplify ZTNA implementation. Barracuda goes to market via channel partners and a network of MSPs

globally.

Barracuda's SD-WAN is offered as part of the CloudGen Firewall and SecureEdge with over 100 predefined apps, and it integrates with major cloud service providers. Barracuda offers straightforward policy configuration and management with granular options for general traffic and SD-WAN policy profiles. However, its UI is outdated and cumbersome, resembling a Windows thick client with configuration trees. It supports multiple admins, rule testing, and usage indicators but locks rules based on active changes to prevent errors. The vendor's traffic encryption is impressive, offering unlimited licenses for S2S and C2S VPN tunnels, including a proprietary TINA mode. However, the vendor lacks advanced cipher support to leverage PQC in secure tunnels. Barracuda's CloudGen Firewall overall is below par with a cloud offloading capability that is less than optimal for any architecture larger than an SMB. Barracuda works for large enterprises in need of a capable SD-WAN but is suited for midlevel enterprises with minimal footprint and low bandwidth needs.

View Barracuda's detailed scorecard.

3. **WatchGuard Technologies shines in ease of use but trails in integrating ZTE/SASE.** WatchGuard, founded in 1996, delivers enterprise firewall solutions with a vision to deliver enterprise capabilities and be the go-to security platform for midmarket organizations globally. The vendor's strategy is to provide this capability via an MSP-focused security platform to support its 100% channel model, selling through MSPs. WatchGuard, however, is slow to innovate and embrace cloud-native security as it currently lacks comprehensive ZTE/SASE solutions

that can tie to its built-in SD-WAN capability. The vendor's pricing is simple and straightforward, offering customers three license options and payment plans under its FlexPay program. Its roadmap remains simplistic with the vendor taking a late market approach to developing ZTE/SASE and consolidating management with its Firebox, set for release at the tail-end of this year.

WatchGuard delivers ease of use and management for day-to-day operations but lacks features such as automated alerting or notifications for shadow and stale rules. WatchGuard's Firebox firewalls integrate with APT Blocker, its dual-engine cloud-based sandbox powered by WatchGuard and Bitdefender, to inspect and block suspicious traffic and files with verdicts issued on files in one minute and executables in five. Through ThreatSync extended detection and response (XDR) and network analysis and visibility (NAV) integration, Firebox can automate host isolation based on analysis completed in sandbox. Reference customers praise its simplicity for creating and managing policies by noting the intuitive implementation and use of template creation. SMBs looking for simple, manageable firewalls at low cost should look to WatchGuard Technologies.

View WatchGuard's detailed scorecard.

4. **Forcepoint promotes its ZTE/SSE capabilities but neglects its on-premises firewall.** Forcepoint has gone through a series of acquisitions, rebranding, and restructuring as it reinvents itself as a cybersecurity vendor. The vendor acquired enterprise firewalls Stonesoft and Sidewinder but has now turned its attention away from its on-premises firewalls to focus on its ZTE/SASE services. The

vendor's overall vision is to secure customers with a data-security-focused SASE solution. Its innovation and roadmap are aligned to the vendor's Forcepoint ONE ZTE/SASE offering and not on further developing its hardware appliance for on-premises use cases.

Forcepoint's current lineup includes its 3500 Series, which provides high-end performance comparable to other vendors in this evaluation. The vendor claims 40 Gbps of threat prevention throughput without built-in offloading via dedicated ASICs or CPUs. Additionally, Forcepoint is one of the few vendors on this evaluation that supports inspection and decryption of HTTP3/QUIC traffic. However, it doesn't offer DNS over QUIC (DoQ) or DNS over HTTP/3 (DoH3). Forcepoint provides localized management of its firewalls via Security Management Center, but the UX and UI are dated and inconsistent when compared to its Forcepoint ONE counterpart. Enterprises that are looking for SSE and plan to reduce on-premises deployments should consider Forcepoint. Forcepoint declined to participate in the full Forrester Wave evaluation process.

View Forcepoint's detailed scorecard.

Evaluation Overview

We grouped our evaluation criteria into three high-level categories:

1. **Current offering.** Each vendor's position on the vertical axis of the Forrester Wave graphic indicates the strength of its current offering.

2. **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies, including elements such as vision and innovation.
3. **Market presence.** The size of each vendor's marker on the graphic reflects Forrester's assessment of its market presence.

Vendor Inclusion Criteria

Each of the vendors we included in this assessment has:

1. **A physical, on-premises, content-aware network firewall appliance for north-south and east-west use cases.** The solution must feature layer 7 content inspection with technologies like IDS/IPS, which are often required by Forrester clients. Software-only solutions and solutions embedded within a hypervisor or delivered solely from the cloud are not evaluated in this Forrester Wave.
2. **Enforcement of Zero Trust access natively or through integration.** The solution must feature a capability that enables it to serve as an enforcement point for Zero Trust access, leveraging context-based policies for secure access between entities and enterprise-controlled resources beyond traditional VPN.
3. **At least $90 million in annual category revenue.** Vendors in this report have at least $90 million in firewall revenue in the previous 12-month period.
4. **A significant global presence.** Each vendor included in this report must sustain at least 30% of its firewall revenue outside its home region.
5. **Mindshare among Forrester clients within the industry.** Vendors we are evaluating are frequently mentioned in Forrester client inquiries, vendor

selection RFPs, shortlists, consulting projects, and case studies. These vendors are also mentioned by other vendors during Forrester briefings as viable and formidable competitors.

Supplemental Material

Online Resource

We publish all our Forrester Wave scores and weightings in an Excel file that provides detailed product evaluations and customizable rankings; download this tool by clicking the link at the beginning of this report on Forrester.com. We intend these scores and default weightings to serve only as a starting point and encourage readers to adapt the weightings to fit their individual needs.

The Forrester Wave Methodology

A Forrester Wave is a guide for buyers considering their purchasing options in a technology marketplace. To offer an equitable process for all participants, Forrester follows The Forrester Wave™ Methodology to evaluate participating vendors.

In our review, we conduct primary research to develop a list of vendors to consider for the evaluation. From that initial pool of vendors, we narrow our final list based on the inclusion criteria. We then gather details of product and strategy through a detailed questionnaire, demos/briefings, and customer reference surveys/interviews. We use those inputs, along with the analyst's experience and expertise in the marketplace, to score vendors, using a relative rating system that

compares each vendor against the others in the evaluation.

We include the Forrester Wave publishing date (quarter and year) clearly in the title of each Forrester Wave report. We evaluated the vendors participating in this Forrester Wave using materials they provided to us by July 19, 2024, and did not allow additional information after that point. We encourage readers to evaluate how the market and vendor offerings change over time.

In accordance with our vendor review policy, Forrester asks vendors to review our findings prior to publishing to check for accuracy. Vendors marked as nonparticipating vendors in the Forrester Wave graphic met our defined inclusion criteria but declined to participate in or contributed only partially to the evaluation. We score these vendors in accordance with our vendor participation policy and publish their positioning along with those of the participating vendors.

Integrity Policy

We conduct all our research, including Forrester Wave evaluations, in accordance with the integrity policy posted on our website.