axis

Securing **third-party access** with Axis

Connect your business ecosystem while keeping third-party risk off your network.

Brief Summary

Legacy access solutions amplify third-party risk.

Zero Trust Network Access (ZTNA) minimizes third-party risk while helping IT adopt a Security Service Edge (SSE) strategy.

Atmos is the trusted Security Service Edge (SSE) platform with the most advanced ZTNA offering.

In February 2022, Toyota completely halted their Japan-based operations after one of their third-party suppliers suffered a major data breach.

Not only did the third-party organization, Kojima, have access to Toyotas network and manufacturing plants, impacting production, but also affected operations of other Toyota subsidiaries as well.

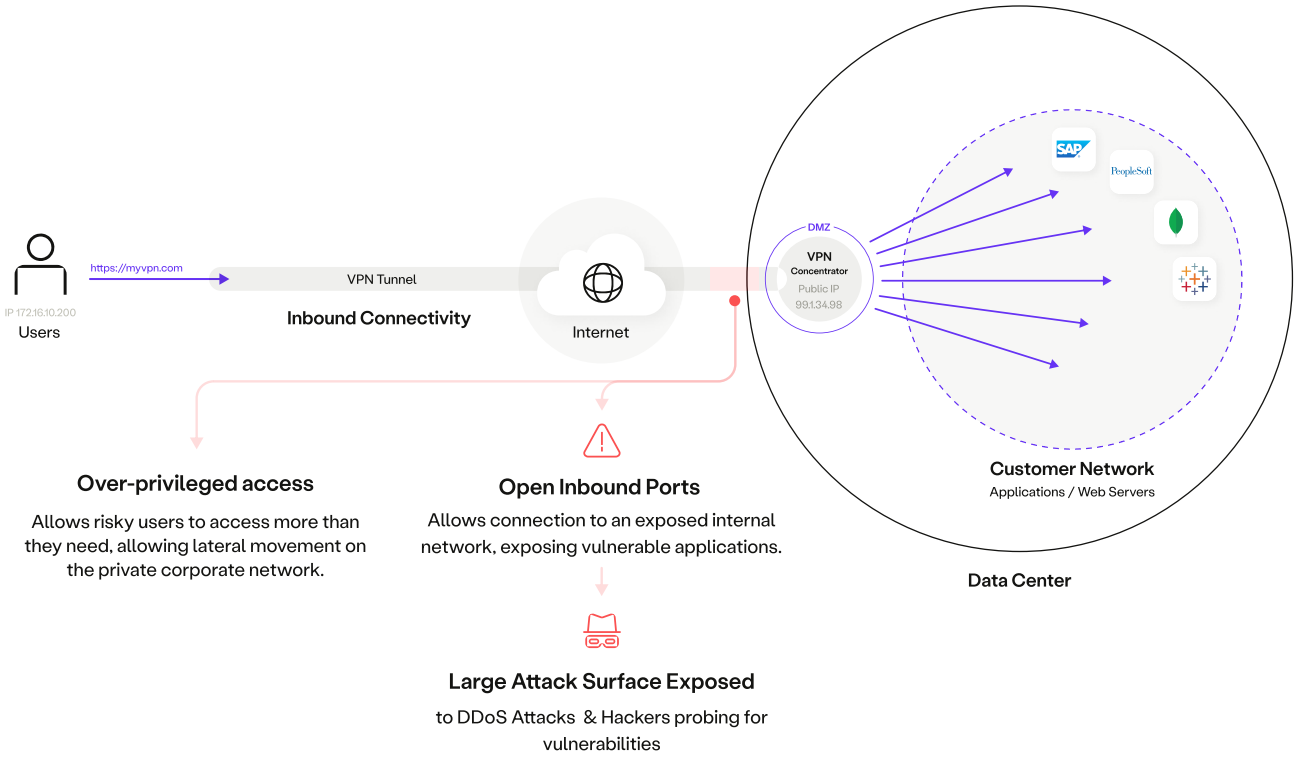
Not only was Toyotas network, data, and infrastructure put in danger, but ultimately production was halted, hurting Toyota's bottom line.

This is a word of warning for many. While we should not discourage the development of our business ecosystems, Security leaders must find better ways of enabling third-party access while never compromising the business or its data.

Third-party access from the past

In the past, third-party access depended heavily on remote access VPN technology. Whether accessing through a partner portal or directly to a data center application, a third-party user needed to download a client onto their device, wait for an admin to manually update ACL and FW policies, and only then could attempt access.

However, once this attempt was successful, the corporate network would open up like a treasure chest, giving the user access to not only the corporate network, but also all the crown jewels. This is the trouble with VPN, not only is network access extended to an untrusted user, on an untrusted device, accessing from an untrusted network, but once that third-party user is on the network, they can often access the entirety of the network with little restraint. This two-fold VPN problem is really at the crux of third-party risk.



Traditional VPN

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

Embracing **a modern approach** to secure third-party access

Whether third-party risk is introduced because of a weak password, outdated VPN software, BYOD devices, or simply users disregarding an organizations security policy, it's safe to say that security teams need a modern solution that will address these core areas:

Keep third-party users off the network.

Third-party users should never be extended network access, as they only need access to specific internal applications. Modern third-party access must break the idea that application access = network access. Instead, user access must be defined on a least-privilege basis.

Empower productivity, not risk

It's not wrong for the enterprise to want both strong security and a great user experience. In fact, who said you had to choose? Security Leaders must adopt solutions that encourage strong partnerships by enabling simple, easy access, while ensuring third-party risk doesn't touch your business resources and data.

Better security through better visibility and control

"Visibility" is not IP address and Port data, just as "Control" is not through the means of network segmentation. True visibility allows IT teams to know exactly what users are accessing, how they are accessing it, and what actions were taken during access. True control gives IT the means to authorize activity down to the granular-level of user or device.

These things are not possible with legacy access solutions, like VPN, but are with Zero Trust Network Access (ZTNA) solutions as part of a great Security Service Edge (SSE) platform.

Zero Trust Network Access (ZTNA)

Created in April of 2019 by **Gartner**, the term Zero Trust Network Access (ZTNA) represents a new technology subset that falls within a Security Service Edge (SSE) platform. The ZTNA portion of SSE is designed to specifically secure access to all 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.

Security Service Edge (SSE)

A Security Service Edge (SSE) platform is a set of integrated, cloud-delivered, security services that broker secure connections between authorized users and business resources by using identity and policy. An SSE platform consolidates three primary solutions into a single cloud offering, ZTNA for private apps, CASB for SaaS apps, and SWG for all web access. Some more advanced SSE platforms also include Digital Experience Monitoring (DEM) capabilities.

Elegant and secure **third-party access with Atmos**

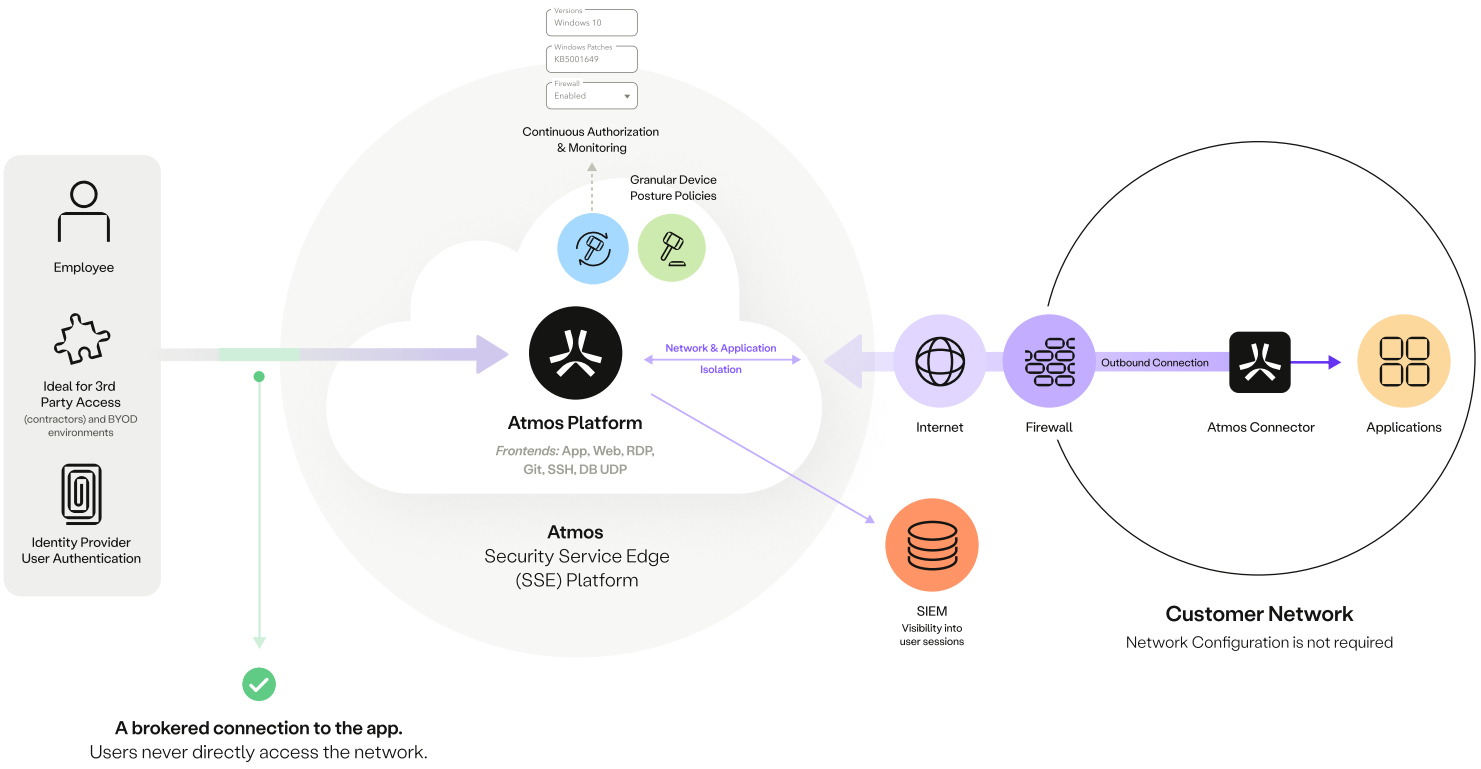
Today the modern business is highly integrated, meaning that business success often depends on the partnerships established through contractors, suppliers, vendors, partners, and B2B customers. It's the security team's duty to ensure that these often risky users can access business resources without putting the business at risk. For this reason many organizations are beginning to adopt a Security Service Edge (SSE) platform.

With 350 PoPs across the globe, Atmos by Axis provides the most reliable, available, and scalable Security Service Edge (SSE) platform designed for secure connectivity to all business resources.

As part of the greater SSE platform, Atmos ZTNA specifically ensures that private application access can be granted without having to require access to the corporate network. This decoupling helps reduce network security risks - like overprivileged access, BYOD risk, and lateral propagation in the event of a breach.

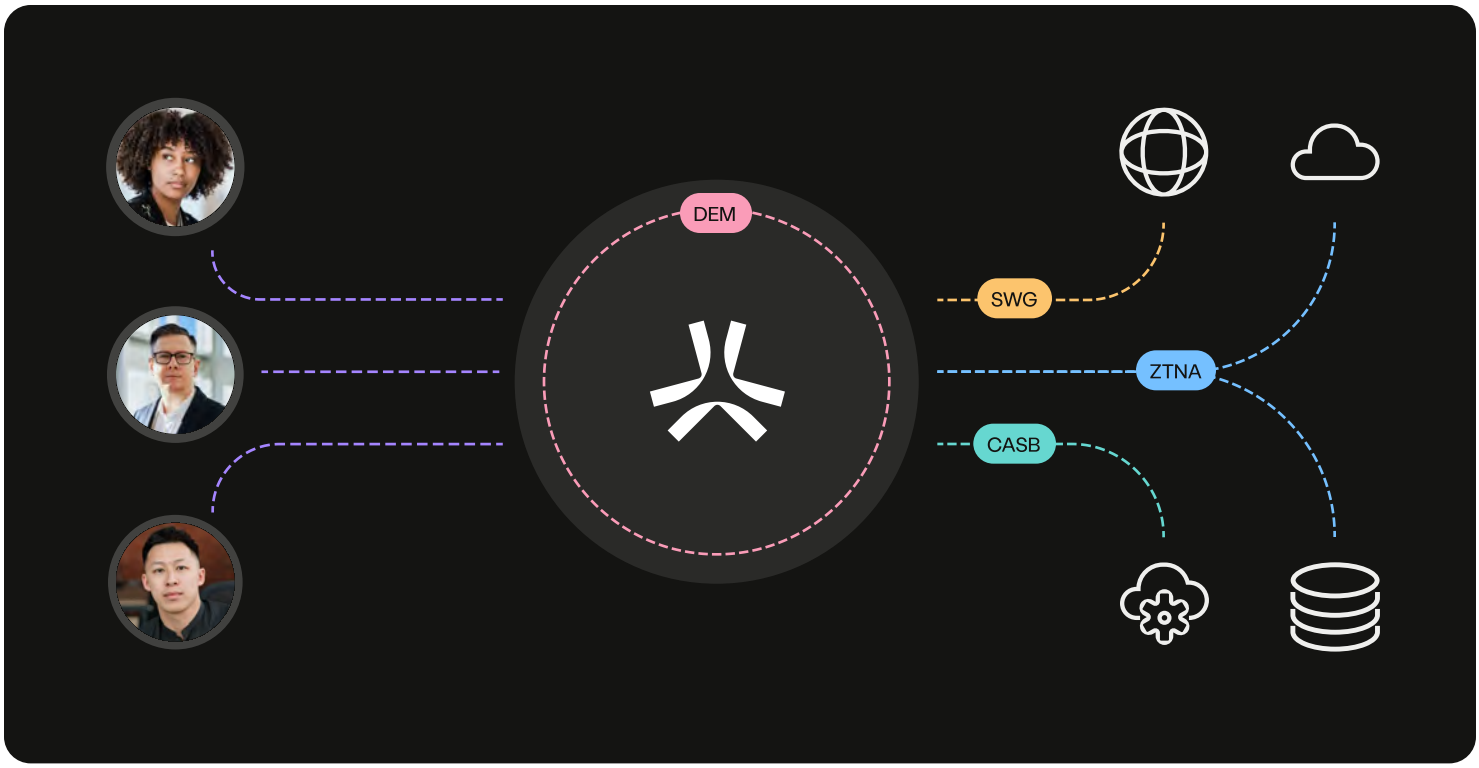
Unlike a VPN concentrator, Atmos uses a service-initiated architecture to leverage what we call outbound-only connections. This connection type ensures that the network infrastructure and business applications are masked from the Internet and cannot be located or DDoSed because they do not listen for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

Atmos 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.



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 Atmos-managed application, the user is redirected to the associated application identity provider
3. Atmos 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: Atmos can actively inspect traffic and can close the session due to a security event.
5. Atmos 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 Atmos Connector via specific port to the Atmos 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.

Benefits of **Atmos SSE**



Universal access for all

Whether you're supporting partners, suppliers, contractors, B2B customers, (and of course your employees) Atmos provides universal secure access to every type of user. So as your secure access needs grow, Atmos grows along with you.

Flexibility with robust agent and agentless access

Atmos is the only SSE service that supports all ports and protocols, even VOIP, ICMP, AS400 apps, and RDP, SSH, Git and DG via agentless web browsing – plus common SaaS apps and Internet protocols. This means you can eliminate the headache of requiring third parties to download clients onto their BYOD devices and make access easy.

Granular and adaptive access control without the complexity

Easily implement least-privileged access for third-party users with simple yet granular policy-based access. 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.

Enhanced monitoring and threat detection

Unlike other SSE platforms, Atmos is designed to inspect all traffic. Gain deep visibility into what third-parties and employees are accessing and identify security risks at the source for quick remediation. Gain deep visibility into what third-parties and employees are accessing and identify security risks at the source for quick remediation.

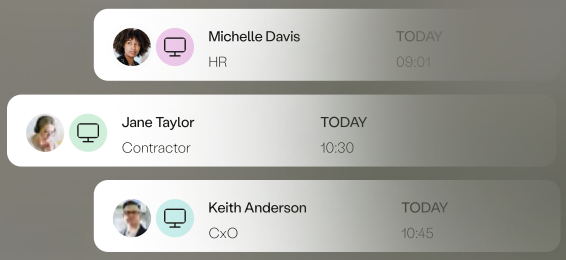
See how Atmos can **secure your third-party users**

Overall, an SSE platform can provide a comprehensive security solution that can help businesses overcome the risks associated with third-party users and legacy access solutions, by providing a secure and compliant access to company's resources, while protecting sensitive data and infrastructure.

This is why **65% of organizations** plan to adopt an SSE platform in the next two years, the question is will you?

Ready to explore **a safer approach to third-party access** with Atmos?

Get started with one of these common third-party use cases:



Contractor access

Learn more →

Partner access to OT

Learn more →

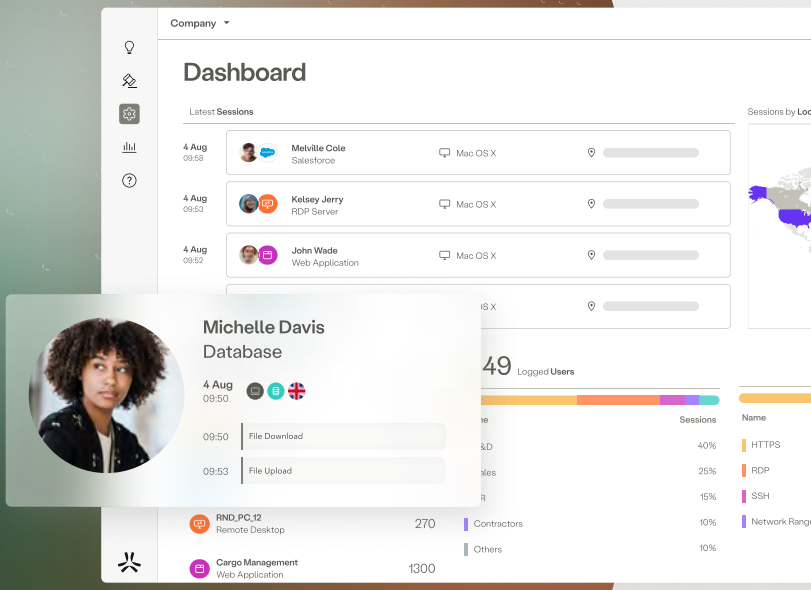
B2B customer access

Learn more →

Discover **Atmos** by axis

Learn more about Atmos SSE

Request a free trial



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.