The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers, Q4 2018

Tools And Technology: The Security Architecture And Operations Playbook

by Chase Cunningham
November 8, 2018

Why Read This Report

In our 15-criterion evaluation of Zero Trust eXtended ecosystem providers, we identified the 14 most significant ones — Akamai Technologies, Centrify, Cisco, Cyxtera Technologies, Forcepoint, Fortinet, Illumio, Microsoft, Okta, Palo Alto Networks, Sophos, Symantec, Trend Micro, and VMware — and researched, analyzed, and scored them. This report shows how each provider measures up and helps security professionals make the right choice.

Key Takeaways

Palo Alto Networks And Symantec Lead The Pack

Forrester's research uncovered a market in which Palo Alto Networks and Symantec are Leaders; Okta, Cisco, Centrify, Illumio, Forcepoint, Cyxtera, Microsoft, and Akamai are Strong Performers; Trend Micro, and VMware are Contenders; and Sophos and Fortinet are Challengers.

Security Pros Want A Strategic Partner For Zero Trust

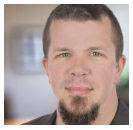
This market is growing because more security leaders see Zero Trust as a way to address their top challenges. Growth is in large part due to security pros increasingly relying on vendors to act as both technical integrator and long-term partner for planning and actualizing the architectural recommendations of the Zero Trust eXtended ecosystem framework.

Zero Trust Framework Alignment And Securing Access Are Key Differentiators

Historically, security pros relied on next-generation firewalls and other legacy access technology to enforce Zero Trust microperimeters. Today, there is a variety of adaptive software-based approaches that can accomplish this while more fully integrating the components and capabilities of the extended ecosystem framework. Vendors that clearly align their future vision and road maps to Zero Trust will create differentiation.

The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers, Q4 2018

Tools And Technology: The Security Architecture And Operations Playbook



by Chase Cunningham
with Stephanie Balaouras, Robert Perdoni, and Peggy Dostie
November 8, 2018

Table Of Contents

Related Research Documents

The Eight Business And Security Benefits Of Zero Trust

Five Steps To A Zero Trust Network

The Forrester Tech Tide™: Zero Trust Threat Prevention, Q3 2018

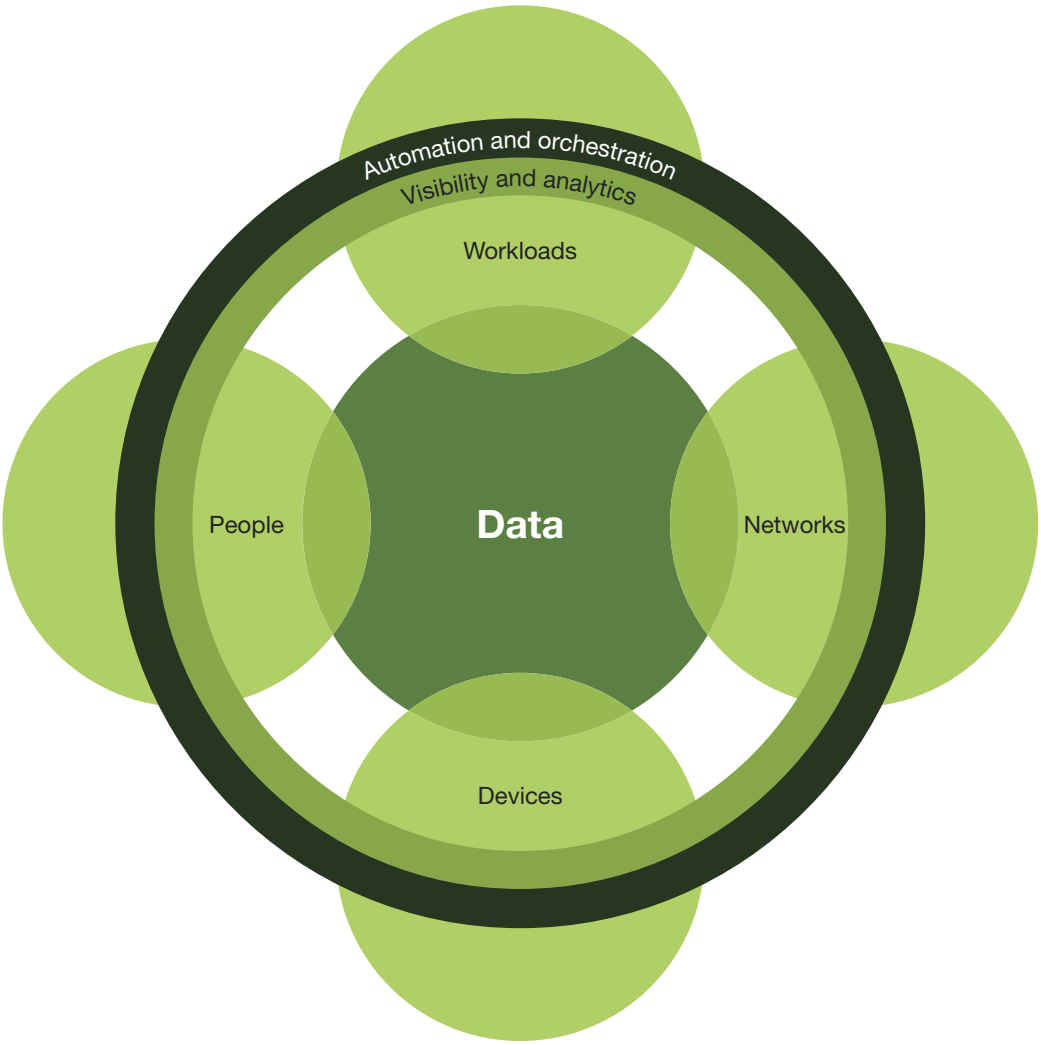
FORRESTER®

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

Zero Trust Is More Than A Concept; It's A Concrete Framework

Forrester introduced Zero Trust nearly a decade ago, and, initially, it was a concept focused on: 1) segmenting and securing the network across locations and hosting models and 2) preaching the Zero Trust gospel — the need to challenge and eliminate the inherent trust assumptions in our security strategies that made us vulnerable to external and internal attacks. This etched Zero Trust into the collective lexicon of an industry. The concept of Zero Trust and its benefits have evolved significantly, however. Zero Trust is now a strategic initiative that we have combined with a focused framework to allow decision makers and security leaders to move toward pragmatic implementations (see Figure 1).

FIGURE 1 The Zero Trust eXtended Ecosystem Framework



Zero Trust Is Going Mainstream

The entire security industry is talking about Zero Trust, and numerous vendors have embraced it and now use it to market and position their capabilities as well as guide their future road maps; the time to formalize the evaluation criteria for vendors in this space is now. This Forrester Wave™ helps security professionals identify which vendors have internalized and most closely aligned to Forrester's Zero Trust eXtended (ZTX) framework. This evaluation also shows how each vendor's portfolio maps and delivers on specific components of the ZTX framework, so that security professionals understand which combination of vendors can best assist them on their Zero Trust journey.

Zero Trust eXtended Ecosystem Providers Evaluation Overview

To assess the state of the Zero Trust eXtended ecosystem providers market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of top Zero Trust eXtended ecosystem vendors. After examining past research, user need assessments, and vendor and expert interviews, we developed a comprehensive set of 15 evaluation criteria, which we grouped into three high-level buckets:

- **Current offering.** Each vendor's position on the vertical axis of the Forrester Wave graphic indicates the strength of the vendor's current offering. Key criteria for these solutions include all seven of the ZTX ecosystem pillars: network security, data security, workload security, workforce security, device security, visibility and analytics, automation and orchestration, as well as manageability and usability and API usage.
- **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. We evaluated vendors' product visions as applied specifically in a Zero Trust-focused organization, planned enhancements to better enable Zero Trust strategies, and their go-to-market approach for Zero Trust strategically aligned organizations.
- **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's enterprise install base and number of enterprise customers.

Evaluated Vendors And Inclusion Criteria

Forrester included 14 vendors in the assessment: Akamai, Centrify, Cisco, Cyxtera, Forcepoint, Fortinet, Illumio, Microsoft, Okta, Palo Alto Networks, Sophos, Symantec, Trend Micro, and VMware (see Figure 2). Each of these vendors has:

- **Notable revenues.** Vendors must have at least $75 million in annual revenues.
- **ZTX technical capabilities.** Vendors must have capabilities in at least three of the seven ZTX components: 1) network security; 2) device security; 3) people/identity security; 4) workload/application security; 5) data security; 6) security visibility and analytics; and 7) security automation and orchestration.

- **ZTX alignment.** Vendors must be strategically aligned with the ZTX framework and overall Zero Trust concepts
- **APIs for integration.** Vendors must have a defined and documented API layer — with a healthy number of partners integrating with the vendor's API.
- **Forrester mindshare.** Forrester clients regularly list this vendor as one they shortlist for ZTX components.

FIGURE 2 Evaluated Vendors And Product Information

Vendor name	Product evaluated
Akamai Technologies	Enterprise Application Access, Enterprise Threat Protector, Kona Site Defender, Bot Manager, Web App Protector, Ion, Dynamic Site Accelerator
Centrify	Next-Gen Access Platform
Cisco	Cisco Trusted Access Portfolio
Cyxtera Technologies	AppGate SDP
Forcepoint	Dynamic Data Protection
Fortinet	Fortinet Security Fabric
Illumio	Illumio Adaptive Security Platform (ASP)
Microsoft	Azure Active Directory Conditional Access, Microsoft 365, Windows Defender ATP, Office 365 ATP, Azure ATP, Microsoft Intune, Microsoft Cloud App Security
Okta	Okta Identity Cloud
Palo Alto Networks	(Network) PAN-OS 8.1, Panorama (cloud-delivered) GlobalProtect Cloud Services, Magnifier (cloud security) VM-Series, Aperture, Evident (endpoint) Traps
Sophos	Zero Threat framework technologies include Sophos Central, Sophos Endpoint Protection, Intercept X, Sophos Mobile, SafeGuard Encryption, Intercept X for Server, XG Firewall, SG UTM, Sophos Secure Wi-Fi, Sophos Secure Web Gateway, Sophos Secure Email Gateway, Phish Threat
Symantec	Symantec Integrated Cyber Defense (ICD)
Trend Micro	Network Defense, Hybrid Cloud Security, User Protection (Endpoint, EDR, Email, Web, Cloud App Security)
VMware	vSphere, Workspace ONE, vRealize Automation, vRealize Network Insight, NSX, AppDefense

Vendor Profiles

We intend this evaluation of the Zero Trust eXtended ecosystem providers market to be a starting point only and encourage clients to view detailed product evaluations and adapt criteria weightings to fit their individual needs through the Forrester Wave Excel-based vendor comparison tool (see Figure 3 and see Figure 4). Click the link at the beginning of this report on Forrester.com to download the tool.

FIGURE 3 Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers, Q4 2018

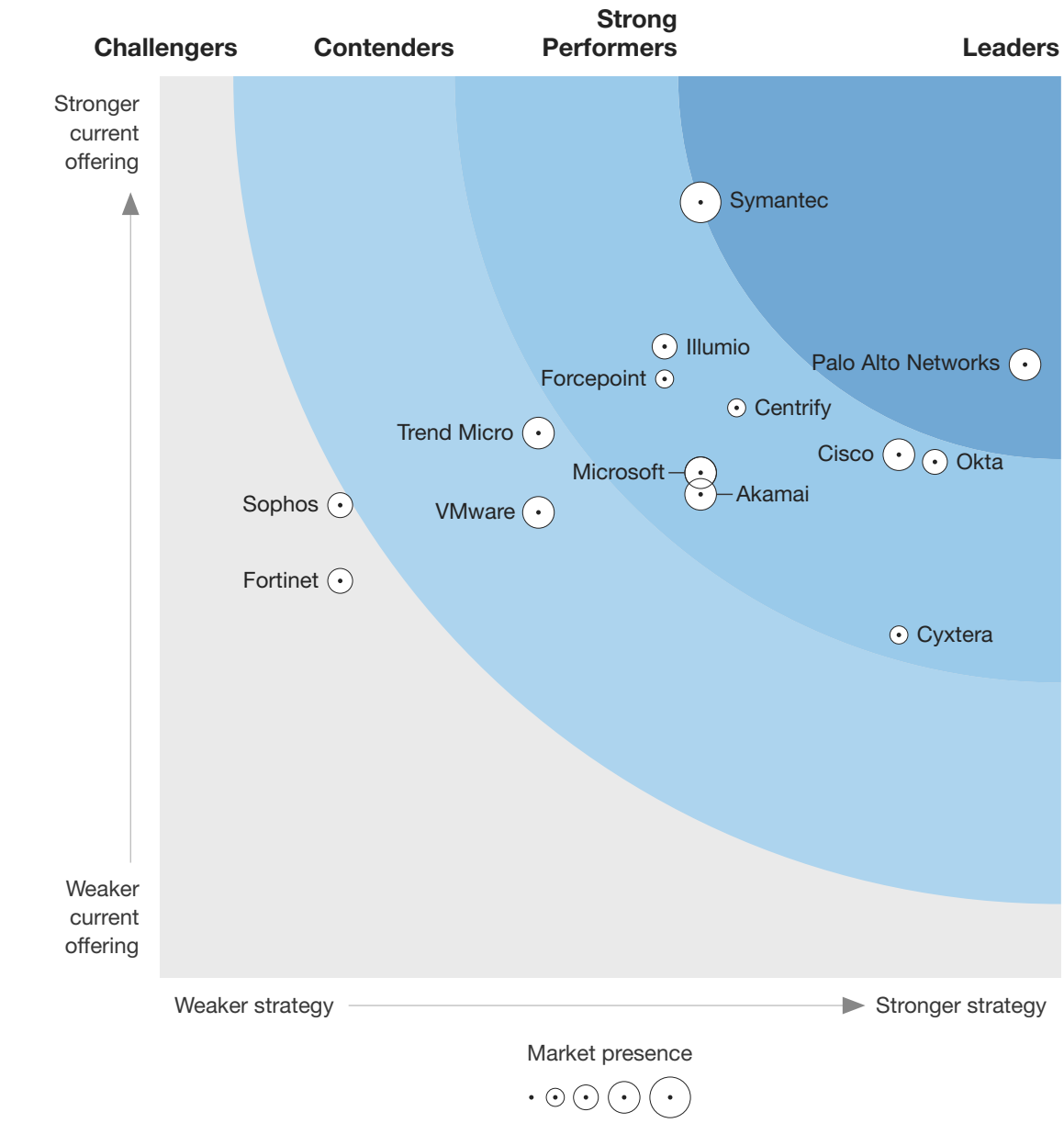


FIGURE 4 Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers Scorecard, Q4 2018

	Forrester's weighting	Akamai	Centrify	Cisco	Cyxtera	Forcepoint	Fortinet	Illumio
Current offering	50%	2.68	3.16	2.90	1.90	3.32	2.20	3.50
Network security	10%	5.00	3.00	5.00	3.00	3.00	5.00	3.00
Data security	21%	1.00	1.00	3.00	1.00	5.00	1.00	3.00
Workload security	10%	5.00	5.00	3.00	5.00	3.00	3.00	5.00
People/workforce security	19%	3.00	5.00	3.00	1.00	3.00	1.00	3.00
Device security	15%	1.00	3.00	3.00	1.00	3.00	3.00	3.00
Visibility and analytics	5%	3.00	3.00	3.00	3.00	3.00	3.00	5.00
Automation and orchestration	5%	3.00	3.00	3.00	3.00	3.00	3.00	5.00
Manageability and usability	10%	3.00	3.00	1.00	1.00	3.00	1.00	5.00
APIs	5%	3.00	3.00	1.00	3.00	1.00	3.00	1.00
Strategy	50%	3.00	3.20	4.10	4.10	2.80	1.00	2.80
ZTX vision and strategy	55%	3.00	3.00	5.00	5.00	3.00	1.00	3.00
ZTX road map and differentiation	35%	3.00	3.00	3.00	3.00	3.00	1.00	3.00
Market approach	10%	3.00	5.00	3.00	3.00	1.00	1.00	1.00
Market presence	0%	3.70	2.00	3.70	1.30	2.00	3.00	2.30
Install base	35%	5.00	3.00	5.00	1.00	3.00	3.00	3.00
Percentage investing in portfolio	50%	3.00	1.00	3.00	1.00	1.00	3.00	1.00
Portfolio growth rate	15%	3.00	3.00	3.00	3.00	3.00	3.00	5.00

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

FIGURE 4 Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers Scorecard, Q4 2018 (Cont.)

	Forrester's weighting	Microsoft	Okta	Palo Alto Networks	Sophos	Symantec	Trend Micro	VMware
Current offering	50%	2.80	2.86	3.40	2.62	4.30	3.02	2.58
Network security	10%	3.00	3.00	5.00	3.00	5.00	3.00	3.00
Data security	21%	3.00	1.00	3.00	3.00	5.00	3.00	1.00
Workload security	10%	5.00	3.00	5.00	3.00	3.00	5.00	3.00
People/workforce security	19%	3.00	5.00	3.00	1.00	5.00	1.00	3.00
Device security	15%	3.00	3.00	3.00	3.00	5.00	5.00	3.00
Visibility and analytics	5%	1.00	3.00	3.00	3.00	3.00	3.00	3.00
Automation and orchestration	5%	3.00	3.00	3.00	3.00	3.00	3.00	3.00
Manageability and usability	10%	1.00	3.00	3.00	3.00	3.00	3.00	3.00
APIs	5%	1.00	1.00	3.00	3.00	3.00	1.00	3.00
Strategy	50%	3.00	4.30	4.80	1.00	3.00	2.10	2.10
ZTX vision and strategy	55%	3.00	5.00	5.00	1.00	3.00	3.00	3.00
ZTX road map and differentiation	35%	3.00	3.00	5.00	1.00	3.00	1.00	1.00
Market approach	10%	3.00	5.00	3.00	1.00	3.00	1.00	1.00
Market presence	0%	4.00	3.00	4.00	3.00	4.70	3.70	4.00
Install base	35%	5.00	3.00	5.00	3.00	5.00	5.00	5.00
Percentage investing in portfolio	50%	3.00	3.00	3.00	3.00	5.00	3.00	3.00
Portfolio growth rate	15%	5.00	3.00	5.00	3.00	3.00	3.00	5.00

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

Leaders

› **Palo Alto Networks.** Palo Alto Networks was unparalleled in the Zero Trust movement for a few years and continues to understand the reasons for using Zero Trust technologies and the technical steps needed to enable Zero Trust for enterprises. The company has acquired and integrated tooling from organizations that have strong cloud capabilities (Evident.io and RedLock), user analytics (Magnifier [Lightcyber]), and endpoint security (Traps), all while ensuring that customers

are engaged in both strategic alignment and optimal tool use. Oddly, while the technology stack directly speaks to the benefits of Zero Trust, Palo Alto's messaging and marketing have not focused on Zero Trust (even after the company hired the Forrester analyst who developed it).

› **Symantec.** Symantec is a juggernaut, given its breadth of security solutions. The company has extensive endpoint, network security, and threat identification capabilities. Zero Trust is somewhat new to Symantec, and the company is quickly ramping up its strategic alignment to the broader ZTX framework, and it certainly understands how it plays in this industry initiative. Customers we interviewed spoke very highly of the broad capabilities of Symantec for endpoint and network security, but the data security tool sets were noted as for administrators.

Strong Performers

› **Okta.** Okta is skilled at securing end users and their ability to access the network, which is a key factor for all Zero Trust strategies and organizations. The company has spent significant time and resources to enable easy security for end users and enterprises, and thanks to its exceptional growth and expansion, it has a strong install base that are "in love" with the solution. End users noted the system's easy rollout and manageability as well as the company's focus on alignment with the broader strategic needs of organizations that are on a Zero Trust journey. Okta also has invested heavily in growing its Zero Trust network and other ZTX capabilities by acquiring ScaleFT in the latter part of 2018.

› **Cisco.** The Cisco name is well known in the security space, and its gravitas as a global entity in the network area has been established for decades. The company's return to enabling security operations more strategically has coincided with the explosion of Zero Trust, and Cisco is doing a good job of establishing its presence here. Interviewees typically noted the vendor's strong capability in network security and configuration but were also quick to note that legacy user interfaces and the spread of capabilities over such a vast functional expanse was at times confusing and hindering. Following the cutoff date for this report and therefore excluded from the scores, Cisco completed its acquisition of Duo Security to expand on the Cisco approach to Zero Trust. Duo enables customers to verify user and device trust to more securely control access to applications.

› **Centrify.** Centrify has been a noted proponent of Zero Trust in its marketing and messaging and has long been a leader in both privileged identity management (PIM) and identity-as-a-service) IDaaS. In mid-2018, Centrify announced that a private equity firm had acquired a majority interest in the company. Centrify has subsequently announced a spin-out of its IDaaS business, named Idaptive, to "better focus on customer outcomes." While this strategy is understandable and makes sense on both a business and technology standing, it will be incumbent on the firm to continue with its respective Zero Trust-focused offerings and innovations. References noted the integration of response and remediation tooling as a key capability for optimal security administration.

- **Illumio.** A key factor for any Zero Trust enterprise or strategy is to know what assets and controls are in place and to be able to understand, with context, what transactions and threats are critical to the business. In this regard, Illumio shines. The technology provided by the vendor aligns well with enabling the establishment of Zero Trust for an organization, and its ability to provide the contextual insight of threat areas and workflows for both security and continuity stand out in the space. Users were quick to note the vendor's strong capability in enabling microsegmentation on the fly combined with its focus on visualization and usability, all key points in any Zero Trust system.
- **Forcepoint.** Forcepoint is one of the few vendors in this Forrester Wave that has a strong background in the federal space, not surprising given that it is in fact an independent joint venture of Raytheon. The company has a strong focus on security user behavior analytics (SUBA) and data security and has even acquired a company, RedOwl Analytics, solely to enable this capability. Forcepoint sets a strong standard in analytics and data control when compared with the ZTX framework requirements. Interviewees noted the strength of the system in identifying potentially malicious actions based on user activity but also referenced the system's issues around ease of integration with other response tools and analytics sets.
- **Cyxtera Technologies.** Cyxtera is a new player to the Zero Trust market. It has a strong capability set for enabling cloud workload security and application isolation and security. This solution set is directly related to the ZTX workloads area, and Cyxtera excels in this regard. The company leans heavily on its marketing as a Zero Trust-focused vendor, but its overall role in the larger ZTX platform play remains to be seen. Users Forrester interviewed noted the strength of the solution set for cloud and apps but also noted its lack of capabilities in the people/workforce and specific data security areas.
- **Microsoft.** Microsoft is a giant in any technology space, but a new one to Zero Trust. Microsoft has vast resources at its disposal and controls its own massive cloud infrastructure, all while moving to enable better security for its O365 users. Microsoft has been noted as understanding the needs of Zero Trust enterprises and use cases, but the users we interviewed often referred to the vendor solution set as slow to roll out. They also noted that it could obtrusive, because end users that are "100% O365" will be the ones to gain the most from the system; this could be limiting for organizations that seek to operate with hybrid or legacy systems.
- **Akamai Technologies.** Akamai is a powerhouse in the network security space and has spent both time and resources in extending its capabilities into other areas of security for clients. This includes DDoS, botnet mitigation, malware protection, and application microsegmentation capabilities. The vendor has a well-established global customer base across multiple verticals and a broad partner ecosystem. Akamai security solutions are delivered as SaaS and provide a wide range of configuration options. Akamai's understanding of the importance of Zero Trust is clearly evident, and it has begun recently to sponsor Zero Trust-related research to promote its space in the arena. Customers reported some issues with ease of deployment and integration with other common tool sets for security administration.

Contenders

› **Trend Micro.** Trend Micro has strong antimalware and endpoint security, cloud workload security, as well as significant capability in the network security pillar of ZTX. The systems' interoperability aided users most directly if they were willing to buy in completely to Trend Micro's offering. The network tooling's ability to provide insight into encrypted traffic streams is also of note for those organizations struggling to gain insight into dark corners of a network. Forrester thinks that Trend Micro understands Zero Trust even though it hasn't led any appreciable research, and its tailored focus on enabling Zero Trust strategically remains to be seen.

› **VMware.** Obviously an extremely capable player in virtualization and the use of virtual resources, VMware also fares well in the security space. The company has done a good job recently in enabling more-diverse security controls, but interviewees often noted the hindrances of deployment for NSX at larger enterprise levels and referenced the system's less-than-optimal user interfaces for security management across the pillars of ZTX. VMware is moving toward a more focused enablement for Zero Trust as the industry embraces the concept. With its broad user base and powerful virtualization tool sets, VMware has exceptional potential to be a leader in Zero Trust.

Challengers

› **Sophos.** Sophos has evolved into a modern next-generation leader that, through the release of its Intercept X endpoint and XG firewall product ranges, has seen the growth of unified threat management in cybersecurity and has positioned itself to gain its share of the ground within this growing market segment. Sophos possesses strong capabilities in endpoint security and also plays well in the people/workforce pillar of ZTX, as it offers email security and phishing training. However, end user interviewees noted that the system seemed disjointed at times when considered as a true "single platform" and noted the limitations across the broader scope of strategic security focuses such as Zero Trust. Sophos also is one of the few security vendors in this Forrester Wave that has specific security around wireless/Wi-Fi, which is important for branch offices and the mobile workforces of today. Its specific alignment with current and future Zero Trust and ZTX initiatives is improving. Sophos positions its Synchronized Security and other strategic initiatives to encompass ZTX, but at the time of this evaluation, it's still evolving compared with competitors with a more focused alignment.

› **Fortinet.** Fortinet is a legacy network security vendor noted for its ability to enforce security controls at the network layer without impacting the broader network throughput. The vendor has begun to scratch at the broader components of the ZTX extended ecosystem, but its strength for now remains almost entirely at the network pillar. End users typically noted the tools' singular focus in network security as "extremely useful but limited in scope."

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

The online version of Figure 3 is an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings. Click the link at the beginning of this report on Forrester.com to download the tool.

Data Sources Used In This Forrester Wave

Forrester used a combination of three data sources to assess the strengths and weaknesses of each solution. We evaluated the vendors participating in this Forrester Wave, in part, using materials that they provided to us by September 23, 2018.

- **Vendor surveys.** Forrester surveyed vendors on their capabilities as they relate to the evaluation criteria. Once we analyzed the completed vendor surveys, we conducted vendor calls where necessary to gather details of vendor qualifications.

- **Product demos.** We asked vendors to conduct demonstrations of their products' functionality. We used findings from these product demos to validate details of each vendor's product capabilities.
- **Customer reference calls.** To validate product and vendor qualifications, Forrester also conducted reference calls with three of each vendor's current customers.

The Forrester Wave Methodology

We conduct primary research to develop a list of vendors that meet our criteria for evaluation in this market. From that initial pool of vendors, we narrow our final list. We choose these vendors based on: 1) product fit; 2) customer success; and 3) Forrester client demand. We eliminate vendors that have limited customer references and products that don't fit the scope of our evaluation. Vendors marked as incomplete participants met our defined inclusion criteria but declined to participate or contributed only partially to the evaluation.

After examining past research, user need assessments, and vendor and expert interviews, we develop the initial evaluation criteria. To evaluate the vendors and their products against our set of criteria, we gather details of product qualifications through a combination of lab evaluations, questionnaires, demos, and/or discussions with client references. We send evaluations to the vendors for their review, and we adjust the evaluations to provide the most accurate view of vendor offerings and strategies.

We set default weightings to reflect our analysis of the needs of large user companies — and/or other scenarios as outlined in the Forrester Wave evaluation — and then score the vendors based on a clearly defined scale. We intend these default weightings to serve only as a starting point and encourage readers to adapt the weightings to fit their individual needs through the Excel-based tool. The final scores generate the graphical depiction of the market based on current offering, strategy, and market presence. Forrester intends to update vendor evaluations regularly as product capabilities and vendor strategies evolve. Vendors marked as incomplete participants met our defined inclusion criteria but declined to participate in or contributed only partially to the evaluation. For more information on the methodology that every Forrester Wave follows, please visit The Forrester Wave™ Methodology Guide on our website.

Integrity Policy

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

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

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.

141666