IDC MarketScape

IDC MarketScape: Worldwide Zero Trust Network Access 2023 Vendor Assessment

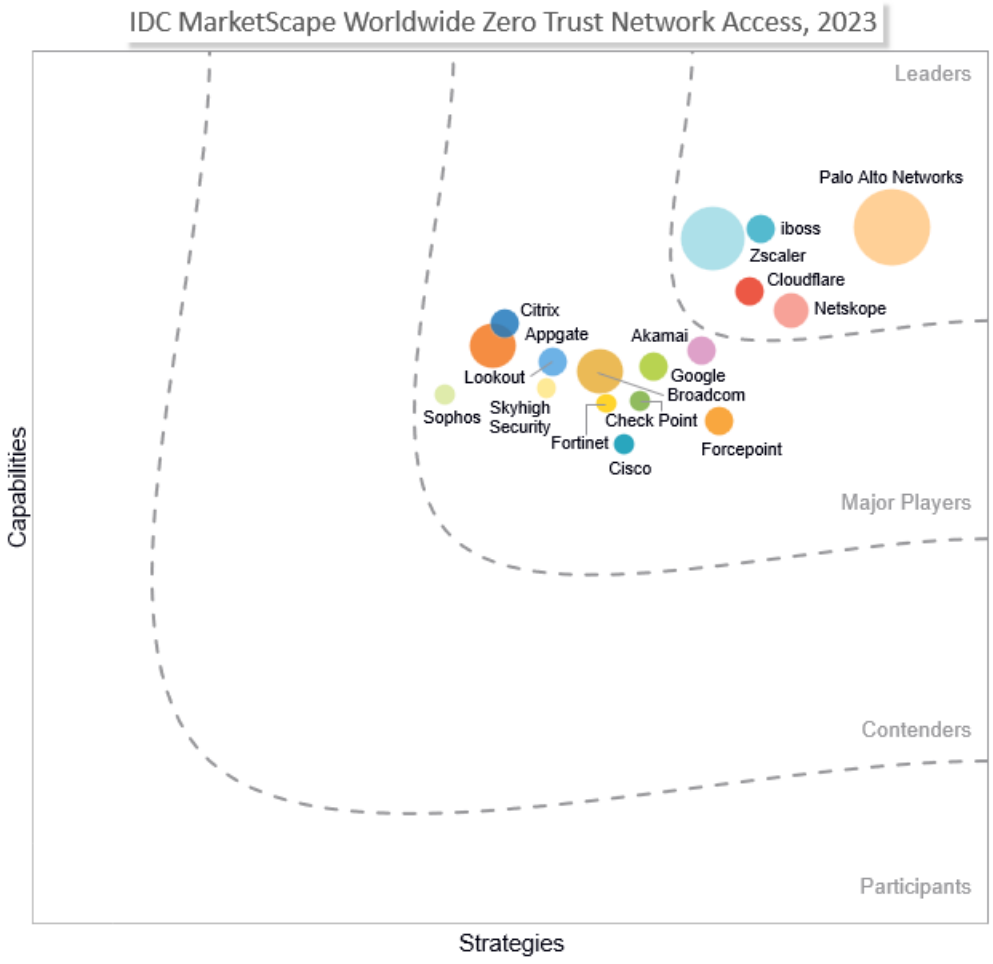
Pete Finalle Christopher Rodriguez

THIS IDC MARKETSCAPE EXCERPT FEATURES IBOSS

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Zero Trust Network Access Vendor Assessment



Source: IDC, 2023

June 2023, IDC #US50844623ee

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

IN THIS EXCERPT

The content for this excerpt was taken directly IDC MarketScape: Worldwide Zero Trust Network Access 2023 Vendor Assessment (Doc # US50844623). 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

Zero trust network access (ZTNA) is a modern approach to enabling secure user access to applications and resources. ZTNA solutions enforce zero trust principles such as least privileged access, strong authentication, granular policies controlling access, and continuous monitoring and threat detection. ZTNA solutions are most often compared with VPNs, as both are network-based solutions that enable secure access. However, ZTNA provides a greater degree of security and privacy compared with VPN in the following ways:

- Using network elements to limit access to only specific applications or resources to prevent lateral movement throughout the network
- Obscuring unapproved resources from unauthorized users to reduce probing, scanning, or denial-of-service attacks
- Enforcement of encryption and mutual authentication to prevent man-in-the-middle (MitM) attacks
- Strong attestation as to claimed identity to enforce access policies
- Behavioral detections to prevent insider threats or compromised credentials

Prior to 2020, ZTNA was an emerging market, offering security and privacy improvements over prior models for network access. Considering that VPN-based access had the most room for improvement in terms of security and user experience, ZTNA found a growing following in addressing the remote user use case.

Then in March 2020, the COVID-19 pandemic drove a broad shift in work models. Businesses switched to work-from-home (WFH) models over the course of just a few strenuous weeks. While IT organizations focused on scaling-up existing remote access systems, they quickly found legacy tools and processes to be incompatible with requirements for scale, ease of use, and trustworthy security. Workers had to bring their devices back into the office for the help desk to install client software, while network teams attempted to scale up legacy VPN deployments. While organizations ultimately "made it work," the reliance on legacy VPNs proved to be a business hindrance with subpar results.

The limitations of legacy VPNs for secure remote access have only become increasingly clear over recent years. Even as businesses have shifted back to in-office work, the need for ZTNA lingers as most organizations have settled on a hybrid model that emphasizes flexibility and boosts productivity. ZTNA is the modern solution that empowers businesses to enable "anywhere access" securely.

To be clear, ZTNA is not solely a tool for secure remote access. Zero trust principals argue the need to extend zero trust principles to all access requirements and work models, including on-premises users. Across the board, ZTNA solutions address the key capabilities germane to user access needs –

supporting on-premises or remote access and managed or unmanaged devices — with slight variations in approach and capabilities from vendor to vendor.

Ultimately, a complete zero trust strategy would also address all other use cases beyond user access, including all device types, IT environments, and workloads. ZTNA is one important piece of the puzzle. However, considering the myriad network configurations possible, industry-specific security and compliance requirements, and specialized devices and applications, zero trust represents a broad practice area that can span many adjacent technologies such as microsegmentation, cloud workload protection, and identity.

For the purposes of this study, ZTNA solutions focus primarily on enabling user access to specific resources and leverage core zero trust tenets to ensure security and privacy. The ability to support broader zero trust strategies for adjacent use cases, device types, environments, or workloads is factored in as a potential strategic differentiator for ZTNA adopters that are interested in implementing a complete zero trust strategy.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

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

- **Granular authorization:** Ideally, only one entity is connected to another, specifically and purposefully. Full network access is not provided — instead, users are provided with controlled, conditional access to only the specific application required.
- **Strong identity and authentication practices:** There is support for MFA and continual monitoring. User identity is validated for each session and during sessions.
- **Dynamic context-based policies:** Geographic location, application type and risk level, time of day, and device type/status are useful contextual factors for determining risk thresholds.
- **Universal application of zero trust:** Zero trust must be extended to all entities, subjects, and resources. Note that "subjects" typically refers to human users but should also account for devices, applications, and workloads that communicate with each other.
- **Continuous threat detection/protection:** Threat intelligence and security analytics are key to identifying zero-day threats and threats that abuse their "trust" status, including insider threats and compromised accounts.
- **"Need to know" access only:** Data and resources are protected entirely behind policy enforcement points and are accessible to only authorized users under specific controlled conditions and are invisible to all other users.

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

- **Market participation:** The vendor began selling ZTNA products to customers in January 2022 or earlier.
- **Market presence:** ZTNA revenue for CY2022 reached a threshold determined by IDC through research or existing data.

ADVICE FOR TECHNOLOGY BUYERS

IT organizations have become very familiar with the limitations of legacy enterprise VPNs over the years. Limitations such as poor user experience and resource-hungry client software are easily understood and highly visible to IT buyers. VPNs have long been associated with security concerns as well, including the tendency to provide overly permissive networkwide access and lack of threat monitoring. The security weakness of VPNs has only become more apparent in recent years as security researchers discovered zero-day vulnerabilities in commercial enterprise VPN solutions.

However, in practice, VPN has not been displaced completely. ZTNA deployments are often methodical processes that unfold over months or years. Enterprises may focus on specific applications or use cases based on ease of implementation or risk concerns. In the meantime, VPNs have a role to play, maintaining a familiar, if not imperfect, option for enabling access to important business applications. Thus this IDC MarketScape analysis factors in deployment flexibility and ability to support a unified approach to ZTNA and VPN access. This approach will enable businesses to implement ZTNA in a low-stakes, frictionless manner that facilitates the broader goal of security modernization and eventual retirement of legacy systems.

While ZTNA has had strong adoption related to support for remote/hybrid use cases, ZTNA should not be solely thought of as a remote access tool. The value of ZTNA is increasingly represented by the need for more robust security across all access methods, locations, and use cases. Zero trust principles must be extended to all access requirements and work models, including on-premises users.

For most IT buyers, ZTNA solutions that focus primarily on user access will be the top priority, and understandably so. However, IT buyers may also want to consider the ability to build upon the ZTNA solution, with plans to eventually reach a full zero trust architecture as budget and time permit. Depending on the organization, a zero trust architecture may span across adjacent technologies such as microsegmentation, cloud workload protection, and identity. As such, IDC has made note of ZTNA solutions that offer expanded zero trust capabilities outside of core ZTNA functionality as potential strategic differentiators.

ZTNA has a unique adoption road map, which typically emphasizes lower-cost/less granular access plans over premium, zero trust–centric plans, at least initially. ZTNA solutions offer multiple deployment options:

- Contractor, remote worker, branch office, and main office
- Agentless and agent based
- Resource portal, secure enclave, and gateway mode

Owing to the dynamic nature of most companies' personnel and security requirements, most deployments are considered a hybrid model, utilizing varying levels of identity, access, and security depending on user type. However, the consistent theme across the entire ecosystem is that businesses are transitioning users from the lowest levels of security to more granular, zero trust aligned levels.

Security capabilities also typically increase through the ZTNA life cycle. Adopting organizations may only start out with basic authentication and evolve to MFA usage, monitoring and alerting, and active threat blocking. Additional capabilities, such as DLP, RBI, and UEBA, serve as the next step for most

vendors. These extended zero trust capabilities often act as an introduction to an integrated security platform solution, as enterprises hope to leverage zero trust access policies alongside additional protections that go far beyond the commonly accepted definition of ZTNA.

These integrated security platforms include ZTNA as a core capability, which is a serious consideration for ZTNA buyers. While the risk mitigation benefits of ZTNA are important from a security perspective, IT buyers are increasingly focused on the need for security integration. Most ZTNA vendors now offer their solution as an integrated component in a converged, cloud-delivered network security platform. IDC refers to this integrated security services platform as network edge security as a service (NESaaS). For IT buyers, the need to consolidate security technologies into a single technology stack is based largely on practical business considerations at this time. However, simplification of security processes and reduction of security silos will also help enterprises mitigate gaps in security posture.

For vendors, a NESaaS strategy is part of a broader push toward a security panacea called "secure service edge (SSE)" in marketing literature. SSE further rolls up into a broader "secure access service edge (SASE)" strategy that postulates the benefits of converged networking and security. In a much more practical sense, NESaaS vendors are driven to deliver much more than simple consolidation and bundled pricing. True integration of key technologies, such as secure web gateway, cloud access security broker (CASB), and ZTNA, is driving improved security posture and outcomes, as well as performance benefits that facilitate business goals for productivity and security.

Such a consolidation strategy may be of little or no interest to some IT buyers, including large enterprise organizations with broad security and compliance teams and deep budgets capable of accommodating best-of-breed solutions. Nevertheless, ZTNA solutions are inherently buttressed by the broader security portfolio to the extent that a vendor is able to cross-pollinate features, functionality, and security intelligence across the portfolio. As such, this IDC MarketScape provides an overview of available ZTNA solutions on their own merit — while factoring in the advantages of the broader vendor portfolio as their competitive differentiators.

Overall, ZTNA is on an accelerated path toward NESaaS convergence. IT buyers' zero trust plans should heavily consider the road map plans of vendors working toward a NESaaS. IT buyers may want to consider the ability to implement a NESaaS with the same vendor that provides their ZTNA solution, if not immediately, then at some point in the future. For more information about the NESaaS market, see *IDC MarketScape: Worldwide Network Edge Security as a Service 2023 Vendor Assessment* (IDC #US50723823, forthcoming), published as a companion piece to this document.

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.

iboss

iboss is positioned in the Leaders category in the 2023 IDC MarketScape for worldwide zero trust network access.

iboss is a provider of network security as a service. The company has roots as SWG as a service, expanding its solution in recent years to represent a comprehensive enterprise security portfolio based on zero trust principles.

Strengths

For iboss, zero trust principles are baked into the entirety of its cloud-delivered suite of security solutions. The iboss ZTNA solution provides contextual, granular policy enforcement; threat detection; and data protection for all users and resources through its cloud service. The cloud service is based on a containerized architecture to enable the full stack of network security functionality to be applied in all and any iboss POPs. The approach allows a modular, performant, edge protection model that supports a consistent, secure experience across all users and managed and unmanaged devices.

The iboss solution conceals all applications and resources behind its cloud edge service to protect against scanning and probing. The service is built on the iboss cloud that leverages browser isolation to completely separate user subjects from internal resources and data. The iboss method turns users' browsers into clients, streaming all functionality and data as pixels rather than data or code. As a result, no data is ever allowed to land on end users' devices.

The solution can also be deployed as a reverse proxy depending on specific use cases and can be deployed to cohabitate in users' cloud environments for intracloud protection.

Challenges

While not integral to the market definition, iboss lags in the area of DEM. The addition of DEM would help customers troubleshoot and understand the root cause of any connectivity challenges.

iboss solutions are designed for enterprise users that have the luxury of learning a complex management system. Improvements in aspects of user interface and automated policy systems will help lower barriers to adoption for midsize enterprises and smaller businesses.

The solution is not complemented by a traditional network firewall device for on-premises protection or specialized use cases, although iboss notes that its on-premises private containerized cloud gateways can be deployed as firewalls as well. The iboss gateways offer routing and firewalling capabilities in addition to deep content proxy capabilities.

Consider iboss When

iboss has invested heavily into its cloud platform to ensure a secure, performant user experience across all devices, personal, managed, and unmanaged, as well as for all users whether employees, contractors, or others. By ensuring that the solution's architecture is fundamentally built on key zero trust principles, iboss enables customers to start with the use cases that are most important to their specific security modernization goals. The iboss approach has been aligned with large enterprise organizations in need of SaaS security for network modernization.

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 graphics provides a visual representation of several factors that are translated into a positioning along each axis. Existing product-specific features and functionality are an important component 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 graphics 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

ZTNA is a new category of access security and control solutions. ZTNA establishes secure connections from an authenticated user to only authorized applications based on context-aware, identity-aware, and device-aware policies. ZTNA is built on key principles of application- and user-centric protections and least privilege access, thereby preventing unauthenticated users from connecting or sending any traffic to unauthorized applications. Importantly, ZTNA solutions are designed to support complex and distributed network environments featuring combinations of on-premises and remote users, myriad devices, and data and workloads spread across multiple cloud and local computing environments.

ZTNA is a component of a zero trust strategy to realign security practices and tooling into a modern security architecture that ensures least privilege access to data and resources. According to zero trust principles, access decisions should be based on strong identity validation and context-aware policies (e.g., location, time, device type/status, user behavior) and on authentication that is as accurate as possible and with authorization that is as granular as possible. IDC notes that a full zero trust strategy

may include third-party tooling for related functions, such as data protection, identity and access management, or device protection, that are not included in ZTNA market measurement practices.

Zero trust architecture is the blueprint by which enterprises can implement these zero trust concepts. Accordingly, zero trust architecture features the following foundational elements:

- **Granular authorization:** Ideally, only one entity is connected to another, specifically and purposefully. Full network access is not provided — instead, users are provided with controlled, conditional access to only the specific application required.
- **Strong identity and authentication practices:** There is support for MFA and continual monitoring. User identity is validated for each session and during sessions.
- **Dynamic context-based policies:** Geographic location, application type and risk level, time of day, and device type/status are useful contextual factors for determining risk thresholds.
- **Universal application of zero trust:** Zero trust must be extended to all entities, subjects, and resources. Note that "subjects" typically refer to human users but should also account for devices, applications, and workloads that communicate with each other.
- **Continuous threat detection/protection:** Threat intelligence and security analytics are key to identifying zero-day threats and threats that abuse their "trust" status, including insider threats and compromised accounts.
- **"Need to know" access only:** Data and resources are protected entirely behind policy enforcement points and are accessible to only authorized users under specific controlled conditions and are invisible to all other users.

A guiding principle of zero trust is to connect users to only limited and specific applications and resources based on the assumption that the network has already been compromised. This "assumed breached" stance thus reinforces the need to move away from implicit trust based on user location and an overreliance on perimeter-based protections.

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 of available ZTNA solutions on their own merit while factoring in the advantages of the broader vendor portfolio as their competitive differentiators. ZTNA is an updated approach for enabling secure user access to important business applications and resources. The market is rapidly evolving beyond simple needs for remote user access to support all use cases, devices, and environments. As such, there remains a wide range of capabilities and approaches for security buyers to consider.

"The ZTNA market is at a critical juncture as vendors race to deliver strong zero trust capabilities while meeting the broadest set of buyer needs," according to Pete Finalle, research manager for the IDC Security and Trust team. "At the same time, enterprise buyers are approaching their ZTNA planning in the context of their broader security plans."

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