7 Effective Steps for Implementing Zero Trust Network Access

Published 3 October 2022 - ID G00772715 - 18 min read

By Analyst(s): Dale Koeppen, Neil MacDonald, John Watts

Initiatives: Infrastructure Security

Zero trust network access is now typically deployed to replace remote-access VPN, but overly complex policies are inhibiting adoption. Security and risk management leaders must adopt a continuous life cycle approach to remote-access management in order to achieve success.

Additional Perspectives

- Summary Translation: 7 Effective Steps for Implementing Zero Trust Network Access
  (25 October 2022)

Overview

Key Findings

- Historical architectural behavior remains consistent amongst remote access buyers and this behavioral gap creates a challenge for zero trust network access (ZTNA) adoption. ZTNA is not a “fire and forget” technology; it is inherently dependent on a continuous iterative process, which requires the access policy to adjust as the business and risk levels change.
- Some end-user organizations have reported that they have completely replaced traditional VPN with a cloud-hosted ZTNA solution, but experienced challenges with policy development during the implementation.
- ZTNA might provide benefits over traditional VPN; however, its deployment should be in alignment with the business’ zero trust strategy, with the business leaders’ remote-access requirements for its user base, and conducted using a risk-based methodology to optimize the organization’s security posture.
- In 2022, a strong interest and trend toward implementing zero trust strategies into the business environment has continued. Inquiries on this topic have grown 34% in the first 6 months of 2022, as compared with the same period in 2021.

Recommendations

Security and risk management leaders responsible for infrastructure security should:

- Use a continuous life cycle approach to gain a clearer understanding of remote-access risk levels and the necessary policy requirements, and to be in a position to adjust access policies based on the business’ risk appetite.
- Use the tenets of zero trust to develop key dialogues with business leaders, which will provide guidance and help attain their business objectives prior to implementing any ZTNA technologies, rather than function as a siloed answer.
- Build policy governance paradigms to help define “who has access to what,” based on user, device, application and data classifications. Start with identity and access requirements.
- Conduct regular assessments to confirm the isolation of the protected resources and validation of the user access rights to the resources.

Introduction

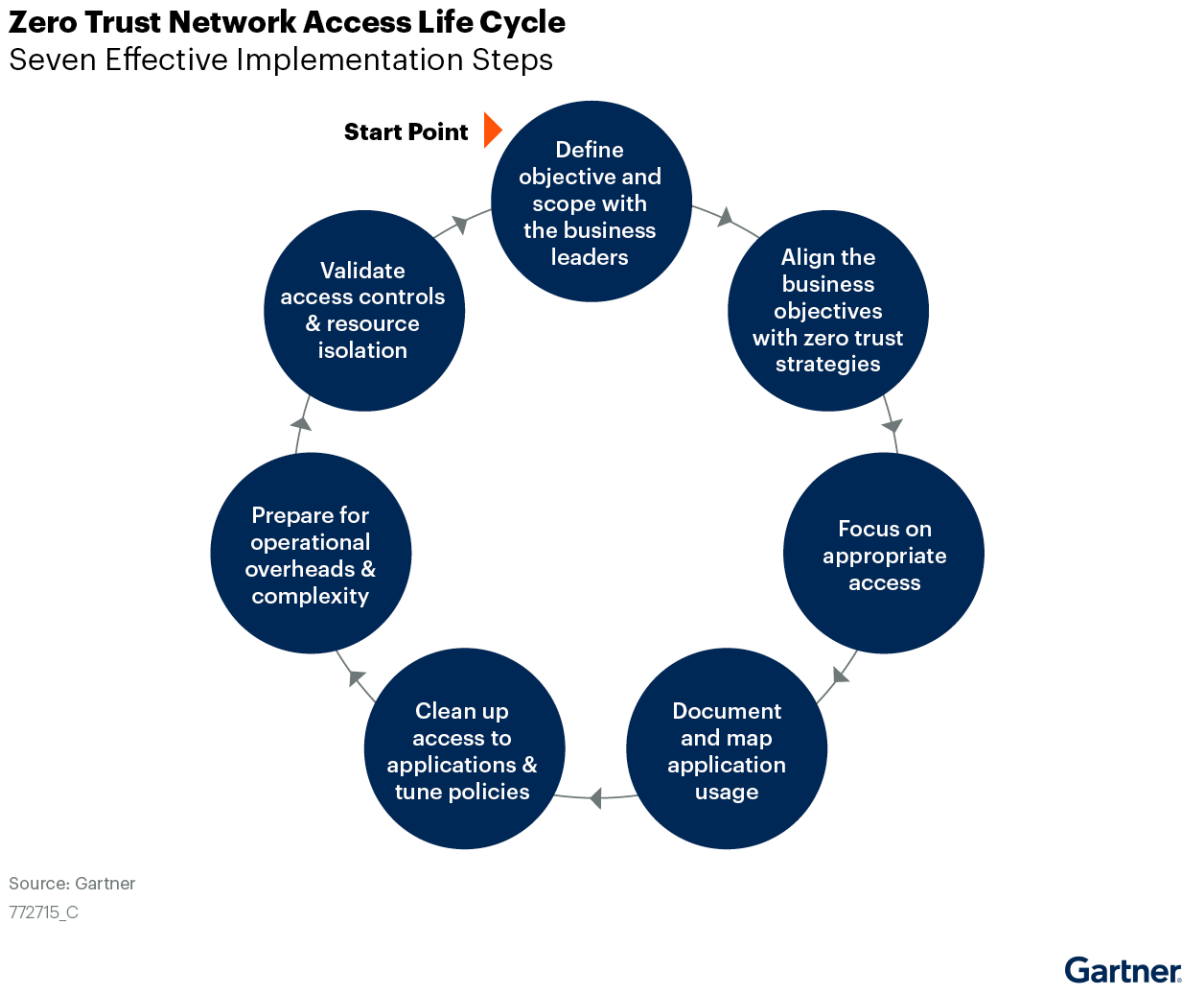
ZTNA offerings are becoming increasingly popular as a method for providing users least privilege to business applications, in lieu of traditional remote-access VPN. Traditional remote-access VPNs are still mostly visible in the form of license renewals and gateway upgrades. However, these mature VPN technologies continue to address situations where the ZTNA stack didn't meet the technical requirements for integration, or where the ZTNA pilot hasn't convinced key decision makers.

While many clients and vendors have consolidated ZTNA into the cloud-delivered approach of security service edge, Gartner still sees this ZTNA capability deployed as a stand-alone solution for some specific use cases, such as securing remote access to an extended workforce that remotely maintains operational technology (OT) or Internet of Things infrastructure, or application access where specific supervised session management is a requirement.

Despite the continued steady adoption of ZTNA, and the security benefits that it provides, end-user organizations still struggle with policy development to successfully deploy ZTNA. This research note outlines a practical approach that businesses can embrace so that security and risk management leaders can avoid the pitfalls and enable a smoother and more effective ZTNA implementation.

ZTNA implementation requires a continuous life cycle approach, and this approach can be broken down into seven steps that are crucial to a successful deployment. These steps are outlined in Figure 1 and elaborated on in the Analysis section further down.

Figure 1: Zero Trust Network Access Life Cycle



Analysis

Define Objective and Scope With Business Leaders

One of the more challenging aspects of an effective implementation of ZTNA is managing the expectations of both the business leaders and the end-user community. Some business leaders will have concerns about implementing ZTNA and its impact on end-user experience, policy administrators or change management processes.

Security and risk management leaders must work with the business leaders to understand their objectives in order to develop a strong foundational zero trust strategy. Collaboration with the business leaders is the “must-have” groundwork that drives the eventual mapping between the business objectives and the end-state goal of selecting, implementing and configuring a ZTNA technology solution to achieve the desired outcome.

While consulting with the business leaders, emphasize how ZTNA will mitigate business risk while improving usability and manageability. Advise these business leaders that the new ZTNA model allows for a more secure connection to resources than traditional access methods, while establishing a stronger security posture for the business. The enhanced security that is possible within ZTNA solutions and the flexibility of policy adjustment will help to alleviate concerns about transitioning to this new technology.

Develop a structured scope that consists of a core group of applications, users and devices, generally starting with an "easy use case" as part of an initial proof of concept, like fully remote knowledge workers. Then work with the business leaders to identify the most complex users within this group, such as privileged contractors doing remote maintenance or local admin working remotely. By identifying both ends of the ZTNA user spectrum and the deployment complexity, security and risk management leaders will set the right expectations about transition steps and timeframes.

This group will form the baseline from which to measure progression and should outline the applications that will and will not be included, like legacy technologies that are not suited for ZTNA (e.g., mainframes), as well as which uses will be included as part of the initial project. This structured grouping will follow through each section described throughout this research, and the business will iterate with additional applications and users over time.

Choosing a ZTNA technology provider ideally should not precede strategic planning with business leaders. The strategic planning will eventually shape the feature requirements and drive the selection of the evaluation metrics for a potential ZTNA technology provider. However, Gartner has witnessed examples where a small pilot with a ZTNA provider helped refine expectations and increased internal knowledge. If a ZTNA product has been acquired, proceed with the recommendations in this research and adjust the business expectations based on the product's capabilities.

Align Business Objectives With Zero Trust Strategies

Zero trust is a strategic approach that replaces implicit trust with continuously assessed explicit trust. It is based on identity and context that is supported by security infrastructure that adapts to an organization's risk appetite to improve the security maturity. At the highest business level, several key principles of zero trust are:

- Operate on an assume-compromised model.
- Use identity and context as the foundation for access decisions.

- Never implicitly trust; always verify before allowing access.
- Provide just enough access to resources.
- Remove implicit trusts; implement explicit trust.
- Encrypt data at rest and in motion.
- Monitor in real time and validate all actions.

Ultimately, zero trust securely connects users to applications. Security and risk management leaders must balance the security of the organization against the business goals for each business unit and build policies that enhance business productivity. For example, setting a continuous trust assessment dependent on a highly variable context or taking binary block-and-allow actions result in end-user frustration. ZTNA must rely on quality signals to build a reliable trust score, and provide a good context and messaging to end users about why access is restricted or blocked. This approach will vary depending on industry type, business size, regulatory requirements, cloud adoption roadmap and the internal data classification.

The building blocks for a zero trust strategy are as follows:

- A **common identity management construct** that defines:
  - The users (accounts) requiring access to a destination
  - The devices (source endpoints) being used to access a destination service
- A set of **adaptive access controls** that defines the permissions, which require:
  - Integration with the identity construct
  - Establishment of device context associated with the user requiring access
  - Identification and discovery of the workloads, systems and applications as the destination
  - The appropriate access control based on risk tolerance

This approach and its principles should become a guiding star for security and risk management leaders as they progress with the deployment of ZTNA and any other related technology that may align with zero trust principles. [1]

Focus on Identity and Appropriate Access

Some end-user organizations have reported that they have configured ZTNA to grant users access to all applications, which is similar to the configuration of their traditional VPN systems. The problem with this approach is that the enterprise is not receiving the full benefit and value of ZTNA.

To successfully realize the full benefits of ZTNA, the business should identify the "user-to-application-to-data" use cases where ZTNA will have the greatest impact (for example, controlling access to sensitive applications and data or granting access to particular user groups like contractors). It should also apply specific policies to the appropriate areas within the business where secure access is required.

The access use cases are defined within a business access policy, and the access policy should be a combination of user and/or device identity, associated with supporting contextual data. This is then mapped to a series of controls or permissions based on the security risk appetite of the business. The identity and context become the critical elements that will drive the decision process around which use cases gain access to applications and data, and what level of access or permissions they are granted.

ZTNA is heavily dependent on identity access management, which is supported by several admin-time and runtime pillars, including identity governance and administration (IGA) and access management (AM), respectively, among others. IGA, together with other admin-time identity security posture tools like cloud infrastructure entitlement management, is fundamental in reducing the attack surface and making sure that identities are carrying only the necessary amount of privileges — no more, no less. These identities can then be used at runtime, served by AM tools for enforcing authentication and authorization, at the moment a resource is used. The associated ZTNA technology relies on what AM passes on in time of execution (i.e., account permissions, user behavior, and other identity-session-calculated risks) in order to decide whether to allow, deny access, or step up authentication to a protected resource under scope of that ZTNA tool. For more information, see Quick Answer: How Do Access Management and Zero Trust Network Access Tools Work Together?

Document and Map Application Usage Before Starting 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, or use other existing data flow mapping tools. However, some early adopters have reported that they "got ahead of the curve" by starting a discovery process before implementing the ZTNA solution.

Gartner observes two main approaches:

1. **Comprehensive, but time-consuming:** Define the policy by mapping applications and users before implementing. This is the preferred approach if additional zero-trust-aligned technologies are intended to be deployed on top of the ZTNA deployment. Example: Microsegmentation or identity-based segmentation.

2. **Tactical and incremental:** Identify a purposely small and isolated group of applications, and a small team of users to start with. Use it as a benchmark for evaluating the total time needed, the robustness of the workflow management and the documentation process.

Use the work initially conducted through collaboration with the business leaders from different departments (marketing, finance, sales, etc.) to determine which applications your teams should require access to, including contractors (if any). Security leaders are then able to develop the theoretical access policy and associated work profiles. Work profiles define the possibilities for remote work access and, therefore, the associated security requirements (see Figure 2). The security team's goals should be:

- Gather enough information to understand the remote work strategy based on the user role and team.
- Inventory the key applications and computing models for each user category.
- Identify data privacy requirements.
- Map these remote work profiles with existing risk assessments based on the employee's role.

Figure 2. Key Components of an Employee's Remote Work Profile

Key Components of an Employee's Remote Work Profile

	Employee Role	Remote Work Strategy	Client Compute(s)	Application and Data
	• Access: – Applications – Structured Data – Unstructured Data (e.g., Email) • Technological Savviness • Fit to Remote Work • Risks Exposure	• Frequency: – Not Suitable – Impossible – Emergency Only – Occasional – Part Time – Most Time • Work Location – Fixed (e.g., Home, Co-working Space, Flex Office) – Mobile (e.g., Travel)	• Managed Laptop • Bring Your Own Device (BYOD) • On-Premises Workstation Accessed Remotely • Desktop as a Service (DaaS) • Virtual Desktop Infrastructure (VDI)	• On-Premises: – Public Facing – Internal – Air Gapped (e.g., SOC) • IaaS • SaaS
Stakeholder	Business Leaders	HR, Business, Finance	CIO	CIO
CISO's Role	Understand	Adapt	**Influence**	**Influence**

Source: Gartner
724856_C

Gartner

The access policy and work profiles should be based on the supporting zero trust strategies and should be in alignment with the business' access expectations.This provides the business with a set standard for each team, determining which applications to allow and what level of risk-appropriate access should be granted. This enables the security team to progress more rapidly with the ZTNA deployment.

Early adopters have reported that performing application mapping prior to a ZTNA deployment helped validate the policy. Application mapping tools identify who is using each application and how the application is being accessed; they can also map application-to-application dependencies.

ZTNA project managers report that even with application discovery tools at their disposal, it is a lot of work to identify which users need access to which applications. One suggestion is to reverse the approach and identify a single application, then map the users. It's best to start this effort early and then iterate with additional applications as needed.

Many of the ZTNA vendors provide this functionality as part of the solution if deployed in an “open” or “monitor” mode, and some adopters have used this to their advantage. Other methods, like using toolsets that are already deployed within the organization, can assist in the process. It is not a mandatory step to perform a tools-based mapping of the applications; however, it does help the process of a ZTNA deployment if a tool is available for use.

Through a process of elimination, security leaders can leverage these mapping tools to validate that the theoretical policies defined are meeting the access expectations of the business leaders. It is not unusual to identify other access use cases during this process that may not have been identified during the development of the access policy.

While many organizations do not have a process for revising access policies, it is critical to do so. Initially, keep the access policies relatively broad, then increase the granularity of the policies over time based on the risk appetite of the business. This will lower your operational cycles and troubleshooting during the initial stages of deployment. Avoid setting and forgetting the policy.

By establishing the policy first and then validating the application usage, a business can map and document the theoretical with the actual. This will potentially close out any unforeseen gaps or establish new policy for use cases that the business was unaware of. This cements the product into a strong tactical position to meet the organization’s primary goal of deploying zero trust technologies across the enterprise.

Clean Up Access to Applications

During the discovery and mapping stage, many existing application access policies are likely to require adjustment and tuning. This is a good opportunity to eliminate application access privileges and entitlements that are no longer relevant. By this stage of the process, security leaders should have a good understanding of:

- Which users or systems need access to the applications and data sources

- Which established business data sources are protected by the applications, and the classification of the data that needs to be accessed
- How and where the users should access the applications and data
- Who is entitled or using privileged access and for what purpose
- Which resources are sanctioned by the business, and validation that users are using them in the intended manner
- Which applications are not sanctioned and why these applications are being used
- Which applications or tools should be eliminated or restricted in usage

Some organizations have reported to Gartner that they aligned their remote access upgrade with the overall roadmap for application and services modernization. This prompted the business to postpone changes in access to certain applications, because the application was on a plan to be migrated toward a SaaS model.

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, which is an example of poor user life cycle management. Some early adopters also reported that they terminated access privileges of their parties (contractors) with whom they no longer had business relationships.

During this application cleanup process, both IGA guidelines and the access policy should be maintained and updated if necessary, so that the baseline business policies do not fall out of synchronization with the changes being implemented.

Prepare for Operational Overhead and Complexity

Security is a continuous life cycle; it is forever evolving, and it is not realistic to take a “set and forget” approach with ZTNA policies. Organizations that are experienced with ZTNA deployments have reported that they are continuously tuning the policy. As new applications or data sources (including seasonal applications) are deployed, the ZTNA team will need to add new access policies to accommodate the changes with the business. Existing access policies may also need to be modified as an application or data source (type) evolves, or when security leaders identify the need for more granular or restrictive policies.

This can also potentially influence process changes if service desks or the ZTNA implementation teams are not prepared and become inundated with access requests to open up access to other resources that may have previously been accessible. The ZTNA tools capabilities should be used to their full extent to facilitate and document any policy changes.

The ZTNA team should adopt the mindset that there will always be a need to improve and refine the access policies over time. It is important to stay in communication with the application and system owners to understand:

- Which resources within the business unit should users be accessing?
- Which internal and external users need access, and how should they be accessing the systems?
- What resources within the business unit require elevated privilege and why?
- What applications or data should be restricted or require additional approvals with the business unit?
- Are there any new projects or major changes approaching that may require policy modifications?

Answers to these questions will potentially prompt changes to the established access policy and drive the process toward newly modified, tested and validated access policies within the ZTNA life cycle.

Overly restrictive or numerous granular policies will initially impact service desk teams or the ZTNA implementation team, and so a clear exceptions process must be developed to address access request modifications. The business must determine how much autonomy it should grant the support teams to make any access modifications, and what level of access change will be permitted. The exceptions process must maintain a validation step so that as access policies are modified, they continue to align with the business expectations and don’t introduce unnecessary risk.

Deployment of ZTNA policies may introduce some operational changes. For example, the help desk and IT support should be aware that typical endpoint management, which may have relied on Layer 3 VPN access to the endpoint (for tasks like patching or remote support), will require an alternate management path. Many of the ZTNA providers steer traffic at the application layer (Layer 7), so automated updating tasks that may have worked successfully on the traditional VPN may no longer work under the newer ZTNA model. Work with endpoint management teams to modernize endpoint management before implementing the ZTNA solution. (For more information, see Modernize Windows and Third-Party Application Patching.)

Validate Access Controls and Resource Isolation

A key tenet of zero trust is to never implicitly trust, but to always validate. This ideal or principle of validation should also be applied to a business' internal set of security controls and implemented across the enterprise.

Information security is a continuous life cycle of strategy, architecture, implementation, operation and validation. All too often, the validation phase is overlooked; this is where businesses should assess their own security controls and establish a known "as-is" state of compliance at yearly intervals. Validation of security controls should be part of the ZTNA planning process and incorporated into the overall security program. Security leaders should formulate a plan and process to test and validate the effectiveness of the ZTNA policies.

Assurance assessments can come in varying forms, such as internal self-assessments, security reporting tools within the ZTNA solution and/or external consulting firms that provide controls testing services. The goal of the testing plan is to understand two areas: isolation of the protected resources and ensure that the access rights of the users in the system meet the organization's policy for access. This validation establishes a current compliance state of the ZTNA environment and reveals any potential gaps which may need remediating.

It is recommended that once ZTNA technology has been deployed and relative stability has been achieved, the business should conduct an assurance assessment on the ZTNA environment. Security assessments such as these should be conducted on a regular basis and primarily driven by the risk appetite of the organization. Generally, most organizations will perform this step by engaging with an external or third-party security consulting firm, whose consultants are well-versed in modern attack techniques.

Evidence

This research is based on Gartner interviews with multiple early and established adopters of ZTNA technology.

[1] For more information on zero trust maturity models, see the Cybersecurity & Infrastructure Security Agency's CISA Zero Trust Maturity Model. For more information on zero trust architecture, see the Department of Defense's Zero Trust Reference Architecture.

Document Revision History

Best Practices for Implementing Zero Trust Network Access - 10 June 2021

Recommended by the Authors

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

Market Guide for Zero Trust Network Access

Magic Quadrant for Security Service Edge

2022 Strategic Roadmap for SASE Convergence

What Are Practical Projects for Implementing Zero Trust?

Emerging Technologies: Adoption Growth Insights for Zero Trust Network Access

Guidance for Successful Identity Governance and Administration Deployments

IAM Leaders' Guide to Identity Governance and Administration
