The Definitive Guide to ZTNA Adoption

The Challenge with Secure Access Today

You may be reading this guide from the comfort of your home, an office cubicle, or really anywhere in-between. The reality is that the business we exist in today operates much different than it did just a couple years back. The business landscape has changed and with it comes a host of challenges that IT teams must navigate, a core concern being the method of secure connectivity to business applications.

This may sound simple enough, yet with the reliance on the wrong technology, achieving “secure access” becomes an insurmountable feat as problems amplify in the face of cloud and mobility. To no surprise, we see threat actors welcoming this opportunity to take advantage of the technologies that once ensured enterprise security, but now introduce risk.

For this reason, IT and business leaders alike are searching for the modern access solution that will provide organizations with connectivity that is seamless for users and simple for IT. Gartner says that this modern access solution is Zero Trust Network Access (ZTNA) and we agree.

77% of companies believe they will enable a hybrid work environment going forward.

Security threats have risen 500% year over year due to this new work reality.

IT teams have experienced a significant increase in responsibility yet IT budgets are only increasing 4% each year.
What is ZTNA and why now?

VPNs were designed to solve a simpler problem from a simpler time: enable secure access for a small portion of the workforce to applications controlled by IT in a local data center. Sounds simple, right? That was twenty years ago. Users installed complex clients on their desktops and were granted network-level access to a few applications. There was a level of implied trust: users would adhere to using applications they were granted access to and wouldn’t stray. Even better, threat actors weren’t lurking about waiting to infiltrate networks and exfiltrate data.

Fast forward to today and VPNs are showing their age – fragile connections, limited scalability and performance, and complex configuration and maintenance are just a few of the issues surrounding the remote access VPN. Moreover, there are other factors that organizations must consider when implementing a modern access security solution such as identity and device verification, application-level access and enforcement, and flexibility for geographically dispersed employees and third-parties (which make up ~1/3 of the supported workforce).

Today, Zero Trust Network Access (ZTNA) is one of the main components of a Security Service Edge (SSE) platform (ZTNA, SWG, & CASB) which offers IT teams a modern alternative to traditional network security solutions. As the choice access technology, ZTNA enables organizations of all sizes to securely connect users (regardless of their location or device) to applications in the cloud or data center. ZTNA adheres to the zero trust principle “trust no one” and built upon it with holistic adaptive trust principles. Not only must users authenticate themselves and their devices, but once trust is earned, adaptive trust continues to monitor and alter access permissions based on dynamic contextual elements like identity, device, policy, application, and data. The result is significantly reduced risk of malware or threat actors gaining unauthorized access. Moreover, ZTNA also enforces least-privileged access that restricts access to individual, authorized applications, incorporating policy-based segmentation, and minimizing the potential of east-west migration should malware get in.

By 2023 60% of enterprises will phase out their remote access virtual private networks (VPN) in favor of ZTNA.

Gartner market guide for ZTNA
In contrast to traditional security solutions like VPNs, ZTNA offers significant benefits, including:

- Rapid onboarding of employees, contractors, and third-parties without the headaches and complexity of onboarding users via VPNs
- Streamlined application access for geographically dispersed workforces for better productivity and collaboration
- Clientless-first access to numerous to web, RDP, SSH, Git, and DB applications
- Simple client available for any port/any protocol access including VOIP, ICMP, and AS400 (without complex training or helpdesk support needed)
- Zero Trust security features including continuous user and device authentication and authorization to prevent unauthorized users or malware penetration

<table>
<thead>
<tr>
<th>ZTNA +</th>
<th>VPN -</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supports hybrid workers</td>
<td>Supports remote workers</td>
</tr>
<tr>
<td>Seamless experience with always-on design and IDP integration</td>
<td>Frustrating experience with tedious login requests</td>
</tr>
<tr>
<td>Direct access to business resources with automatic brokering</td>
<td>Slow experience due to datacenter backhaul</td>
</tr>
<tr>
<td>Users access authorized apps, not the corporate network</td>
<td>Place risky employees and third-parties on corporate network</td>
</tr>
<tr>
<td>Apps and network are made invisible to unauthorized users</td>
<td>VPN infrastructure is exposed to threats i.e. Ransomware</td>
</tr>
<tr>
<td>Management is simple with granular zero trust policy</td>
<td>Network segmentation is complex to manage</td>
</tr>
</tbody>
</table>
ZTNA Architecture

ZTNA solutions, like Atmos ZTNA, start with a cloud-enabled control point. This serves as a distributed authentication, authorization, and policy enforcement point that governs transactions between users and applications. ZTNA brokers all connections by disallowing any inbound connections to applications, increasing application security and reducing the attack surface.

Gartner. Conceptual Model of Service-Initiated ZTNA

1. **Register Application**
   A user attempts to access a business app
   Secure access to major apps – even VOIP, ICMP, and AS400 – and support client or clientless access.

2. **Connect to Provider**
   ZTNA mediates the request
   Avoid passthrough connections that can lead to risk – a ZTNA cloud node becomes the first stop for all business resource traffic.

3. **Authentication**
   ZTNA validates identity & policy
   Identity integrates into the ZTNA platform aiding in zero trust access and automatically adapts access rights based on changes in context (device posture, location etc.).

4. **Verify Identity**
   ZTNA securely connects to resource
   The ZTNA service automatically brokers connections to individual, specific applications while keeping users off the network. Private applications are made invisible to the Internet and connections to SaaS apps are quick and seamless.

5. **Session Established**
   ZTNA inspects traffic & monitors user experience
   The ZTNA platform provides visibility into user activity, granting awareness of any malicious activity, and gives insight into the access experience for the end-user.
Once a user authenticates to the control point, individual time-based sessions are established to specific applications. All sessions are governed by policies established by IT administrators and follow users regardless of their location. Further, every session is continually authorized and authenticated, and each device is continuously evaluated; should the device change location actions can be taken to limit application access, curtail file downloads, or possibly even quarantine the device for remediation.

The user experience, on the other hand, is vastly simplified over traditional VPNs or similar security models. Atmos ZTNA, as a core component of the overarching Atmos SSE platform, provides both clientless and client-based capabilities. Many transactions can be handled without using a client, including web, RDP, SSH, and other sessions. For any port/any protocol access, a lightweight client is widely available for the device of choice providing quick and secure access to apps and resources needed to remain productive.

The result is a network that is much more secure than a traditional security stack of firewalls, intrusion detection, and endpoint management tools provide. And, because of Axis’ Application Isolation Technology, applications themselves are more secure while taking advantage of the inherent security of microsegmentation, where east-west traversal is curtailed, significantly reducing the possibility of malware proliferation.

**Achieving Zero Trust with ZTNA**

It is important to underscore that most organizations have already implemented some level of zero trust, whether in the form of two-factor or multi-factor authentication, single sign-on, or policy enforcement. Equally important is that implementing zero trust is a journey – no two network topologies are the same. Often security and IT architecture teams are different, requiring collaboration and teamwork to realize the significant security and productivity benefits of ZTNA as a stepping stone towards a holistic [Security Service Edge (SSE)] strategy.

Below is a suggested “adoption” process where steps can be taken sequentially as organizations begin the process of increasing their security profile, streamlining access for their mobile workforce, and reducing the chance of malware penetration and data exfiltration.
The ZTNA Adoption Checklist

Moving from traditional security architectures to ZTNA is Gartner’s recommended first step in modernizing secure enterprise access. Doing so will also free users – and IT departments – from complex connectivity challenges imposed by aging security stacks. Users will be happier and more productive, while IT departments can focus on other critical tasks. The following sections outline best practices for IT teams looking to migrate from traditional access solutions to a modern ZTNA.

1 Understand your environment

Organizations today often have hundreds or thousands of applications in use (whether known or unknown), including CRM and ERP systems, as well as remote desktops like RDP and VDI. Having an inventory of what applications are in use today can be helpful when determining who can access which applications; however, modern-day ZTNA solutions will have built in app discovery capabilities that enable IT to uncover any shadow IT applications.

Further, determining how users access your organization’s applications can lead to insights. For example, are some users leveraging BYOD more than others? On the other hand, do users still access applications hosted on-premises?

It’s important to gain initial visibility into your current environment so that you can prevent any roadblocks that have the potential to arise mid-deployment.

2 Start with high risk areas – aka remote access

Today’s workforce is composed of employees, third-parties, customers, and merged or acquired users – with many working remote. All need streamlined access to business resources, ideally without the need for much configuration or a client on the end-point. Consider starting deployment with a small subset of these remote users (such as your executive team, developers, or third-party users) and learn how to configure and enforce least-privilege access policies with ZTNA. Follow up this deployment with the rest of your remote workforce.
3 Expand access to in-office workers (and beyond)

With 77% of organizations adopting some form of hybrid work, it’s important that ZTNA access eventually extends to support the in-office user as well. With workers coming and leaving the office constantly while accessing sensitive data, it’s important that zero trust and least-privileged access is enforced universally as to not create security gaps that put your network at risk. Additionally, this provides your hybrid workforce with a completely seamless and consistent access experience whether at home or in the office.

Mergers and acquisitions also benefit from ZTNA. Solutions like Atmos ZTNA instantly and simply enable low-risk, zero trust access to applications and resources across organizations in advance of merging network topographies. Using cloud-based technologies, Axis’ highly-scalable services broker agentless access to resources anywhere, while isolating them from potentially compromised users, devices, and networks. Deployment is rapid without extensive network changes, while a central cloud console manages it all through cross-application policies, ensuring that only authorized users get access to applications they’re entitled to.

4 The next step in SSE deployment

At this point 1/3 of your overall SSE deployment is completed! You have successfully minimized access risk in areas of highest concern and can look to further SSE deployment by evaluating existing contracts and putting together a phase-out plan for perimeter-based security technologies. IT can consolidate contracts by selecting a single SSE vendor that can provide ZTNA, SWG and CASB. These decisions will not only impact infrastructure at the corporate office, but can also help accelerate branch office transformation projects – helping to minimize unnecessary MPLS costs, and instead investment in cloud-based security edge services at the branch.

If you want to learn more about how to deploy a SSE platform, check out the [Architect’s Guide to Adopting Security Service Edge (SSE)](#) or get to know [Atmos, our award-winning SSE platform](#).
Modern Secure Remote Access with ZTNA

Businesses today require rapid development, high levels of collaboration and teamwork, and data security and integrity. Central to each of these needs is a modern, flexible, scalable, and secure network that facilitates communication rather than hindering it. While traditional architectures like VPNs may still have limited relevance for some, the complexity of managing and maintaining aging infrastructure only serves to consume resources better spent elsewhere.

ZTNA is the future of modern access and overcomes the challenges of workforce mobility, network access security, and scalability without the headaches of complex configuration and deployment. The modern workplace requires that access is seamless while resources are secure, and Atmos ZTNA provides the path to achieving both.

With Atmos ZTNA, IT teams can:

→ Deploy in minutes or hours rather than weeks or months
→ Deliver productivity and collaboration for globally distributed workforces
→ Improve visibility and experience through detailed insights into user and app activity
→ Reduce risk of data loss and malware penetration while improving compliance
→ Simplify IT management through intuitive zero trust policies and granular access controls

Begin modernizing access for your modern workplace with Axis.
Sign up and try Atmos Security Service Edge (SSE) Platform for free.

Get Started

About Axis

At Axis we believe in a world in which workplace connectivity is always secure and seamless. With over 350 PoP locations, our cloud-delivered security service edge (SSE) platform makes securing access to business resources impossibly simple for IT and completely seamless for users. With Axis, our customers are able to make hybrid work simple, turn digital experience into a competitive advantage, and can better protect their data from cyber threats – even as it moves to cloud.

www.axissecurity.com