Building Zero Trust Security with Visibility and Segmentation

FEATURING RESEARCH FROM FORRESTER

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

Illumio has been named a leader in The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q4 2019 report, receiving the highest overall ranking in the current offering category and the highest scores possible in the workload security, visibility and analytics, automation and orchestration, manageability and usability, APIs, vision and strategy, and advocacy criteria.

TAKING SECURITY BEYOND THE PERIMETER

"Never trust, always verify." This Zero Trust philosophy-turned-strategy fundamentally changes the way we approach security since trust is a vulnerability that can be exploited. Gone are the days of focusing on perimeter-based security and legacy firewalls to prevent breaches. The growing complexity of dynamic workloads moving across data center and multi-cloud environments, combined with an influx of new vulnerabilities and risks from hackers and targeted threats such as ransomware and malware outbreaks, have exposed the inadequacy of traditional security models.

The shift from assuming internal traffic within the network is trusted to eliminating automatic access for any source – internal or external – is now necessary to protect our increasingly heterogeneous infrastructure environments.

So how should you go about building a Zero Trust strategy? Forrester's Zero Trust eXtended (ZTX) framework helps organizations understand the pillars (or focus areas) where Zero Trust principles must be applied in the enterprise ecosystem, including workload/application security, network security, people/workforce security, data security, device security, automation and orchestration, and visibility and analytics.

Applying Zero Trust principles will give you greater visibility and a full understanding of your applications and their interdependencies, with granular control and automated whitelisting of all communications across workloads to reduce the attack surface and improve your security posture.

START YOUR ZERO TRUST JOURNEY WITH A MAP

The end goal is clear: eliminate all unauthorized access. But getting there is a journey. It involves technology, people, processes, and adoption. While every journey benefits from having a map to guide where you're going from the get-go, your Zero Trust strategy should be no different.

Gaining deep visibility into network flows, data, applications, users, and devices is a critical first step of Zero Trust. Using a map to gain a foundational understanding of all applications and their network connections is the key to success. The insights you gain from the map will help you break down organizational silos and engage business and IT stakeholders in designing Zero Trust policies.

IN THIS DOCUMENT

ZERO TRUST IS A TEAM SPORT

Zero Trust is built upon your existing ecosystem of solutions and products, and you must determine what other essentials are needed for your journey. API integration, heterogeneous support, and analytics are all critical capabilities to automate Zero Trust and make it easy to manage and deploy at scale.

SEGMENTATION IS KEY

Zero Trust is strategically focused on preventing lateral movement of attackers by enabling microsegmentation. Architecturally, Zero Trust mandates that you segment across environments in order to isolate threats and limit the impact of breaches. The understanding you gained from mapping helps you decide where and what to segment – and is necessary for effective segmentation design.

LEADING THE WAY WITH ILLUMIO ASP

The Illumio Adaptive Security Platform® (ASP) was built from the ground up to enable organizations to secure down to "microperimeters" around applications and maintain policy consistently across any data center and any cloud on bare-metal servers, virtual machines, and containers. By decoupling segmentation from your network and underlying infrastructure, Illumio provides a fast, safe, and effective approach to Zero Trust segmentation.

Illumio's host-based approach closely aligns with Zero Trust principles and Forrester's ZTX framework:

- Eliminating blind spots inside and across high-value systems with a real-time application dependency map that gives you visibility across all environments.
- Enabling the principles of network isolation, segmentation, and security by enforcing default-deny segmentation and granular policy design and testing.
- Securing your business-critical applications and workloads with granular policy control at massive scale and process-level enforcement.
- Ensuring people only have access to what they're entitled to through user-based segmentation and remote access control.
- Maximizing ease of use by allowing you to leverage existing investments to achieve Zero Trust through programming existing firewalls, switches, and load balancers to enforce segmentation.
- Automating and orchestrating security workflows such as incident response, remediation, and vulnerability management by integrating with leading security tools.

FORRESTER®

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

The 14 Providers That Matter Most And How They Stack Up

by Chase Cunningham
October 29, 2019

Why Read This Report

In our 16-criterion evaluation of Zero Trust eXtended (ZTX) ecosystem providers, we identified the 14 most significant ones — Akamai Technologies, Check Point, Cisco, Cyxtera Technologies, Forcepoint, Forescout, Google, Illumio, MobileIron, Okta, Palo Alto Networks, Proofpoint, Symantec, and Unisys — and researched, analyzed, and scored them, based on their mapping against Forrester's ZTX framework. This report shows how each provider measures up and helps security and risk (S&R) professionals make the right choice.

Key Takeaways

Cisco, Illumio, Palo Alto Networks, Akamai Technologies, And Okta Lead The Pack

Forrester's research uncovered a market in which Cisco, Illumio, Palo Alto Networks, Akamai Technologies, and Okta are Leaders; Cyxtera Technologies, MobileIron, Symantec, Unisys, Forcepoint, Google, Check Point, and Forescout are Strong Performers; and Proofpoint is a Contender.

Platforms Are Powerful

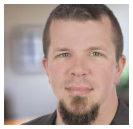
Until now, technology fragmentation has affected the ability of S&R leaders to really build a future-state of security. That's no longer the case. Organizations seeking to enable Zero Trust as a long-term goal can get real benefits from choosing a single vendor. Vendors that stand out in this still-evolving space offer integrated, real-world capabilities, not just marketing shenanigans.

Ease Of Use Matters — A Lot

The industry is aware of what's necessary to enable Zero Trust at the technical level, thanks to the formalization of ZTX. The difficulty of deploying and using these tools remains an issue for security pros and end users. Designing tools that take administrator and end user experience into account are critical capabilities for making ZTX successful.

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

The 14 Providers That Matter Most And How They Stack Up



by Chase Cunningham
with Joseph Blankenship, Matthew Flug, and Diane Lynch
October 29, 2019

Table Of Contents

Related Research Documents

Five Steps To A Zero Trust Network

The Zero Trust eXtended (ZTX) Ecosystem

Zero Trust For Compliance

Zero Trust Is A Journey, And Vendors Can Help You Get There

Forrester's Zero Trust framework is recognized as a preferred approach to cybersecurity. While Zero Trust doesn't refer to a specific technology, the application of several technologies enables it. This evaluation focuses on how each vendor's portfolio maps and delivers on specific components of ZTX to provide enterprise security professionals who are actively adopting or managing Zero Trust a clearer understanding of which vendors best align to help them on their Zero Trust journey. Security pros implementing technology to support Zero Trust should look for providers that:

- **Actively advocate for Zero Trust.** Due to the rapid adoption of Zero Trust and ZTX as security initiatives, Forrester has recognized a real need to more clearly align the message and importance of this key strategy.[1] Security pros must understand the benefits of Zero Trust and know how the vendor community can help them achieve their objectives. Vendors that align themselves to the Zero Trust framework, deliver real Zero Trust capabilities, and are active participants in the community are well positioned to educate the market and drive adoption.
- **Support microsegmentation.** Creating microsegments is a critical capability for Zero Trust solutions. Some vendors focus more on users or identities as the point of segmentation; others push for segmentation at the network layer; and a handful of vendors deliver microsegmentation at the device level.[2] The good thing is that all these approaches are valid and useful for enabling Zero Trust. The bad thing is that, thanks to the many different methods of enabling segmentation, there's a disparity regarding which method is best. Each approach has specific benefits to enable Zero Trust and can be vectored to best benefit different organizations of different sizes. The most important takeaway is that there's now no excuse not to enable microsegmentation for any company or infrastructure. It's no longer a question of whether you can do it — the question now is how you do it.
- **Enforce policy everywhere.** Enabling Zero Trust across infrastructures requires that administrators and security pros be able to command and control infrastructure components in disjointed and disparate environments.[3] ZTX policies enable vendors' capabilities to translate into ZTX solutions. The only way this is possible is with the use of integrated and optimized policy-based offerings that leverage APIs and "hook" into other capabilities throughout the ZTX ecosystem. Vendors with extensive integrations and well-documented APIs are well positioned to enable policy creation and enforcement across the enterprise.
- **Provide identity beyond identity and access management (IAM).** Zero Trust mandates that more-granular security must start with the user, but interestingly, it's not limited to the user identity. A fundamental requirement for adopting Zero Trust is that security must focus on where the threat is most likely to occur — in most cases, with the end user. However, today's bring-your-own-device (BYOD) world also mandates paying attention to the devices those users leverage for work and any operational technology (OT) or internet-of-things (IoT) devices on the network. End users are typically most directly referenced as identities in IAM programs, but the need for identity use and analytics now goes beyond that singular aspect.[4] While this is still correct in the grand concept of

an IAM program, successful Zero Trust implementations focus on the telemetry and metrics derived from identities beyond end users alone, such as those from device data points like IP address, MAC address, and operating system. Essentially, everything has an identity and must be under consideration for ZTX — users, devices, cloud assets, and network segments. Monitoring the behaviors of this identity enables more understanding of what that entity is actually doing to better identify malicious behavior.[5]

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 doesn't represent the entire vendor landscape. You'll find more information about this market in our report "The Zero Trust eXtended (ZTX) Ecosystem."

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™: Zero Trust eXtended Ecosystem Platform Providers, Q4 2019

THE FORRESTER WAVE™

Zero Trust eXtended Ecosystem Platform Providers

Q4 2019

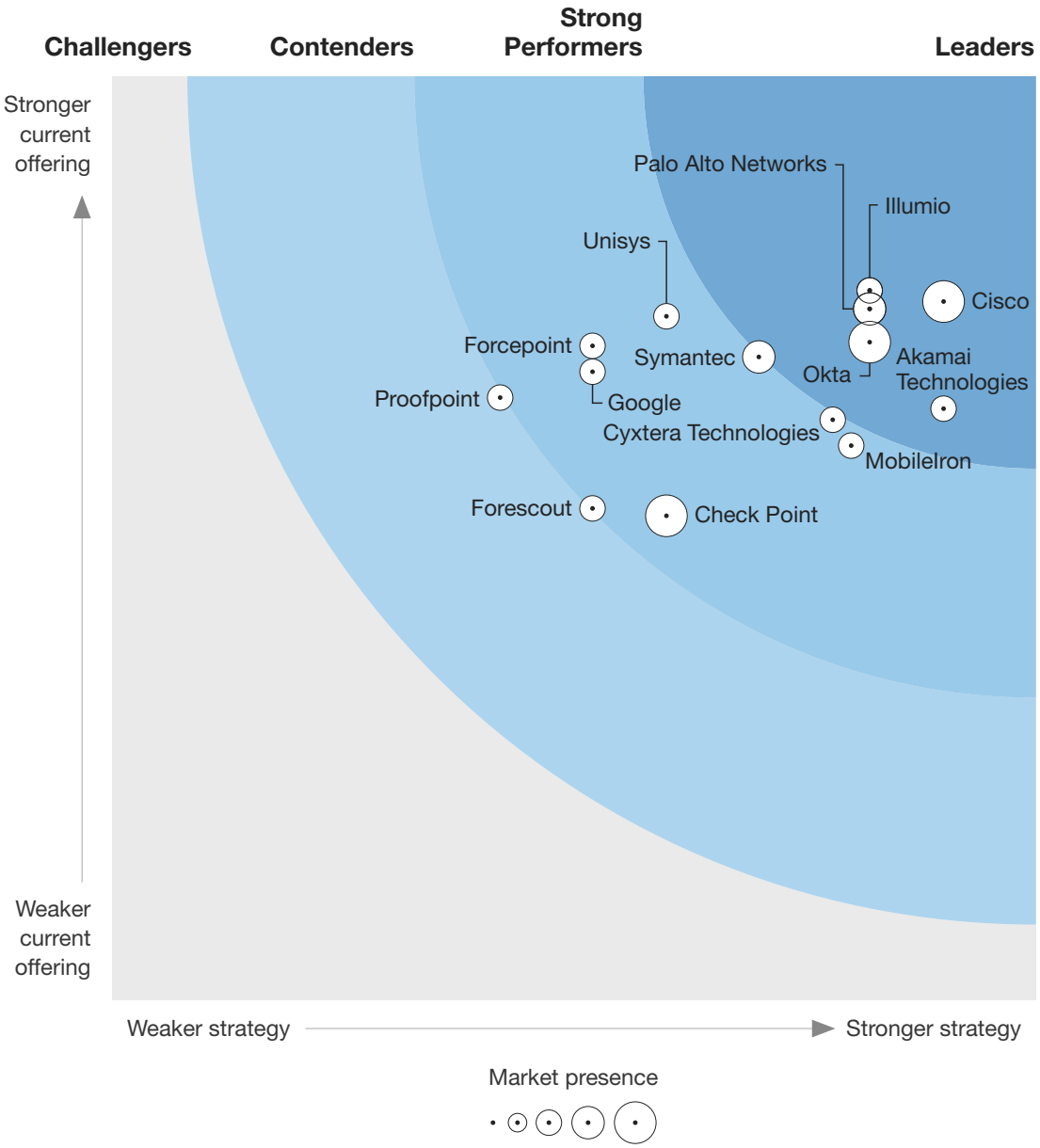


FIGURE 2 Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers Scorecard, Q4 2019

	Forrester's weighting	Akamai Technologies	Check Point	Cisco	Cyxtera Technologies	Forcepoint	Forescout	Google
Current offering	50%	3.20	2.62	3.78	3.14	3.54	2.66	3.40
Network security	12%	3.00	5.00	5.00	5.00	5.00	3.00	3.00
Data security	17%	1.00	3.00	1.00	1.00	5.00	1.00	3.00
Workload security	12%	5.00	3.00	3.00	5.00	3.00	1.00	5.00
People/workforce security	15%	5.00	1.00	5.00	3.00	3.00	3.00	5.00
Device security	14%	3.00	1.00	5.00	3.00	3.00	5.00	3.00
Visibility and analytics	5%	3.00	5.00	5.00	3.00	5.00	5.00	3.00
Automation and orchestration	8%	3.00	3.00	3.00	3.00	3.00	3.00	3.00
Manageability and usability	10%	3.00	3.00	5.00	3.00	3.00	3.00	3.00
APIs	7%	3.00	1.00	3.00	3.00	1.00	1.00	1.00
Strategy	50%	4.50	3.00	4.50	3.90	2.60	2.60	2.60
ZTX vision and strategy	30%	5.00	3.00	5.00	3.00	3.00	3.00	3.00
ZTX roadmap and differentiation	25%	3.00	3.00	3.00	3.00	3.00	3.00	3.00
ZTX advocacy	25%	5.00	3.00	5.00	5.00	3.00	3.00	3.00
Market approach	20%	5.00	3.00	5.00	5.00	1.00	1.00	1.00
Market presence	0%	3.00	4.40	4.40	3.00	3.00	3.00	3.00
Install base	30%	3.00	5.00	5.00	3.00	3.00	3.00	3.00
Customers investing in portfolio	40%	3.00	5.00	5.00	3.00	3.00	3.00	3.00
Portfolio growth rate	30%	3.00	3.00	3.00	3.00	3.00	3.00	3.00

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

FIGURE 2 Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers Scorecard, Q4 2019 (Cont.)

	Forrester's weighting	Illumio	MobileIron	Okta	Palo Alto Networks	Proofpoint	Symantec	Unisys
Current offering	50%	3.84	3.00	3.56	3.74	3.26	3.48	3.70
Network security	12%	3.00	3.00	5.00	5.00	3.00	5.00	5.00
Data security	17%	3.00	1.00	1.00	3.00	1.00	3.00	3.00
Workload security	12%	5.00	3.00	3.00	5.00	3.00	5.00	3.00
People/workforce security	15%	3.00	5.00	5.00	3.00	5.00	3.00	3.00
Device security	14%	3.00	5.00	3.00	3.00	5.00	3.00	3.00
Visibility and analytics	5%	5.00	1.00	3.00	5.00	3.00	3.00	5.00
Automation and orchestration	8%	5.00	3.00	5.00	5.00	5.00	3.00	5.00
Manageability and usability	10%	5.00	3.00	5.00	3.00	3.00	3.00	5.00
APIs	7%	5.00	1.00	3.00	3.00	1.00	3.00	3.00
Strategy	50%	4.10	4.00	4.10	4.10	2.10	3.50	3.00
ZTX vision and strategy	30%	5.00	3.00	5.00	5.00	3.00	3.00	3.00
ZTX roadmap and differentiation	25%	3.00	5.00	3.00	5.00	3.00	3.00	3.00
ZTX advocacy	25%	5.00	5.00	5.00	3.00	1.00	5.00	3.00
Market approach	20%	3.00	3.00	3.00	3.00	1.00	3.00	3.00
Market presence	0%	3.00	3.00	4.40	3.60	3.00	3.60	3.00
Install base	30%	3.00	3.00	3.00	3.00	3.00	5.00	3.00
Customers investing in portfolio	40%	3.00	3.00	5.00	3.00	3.00	3.00	3.00
Portfolio growth rate	30%	3.00	3.00	5.00	5.00	3.00	3.00	3.00

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

Vendor Offerings

Forrester included 14 vendors in this assessment: Akamai Technologies, Check Point, Cisco, Cyxtera Technologies, Forcepoint, Forescout, Google, Illumio, MobileIron, Okta, Palo Alto Networks, Proofpoint, Symantec, and Unisys (see Figure 3).

FIGURE 3 Evaluated Vendors And Product Information

Vendor	Product evaluated
Akamai Technologies	Zero Trust Security
Check Point	Check Point Infinity Security Access
Cisco	Duo Beyond; Tetration; SD-Access
Cyxtera Technologies	AppGate SDP
Forcepoint	Forcepoint Zero Trust Suite
Forescout	The Forescout Platform
Google	Context-Aware Access for Enterprise
Illumio	Illumio Adaptive Security Platform
MobileIron	MobileIron Zero Trust Platform
Okta	Okta Identity Cloud
Palo Alto Networks	Palo Alto Networks
Proofpoint	Proofpoint
Symantec	Symantec Integrated Cyber Defense
Unisys	Unisys Stealth; Unisys Solutions Services

Vendor Profiles

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

LEADERS

- **Cisco excels in Zero Trust, with a renewed and targeted focus.** Cisco has been a powerhouse in the networking space for decades, and after a few years of deprioritizing security, it's come roaring back into the sector with Zero Trust as its driving initiative. The company spent significant time and expense to realign much of its security portfolio to enable or enhance Zero Trust for its customers. Cisco has spent the past year working to integrate and operationalize the authentication technology from its acquisition of Duo. The integration of Duo's strong authentication offering and the simplicity of its UIs and tooling have strengthened the Cisco offering considerably.

  The interoperability and use for the Duo integration, combined with the other component offerings from Cisco's WWW (Workforce, Workload, and Workplace) approach to Zero Trust, are closely mapped to the ZTX ecosystem. The combination of Cisco's networking and device tooling, new offerings for analytics and cloud workloads, and Duo's focus on users and endpoints supports multiple components of ZTX. Deployment and ease of use are strengths across the portfolio. Cisco has adopted a Zero Trust strategy and is well positioned as a prominent Zero Trust player.

- **Illumio enables microsegmentation for Zero Trust infrastructures.** The focus that the team at Illumio has adopted to clarify how the vendor enables Zero Trust for its specific technical offering has paid off. Illumio's core capability is a strong ability to provide a well-defined and clearly illuminated asset map across the infrastructure. The vendor adds the ability to hook in encryption, mandate its use for legacy and newly discovered applications, and then control user access to systems on the fly. A well-engineered collection of APIs adds to Illumio's strength in mapping and discovering.

  Reference customers spoke highly of the use and power that the Illumio APIs afford them. Illumio's marketing literature states that it "want[s] to leverage what is already deployed." This clearly speaks to the vendor's understanding of how users can utilize a variety of tools to enable Zero Trust. More importantly, it emphasizes the solution's ability to provide value from the plethora of tooling that organizations already employ.

- **Palo Alto Networks is still a Leader, but the competition is playing for keeps.** Palo Alto Networks was one of the first vendors to embrace Zero Trust, back when it was still just a network security story. During the past year, the vendor has made numerous acquisitions to broaden its portfolio and continue its ZTX evolution. The acquisition of vendors such as PureSec, RedLock, and Twistlock, in particular, extended Palo Alto Networks' capabilities from the network into the cloud and workloads. This expansion has also led to tool sprawl and a longer integration cycle for the acquired companies, a common problem during any course of expedited acquisitions.

While Palo Alto Networks has a strong offering for Zero Trust enablement, and the added component technologies have further enhanced it, users have to be familiar with a variety of tools and multiple, separate UIs — something that could be problematic for new users or those unfamiliar with the new tools. Palo Alto Networks has all the necessary pieces to build Zero Trust for an enterprise. Buyers should, however, be aware that they'll have to work until the acquisitions are completely integrated to get full benefits from the product additions, which could take months or even longer.

› **Akamai Technologies enhances Zero Trust for critical users.** Akamai is one of the genuine true believers in the Zero Trust framework. It's also one of the few vendors that has not only embraced Zero Trust as part of its go-to-market but also deeply engaged in its own internal Zero Trust journey. The vendor has published its Zero Trust learning and education course to help familiarize its customers, and the industry, with the benefits and specifics of the strategy.

Akamai has a well-aimed approach to solving the crux of the problem by eliminating the VPN and baking in more security for its customers, with a focus on mitigating the threats that proliferate across enterprises via shared credentials and excessive accesses.

› **Okta makes user-focused Zero Trust easy.** Okta's Zero Trust approach can be summed up in two words: "identity rules." Since acquiring ScaleFT in the latter part of 2018, Okta has invested heavily to extend the fabric for security-focused infrastructures outward to the end user and inward for the infrastructure itself. The vendor's approach to Zero Trust enablement is bound to user identity. Leveraging the connectivity and control the ScaleFT offering brings to the network pillar of ZTX, the vendor extends enterprise security controls outward to the network edge, be it on-premises, off-premises, in the cloud, or at the local coffee shop.

The employee experience in this solution is high — when Okta is doing its thing, end users never really know that they're operating in a secure fashion, much less in a Zero Trust system. Of all the vendors we analyzed for this research, Okta has the cleanest and most easily usable administrator UI. This is a benefit for anyone administrating the technology for ZTX.

STRONG PERFORMERS

› **Cyxtera Technologies delivers Zero Trust for the data center.** Cyxtera is now a real player in the Zero Trust market. The vendor continues to develop strong technical assets aimed at cloud workload security as well as application isolation and security and demonstrates a sound understanding of cloud infrastructure. This understanding, combined with leadership and service offerings that strategically focus on big cloud and security provision for major federal agencies, speaks to the veracity of Cyxtera's approach in this space.

The company has a strong external marketing effort as a vendor focused on Zero Trust. Other than a few slight bumps with confusing cross-pollination on other industry initiatives and ZTX, the Cyxtera brand is well vectored to educate the market and the industry on its approach to

Zero Trust. Reference customers noted the strength of the solution for cloud and apps but also mentioned a hindrance in the people area, compared with other vendors in the space. If your organization wants to better secure the data center and big infrastructure for the cloud, Cyxtera is a go-to vendor.

› **MobileIron is new to Zero Trust, but it's focused on the future.** MobileIron is actively engaged in enabling Zero Trust mobile solutions for a variety of agencies within the US government that are deeply engaged with evolving their future networks and security postures. MobileIron's position — that the most comprehensive place to "start" a Zero Trust enterprise is with the device — aligns with current thinking about how enterprises will manage, maintain, and defend the increasingly disparate mobile infrastructure of the future. MobileIron's newly released Authenticator, which enables passwordless authentication to cloud services, is a must for future-state Zero Trust enterprises and speaks to its innovation in this space. A federated policy engine enables administrators to gain better control and increased operational command of the myriad devices and endpoints that are present in today's enterprise systems.

  The product suite is also well integrated, with a wide variety of application- and cloud-based tools and infrastructure components that are a necessity for enterprises. MobileIron has addressed many key components of a Zero Trust strategy, with a focus on innovation and ease of use for end users. It also has a capability to mandate email classification as emails leave or transit the enterprise, which is a useful tool that is directly in line with industry best practices and Zero Trust.

› **Symantec has a powerful platform for big enterprise Zero Trust.** Although Symantec appears to be in a state of flux due to its acquisition by Broadcom, this vendor still has solid Zero Trust chops.[6] The company's earlier acquisition of Luminate adds to its capabilities in the software-defined perimeter (SDP) space and in extending its solution in the network pillar of ZTX.

  The only real chink in the Symantec portfolio is the vendor's legacy approach to data loss prevention (DLP). Reference customers noted that they "don't really use the DLP as it was intended." In truth, however, that's common for most DLP tools in the industry today. The most interesting capability in the Symantec platform for Zero Trust is the update to the Risk Fabric system. This includes the analytics, context, and ability to remediate issues as they map to behavior and the threat activity's kill chain position. These are useful capabilities for the ZTX visibility and analytics pillar.

› **Unisys Stealth offers a unique approach to microsegmentation and Zero Trust.** Stealth is the Unisys Zero Trust product, and it's a good name for a product that, in truth, has grown from this vendor's heavy interaction and work with select and sensitive government agencies and groups within the US federal government. Being one of the few providers in this space specifically cleared to work on enabling Zero Trust for some of the most highly protected spaces, also known as classified networks, within the National Security Agency (NSA) and the Defense Information Systems Agency (DISA) speaks to the validity of the approach that Unisys Stealth provides.

Unisys's offering is well aligned to the main tenets of Zero Trust, as it delves into the process of discovering, identifying, mapping, and cloaking those assets that shouldn't be visible or accessible to those who aren't at the need-to-know level. Additionally, Unisys engineered and built its own innovative, proprietary offering at the protocol level to enable microsegmentation and Zero Trust. Its use of the affinity-level setting on its tooling is a useful function and one of the few real applications of actual machine learning that we've seen in production in any security analytics or automation system.

› **Forcepoint still excels at taking care of the data.** Forcepoint has a substantial focus in the security user behavior analytics (SUBA) approach to enable Zero Trust, which is useful. The solution continues to evolve to further enhance an administrator's understanding of risky actions as users traverse a network and to provide vectored insight into the data that those particular user groups access.

Forcepoint's solution is a platform built around DLP and a cloud access security broker (CASB), with tangential control points in the other areas of ZTX. While that approach is useful, reference customers noted a requirement to be "100% Forcepoint" to get total value from the system.

› **Google has the capabilities to build a Zero Trust infrastructure.** Google is new to the Zero Trust world as a solutions provider but not to Zero Trust as a guiding principle for its own internal security. Many folks across the industry are aware of the Google BeyondCorp approach to security. Google has employed Zero Trust within its own infrastructure and network in varying stages since 2011 and has noted specific benefits to its defensive posture. In other words, Google has done a great job of living the tenets of Zero Trust. More recently, Google rolled out its platform play, called context-aware access, for enabling BeyondCorp (AKA Zero Trust) for its clients.

While its marketing strategy around BeyondCorp and Zero Trust can be confusing, Google clearly believes in the merit of the approach and has a solid offering to enable the main tenets of the strategy. Its approach is cloud focused, using user and machine identities as what are essentially pivot points in the architecture. This is a necessity in today's user-enabled, cloud-enabled, and mobile-enabled world.

› **Check Point has plenty of technology that customers can use to deploy Zero Trust.** Check Point is another large vendor that has recently realigned its strategy to Zero Trust. Reference customers noted the company's capability in offering a comprehensive security platform that enables a Zero Trust end state. They stated that to get the maximum value out of the Check Point tooling, they had to use 80% to 90% of the product portfolio to get the maximum value and noted that it "didn't always play well with others."

Check Point's Infinity system is basically the vendor's one-stop shop for Zero Trust for those that are willing to leverage most of its total offering. Additionally, Check Point is offering Zero Trust workshops for potential clients and current customers, which could be beneficial to aid in the education, guidance, and deployment of its tools and assets to enable Zero Trust.

› **Forescout is the vendor for Zero Trust IoT/OT focused security.** IoT/OT device security is one of the hardest problems to solve within the enterprise. This is Forescout's sweet spot, and the vendor's platform and capabilities for IoT/OT security shine above those of the competition. Maximum visibility, leading to maximum operational control and, ultimately, security, is the crux of Forescout's approach to Zero Trust.

Forescout's platform is useful for these applications, and its integration with almost every device available on the market is notable. Forescout is a useful platform for organizations that seek to know what devices are "talking" on their network and strive to gain insight and control for hardcore device security.

CONTENDERS

› **Proofpoint secures users and email, both critical for Zero Trust enterprises.** Proofpoint is a new addition to the Zero Trust world, with a specific focus on the people side of ZTX. Its Very Attacked Person (VAP) solution, backed with data science, is one of its most interesting offerings. Essentially, this system looks at the critical areas of risk and threats that target users and high-value users within an enterprise and applies controls to its asset accesses and use accordingly. This is extremely useful and applicable for Zero Trust organizations.

The company's background and history of helping organizations address the issues around social engineering and securing the human component are noteworthy as well. In 2018, Proofpoint acquired Meta Networks to bolster its security capabilities in the SDP space. When it comes to advocacy, there's a bit of a disconnect between the Zero Trust public side of the company and the public side of Meta Networks. While Meta Networks has a variety of material and advocacy related to Zero Trust, Proofpoint, at the time of this research, does not.

Evaluation Overview

We evaluated vendors against 16 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. Key criteria for these solutions include network security, data security, workload security, people/workforce security, device security, visibility and analytics, automation and orchestration, manageability and usability, and APIs.

› **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. We evaluated vendors' ZTX vision and strategy, ZTX roadmap and differentiation, ZTX advocacy, and market approach.

› **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's install base, customers investing in its portfolio, and portfolio growth rate.

VENDOR INCLUSION CRITERIA

Forrester included 14 vendors in the assessment: Akamai Technologies, Check Point, Cisco, Cyxtera Technologies, Forcepoint, Forescout, Google, Illumio, MobileIron, Okta, Palo Alto Networks, Proofpoint, Symantec, and Unisys. Each of these vendors has:

- **Notable revenues.** Vendors must have at least $25 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.
- **Zero Trust advocacy.** Vendors must demonstrate that they're following their own advice in relation to enabling or leveraging Zero Trust in their own organizations, not solely in a sales capacity. Additionally, vendors must show a clear and concise public-facing lexicon and messaging around their Zero Trust offerings.

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 August 26, 2019, 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.

SURVEY METHODOLOGY

The Forrester Analytics Global Business Technographics® Security Survey, 2019, was fielded between April and June 2019. This online survey included 3,890 respondents in Australia, Canada, China, France, Germany, India, the UK, and the US from companies with two or more employees.

Forrester Analytics' Business Technographics ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of business and technology products and services. Dynata fielded this survey on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates.

Endnotes

[1] Source: Forrester Analytics Global Business Technographics Security Survey, 2019.

[2] See the Forrester report "No More Chewy Centers: The Zero Trust Model Of Information Security."

[3] See the Forrester report "The Zero Trust eXtended (ZTX) Ecosystem."

[4] See the Forrester report "Making The Business Case For Identity And Access Management."

[5] See the Forrester report "Pull Your Head Out Of The Sand And Put It On A Swivel: Introducing Network Analysis And Visibility."

[6] Source: Merritt Maxim, Andras Cser, Christopher Sherman, Jeff Pollard, Joseph Blankenship, and Stephanie Balaouras, "Broadcom Buys Symantec's Enterprise Biz: Good News For Investors, Bad News For Enterprises," Forrester Blogs, August 9, 2019 (https://go.forrester.com/blogs/broadcom-buys-symantecs-enterprise-biz-good-news-for-investors-bad-news-for-enterprises/).

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.

ABOUT ILLUMIO

Illumio enables organizations to realize a future without high-profile breaches by providing visibility, segmentation, and control of all network communications across any data center or cloud. Founded in 2013, Illumio's Adaptive Security Platform® uniquely stops the lateral movement of attackers with real-time application dependency mapping coupled with security segmentation across container, virtual machine, and bare-metal environments. The world's largest enterprises, including Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite, trust Illumio to reduce cyber risk.

Visit illumio.com to learn more about how Illumio helps organizations operationalize Zero Trust