IDC MarketScape

IDC MarketScape: Worldwide Network Edge Security as a Service 2023 Vendor Assessment

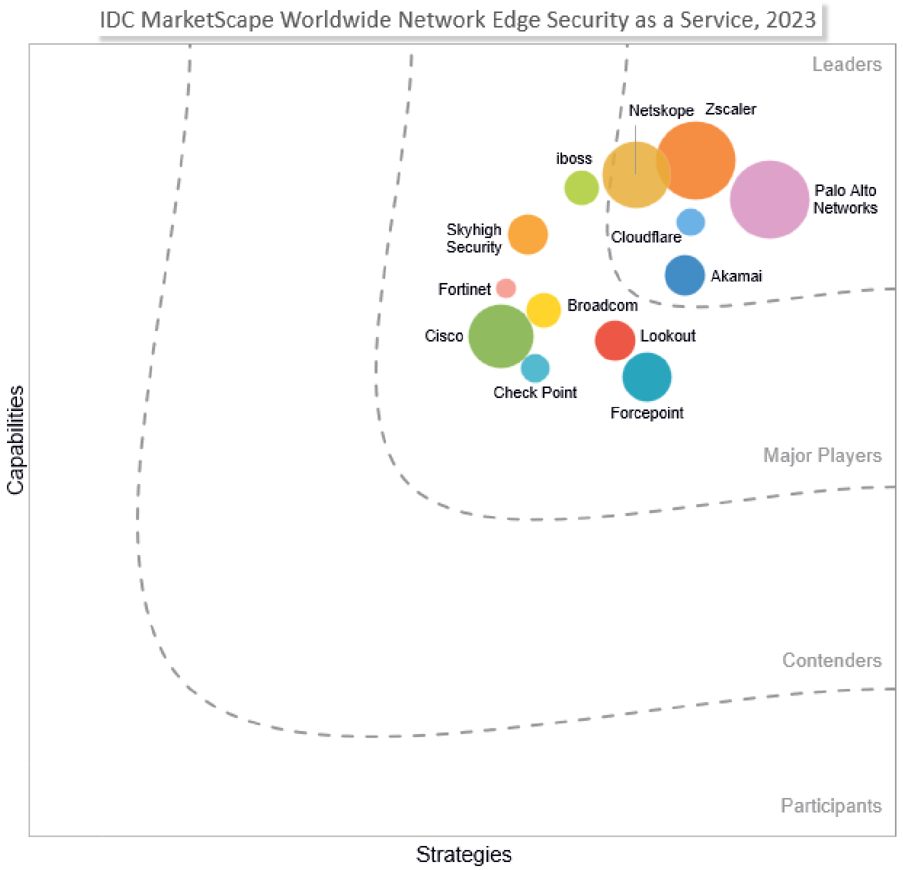
Pete Finalle Christopher Rodriguez

THIS IDC MARKETSCAPE EXCERPT FEATURES ZSCALER

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Network Edge Security as a Service Vendor Assessment



Source: IDC, 2023

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

June 2023, IDC #US50723823e

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Network Edge Security as a Service 2023 Vendor Assessment (Doc # US50723823). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Essential Guidance, Vendor Summary Profile, Appendix and Learn More. Also included is Figure 1.

IDC OPINION

The network security market is in the process of a much-needed convergence trend. Security vendors have shifted from a focus on a la carte, individualized security services to a consolidated, cloud-delivered network security platform that treats individual services as optional modules. IDC refers to this integrated security services platform as network edge security as a service (NESaaS). At its core, NESaaS includes three key capabilities: secure web gateway (SWG), cloud access security broker (CASB), and zero trust network access (ZTNA). These core capabilities address key use cases that are most cited as top-of-mind concerns for securing users and their access and devices:

- The protection of users accessing the web from malware, phishing, and other data theft, risky, or unapproved activities
- The security and privacy of users accessing internal applications
- The security and privacy of data accessed and generated in cloud applications

Convergence is not an overnight process, and the definition of NESaaS continues to evolve. Vendors also incorporate existing network security technologies, adapted to the demands of a cloud delivery model. Firewall as a service is a pertinent example, as it provides the ability to extend security controls to users, resources, device types, and use cases beyond what is possible with SWG, CASB, and ZTNA.

NESaaS also includes optional add-on services to further boost security posture, such as sandboxing, remote browser isolation (RBI), data leakage prevention (DLP), web application firewall (WAF), and deception. These additional capabilities are offered as add-on subscriptions or built-in features, which help buyers address specific use cases.

NESaaS describes a converged security solution that is part of a broader push toward networking and security convergence called "secure access service edge" (SASE). SASE postulates the benefits of integrating networking and security into a single cloud service. Given the complexities of fully converging all networking and network security functions into a single-vendor SASE solution, "secure service edge" (SSE) was introduced as a category of solutions that delivered the security convergence aspects of SASE. NESaaS is most comparable to SSE but is less prescriptive, allowing IT buyers to invest in a converged security solution in part or in full, as dictated by their security transformation plans and timelines. Furthermore, NESaaS treats networking capabilities such as SD-WAN and DEM as optional points of integration, allowing IT buyers to integrate networking functionality where it is most beneficial or practical.

However, enterprise IT buyers also face a practical need to focus on specific security use cases, even through convergence cycles. Often, these buyers will prioritize certain functions over others at various points in their security maturity cycles.

On a strategic level, NESaaS vendors are driven to deliver not just simple consolidation and bundled pricing but also greater value to customers as competitive points of differentiation. True integration of key technologies such as SWG, CASB, and ZTNA is driving improved security posture and outcomes as well as performance benefits that facilitate business goals for productivity and security.

As enterprises work through the process of modernizing their cybersecurity systems, opportunistic adoption of NESaaS is anticipated to accelerate. Furthermore, despite NESaaS promoting a single-solution approach, vendors find substantial success by offering an entry point into the solution — most commonly SWG, which offers a foundational level of protection against modern threats. The strategy allows NESaaS vendors to eventually displace competition as their clients' renewal cycles allow.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

IDC has identified the following key attributes that must be present in the solution to qualify for inclusion in this IDC MarketScape analysis:

- NESaaS solutions may be marketed or sold as SASE or SSE.
- The solution should include a minimum of four of the core NESaaS capabilities: firewall, secure web gateway, cloud access security broker, and virtual private network (VPN)/zero trust network access.
- The core NESaaS functions (firewall, SWG, CASB, and VPN/ZTNA) must be developed/integrated in-house and not through strategic partnerships.
- There are no minimum inclusion requirements for optional components, such as software-defined wide area networking (SD-WAN), digital experience management (DEM), web application firewall, intrusion detection and prevention (IDP), remote browser isolation, sandboxing emulation, deception, email/messaging security, and device security.
- Vendors continue to sell NESaaS as a specific solution with its own SKU alongside discrete standalone products with separate SKUs. While not all NESaaS sales include the full set of NESaaS functionality, partial solutions may be considered in this analysis. In keeping with the spirit of the convergence trend represented by NESaaS, SSE, and SASE, the sales of one-off security services are not considered in this analysis. For example, a one-off CASB sale is considered separately under IDC's CASB market research coverage.

In addition, this IDC MarketScape analysis includes the following requirements for market participation and presence:

- The vendor began selling NESaaS products to customers in January 2022 or earlier.
- NESaaS revenue for CY22 reached a threshold determined by IDC through research or existing data.

ADVICE FOR TECHNOLOGY BUYERS

For IT buyers, the need to consolidate security technologies into a single technology stack is based largely on practical business considerations around tightening budgets, limited staffing, and numerous complex security and regulatory requirements. However, vendors are still in the process of either filling any missing gaps in their security offerings or integrating these solutions into a single coherent architecture. Some competitors are further along than others, which represents a significant portion of the analysis presented in this research document.

As a result, buyers must make a critical decision: Are the benefits of a converged cloud security platform worth the trade-offs that may be required in terms of specific features or best-of-breed functionality? If so, then logical follow-up questions include:

- What specific core features are most valuable to a specific organization?
- Which vendors excel in these desired functional areas?

For IT buyers that are most heavily invested in developing a robust zero trust strategy, it may make sense to focus more heavily on the differentiation in ZTNA capabilities offered by a NESaaS vendor. For more information on ZTNA, see *IDC MarketScape: Worldwide Zero Trust Network Access 2023 Vendor Assessment* (IDC #US50844623, forthcoming), published as a companion to this research document.

Throughout the research process, IDC noted the frequency of SWG adoption as a lead-in for NESaaS adoption, followed closely by ZTNA and then CASB. The progression is logical. SWG provides a crucial foundational layer of protection against threats that end users may encounter throughout the typical workday. Many of these threats, such as ransomware and phishing attacks, are severe risks to the device, sensitive corporate data, and private user data.

ZTNA and CASB are popular complements to SWG. These solutions provide a means for users to access important applications, data, and resources in a secure manner controlled by the IT organization. Both ZTNA and CASB offer specialized protections including granular policy enforcement, data protection, and threat detection and prevention. The key difference is whether the organization owns the application/resource in question or if a cloud provider owns the application/infrastructure. The shared responsibility model for cloud security introduces limitations to the type and extent of controls possible for IT organizations. While ZTNA vendors are working to extend zero trust controls to cloud applications, CASB solutions are designed to provide essential security capabilities, given the technical requirements of cloud environments.

Function-specific concerns aside, IDC notes that cybersecurity cannot exist in a vacuum. Policies and protections must be applied without hampering the IT organization or hindering the end user. The analysis of the NESaaS solutions represented in this IDC MarketScape document places extra emphasis on the ability to integrate multiple disparate technologies into a common platform. That singular goal is expressed in myriad manners, with varying degrees of relevance and impact to buyers.

For vendors, the ability to deliver a single unified agent is a critical value for IT organizations that already face pushback when presented with a requirement to install additional software on end-user devices. Similarly, a single coherent management system is critical to simplify workflows and offload pressure from overtaxed IT organizations, including security analysts. Other factors may not be as immediately obvious to security buyers as a unified agent or management console. For example, IDC takes into account the level of integration "under the hood" that will pay dividends through improved threat detection rates and lower false positives.

Similarly, the importance of the cloud delivery model has been emphasized in this analysis, as poor cloud design or performance can have a hindering impact on IT buyers. Ultimately, these factors have been compared based on outcomes when possible. For example, latency is highly visible and impactful to end users. Thus, while the scale of a vendor's cloud is important, IDC acknowledges the possibility that efficient cloud design may also have a positive impact on the overall user experience.

The IDC MarketScape process is comprehensive and considers factors for success that may not be highly visible to IT buyers but affects their likelihood of project success to varying degrees. As such, market visibility, influence, product development, and other factors are considered under the strategy axis. While these factors may or may not directly influence the security outcomes for a particular buyer, they do directly impact the ability of the vendor and solution to adapt to the next wave of needs – an important consideration in a rapidly developing market such as NESaaS. For a complete overview of the factors considered under the "capabilities" and "strategy" components of the IDC MarketScape research process, see the Strategies and Capabilities Criteria section in the Appendix.

VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

Zscaler

Zscaler is positioned as a Leader in this 2023 IDC MarketScape for worldwide NESaaS.

Zscaler is a specialist in cloud security services, pioneering the SWG-as-a-service market before adding firewall as a service, CASB, DLP, and ZTNA for a complete NESaaS solution.

Strengths

Zscaler offers a suite of cloud services spanning threat prevention, data protection, and performance monitoring capabilities as an integrated offering called Zscaler for Users. At its core, the Zscaler NESaaS solution offers CASB, ZTNA, SWG, firewall as a service, and DLP functionality. Zscaler offers a range of capabilities that can be layered on, including sandboxing analysis, remote browser isolation, WAF, and deception. These solutions are offered in a "good, better, best" licensing subscription model. In the top subscription tier, deception lures are built into client connectors as a passive form of threat detection, and BYOD access can be directed through an isolated browser instance for added protection.

The strength of Zscaler for Users is based on the reliability and performance of the company's cloud infrastructure, which the company has built out for well over a decade. All user and device traffic are passed through the Zscaler Zero Trust Exchange platform for comprehensive visibility and control and to ensure a consistent security posture.

Zscaler for Users is complemented by value-added services including Zscaler Digital Experience (ZDX) for DEM. ZDX provides end-to-end visibility into the user experience and, as a result, measures reliable connections to the Zscaler cloud, SaaS services, the internet, and private applications. ZDX provides AI-driven troubleshooting that rapidly isolates issues from the device, hop by hop, through the network to the application.

Zscaler also provides zero trust connectivity to secure workloads including Zscaler API integrations with popular enterprise SD-WAN solutions. It also provides zero trust connectivity services for the public cloud and branch offices that eliminate the attack surface in the enterprise and provide secure internet access and segmentation for workloads.

The Zscaler NESaaS offering includes the ZPA solution for ZTNA (part of Zscaler for Users). However, the broader Zscaler zero trust suite includes Zscaler for Workloads, comprising Zscaler Posture

Control for CNAPP, Zscaler Workload Communications, and Zscaler for IoT/OT. As a result, the Zscaler zero trust portfolio extends protection across all users, devices, and resources, including external and internal applications.

Challenges

Zscaler Internet Access (ZIA) runs in slightly different datacenters as compared with the ZPA solution for ZTNA. Zscaler builds its cloud to the specifications required to support low-latency and performant applications. However, the implication is that the Zscaler NESaaS offers loose integration as compared with competing solutions that run the full security stack across all POPs.

The new Zero Trust Branch Connectivity solution may create a coopetition status with SD-WAN partners. DEM may further help customers troubleshoot performance challenges, but ideally, future versions will help automate corrective actions.

Consider Zscaler When

Zscaler focuses extensively on delivery security from the cloud and has built out functionality and integrations to deliver on the value and agility promised by cloud security. Zscaler is a short-list vendor for enterprise organizations considering a move to cloud security as a digital transformation initiative or specific use case. With an extensive track record in cloud scale and reliability and with a breadth and depth of security capabilities, Zscaler has proven the ability to support the most demanding enterprise organizations.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC notes that the graphic provides a visual representation of several factors that are translated into a positioning along each axis. Existing product-specific features and functionality are important components of the "capabilities" axis, but many more factors are considered as well. Similarly, the "strategies" axis heavily considers the vendor's plans for future product developments. However, several factors are also considered, including the strength of the overall business and go-to-market plans. These factors may have a long-term impact on the solution, and IDC has adjusted the weights of these criteria accordingly. Overall, several factors go into each vendor assessment, and readers are advised to consider the graphic in the context provided in the vendor profiles.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

Network edge security as a service is an integrated security solution that offers multiple network security technologies as an integrated cloud-delivered service to address key customer use cases of access policy enforcement and threat detection. Whether accessing from an SD-WAN gateway, on-premises security appliance, or remotely, network traffic is intercepted and steered to the security provider's cloud where relevant security inspections and policy enforcement occur. At this control point, connections are subject to policy enforcement including ZTNA controls, firewall policies, cloud access security broker (CASB), data protections, and content filtering.

Traffic is inspected for threats through various means including SWG and intrusion prevention. Advanced threat detection capabilities, such as DLP, remote browser isolation, deception, and sandboxing emulation, may be utilized as well. Networking functions, such as SD-WAN and/or digital experience monitoring, may also be applied. These functions may be performed in the cloud or in coordination with SD-WAN (including standalone solutions or built-in functionality). (Note: SD-WAN and other networking functionality are not universally required by IT buyers or offered by vendors at this time and thus are not considered to be definitional requirements in this analysis.)

LEARN MORE

Related Research

- *Worldwide Trusted Access and Network Security Forecast, 2022-2026: Evolving Perimeter Complexities Accelerate the Shift to Service-Oriented Architecture* (IDC #US49930220, December 2022)
- *Worldwide Zero Trust Network Access and Network Edge Security as a Service Market Shares, 2021: Balancing Integration and Specialization* (IDC #US49628622, September 2022)
- *Worldwide Zero Trust Network Access Forecast, 2022-2026: Transforming Network Security, Traversing Convergence* (IDC #US49100522, June 2022)
- *IDC's Worldwide Security Products Taxonomy, 2022* (IDC #US48813222, February 2022)
- *IDC MarketScape: Worldwide Cloud Security Gateways 2021 Vendor Assessment* (IDC #US48334521, November 2021)

Synopsis

This IDC study provides an overview and comparison of options in the network edge security-as-a-service (NESaaS) market. The need to consolidate security technologies into a single technology stack has emerged as a top-of-mind concern in recent years, driven by practical business considerations around tightening budgets, limited staffing, and numerous complex security and regulatory requirements. In response, vendors have raced to fill in the gaps in their portfolios and to unify multiple, existing, discrete security technologies into a single coherent platform. As a result, the NESaaS market has emerged as one of the most important developments for security buyers as well as a focal point for security vendors.

"The NESaaS market is developing quickly and offers a vast complexity of options," says Pete Finalle, research manager for IDC's Security and Trust practice. "In theory, NESaaS could be a simple bundling exercise, but in practice, it is much more involved as vendors race to deliver truly beneficial security outcomes for enterprises."

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com