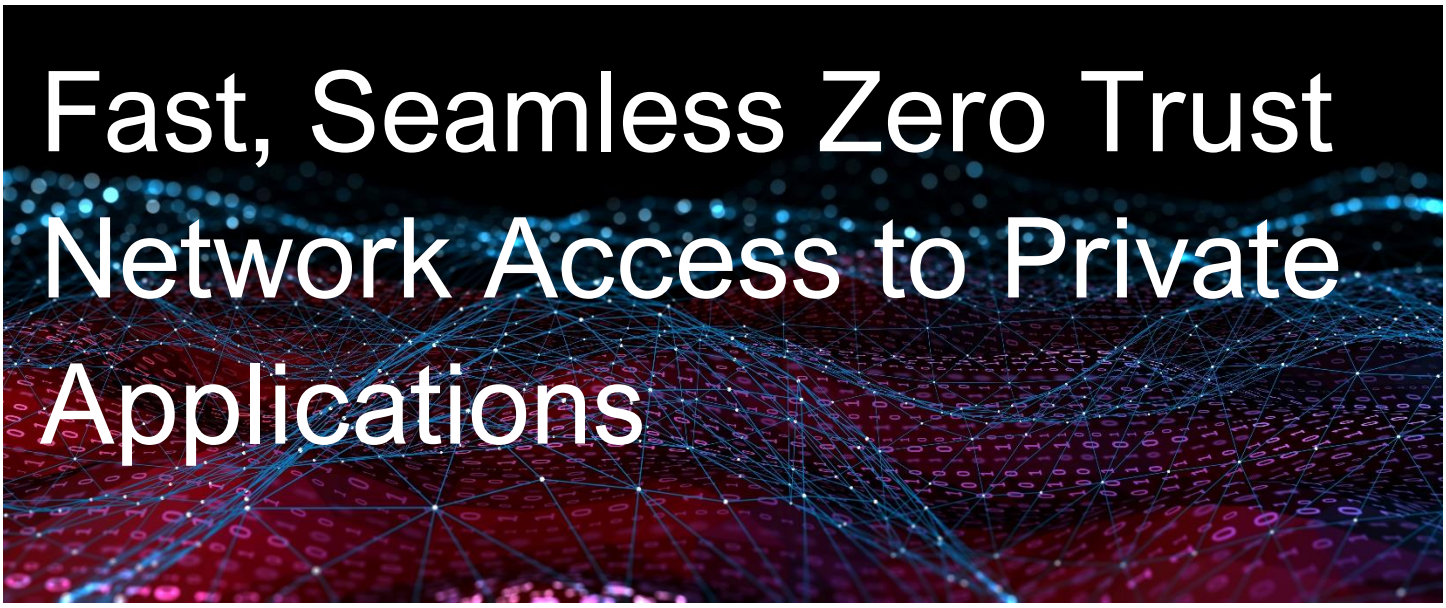
CATEGORY: Solutions Brief

Fast, Seamless Zero Trust Network Access to Private Applications



Solution: Secure Access Services Edge (SASE) ▪ **Industry**: Any vertical ▪ **Use Case**: Secure Private Access

Secure Private Access (SPA) from Exium provides fast, seamless way of accessing private applications without the clunkiness of VPN infrastructure. SPA is a cloud-based Software Defined Perimeter (SDP) or Zero Trust Network Access (ZTNA) solution that is delivered through Exium's Intelligent Cybersecurity Mesh.

Legacy networking and security approaches fail the needs of today's hybrid workforce. Connecting users to private apps shouldn't be slow, complicated, or risky. Hybrid work and cloud transformation have upended perimeter-based network security models, with private applications moving to the cloud, and users accessing applications over the public internet, on any device, from any location. Traditional approaches that rely on legacy VPNs and firewalls to control application access have become ineffective in the cloud and mobile-first world.

What is ZTNA?

Zero Trust Network Access (ZTNA) is the modern remote access solution built on the principle of Zero Trust. ZTNA provides streamlined and secure access to private resources hosted in data centers and public cloud environments. Authenticated users gain direct access only to authorized applications, not the underlying network.

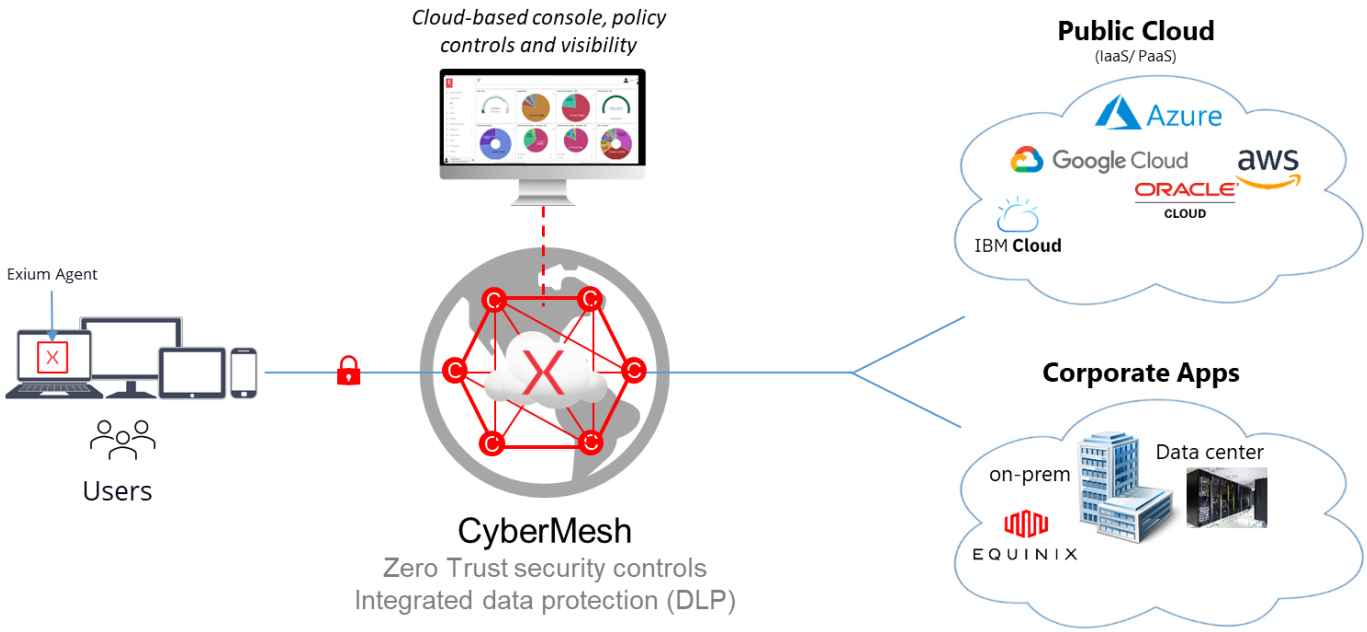
> *"By 2025, at least 70% of new remote access deployments will be served predominantly by zero trust network access (ZTNA) as opposed to VPN services."*
>
> **Gartner®, Emerging Technologies: Adoption Growth Insights for Zero Trust Network Access**

Exium Secure Private Access

Exium Secure Private Access ensures zero trust security for remote employees connecting to your internal network from any device, at any time, and from anywhere.

Even with the trend toward higher cloud and SaaS adoption, organizations still have a variety of private applications that need the same level of secure and reliable access control. Regardless of whether these applications are hosted in the data center or at a third-party cloud provider, many of the same cybersecurity threats exist since employees are still connecting through a variety of personal and company-issued devices.

Traditional virtual private network (VPN) solutions lack the granular access control required for a zero-trust security model. VPNs, for example, have no way of knowing whether the device authenticating to the network is in the hands of the right individual. Stolen credentials can grant access to the network and deliver a malicious payload weeks and months before ever being noticed. This can easily compromise the entire business.



Exium SPA overcomes this by providing Zero Trust Network Access (ZTNA) capabilities to provide secure remote access to internal private applications, regardless of whether they are hosted by a public cloud service provider or in your organization's private data center.

With all traffic directed through a fully encrypted tunnel, your private applications are never exposed to the public internet. This, combined with its granular zero trust capabilities, ensures a higher level of security for remote employees connecting to your internal private network.

How It Works?

Adjacent to the internal applications running in a public cloud, data center, or on-premise server, SPA places a small piece of software called Cyber Gateway (CGW), deployed as a container or a VM, which is used to extend a highly secure Zero Trust Path out to the Intelligent Cybersecurity Mesh.

The CGW establishes an outbound connection, and does not receive any inbound connection requests, thereby preventing DDoS and other cyberattacks. Private Access utilizes a lightweight Exium Client installed on a Microsoft Windows, Apple macOS, iOS, Android or a Linux device. The Exium Client steers Private Access application traffic to the Exium Intelligent Cybersecurity Mesh using either DNS or the IP address.

Moreover, within Exium service, both the user devices and the CGW use battle-tested hardware root-of-trust eliminating credential theft and man-in-the-middle attacks. A Mesh Cybernode approves access and stitches together the user-to-application session. SPA is 100 percent software defined, so it requires no appliances and allows users to benefit from the cloud

and mobility while maintaining the security of their applications.

SPA provides zero trust, secure remote access to internal applications running in public cloud environments or private data centers, reducing risk and simplifying security operations. With SPA, applications are never exposed to the internet, making them inaccessible to unauthorized users.

ZTNA Benefits and Capabilities

Zero Trust Access: ZTNA provides access to private applications, not the network. With granular application-level access control policies, trust is granted based on user identity, group membership, and the security posture of the devices.

Reduce Attack Surface: Minimize the attack surface and eliminate lateral movement by making applications invisible to attackers and unauthorized users while enforcing least-privileged access.

Enforce least-privileged access: Application access is determined by identity and context— not an IP address—and users are never put on the network for access

Enhanced User Experience: Connecting users directly to private apps eliminates slow, costly backhauling over legacy VPNs while continuously monitoring and proactively resolving user-experience issues.

Boost hybrid workforce productivity: Fast, seamless access to private apps whether you're at home, in the office, or anywhere.

Why Exium Zero Trust Secure Private Access?

Exium's Intelligent CyberSecurity Mesh, which runs our SPA service, is built on 5G technology. This gives our cloud security services advantages over legacy providers that built their tech years ago.

SPA applies the principles of least privilege to give users secure, direct connectivity to private applications running on-prem or in the public cloud while eliminating unauthorized access and lateral movement. As a cloud-native service built on a holistic secure access services edge (SASE) framework, SPA can be deployed in a matter of minutes to replace legacy VPNs and remote access tools.

> *"The continued proliferation of advanced threats such as ransomware is a disruptive problem for organizations of all sizes. We were looking for a solution where security is built in, not bolted on. The Exium SASE solution is really attractive as it provides the most advanced identity-based access with tightly integrated networking to deliver the greatest performance and security while also improving operational efficiency and lowering costs."*
>
> **Director of IT Security Architecture, Fortune 500 Company in the Retail Industry**

Below are SPA key features and benefits:

Superior User Experience through an integrated 5G acceleration & QoS and a single-pass networking + security architecture. Most legacy providers deliver security and networking using separate offerings that are bolted together.

Robust Security that leverages the 5G trust model and hardware root of trust. 5G has evolved over generations of mobile technology. Mobile tech runs billions of devices globally and is battle tested by industry, carriers, and governments to make it secure. The trust model (how encryption keys are exchanged) is open to auditing and has undergone more scrutiny than any proprietary, closed model from legacy security providers. With 5G, encryption keys are protected in the hardware root of trust (similar to how Apple protects credit card info on devices) making them much more difficult to steal than how competitors store them in software. 5G security is simply better.

Protect Data and Mitigate Insider Risk by detecting data usage, activities, and behavior anomalies (UEBA),

enforce advanced DLP rules and policies, and apply adoptive access policy based on user risks.

Simplify Operations by leveraging the CyberMesh SASE platform that unifies ZTNA, CASB, SWG, and Cloud Firewall with one client, one policy engine, and a single management console, providing consistent policy enforcement, ease of management, and visibility. Cloud-native platform eliminates legacy VPNs that are difficult to scale, manage, and configure.

Instant Deployment and Discovery by automatically discover applications so you can easily build policies around them.

Single Sign-On (SSO) – SPA can be tied directly to your existing authentication infrastructure, leveraging SSO to further reduce complexity.

Real-Time Visibility via dashboards that provide unparalleled visibility into your users and applications, and the health of your organization's applications and servers

SPA gives Workspace admins control over applications and the users authorized to access them. Workspace admins create and manage policies for users, user groups, applications, and application groups within Exium Admin Console.

SPA allows an organization to phase out legacy VPN hardware, and move towards a more secure, cloud-first, remote access architecture. End the high capital investment, refresh cycles, and ongoing management costs of VPN appliances. SPA drastically reduces the complexity of network and security architectures, accelerating cloud adoption. With SPA, User access is based on policies created by the workspace admin within the Exium Admin Console resulting in a simple, secure, and effective way to access internal applications.

Top Use Cases	
Security Transformation	Zero Trust Network Access (ZTNA) that connects authenticated users to authorized applications, not the underlying network.
Phase out legacy VPN hardware	Phase out legacy VPN hardware, and move towards a more secure, cloud-first, remote access architecture. End the high capital investment, refresh cycles, and ongoing management costs of VPN appliances.
Enhanced Digital Experience	Deliver an enhanced digital experience for accessing applications in public clouds, on-prem, and data center environments
Limit Private Apps Exposure	Provide employees with remote access to apps in the public cloud without needing to expose them publicly
Support Hybrid Cloud	Deliver a seamless end-user experience for accessing applications in private data centers and public cloud environments.
DevOps Access	Native access to resources hosted in the virtual private cloud (VPC) environments.
M&A Integration	Provide day-one access to internal resources without the complexity of combining networks.

EXIUM

Ready to secure access to your Internal Apps?

Test Drive Here