Enterprise Strategy Group | Getting to the bigger truth.™

RFP Checklist:

Ten Things Organizations Should Look for When Considering ZTNA Solutions

As organizations move forward with long-term planning to ensure application-focused, secure access for a highly distributed workforce and application environment, IT leaders should add the following items to their RFP checklist.

Zero trust network access solutions should:

1. FOCUS ON LEAST-PRIVILEGE AND ZERO TRUST.

While it may seem as though all tools positioned as zero trust network access would inherently support zero trust principles, including least-privilege, that is not always the case. ZTNA is not simply moving VPN to the cloud, but fundamentally changing the way users remotely access corporate resources. ZTNA tools must take a default deny posture and ensure access is provided only to a specific application or resource and not the broader network segment. Further, this access should not be granted until proper authentication has occurred. Additionally, authentication should be based on a variety of factors, including identity, device, and deeper context of the request, such as time and geolocation.

2. CONTINUOUSLY ASSESS AND MONITOR CONNECTIONS.

Just as importantly, even after the initial connection is initiated, the session should be continually assessed. If the risk level changes due to the health of the device or activity of the user, the session may need to be reauthorized, the level of access may be reduced (to read-only for example), or the connection may be terminated.

3. PROVIDE GRANULAR VISIBILITY AND REPORTING.

ZTNA solutions facilitating access on an application-by-application basis provide a deeper level of visibility than traditional VPN solutions. Rather than reporting on IP addresses and higher-level network access, ZTNA solutions should report on groups and users as well as the specific applications they are accessing. This enables administrators to investigate issues and troubleshoot problems much more quickly and efficiently.

4. SUPPORT BOTH AGENT-BASED AND AGENTLESS DEPLOYMENTS.

An agent-based ZTNA approach is required for access to some types of applications and for better visibility into the health and posture of the user's device prior to authenticating. Yet agentless models can provide an attractive alternative to support third-party access and prevent agent sprawl in cases where that may be a concern. The flexibility to support both models allows organizations to expand ZTNA deployments to additional use cases over time.

5. ENABLE ACCESS TO DIFFERENT TYPES OF APPLICATIONS.

Many applications are shifting to the cloud, yet a number continue to remain in on-premises data centers for one reason or another. Similarly, many applications are web-based, but others rely on SSH, RDP, or other non-web protocols. ZTNA solutions should provide access across a variety of different application locations and types. When combined with the support for both agent and agentless approaches, broad application coverage can provide organizations a path towards full VPN replacement.

6. BE BUILT ON A SCALABLE AND RELIABLE PLATFORM.

ZTNA solutions delivered via the cloud require a global infrastructure to ensure minimal latency for users accessing corporate resources. One of the key issues with VPN is the need to backhaul traffic to a central point, which can affect performance and negatively impact the user experience and productivity. If ZTNA traffic must be routed to data centers in other countries or regions, only to circle back to the region of origin, the same issues can occur. With application access as critical to business productivity as it is today, a global distributed infrastructure to ensure minimal latency and provide redundancy, coupled with service level agreements (SLA) guaranteeing at least five nines uptime, is critical to ensure users can quickly access the resources they require to do their jobs at all times.

7. INCLUDE A BROAD ECOSYSTEM OF IDENTITY INTEGRATIONS.

Many organizations now use a variety of identity providers across their on-premises and cloud environments. This creates complexity, but consolidating providers is often not possible. As a result, ZTNA solutions should offer integrations with a wide range of identity vendors to simplify deployment and help reduce complexity.

8. ENSURE CONSISTENT USER EXPERIENCES.

Today, security solutions must not only protect but also enable the business. Solutions must be easy for users to navigate and not impact their productivity. With many organizations planning for a shift toward hybrid work, ensuring consistency for users wherever they are and whatever resource they are accessing is critical. There may be small differences based on the type of the device being used or additional authentication mechanisms depending on the level of risk. However, the core method of how users access the applications they use to do their jobs should not deviate widely based on where they are.

9. INCORPORATE INTEGRATIONS WITH BROADER ZERO TRUST OR SASE PLATFORMS.

The goal of ZTNA is to prevent attacks from occurring by limiting access. Yet the reality is that threats can and do slip through. So, while ZTNA may be undertaken as a standalone project, it is increasingly part of a broader initiative to incorporate additional context and capabilities through the integration with threat prevention and DLP tools. This is often accomplished through secure access service edge (SASE). SASE architectures converge a variety of security and network capabilities in a cloud-delivered model to provide centralized management and consistent, distributed enforcement for users regardless of location. While SASE is a broad initiative incorporating a long list of capabilities, ZTNA has quickly become a critical component of the architecture. By including ZTNA in a SASE architecture, organizations can limit their threat surface, prevent threats that do bypass defenses from compromising systems, and ensure that attempts to exfiltrate data by attackers or malicious insiders are prevented.

10. PROVIDE A CONSISTENT MANAGEMENT EXPERIENCE.

Similarly, security teams are too often overworked and understaffed. Finding solutions that support organizational efficiency to overcome these issues and ensure consistent security by avoiding human error is critical. This requires more than just functional integrations to support broader zero trust and SASE approaches, but a common management experience so that access rules are consistently applied with administrators having to replicate policies.