

# Using Axis as a *VPN Alternative*

The modern workplace calls for a new approach to remote access

## Brief Summary

- Accelerating to a modern workplace means saying goodbye to VPN
- The difference between VPN and Axis ZTNA
- Unique capabilities that set Axis ZTNA apart



# Accelerating to a modern workplace means saying goodbye to VPN

Spurred by the need to ensure business continuity during the pandemic, and to outpace competition, every organization is in a race to adopt the right digital solutions that will keep their users happy, motivated, and productive. They've adopted new collaboration apps like Zoom and Microsoft Teams, doubled down on scalable public cloud services, and even allow for more flexible work environments. With this modernization underway, many IT leaders are also considering better ways of providing remote access to private applications for their employees and third-parties - and moving away from VPN.

Prior to the pandemic, a mere 30% of employees worked from home. Today, 77% of businesses plan to embrace hybrid work to retain top employees who now prefer work from home, and to access new, less expensive talent pools. VPNs tend to hinder productivity and frustrate employees.

Partners, suppliers, vendors and customers also play a key role in driving revenue for the business. One out of every three users who require access to resources

are third-parties, and they rarely allow a VPN client to be deployed on their devices.

As you can imagine, this modern workplace also comes at a cost. IT spend is estimated to reach \$2 trillion in 2022 much of which will be to modernize IT infrastructure and support this new work environment. Yet, this only represents a 4% increase in avg IT budgets - so continuing to spend heavily on legacy remote access technologies is not an option.

Even in the midst of enabling work from anywhere, securing third-party access and modernizing infrastructure, the brand's reputation must remain protected. With every user, device and application connecting over the Internet, the potential attack surface increased exponentially - and placing users onto the corporate network via a VPN has become the biggest risk of all.

To support this new environment 60% of businesses will replace their VPN with ZTNA by 2023.

## ZTNA:

Gartner

Created in April of 2019 by Gartner, the term **Zero Trust Network Access (ZTNA)** represents a set of new technologies designed for secure access to private applications. Also referred to as Software-defined perimeter (SDP), ZTNA technologies use granular access policies to connect authorized users to specific applications, without the need for access to the corporate network, establish least-privileged app-level segmentation as a replacement for network segmentation, and without exposing the applications location to the public internet unlike a VPN concentrator.

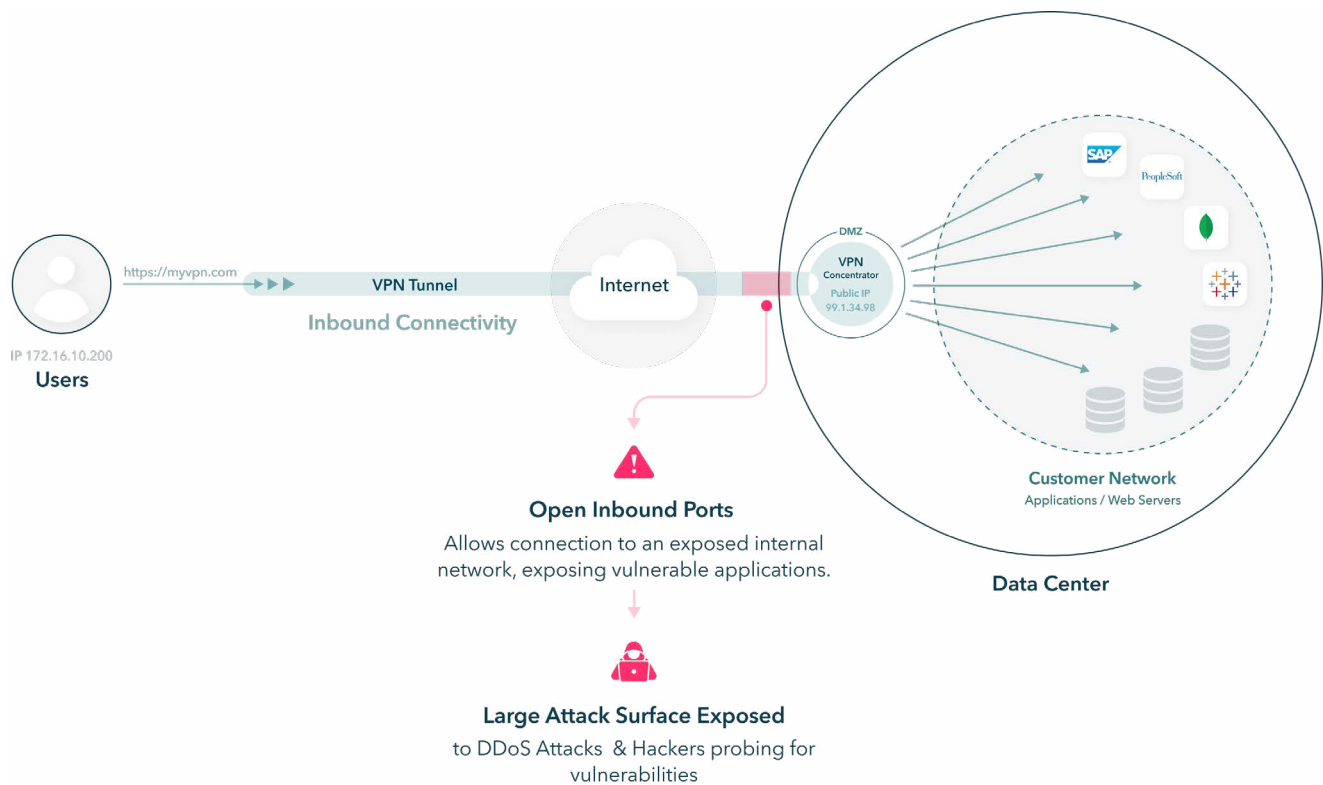


# The difference between VPN and Axis ZTNA

## Remote access VPN

Over the past 20 years VPN has allowed remote employees and third-parties to access the network - and the private resources running within it. VPN concentrators listen for inbound calls from VPN clients, and serve as a beacon for the clients - providing an entrypoint into the corporate network. In an effort to minimize the risk of this flawed architecture, firewalls, load balancers,

DDoS prevention, and VPN concentrators all became requirements of connecting remote users to private applications. This leads to more complexity, more costs, and more risk. Over the past few years popular VPNs services like Pulse Secure, Cisco AnyConnect, Fortinet and Palo Alto Global Protect have all been exploited due to this architecture.



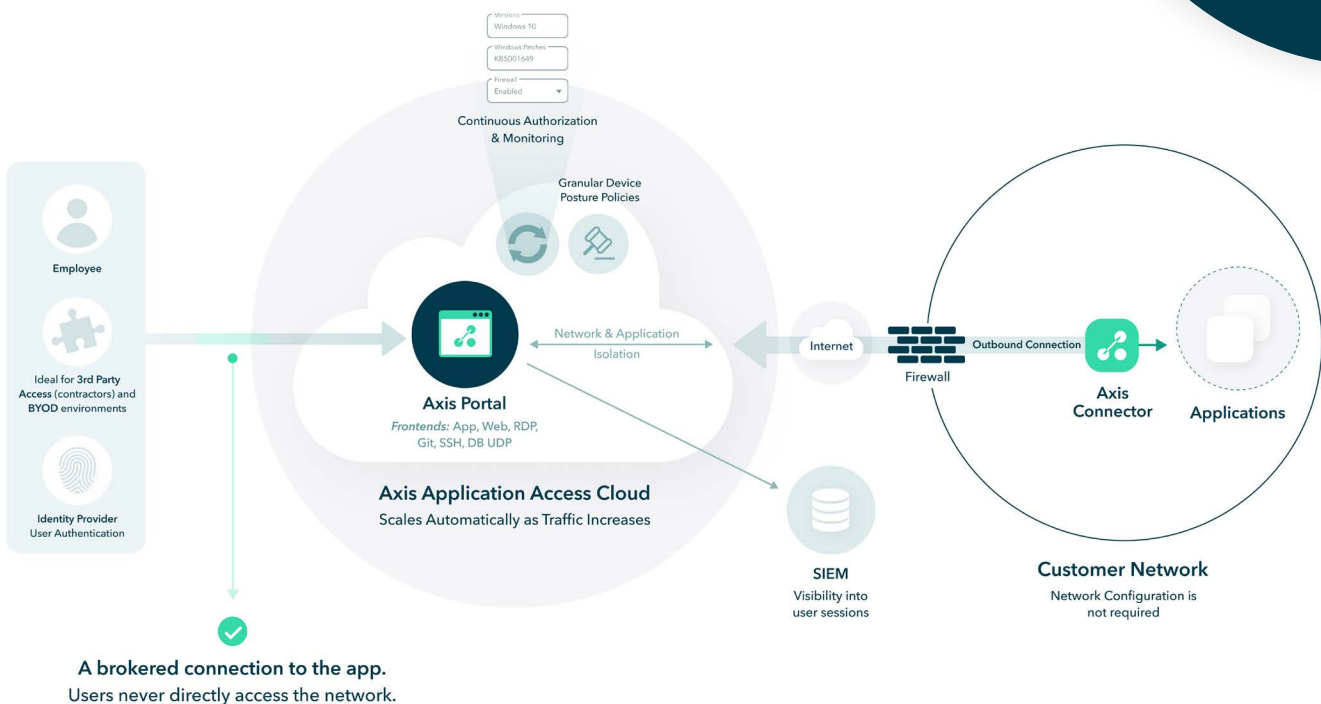
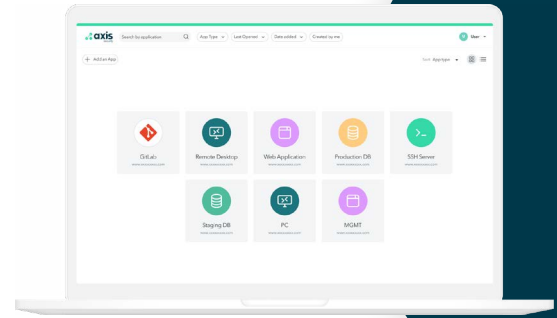
**Traditional VPN** VPNs provide wide-open network access to all applications, servers and resources on a given segment.



## Axis ZTNA

With 350 PoPs across the globe, Axis is the most reliable, available and scalable zero trust platform designed for connectivity to business resources.

The Axis ZTNA service was designed to provide users with fast, secure, reliable access to private resources. Here's what's happening in real time when connecting through Axis (clientless):




1. The user requests access to an internal application  
*Sample URL: hr-app-tenant.axisapps.io*
2. If the user is not actively logged into an Axis-managed application, the user is redirected to the associated application identity provider
3. Axis checks the user's access request against the customer's defined policies.
4. The user is continuously authorized according to their identity, group, and other contextual criteria.  
**NOTE:** Axis can actively inspect traffic and can close the session due to a security event.
5. Axis checks for an existing connection to the application for potential reuse.
6. If no connection exists, a new connection is established from the application to the Axis Connector via specific port to the Axis Cloud.
7. The established connection is returned to the dedicated front end.
8. The front end web establishes a connection to the application.
9. The requested website is returned to the user.



Axis ensures that application access can be granted without having to require access to the corporate network. This decoupling helps reduce network security risks - like insider threats or ransomware spreading, by minimizing lateral movement through application-level segmentation.

Unlike a VPN concentrator, Axis uses a service-initiated architecture to leverage what we call outbound-only connections. This connection type ensures that the network infrastructure and business applications are masked from the Internet and cannot be located or DDoSed because they do not listen for any inbound pings. They sit behind the Axis connector, which exclusively speaks with the Axis service edge. Think of Axis as the intermediary between the entity (user or app) and the application.

Axis treats the Internet as the new corporate network and ensures that dynamic Internet-based encrypted micro-tunnels replace traditional network connections like always-on VPN, MPLS and dedicated site-to-site connections for public cloud. This reduces costs, and frees up time for network and security teams to focus on more strategic projects vs. managing expensive appliances, updating versions, deploying hardware and planning renewals.

	VPN	 axis ZTNA
User Experience	<p><b>Poor user experience</b></p> <p>VPNs force users to deploy a client on their device, and reconnect to the corporate network every time a user moves locations. This feels invasive and is frustrating for every user. Since VPN gateways have limited points or presence, suboptimal flows add latency, cutting into user productivity.</p>	<p><b>Seamless user experience</b></p> <p>Axis offers both client and clientless access methods. A single zero trust policy follows the user and ensures they only have access to the specific resources they need. The always on user experience allows customers to simply work and not worry about reconnecting to a network. Cloud-delivered ZTNA services offer global PopS that securely extend connectivity out to every users locations - via the Internet.</p>



## Security

The business must protect data from cyber adversaries - at all costs

## Increased risk

Cyber criminals are actively targeting VPN and VDI technologies with internet-based attacks. These network-centric access methods place users onto the corporate network, and expose infrastructure to the open Internet. With a simple port scan an adversary can target infrastructure with an outdated posture, steal credentials, and access the corporate network as if they were a legitimate user.

## Zero attack surface

Axis is designed to never inherently trust anything. Only after proper inspection, and validation, does the ZTNA service connect users to specific resources. These surgical 1:1 connections are outbound-only from the resource, to the authorized user - and without placing users on the corporate network. This least-privilege access design ensures that users and threats cannot propagate laterally across the environment. Axis also protects resources by placing them behind the ZTNA service - making them invisible to the Internet. Access rights then auto-adapt based on changes in context - relationship with company, device posture, location etc.

## Ease of use

As the business grows, and continues to adopt the cloud, simplicity and scale have become a priority.

## More complexity and costs

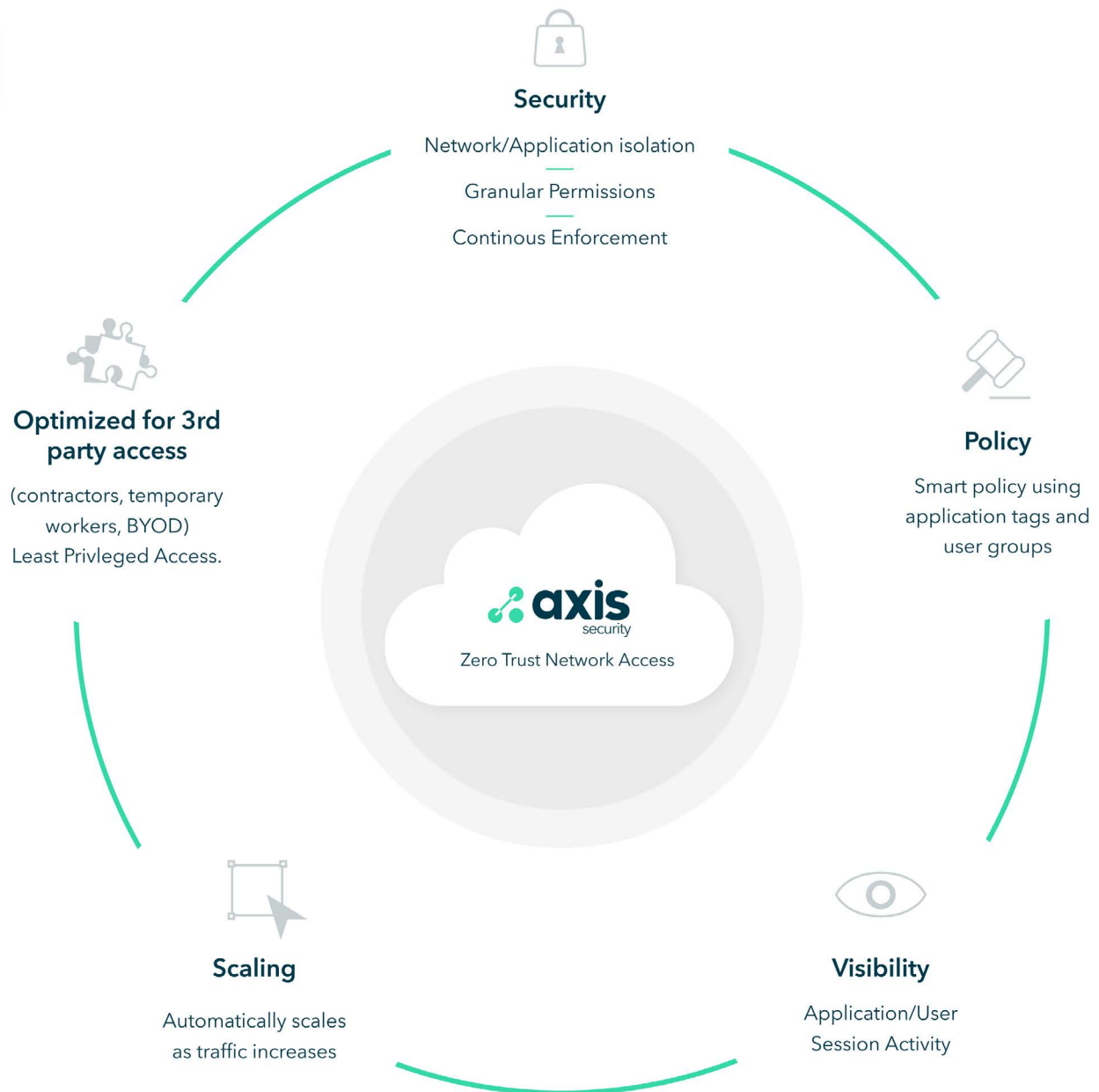
Scaling VPN services requires adding capacity, which requires purchasing, deploying, and managing more appliances. This is not just the VPN concentrator, but the entire inbound gateway that is required because of it. The loadbalancer, external firewall front-ending the VPN, DDoS service, the VPN itself, the internal firewalls used for network segmentation and the site-to-site MPLS infrastructure connecting the datacenter to various public cloud providers must all be considered. This constant game of appliances is a challenge to manage and drives costs through the roof when you consider both CapEx and OpEx spend on maintaining the entire gateway. It's also completely unnecessary now with ZT

## Simple to manage

The cloud-delivered services require no appliances. Like their destination cloud cousins, these brokering services are completely maintained by the vendor themselves. The services are designed for reliability, availability and to automatically scale as the traffic demands increase. They ensure the fastest experience possible - without disruption to the business. API integrations with key ecosystem services like IDP, endpoint security and SIEM, help expedite the deployment process. These services charge on a per user, per year basis, so capacity and appliances costs are no longer a factor. IT can spend less time and money on connectivity services, and instead focus on the strategic projects that are key to their modern workplace initiatives.



# Unique capabilities that set Axis ZTNA apart



→ **Per application-level segmentation, without network segmentation**

Reduces the potential attack surface by only allowing access to specific resources. This limits lateral movement across the network, removes the need for complex network segmentation efforts, and reduces the potential attack surface of the business.

---

→ **Seamless access to apps from any device with or without a client**

Enables authorized remote employees and third-parties to securely access business resources from the device of their choice, and in the most seamless way possible. The clientless method also supports browser-based RDP sessions - reducing the need for VDI.

---

→ **The broadest support of private applications on the market**

Support all TCP and UDP traffic, including VOIP, peer-to-peer, and server-to-client workflows which are difficult for most ZTNA vendors. Now IT teams can replace VPN for good.

---

→ **Ability to inspect traffic flowing to private resources**

For the first time, gain deep visibility into what employees and third-parties are accessing. Record brush.

---

→ **API-powered contextual access controls**

Automatically adapt access rights based on changes in key criteria including: User location, identity, device posture. This continuous adaptive risk assessment helps to better protect business data.

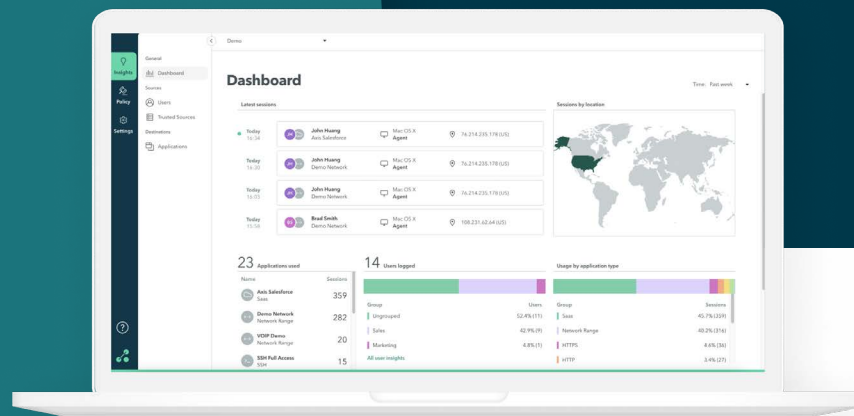
---

→ **100% cloud-delivered architecture across 350 global service edges**

IT can stop spending time on managing VPN appliances. With Axis every connection is brokered in the Axis PoP best suited to provide the connection - even in the case of a disaster. IT can rest assured that they'll be able to minimize disruption and maximize uptime.







Learn more about ZTNA  
and how you can use it as an alternative to your VPN  
by requesting a *free trial!*

Get Started

## About Axis Security

Through its world-class research & development, founding team which hails from Israel's acclaimed Unit 8200, and over 350 cloud service edges, Axis aims to accelerate the world's transition to a modern workplace where hybrid work is made simple, digital experience becomes a competitive advantage, and business data remains protected from cyber threats - even as it moves to cloud.

Axis Security is a privately-held company backed by Spark Capital, Canaan Partners, Ten Eleven Ventures and Cyberstarts. It is headquartered in San Mateo, California with research and development in Tel Aviv, Israel.