Enable End-to-End Zero Trust To Achieve Effective Outcomes

FEATURING RESEARCH FROM FORRESTER

The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q3 2020

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, remote users, and endpoints, 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. For effective Zero Trust, you need to have visibility into communications and restrict traffic – across endpoints, between remote users and applications, and dynamic workloads that move inside your data centers and public cloud 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 allow listing of all communications across workloads to reduce the attack surface and improve your security posture.

Illumio has been named a leader in The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q3 2020 report, receiving the highest ranking in the three major categories: current offering, strategy, and market presence and the highest scores possible in the criteria of network security, workload security, visibility and analytics, APIs, future state of zero trust infrastructure, vision and strategy, advocacy, mission completion, customers investing in portfolio, and portfolio growth rate.

LEADING THE WAY WITH ILLUMIO CORE AND ILLUMIO EDGE

Illumio was founded on the principle of least privilege to help organizations stop the lateral movement problem, or the ability for malicious actors to traverse a network in the data center and cloud.

Illumio Core (previously known as Illumio Adaptive Security Platform) 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.

IN THIS DOCUMENT

In the last year, we have expanded our portfolio with the introduction of Illumio Edge and our new partnership with CrowdStrike to stop ransomware propagation and attacker lateral movement in its tracks. This new offering enables containment by default, complementing CrowdStrike's state-of-the-art malware prevention, to ensure that in the case of never-before-seen ransomware, the first endpoint infected is always the last endpoint infected.

Illumio Core and Illumio Edge help organizations deploy end-to-end Zero Trust segmentation from the data center and cloud to endpoints. This approach shifts the conversation to preventative containment, with a focus on preventing lateral movement between endpoints, between users and data center applications, and inside your data center and cloud environments. As a result, micro-segmentation – a security control to stop lateral movement – has become a foundational component for Zero Trust.

3 STEPS TO ENABLE ZERO TRUST SECURITY

Illumio has three practical steps to help you to quickly implement a holistic and highly effective security strategy for Zero Trust:

Step 1: Discover: Seeing how your users, devices, and apps are connected is a critical first step to understand what's communicating and what shouldn't be.

- Use a real-time map to see everything across your endpoints and application flows and identify high-value systems and critical applications.
- Map the connections of sensitive data across users, devices, networks, workloads, and applications to understand what should be allowed to communicate based on least privilege.
- Enable a single source of truth to facilitate collaboration and engage business and IT stakeholders in designing Zero Trust microperimeters and security policies.

Step 2: Define : Architect optimal micro-segmentation controls with automated policy creation to reduce risk and deployment complexity.

- Define and automate the right level of Zero Trust segmentation controls (from environment to application to process levels) across endpoints and East-West traffic.
- Identify and map segmentation policy based on the exploitability of vulnerabilities and use segmentation as a compensating control when you can't patch.
- Visualize and test policies before enforcement to ensure you don't break applications while provisioning security at birth in cloud-native applications.

Step 3: Enforce: Enable a default-deny policy that's decoupled from your network to enforce effective Zero Trust controls wherever your endpoints and workloads live.

- Use an allowlist to ensure that only authorized connections can take place across users, devices, networks, applications, and workload communications.
- Secure data in transit without requiring any changes or upgrade to the existing network.
- Continuously monitor and adjust dynamic Zero Trust policies as your environment changes.
- Seamlessly integrate with third-party IT tools to orchestrate adaptive Zero Trust across your on-prem and multi-cloud environment to reduce security silos.

FORRESTER®

The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q3 2020

Tools And Technology: The Zero Trust Security Playbook

by Chase Cunningham
September 24, 2020

Why Read This Report

In our 19-criterion evaluation of Zero Trust platform providers, we identified the 15 most significant ones — Akamai Technologies, Appgate, BlackBerry, Cisco, Forcepoint, Google, Guardicore, Illumio, Ionic Security, Microsoft, MobileIron, Okta, Palo Alto Networks, Proofpoint, and Unisys — and researched, analyzed, and scored them. This report shows how each provider measures up and helps S&R professionals select the right one for their needs.

Key Takeaways

Delivering Zero Trust Security Demands A Platform, Not A Portfolio, Approach

Forrester's research uncovered a market in which Illumio, Cisco, Appgate, Akamai Technologies, MobileIron, and Palo Alto Networks are Leaders; Microsoft, Guardicore, Unisys, Okta, Google, BlackBerry, and Forcepoint are Strong Performers; and Ionic Security and Proofpoint are Contenders.

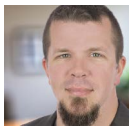
Remote Workforce Security And Ease Of Use Are Key Differentiators

As legacy technology becomes outdated and less effective, improved technical capabilities powering the future of work will dictate which providers will lead the pack. Vendors that can provide a secure remote workforce, Zero Trust mission completion, and easy-to-use technology position themselves to successfully deliver true Zero Trust to their customers. ZT is not just about firewalls anymore; the post COVID-19 world demands that organizations employ this critical strategy that focuses on the bigger picture.

This PDF is only licensed for individual use when downloaded from forrester.com or reprints.forrester.com. All other distribution prohibited.

The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q3 2020

Tools And Technology: The Zero Trust Security Playbook



by Chase Cunningham
with Joseph Blankenship, Alexis Bouffard, and Peggy Dostie

September 24, 2020

Table Of Contents

Related Research Documents

Enhance EX With Zero Trust

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

The Zero Trust eXtended (ZTX) Ecosystem

Share reports with colleagues.
Enhance your membership with Research Share.

FORRESTER®

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

© 2020 Forrester Research, Inc. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. Unauthorized copying or distributing is a violation of copyright law. Citations@forrester.com or +1 866-367-7378

For Zero Trust, There's A Difference Between A Platform And A Portfolio

In "The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q4 2019," we discussed how Zero Trust (ZT) is a journey and not a singular destination.[1] It may take organizations years to achieve an end state that is emblematic of real Zero Trust. In 2020, the COVID-19 crisis accelerated that journey, as the entirety of the world's workforce was essentially shoved outside of any defined network perimeter. This new reality forced organizations globally to enable ZT capabilities for their users and to enhance their security posture in a manner that is entirely reliant on Zero Trust eXtended (ZTX) principles.[2] For security and risk (S&R) leaders, this means securing end users who are now working remotely as well as fixing the anomalies configuration issues that this new model revealed. Operating in a Zero Trust manner in the post COVID-19 world mandates that organizations leverage the power that ZT platforms offer to operate at the scale and dynamism that are now necessary to keep enterprises secure and functional in the expanded infrastructure of today.

As a result of these trends, S&R leaders should look for ZT platform providers that:

- **Are part of the ZT journey for the long haul and work to continue the mission.** In the past, S&R leaders would often say, "Zero Trust sounds great, but it's too big to tackle." That can be true. However, ZTX platform providers that clearly latch onto and integrate into customers' ZT journeys will help their customers all along their journey. S&R pros should focus on procuring products and capabilities from vendors that have specific offerings built into their procurement that guarantee a service or investment from the vendor that will help push the mission toward completion.
- **Use ZT platforms to enhance user experience and increase user security acceptance.** No solution will be beneficial if an end user decides to work around it. The movement to eliminate passwords and VPNs is powerful because it helps users operate in a more secure fashion while making their daily lives and jobs easier.[3] Good ZTX platforms integrate security solutions into nearly invisible security tooling that end users will not only be OK with, but will actually want. Seek out ZTX platforms that empower end users and make security so fundamental to these users' daily technology interactions that they can't avoid operating in a more secure fashion, making your organization excel in a more secure ZT posture.
- **Offer analytics that power outcomes as part of the ZTX ecosystem.** The days of "analysis paralysis" need to go the way of the dinosaur. If a system can't provide an action based on a series of inputs and validated telemetry, what good is it? The ZTX platforms that have integrated outcomes based on their vast telemetry and inputs are head and shoulders above those that just offer "more stuff." To achieve a ZT end state, analytics must power decision making and action.
- **Don't require rip and replace.** Old approaches to infrastructure required organizations to remove and replace old security hardware (or software) as new tooling and technologies were made available. That is a costly and often negative-return operation for any size organization. In the more virtual, digital, and dynamic world that ZT organizations find themselves in today, powerful platform providers work around the need for rip and replace. The vendors able to layer into existing security infrastructure components are clear frontrunners in their ability to enable a Zero Trust end state.

FORRESTER®
© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

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. You'll find more information about this market in our reports on Zero Trust and ZTX.

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.

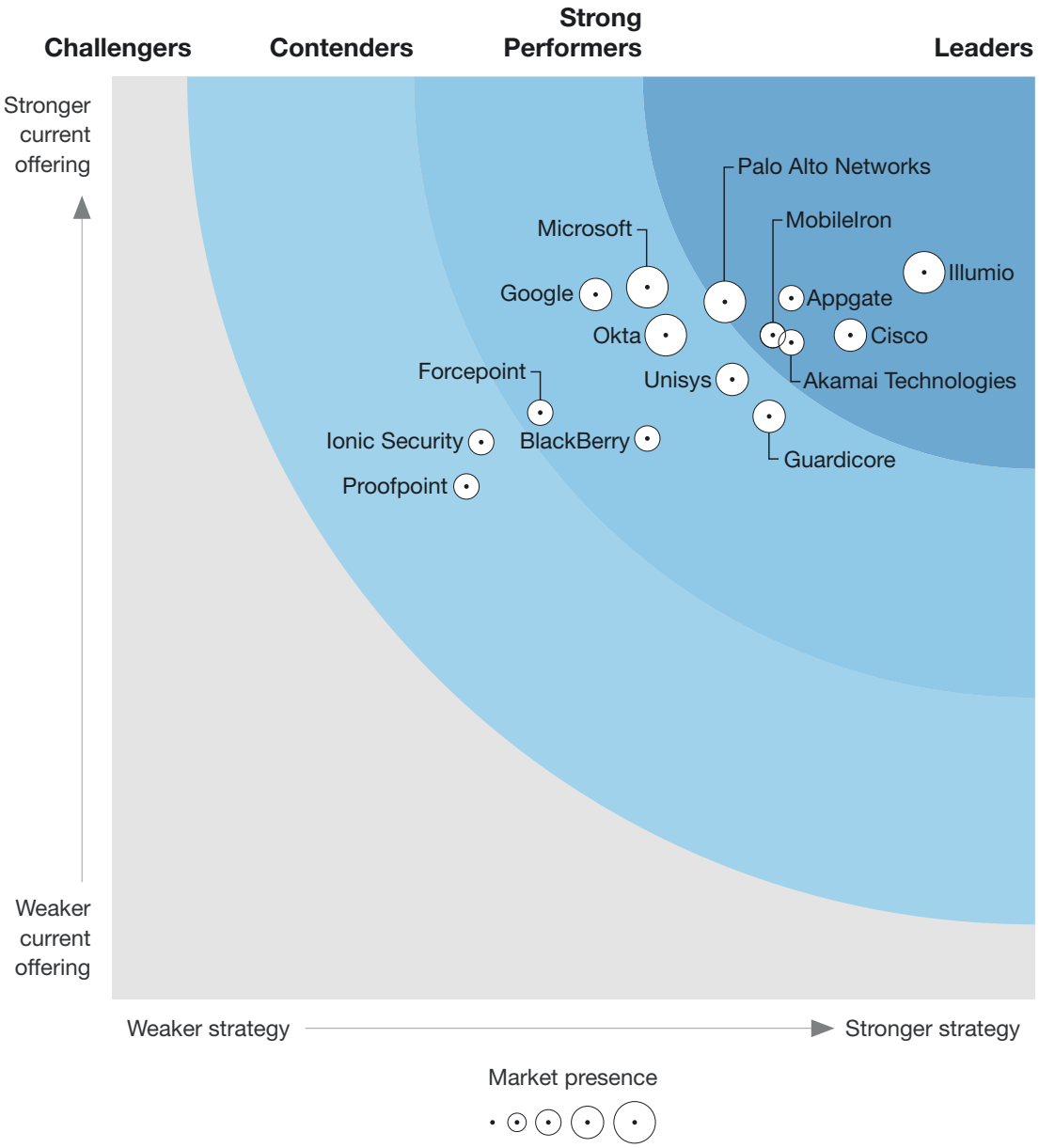
FORRESTER®
© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FIGURE 1 Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q3 2020

THE FORRESTER WAVE™

Zero Trust eXtended Ecosystem Platform Providers

Q3 2020



FORRESTER®
© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FIGURE 2 Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers Scorecard, Q3 2020

	Forrester's weighting	Akamai Technologies	Appgate	BlackBerry	Cisco	Forcepoint	Google	Guardicore	Illumio
Current offering	50%	3.56	3.80	3.04	3.60	3.18	3.82	3.16	3.94
Network security	9%	5.00	5.00	3.00	5.00	3.00	3.00	3.00	5.00
Data security	10%	3.00	3.00	3.00	3.00	5.00	3.00	3.00	3.00
Workload security	10%	5.00	5.00	3.00	3.00	3.00	5.00	5.00	5.00
People/workforce security	11%	3.00	3.00	3.00	3.00	3.00	5.00	3.00	3.00
Device security	11%	3.00	3.00	5.00	5.00	3.00	3.00	1.00	3.00
Visibility and analytics	9%	3.00	3.00	1.00	3.00	5.00	3.00	5.00	5.00
Automation and orchestration	10%	3.00	5.00	3.00	3.00	1.00	5.00	3.00	3.00
Manageability and usability	11%	3.00	5.00	3.00	3.00	3.00	3.00	3.00	3.00
APIs	9%	5.00	3.00	3.00	3.00	3.00	3.00	3.00	5.00
Future state of Zero Trust infrastructure	10%	3.00	3.00	3.00	5.00	3.00	5.00	3.00	5.00
Strategy	50%	3.68	3.68	2.90	4.00	2.32	2.62	3.56	4.40
ZTX vision and strategy	16%	3.00	5.00	3.00	5.00	3.00	3.00	5.00	5.00
ZTX roadmap and differentiation	14%	3.00	3.00	3.00	3.00	1.00	3.00	5.00	3.00
ZTX advocacy	15%	5.00	5.00	5.00	5.00	3.00	3.00	5.00	5.00
Market approach	19%	5.00	5.00	3.00	5.00	3.00	1.00	5.00	5.00
ZT mission completion	20%	3.00	3.00	1.00	3.00	1.00	3.00	1.00	5.00
ZT technology expansion	16%	3.00	1.00	3.00	3.00	3.00	3.00	1.00	3.00
Market presence	0%	3.00	2.80	3.00	3.60	2.20	3.60	3.60	4.40
Install base	30%	3.00	3.00	3.00	5.00	3.00	5.00	3.00	3.00
Customers investing in portfolio	40%	3.00	1.00	3.00	3.00	1.00	3.00	3.00	5.00
Portfolio growth rate	30%	3.00	5.00	3.00	3.00	3.00	3.00	5.00	5.00

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

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FIGURE 2 Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers Scorecard, Q3 2020 (Cont.)

	Forrester's weighting	Ionic Security	Microsoft	MobileIron	Okta	Palo Alto Networks	Proofpoint	Unisys
Current offering	50%	3.02	3.86	3.60	3.60	3.78	2.78	3.36
Network security	9%	1.00	3.00	3.00	3.00	5.00	3.00	3.00
Data security	10%	5.00	3.00	3.00	3.00	3.00	3.00	3.00
Workload security	10%	3.00	5.00	5.00	5.00	5.00	1.00	3.00
People/workforce security	11%	3.00	5.00	5.00	3.00	3.00	5.00	3.00
Device security	11%	3.00	5.00	3.00	3.00	3.00	3.00	3.00
Visibility and analytics	9%	1.00	3.00	3.00	3.00	3.00	5.00	5.00
Automation and orchestration	10%	3.00	5.00	3.00	3.00	5.00	3.00	3.00
Manageability and usability	11%	3.00	3.00	3.00	5.00	3.00	1.00	3.00
APIs	9%	5.00	1.00	5.00	5.00	3.00	3.00	5.00
Future state of Zero Trust infrastructure	10%	3.00	5.00	3.00	3.00	5.00	1.00	3.00
Strategy	50%	2.00	2.90	3.58	3.00	3.32	1.92	3.36
ZTX vision and strategy	16%	3.00	3.00	3.00	3.00	3.00	3.00	3.00
ZTX roadmap and differentiation	14%	1.00	3.00	5.00	3.00	3.00	3.00	3.00
ZTX advocacy	15%	3.00	5.00	5.00	3.00	3.00	1.00	5.00
Market approach	19%	3.00	3.00	3.00	3.00	3.00	1.00	5.00
ZT mission completion	20%	1.00	1.00	3.00	3.00	3.00	1.00	3.00
ZT technology expansion	16%	1.00	3.00	3.00	3.00	5.00	3.00	1.00
Market presence	0%	2.40	4.20	2.40	4.20	4.20	3.00	3.60
Install base	30%	1.00	5.00	3.00	5.00	5.00	3.00	3.00
Customers investing in portfolio	40%	3.00	3.00	3.00	3.00	3.00	3.00	3.00
Portfolio growth rate	30%	3.00	5.00	1.00	5.00	5.00	3.00	5.00

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

FORRESTER®
© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

Vendor Offerings

Forrester included 15 vendors in this assessment: Akamai Technologies, Appgate, BlackBerry, Cisco, Forcepoint, Google, Guardicore, Illumio, Ionic Security, Microsoft, MobileIron, Okta, Palo Alto Networks, Proofpoint, and Unisys (see Figure 3).

FIGURE 3 Evaluated Vendors And Product Information

Vendor	Product evaluated
Akamai Technologies	Zero Trust Security
Appgate	Appgate SDP
BlackBerry	BlackBerry Spark
Cisco	Duo Beyond; Tetration; SD-Access
Forcepoint	Forcepoint Dynamic Security Solutions
Google	BeyondCorp Remote Access
Guardicore	Guardicore Centra Security Platform
Illumio	Illumio Core; Illumio Edge
Ionic Security	Machina
Microsoft	Microsoft 365; Azure
MobileIron	MobileIron Zero Trust Platform
Okta	Okta Identity Cloud
Palo Alto Networks	Palo Alto Networks
Proofpoint	Meta
Unisys	Unisys Stealth; Unisys Security Solutions Services

FORRESTER®
© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

Vendor Profiles

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

LEADERS

- **Illumio enables Zero Trust intelligently.** In the past, Illumio delivered a strong platform focused on visibility and analytics that provided clear and useable information on the entirety of an infrastructure. The vendor has continued that powerful capability but has now bolstered that efficacy with a move to the endpoint. By teaming with CrowdStrike, a leading endpoint security provider, Illumio has helped bridge the gap in security beyond the perimeter for organizations and is well aligned for the future of work.

  Feedback from reference customers indicates that the platform is able to "bolt into" organizations' existing security tooling and up-level the capability significantly. As an added organizational benefit, Illumio offers its solution via a singular SKU for procurement purposes and guarantees a dedicated Illumio engineer for a period to ensure that the Zero Trust mission is well supported for clients. Should Illumio move to securing mobile devices via partnership or internal development as well they will be the shining star of what ZTX is all about. Using this system does require a concerted effort and focused strategic plan; users would be wise to remember that. There is no "easy" button for ZT even with a partner like Illumio. Enterprises looking for a solution that is ahead of the requirements for the future of work and want a holistic ZT offering should evaluate Illumio.

- **Cisco pushes the Zero Trust envelope the right way.** Cisco's use and integration of the capabilities offered through the Duo Security acquisition could have easily been a flash in the pan, but that's not the case. The Duo Security offering has been fully integrated into the Zero Trust-focused Cisco Zero Trust portfolio approach for the Workforce, Workplace, and Workload (WWW). While the past performance of its firewalls and network security solutions remain powering security operations in the background, the WWW approach based on ZTX is front and center in the vendor's platform, offering integrated analytics and automated decision making and deploying segmentation controls across the entire infrastructure.

  Reference customers spoke highly of the newly improved UIs for administrators and the ability of the system to leverage powerful internal analytics to push the control capabilities outside the perimeter all the way to the user and their devices. Customer references also noted that leveraging Cisco's capabilities still requires a "lot of Cisco-specific knowledge," which is a point to consider on the human capital side. Organizations that have a well-constructed security apparatus in place and are moving to a more mobile workforce should consider bolstering those capabilities with the ease of use Cisco now provides.

- **Appgate embraces SDP as the engine to drive Zero Trust for enterprises.** Cyxtera, a privately held company offering secure data center infrastructure, spun out Appgate into a new company on January 1, 2020. Appgate is now behind the Appgate SDP platform. One of the first companies to

FORRESTER®
© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

latch onto the #killtheVPN movement, Appgate has made that difficult technical task an easy one. The vendor's strong presence in a variety of already engaged Zero Trust mega-enterprises and DoD organizations speaks to the offering's capability and is indicative of its ability to power enterprises on a long-term journey to Zero Trust.

Reference customers spoke highly of the system's ability to move "corporate security outside the firewall" and to "make every access request part of the solution, not the problem." While the vendor is not fully deploying password elimination technology, the platform does integrate with solutions that do. Therefore, it integrates the tooling to minimize security hindrances for corporate users. While Appgate is well aligned to ZT, there has been a lot of transition due to its spinout from Cyxtera, which could be a hindrance as things settle out at the corporate level. Any enterprise seeking a simple but effective way to eliminate the threats present for enterprises using hybrid infrastructure should explore Appgate's offerings.

› **Akamai Technologies is a true believer and provider of Zero Trust, and it shows.** From its CEO all the way to its newest employee, Akamai truly believes in the tenets and implementation of Zero Trust for its customers and for itself. This should be a key point for potential clients — the company is seriously engaged in the same endeavors that they will be undertaking as part of their Zero Trust journey. Coupled with this fervent belief is the power the Akamai platform provides. From DDoS capabilities that have notably defended massive mutli-terabyte DDoS attacks to MFA and access controls that are a lynchpin for organizational Zero Trust, Akamai has it.

Reference customers noted the deep dedication of the Akamai technical team to the mission and the platform's ease of deployment both outside and inside of the corporate firewall as key differentiators. Even given Akamai's relative ease of use, reference customers did wish for "dedicated resources" for their ZT projects which could be pivotal for long-term project success. Enterprises seeking to upscale their defenses to be able to take on massive DDoS threats while moving to better secure their users should bet on Akamai.

› **MobileIron progresses strongly to deliver Zero Trust to mobile devices.** Users are more mobile than they have ever been, requiring organizations to have a means of managing and securing those mobile devices. MobileIron is the one vendor in the Zero Trust space that is focused on applying Zero Trust and ZTX concepts to enterprise users' mobile devices. This has never been more necessary than in the full-on remote world that is the result of the COVID-19 pandemic. In early 2020, MobileIron purchased a mobile app automation software company named Incapptic Connect. This was a boon to its Zero Trust capabilities, as it helps enterprise customers accelerate mobile app releases with more built-in security functionality.

MobileIron is a leader in the #killthepassword space and has successfully deployed passwordless capabilities to select customers in a variety of enterprises. Reference customers noted that the administrator's UI and analytics were "lacking." The end user management and device security capabilities, however, came through as powerful solutions to a pressing problem. Enterprises working to get to ZT by eliminating the password and securing users' devices should evaluate MobileIron.

FORRESTER®
© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

› **Palo Alto Networks has a complete toolkit for Zero Trust.** Palo Alto Networks has been on an integration and optimization spree since its 18 months of massive acquisitions.[4] In that time, the vendor has essentially either procured, acquired, or built every tool or capability an organization could need to operate a Zero Trust infrastructure. Palo Alto Networks is assembling a robust portfolio to deliver Zero Trust everywhere — on-premises, in the data center, and in cloud environments.

Reference customers noted the multitude of capabilities and powerful options provided by this massive compendium of solutions. They also expressed that all the tooling could be, at times, "daunting" to discern "what goes where." Added to this confusion, reference customers also commented about the myriad of procurement variables that are often complex. They added that many features rely on the Cortex XSOAR product integration for automated interoperability of playbook-related actions. Palo Alto Networks is focusing on the future state of Zero Trust in the cloud and continues to be a force to be reckoned with in the Zero Trust realm. Partnering with Palo Alto Networks makes a lot of sense for enterprises that will be heavily cloud- and app-focused in the future.

STRONG PERFORMERS

› **Microsoft provides Zero Trust for Office 365 and legions of remote workers.** A clear juggernaut in the cloud and end user computing spaces, Microsoft has returned to the ZT world after revising its approach over 2019, with a renewed and specific focus. While other vendors in this space must offer tooling in pieces and parts to apply ZT to massive infrastructure, Microsoft is its own cloud enterprise. Microsoft has been one of the dominant providers of ZT-related remote work capabilities through O365 thanks to the fallout and push to remote work that the COVID-19 pandemic placed on organizations.

Tying in the capability that Azure offers cloud users and developers, Microsoft has a solid ZT product portfolio that can be leveraged. Microsoft has vast capabilities due to its size, but customer references did note that size could be daunting, and there was a lack of specific technical assistance in many cases for implementation. Any large organization that has a significant investment in Microsoft, O365, or Azure is wise to work with Microsoft's platform to move toward a Zero Trust future.

› **Guardicore understands the realities of implementing ZT for organizations.** Guardicore is charging into the Zero Trust space, with an approach to enabling Zero Trust that is emblematic of the largest players in that the vendor offers easy visibility and insight into the core infrastructure configurations and the ability to apply dynamic policy control. Guardicore couples these capabilities with its efforts to help organizations test their infrastructure with ZT automated penetration testing with the inclusion of the Infection Monkey, giving enterprises a new and powerful solution set for true ZT implementation.

FORRESTER®
© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

Guardicore's capability for Zero Trust is also evident in its ability to aid in testing controls and configuration. Users can test the implementation of that tooling to validate it and get a customized ZT report that validates the security of that system based on both the ZTX framework and the MITRE ATT&CK framework. The vendor currently has limited ZT scope and lacks broader solutions across the ZTX framework. Guardicore is currently best suited to small and midsize enterprises that are moving to the cloud and require segmentation therein.

› **Unisys has proven its Zero Trust chops.** Unisys has been one of the few companies to openly advertise its Zero Trust offerings while simultaneously opening it up to hackers for live testing. At the 2020 RSA Conference, Unisys sponsored a 24-hour hackathon against a simulated virtual environment it constructed that focused on a Zero Trust implementation of Unisys Stealth.[5] The solution had zero incidences of compromise or lateral movement within the simulated enterprise.[6] This is a testament to the vendor's faith in its product and the willingness to actively engage the broader community.

Reference customers noted the platform's upgraded UI and administrator capabilities as "making their life easier" while the system deploys microsegmentation at enterprise scale. References stated that the system could be a quagmire of configuration if there is a lack of specific technical focus during deployment, especially in multicloud environments. In Q1 of 2020, Unisys landed a deal with SAIC to provide its software, including Unisys Stealth, to SAIC clients.[7] The solution is now being sold by SAIC and has a variety of customers in the US DoD and various three-letter US government agencies. Organizations looking to "cloak" their most valuable assets and deploy network-based microsegmentation should assess Unisys.

› **Okta continues to be serious about Zero Trust.** Okta has pivoted slightly from being a forefront ZT "tool" to a more backend provider for Zero Trust solutions in 2020. This is evident in that it's not singularly pushing Okta as a product for ZT. Instead, the vendor is adapting to being the power behind ZT authentication for other solutions. Nearly every vendor in the ZT space, and in cybersecurity, is either leveraging Okta's ZT authentication mechanism or is tying into it via their powerful API. While others in the ZT platform provider space have run full force to make acquisitions, Okta has focused on integrating its prior purchases into a seamless ability to interoperate with the compendium of security solutions on the market.

Reference customers for Okta raved about the vendor's ability to integrate and use a variety of authentication methods but were also notably hesitant about its future focus for Zero Trust. Okta is a powerful, broadly adopted platform for solving authentication and authorization for Zero Trust. While Okta's alignment to the "behind the curtain" for ZT enterprises is notable, the potential exists for the company's strategic alignment to slip there and leave the customer wanting in future instances. Should Okta move further into the arena of being a ZT backend for authentication and not delivering full enterprise solutions, its strategic execution for broader ZTX capabilities could stutter. Enterprises seeking a well-integrated Zero Trust authentication solution should assess Okta.

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

- **Google is a ZT player for sure.** Google pioneered the BeyondCorp implementation of ZT for its own infrastructure. Now, the vendor has taken those lessons learned and expanded them into its own ZT product offering. BeyondCorp as a service is essentially Google's specific productized offering for deploying ZT via its Google Cloud Platform properties and/or G Suite. Enterprises can build their own ZT infrastructure using Google phones, cloud, app marketplace, and other available offerings.

  While the vendor's capability is nearly limitless in relation to scale, there is a requirement to use an almost entirely Google technology stack to get the full power of the solution. Despite the popularity of the BeyondCorp approach, reference customers noted the go-to-market for the solution as "confusing." Enterprises from SMBs to mega-organizations can benefit from the power that the Google platform offers, regardless of the confusing nomenclature.

- **BlackBerry brings an innovative approach to Zero Trust.** While other vendors in this space have taken a position of working to employ microsegmentation and end user security at the big infrastructure or endpoint level, BlackBerry has found innovative ways to deploy ZT through containerized workspaces. The vendor's partnership with Awingu and other providers offers an integrated, easy-to-use and manage ZT platform that is deployed in the browser. This means that the heft of security configuration and management for enterprises is effectively minimized, and end users have only to download an agent and use the system to operate in a self-contained ZT environment.

  End users appreciate the solution for the ease of use, and reference customers noted that the ability to employ solutions all the way from DLP to SSO is minimally invasive. The days of enterprise users jumping on their BlackBerry device to send emails may be gone, but the days of BlackBerry as a key Zero Trust platform have just arrived. While the company is well-aligned to the future of ZT, the solution relies on a variety of partners and integrated technologies, which, if changed or modified, could be problematic for customers. Enterprises looking for easy-to-use ZT capabilities built into a browser-based solution should seek out BlackBerry's technology stack.

- **Forcepoint's analytics provide a powerful lens to observe ZT.** Forcepoint's ZT platform is powered by the vendor's intelligent analytics and its focus on user behaviors. While others in this space have shifted their focus to pushing controls outward to the entity and users, Forcepoint has dialed in its insight and analysis to analyze user activities as they operate in a ZT infrastructure. Forcepoint's platform allows admins to see, with context, all of the actions that a user is performing which might be indicative of threatening or malevolent actions and then employ a fix.

  The overall alignment and long-term focus of Forcepoint for ZT remains slightly muddled as the company has had many leadership changes and has not invested heavily in ZT-related additions or acquisitions in quite some time. Forcepoint has the platform to meet the needs of enterprises that want intelligent and focused UBA and advanced insider threat capabilities.

FORRESTER®
© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

CONTENDERS

› **Ionic Security leans in on Zero Trust for developers and third parties.** Ionic is primarily a data security provider that has significant chops for those seeking to enable Zero Trust for developers, contractors, and third parties. The vendor's system makes granular authorization easy and helps make encryption more achievable at scale. By solving that extremely important problem, Ionic makes ZT more achievable at a broader scale and helps organizations solve the problem of making outside connections touching an infrastructure to be more ZT powered, and by integrating with major cloud providers like Microsoft Azure and Google the platform can aid in data security issues there as well.

Ionic is fairly new to the Zero Trust space, but the vendor has a strong ZT future. This is evidenced by the vendor's capabilities demonstration and the feedback provided by customer references as Ionic adds in other needed technical assets and capabilities. Reference customers remarked that Ionic seemed to "stop at encryption" and they weren't often aware of the vendor's capabilities beyond that single capability. Ionic offers more than just that and is positioned to be a real ZT powerhouse should it push those offerings into the market with a clear alignment to ZT enablement. Enterprises that struggle with implementing and maintaining consistent data handling requirements would be wise to explore Ionic's offerings.

› **Proofpoint adds to its ZT capabilities via smart acquisitions.** A relative newcomer to the ZT space, Proofpoint has invested heavily to help its customers in their pursuit of Zero Trust. With the acquisitions of ObserveIT and Meta Networks last year Proofpoint added additional insight into the analysis and insider threat-ish areas of Zero Trust for clients. The tie-in from the Meta Networks acquisition aids the Proofpoint capabilities for helping to secure user access and links into the network pillar of ZTX.

Proofpoint's platform is aimed almost entirely at providing the administrators deep insight into the "who, what, where" side of Zero Trust analytics and is very useful there. The vendor also has strong capabilities for securing email systems and inboxes for organizations, which is a last mile for many organizations with respect to phishing. Continued integration of the functionality gained via acquisition will increase Proofpoint's capacity to aid organizations' ZT efforts. Reference customers, however, noted the disjointed nature of implementation as an issue. They also stated that the recent acquisitions have "yet to bear fruit" for current users of the platform. Enterprises that are extending from email security to a Zero Trust framework, and existing Proofpoint customers, should consider Proofpoint.

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

Evaluation Overview

We evaluated vendors against 19 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, APIs, and future state of Zero Trust infrastructure.
- **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. We evaluated ZTX vision and strategy, ZTX roadmap and differentiation, ZTX advocacy, market approach, ZT mission completion, and ZT technology expansion.
- **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 the portfolio, and portfolio growth rate.

VENDOR INCLUSION CRITERIA

Forrester included 15 vendors in the assessment: Akamai Technologies, Appgate, BlackBerry, Cisco, Forcepoint, Google, Guardicore, Illumio, Ionic Security, Microsoft, MobileIron, Okta, Palo Alto Networks, Proofpoint, and Unisys. Each of these vendors has:

- **Notable revenues.** Vendors must have at least $20 million in ZT-specific revenue.
- **ZTX technical capabilities.** Vendors must have capabilities in at least four 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 (top 50% of yearly inquiries based on end user interactions) 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.

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

› **Public ZT initiative references.** Vendors must have clearly noted and referenceable ZT initiatives (to include but not limited to reference architectures, customer stories, designs, etc.) in the public domain specifically citing how their solution enables ZT.

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.

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

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 July 14, 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] See the Forrester report "The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q4 2019."

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

[3] See the Forrester report "Enhance EX With Zero Trust."

[4] Source: "Palo Alto Networks Closes Acquisition of Evident.io," Palo Alto Networks press release, March 26, 2018 (https://www.paloaltonetworks.com/company/press/2018/palo-alto-networks-closes-acquisition-of-evident-io).

Source: "Palo Alto Networks Closes Acquisition of Secdo," Palo Alto Networks press release, April 24, 2018 (https://www.paloaltonetworks.com/company/press/2018/palo-alto-networks-closes-acquisition-of-secdo).

Source: Ron Miller, "Palo Alto Networks to acquire RedLock for $173M to beef up cloud security," TechCrunch, October 3, 2018 (https://techcrunch.com/2018/10/03/palo-alto-networks-to-acquire-redlock-to-beef-up-cloud-security/).

Source: Ron Miller, "Palo Alto Networks to acquire Demisto for $560M," TechCrunch, February 19, 2019 (https://

FORRESTER®
© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

techcrunch.com/2019/02/19/palo-alto-networks-to-acquire-demisto-for-560m/).

Source: Stephanie Condon, "Palo Alto Networks to acquire Twistlock, PureSec," ZDNet, May 29, 2019 (https://www.zdnet.com/article/palo-alto-networks-to-acquire-twistlock-puresec/).

Source: Ron Miller, "Palo Alto Networks intends to acquire Zingbox for $75M," TechCrunch, September 5, 2019 (https://techcrunch.com/2019/09/04/palo-alto-networks-intends-to-acquire-zingbox-for-75m/).

Source: "Palo Alto Networks Announces Intent to Acquire Aporeto," PR Newswire press release, November 25, 2019 (https://www.prnewswire.com/news-releases/palo-alto-networks-announces-intent-to-acquire-aporeto-300964886.html).

Source: "Palo Alto Networks Completes Acquisition of CloudGenix," PR Newswire press release, April 21, 2020 (https://www.prnewswire.com/news-releases/palo-alto-networks-completes-acquisition-of-cloudgenix-301044699.html).

[5] Source: "Unisys Stealth®: Capture the Flag Challenge," Hackathon, February 26, 2020 (https://www.hackathon.com/event/unisys-stealth--capture-the-flag-challenge-5e3319c1bfeebd001b2de439).

[6] Source: "Participants Unable to Hack Unisys Stealth® Solution During Contest Held at RSA 2020 Conference," PR Newswire press release, March 9, 2020 (https://www.prnewswire.com/news-releases/participants-unable-to-hack-unisys-stealth-solution-during-contest-held-at-rsa-2020-conference-301019105.html).

[7] Source: Michelle Caffrey, "Unisys lands $200M in new contracts in Q1," Philadelphia Business Journal, April 30, 2020 (https://www.bizjournals.com/philadelphia/news/2020/04/30/unisys-lands-200m-in-new-contracts-in-q1.html).

FORRESTER®
© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

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.

ABOUT ILLUMIO

Illumio enables organizations to realize a future without high-profile breaches by preventing the lateral movement of attackers across any organization. Founded on the principle of least privilege in 2013, Illumio provides visibility and segmentation for endpoints, data centers or clouds. The world's leading organizations, including Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite, trust Illumio to reduce cyber risk. For more information, visit https://www.illumio.com/what-we-do and engage us on LinkedIn and Twitter.