Vendor Assessment Community

IANS

ZERO TRUST NETWORK ACCESS

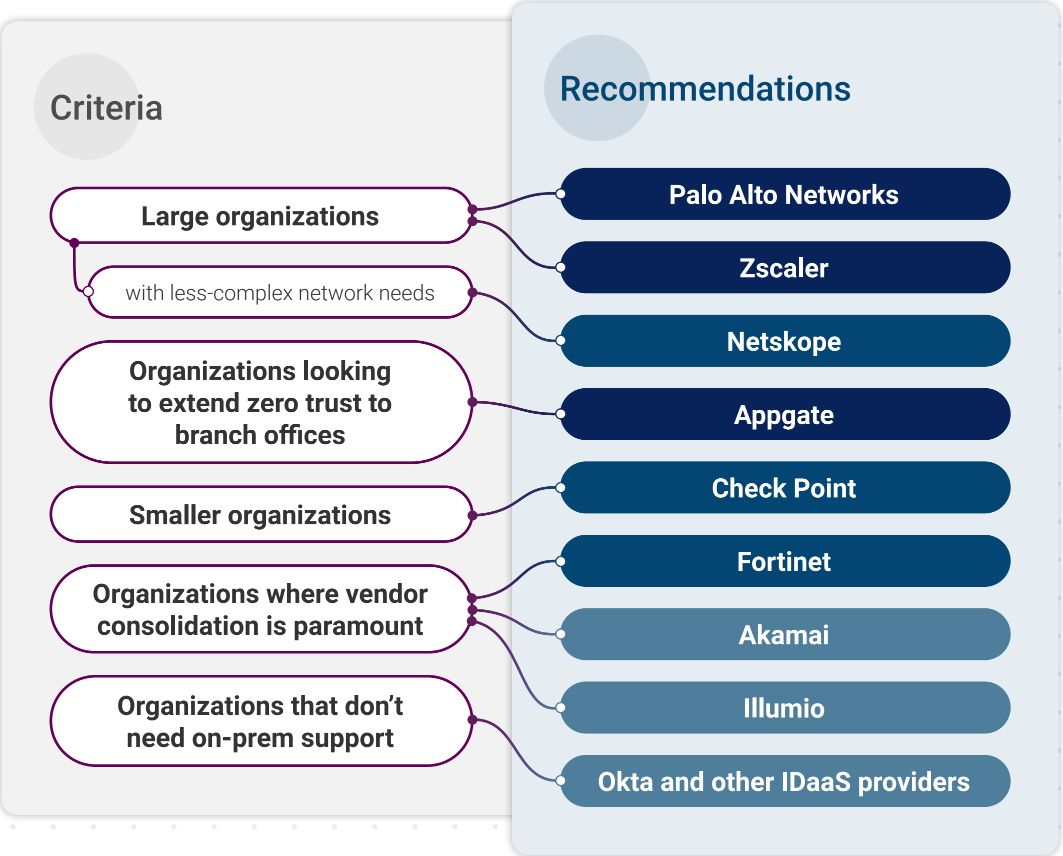
Market Guide

DAVE SHACKLEFORD, IANS FACULTY | MAY 2024

The Takeaway

Top zero trust network access (ZTNA) vendor options to date include: leaders like Palo Alto, Zscaler and Appgate; some challengers like Netskope, Fortinet and Perimeter 81; and some emerging innovators like Okta, Illumio and Akamai. This report details IANS' take on the current ZTNA market and provides our key recommendations for organizations looking to make an investment in ZTNA this year.

ZTNA Fit Guide



Criteria

Large organizations

with less-complex network needs

Organizations looking to extend zero trust to branch offices

Smaller organizations

Organizations where vendor consolidation is paramount

Organizations that don't need on-prem support

Recommendations

Palo Alto Networks

Zscaler

Netskope

Appgate

Check Point

Fortinet

Akamai

Illumio

Okta and other IDaaS providers

This summary report provides high-level insights from our Zero Trust Network Access Market Guide.

The complete Zero Trust Network Access Market Guide is a comprehensive, full breakdown that offers a detailed market overview and is available to

IANS clients through the IANS Portal or to non-clients upon request by contacting us at info@iansresearch.com.

The Market Space Today

ZTNA is a market made up of products and services that create an identity- and context-based logical access boundary that encompasses enterprise users and their cloud-based or hosted services or applications. This allows traditionally on-premises controls and capabilities like URL content filtering, user behavior monitoring and even core network traffic filtering to be offloaded to a cloud-based service provider. In addition, the notion of zero trust has expanded to allow for policies that determine what a user's normal access pattern is, and then automatically instantiate security capabilities when that pattern does not match. For example, a user logging in from a different device or failing authentication a certain number of times may be quarantined or required to enter an additional out-of-band authentication credential or token.

The market is converging somewhat, with cloud access security brokers (CASBs), secure service edge (SSE) vendors, content delivery networks (CDNs) and even identity-brokering solutions (sometimes called identity as a service, or IDaaS) all starting to offer ZTNA-like features and functionality. In essence, traditional market players like Zscaler are now moving into SSE/secure access service edge and CASB, and providers like Palo Alto that focused more on SSE/SASE are now expanding to ZTNA and CASB. IANS sees this market converging even more in the next one to two years, and what acronym "sticks" to describe it remains to be seen.

Main Features to Look For

Organizations considering ZTNA solutions should ensure the vendors they consider have a number of key features in place. Most of these are focused on flexible device and user identification and authentication, access control policies, and support for a variety of applications and services.

Shortlist Criteria

Primary considerations in terms of controls and capabilities for ZTNA include:

Endpoint client overhead and ease of deployment

Any leading ZTNA should have a relatively lightweight client that's installation and operation are both easy to deploy and validate.

Strong authentication

ZTNA should allow teams to create flexible authentication policies that integrate with MFA, directory services like AD and SSO, and any additional endpoint clients or certificates present. Step-up authentication (which triggers additional requirements if conditions aren't met) should be a staple.

Behavioral analysis

Many ZTNA solutions tout their machine learning (ML) and AI capabilities, which actually hold some water based on observation of numerous user accounts connecting to resources (any mature solution should be able to speak to this because monitoring and pattern recognition of many user activities is pivotal to security capabilities). Anomalous behaviors and conditions should be easy to codify and enforce in policy (e.g., a user's phone and laptop located in different countries shouldn't simultaneously be able to access protected resources).

Continuous monitoring

ZTNA should be capable of continuously monitoring any user access to resources to detect unusual behaviors or actions that may indicate a compromised system or account.

Flexible reporting

ZTNA reporting should focus on user and device behaviors, as well as any industry or cloud provider benchmarks, e.g., Center for Internet Security, AWS, Azure or Salesforce best practices, etc. Compliance-centric reporting should also be available, including leading regulations like PCI DSS and HIPAA.

Strong visualization

Given the vast array of different objects and services that might be available within any one cloud environment, let alone several, ZTNA should emphasize visualization of things like cloud networking, IAM policies and role assignments, and integrations across cloud services.

Top Solutions Compared

The table below provides a comparison of the top vendors in terms of technology, sales process, time to value, total cost of ownership, operations/maintenance and support.

Vendor	Technology	Sales Process	Time to Value	Total Cost of Ownership	Operations/ Maintenance	Support
Palo Alto Networks Prisma Access	Good	Average/Expected	Average/Expected	Average/Expected	Good	Good
Zscaler ZIA and ZPA	Good	Good	Good	Average/Expected	Good	Average/Expected
Appgate SDP	Good	Good	Good	Good	Average/Expected	Average/Expected
Netskope	Good	Good	Average/Expected	Average/Expected	Average/Expected	Good
Fortinet	Average/Expected	Good	Good	Good	Average/Expected	Average/Expected
Check Point Perimeter 81	Average/Expected	Average/Expected	Average/Expected	Good	Average/Expected	Average/Expected
Okta	Average/Expected	Average/Expected	Needs Attention	Needs Attention	Average/Expected	Good
Illumio Edge	Average/Expected	Average/Expected	Needs Attention	Average/Expected	Needs Attention	Average/Expected
Akamai Enterprise Application Access	Average/Expected	Average/Expected	Needs Attention	Needs Attention	Average/Expected	Average/Expected

Good Average/Expected Needs Attention

Source: IANS, 2024

Use Cases to Consider

Most users of ZTNA platforms want their tools to help with the following use cases.

Network access coverage

Breadth of coverage and granularity of access control policies should be considered a starting point.

Identity policy flexibility and granularity

User grouping and endpoint controls should be integrated with user directories, if at all possible, and endpoint identity controls should be easy to implement for a diverse group of systems. Ideally, ZTNA solutions can also integrate with other identity services and platforms like Microsoft Conditional Access, for example.

Flexible application connectivity

ZTNA should make it relatively simple to connect to both cloud and on-premises resources, with a streamlined user experience.

Cloud service integration

Are API-based methods supported for cloud services? This can greatly simplify integration with SaaS products for DLP and other policy controls.

Behavioral analysis for end-user activity

Strong ZTNA options should ideally have a massive-scale ML model that constantly evaluates common end-user activities and behaviors to better spot anomalies and illicit access attempts.

This summary report provides high-level insights from our Zero Trust Network Access Market Guide.

The complete Zero Trust Network Access Market Guide is a comprehensive, full breakdown that offers a detailed market overview and is available to

IANS clients through the IANS Portal or to non-clients upon request by contacting us at info@iansresearch.com.

Dave Shackleford

IANS FACULTY

Dave is the founder and principal consultant with Voodoo Security, an information security consulting firm with broad expertise. He is also a senior instructor, analyst and course author for the SANS Institute and a VMware vExpert with extensive experience designing and configuring secure virtualized infrastructures. Learn more.

Disclaimer: *Any views or opinions presented in this document are solely those of the Faculty and do not necessarily represent the views and opinions of IANS. Although reasonable efforts will be made to ensure the completeness and accuracy of the information contained in our written reports, no liability can be accepted by IANS or our Faculty members for the results of any actions taken by the client in connection with such information, opinions, or advice.*