CRO CYBER RATINGS.ORG

Choosing the Right ZTNA Offering for Your Organization

Zero Trust is a security model that replaces legacy models that assume anything inside a network is safe. It is gaining popularity especially as multi-cloud use and remote work continue to decentralize IT infrastructure and dissolve the traditional network perimeter. Vendors that provide Zero Trust Network Access (ZTNA) technologies and platforms help IT teams implement Zero Trust principles more easily.

But how do you choose the best ZTNA vendor for your organization? With so many options in the market, it can be challenging to find the right fit for your needs and goals.

In this brief, we'll share some tips and criteria to help you evaluate and select the right ZTNA offering for your organization.

KEY FINDINGS

- Zero Trust is a security model that replaces legacy models that assume anything inside a network is safe. Zero Trust Network Access (ZTNA) is a technology that enables IT teams to implement Zero Trust principles more easily.
- ZTNA can address different use cases, such as remote access for your workforce, BYOD and third-party access, and cloud and hybrid environments. You need to identify your use case before choosing a ZTNA vendor.
- ZTNA vendors differ in their features and capabilities. You need to look for key features, such as identity-centricity, default "deny" response, context-awareness, application-centricity, and continuous verification. You may also want to look for advanced features, such as complete protection, seamless integration, scalability and performance, visibility and analytics.

RECOMMENDATIONS

- Identify your use case for ZTNA and prioritize your needs and goals.
- Look for key features that match your use case and differentiate ZTNA products.
- Institute a formal Request for Information and request a demo or a trial to test their products in your own environment.
- Compare different ZTNA vendors based on your criteria and choose the one that meets your needs, goals and budget.

To choose the best ZTNA vendor for your organization, we recommend following a systematic process that involves identifying your use cases, looking for key features that support those use cases, instituting a formal request for information, and testing the offerings so that you can compare based on your criteria.

INTRODUCTION

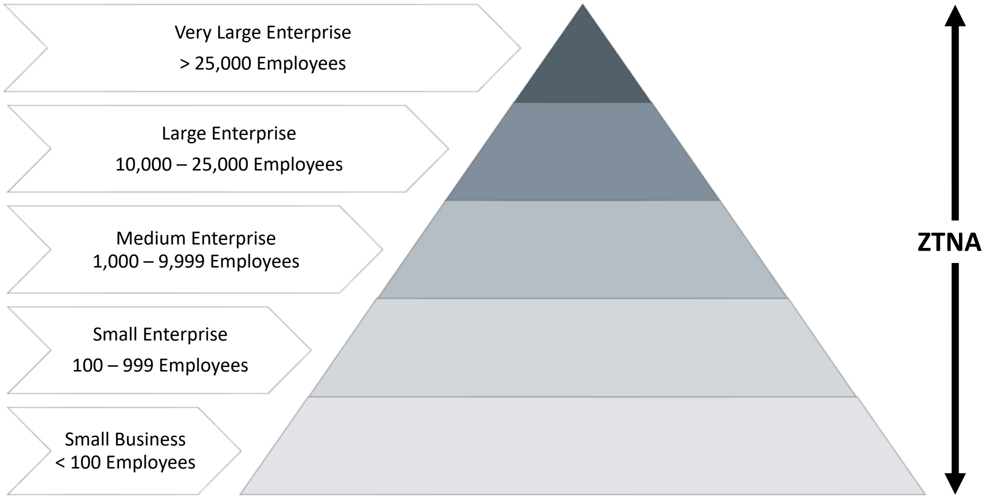
The Zero Trust Network Access (ZTNA) market is expected to thrive in the next few years as organizations seek to refresh their network security and support their digital transformation initiatives. According to Gartner, ZTNA will be the fastest-growing network security market segment worldwide, with a compound annual growth rate (CAGR) of 27.5%, increasing from $633 million to $2.1 billion worldwide between 2021 and 2026.

Despite this growth projection, the market is facing some challenges such as the lack of standardization and interoperability among different ZTNA vendors and solutions, the complexity and cost of migrating from legacy VPN solutions to ZTNA solutions, and the resistance to change and trust issues among some IT teams and end-users who are accustomed to VPN solutions. There are also regulatory and legal barriers that may limit the adoption of ZTNA solutions in some regions or industries.

For the ZTNA market to live up to its potential, vendors need to work with standards bodies to build buyer confidence in the market and then differentiate themselves based on the strength of their brand, innovation, feature sets, and how well their offering match the needs and goals of their target customers. They also need to provide flexible and scalable deployment models that can support different use cases and environments to facilitate customer migration from VPNs to ZTNA. They should show clear evidence of their compliance with regulatory and legal requirements to meet specific performance, reliability, security, and privacy standards.

MARKET DIRECTION

The market for ZTNA ranges from small and medium businesses (SMBs) to large and very large enterprises. Typical use cases are remote access, third-party access, BYOD access, IoT access, and data center segmentation. ZTNA is being adopted globally, with North America and Asia-Pacific leading. The leading sectors for ZTNA are financial services, healthcare, manufacturing, government, and education.



Market drivers:

- Increasing demand for secure and seamless remote access for distributed workforce and applications.
- Rising adoption of cloud-based services and hybrid environments requiring consistent and granular access policies across different platforms.
- Growing awareness of the benefits of ZTNA over legacy VPN solutions, such as reduced attack surface, improved user experience, lower operational costs, and enhanced compliance.
- The evolving threat landscape requiring continuous verification and dynamic access privileges based on contextual factors.

Challenges:

- Lack of standardization and interoperability among different ZTNA vendors and solutions.
- Complexity and the cost of migrating from legacy VPN solutions to ZTNA solutions.
- Resistance to change and trust issues among some IT teams and end-users accustomed to VPN solutions.
- Regulatory and legal barriers that may limit the adoption of ZTNA solutions in some regions or industries.

Opportunities:

- The emergence of Secure Access Service Edge (SASE) as a converged framework that integrates ZTNA with other security functions, such as cloud access security broker (CASB), secure web gateway (SWG), and firewall as a service (FWaaS).
- The introduction of new features, capabilities, deployment models, and pricing strategies that may accelerate market adoption.
- The expansion of ZTNA use cases beyond remote access to include BYOD and third-party access, cloud-native and legacy applications, IoT devices, and microservices.
- The integration of ZTNA with other security tools, such as endpoint protection, identity and access management (IAM), threat intelligence, and analytics.

ANALYSIS

ZTNA is a security model that applies the principle of "never trust, always verify" to network access. It assumes that every user and device is a threat and requires them to prove their identity before granting them access to specific network resources. It also monitors and verifies their status throughout the session and adjusts their access privileges based on changes in risk level.

ZTNA can help companies protect their networks from today's threats, such as data breaches, ransomware attacks, phishing scams, and insider threats. It can also help improve user experience, operational efficiency, compliance posture, and business agility. There are many ZTNA offerings in the market, each with their own strengths and weaknesses. Be aware: some vendors may claim to offer ZTNA but may not meet the core requirements of Zero Trust.

IDENTIFYING YOUR USE CASE

The first step in choosing a ZTNA vendor is to identify your use case. What are you trying to achieve with ZTNA? Who are the users and devices that need secure access to your network resources? Where are they located and what are they accessing?

Some of the common use cases for ZTNA are:

- Remote access for your workforce: If you have a distributed workforce that needs to access your network from anywhere, you need a ZTNA solution that can provide secure and seamless access to your applications and data, regardless of location or device.
- BYOD and third-party access: If you allow your employees to use their own devices or grant access to third-party partners, contractors, or vendors, you need a ZTNA solution that can verify the identity and security posture of every device and user before granting access to your network resources.
- Cloud and hybrid environments: If you have migrated some or all of your applications and data to the cloud or have a hybrid environment that combines on-premises and cloud resources, a ZTNA solution can provide consistent and granular access policies across different platforms and environments.

Once you have identified your use case, you can narrow your search based on the features and capabilities that match your needs.

LOOK FOR KEY FEATURES

- Identity-centric: A ZTNA tool should grant users conditional access to as few network resources as possible -- the ones they need to do their jobs -- based on pre-established identities, roles and permissions.
- Default "deny" response: A ZTNA tool should reject all requests by default, unless they are explicitly allowed by the access policies.
- Context-aware: A ZTNA tool should consider contextual factors, such as device security posture, location, time, and behavior, when making access decisions.

- Application-centric: A ZTNA tool should provide access only to specific applications or services, not to the entire network or segment.
- Continuous verification: A ZTNA tool should monitor and verify the user and device status throughout the session, not just at the initial login. This enables dynamic adjustment of access privileges based on changes in risk level.

In addition to these core features, you may also want to look for some advanced features that can enhance your ZTNA experience:

- Completeness of the offering: Does the ZTNA tool cover all types of users (remote and in-office), devices (BYOD, corporate issued and IoT), and workloads (cloud-native, legacy on-premises and traditional cloud)?
- Integration: Does the ZTNA tool integrate well with your existing identity providers (IDPs), single sign-on (SSO) tools, multi-factor authentication (MFA) tools, and endpoint security software to leverage your existing investments and simplify management?
- Scalability and performance: Is the ZTNA tool able to scale up or down as your needs change, without compromising performance or user experience?
- Deployment Models: Does it support different deployment models (cloud-based, on-premises or hybrid) based on your preferences?
- Visibility and analytics: Does the ZTNA tool provide comprehensive visibility into who is accessing what, when, where and how on your network?

ASK THE RIGHT QUESTIONS

During the vetting process, consider asking ZTNA vendors the following questions:

- How does this product control, in advance, who is allowed to connect to a given network resource?
- How granular can customers make their access policies?
- What role do contextual risk factors, such as device security posture, play in the authentication process?
- What IAM, SSO and MFA tools does the ZTNA product support?
- What endpoint security software does it support?
- How does this product integrate with existing network infrastructure and security tools?
- How does this product handle different types of applications and workloads, such as cloud-native, legacy on-premises and traditional cloud?
- How does this product scale and perform in different scenarios and environments?
- What deployment options does this product offer (cloud-based, on-premises or hybrid)?
- What visibility and analytics capabilities does this product provide?
- How easy is it to deploy, manage and update this product?
- What support and service level agreements does this vendor offer?

ZTNA PROVIDERS

The ZTNA market is highly competitive and fragmented, with many vendors offering distinct features, capabilities, deployment models, and pricing strategies. The following is a brief overview of some of the ZTNA vendors and their offerings:

Absolute: Absolute provides endpoint security and resilience solutions that enable organizations to secure devices, data, and applications. Its ZTNA offering, Absolute Control, allows organizations to control access to sensitive data and applications based on device health, location, user identity, and behavior.

Akamai: Akamai is a cloud service provider that offers web performance, media delivery, and security solutions. Its ZTNA offering, Enterprise Application Access, provides secure access to applications hosted on-premises or in the cloud without requiring VPNs.

AppGate: AppGate is a cybersecurity company that offers secure access solutions for hybrid IT environments. Its ZTNA offering, AppGate SDP, provides granular access control based on user context, device posture, and application attributes.

Axis Security: Axis Security is a ZTNA startup that offers a cloud-native platform for secure application access. Its ZTNA offering, Axis Application Access Cloud, provides agentless access to any application without requiring network changes or device installation.

Banyan Security: Banyan Security is a ZTNA startup that offers a cloud-native platform for secure access to hybrid IT environments. Its ZTNA offering, Banyan Zero Trust Remote Access, provides continuous verification and dynamic enforcement of access policies based on user identity, device trust, and application context.

Broadcom/Symantec: Broadcom is a semiconductor and infrastructure software company that acquired Symantec's enterprise security business in 2019. Its ZTNA offering, Symantec Secure Access Cloud, provides secure access to applications hosted on-premises or in the cloud without requiring VPNs or exposing the network.

Cato Networks: Cato Networks is a cloud-native networking and security company that offers a converged platform for WAN optimization, SD-WAN, and network security. Its ZTNA offering, Cato Cloud, provides secure access to applications hosted on-premises or in the cloud based on user identity and device posture.

Check Point: Check Point is a cybersecurity company that offers network security, endpoint security, and cloud security solutions. Its ZTNA offering, Check Point Harmony Connect, provides secure access to applications hosted on-premises or in the cloud without requiring VPNs or exposing the network.

Cisco: Cisco is a networking and technology company that offers networking, collaboration, security, and cloud solutions. Its ZTNA offering, Cisco Duo Beyond, provides secure access to applications hosted on-premises or in the cloud based on user identity and device trust.

Citrix: Citrix is a digital workspace company that offers virtualization, networking, and cloud solutions. Its ZTNA offering, Citrix Secure Private Access, provides secure access to applications hosted on-premises or in the cloud based on user identity and device posture.

Cloudflare: Cloudflare is a web performance and security company that offers content delivery network (CDN), DNS, and edge computing services. Its ZTNA offering, Cloudflare for Teams, provides secure access to applications hosted on-premises or in the cloud without requiring VPNs or exposing the network.

Forcepoint: Forcepoint is a cybersecurity company that offers data protection, cloud security, and network security solutions. Its ZTNA offering, Forcepoint Dynamic Edge Protection, provides secure access to applications hosted on-premises or in the cloud based on user identity and device posture.

Fortinet: Fortinet is a cybersecurity company that provides network security, endpoint security, and cloud security offerings. Its ZTNA offering, FortiNAC, provides secure access to applications hosted on-premises or in the cloud based on user identity and device trust.

Juniper Networks: Juniper Networks is a networking and technology company that offers routing, switching, and security solutions. Its ZTNA offering, Juniper Security Director Cloud, provides secure access to applications hosted on-premises or in the cloud based on user identity and device posture.

Mammoth Cyber: Mammoth Cyber is a ZTNA startup that offers a cloud-native platform for secure application access. Its ZTNA offering, Mammoth Zero Trust Network Access, provides agentless access to any application without requiring network changes or device installation.

Netskope: Netskope is a cloud security company that offers cloud access security broker (CASB), secure web gateway (SWG), and data protection solutions. Its ZTNA offering, Netskope Private Access, provides secure access to applications hosted on-premises or in the cloud based on user identity and device posture.

Nordlayer: Nordlayer is a ZTNA startup that offers a cloud-native platform for secure application access. Its ZTNA offering, Nordlayer, provides secure access to applications hosted on-premises or in the cloud without requiring VPNs or exposing the network.

Okta: Okta is an identity and access management (IAM) company that offers single sign-on (SSO), multi-factor authentication (MFA), and lifecycle management solutions. Its ZTNA offering, Okta Identity-Driven Security, provides secure access to applications hosted on-premises or in the cloud based on user identity and device trust.

Palo Alto Networks: Palo Alto Networks is a cybersecurity company that offers network security, endpoint security, and cloud security solutions. Its ZTNA offering, Prisma Access, provides secure access to applications hosted on-premises or in the cloud based on user identity and device posture.

Perimeter 81: Perimeter 81 is a ZTNA startup that offers a cloud-native platform for secure application access. Its ZTNA offering, Perimeter 81, provides secure access to applications hosted on-premises or in the cloud without requiring VPNs or exposing the network.

Ping Identity: Ping Identity is an identity and access management (IAM) company that offers single sign-on (SSO), multi-factor authentication (MFA), and lifecycle management solutions. Its ZTNA offering, PingOne Advanced Services, provides secure access to applications hosted on-premises or in the cloud based on user identity and device trust.

Sangfor: Sangfor is a cybersecurity, cloud computing, and infrastructure optimization company. Sangfor's ZTNA offering, Sangfor Access, provides secure access to applications hosted on-premises or in the cloud based on user identity and device posture.

Sophos: Sophos is a cybersecurity company that provides endpoint security, network security, and cloud security offerings. Its ZTNA offering, Sophos Zero Trust Network Access (ZTNA), provides secure access to applications hosted on-premises or in the cloud based on user identity and device posture.

Tencent: Tencent is a technology conglomerate that offers social media, gaming, e-commerce, and cloud services. Its ZTNA offering, Tencent iOA, provides secure access to applications hosted on-premises or in the cloud based on user identity and device posture.

Versa Networks: Versa Networks is a cloud-native networking and security company that offers WAN optimization, SD-WAN, and network security solutions. Its ZTNA offering, Versa Secure Access, provides secure access to applications hosted on-premises or in the cloud based on user identity and device posture.

VMware: VMware is a digital infrastructure company that offers virtualization, cloud computing, and networking solutions. Its ZTNA offering, VMware Workspace ONE, provides secure access to applications hosted on-premises or in the cloud based on user identity and device posture.

Zscaler: Zscaler is a cloud security company that offers web security, email security, and cloud security solutions. Its ZTNA offering, Zscaler Private Access, provides secure access to applications hosted on-premises or in the cloud without requiring VPNs or exposing the network.

ANALYST BRIEF

AUTHORS

Vikram Phatak, Thomas Skybakmoen

CONTACT INFORMATION

CyberRatings.org

2303 Ranch Road 620 South

Suite 160, #501

Austin, TX 78734

info@cyberratings.org

Please read the disclaimer in this box because it contains important information that binds you. If you do not agree to these conditions, you should not read the rest of this report but should instead return the report immediately to us. "You" or "your" means the person who accesses this report and any entity on whose behalf he/she has obtained this report.

1. The information in this report is subject to change by us without notice, and we disclaim any obligation to update it.
2. The information in this report is believed by us to be accurate and reliable at the time of publication but is not guaranteed. All use of and reliance on this report are at your sole risk. We are not liable or responsible for any damages, losses, or expenses of any nature whatsoever arising from any error or omission in this report.
3. NO WARRANTIES, EXPRESS OR IMPLIED ARE GIVEN BY US. ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, ARE HEREBY DISCLAIMED AND EXCLUDED BY US. IN NO EVENT SHALL WE BE LIABLE FOR ANY DIRECT, CONSEQUENTIAL, INCIDENTAL, PUNITIVE, EXEMPLARY, OR INDIRECT DAMAGES, OR FOR ANY LOSS OF PROFIT, REVENUE, DATA, COMPUTER PROGRAMS, OR OTHER ASSETS, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.
4. This report does not constitute an endorsement, recommendation, or guarantee of any of the products (hardware or software) tested or the hardware and/or software used in testing the products. The testing does not guarantee that there are no errors or defects in the products or that the products will meet your expectations, requirements, needs, or specifications, or that they will operate without interruption.
5. This report does not imply any endorsement, sponsorship, affiliation, or verification by or with any organizations mentioned in this report.
6. All trademarks, service marks, and trade names used in this report are the trademarks, service marks, and trade names of their respective owners.