Best Practices for Implementing Zero Trust Network Access

Published 10 June 2021 - ID G00744105 - 5 min read
By Analyst(s): Lawrence Orans, John Watts, Neil MacDonald

Initiatives: Infrastructure Security

Client inquiries into Gartner on the topic of zero trust network access have more than doubled in the past year. ZTNA deployments must be treated differently than traditional VPNs. Discussions with early ZTNA adopters reveal key factors for success for security and risk management leaders.

Overview

Key Findings

- There is strong interest in zero trust network access (ZTNA). Gartner inquiries on this topic have grown 127% in the first four months of 2021, as compared with the same period in 2020.

- ZTNA adoption has been accelerated by COVID-19 and the shift to remote work, which created scalability and performance issues with traditional virtual private networks (VPNs).

- The most common use case for ZTNA is a partial replacement of a traditional VPN (many end-user organizations have reported that they still need a traditional VPN for some applications).

Recommendations

For security and risk management leaders responsible for infrastructure security:

- Apply specific policies to user groups to control access to sensitive applications early in the deployment. Don't implement ZTNA like it's a traditional VPN (don't provide wide open access to all applications).

- Document application usage before starting your ZTNA implementation, then begin the process of mapping users to applications before deploying your ZTNA solution.
Introduction

Interest in ZTNA is very strong. Inquiries from Gartner clients (end-user organizations only, not vendors) grew 127% during the first four months of 2021, as compared with the first four months of 2020. The most common use case for ZTNA is replacing a traditional VPN.

Although there is a lot of excitement over the benefits of ZTNA, end-user organizations lack experience in implementing it. In this research note, we identify best practices from early adopters, so that you can learn from their experiences and enable a smoother and more efficient ZTNA implementation.

Feedback from early adopters of ZTNA indicates that five points are crucial to a successful project. These are outlined in Figure 1 and elaborated on in the Analysis section further down.

- Clean up application access privileges as part of your ZTNA project by, for example, blocking access for contractors who are no longer associated with your organization.

- Tune your application access policies as an ongoing and iterative process. As your business requirements change, your application access policies should change too.

- Negotiate with business leaders to overcome objections to ZTNA. For example, if business executives express concerns about changes to the user experience, highlight how the ZTNA model can be adapted to ease the user experience (less restrictive authentication) or tighten the user experience (more restrictive authentication) depending on context.
Analysis

Do Not Implement ZTNA Like It’s a Traditional VPN

Some end-user organizations have reported that, initially, they had configured ZTNA to grant users access to all applications, which is similar to how they have configured their traditional VPN. The problem with this approach is that the enterprise is not realizing the full benefit of ZTNA. Before deploying ZTNA, you should identify the use cases where ZTNA matters (for example, controlling access to sensitive applications or granting access to contractors) and apply specific policies to appropriate user groups. By quickly applying policies that restrict access to sensitive applications, end-user organizations will benefit more readily from ZTNA.

Document Application Usage Before Starting Your ZTNA Implementation
Many organizations wait until they implement the ZTNA solution before they start to study the relationship between users and applications. They begin by using the application discovery tools that are provided by the ZTNA vendor. However, some early adopters report that they “got ahead of the curve” by starting a discovery process before implementing the ZTNA solution. For example, they interviewed business leaders of specific departments (marketing, finance, etc.) to determine which applications their teams use and which contractors require access. This approach enabled them to set a standard for each team (which applications to allow) and let them progress more rapidly with the ZTNA deployment. Even with the application discovery tools, ZTNA project managers report that it’s a lot of work to identify which users need access to which applications, so it’s best to start this effort early.

**Clean Up Access to Applications**

Take the opportunity to eliminate application access privileges and entitlements that are no longer relevant. Meet with the business teams and the applications teams to ensure that all user access rights are current. Several early ZTNA adopters reported that they were able to change or eliminate access privileges of users who had transitioned into different roles or who had left the company. Some early adopters also reported that they terminated access privileges of third parties (contractors) with whom they no longer had business relationships.

**Continuously Tune Policies to Meet Changing Business Needs**

End-user organizations that are experienced with ZTNA deployments report that they are continuously tuning remote access policies as their business needs evolve. It’s not realistic to take a “set and forget” approach with ZTNA policies. As new applications (or seasonal applications) are deployed, the ZTNA team will need to add new access policies. Access policies may also need to be updated as an application evolves or when business leaders identify the need for more granular or restrictive policies. The ZTNA team should adopt the mindset that they will always be improving and refining access policies over time.

**Negotiate With Business Leaders to Overcome Objections**
Some business leaders may raise objections about changes to the user experience as a result of migrating to ZTNA. Advise these business leaders that the new ZTNA model allows for greater flexibility than traditional VPNs. Multifactor authentication (MFA), based on context, is an example. MFA can be bypassed if a user attempts to access an application with a corporate owned and managed device. However, MFA will be required if the user attempts to access an application with a personally owned device. The additional flexibility that is inherent in ZTNA solutions may help to alleviate concerns about transitioning to this new technology.

Evidence

We interviewed multiple early adopters of ZTNA technology.

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

- Market Guide for Zero Trust Network Access
- 2021 Strategic Roadmap for SASE Convergence
- What Are Practical Projects for Implementing Zero Trust?