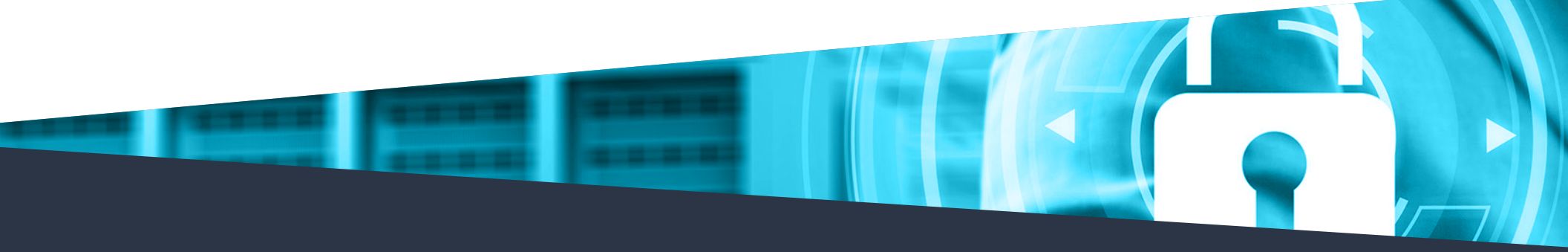

Prepared for

BANYAN SECURITY

Top 10 Points to Consider When Selecting a Zero Trust Network Access Solution

August 2022 EMA White Paper
By Chris Steffen, Managing Research Director and Ken Buckler, CASP, Research Analyst
Information Security, Risk, and Compliance Management

EMA™
IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Executive Summary

Zero trust is a set of principles designed to reduce or remove implicit trust in networked systems by addressing network identity, endpoint health, and data flows, to shift security focus from the network to users and devices. Going beyond the hype and technical jargon, zero trust is a safety net. It augments and reinforces the security measures of existing controls while allowing IT administrators to simplify and flatten their network. Zero trust abandons traditional "castle defense" security models and implements continuous authentication verification and validation, verifying user and device identities and access privileges throughout each entire session. Zero trust network access (ZTNA) is a network-based zero-trust approach that helps mitigate multiple threats, including malware network traversal, compromised credentials, and insider threats. It can also simplify your networks, make adding third parties like contractors both easy and secure, and improve the end-user experience. This white paper will explore the criteria to consider when evaluating a ZTNA solution for purchase and implementation. Properly implemented, an adversary on an organization's network with a ZTNA solution should be unable to do anything at all because they will be unable to see, let alone connect to, any devices or resources, while administrators and users should experience a simplified access experience regardless of location.

Top 10 Points to Consider

Selecting a solution is much more than "does it work?" Instead, multiple aspects must be considered.

1. Solution cost
2. Deployment difficulty
3. Administrative and end-user experiences
4. Integration capabilities
5. Network complexity
6. User, device, resource, and access visibility
7. Metrics and reporting
8. Least privilege access control
9. Continuous authorization
10. Device trust

Solution Cost

Some of the most obvious concerns with any ZTNA solution are upfront and recurring costs. Transparency and simplicity in pricing are extremely important, and organizations should be able to try a solution in a limited deployment scope before being committed to purchasing licenses for every user or device. Organizations shouldn't need to use a complex mathematical formula to estimate their purchase costs. They need to be able to quickly compare pricing and use that pricing as part of their total cost of ownership estimates without worrying about contractual fine print or hidden fees.

How long will a vendor's ZTNA solution take to deploy? Days? Weeks? Months? How much will initial deployment tests cost organizations, and will organizations be able to scale their costs with their deployment size? Not only must a user consider the solution's licensing costs, but also the man hours needed for deployment and maintenance. Imagine the cost to an organization if hundreds of man hours are used on a ZTNA deployment, only to discover it's not compatible with your environment. After all, you can't find out halfway through your deployment that the ZTNA solution you selected isn't compatible with your VPN or won't provide a data feed for your SIEM. Think of all the wasted man hours if you discovered such an issue. Security solutions should be an investment to an organization and you should be able to realize a return on that investment, not a loss.

An organization's infrastructure isn't going to remain static once a ZTNA solution is deployed. Hybrid and multi-cloud infrastructures are the norm today, growing in terms of size and complexity. Automated discovery of resources and applications is necessary to help administrators keep pace as network and cloud infrastructure evolves. Without automated discovery, the security team will spend significant amounts of time working with other teams to verify access requirements not only during initial setup of the ZTNA solution, but continuously as the organization evolves and grows.

Deployment Difficulty

How difficult will it be to deploy the solution to existing devices? What about new devices? Can you easily integrate with your existing infrastructure? Your IT team is extremely busy, typically wearing multiple hats and attempting to juggle system troubleshooting, network management, user access requests, and more. Deployment of a ZTNA solution must be quick and simple to ensure minimal impact to your IT team's precious time.

Automation is key for deployment success, through deployment to existing devices to endpoint management products, or adding the ZTNA solution to device build images. The ZTNA solution must support multiple deployment methods to protect your users faster, without providing additional stress for your IT administrators.

Administrative and End-User Experiences

User experience is critical in any ZTNA solution deployment, or any security deployment for that matter. If end users are unable to accomplish their work due to security controls, those controls are doing more harm than good. A good ZTNA solution must support "work from anywhere," providing the same user experience on or off campus, seamlessly granting users access to the applications and resources they need, and not ever revealing the existence of the ones they don't. Admins should be able to easily see coherent user, device, and resource access activity without having to interrogate different systems based on user or resource location.

Many users reuse passwords, mostly because of password complexity requirements. This means a compromise of a user's home email account could quickly lead to a breach of the enterprise network. With over 22 billion user credentials currently circulating on the dark web, it's time to move beyond password authentication and enable verified users access to infrastructure, applications, and resources with a single click. A mature ZTNA solution will allow users passwordless access to resources, removing reliance on sticky notes, their memory, or password managers to juggle login credentials for every single application or server. Of course, when there aren't any credentials to remember there's no risk of loss or theft, and one of the consistent top sources of filed IT help desk tickets simply goes away.

Identity management becomes more challenging and more complex as organizations grow. Access requests need to be simplified through a single tool instead of distributed across multiple identity management interfaces. A mature ZTNA solution should be capable of simplifying access requests and identity management. This simplification means more efficient help desk employees, spending less time on access requests and more time on solving problems. The IT team should want to install the ZTNA solution because they will consider it a time saver, simplifying their management duties and allowing more time for higher-value activities.

Integration Capabilities

To be truly effective, ZTNA solutions must integrate with your existing environment. This includes integration with IaaS, PaaS, and developer resources, such as SSH, RDP, VNC, Kubernetes, databases, and more. Integration with your existing cloud, identity access management, mobile device management, endpoint detection and response, and user behavior analytics tools is a must.

Automated provisioning of user accounts, such as through IaaS or infrastructure as code, is critical for the success of a full-featured ZTNA solution. At the end of deployment and integration, users should look at the ZTNA solution as an investment, amplifying the return on investment of the security tools already present in your environment.

One of the biggest integration challenges will be the switchover from legacy VPN to ZTNA. The preferred method for implementing this switch is through a service tunnel. This service tunnel would allow legacy VPN to be decommissioned while maintaining traditional network flows and finetuning the ZTNA product in monitoring mode. Once sufficient monitoring is achieved and policies are built, the ZTNA can switch to enforcement mode, with the service tunnel enforcing least-privileged access and continuous authorization with device trust. This method allows transition to a zero-trust architecture while providing security for situations that aren't yet ready for the switchover.

Network Complexity

VLANs, subnets, 802.1X, NAC, whitelisting, etc.—these legacy technologies served their purpose, but it's time to flatten and simplify the network. By flattening the network, additional cost savings can be realized, both in reduced network management man hours and reduced network equipment.

Properly implemented, ZTNA should simplify the network administrator's job, not make it more complex. Reducing network complexity not only makes a network administrator's job easier, but also simplifies incident response in case of a network breach.

User, Device, Resource, and Access Visibility

Lack of visibility means lack of coverage. Lack of coverage means lack of protection. ZTNA solutions must provide full visibility into what's happening across all users, devices, and applications. Every login, every connection, and every administrative escalation need to be recorded and reported to a central management console. Without this full visibility coverage gaps will occur, creating a risk to the enterprise because you can't secure what you can't see. This goes beyond traditional network traffic flow analysis, analyzing user interaction with devices, resources, applications, and data repositories.

Metrics and Reporting

Security is an investment, and any ZTNA solution must provide accurate, actionable reports to help demonstrate that return on investment and progress along the zero trust journey. Accompanying network visibility, administrators and analysts must be able to view insightful, actionable reports of that visibility and take swift action to respond and remediate. This means having the ability to look at overviews of your organization's network and examine what a particular class of worker is accessing (e.g., contractors or drilldown all the way to the host level).

Least Privilege Access Control

Accounting, Human Resources, Sales…these are all separate departments and companies should treat them as such from a network perspective. There's no reason these separate departments should have access to unnecessary resources, let alone be able to communicate with the endpoints used by other departments.

Legacy VPNs and legacy on-premises networking models allow overly broad access to an entire organization's network. This network model allows excessive network traversal, with unintended lateral movement across the entire enterprise.

A mature and properly implemented ZTNA should allow for segregation of employees from other departments regardless of physical location, helping to reduce the possibility for network traversal of malware like ransomware or intentional and unintentional insider threats.

Continuous Authorization

Traditional authentication methods that utilized credential caching were necessary due to bandwidth limitations of early computer networks. However, as computer networks have evolved, authentication methods have not. It's time to change that.

One of the key principles of ZTNA is that users and devices must be continuously verified for authorization. This means a user isn't going to be granted permissions based on initial authentication, but granted or denied access based on authorization that is continuously checked. If a user's access is revoked or a device's security posture becomes unacceptable, their application or resource access should be terminated in real-time. No waiting for active directory replications or network connection timeouts.

Device Trust

Trust-based access control is the next step beyond password-based access and role-based access control. Looking beyond simple user permissions, is the account connected to a trusted device, and is that trusted device compliant with all security requirements? If so, then going "passwordless" is entirely possible, with end user access becoming entirely frictionless.

Let's be honest, most users reuse passwords from other accounts. This means that a compromise of an employee or contractor's streaming media or social networking account can lead to a compromise of an organization's corporate network. Even once it's discovered and passwords are changed, there is typically significant lag time between updating credentials and session timeout.

By combining user and device trust validation, the ZTNA solution should go beyond simple user authentication validation and incorporate device identity and security posture and resource sensitivity, revoking access mid-session if any component fails to pass muster. This protects not only unauthorized device access, but unauthorized data access, and significantly reduces the risk of compromised credentials. While the added security helps the security team sleep at night, the simplified access allows better support for "bring your own device," including remote users, contractors, partners, and other authorized third parties.

Simply put, device trust in ZTNA should provide rapid, secure access to the environment, empowering a more secure, more efficient workforce.

EMA Perspective

With so many vendors offering ZTNA solutions, it's easy to get lost in the noise. When evaluating a ZTNA solution, it's important to look beyond the buzzword hype and understand what the platform is really doing and how it interacts with users, the security team, and network administrators. All of these aspects will help determine if a ZTNA deployment is successful.

Banyan Security can be deployed in most environments in 15 minutes or less and provides a free version for deployments of up to 20 users. It automatically discovers changes to the environment, including new devices, resources, and applications. Integrations are available with Amazon Web Services (AWS), Carbon Black, Citrix, CrowdStrike, Google Cloud Platform (GCP), Jamf, Microsoft Azure, Oracle Cloud Infrastructure (OCI), SAML, VMware, and more, ensuring compatibility with your environment without having to purchase additional security tools to replace your existing coverage. Featuring one-click access to resources, simplified identity management, and a universal user experience regardless of user location, Banyan Security provides an optimized user experience while creating a more secure network.

EMA believes that Banyan Security's ZTNA solution meets all the criteria needed for a successful, secure ZTNA deployment and would be a worthwhile investment for any organization looking to implement secure "work from anywhere" access using a foundation built on zero trust.

About Banyan Security

Banyan Security provides secure, zero trust "work from anywhere" access infrastructure and applications for employees, developers, and third parties without relying on network-centric legacy VPNs. Deep visibility provides actionable insight while continuous authorization with device trust scoring and least privilege access deliver the highest level of protection with a great end-user experience. Banyan Security protects tens of thousands of employees across multiple industries, including finance, healthcare, manufacturing, and technology. To learn more, visit **www.banyansecurity.io** or follow us on Twitter at **@BanyanSecurity**.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at **www.enterprisemanagement.com**. You can also follow EMA on **Twitter** or **LinkedIn**.

1995 North 57th Court, Suite 120, Boulder, CO 80301 +1 303.543.9500 **www.enterprisemanagement.com**

4204.080822