WAVE REPORT

The Forrester Wave™: Zero Trust Platform Providers, Q3 2023

The 14 Providers That Matter Most And How They Stack Up

September 19, 2023

By Carlos Rivera, Heath Mullins with Joseph Blankenship, Dan Beaton, Kara Hartig

FORRESTER®

Summary

In our 28-criterion evaluation of Zero Trust platform providers, we identified the most significant ones and researched, analyzed, and scored them. This report shows how each provider measures up and helps security professionals select the right one for their needs.

Zero Trust Platforms Consolidate And Centralize Zero Trust Security Controls

Organizations are developing strategies and creating roadmaps for implementing and maturing Zero Trust (ZT) architecture. Many of these enterprises suffer vendor sprawl, overlapping capabilities, and security gaps. There is a need to consolidate controls, enable interoperability, and integrate technologies without compromising capabilities. Zero Trust platforms (ZTPs) enable ZT business and security outcomes by offering a unified, comprehensive approach to operationalizing the ZT technology ecosystem. Whether it's in the early stages of the ZT journey or while maturing key areas, ZTPs unite disjointed functions and provide supplemental capabilities and services to enrich cross-functional operations and simplify ZT adoption. No single solution can provide all capabilities needed for an effective ZT architecture. ZTPs combine key ZT functionalities instead of requiring individual bolt-on tooling. This establishes a more harmonious architecture through native and third-party integrations that don't seek to rip and replace but rather anchor and concenter.

As a result of these trends, ZTP customers should look for providers that:

- **Simplify centralized management and usability.** Many vendors claim centralized management, but few provide a shared universal UI and user experience (UX) across multiple ZT components. Security and risk (S&R) pros benefit from uniform visibility, management, and implementation of controls that improve analytics, reduce complexity, and enhance analyst experience (AX). Improving AX relies on streamlining the analyst workflow and providing valuable training on the tools and processes. The ease of use through centralized management allows S&R pros and security analysts to discover, explore, classify, determine, and execute without having to launch multiple disparate UIs or other consoles. Consolidation not only creates a unified control plane but also provides native tools and services to assist with, train on, and increase cyberhygiene awareness, ensuring ZT best practices align with industry standards and requirements.
- **Offer flexible deployment models supporting diverse hybrid architectures.** Gone are the days when enterprises lived and operated within the confines of a traditional perimeter-based network defense. Organizations continue to adopt cloud-based software and services and migrate resources to the cloud. Other organizations either can't move to the cloud or want to retain a level of control by maintaining resources locally. Most organizations will manage and secure hybrid architectures that include on-premises and virtual environments for the foreseeable future. ZTP vendors curate their offerings to address cloud, virtual,

and on-premises by providing flexible deployment modes for key security components that are manageable from a UI hosted in the cloud or deployed locally to meet organizations' individual requirements.

- **Incorporate ZTNA and/or microsegmentation capabilities natively.** As cornerstone technologies or capabilities, Zero Trust network access (ZTNA) and microsegmentation enable core ZT principles — enforcing least privilege, implicitly denying access, and applying comprehensive visibility. ZTNA reduces reliance on legacy VPNs by providing secure end-to-end access to cloud-based, software-as-a-service (SaaS), and on-premises resources. Microsegmentation enables granular access control for assets and applications by creating microperimeters. These technologies enable organizations to deploy ZT controls without negatively impacting the workforce and business operations.

Evaluation Summary

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

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

Figure 1

Forrester Wave™: Zero Trust Platform Providers, Q3 2023

*A gray bubble or open dot indicates a nonparticipating vendor.

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Figure 2

Forrester Wave™: Zero Trust Platform Providers Scorecard, Q3 2023

	Forrester's weighting	Absolute Software	Akamai Technologies	Broadcom*	Check Point Software Technologies	Cisco Systems	Cloudflare	Forcepoint*
Current offering	50%	1.87	3.13	1.81	4.01	2.83	2.97	1.54
Network security	5%	3.00	4.20	1.80	3.80	3.00	1.80	1.80
Zero Trust ecosystem	10%	1.00	3.00	1.00	3.00	3.00	3.00	3.00
Centralized management and usability	10%	1.00	3.00	1.00	5.00	1.00	3.00	1.00
Least-privilege enforcement on all entities	10%	1.00	3.00	3.00	5.00	3.00	3.00	1.00
Visibility and analytics	5%	1.00	3.00	1.00	5.00	5.00	3.00	1.00
Automation and orchestration	5%	3.00	3.00	1.00	3.00	3.00	3.00	1.00
Data security	5%	3.00	3.00	3.00	5.00	3.00	3.00	3.00
Workload/application security	5%	3.00	3.00	1.00	3.00	3.00	3.00	1.00
Hybrid workforce enablement and protection	10%	3.00	3.00	1.00	3.00	3.00	5.00	1.00
Device security	5%	3.00	5.00	3.00	5.00	3.00	1.00	1.00
People/identity security	5%	1.00	3.00	3.00	3.00	5.00	3.00	3.00
Deployment	5%	2.40	2.40	2.40	4.40	3.60	1.60	3.00
Analyst experience	10%	1.00	3.00	1.00	5.00	1.00	3.00	1.00
Product security	5%	3.00	3.00	3.00	3.00	3.00	3.00	1.00
APIs and other integrations	5%	1.00	3.00	3.00	3.00	3.00	3.00	1.00

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

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

	Forrester's weighting	Absolute Software	Akamai Technologies	Broadcom*	Check Point Software Technologies	Cisco Systems	Cloudflare	Forcepoint*
Strategy	50%	2.10	3.00	2.00	3.60	3.30	3.20	1.60
Vision	25%	3.00	3.00	1.00	5.00	3.00	3.00	1.00
Innovation	5%	1.00	3.00	1.00	3.00	3.00	5.00	3.00
Roadmap	10%	1.00	3.00	3.00	3.00	3.00	5.00	3.00
Partner ecosystem	5%	1.00	3.00	1.00	5.00	5.00	3.00	3.00
Adoption	25%	3.00	3.00	3.00	3.00	3.00	3.00	1.00
Pricing flexibility and transparency	5%	3.00	3.00	3.00	3.00	3.00	5.00	1.00
Supporting services and offerings	10%	1.00	3.00	3.00	3.00	5.00	1.00	3.00
Community	15%	1.00	3.00	1.00	3.00	3.00	3.00	1.00
Market presence	0%	2.50	3.00	1.50	5.00	2.50	3.50	1.50
Revenue	50%	1.00	3.00	2.00	5.00	3.00	4.00	2.00
Number of customers	50%	4.00	3.00	1.00	5.00	2.00	3.00	1.00

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

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

	Forrester's weighting	Fortinet	Google	Microsoft	Palo Alto Networks	Trend Micro	VMware*	Zscaler
Current offering	50%	3.01	3.31	3.57	4.54	3.64	1.72	3.10
Network security	5%	3.80	1.80	1.00	3.80	3.80	2.20	3.00
Zero Trust ecosystem	10%	3.00	3.00	3.00	5.00	3.00	1.00	3.00
Centralized management and usability	10%	3.00	3.00	3.00	3.00	5.00	1.00	3.00
Least-privilege enforcement on all entities	10%	3.00	3.00	3.00	5.00	3.00	3.00	3.00
Visibility and analytics	5%	3.00	3.00	5.00	5.00	5.00	1.00	3.00
Automation and orchestration	5%	3.00	3.00	5.00	5.00	5.00	1.00	3.00
Data security	5%	1.00	3.00	5.00	3.00	3.00	1.00	3.00
Workload/application security	5%	1.00	3.00	3.00	5.00	3.00	1.00	3.00
Hybrid workforce enablement and protection	10%	3.00	5.00	5.00	5.00	3.00	3.00	3.00
Device security	5%	3.00	3.00	5.00	5.00	3.00	1.00	3.00
People/identity security	5%	5.00	5.00	5.00	3.00	3.00	3.00	3.00
Deployment	5%	4.40	2.40	2.40	5.00	3.00	2.20	3.00
Analyst experience	10%	3.00	3.00	3.00	5.00	5.00	1.00	3.00
Product security	5%	3.00	5.00	3.00	5.00	3.00	1.00	5.00
APIs and other integrations	5%	3.00	3.00	3.00	5.00	3.00	3.00	3.00

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

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

	Forrester's weighting	Fortinet	Google	Microsoft	Palo Alto Networks	Trend Micro	VMware*	Zscaler
Strategy	50%	2.10	3.10	4.10	4.20	3.10	1.40	3.80
Vision	25%	3.00	3.00	5.00	3.00	3.00	1.00	3.00
Innovation	5%	3.00	5.00	3.00	3.00	3.00	3.00	3.00
Roadmap	10%	3.00	3.00	5.00	5.00	3.00	1.00	3.00
Partner ecosystem	5%	3.00	5.00	3.00	3.00	3.00	3.00	3.00
Adoption	25%	1.00	3.00	3.00	5.00	3.00	1.00	5.00
Pricing flexibility and transparency	5%	1.00	1.00	1.00	3.00	5.00	1.00	3.00
Supporting services and offerings	10%	3.00	3.00	5.00	5.00	3.00	3.00	3.00
Community	15%	1.00	3.00	5.00	5.00	3.00	1.00	5.00
Market presence	0%	3.50	2.50	4.00	3.50	3.00	1.50	4.50
Revenue	50%	4.00	3.00	4.00	3.00	3.00	2.00	5.00
Number of customers	50%	3.00	2.00	4.00	4.00	3.00	1.00	4.00

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

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Vendor Offerings

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

Figure 3

Evaluated Vendors And Product Information

Vendor	Product evaluated
Absolute Software	The Absolute Trust Solution
Akamai Technologies	Akamai Zero Trust Security
Broadcom	Broadcom Zero Trust Network Access
Check Point Software Technologies	Check Point Infinity
Cisco Systems	Cisco Duo
Cloudflare	Cloudflare One
Forcepoint	Forcepoint ONE Zero Trust Network Access
Fortinet	Fortinet Zero Trust Platform
Google	Google Cloud Platform, BeyondCorp Enterprise
Microsoft	Microsoft Zero Trust Platform
Palo Alto Networks	Palo Alto Networks Zero Trust Framework
Trend Micro	Trend Micro Zero Trust Secure Access
VMware	VMware Zero Trust Platform
Zscaler	Zscaler Zero Trust Exchange

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Vendor Profiles

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

Leaders

- **Palo Alto Networks makes network and security convergence a no-brainer.** Since its founding more than 18 years ago, Palo Alto Networks has steered clear of conformity with innovations that began with the introduction of the industry's first next-generation firewall in 2008. The vendor continues this strategy by providing network and security capabilities through its Zero Trust Framework, which leverages the Prisma, Strata, and Cortex solutions with unified management and a dash of AI for IT operations. Palo Alto Networks' prevailing vision to help

enterprises jump-start their ZT journey addresses the struggle organizations face in moving past planning to implementation. Its roadmap, however, is bolder, leaning heavily on the long-term commitment for more AI/ML capabilities to go beyond automated policy creation.

Palo Alto Networks' Zero Trust Framework encapsulates the need to enable and protect a hybrid workforce. One reference customer praised the value of enabling a dynamic and agile workforce to enroll, authenticate, and access resources securely with Prisma Access — deployed as a service through the platform. Agent and agentless deployment options provide a single sign-on (SSO) capability that can take in attributes from multiple identity and access management (IAM) solutions to curate and simplify how users enter credentials and authenticate. The vendor's centralized management is not as consolidated as its competitors', however, and it's sometimes unclear what can and cannot be managed from a single UI. Palo Alto's Zero Trust Framework suits large, established enterprises on a ZT journey with budget for premium network and security capabilities.

- **Microsoft's ZT advocacy shines through its products and supporting services.** Microsoft's modern and holistic approach to ZT has been years in the making. The vendor, along with others in this evaluation, positions its cloud enterprise as a ZTP, emphasizing its efforts to embed ZT principles and methodology into Azure capabilities. Its Copilot theme carries over to a notable vision to provide end-to-end, step-by-step guidance for implementing ZT while leveraging AI. This means customers can take their ZT journey with Microsoft in lockstep. Microsoft further exemplifies its vision through its roadmap that includes Security Copilot and public previews of its ZTNA. Pricing and licensing ZT that considers individual, disparate components within Azure such as Sentinel remains convoluted and demands a great deal of time and effort to budget effectively.

  Microsoft's omnipresence requires it to align its SaaS capabilities with global standards, regulations, and mandates. The vendor simplifies governance, in particular with comprehensive data security, through its classification and visibility of threats and risks. Microsoft supplements ZT ecosystem capabilities through integration and interoperability with third-party vendors to provide granular control over data usage and transmission. Microsoft's ZTP is a modest coupling of key solutions that do not sit entirely under its E5 license, as noted by reference customers, and currently lacks compelling microsegmentation or a real ZTNA solution. The vendor has plans to finalize development of these capabilities in its roadmap. Organizations already leveraging Microsoft's E5 licenses for security

capabilities are well positioned to get an early start on their ZT journey with add-ons through Microsoft.

- **Check Point Software sets the bar for centralized management and usability.** The network security titan has been delivering network security for just more than 30 years with its hardware and software solutions. While many vendors are shifting focus to an all-cloud offering, Check Point Software Technologies has kept its eye on the current and future needs of supporting ZT in a hybrid architecture. Components of its ZTP deploy on-premises as hardware or software, in cloud SaaS, and virtually to address unique architectural requirements. While its innovation investments are substantial, the vendor focuses on M&A, which leaves in-house R&D murky, compared with its rooted beginnings. Check Point's roadmap highlights network and security plans to expand AI and deep learning for improved detection and prevention across threat vectors.

  Check Point's UI provides consistent experience regardless of whether the admin is operating on the Infinity Portal or within individual components. Check Point Infinity Portal provides ease of use and simplicity to network and security professionals without the need to open multiple windows or tabs to perform daily tasks. Each component is centrally managed in a single management console and categorized into pillars to reduce complexity when navigating different solutions. Check Point's microsegmentation capability leverages Azure to simplify network-level deployments but lacks a discernable host-level microsegmentation. The vendor provided one reference customer that has not yet implemented the ZTP. Large enterprises with existing Check Point installations would do well to consider the additional capabilities offered in the platform.

Strong Performers

- **Zscaler has transparent product security but lacks consistent customer experience.** At the peak of the COVID-19 pandemic, Zscaler had great success with ZTNA and provision of secure access for enterprises' remote workers but has struggled to make a case for on-premises use cases. The vendor's strategy to increase client and market penetration focuses on helping customers maximize the value of their Zscaler deployments through training, customer success, product configuration and security audits, and seeding of advanced features in entry-level bundles. The vendor has split messaging that includes delivering a seamless, secure exchange of information and "zero-touch, Zero Trust," with the former representing a more realistic and achievable strategy. Its roadmap highlights enhancements spanning multiple objectives such as stopping

cyberattacks using AI/ML to automate quarantine with remote browser isolation (RBI) and sandboxing.

Zscaler's ZTP, Zero Trust Exchange, combines its secure web gateway (SWG), data loss prevention (DLP), ZTNA, and cloud access security broker (CASB) offerings. Its willingness to provide a software bill of materials at contractual signing allows customers to maintain product security with detailed information that includes SKUs, subcomponents, and licenses. Zscaler has made efforts to consolidate through its Client Connector, which controls and manages Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) via a single agent. However, ZIA and ZPA are still treated as separate components rather than a single solution, which creates an irksome customer experience: Reference customers lament dealing with two separate consoles with "some overlap." Additionally, Zscaler's Zero Trust Exchange is still a cloud-first solution with no real on-premises deployment options outside of its Branch Connector. Enterprises on the path to cloud migration with little or no need to support legacy systems may look to Zscaler to begin or advance their ZT journey.

- **Trend Micro's Vision One enhances AX through analytics but undersells its ZTNA.** Trend Micro has come a long way from its humble beginnings as an antivirus solution. The cybersecurity software company has become somewhat of an unsung hero of security control and visibility for network, endpoints, and applications/workloads. The cost-to-value ratio Trend provides through its native solutions and extensive integrations makes it a viable solution for budget-conscious customers. The vendor has been methodical with its Vision One strategy to operationalize ZT through advanced analytics. However, the vendor's secure access capabilities are underutilized. Trend Micro's roadmap complements its vision with continued emphasis on improving visibility and analytics with modest secure access updates.

  Advanced visibility and analytics are strengths of Trend Micro's Vision One, enabling the vendor to deliver a robust AX. Reference customers laud the value of Vision One in optimizing visibility and control. Much of the information an analyst needs is accessible in a single console. This console provides a risk-scoring metric based on user and device behavior that informs accurate risk-based policy creation in the platform or in third-party solutions via integrations. Its ZTNA and SWG capabilities enable microsegmentation at the network level for user-to-app control. The solution lacks the ability to consider geolocation beyond IP-based and app-to-app communication to effectively enforce microperimeters. Organizations

starting their ZT journey and needing a solution for advanced visibility and analytics to establish a baseline should evaluate Trend Micro.

- **Google's BeyondCorp is the epitome of ZT, but enterprises need to buy into the vision.** Tech titan Google has evolved from a simple search engine into a prominent cloud hyperscaler, security vendor, and ZT advocate that pioneered BeyondCorp. The vendor's commitment to innovation is underpinned by continuous expansion of its partner ecosystem and dedication to advancing native capabilities. Its pricing and transparency are unwieldy. It has multiple models that force customers investing in Google's ZT vision to decide if BeyondCorp Enterprise fits an enterprise that isn't cloud first or if separate pay-as-you-go components of the overarching Google Cloud Platform are enough for hybrid and on-premises environments. Google's roadmap focuses on continuous expansion for compliance coverage, partner integrations, cloud-native security capabilities, and secure enterprise browsers.

  Google's ZT approach is a testament to the effective application of the information security model's core principles. The vendor enables and protects hybrid workforces using Chrome on every device, thereby providing an agentless capability to secure and protect users and their interactions, regardless of location. Reference customers highlight the simplicity of supporting and managing bring-your-own-device, especially when combined with the IAM and DLP offerings. Through BeyondCorp Enterprise, admins make use of disparate solutions under a single console to monitor and perform deep investigative actions. Google's ability to extend to on-premises depends on the presence of Chrome or the ability to deploy an app connector to route traffic to its cloud enterprise. Google BeyondCorp Enterprise is ideal for organizations all in on cloud security solutions that leverage Google's cloud infrastructure and Chrome to secure the hybrid workforce.

- **Cloudflare's innovation is unbound, but change management is counterintuitive.** As one of the younger vendors in this evaluation, Cloudflare has demonstrated continued growth from a humble online honeypot solution in 2009 to its official 2010 launch and now a fully cloud-native ZTP. The vendor's ZTP, Cloudflare One, unifies the visibility and management of the ZTNA, CASB, DLP, and web application firewall (WAF) with plans to continue adding and integrating more functions and capabilities. Cloudflare's roadmap reflects the company's dedication to innovation that takes a customer-led approach in addressing growing trends and unique demands. The vendor's vision, however, is a rather familiar story of becoming the control plane of choice for organizations.

As an access broker and domain name system reverse proxy, Cloudflare One does well in providing a centralized and consolidated platform to manage and orchestrate many of its cloud-native solutions for ease of use and quicker deployments. Various network, DLP, and access control policies are managed from a single console, allowing customers to quickly deploy and protect against internet-born threats. Cloudflare's deployment modes are 100% SaaS-only with connections to other cloud and on-premises resources facilitated only through app connectors in parallel to existing architecture. Auditing configuration management is cumbersome and not intuitive, with one reference customer describing it as "not fully scope" and having to sift through audit trails. Midsize-to-large enterprises with a cloud-first initiative to actively migrate resources and replace legacy WAN and VPN solutions should evaluate Cloudflare One.

- **Akamai Technologies leads with microsegmentation, but its integrations lag.** Akamai Technologies' acquisition of Guardicore in 2021 helped position the vendor as a viable ZTP provider. The company continues its M&A strategy to incorporate more capabilities and supplement existing ones, fulfilling its common, albeit standard, vision of simplifying ZT. Most appealing is the company's decision to stand up a dedicated ZT business unit (BU), led by Guardicore's former CEO, to improve Akamai Technologies' capabilities and integrations with a ZT mindset. This BU primarily addresses internal R&D and doesn't add much in terms of a dedicated support team for organizations beginning or actively implementing a ZT architecture. Akamai Technologies' roadmap reflects planned enhancements of its products to improve integration, coverage, scale, ease of use, and security.

  Akamai Technologies' Zero Trust Security platform is composed of its ZTNA, SWG, and microsegmentation technologies with integrations including its multifactor authentication (MFA) and WAF (web application and API protection) solutions. Its Akamai Guardicore Segmentation continues to be a winning asset for enterprises that value visibility and native firewall capabilities for microsegmentation. Reference customers noted improved UX for DevOps and security because it "put segmentation on top of something without having to rearchitect the system." Akamai Technologies' technology ecosystem also integrates with third-party solutions. Full native integration and feature parity, however, are yet to surface. Reference customers voiced discontent with the need to maintain multiple agents and separate supporting services. Organizations looking to take the stress out of microsegmentation can leverage Akamai Technologies' Zero Trust Security platform.

- **Cisco Systems has a broad product portfolio but lacks true centralized management.** Networking and security stalwart Cisco has a long history of delivering for customers. Its vast partner ecosystem allows the vendor to broaden buying opportunities for customers while delivering the bulk of its bookings and SaaS revenues. Cisco's vision is to deliver better access control and security to enterprises to frustrate attackers. However, the vendor has yet to truly embody that vision in its broader platform, which ultimately frustrates admins attempting to integrate existing architecture. Cisco's community strategy is noteworthy, but it struggles to gain influence: Its coverage of ZT is not as consistent or impactful as others'. Its roadmap hints at eventual delivery of consistent UX but falls short on consolidation and centralized management.

  Cisco's ZTP consists of Duo, Identity Services Engine (ISE), Secure Client, Secure Workload, Umbrella, and other Cisco solutions integrated by its pxGrid and product APIs. Duo effectively enforces least privilege on all entities through contextual policies. It now integrates with ISE without the need for a proxy, which enables cohesive SSO with passwordless MFA support for local and remote workforces. The solution, however, lacks any real centralized management. Unlike others in this evaluation, Cisco still has a fragmented control plane that requires a great deal of time and skill to manage and maintain. Third-party integrations are notoriously difficult and have become a theme over the years, with one reference customer saying it was "always" a challenge. The integration process is not as fluid for third-party products that don't support pxGrid. Enterprises heavily invested in the Cisco technology ecosystem should consider the vendor for ZTP.

Contenders

- **Fortinet provides cost-effective network security but deficient workload security.** Best known for its firewalls, Fortinet has since expanded its coverage through strategic acquisitions and some organic growth. Fortinet's vision focuses on network and security operations center (SOC) interoperability, with an emphasis on interoperability among the many components the vendor offers. Fortinet falls short on its community because it offers little to no peer discussion, guidance, or awareness for the advancement of ZT beyond its product capabilities. Its roadmap is underwhelming and provides entry-level ZT pillar-focused feature updates and capabilities that tie into what it calls "neural network learning," which leverages AI/ML and analytics. Although the vendor is known for providing value at low costs, the FortiFlex point-based system has mute fanfare for a pricing model that makes sense on paper.

Fortinet's components all leverage its FortiOS, which is held in high regard for being easy to use, implement, and manage, thereby reducing the need for admins to relearn disparate UIs for multiple components. This translates into its platform that optimizes network security, allowing admins to gain greater visibility and control of FortiGates and FortiAnalyzer across cloud, virtual, and on-premises environments centrally through FortiManager. Fortinet shines with on-premises environments and can support hybrid networks. However, cloud deployments are not as conclusive, with a reference customer noting capabilities — such as CASB — are not fully developed, affecting its ability to provide effective workload/application security. Enterprises of any size with multiple Fortinet network security solutions will gain value from the vendor's FortiManager component of its ZTP offering.

- **Absolute Software's self-healing security shows promise, but new innovation is scant.** Absolute Software was ahead of its time, becoming the sole cybersecurity software that is factory embedded in endpoints. Finding success in the education sector, the company branched off into other public and private market sectors. Crosspoint Capital finalized acquisition in July 2023, taking the vendor private. Absolute Software's vision for resilient self-healing security is as unique as its capabilities that automate endpoint and network connectivity restoration. However, the vendor offers little innovation, relying on its reputation rather than aligning with current trends and future needs. Absolute Software's roadmap is simple, focusing on mostly table stakes enhancements to improve monitoring with AI, reduce attack surface, and ease deployment.

  The Absolute Zero Trust Solution is built on the vendor's Secure Endpoint and Secure Access solutions, tightly integrating with its SWG. Because it is embedded on devices by default, the vendor is well positioned to provide effective data and device security for managed devices leveraging a single agent to enforce access and compliance policies at the endpoint. Reference customers praise its effectiveness in protecting and securing remote workers and devices. Absolute Software requires that endpoints install and/or register the agent on devices, but unmanaged endpoints are not given any real agentless or clientless alternative for limited or just-in-time/just-enough resource access. Absolute Software doesn't prioritize data security at rest and only offers full-disk encryption via a third-party integration. Organizations with more restrictive requirements and desire to extend network access control capability to the endpoint should evaluate Absolute Software.

- **Broadcom offers broad coverage and an ambiguous vision for its platform.** Broadcom's acquisitions of CA Technologies and Symantec effectively created a one-stop shop for all things security. The vendor's overarching market approach is to focus on a limited set of very large organizations, which initially led to a mass exodus of smaller customers to other vendors. The vendor's ZTP strategy lacks a definitive long-term outlook and maintains a level of segregation of its security offerings into individual segments with short-term enhancements that are reactionary rather than innovative. Broadcom's roadmap, however, seeks to integrate internal product families into a platform via a unified Symantec console slated for release in 2024 in hopes of attracting new customers.

  Broadcom's Symantec ZTP includes mature products, such as the CASB; cloud security gateway (CSG); ZTNA; identity, credential, and access management; endpoint; and DLP with multiple deployment options including cloud, on-premises, and hybrid networks. The CSG and CASB components are of particular note with reverse proxy and extensive application coverage available without the need for third-party integrations. DLP functionality provides customers with the option of performing scans at the endpoint, in the cloud, or on-premises, creating an avenue for specific deployment requirements in complex environments. The UI is easy to understand but dated. Broadcom declined to participate in the full Forrester Wave evaluation process.

Challengers

- **Forcepoint makes headway with ZTE elements but leaves other aspects by the wayside.** Forcepoint, originally founded as a reseller in 1994, morphed through M&A to emerge as a platform security vendor focused on data security, ZTNA, SWG, and RBI. Most recently, the vendor spun off its government business to TPG after Francisco Partners acquired it from Raytheon Technologies. Forcepoint's strategy primarily focuses on enhancing its Zero Trust edge (ZTE) offering, while leaving other ZTP aspects such as its hardware-based solutions by the wayside to maintain stronger on-premises network security. Forcepoint lags in innovation, focusing on integrating acquisitions and building solutions to support current market needs.

  Forcepoint offers multiple products within the ZTP space such as data classification, DLP, user behavior analytics, ZTE, and firewalls. Functionality is on par with other vendors' in the space but lags from a platform perspective because the onus is on SOC analysts to correlate the disparate telemetry information.

Multiple consoles are required to paint a picture, resulting in an extremely manual process for analysts during provisioning or while responding to an incident in real time. Midsize-to-large enterprises and current Forcepoint customers would benefit from evaluating this combined offering. Forcepoint declined to participate in the full Forrester Wave evaluation process.

- **VMware has solid workload protection but needs a more cohesive offering.** VMware is best known for providing the flexibility to deploy virtual machines just about anywhere. The vendor's vision ties to ZT and the ability to provide coverage across multiple pillars of the ZT model. VMware's installed base across most organizational departments (e.g., security, enterprise IT, and vendor virtual-machine-based offerings) provides deep insight into virtual networks and endpoints through network security solutions that include its NSX software-based firewalls. Its acquisition of Carbon Black allowed it to add an endpoint detection and response (EDR) component to its offering, further expanding its endpoint security coverage. The roadmap lags others' in this evaluation and provides some enhancements to VMware-specific capabilities including additional third-party integrations and EDR enhancements for Carbon Black. Broadcom's pending acquisition of VMware may also impact the vendor's strategy, roadmap, and go-to-market approach if Broadcom's previous acquisitions are any indication of the path forward.

  VMware's workload protection capabilities are widely used in cloud, multicloud, and hybrid deployments and have become the de facto standard for cloud migrations. Cloud configuration management, security, governance, and lifecycle management all feature heavily in the product offerings. However, VMware provides no real ZTP solution that unifies its disparate solutions. Organizations that utilize VMware solutions, particularly for virtualized environments or with self-hosted requirements, should investigate VMware's ZTP offering. VMware declined to participate in the full Forrester Wave evaluation process.

Evaluation Overview

We grouped our evaluation criteria 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, totality of the ecosystem, centralized management, visibility and analytics, automation and orchestration, device security, AX, and integrations.

- **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. We evaluated vision, innovation, roadmap, partner ecosystem, adoption, and pricing flexibility and transparency.
- **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's total revenue for the product and the number of current customers.

Vendor Inclusion Criteria

Each of the vendors we included in this assessment has:

- **Strong enterprise support for ZTP functionality.** Vendors must natively provide core functions of a ZTP across a minimum of four ZT domains (pillars) and must include a ZTNA and/or microsegmentation capability. Vendors must also have recent and ongoing adoption among enterprise customers of ZT capabilities that can operate in on-premises, cloud, and hybrid environments.
- **A generally available ZT product as of May 25, 2023.** Forrester did not factor in any functionality released after May 25, 2023. All functionalities were generally available for purchase, not in beta or limited release. The platform was delivered as a product or as-a-service software, not a managed service.
- **A platform that addresses at least three core ZT use cases.** The ZTP must offer a robust foundation to address three or more core use cases across a heterogeneous environment that include enabling and protecting hybrid workforces, monitoring and securing network traffic across the enterprise, preventing lateral movement of unauthorized activity, enforcing least privilege on all entities, and centrally managing key security controls.
- **Mindshare among Forrester's enterprise clients.** The solution has sparked interest, in the form of mentions and inquiries, among Forrester's client base over the past 12 months; end users frequently mention shortlisting the product; and other vendors mention the evaluated vendor as a frequent competitor in the market.
- **Substantial ZT revenue.** We required that vendors have at least $200 million in annual revenue from the ZT platform market in the past four quarters across two or more geographical regions.
- **ZT advocacy.** Vendors advance, engage in, and leverage the operationalization of ZT as an ecosystem to address growing customer needs and challenges that include applying ZT concepts and principles internally through solutions that are part of a marketed ZTP.

Supplemental Material

Online Resource

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

The Forrester Wave Methodology

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

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

We include the Forrester Wave publishing date (quarter and year) clearly in the title of each Forrester Wave report. We evaluated the vendors participating in this Forrester Wave using materials they provided to us by June 14, 2023, and did not allow additional information after that point. We encourage readers to evaluate how the market and vendor offerings change over time.

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

Integrity Policy

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

FORRESTER®

We help business and technology leaders use customer obsession to accelerate growth.

FORRESTER.COM

Obsessed With Customer Obsession

At Forrester, customer obsession is at the core of everything we do. We're on your side and by your side to help you become more customer obsessed.

Research

Accelerate your impact on the market with a proven path to growth.

- Customer and market dynamics
- Curated tools and frameworks
- Objective advice
- Hands-on guidance

Learn more.

Consulting

Implement modern strategies that align and empower teams.

- In-depth strategic projects
- Webinars, speeches, and workshops
- Custom content

Learn more.

Events

Develop fresh perspectives, draw inspiration from leaders, and network with peers.

- Thought leadership, frameworks, and models
- One-on-ones with peers and analysts
- In-person and virtual experiences

Learn more.

FOLLOW FORRESTER

Contact Us

Contact Forrester at www.forrester.com/contactus. For information on hard-copy or electronic reprints, please contact your Account Team or reprints@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

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