The Architect's Guide to

Adopting Security Service Edge *(SSE)*

Author: **Jaye Tillson** | Director of Strategy

axis security

The Architect's Guide to

Adopting Security Service Edge *(SSE)*

Introduction to
Modern Application Access

Architects are **lucky.**

In the fast-paced world of technology, architects have a front row seat to cutting edge innovations, especially in emerging areas of network and security technologies.

In many cases, these innovations come from rising startups with fresh perspectives on the market and solutions.

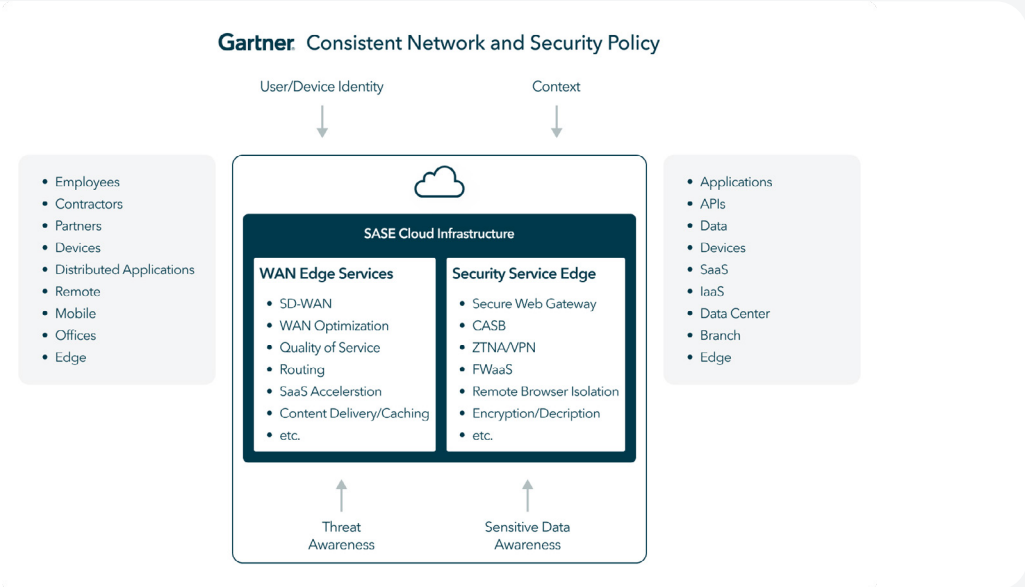
It is up to the architects of today to choose these innovative solutions and technologies that solve long-withstanding problems, one area being secure application access.

Over the decades, enterprises have been able to deliver secure access to business resources through a variety of means: virtual access to desktops and apps with VDI solutions, application access through the corporate network using VPNs, and Internet access using web gateway technologies. However, the issue with all these solutions is that they don't solve the root problem…. The inherent need for network access.

With a now hybrid workforce, and applications that are hosted in the cloud, architects are unable to rely on technologies built for securing network-bound users and applications. Architects must reevaluate how secure application access is delivered.

Gartner has identified this shift, coining a new term, the Secure Access Service Edge (SASE) in 2019. SASE, pronounced "sassy", is not a single product, but rather a modern framework that enables secure connections between users, systems, and endpoint devices anywhere.

SASE Detailed View:



While we can all agree that the direction of SASE is correct, the challenges of implementation have led Gartner to further define this framework, breaking it down into two main categories: **(1)** WAN Edge Services and **(2)** Security Service Edge (SSE).

In this guide our focus is to help you navigate through the value of the SSE half of the SASE strategy and some real-world tips on successful deployments:

- **Why SSE is the Future of Security.**
  The Architect's journey should always begin with a thorough understanding of a framework or platform prior to production deployment recommendations.
- **Business Use Cases for Easy Wins.**
  Architects live in a world that spans between technology and business, so it is important to understand what use cases can provide quick wins and have the most positive impact to your business.
- **Top Four Recommendations for a Successful SSE Journey.**
  Gartner recommends starting your SSE journey by first deploying a Zero Trust Network Access (ZTNA) service. Learn deployment recommendations from real-world examples and avoid common pitfalls.

Want an overview on SSE? Watch this "What is Security Service Edge (SSE)?" video

This is a thoughtful (non-technical) video you can watch and share with others to understand why SSE implementation is critical on the road to SASE.

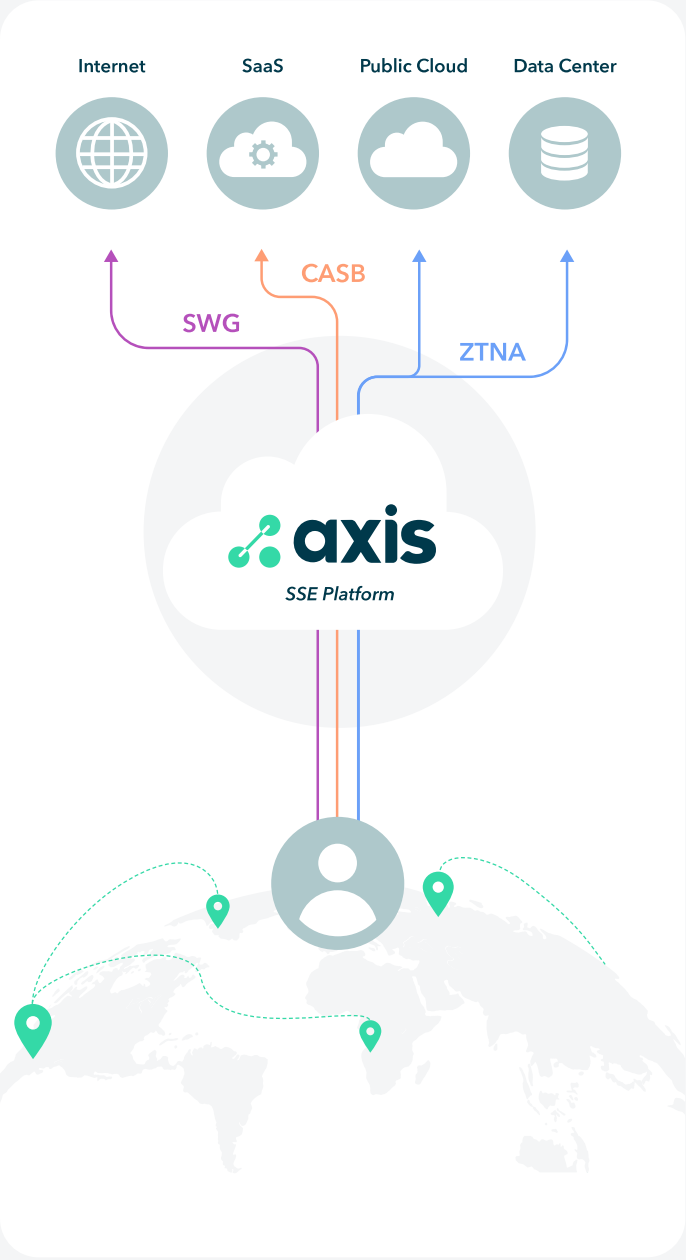
Watch Now

Why SSE is the Future of Security

An SSE platform provides unified secure access, visibility and control to all business applications, consolidating three primary solutions into one cloud offering (ZTNA, SWG, and CASB).

The capabilities must include ZTNA for private apps, CASB for SaaS apps, and SWG for all web access. More importantly, each of these capabilities must be natively built into a single SaaS offering to reduce the operational costs and barriers enterprises typically encounter with disparate products and frameworks.

Additionally, SSE provides a single unified platform for all application access while decoupling application access from the corporate network. An SSE platform serves as an overlay on the existing network, allowing IT to modernize and simplify connectivity while strengthening security, without having to make complex network architecture changes.



So, what isn't considered SSE?

Let's go back to the year 2007 when some of the first cloud secure web gateways were being built. At that time cloud platforms like AWS and Azure weren't trusted, many SaaS apps like Office 365, Zoom, and Slack didn't even exist yet. If you are looking for a true SSE platform that has natively built all the capabilities into a single cloud platform offering, vendors that have been around for 10+ years might not be the best option. In this case, older does not mean better as many have acquired one-off companies, built separate VMs, or stitched together separate infrastructure to create a Frankenstein-like SSE platform. The result is often felt by the customer as user experience, management, and visibility suffer because of multiple solutions disguised as a single platform. The "cutting-edge" vendors developed a decade ago are now "legacy" vendors - and it is time for the new generation of security platforms to replace them.

SSE Guiding Principles

- **Look for singular architecture built for the cloud and hosted within the cloud.**

  An SSE platform must provide a unified architecture for all ZTNA, SWG CASB, and Digital Experience capabilities (not integrations from different products the vendor has built). View and control everything in a single pane of glass across cloud environments, workforce users, and work locations.

- **Flexible and intelligent traffic management.**

  Enterprises need to control how and where application traffic is brokered, and stored, for compliance, security, and performance reasons. An SSE platform must provide public and private edge locations, globally, and offer simple, yet effective, management for admins to control traffic based on specific criteria.

- **Decouple users and devices from the network.**

  Application access should be controlled via identity and application-based policies. The concept of the corporate network should be limited to IT-controlled server infrastructure and assets, and the user networks should all be treated as untrusted. Decoupling the network allows enterprises to focus on security controls without needing to worry about placing risk on the network. This not only allows for reduced lateral movement on the network, but also minimizes the overall attack surface by placing applications and resources behind the SSE platform where they cannot be attacked.

- **Unified visibility and protection for all app access: Private, SaaS, and Web.**

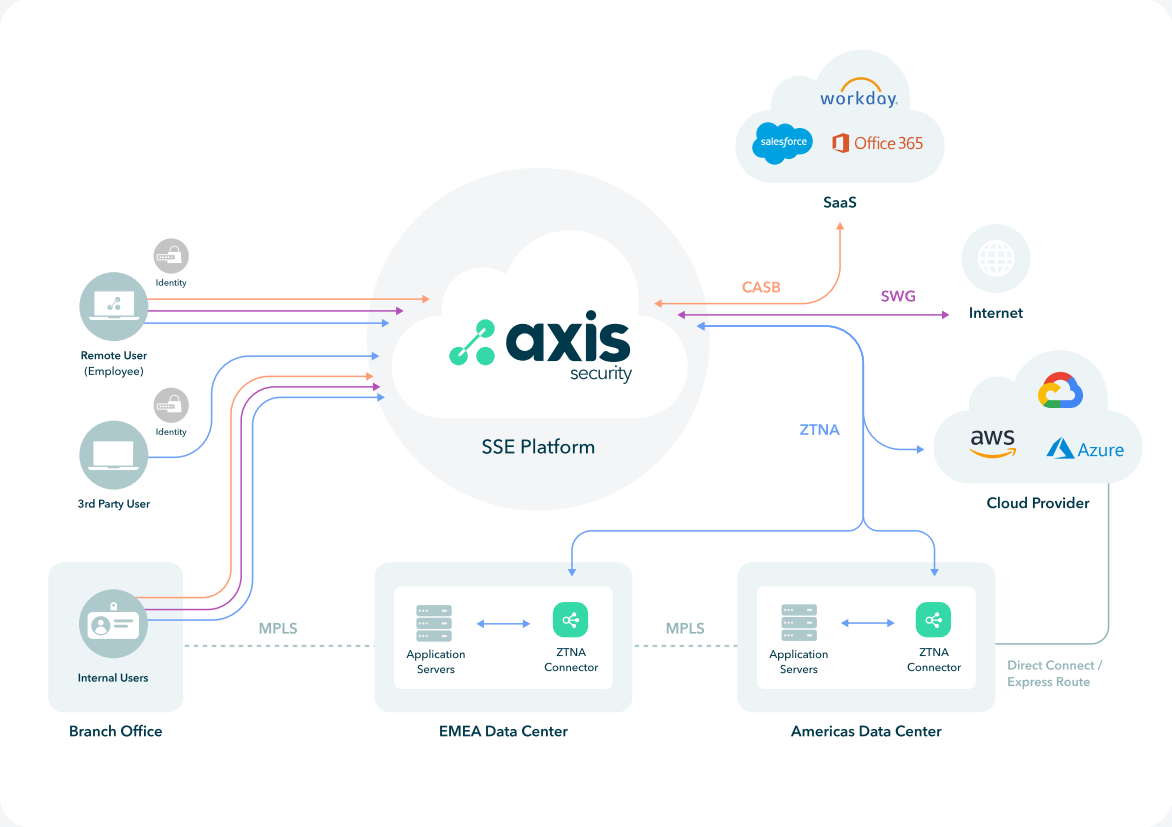
  Enterprises should not have to worry about what type of application or data is being accessed by users and devices. The platform should provide uniform visibility and control over all these applications. This will also ensure that policy management is as simple as possible.

Business Use Cases *for Easy Wins*

Before we dive into deployment recommendations, let's cover some of the most common use cases that IT leaders should begin with. Just like with any new journey, it is important to educate, plan, and take a phased approach, rather than attempting to change everything at once. Below are some recommended use cases:

Remote Access to Private Applications

Many enterprises are still using legacy VPN to provide network access to remote employees, and extended business ecosystems, who only really need access to a limited number of private applications. Gartner recommends prioritizing ZTNA for VPN replacement as the initial use case for SSE deployment and believes that 60% of enterprises will replace VPNs in favor of ZTNA by 2023. By prioritizing ZTNA adoption for business-critical applications, IT can significantly reduce risk while also providing a better user experience for the business.



Secure Access to SaaS Applications

There are millions of websites and SaaS applications users can access, so it is important to simplify things as much as possible by categorizing apps into a few buckets based on business need, data leakage risk, and user performance impact risk.

Define the business application services used by your enterprise, such as Office 365, Salesforce, Workday, etc. These services will typically require controlled access, visibility for threat detection, threat prevention, and data loss prevention. This is where a SWG solution becomes incredibly important and should be deployed. As enterprises shift to SaaS offerings, a large portion of customer/user data, financial data, intellectual property and other critical data is spread across the globe. Protecting access to these services with such data is critical.

For the rest of the Internet and web applications, a SWG allows enterprises to gain a baseline level of security and control by assessing and categorizing the following:

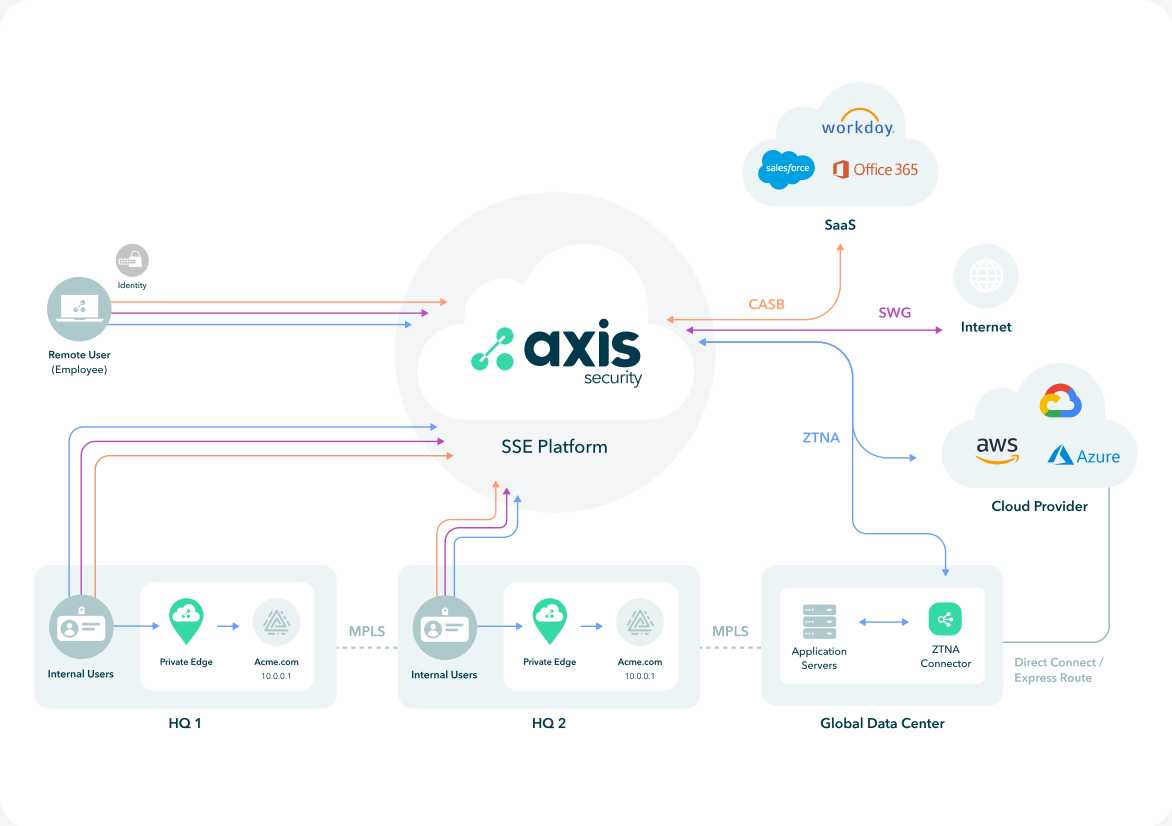
- Business Critical
- Business Important
- Business Low
- Personal, Blocked and Malicious

The key is to provide the best user experience and lowest level of risk without compromising security. Having the choices to block by DNS or URLs with SSL/TLS inspection are critical in the SSE platform to use the right settings for the right use cases.

Return to Office

As organizations allow employees to return to the office, or work in a hybrid context, it is important that users receive the same zero trust standard and consistent access experience. Consider re-evaluating policies if traditionally you have blocked access to streaming audio, streaming video, and social media sites. This is especially important if your employees have been allowed to use these sites from their devices used to access work resources while at home or remote.

The best way to allow this is to provide all office locations with (guest) networks that only have Internet connectivity. This removes the risk of lateral movement or the "blast radius" if the Offices have network connectivity to datacenters and other Office locations, while still providing employees with the same experience. Have a plan in place to start reducing Branch Connectivity (discussed in the next sections below) to make this a more permanent stance.

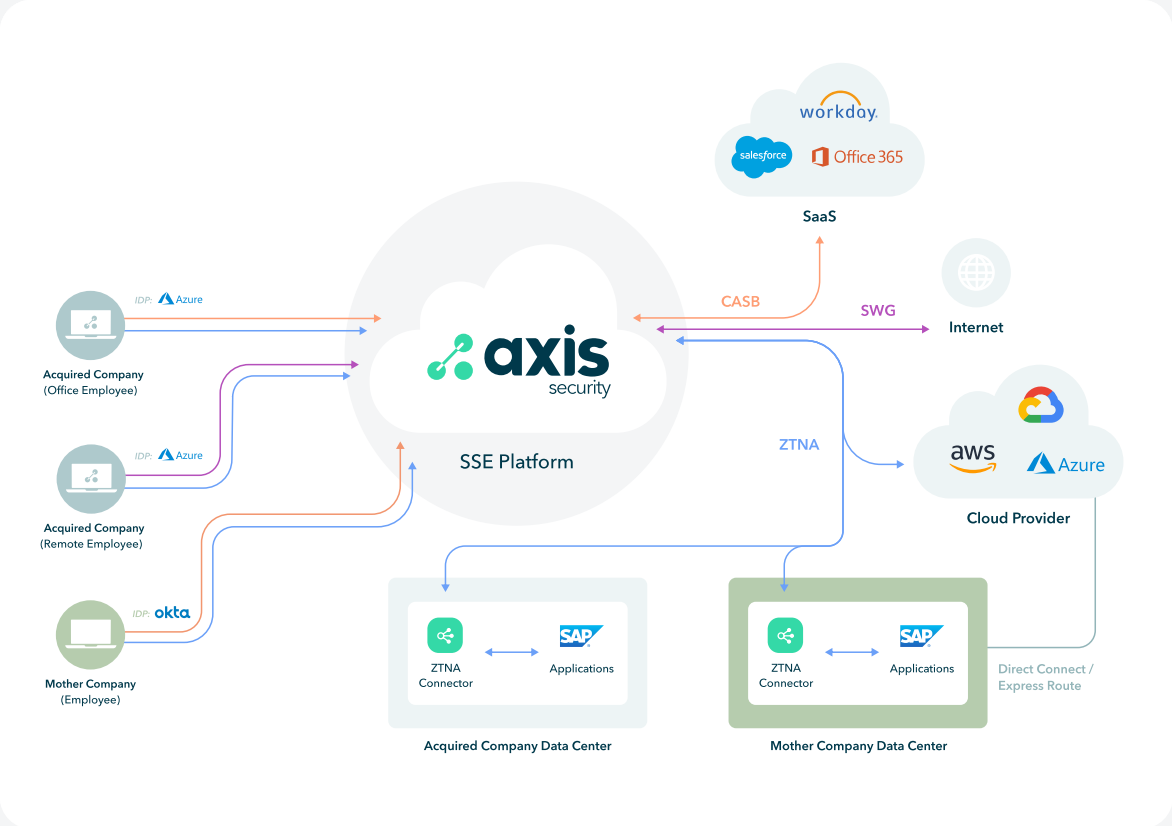


Mergers & Acquisitions: Accelerate IT Integration

M&A is not easy; however, the good news is there is an easy way to provide Day 1 access to the most important applications for users on “both sides” - without integrating networks or infrastructure. The key is having a prioritized list of Day 1 applications, such as HR, ERP, and other web-based tools that need to be accessed using the SSE platform.

The second factor will be having an identity strategy to ensure the users can access these apps using strong authentication even prior to consolidating the directories, users, and groups from all organizations in the M&A situation.

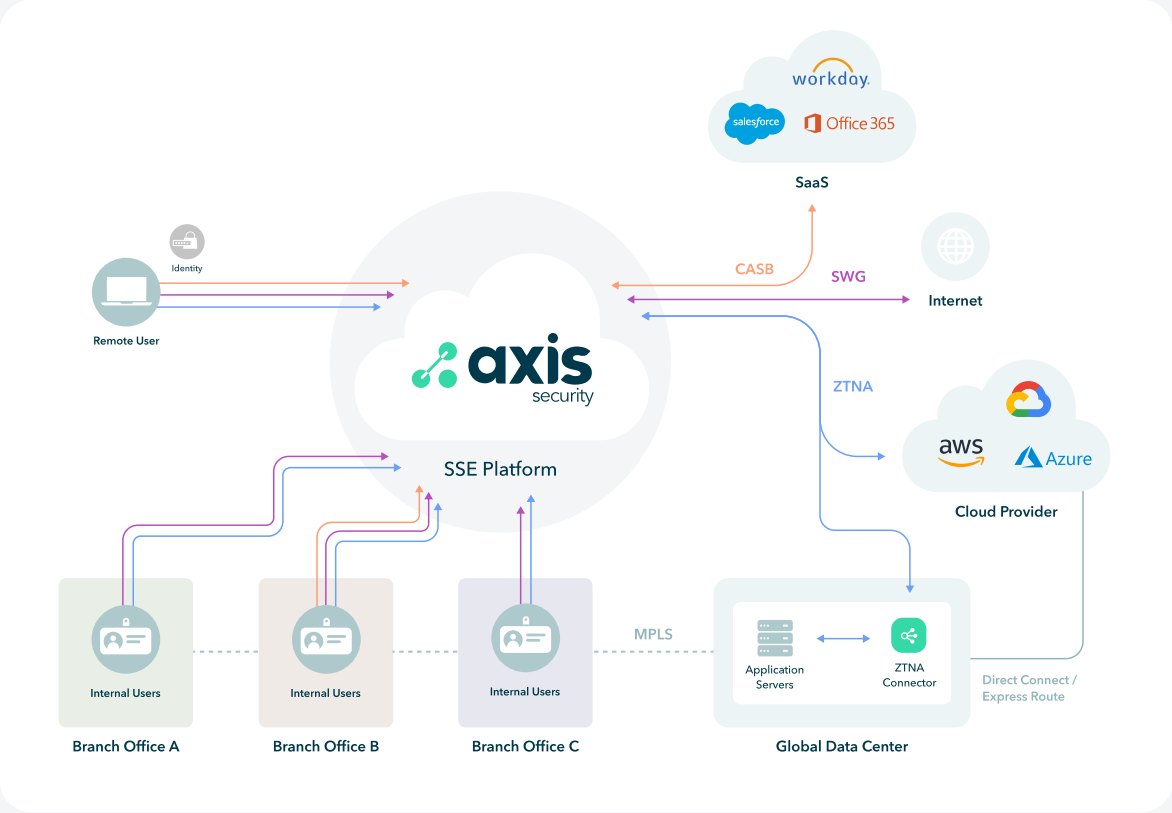
The SSE platform should provide the ability to integrate with multiple Identity Providers to achieve the application access requirements for all users.



Branch Connectivity Reduction

Enterprises over the past few years have reduced MPLS spend and optimized branch connectivity using SD-WAN technologies. The reality is that not every branch location truly requires SD-WAN. Branches where most traffic is destined for the Internet should just connect through an SSE service instead. Additionally, since SD-WAN services are designed to connect users to a network, the "blast radius" and risk of lateral movement is often increased if not coupled with an SSE service.

To combat this, it is simple to assess the requirements with an SSE platform and start removing all network connectivity from branch offices that do not require low latency direct connectivity to a main datacenter or hub. An SSE platform will provide high-speed, low-cost Internet services at these branch offices while lateral movement is minimized through implementation of least-privileged access policies.



Top Recommendations

Successful SSE Deployment

We've led deployments for many enterprises, and have developed a few recommendations on where to begin along the way. The easiest way to reduce the overall risk to your data, networks, servers, and applications is to first take users off the network. This starts with ZTNA.

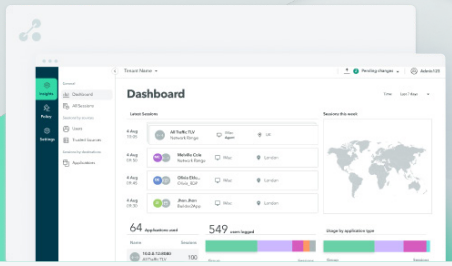
Many breaches that have resulted in data loss, data exfiltration, can be traced back to a compromised user or server. In either case, malicious malware is typically deployed, and can then spread laterally across the network. If all data centers, Cloud VPNs, and branch offices all have network routing and connectivity, the blast radius is exponential.

When deployed properly a ZTNA service can significantly reduce that blast radius, and, at a minimum, make it much harder for a bad actor to gain access to important data.

We have compiled a list of the top business and technical recommendations to ensure successful ZTNA deployment on your path to holistic SSE.

For more detailed information on recommendations, request an Axis demo.

Request a Demo



App Discovery and Least Privileged App Access

Problem:

Organizations have different teams, such as Networking, Security, Cloud, Infrastructure, and of course individual Application Owners. In most cases, application access from a network and VPN perspective were not required because full network-level access was provided for most users (yes, it is possible to limit subnet access in VPN policies, but in many cases, this has not been implemented by many enterprises).

Moving to a ZTNA solution is simple but requires some application awareness, unlike a VPN. The problem usually starts with false assumptions: the ZTNA owners in the IT department have knowledge or expertise in every application deployed in an enterprise. This problem is multiplied as the organization size increases. This causes many applications in a ZTNA platform to not include all the correctrights hostnames or ports, resulting in application access issues. In other cases, this is operationally overwhelming as it takes a lot of time, effort, and manual creation of individual applications when there are thousands across the enterprise.

Lastly, many customers have moved to a ZTNA platform and simply left the VPN-like policies in place by allowing full network access instead of least-privilege application access. Why? Because it is a 1:1 replacement of a known technology configuration and less operational overhead. The bad? All you have done is replace a VPN product with a ZTNA product that is not providing much better security than the VPN.

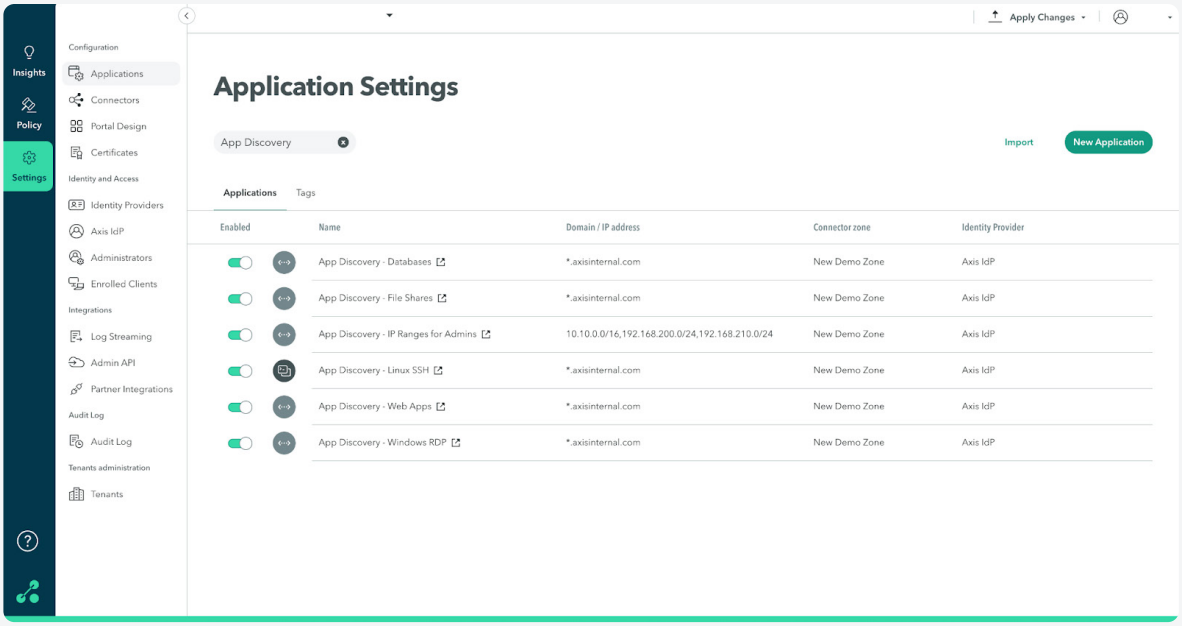
Recommendations:

Prioritize and publish the top 10-20 business critical applications to authorized users, groups, and other required conditions (such as device posture checks, geolocation restrictions, etc). These should be applications that fall into these categories:

- Used by over 90% of your user population
- Contain sensitive user, financial or customer data
- Contain intellectual property
- Are considered business critical (Business loses money each minute apps are not accessible)
- Prioritize and publish the applications accessed by 3rd party contractors and extended business ecosystem users. Try to focus on the application types that can be published clientless to reduce operational burden and troubleshooting with 3rd party user devices your enterprise does not manage

- Add a different application range for the "high risk" protocols that can potentially cause the most damage. The ZTNA solution should provide an option to determine wildcards or ranges so you do not have to start with each specific hostname, and break out these applications: RDP, SSH, Telnet, FTP, SMB/CIFS, NFS. Ensure only authorized users can remote into servers via RDP/SSH/Telnet specifically.
- Use the ZTNA Application Discovery capabilities to learn what other applications and servers are visible and accessible. Like most organizations, you will not know every single application, server, service, and port used by all your users and devices. Make sure the ZTNA Application Discovery is used in a phased approach.

  If your existing access (on network or VPN) provides access to all networks, start with App Discovery for all those network ranges and domains for all other destinations not defined in the above bullet points. Create a process to analyze the discovery apps on a weekly, bi-weekly, or month basis to start defining the applications individually for authorized users and groups. Over time you will have less "open" access in the Application Discovery, but it is important to understand most organizations will need this in the first 6-12 months to get a true understanding of application access requirements for all the different user types.



> As a phase 1 for employees, discovering what applications/protocols they access during "learning mode" is a way of deploying quickly but with little operation overhead; the application segmentation can be done in phases over time. It is critical to not allow networked-based access by IP addresses or enable ICMP for most of your users. However, the ZTNA solution should support those as IT engineers still need network access and to use tools. ZTNA should make it easy to limit that type of access only to personnel requiring such access

Identity Strategy

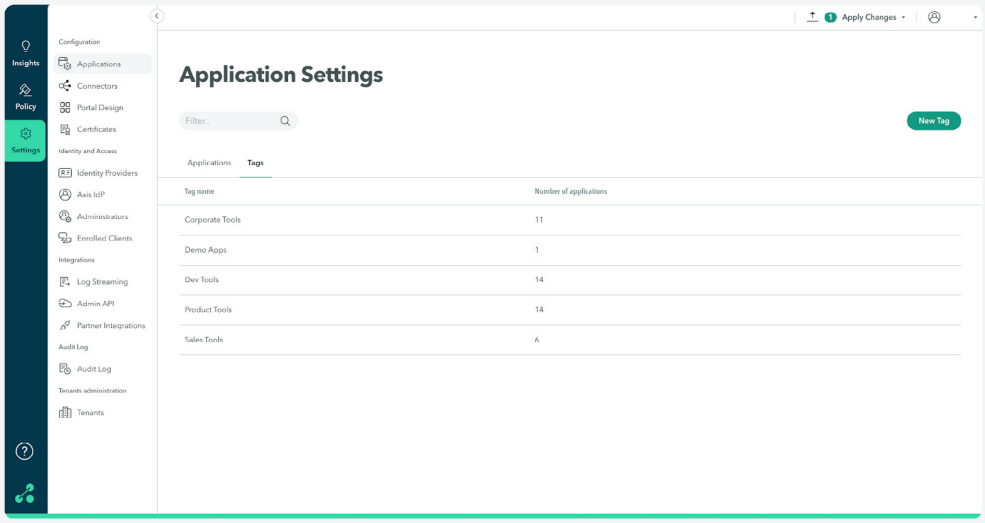
Problem:

Corporate identities and directories usually have years or decades of history, changes (growth, M&A activity, turnover), and sometimes lack of consistency. The larger the organization the more complicated the Identity Strategy can be, but it is important to start shifting to more of an application or use case-based approach when identifying group memberships. This can make the migration from on-network users to a ZTNA platform easier and scalable no matter the size of the organization.

Recommendations:

- Determine if any existing patterns or conventions exist for Groups and how users are added to them. Are Groups created by roles (such as Sales, Marketing, Accounting), by application (such as SAP, O365, Jira) or combination of these types.
- If possible, start creating Groups that are specific to applications or use cases that ZTNA policies can be applied to. The goal is to reduce the number of objects (groups and policies) needing to be configured in the ZTNA solution. This can be done in phases, with the most critical applications and use cases being addressed first. Continue creating these application and use case-based groups over time, but minimize operational efforts by only doing this for important applications.
- In many cases, nested groups can be utilized and can minimize the Identity changes. For example, if everyone in the Sales group accesses Salesforce, simply create a Salesforce or Sales Tools group and add the Sales group to it instead of all the individual sales users.
- Implement employee and application onboarding process to ensure users are added to the use case and application groups when joining the organization.
- Determine if full time employees are differentiated from contractors (3rd party as well as temp employees)?
- Determine if all users can authenticate to a single Identity Provider or if they are separated.
- Connect all Active Directories to your Identity Provider to ensure all users are synchronized and can authenticate using this provider via SAML 2.0.

→ Identity Strategy



> Whether an organization decides to create identity groups based on departments or job roles (Sales, Marketing, IT, etc) or via application access, it is important to tag applications in the ZTNA platform. This not only makes it easier to group applications together for reduced number of policies and less operational burden, but it also enables you to easily match those groups to the tags instead of mapping access to each individual application!

DNS-First Strategy

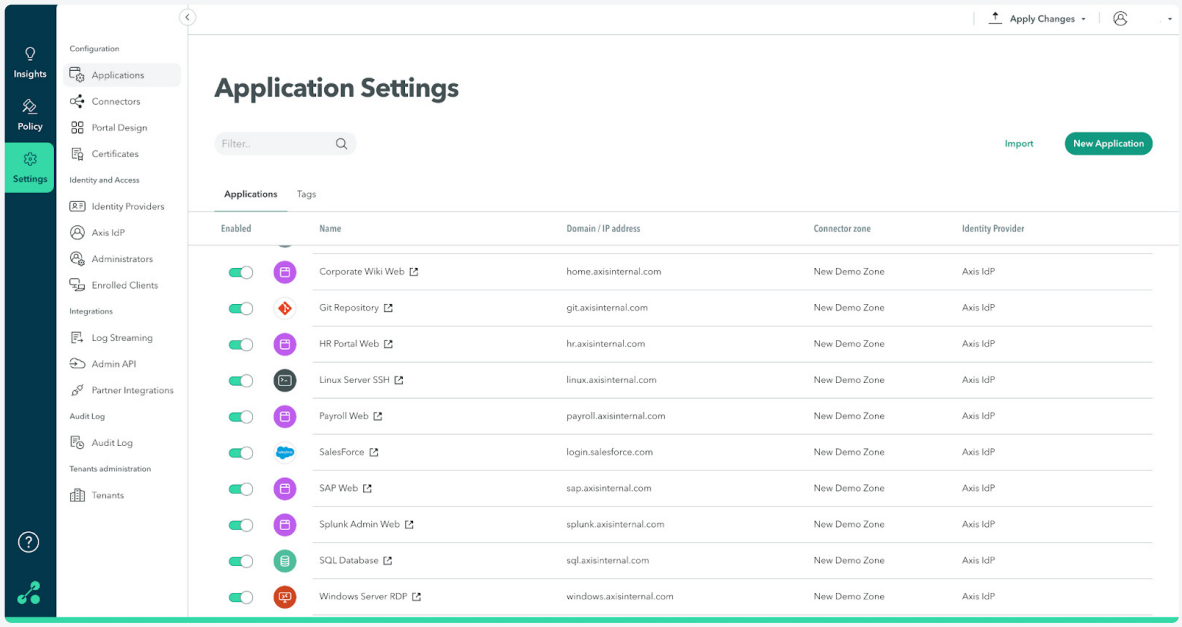
Problem:

Many organizations still provide application access via IP address. This could be to internal web applications, thick client applications, or connectivity to servers using protocols such as RDP and SSH. An internal IP range might not be intellectual property, but it is still a risk when there is malicious intent. Networks can change, networks need to be connected, and having IP address overlap causes additional burden on the networking team. IP addresses are also not user friendly.

Recommendations:

- Take inventory of the top 50 applications that are business critical or have been prioritized for access through the ZTNA solution. Ensure that internal DNS records exist for these applications and that users are made aware of the DNS records in case the users have bookmarks, shortcuts, or saved IP addresses on their computers. When most users start accessing applications via DNS in a ZTNA solution, it allows IT to make network changes, obfuscate the internal IP ranges.

- DNS access for end-user applications can proactively enable your enterprise to have smoother, faster, and lower-cost M&A activities. In many cases, there are network overlaps that require complex network connectivity and network address translation (NATing). With a ZTNA solution, all the applications that are accessed via DNS can have overlapping IP addresses without problems or a need to connect the networks.
- There might be some legacy systems or hard-coded IP addresses in certain thick client applications that are not easily changed. It is recommended to add this application using both DNS and IP address(es) into the ZTNA solution to ensure backwards compatibility.
- What about IT power users such as Network Engineers that need traditional network access? A ZTNA solution should allow your enterprise to provide IP-based access and optionally allow ICMP for troubleshooting to only these users. This strategy allows IT personnel to have network access to operate the network and systems, and still reduces the risk of all other users that have no technical need to have network access.



> When DNS is used, it allows for future network overlaps by decoupling the network from user access and also helps reduce risk by hiding the true IP addresses of servers

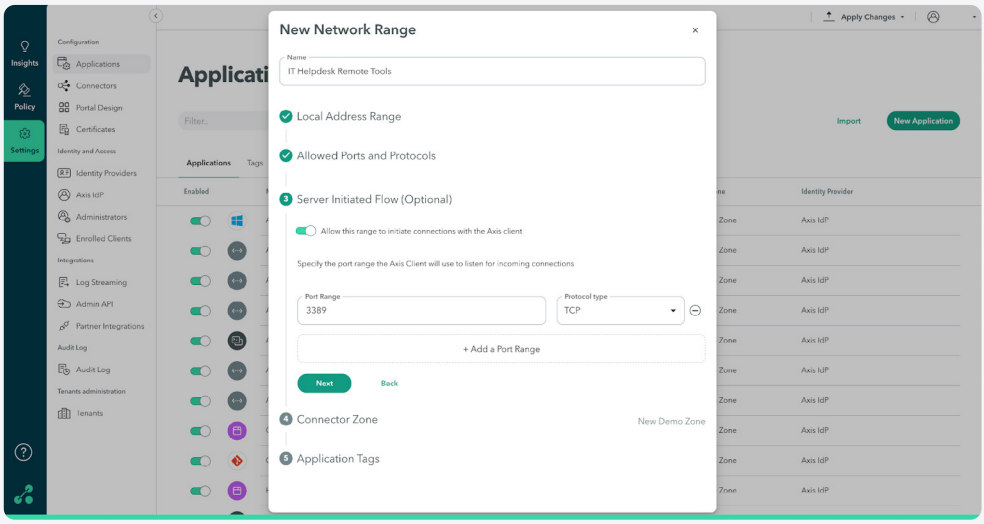
Server-Initiated and Peer-to-Peer Apps

Problem:

Modern software including endpoint agents are typically client-initiated and will work through a ZTNA solution. However, many enterprises do not consider server-initiated or peer-to-peer requirements when evaluating ZTNA vendors. This has in many cases required enterprises to deploy the ZTNA solution for certain users and keep the traditional VPN for other users (use cases) requiring these types of connectivity. This results in overlapping solutions, additional operating costs, and additional risk of still having users on the network with the VPN.

Recommendations:

- Take inventory of server-initiated and peer-to-peer applications. This list could include on-premises VOIP services, on-premise Chat services, Active FTP services, security and forensics software that requires IT to push commands to remote devices (not client-pull), and remote IT support tools (not client-pull).
- Ensure the ZTNA solution can support these use cases and traffic flows to ensure a single solution can replace all the remote access VPN use cases.
- Decide on a strategy to replace or upgrade server-initiated services with more modern client-initiated services where possible. This can lead to less operational overhead and a better user experience.



> Many organizations still have legacy tools, VOIP, or sever-initiated flows required for users. This might include pushing out patches to remote devices or IT personnel needing to RDP into a remote employee's machine for troubleshooting. Making sure the ZTNA tool offers this capability allows you to truly replace VPN but without placing the remote users onto the corporate network!

Get Started with ***SSE***

When starting your journey to SSE, the recommendation is to start by securing access to private applications with a ZTNA solution. Careful planning and prioritization of the most critical applications, data, assets and user types is key to successful deployments. Taking advantage of the best practices and recommendations will allow you to repeat this process for all your private apps and then extend the same secure access and protection to your web and SaaS applications.

Focus on the business use cases that are most critical to your organization and apply those recommendations to each use case. Remember, choose an SSE platform that will partner with you and your end users to deliver secure, simple, seamless access that meets the growing and evolving needs of your business.

Come start your SSE journey with Axis by signing up for a free trial.

Get Started

Jaye Tillson
Director of Strategy

Jaye Tillson is a Director of Strategy at Axis Security and has 20+ years of experience implementing strategic global technology programs, helping organizations achieve digital transformation.

Jaye is passionate about working with large enterprises on their strategic journey towards zero trust where he can bring forth real world experience on issues and problems.

These best practices are based on his experiences gained from working in close collaboration with multiple global business throughout his career.

About Axis Security

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.