The Forrester Wave™: Enterprise Firewalls, Q3 2020

The 11 Providers That Matter Most And How They Stack Up

by David Holmes
August 10, 2020

Why Read This Report

In our 34-criterion evaluation of enterprise firewall providers, we identified the 11 most significant ones — Barracuda Networks, Check Point Software Technologies, Cisco, Forcepoint, Fortinet, Huawei, Juniper Networks, Palo Alto Networks, SonicWall, Sophos, and WatchGuard — and researched, analyzed, and scored them. This report shows how each provider measures up and helps security and risk professionals select the right one for their needs.

Key Takeaways

Palo Alto Networks And Cisco Lead The Pack
Forrester's research uncovered a market in which Palo Alto Networks and Cisco are Leaders; Check Point Software Technologies, Fortinet, Forcepoint, Sophos, Juniper Networks, and Huawei are Strong Performers; and Barracuda Networks, WatchGuard, and SonicWall are Contenders.

Cloud And Zero Trust Are Key Differentiators
As legacy, on-premises technology becomes outdated and less relevant, improved delivery and reach will dictate which providers will lead the pack. Vendors that can provide Zero Trust and cloud control position themselves to successfully deliver security and manageability to their customers.

The Forrester Wave™: Enterprise Firewalls, Q3 2020

The 11 Providers That Matter Most And How They Stack Up

by David Holmes
with Joseph Blankenship, Matthew Flug, and Peggy Dostie

August 10, 2020

Table Of Contents

Related Research Documents

The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q4 2019

Now Tech: Enterprise Firewalls, Q1 2020

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Enterprise Firewalls Will Take Enterprises To The Zero Trust Edge

Mark Twain is quoted as having said, "The reports of my death have been greatly exaggerated." The enterprise perimeter could make a similar observation: The death of the perimeter has not yet come to pass despite numerous reports to the contrary. The guardian of that perimeter, the enterprise firewall, has not only avoided obsolescence, it's become the foundational platform for network security functions like malware detonation, signature-based content inspection, and incident response. Yet the current pandemic may pose the most difficult challenge to the relevance conventional enterprise firewalls: Applications have fled to the cloud, and users work remotely. The lockdown will accelerate the shift to concentrating security services at a Zero Trust edge.

Security buyers looking to build the enterprise connectivity architecture of the future should consider enterprise firewall solutions that:

- **Support the Zero Trust edge model.** The Zero Trust edge (ZTE) describes the security stack fully or partially edge-delivered and consumed as a service. The Zero Trust edge includes content inspection, intrusion detection/prevention (IDS/IPS), malware detonation, DNS firewalling, secure web gateway (SWG), CASB, and most importantly, Zero Trust network access (ZTNA). Branches use SD-WAN to connect to the edge network instead of backhauling traffic to the security stack in the data center. Nearly every firewall vendor evaluated in this report recognizes the opportunity (and threat) of ZTE and has a strategy to address it.
- **Extend management into the cloud.** Multiple vendors in this report can manage native public cloud security objects, like AWS security groups, containers, and Azure and Alibaba firewall objects. We describe this capability as the fourth generation of firewalls, or FW4. The value proposition of FW4 derives from the fact that network security functions are already controlled through the firewall management console and log collectors and that no retraining or new vendor vetting is necessary in this model. FW4 solutions consolidate and normalize various public cloud provider security interfaces into one that end users already know.
- **Feature a strong endpoint or tight integration with an endpoint leader.** According to a 2020 Forrester survey, over 50% of employees who went home for pandemic lockdown hope to stay there even after the lockdown is over.[1] For remote users, a strong endpoint component is necessary to direct traffic through to a vendor edge network for content inspection and secure remote access. When a remote client host becomes compromised, the endpoint component needs to isolate and assist incident response. Endpoint has not been a core strength for enterprise firewall vendors in the past, but the pandemic lockdown and the future of remote work make this functionality a priority.

Evaluation Summary

The Forrester Wave™ evaluation highlights Leaders, Strong Performers, Contenders, and Challengers. It's an assessment of the top vendors in the market and does not represent the entire vendor landscape.

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 Figure 1 and see Figure 2). Click the link at the beginning of this report on Forrester.com to download the tool.

FIGURE 1 Forrester Wave™: Enterprise Firewalls, Q3 2020

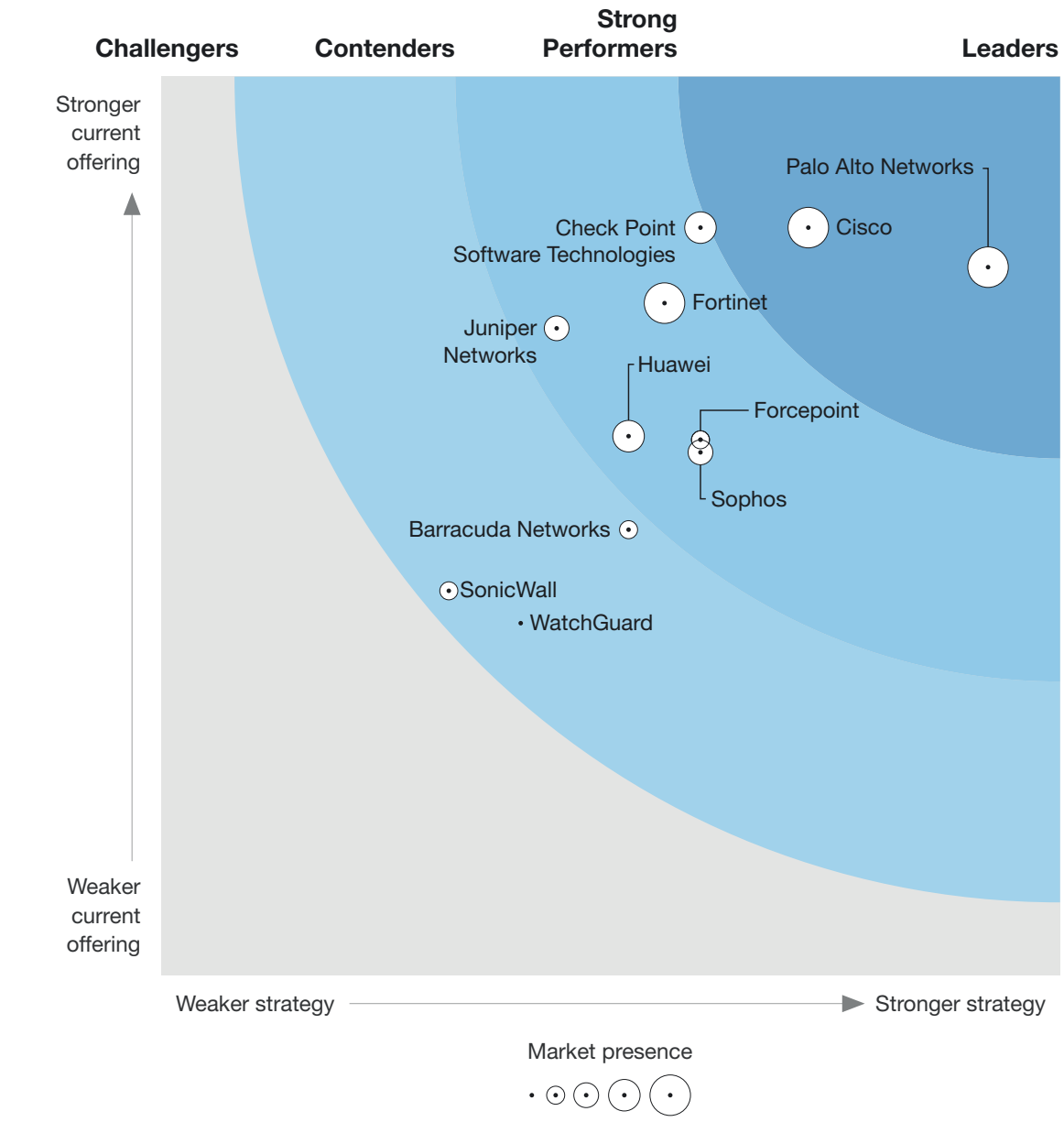

FIGURE 2 Forrester Wave™: Enterprise Firewalls Scorecard, Q3 2020

	Forrester's weighting	Barracuda Networks	Check Point Software Technologies	Cisco	Forcepoint	Fortinet	Huawei
Current offering	50%	2.48	4.16	4.16	2.98	3.74	3.00
Policy creation and management	4%	3.00	5.00	5.00	5.00	3.00	3.00
Rule management over time	3%	1.00	5.00	3.00	1.00	3.00	3.00
Management API	3%	3.00	5.00	5.00	5.00	3.00	3.00
Management plane security	2%	3.00	3.00	5.00	1.00	5.00	3.00
Usability	5%	1.00	5.00	5.00	3.00	3.00	3.00
TLS decryption	5%	3.00	1.00	5.00	3.00	5.00	5.00
High availability and clustering	4%	1.00	5.00	5.00	5.00	5.00	3.00
Centralized management	3%	3.00	5.00	3.00	5.00	5.00	3.00
Cloud-delivered components	5%	1.00	3.00	5.00	1.00	1.00	3.00
Incident response and SOC automation	4%	3.00	5.00	5.00	3.00	3.00	5.00
User and application context	3%	3.00	5.00	5.00	3.00	3.00	3.00
IDS/IPS	4%	1.00	5.00	5.00	1.00	3.00	5.00
Automated malware analysis	4%	3.00	5.00	3.00	1.00	5.00	5.00
Email, web, and email filtering	2%	3.00	5.00	3.00	3.00	5.00	3.00
Threat intelligence	3%	1.00	5.00	5.00	3.00	3.00	3.00
Risk scoring	3%	3.00	1.00	3.00	5.00	3.00	3.00
Microsegmentation	5%	3.00	3.00	5.00	3.00	3.00	3.00
Zero Trust	2%	1.00	5.00	5.00	3.00	1.00	1.00
Workload protection	5%	1.00	5.00	5.00	1.00	5.00	1.00
Endpoint	5%	3.00	5.00	3.00	5.00	3.00	1.00

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

FIGURE 2 Forrester Wave™: Enterprise Firewalls Scorecard, Q3 2020 (Cont.)

	Forrester's weighting	Juniper Networks	Palo Alto Networks	SonicWall	Sophos	WatchGuard
Current offering	50%	3.60	3.94	2.14	2.91	1.96
Policy creation and management	4%	5.00	3.00	3.00	3.00	1.00
Rule management over time	3%	5.00	3.00	3.00	5.00	3.00
Management API	3%	5.00	3.00	3.00	3.00	1.00
Management plane security	2%	3.00	3.00	1.00	5.00	3.00
Usability	5%	3.00	5.00	3.00	3.00	3.00
TLS decryption	5%	5.00	3.00	1.00	3.00	3.00
High availability and clustering	4%	1.00	1.00	3.00	1.00	1.00
Centralized management	3%	5.00	3.00	3.00	3.00	1.00
Cloud-delivered components	5%	3.00	5.00	1.00	1.00	1.00
Incident response and SOC automation	4%	5.00	5.00	3.00	3.00	3.00
User and application context	3%	3.00	5.00	3.00	5.00	3.00
IDS/IPS	4%	5.00	5.00	3.00	5.00	1.00
Automated malware analysis	4%	5.00	5.00	3.00	5.00	1.00
Email, web, and email filtering	2%	5.00	3.00	3.00	3.00	1.00
Threat intelligence	3%	3.00	5.00	3.00	5.00	3.00
Risk scoring	3%	3.00	5.00	1.00	3.00	1.00
Microsegmentation	5%	3.00	3.00	0.00	0.00	0.00
Zero Trust	2%	1.00	5.00	1.00	3.00	1.00
Workload protection	5%	5.00	5.00	3.00	1.00	1.00
Endpoint	5%	3.00	3.00	3.00	5.00	3.00

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

FIGURE 2 Forrester Wave™: Enterprise Firewalls Scorecard, Q3 2020 (Cont.)

	Forrester's weighting	Barracuda Networks	Check Point Software Technologies	Cisco	Forcepoint	Fortinet	Huawei
Current offering	50%	2.48	4.16	4.16	2.98	3.74	3.00
Firewall-as-a-service	5%	1.00	5.00	5.00	3.00	3.00	3.00
Software-defined WAN	5%	5.00	1.00	1.00	5.00	5.00	3.00
IPSec and VPN	2%	5.00	5.00	3.00	3.00	5.00	1.00
Certifications	2%	1.00	5.00	3.00	3.00	3.00	5.00
Performance characteristics	4%	3.00	3.00	1.00	3.00	5.00	3.00
ICS/OT/IoT	5%	5.00	5.00	5.00	1.00	5.00	1.00
Additional security control integrations	3%	3.00	5.00	5.00	3.00	5.00	3.00
Strategy	50%	2.60	3.00	3.60	3.00	2.80	2.60
Product vision	30%	3.00	3.00	5.00	3.00	3.00	1.00
Roadmap	30%	3.00	3.00	3.00	3.00	3.00	3.00
Business execution	10%	3.00	1.00	3.00	3.00	5.00	5.00
Delivery model	20%	1.00	3.00	3.00	3.00	1.00	3.00
Supporting products and services	10%	3.00	5.00	3.00	3.00	3.00	3.00
Market presence	0%	2.00	4.00	5.00	2.00	4.25	3.25
Product revenue	75%	2.00	4.00	5.00	2.00	4.00	3.00
Enterprise clients (5,000+ employees)	25%	2.00	4.00	5.00	2.00	5.00	4.00

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

FIGURE 2 Forrester Wave™: Enterprise Firewalls Scorecard, Q3 2020 (Cont.)

	Forrester's weighting	Juniper Networks	Palo Alto Networks	SonicWall	Sophos	WatchGuard
Current offering	50%	3.60	3.94	2.04	2.91	1.96
Firewall-as-a-service	5%	1.00	5.00	0.00	1.00	0.00
Software-defined WAN	5%	3.00	3.00	3.00	3.00	3.00
IPSec and VPN	2%	3.00	3.00	1.00	3.00	3.00
Certifications	2%	3.00	3.00	3.00	5.00	5.00
Performance characteristics	4%	5.00	3.00	1.00	1.00	3.00
ICS/OT/IoT	5%	3.00	5.00	1.00	3.00	3.00
Additional security control integrations	3%	3.00	5.00	3.00	3.00	3.00
Strategy	50%	2.20	4.60	1.60	3.00	2.00
Product vision	30%	3.00	5.00	3.00	3.00	1.00
Roadmap	30%	1.00	5.00	1.00	3.00	3.00
Business execution	10%	3.00	3.00	1.00	5.00	3.00
Delivery model	20%	1.00	5.00	1.00	1.00	1.00
Supporting products and services	10%	5.00	3.00	1.00	5.00	3.00
Market presence	0%	2.75	4.50	2.00	2.50	1.00
Product revenue	75%	3.00	5.00	2.00	2.00	1.00
Enterprise clients (5,000+ employees)	25%	2.00	3.00	2.00	4.00	1.00

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

Vendor Offerings

Forrester included 11 vendors in this assessment: Barracuda Networks, Check Point Software Technologies, Cisco, Forcepoint, Fortinet, Huawei, Juniper Networks, Palo Alto Networks, SonicWall, Sophos, and WatchGuard (see Figure 3).

FIGURE 3 Evaluated Vendors And Product Information

Vendor	Product evaluated	Product version evaluated
Barracuda Networks	Barracuda CloudGen Firewall	8.0.2
Check Point Software Technologies	Check Point Security Gateway	R80.40
Cisco	Firepower Threat Defense	6.5
Forcepoint	Forcepoint NGFW	6.7
Fortinet	FortiGate	6.2.3
Huawei	USG Series Firewall	V600R007
Juniper Networks	SRX Series Next Generation Firewalls	
Palo Alto Networks	Next-generation firewall appliances: Next-generation firewall operating system: PAN-OS Next-generation firewall central management, reporting, and logging: Panorama Subscriptions: WildFire (advanced malware analysis), AutoFocus (threat intelligence service), PAN-DB (URL filtering), DNS Security service, and GlobalProtect (extending security to mobile workers) 5G-ready next-generation firewall: K2-Series	PAN-OS 9.1
SonicWall	Firewalls: TZ, NSa, NSv, & NSsp Series Firewall manager: CSC & GMS	6.5.4
Sophos	Sophos XG Firewall	V18
WatchGuard	WatchGuard Firebox and Fireware OS	12.5.3

Vendor Profiles

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

Leaders

› **Palo Alto Networks is moving aggressively to the cloud.** Migration to the cloud is inevitable, and the user exodus caused by the pandemic is accelerating that trend. Palo Alto Networks has been aggressively acquiring strategic technologies to enable a cloud-delivered future. For example, the vendor's recent acquisition of CloudGenix for SD-WAN is an onramp to its Prisma Access.

Cloud-delivered Prisma Access is the vendor's ZTNA solution, which enables secure work-from-home connectivity for many during the pandemic. With its combination of NGFWs, Cortex, Strata, and Prisma Access platforms, Palo Alto Networks is aiming to own not just the enterprise firewall market, but the cloud-security stack market of the future.

Palo Alto Networks' next-generation firewalls have unique capabilities like recording PCAPs of the transmissions of suspected malware, and the ability to provide MFA for legacy applications that don't support it. Palo Alto Networks is also one of the few firewall vendors with a container security solution that integrates with the firewall's cloud management console. Palo Alto Networks' Demisto acquisition demonstrates dedication to incident response automation. Firewall administrators in years past gushed how easy Palo Alto Networks was to use, but the company may be slipping in its customer experience journey. One reference customer felt neglected, saying, "I love the product, but I struggle with the relationship." Enterprise security buyers with a preference for a single solution vendor should look to Palo Alto Networks to enable their SOC staff and security program.

› **Cisco has all the security you can eat and more.** Cisco's security business is growing (6% YoY).[2] The vendor's acquisitions of SourceFire, OpenDNS, and Duo integrate well into its enterprise firewall and associated services. The vendor's Umbrella platform maps to a Zero Trust edge approach and incorporates major security services, like firewalls and CASBs, that can be cloud-delivered. Cisco is the gold standard for online technical documentation, certification, and is a member of numerous standards bodies. Cisco has at least three firewalls, Meraki, ASA, and the one being evaluated in this report, Firepower Threat Defense (FTD).

FTD has tie-ins with endpoint (through Cisco AMP) and microsegmentation (through a Cisco Tetration module). FTD has a unique capability to identify user and application traffic via custom Lua scripts, and PCAPs can be loaded and tested against them. In the past, buyers worried about integration and if the pieces would "talk" to each other properly. A customer reference for this report was initially similarly skeptical, but said, "They won me over. Cisco has really fixed their problems and done their own testing." Multiple reference customers expressed that the vendor needs to improve FTD's usability, and value for price was cited as a weakness as well. Very large enterprise buyers with an existing Cisco ecosystem, distributed campuses, thousands of workers, and a diverse set of requirements should consider Cisco's Firepower Threat Defense firewall and Umbrella platform.

Strong Performers

› **Check Point Software Technologies' security is broad and deep.** The oldest and largest security company in Israel, Check Point has long been the standard bearer to which other firewall vendors have compared themselves for centralized management and usability. Today, the company's tagline is "Secure Your Everything," and the vendor is embarking on a strategy to help customers do just that. Check Point acquired Dome9 for cloud guardrails, Protego for workload security, and Cymplify for an ambitious IoT security strategy. Check Point has a well-publicized threat intelligence team and a global incident response service that fights nation-state battles.

Check Point's NGFW has an intuitive and pleasing aesthetic. One reference customer concurred, saying, "I really love the UI for managing the whole network. The SmartConsole makes it so easy." Check Point's cloud workload protection, endpoint protection, and centralized management are solid. The vendor's integration to many SIEM and SOAR solutions enable security operations. Check Point's strategic weakness is its hands-off approach to SD-WAN. It's the last of the big firewall vendors that explicitly rely on an SD-WAN partner vendor like SilverPeak or Velocloud (part of VMware), yet SD-WAN is a strategic point of control for vendors looking to boost customers into their Zero Trust edge networks and security services in the cloud. Large enterprises with many high-security requirements that are happy with their current SD-WAN vendor, and manufacturers with IP-based ICS/SCADA networks should look to Check Point.

› **Fortinet focuses on performance.** Fortinet's first product was the FortiGate firewall. After a public offering in 2009 (Nasdaq: FTNT), Fortinet grew its business greatly by building its product portfolio into a fabric of adjacent networking and security technologies with the flagship enterprise firewall at the center. Today, the vendor offers secure wireless, secure WLAN, 3G/4G/5G connectivity, application security, SIEM, SOAR, and secure email gateway solutions. Fortinet firewalls are deployed where high performance matters — in data centers, colos, and telco networks around the world.

  More than other firewall vendors, Fortinet invests in custom silicon to accelerate network and security policy. But this reliance on hardware is a double-edged sword. Fortinet has a strong combination of firewall, SD-WAN, and routing, but the vendor is behind in offering its own hosted cloud security services, including firewall-as-a-service and ZTNA. One reference customer said, "We chose them because they were more bang for the buck. Also, they had a lot more flexibility than other vendors." Security pros looking for on-premises appliances with a focus on performance and should consider Fortinet's FortiGate firewall.

› **Forcepoint focuses on human-centric cybersecurity.** Initially a fusion of WebSense's web filter, the Stonesoft NGFW, and a CASB acquired from Imperva, Forcepoint looked well-integrated. Forcepoint is majority-owned by major defense contractor Raytheon Technologies. Wisely choosing the tagline "Human-centric Cybersecurity" instead of something defense-related like "military-grade" security, the vendor aspires to be an enterprise vendor. Given its heritage with federal agencies, Forcepoint's NGFW has more robust data security features than its enterprise market competitors.

  With its endpoint agent, for example, Forcepoint can detect when an insider is attempting to access critical data, increase the user's risk score at the firewall, and then capture video of the user's activities after. Forcepoint engineered multitenancy into its cloud-based centralized management, added clustering up to 16 devices, and added zero-touch SD-WAN deployment into its most recent releases. Forcepoint lacks the robust solutions for IoT/OT, workload protection and microsegmentation that some of its more established competitors feature. Reference customers cited the vendor's IDS/IPS as needing improvement. Federal agencies may already be familiar with Forcepoint, but high-security enterprise buyers looking for integrated data security should evaluate Forcepoint.

› **Sophos surprises with innovative, unique features.** Founded in Oxford in 1985, Sophos is headquartered in the UK, with a heavy presence in EMEA. Sophos has long been well-respected for its research arm, SophosLabs. With intuitive interfaces, tactical features, and its long presence in EMEA, Sophos XG firewall will continue to flourish there and in markets where the vendor can provide a value-oriented, tactical, next-generation firewall or even a hardware-based UTM for the really conventional buyer.

The Sophos endpoint client enables the XG firewall to automatically isolate an infected host from its peers. Customer references indicate they chose the XG firewall specifically for this feature, as it enabled remote threat mitigation. Sophos also has an ultra-thin SD-WAN that performs hardware split tunneling for use by corporate execs or ultra-small offices. Interestingly, the vendor offers centralized management for free. Like the other firewall vendors that straddle the line between SMB and enterprise, Sophos lacks a global vendor network from which to deliver rich cloud security services like CASB and ZTNA. For the on-premises enterprise market, Sophos will need to add custom hardware offloads if it wants to jump to the 10G/40G feeds common there. In the meantime, small to medium buyers, especially those in the services, government, and manufacturing verticals, should put Sophos XG on their shortlist.

› **Juniper Network's Connected Security strategy is connecting with customers.** Juniper is an engineering-driven company with a long history of supporting telco vendors where they made ultra-fast routers for the infrastructure business. In 2004, Juniper acquired the NetScreen firewall, which became SRX. After going quiet in the security market since 2016, Juniper is roaring back, with a focus on the enterprise market. Juniper has compelling, well-executed security components that play to its infrastructure strengths, but its overall short-term strategy must include catching up to larger, more-established competitors, while outpacing smaller vendors.

One of Juniper's most unique features is the Policy Enforcer. The SRX firewall uses it to push security policy decisions to other parts of the network — its MX routers for faster blocking or Carbon Black endpoints for host isolation. Juniper is also one of a few firewall vendors to apply machine learning to encrypted traffic to augment malicious behavior detection. Customer references specifically praised Juniper's performance with threat prevention enabled. SRX uses the Juniper ATP Cloud sandbox in the cloud, where the vendor is building its Zero Trust edge vendor network. However, the vendor has catching up to do in the cloud. It lacks its own CASB and ZTNA, both of which will become crucial, must-have features in the next three years. Enterprise buyers looking for excellent performance and solid integration with existing Juniper routers and security vendors like Carbon Black and NetSkope can get Connected Security from Juniper's SRX.

› **Huawei leads the China market.** Founded in China by Ren Zhengfei in 1987, Huawei has always been a telecommunications equipment company, but is branching into other technology areas, including security. Today, the Asian conglomerate boasts annual revenues exceeding $100 billion.[3] Huawei has global services and support in seven countries. Mexico serves as the support center for North America. The vendor's vision for network security in the future closely aligns to those

of other firewall vendors in bridging the gap between on-premises and their own cloud security services. Huawei has some vendor network services, currently offering firewall-as-a-service (but for SMB) and SD-WAN initialization from the cloud. The vendor lacks ZTNA and CASB, two services that will be critical cloud features for a Zero Trust Edge network.

Huawei refers to its USG series as the world's first AI firewall, and it is one of only a handful of vendors in this analysis to apply ML to encrypted traffic analysis. It's little surprise that Huawei's USG firewall strategy has advanced 5G support earlier than other vendors. Reference customers were unanimous in their praise for both the value provided and the total cost of ownership of the USG firewall series, and all would recommend it to a colleague. Chinese buyers looking for an enterprise firewall should evaluate Huawei. Geopolitical concerns, however, may influence the selection and deployment of Huawei equipment in many Western countries.

Contenders

› **Barracuda Networks punches above its weight.** Recently taken private by Thoma Bravo, Barracuda's new management does brisk business in EMEA and the turbulent APAC market. Barracuda identified key recent technological trends in the firewall market and executed on them. The vendor was among the first firewall vendors to spot the significance of SD-WAN and cloud integration for the firewall market, and it has a strong play for IoT/ICS/OT environments. Barracuda's CloudGen firewall is an excellent on-ramp to Azure and, someday, AWS.

Barracuda is heavily invested in the Microsoft ecosystem. It was the first firewall to achieve Microsoft Azure certification and is ahead of competitors in Azure integration for both security and virtual WAN. Barracuda is the only firewall vendor building a DIY security-stack-in-the-public cloud, which is bold. Barracuda's on-premises firewalls are a good fit for the OT environments in which they actively compete, but the vendor lacks generalized firewall-as-a-service, CASB, and Zero Trust Network Access. Midmarket buyers and those interested in building a DIY security stack in the cloud should consider Barracuda.

› **WatchGuard excels in distributed deployments.** WatchGuard is one of the original firewall companies and remains independent in the market. After a long crusade during the small-market unified threat management (UTM) wars, WatchGuard's vision now is to bring enterprise-grade firewall capabilities to the midmarket. In June, WatchGuard closed the acquisition of Panda Security to add endpoint protection to its portfolio.[4] While many of the features in the WatchGuard Firebox come from those UTM days, they translate decently to the firewall market.

Today, customers use WatchGuard as a template for distributed environments, where a small to medium-size firewall needs to be replicated reliably. WatchGuard's cloud-based RapidDeploy and WatchGuard Cloud management options help create and manage firewall policy for these distributed environments (such as retail outlets, manufacturing locations, and healthcare facilities). Reference customers cited the flexibility that WatchGuard provides for integration with best-of-breed antivirus solutions as a strength, and specifically praised the Firebox's "extremely low failure

rate." The Firebox does lack many advanced features like workload protection, microsegmentation integration, and firewall-as-a-service. Security pros looking to deploy and manage thousands of small firewalls in dispersed physical locations can build and repeat a great template with the WatchGuard Firebox.

› **SonicWall reemerges as a standalone firewall vendor.** In 2012, SonicWall became a Dell subsidiary. The vendor detached, with the help of private equity, in 2016 and now stands as standalone firewall vendor. SonicWall recognizes that the future will see the proliferation of cloud-hosted security services, but the vendor has a lot catching up to do to get there.

SonicWall's on-premises firewall product series is sold with a basic feature set — policy creation, malware analysis, and SD-WAN for free. The vendor still needs to invest in critical technologies that are needed by enterprises now — SOAR integration for incident response, firewall as a service, and cloud security extensions. Reference customers reported dissatisfaction with its reporting and analytics. But SonicWall does have its fans. A customer reference commented that SonicWall, as a company, "Helps me out when I need them, even with sales and pricing." SMB and education buyers should evaluate SonicWall from a value perspective. Enterprise architects looking for a properly sized tactical solution to stamp out for hundreds of retail outlets should evaluate SonicWall.

Evaluation Overview

We evaluated vendors against 34 criteria, which we grouped into three high-level categories:

› **Current offering.** Each vendor's position on the vertical axis of the Forrester Wave graphic indicates the strength of its current offering. Our evaluation of each vendor's current offering covered the breadth of each solution as it related to integration with adjacent security functionality (like workload security or microsegmentation), the ability of each solution to assist incident response (host isolation), usability, manageability, and performance.

› **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. We evaluated each vendor's strategic vision and roadmap as it aligned to a Zero Trust edge architecture, where many security functions are delivered from a secure edge and both on-premises and remote users have the ability to access enterprise resources with Zero Trust rather than user-to-site VPN. For vendors not (yet) aligning to the Zero Trust edge architecture, we evaluated their roadmap as it aligned to their own stated strategy and feedback we've heard from Forrester clients.

› **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's enterprise firewall revenue and number of enterprise customers (with 5000 or more employees).

Vendor Inclusion Criteria

Forrester included 11 vendors in the assessment: Barracuda Networks, Check Point Software Technologies, Cisco Systems, Forcepoint, Fortinet, Huawei Technologies, Palo Alto Networks, Sophos, SonicWall and WatchGuard. Each of these vendors has:

- **An on-premises, content-aware network firewall appliance.** We included vendors with on-premises appliances as these are still the most common north-south perimeter defenses. The solution had to feature both integrated IDS/IPS and automated malware analysis components, both of which are often required by Forrester clients. We did not include solutions that were primarily software based, existed within the control plane of a hypervisor, or were primarily cloud- or edge-hosted at this time.
- **A global presence.** Each vendor included in this report had to sustain at least 20% of its firewall revenue outside its primary region. This requirement had the effect of excluding three vendors, Hillstone, H3C, and QiAnXin, who do nearly 100% of their business in AP.
- **Significant enterprise firewall revenue.** In order to compare the most significant of these vendors, we stipulated that those vendors with a global presence must also show at least $75 million in firewall revenue.

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

To help you put research into practice, connect with an analyst to discuss your questions in a 30-minute phone session — or opt for a response via email.

Learn more.

Analyst Advisory

Translate research into action by working with an analyst on a specific engagement in the form of custom strategy sessions, workshops, or speeches.

Learn more.

Webinar

Join our online sessions on the latest research affecting your business. Each call includes analyst Q&A and slides and is available on-demand.

Learn more.

Forrester's research apps for iOS and Android.
Stay ahead of your competition no matter where you are.

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 Guide 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 April 24, 2020 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 The Forrester Wave™ 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 The Forrester Wave™ And The Forrester New Wave™ Nonparticipating And Incomplete Participation Vendor 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.

Endnotes

[1] Base: 1,606 to 1,755 global purchase influencers (past 12 months/next 12 months) who responded during the COVID-19 pandemic; 1,606 of them have had their organizations transition to full-time remote work as a result of the pandemic. Source: Forrester Analytics Business Technographics® Priorities And Journey COVID-19 Recontact Survey, 2020.

[2] Source: "Cisco Reports Third Quarter FY20 Earnings," Cisco press release, May 13, 2020 (https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=2074002).

[3] Source: Dan Strumpf, "Huawei's Revenue Hits Record $122 Billion in 2019 Despite U.S. Campaign," The Wall Street Journal, December 30, 2019 (https://www.wsj.com/articles/huaweis-revenue-hits-record-122-billion-in-2019-despite-u-s-campaign-11577754021).

[4] Panda Security is an endpoint protection software provider based in Madrid and Bilbao, Spain.

We work with business and technology leaders to drive customer-obsessed vision, strategy, and execution that accelerate growth.

PRODUCTS AND SERVICES

- Research and tools
- Analyst engagement
- Data and analytics
- Peer collaboration
- Consulting
- Events
- Certification programs

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.