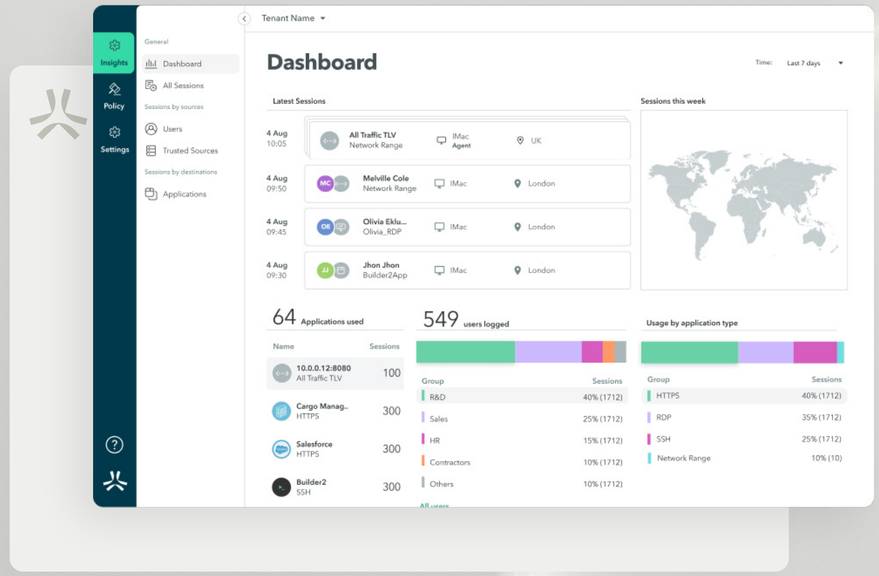
Atmos

by Axis

Secure the Modern Workplace with the world's most elegant Security Service Edge (SSE) platform.



When connectivity is in sync with the workplace you can:

Enable the distributed enterprise

77% of companies will allow hybrid work. Empower employees to work from anywhere by seamlessly connecting employees to apps from any location, device, or network.

Secure third-party access

1/3 users are partners, suppliers, vendors or customers. Enable the business ecosystem to securely access sensitive data - without extending network access or installing an agent.

Modernize infrastructure

Transform the network to a modern cloud architecture. Replace legacy appliances, simplify hybrid-cloud adoption, reduce infrastructure costs and introduce automation.

axis

To outpace competition IT has been asked to invest in services designed to ensure the productivity of the workforce, and its supply chain. This has created an opportunity for IT to define the new technologies that will connect their users to key business resources like M365, Salesforce and SAP. Ninety percent of IT leaders have plans to adopt SaaS and hybrid cloud services that extend connectivity out to their workforce. In this modern workplace every user, application, and their device are connected to the Internet.

Unlike the traditional network, the Internet cannot be controlled by IT. Because of this, the network solutions that worked for the past 30 years are not only obsolete, but they place users on the network and expose infrastructure to the Internet. A new approach is needed in order to securely, and seamlessly, control access over the Internet.

Axis aims to accelerate the transition to the modern workplace, through security connectivity with its platform. Short for "Atmosphere," Atmos by Axis is a Security Service Edge (SSE) platform that uses 350 edge locations to elegantly connect users, and servers, to the business resources needed for work. The platform artfully integrates Atmos ZTNA, Atmos SWG, Atmos CASB and Atmos Experience into one, cloud-delivered, platform that feels weightless, and is controlled by a single pane of glass.

axis

Super Simple

Atmos minimizes complexity.

Direct the orchestra of users and apps from one pane of glass. It's cloud design lightens the management burden for IT, and is equipped with an elegant policy-tagging system for simplicity.

Super Smart

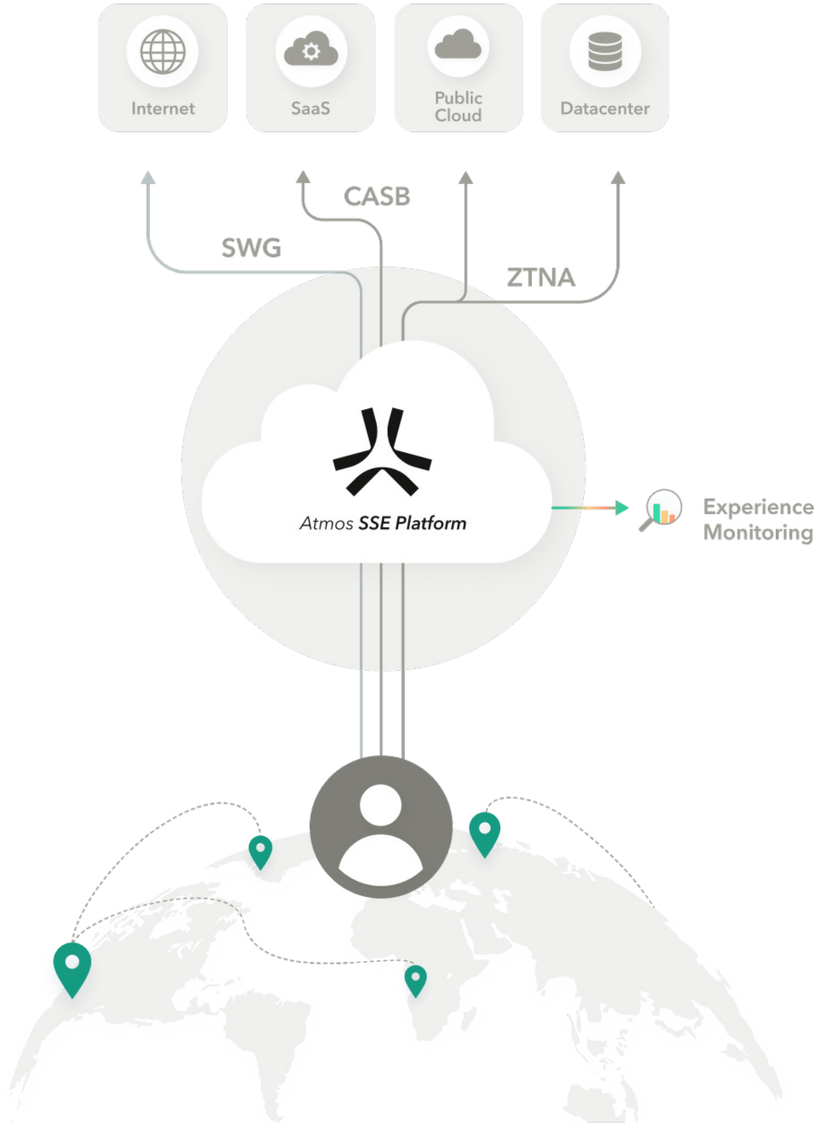
Atmos proves being smarter, cooler.

Auto-sync with the environment with a cybersecurity mesh of IDP and endpoint services to auto-tune policies, and fluently adapt access rights. Even react faster to user experience issues.

Super Secure

Atmos makes security omnipresent.

Inspect traffic to elevate visibility and prevent ransomware. Protect against data leakage. Detect and respond faster to protect against threats.



Atmos Capabilities

Zero trust network access (ZTNA)

Atmos ZTNA is the most advanced ZTNA service in the industry. It uses identity, policy and context to broker secure, one-to-one, connections to private apps (even VOIP, AS400, and ICMP). It fully replaces VPN, and avoids the need for network access or exposure.

Secure web gateway (SWG)

Atmos Web Gateway uses advanced SSL inspection, URL filtering, and DNS filtering, to ensure that authorized users get fast, secure access to the Internet - while protecting the business from Internet-based threats that aim to harm it.

Cloud access security broker (CASB)

Atmos CASB mediates the connections between users and cloud applications, and helps discover Shadow IT to apps. Atmos CASB ensures sensitive business data in motion remains protected, while helping prevent cyberthreats.

Digital experience monitoring (DEM)

Atmos Experience ensures user productivity by measuring hop-by-hop metrics, and monitoring app, device and network performance. IT can easily pinpoint connectivity issues, and reduce mean time to innocence.

Single pane of glass

With the Atmos Dashboard IT can manage access to all private apps, Internet, SaaS apps, and digital experience monitoring from one console. Easily define policies, track user activity, manage tenants, and oversee a cybersecurity mesh of SSE, IDP, and endpoint security.

Inspection of all traffic

View user activity, files downloaded, commands used and block malicious actions by inspecting all private and public traffic with Atmos ZTNA and Atmos Web Gateway.

Application discovery

Shine light on unsanctioned applications, and domains, easily define policies for each, and reduce the organization's overall attack surface.

Automated alerts and data classification

Atmos uses AI to generate alerts, automatically detect potential security events, and improves the classification of data.

Agent and agent-less

Atmos Agent forwards traffic to the Atmos platform, performs device posture assessment, and integrates with existing endpoint solutions.The agent supports iOS, Android, Mac and Windows. Atmos "Air" is the agentless access mode. It secures access to web-based apps - even browser-based RDP, SSH, Git and database.

Server-to-server access

Atmos ensures servers safely communicate with other servers, applying zero trust to non-user entities.

Data leakage prevention

Protect sensitive data from leaking out to the Internet by sitting inline and enforcing policies that block file downloads, copy and paste, and help meet compliance standards. Support agentless and agent-based deployments.

Detection and response

Prevent malware-based attacks before they even begin with advanced malware scanning and detection. Increased insights allow teams to respond to security events faster than ever.

axis

To learn more visit us at
www.axissecurity.com