Market Guide for Zero Trust Network Access

Published 17 February 2022 - ID G00730534 - 12 min read

By Analyst(s): Aaron McQuaid, Neil MacDonald, John Watts, Shilpi Handa

Initiatives: Infrastructure Security

ZTNA augments traditional VPN technologies for application access, and removes the excessive trust once required to allow employees and partners to connect and collaborate. Security and risk management leaders should pilot ZTNA projects as part of an SSE strategy or to rapidly expand remote access.

Additional Perspectives

- Summary Translation: Market Guide for Zero Trust Network Access (10 March 2022)
- Invest Implications: Market Guide for Zero Trust Network Access (22 February 2022)

Overview

Key Findings

- An increased focus by end-user organizations on zero trust strategies — and a desire to provide a more secure, flexible hybrid workforce connectivity — is driving increased interest in the ZTNA market.
- Organizations cite VPN replacement as their primary motivation for evaluating ZTNA offerings, but find that justification comes from risk reduction, not from any cost savings.
- Agent-based ZTNA is increasingly deployed as part of a larger SASE architecture or SSE offering for the extended workforce, while clientless ZTNA continues to grow in popularity to support third-party and BYOD use cases.
- Vendors continue to expand offerings into the data center with identity-based segmentation as separate products or combined with ZTNA offerings — blurring the lines between segmentation technologies.

Recommendations

Security and risk management leaders responsible for infrastructure security should:

- Establish a high-level zero trust strategy first and ensure that your identity and access management technologies and processes are well understood and mature before selecting and implementing a ZTNA solution.
- Assess your current VPN landscape if VPN replacement is the primary goal to quantify the capabilities of a ZTNA vendor — and if there are sufficient benefits of implementing ZTNA to replace the VPN.
- Consolidate agent-based ZTNA selection with the choice of SSE provider as part of the wider SASE architecture decisions to avoid the complexity and potentially unsupported configurations of multiple agents on managed devices.
- Prioritize ZTNA vendor selection based on the desired end-user access use cases, as well as the endpoint and application architecture of the organization.

Market Definition

Gartner defines zero trust network access (ZTNA) as products and services that create an identity- and context-based, logical-access boundary that encompass an enterprise user and an internally hosted application or set of applications. The applications are hidden from discovery, and access is restricted via a trust broker to a collection of named entities. The broker verifies the identity, context and policy adherence of the specified participants before allowing access, and minimizes lateral movement elsewhere in the network. ZTNA removes excessive implicit trust that often accompanies other forms of application access, such as legacy VPN. ZTNA, along with CASB and SWG, is one of the core technologies that make up the security service edge (SSE) market. Gartner is seeing increased consolidation of these offerings and expects this trend to accelerate in the future.

Market Description

The ZTNA market has evolved from primarily being a VPN replacement to a key component of a standardized architecture for (remote and small branch) user to application zero trust networking. ZTNA has yet to gain major traction in the large branch or campus environments due to high per-user cost and existing investment in appliance-based solutions. Gartner views ZTNA technology as an important organizational step toward increasing the maturity of your zero trust program. When combined with SWG and CASB offerings, ZTNA forms one of the key technological underpinnings of the emerging SSE market.

ZTNA provides controlled identity- and context-aware access to resources, reducing the surface area for attack. ZTNA starts with a default deny posture of zero trust. It grants access based on the identity of the humans and their devices — plus other attributes and context, such as time/date, geolocation, device posture, etc. — and adaptively offers the appropriate trust required at the time. The result is a more resilient environment, with improved flexibility and better monitoring. ZTNA will appeal to organizations looking for more flexible and responsive ways to connect and collaborate with their digital business ecosystems, remote workers and partners.

The isolation afforded by ZTNA improves connectivity, removing the need to directly expose applications to the internet. The internet remains an untrusted transport; a trust broker mediates connections between applications and users. The broker can be a cloud service managed by a third-party provider or a self-hosted service (in the form of a physical appliance in the customer's data center, or a virtual appliance in a public infrastructure as a service [IaaS] cloud). Once the broker has evaluated a user's credentials and their device's context, the broker communicates to a gateway function placed logically close to applications. In most cases, the gateway establishes an outbound communication path to the user. In some ZTNA products, the broker remains in the data path; in others, only the gateway does.

Optimally, user and device behavior are continuously monitored for abnormal activity, as described in Gartner's Continuous Adaptive Risk and Trust Assessment (CARTA) framework (see Zero Trust Is an Initial Step on the Roadmap to CARTA). In a sense, ZTNA creates individualized "virtual perimeters" that encompass only the user, the device and the application.

Market Direction

The ZTNA market has continued to mature and grow at a rapid pace. In our Forecast: Enterprise Network Equipment by Market Segment, Worldwide, 2019-2025, 4Q21 update, Gartner captured a 60% YoY growth rate for ZTNA. The market is increasingly converging toward an SSE agent-based architecture for the majority of deployments. We are also seeing increased demand for agentless-based deployments in the case of unmanaged devices and/or third-party access. Security and risk management leaders will need to ensure that their chosen vendor supports both approaches to cover the most common use cases.

In the near to midterm, stand-alone ZTNA vendors will find it increasingly difficult to compete with fully integrated SSE and SASE offerings. These vendors should expand their offerings to include SWG, DLP and CASB offerings, or partner with third-party providers.

Market Analysis

Benefits and Uses

The benefits of ZTNA are immediate. When replacing legacy network-level VPN access, ZTNA provides contextual, risk-based and least privilege access to applications (not networks). When replacing applications exposed in DMZs with ZTNA, services are no longer visible on the public internet and are thus shielded from attackers. In addition, ZTNA brings significant benefits in user experience, agility, adaptability and ease of policy management. For cloud-based ZTNA offerings, scalability and ease of adoption are additional benefits. ZTNA enables digital business transformation scenarios that are ill-suited to legacy access approaches. As a result of digital transformation efforts, most enterprises will have more applications, services and data outside of their borders than inside. Cloud-based ZTNA services place the security controls where the users and applications are — in the cloud. Some of the larger ZTNA vendors have invested in hundreds of points of presence (POPs) worldwide to satisfy both latency-sensitive requirements and regional logging and inspection requirements.

Several use cases lend themselves to ZTNA:

- Opening applications and services to named collaborative ecosystem members — such as distribution channels, suppliers, contractors or retail outlets — without requiring a VPN or DMZ. Access is more tightly coupled to users, applications and services.

- Deriving personas based on user behavior — for example, if a user's phone is in one country, but their PC is in another country, and both are attempting to log on to the same application, legitimate access should be permitted, while compromised devices should be blocked.
- Carrying encryption all the way from the endpoint to the ZTNA gateway (which may run on the same server as the application it protects) for scenarios where you don't trust the local wireless hot spot, carrier or cloud provider.
- Providing application-specific access for IT contractors and remote or mobile employees as an alternative to VPN-based access.
- Controlling administrative access to applications, such as IaaS/PaaS applications as a lower-cost alternative to full privileged access management (PAM) tools.
- Extending access to an acquired organization during M&A activities, without having to combine networks, combine directories or configure site-to-site VPN and firewall rules.
- Isolating high-value enterprise applications in the network or cloud to reduce insider threats and affect separation of duties for administrative access.
- Authenticating users on personal devices — ZTNA can improve security and simplify bring your own device (BYOD) programs by reducing full management requirements and enabling more-secure direct application access.
- Creating secure enclaves of Internet of Things (IoT) devices or a virtual appliance-based connector on the IoT network segment for connection.
- Protecting internal systems from hostile networks, such as the public internet, by removing inbound access (leveraging phone home), thus reducing attack surface.

Risks

Although ZTNA greatly reduces overall risks, it doesn't eliminate every risk completely, as these examples illustrate:

- The trust broker could become a single point of any kind of failure. Fully isolated applications passing through a ZTNA service will stop working when the service is down. Well-designed ZTNA services include physical and geographic redundancy with multiple entry and exit points to minimize the likelihood of outages affecting overall availability. Furthermore, a vendor's SLAs (or lack thereof) can indicate how robust they view their offerings. Favor vendors with SLAs that minimize business disruptions.

- The location of the trust broker can create latency issues for users, negatively affecting the user experience. Well-designed ZTNA offerings provide multiple POPs with distributed copies of the enterprise's policies, combined with peering relationships to improve redundancy while decreasing latency.

- Attackers could attempt to compromise the trust broker system. Although unlikely, the risk isn't zero. ZTNA services built on public clouds or housed in major internet carriers benefit from the provider's strong tenant isolation mechanisms. Nevertheless, collapse of the tenant isolation would allow an attacker to penetrate the systems of the vendor's customers and move laterally within and between them. A compromised trust broker should fail over to a redundant one immediately. If it can't, then it should fail closed — that is, if it can't deflect abuse, it should disconnect from the internet. Favor vendors that adopt this stance. In addition, verify that vendors maintain their own security operations teams that diligently monitor their infrastructure for issues affecting the integrity of the service (see Risk-Based Evaluations of Cloud Provider Security).

- Compromised user credentials could allow an attacker on the local device to observe and exfiltrate information from the device. ZTNA architectures that combine device authentication with user authentication contain this threat to a degree — stopping the attack from propagating beyond the device itself. We suggest that, when possible, MFA should accompany any ZTNA project (see Enhance Remote Access Security With Multifactor Authentication and Access Management).

- Given the concerns with trust broker failure and user credentials, ZTNA administrator accounts are ripe for attack. Limit the number of administrators and monitor their activities to reduce insider threats, and to favor vendors that require strong authentication for administrators by default.

- Some ZTNA vendors have chosen to focus their developments on supporting web application protocols only (HTTP/HTTPS). Carrying legacy applications and protocols through a ZTNA service could prove to be more technically challenging for vendors to develop and for customers to deploy.

- Some vendors have adopted the usage of dTLS to enable more effective transport for real-time communication applications. Clients should ensure that their providers support this protocol if they intend to leverage real-time applications over ZTNA.
- The market is in flux, and smaller vendors could disappear or be acquired.

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Market Introduction

The vendor selection is based on the old list from the previous Market Guide, client inquiry and internal discussion among the author team (see Note 1).

Table 1: Representative Vendors of ZTNA

(Enlarged table in Appendix)

Vendor	Product or Service Name
Absolute Software (NetMotion)	NetMotion ZTNA
Akamai	Enterprise Application Access
Appgate	Appgate SDP
Axis	Axis Platform
Banyan Security	Zero Trust Remote Access
Bitglass	Zero Trust Network Access
BlackRidge	Transport Access Control
Broadcom	Symantec Secure Access Cloud
Cato	Cato Secure Remote Access
Check Point Software Technologies	Harmony Connect
Cisco	Duo Beyond
Citrix	Secure Private Access
Cloudaemon	Taiji Perimeter
CloudDeep Technology (China only)	Deep Cloud SDP
Cloudflare	Cloudflare Access
Cognitas Technologies	Crosslink
Cyolo	Zero Trust Network Access (ZTNA) 2.0
Deloitte (Transientx)	TransientAccess
Forcepoint	Private Access
Google	BeyondCorp Remote Access Google Cloud Platform Identity-Aware Proxy
InstaSafe	Zero Trust Remote Access
Ivanti	Ivanti Neurons for Secure Access
Jamf	Jamf Private Access
McAfee	MVISION Private Access
Microsoft	Azure AD Application Proxy Web Application Proxy for Windows Server
NetFoundry	Zero Trust Networking Platform
Netskope	Netskope Private Access
Okta	Okta Identity Cloud
Palo Alto Networks	Prisma Access
Perimeter 81	Zero Trust Network Access
Safe-T	Zone Zero
SAIFE	Continuum
Systancia	Systancia Gate
Trusfort	Zero-Trust Business Security
Twingate	Twingate
Unisys	Stealth
Verizon	Verizon Software Defined Perimeter (SDP)
Versa	Versa Secure Access
Waverley Labs	Open Source Software Defined Perimeter
Zentera Systems	Secure Access ZTNA
Zero Networks	Access Orchestrator
Zscaler	Private Access

Source: Gartner (February 2022)

Market Recommendations

Given the significant risk that the public internet represents — and the attractiveness of compromising internet-exposed systems to gain a foothold in enterprise systems — enterprises need to consider isolating digital business services from visibility by the public internet. ZTNA cloaks services from discovery and reconnaissance and erects true, identity-based barriers that are proving to be more challenging for attackers to circumvent than traditional network level VPNs and firewalls.

For legacy VPN access, look for scenarios in which targeted sets of users can be switched to performing their work through a ZTNA, providing immediate value in improving the overall security posture of the organization. In most cases, you can start with contractor and/or third-party access, and then move on to employee-facing applications as you progressively replace your legacy VPN. A ZTNA project is a step toward a more widespread zero trust networking (default deny, zero implicit trust) security posture. Specifically, nothing can communicate (or even see) an application resource until sufficient trust is established, given the risk and current context to extend network connectivity.

Be aware that ZTNA is an (albeit important) component of a zero trust strategy. Do not assume that purchase of a ZTNA (or any product) is the only thing you must do as you implement a general zero trust architecture.

For DMZ-based applications, evaluate what sets of users require access. For those applications with a defined set of users, plan to migrate them to a ZTNA service during the next several years. Use the migration of these applications to public cloud IaaS as a catalyst for this architectural shift. Consider placing them in a private IP space with no access except through a ZTNA service. This does not apply to public-facing citizen or consumer applications that are not in scope for ZTNA due to licensing, account and identity management challenges for these types of public-facing applications.

Evidence

[1] Top Routinely Exploited Vulnerabilities, Cybersecurity and Infrastructure Security Agency (CISA).

Note 1
Representative Vendor Selection

The vendors named in this guide were selected based on client inquiry and the authors' collective experience.

Document Revision History

Market Guide for Zero Trust Network Access - 8 June 2020

Market Guide for Zero Trust Network Access - 29 April 2019

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Quick Answer: Does SASE Replace SD-WAN?

2021 Strategic Roadmap for SASE Convergence

Best Practices for Implementing Zero Trust Network Access

Enhance Remote Access Security With Multifactor Authentication and Access Management

---

Table 1: Representative Vendors of ZTNA

Vendor	*Product or Service Name*
Absolute Software (NetMotion)	NetMotion ZTNA
Akamai	Enterprise Application Access
Appgate	Appgate SDP
Axis	Axis Platform
Banyan Security	Zero Trust Remote Access
Bitglass	Zero Trust Network Access
BlackRidge	Transport Access Control
Broadcom	Symantec Secure Access Cloud
Cato	Cato Secure Remote Access
Check Point Software Technologies	Harmony Connect
Cisco	Duo Beyond
Citrix	Secure Private Access
Cloudaemon	Taiji Perimeter
CloudDeep Technology (China only)	Deep Cloud SDP
Cloudflare	Cloudflare Access

Vendor	*Product or Service Name*
Cognitas Technologies	Crosslink
Cyolo	Zero Trust Network Access (ZTNA) 2.0
Deloitte (Transientx)	TransientAccess
Forcepoint	Private Access
Google	BeyondCorp Remote Access Google Cloud Platform Identity-Aware Proxy
InstaSafe	Zero Trust Remote Access
Ivanti	Ivanti Neurons for Secure Access
Jamf	Jamf Private Access
McAfee	MVISION Private Access
Microsoft	Azure AD Application Proxy Web Application Proxy for Windows Server
NetFoundry	Zero Trust Networking Platform
Netskope	Netskope Private Access
Okta	Okta Identity Cloud
Palo Alto Networks	Prisma Access
Perimeter 81	Zero Trust Network Access

Vendor ↓	*Product or Service Name* ↓
Safe-T	Zone Zero
SAIFE	Continuum
Systancia	Systancia Gate
Trusfort	Zero-Trust Business Security
Twingate	Twingate
Unisys	Stealth
Verizon	Verizon Software Defined Perimeter (SDP)
Versa	Versa Secure Access
Waverley Labs	Open Source Software Defined Perimeter
Zentera Systems	Secure Access ZTNA
Zero Networks	Access Orchestrator
Zscaler	Private Access

Source: Gartner (February 2022)