White Paper

axis security

Overcoming the Legacy VPN Dilemma

Zero Trust Access with Application Access Cloud

The Threat Landscape Has Changed

Business has grown beyond the confines of standard organizations. Now, employees and partners interact with company apps and data from any location (e.g. home offices, customer sites, or partner facilities). But even though many aspects of offsite connectivity have evolved, others desperately need to. While staff and integrated 3rd party remote work models are commonplace, the access models enabling them are outdated and broken.

As far back as the 1980s, companies have relied on firewalls to enforce perimeter security. Inside that perimeter, many networks still remain relatively "flat" and open; most resources can communicate with one another rather freely. Unfortunately, that means a bad actor could breach the perimeter or compromise a trusted endpoint under this security model. By attaining a foothold, they can often cause widespread damage to a company's environment or brand.

When 3rd parties enter the picture, the level of risk heightens even further. They are regularly targeted by bad actors at a growing rate, due to the potential to hack into that 3rd party's systems to compromise the data or customer environments of the parent org.

Many enterprises are engaged in digital transformation, migrating resources to the cloud and enabling a single-ID access to systems apps and data, an ID that allows access across both cloud and internal environments. Governing access across these environments is identity.

The maturation of Zero Trust has evolved the concept of Identity as the new "perimeter," necessitating a new approach to accessing company assets. A Zero-Trust approach, that aligns to how modern businesses work within the new risk landscape, is quickly becoming an essential requirement for both business and IT. Adjusting to this new reality is no longer optional. It demands security models that better mirror the way businesses operate, compete and grow through, for example, their partnerships, acquisitions and digital transformation. The new perimeter is essential, but not without new access approaches such as zero trust.

Move Faster than the Competition

As we've seen recently, the business environment can change in mere hours. Businesses that can adjust, survive (or even thrive) under these changes stand to overcome competitors that can't. Today an org's ability to quickly extend proprietary security routines to protect 3rd parties, acquired companies, and even current employees in new markets has become even more crucial to winning.

But technology, usually an enabler, actually hinders businesses in these efforts. "Enablement" typically describes the controlled sharing of data and applications private to the enterprise. Ideally this sharing should be fast to deploy, easy for the user and secure for the enterprise. Unfortunately, legacy technology often aggravates deployment, reduces ease of use, and exposes security vulnerabilities.

Legacy Technology: Difficult to Deploy and Use

Technology needs to help IT and users, not hinder them. To move quickly, businesses need to enable users quickly. VPNs, for example, are problematic for both IT and the user. The typically clumsy VPN client software makes deployment, training, and ongoing support difficult. In many instances, a VPN requires that the user utilize a pre-configured company-owned personal computing device to gain access to needed resources. Hardware issues, limited scalability and licensing dependencies only serve to slow deployments to new users even further.

Network Access: Permissive, Uncontrolled

Letting untrusted users (AKA everybody) into your network is the ultimate lose-lose scenario. You lose control, because networks are open by design. You lose visibility, because from the moment an endpoint enters the network, they can pass arbitrary bits in every way. You've given endpoints access on the network layer, leaving your infrastructure exposed.

Legacy technologies aggravate 3rd party and employee security risks for a couple of reasons. First, because VPNs operate under an excessively permissive "You're home free and unobserved if you can authenticate once" posture, IT is unnecessarily blind to user activity post-authentication. No one can be truly trusted when they are transported across the perimeter, onto the actual network, and to the door of applications that are, more often than not, both full of valuable data and easy to exploit vulnerabilities. Today, user activities need to be continuously monitored and access continuously validated to assure the security of the enterprise.

Existing remote access solutions, namely DMZs and VPNs, were designed for businesses from another more permissive IT era. Since then, they have been rendered virtually ineffective by the following macro-trends dissolving the perimeter:

- Cloud proliferation
- BYOD
- IoT
- SaaS adoption
- Remote work

Enterprise Applications: Too Vulnerable to Expose

As implied above, when applications are broadly exposed to increasingly large numbers of users, it poses increasing risk. The average application has dozens of vulnerabilities, spread across a broad system, network and software attack surface. OWASP's Top 10 most common application vulnerabilities are present in many applications and are easily exploitable using common tools and well documented techniques. Network-level access technologies aggravate the risks posed by these vulnerabilities by finding these holes in the application's attack surface and exposing them directly to potentially dangerous users.

Even worse, these vulnerabilities increase in number and severity over time, especially in unmaintained (but still business-critical) applications that users need most.

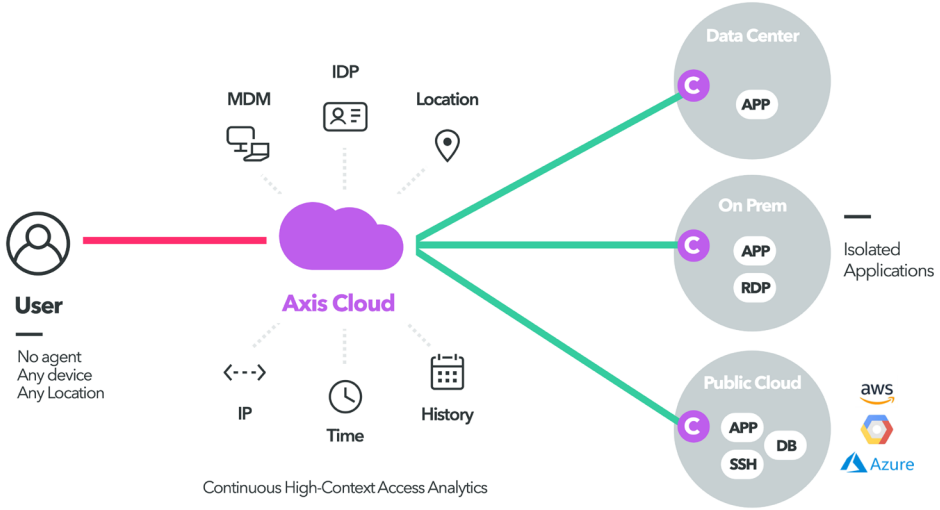
Even if ease of use and network security issues can be rationalized by the business, most enterprise security organizations won't accept the multiplied risk posed by overexposing application vulnerabilities to relatively untrusted users. For this reason alone, many organizations choose not to move forward with widening access. Their business' ability to thrive on change is, officially, limited by IT.

The Application-Level Access Solution

It's why we've developed the App Access Cloud, a new approach to application access. It makes private apps access simple to implement, highly secure and tightly managed. App Access Cloud was conceived to enable employee and third party access anywhere, without the compromise and complexity of legacy (or even virtualized) network-level solutions.

Instead of tunneling users through the local network, they are brought directly to the app via a single centralized location – the Application Access Cloud. It mediates access between users and private apps without ever touching your network or the apps themselves. No VPN tunnels or agents are required. No lengthy deployment or complex configurations. No network security risks. Instead, users seamlessly connect to the apps they need to work in the simplest and most secure way possible for them, the apps and the enterprise. And at its foundation, App Access Cloud assumes users, devices and the underlying network are compromised and hostile and establishes a secure virtual infrastructure over it that is governed by strict zero trust principals.

Simple Deployment and Access.



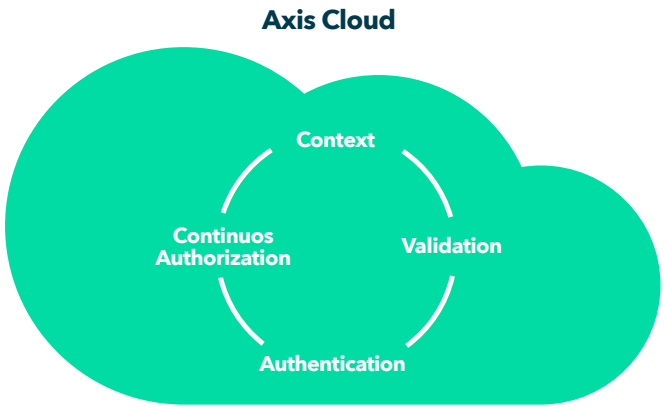
Simple deployment

- 10 minutes
- Software only
- IDP integration, DNS configuration, certificate issuance are all optional

To deploy Axis Security, simply deploy one or more connectors on the enterprise network. The connector is a lightweight, software-based, secure component that takes about 3 minutes to install. It's the only thing installed in the enterprise network. The user endpoints are never introduced into the network. This is the only deployment on your end, and no changes to the application, network, or connecting devices are required. The whole thing takes minutes.

The connectors connect back to the Application Access Cloud, and mutually authenticate using a single-use certificate. Once the connection is made, applications can be published on the Application Access Cloud and made available to end-users.

Unique Technology Approach.



The Application Access Cloud serves as a transparent front-end to the applications published. In most cases, users are not even aware it is brokering their requests. Behind the scenes, each user request is checked against policy – identity, device posture, time of day, geoIP, history of usage – before connecting to the application. The context added for policy purposes also enriches the activity logs that can be pivoted by user, device, or application.

When a user is authorized to access a resource, they gain a temporary one-to-one connection to the authorized resource, and it alone. The session is not only an authorized session, Axis Security takes a continuous authorization approach: each user request in the session is individually authorized. Some requests may even be blocked in an allowed session. i.e: an organization can grant access to an RDP server for unmanaged devices, but block file-transfer requests over that same session. Policies may also specify that users outside Europe who use unmanaged devices will have their sessions visually recorded.

Application Access Cloud reduces the attack surface significantly – and not just by removing your resources and applications from the public Internet. Traditional solutions provide network access by essentially acting like an ethernet cable, blindly passing arbitrary bits – bad and good – back and forth. The Application Access Cloud, however, applies Application Isolation Technology to deliver managed and controlled access without allowing users onto the application's network. Every request gains user and situational context. The request also gets validated against the protocol through a process of deconstruction, sanitization, and reconstruction. Only then does the application-level request get authorized against the policy, and then is relayed (the application layer only) to the application. Users gain application access without actually touching the application itself.

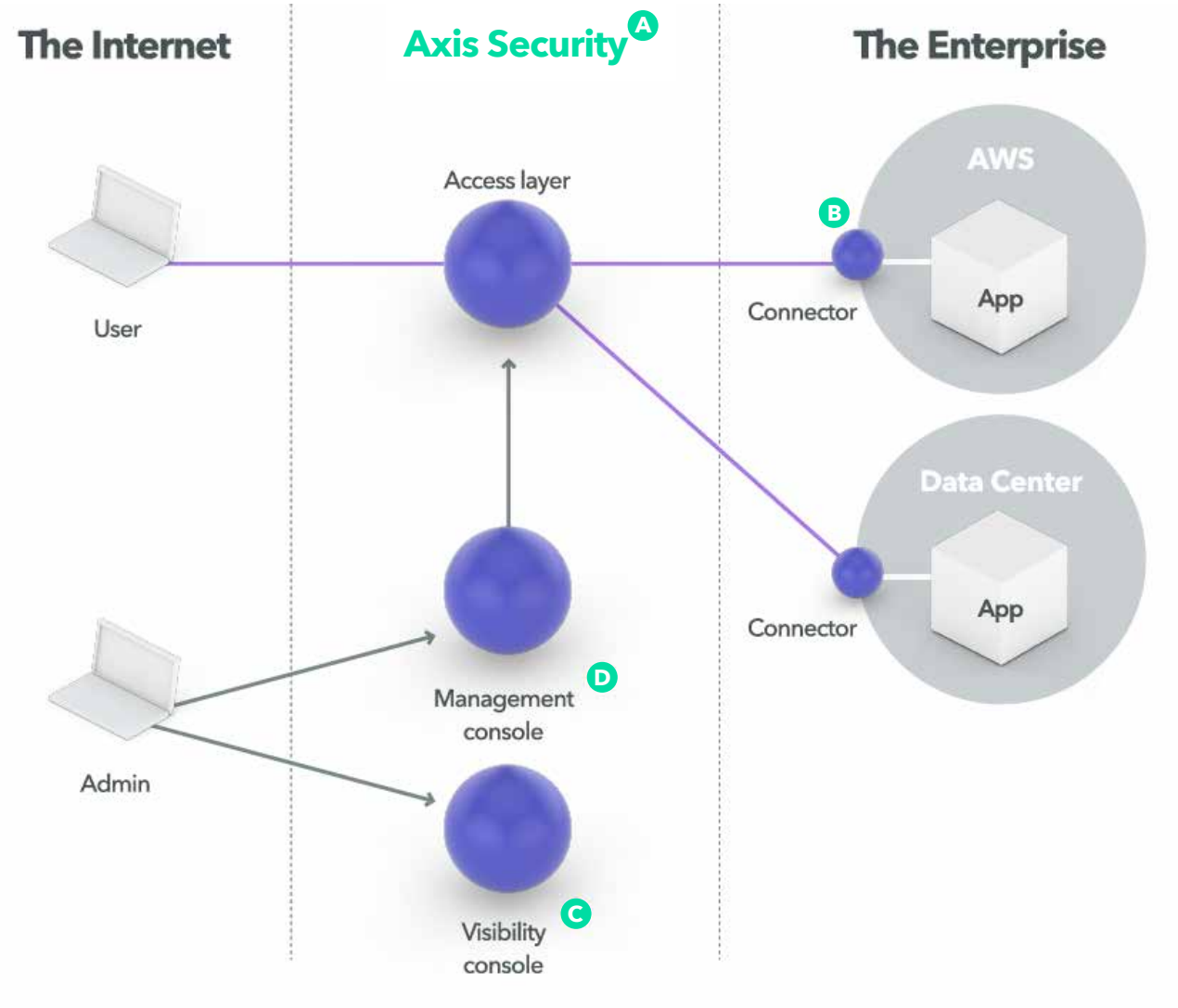
Applications published through the Application Access Cloud enjoy security upgrades out of the box. TLS 1.3 is enabled on every application, even those who currently don't support TLS at all. Protocols are hardened against known attacks, headers and channels are limited to a whitelist, and the underlying infrastructure becomes invisible to the users.

The Axis Security Approach

Contrary to what you may have read in the past: users actually rarely need network access. In nearly every use case, all a user needs is application access. This is where Axis Security's Application Access Cloud does its best work.

Axis Security provides:	...Enabling you to:
Confidence that every single packet is authenticated, and that packets are only relayed on the application layer.	Eliminate network scans, n-day attacks, and the use of stolen app credentials.
A brokered connection to the app instead of gaining direct network-level access to an application and its host as with a VPN.	Limit the attack surface and lateral network attacks.
Seamless access to apps from any device anywhere without a need for additional software or user action.	Use BYOD and painless as-needed access to apps and data and deploy widely without administrative overhead.
Deep packet inspection to gain visibility into the actual user actions performed at the application level.	Attain true visibility, policy control, and business-ready analytics. It also enables session recording feature controls and more.
Continual assessment of user behaviors against policy baselines to identify and act on potential violations in near real-time.	Limit the potential for credential-based compromise (often harder to detect).
Detection of potentially malicious actions that can be addressed from within the platform or through other solutions over APIs.	Try a flexible approach to continuously and rapidly detect and respond to malicious events.
Agentless deployment, cloud implemented broker technology and centralized management.	Streamline implementation and maintenance, allowing for quick value realization and automated scalability.

Structure



A. SaaS

A highly scalable and redundant cloud application used to authenticate, authorize, route, and log every packet sent to the system. The enterprise infrastructure is only accessed by it, and is completely isolated from the wild internet. It controls the and runs declarative rules and AI on the accumulated data to block or alert on suspicious activity.

B. Connector

The connectors are lightweight containers deployed on the enterprise network. They mutually authenticate with the SaaS and communicate using a light and limited applicative protocol. They relay authorized connections to whitelisted apps, taking control of every layer but the application layer.

C. Visibility Console

A web service that allows the administrator to view the activity in the different apps, and the alerts triggered in the system. Data can be pivoted by app, session, user, user-group, site, etc.

D. Management Console + API

Used to manage the Axis policy, applications, connectors, users, and all other components. Administrators use our web interface or API to interact with the system and its configurations.

Worry-free Application Access

At a time when businesses need to extend access, security threats to that access grow even more dangerous and consequential. New problems arise, requiring new and innovative solutions to increase competitiveness and assure airtight security. Security and access problems result from extending access to both employees and 3rd parties to private applications, on-site, and in the cloud. VPNs only aggravate these problems further. Axis Security delivers a modern cloud-centric solution that makes application access simple, secure, and tightly managed. It's not only a game-changer for businesses; it's a zero-trust solution that might save them.

Axis Security
3 East Third Ave, Suite 203,
San Mateo, CA 94401

Phone: +1-650-850-8991
Email: info@axissecurity.com