ANALYST CONNECTION

Sponsored by: Citrix, a business unit of Cloud Software Group

ZTNA adoption and the discontinuation of VPN services is a unique journey that is based on existing security investments, business goals and workflows, and budget/timeline. Choosing a suitable ZTNA vendor to meet these needs can make all the difference between a seamless deployment and continuing to rely on VPNs for the foreseeable future.

Careful Considerations for Choosing a Zero Trust Network Access Product and Vendor

July 2024

Questions posed by: Citrix, a business unit of Cloud Software Group

Answers by: Pete Finalle, Research Manager, Security & Trust; Christopher Rodriguez, Research Director, Security & Trust; and Mike Jude, Research Director, Endpoint Security

Q. What is driving the need for zero trust network access?

A. Zero trust network access (ZTNA) adoption is being driven by the emergence of hybrid work and the need to securely connect users and devices regardless of their location to applications and resources both on premises and in the cloud as well as a waning desire from buyers to depend on legacy backhauling technologies, such as virtual private networks (VPNs). Migrating away from VPNs has two key benefits — improving overall connectivity and performance to enable productivity across the enterprise and reducing security risks through the embrace of a modern, zero trust approach to access. Specifically, least-privilege access and continuous monitoring and enforcement even for authenticated and established user sessions helps reduce security risks.

However, despite the need for ZTNA adoption, many customers struggle to fully deploy the technology and VPN reliance remains for custom or legacy applications that cannot be quickly ported over to the new technology. In these cases, a vendor that can provide a suitable upgrade path is a necessity for a smooth and successful migration. ZTNA solutions that share a management interface and agent/software and provide operational flexibility with VPNs can be invaluable for customers navigating a complex migration.

Every zero trust journey is unique and dependent on existing security and networking infrastructure, business requirements, industry-specific compliance audits, budget allocation, and new security deployment timelines. Thus the in-house components with which a ZTNA solution integrates should be chosen through a strategic lens that best aligns with customer business goals and workflows. In addition, not all integrations are created equal and the volume of integrations is often less impactful on security posture than deeper integrations across critical components.

Q. How does VDI play into the broader ZTNA space with respect to securing access to virtualized applications?

A. Virtual desktop infrastructure (VDI) is an integral business application that not only creates a streamlined work environment across dissimilar devices and operating systems but also simplifies the security of endpoint devices and the access path on the network. VDI was designed to be application focused and hence does not provide any access to the underlying network. Access to applications granted by the administrators to VDI users is tightly controlled and can be revoked dynamically. Hence, VDI was designed on the zero trust principles long before zero trust frameworks gained adoption.

By integrating with a VDI solution, ZTNA can extend zero trust concepts and policies end to end, from the network access to the endpoint. Thus meaningful integrations between ZTNA and VDI can benefit buyers by providing a shared identity and device posture as well as a streamlined experience across virtualized, web, and cloud resources. ZTNA and VDI are a logical integration that ultimately improve the application end-user experience while regulating what can be accessed and how it is accessed. For external traffic, best-of-breed ZTNA solutions should be capable of coexisting with secure web gateway (SWG) and cloud access security broker (CASB) controls offered by other third-party security service edge (SSE) vendors.

The combination of VDI and ZTNA is a mutually beneficial relationship that combines enhanced visibility of network traffic that is in motion with deeper, device-level detail regarding what is happening on the endpoint. This has the effect of significantly improving the ability to implement consistent security controls across both technologies and reducing blind spots throughout the network environment. In addition, application end users also benefit from this combination through a unified access experience, which simplifies usage, without requiring additional consoles, agents, or configurations on the endpoint. Further benefits exist for IT helpdesk and technical personnel as the unification of VDI and ZTNA reduces management complexities and streamlines remediation workflows, resulting in improvements to overall enterprise operational efficiency and important IT metrics such as time to remediation.

Q. When does it make sense to deploy a best-of-breed ZTNA solution that is not part of an SSE or SASE solution?

A. Current SSE and SASE offerings attempt to be all things to everyone by integrating as many security components together as possible, with little regard to vertical industry requirements, number of users/devices/resource locations, and existing technical investments. This can steer customers away from top-quality, standalone products, which do not inherently require or benefit from tighter integrations with the rest of the SSE/SASE stack. In fact, many buyers can benefit from choosing best-of-breed solutions in situations where they are enhanced more by integrations outside of network security platforms.

For these buyers, this could mean retaining well-entrenched products, which they are satisfied with, instead of downgrading to a lower functionality product that is more deeply integrated with their SSE/SASE. This scenario is typically limited to established security components such as CASB, SWG, and firewall. However, ZTNA is often a net-new addition and focused specifically on access control for only known, authorized users to limited private resources compared with the broad internet access controlled by CASB and SWG, with buyers faced with the opportunity to be fastidious from the very beginning. ZTNA products vary significantly in capabilities and performance and choosing to invest in the right product for meeting strict security goals is often more important than any commitment to an SSE/SASE provider's platform.

Thus the importance of choosing a suitable ZTNA vendor cannot be overstated as switching vendors or migrating to new solutions after the process of decoupling from VPNs has begun is both costly and time-consuming. For most buyers, the correct ZTNA vendor is the one that can help them cross the finish line, accomplishing complete VPN replacement over a reasonable amount of time. This requires simplifying the adoption process, providing comprehensive application discovery and compatibility, and aiding buyers in integrating legacy applications and difficult-to-secure devices into the solution. In addition, vendors that provide both a VPN and ZTNA product are uniquely situated to provide a smooth transition from one technology to the other, which allows for a quicker migration with minimal impact on business productivity.

Standalone ZTNA solutions should also offer flexible interoperability, which allows buyers to custom tailor the rest of their network security stack to meet their needs. Choosing a best-of-breed ZTNA solution should not limit a buyer to that vendor's ecosystem; it should instead allow buyers to choose other products or SSE components while leveraging existing, meaningful integrations that allow for simplified management, policy portability, telemetry sharing, and indicators of compromise/threat-detection sharing.

This creates a best-of-both-worlds type of scenario, where the benefits of best-of-breed products do not limit the cross-functional benefits of a multivendor network security deployment. Thus flexibility and multivendor compatibility are extremely important for maximizing best-of-breed investments so that these products do not function in a vacuum, isolated from other tools that would benefit from deeper cooperation.

Q. When selecting a ZTNA solution, who are the key stakeholders/ decision-makers?

A. Like legacy VPN products, ZTNA affects all personnel within an adopting organization, making the entire company a stakeholder with a vested interest that reliance on a VPN is reduced, if not eliminated, and that ZTNA is broadly adopted and able to secure as many users/devices and applications/resources as possible. In addition, ZTNA is not only a security tool but also a networking/access technology, and both networking and security teams are likely to have a hand in managing the solution as well as approving its purchase in the first place. A successful ZTNA deployment must satisfy the goals and requirements of either department, and with a direct correlation to productivity enablement, many other decision-makers are likely to weigh in before committing to a ZTNA vendor.

However, adoption is still a journey for ZTNA and few enterprises are in a position to quickly rip and replace their existing VPN solutions, which places a significant burden on decision-makers. Choosing the correct ZTNA vendor requires not only foresight but also that other security and networking goals align with the decision. While it is important for a ZTNA to be broadly integrated across other security tools and products, it is often more important for buyers that it is tightly integrated with their existing products and tools that comprise essential business workflows. Thus most ZTNA purchases are made with familiar vendors, which can maximize existing investments and reduce the complexity of integration with existing security products.

About the Analysts

Pete Finalle, *Research Manager, Security & Trust*

Pete Finalle is a research manager for IDC's Security & Trust team, currently responsible for the Trusted Access and Network Security coverage area. Pete's core research coverage is focused on network security hardware, software, and public cloud services, spanning foundational components such as firewall, IDS/IPS, VPN, NAC, SWG, and CASB as well as new concepts such as zero trust network access and network edge security as a service.

Christopher Rodriguez, *Research Director, Security & Trust*

Christopher Rodriguez is a research director in IDC's Security & Trust research practice focused on the products designed to protect critical enterprise applications and network infrastructure. IDC's Security & Trust research services — to which Chris contributes — include Network Security Products and Strategies and Active Application Security and Fraud.

Mike Jude, *Research Director, Endpoint Security*

Dr. Mike Jude is the research director for the IDC Endpoint Security practice within the Security & Trust group. Jude's core research coverage includes solutions that defend personal computing devices, physical servers, and mobile devices against a widening array of cyberattacks.

MESSAGE FROM THE SPONSOR

Citrix, a business unit of Cloud Software Group, pioneered secure remote access for the workplace. Built with a zero-trust architecture, the Citrix platform is designed for enterprises seeking to expand beyond traditional virtual desktop infrastructure (VDI) to modern desktop-as-a-service (DaaS). To power today's hybrid workforce, Citrix gives IT the ability to deliver, secure, and manage any application for any user on any device, both on-premises and in the cloud. www.citrix.com

IDC Custom Solutions

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
blogs.idc.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.