**CATEGORY**: Solutions Brief

# AI-Powered Secure Access & Digital Experience for SaaS and Internet

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

**As companies embrace digital transformation, the old model of data center based perimeter security no longer works. More and more applications are in the cloud and users work from anywhere. Securing modern users and apps requires a modern cloud security solution.**

The digital transformation to cloud and mobile is inverting the legacy appliance-based security stack to the cloud to better protect an increasing base of remote workers. Legacy security appliances located in offices force traffic hair-pinning with VPNs to central data centers which is no longer sufficient and results in a poor user experience.

Business units and users continue to freely adopt new apps and cloud services, where the average company with 500-2000 users accesses 805 distinct apps. Legacy security solutions are mostly blind to these growing shadow IT apps and cloud services and less than 3% are managed by IT. All stages of the cyber kill chain are now cloud-enabled, including reconnaissance, weaponization, delivery, and call back communications.

## Secure Internet Access

Securing today's cloud- and mobile-first enterprise requires a fundamentally different approach built on zero trust. Exium Secure Internet Access (SIA) is a secure internet and web gateway delivered as a service from the cloud. Think of it as a secure internet onramp—all you do is make Exium your next hop to the internet. No matter where users connect—a coffee shop in London, a hotel in Tokyo, or the office—they get identical protection.

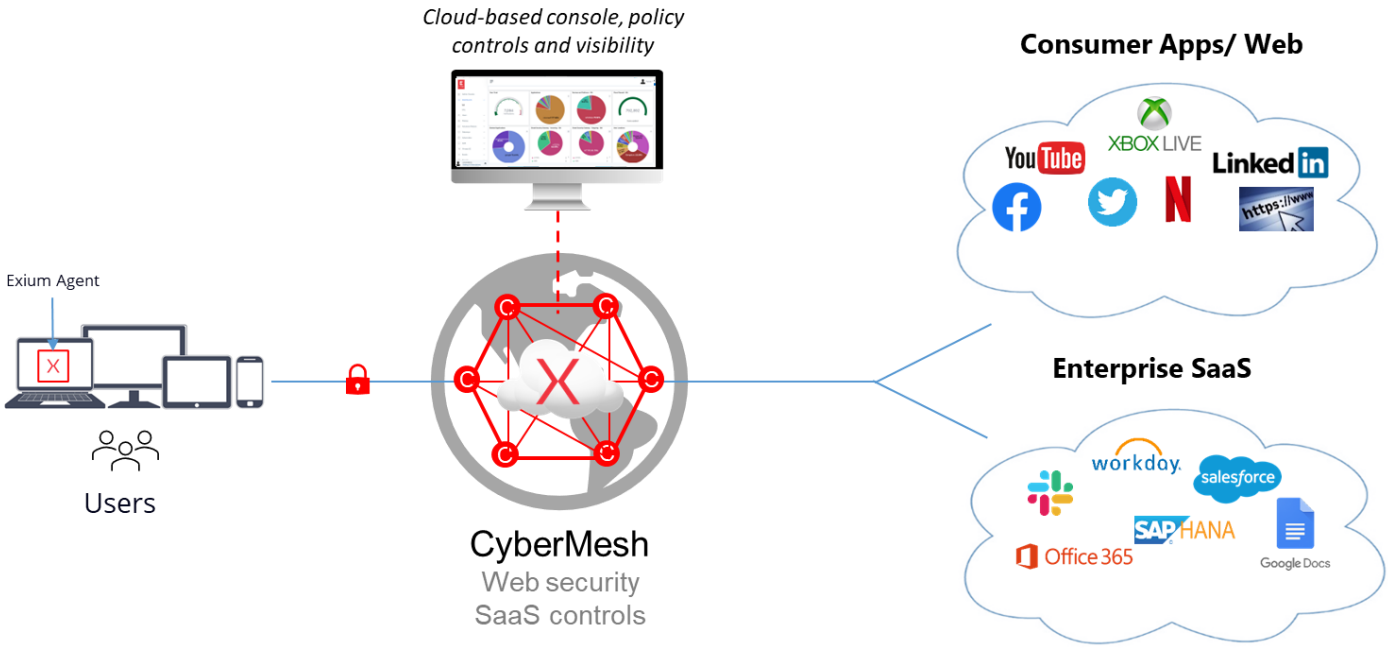
> *"More than half of web traffic today is related to apps and cloud services, and more than two-thirds of malware is delivered from cloud apps versus the web. Legacy web proxy gateways cannot decode apps and cloud services to detect these cloud delivered threats."*

Exium SIA uses the latest 5G networking and security technology to deliver a malware-free internet experience for your users. Internet security is essential and when it is coupled with an outstanding user experience it makes things a lot easier for both users and the company.

The trend in work-from-anywhere and BYOD policies means your employees are connecting to trusted and untrusted websites and SaaS applications around the clock. Using personal devices to access these third-party web services puts your corporate data and organization at considerable risk.

With Exium Secure Internet Access, employees can safely connect to SaaS apps, click on web links, and open email attachments without the fear of infecting their devices. Our Intelligent Cybersecurity Mesh or CyberMesh lets you embrace the cloud with the confidence you need to keep your distributed workforce secure wherever they are.

Unlike traditional solutions that require integrating separate point products, Exium SIA combines the best of secure web gateways, intrusion detection and prevention services, DNS, and CASB offerings into a single, easy-to-use, and cost-effective cloud-based service.




# How It Works

Secure Internet Access sits between your users and the internet, inspecting every nibble (half-byte) of traffic inline across multiple security techniques. You get full protection from web and internet threats on a cloud platform that supports Zero-Trust network access, Next Gen Cloud Firewall, Content/ URL Filtering, DNS security, Cloud Access Security Broker (CASB), Distributed Denial of Service (DDoS) mitigation, Man-in-the-middle (MiTM) attacks protection, and Data Loss Prevention (DLP).

Secure Internet Access utilizes a lightweight Exium Client installed on a Microsoft Windows, Apple macOS, iOS, Android or a Linux device. The Exium Client steers application traffic to the Exium Intelligent Cybersecurity Mesh using either DNS or the IP address.

Exium provides a globally available, cloud-based security platform for securing remote workers' access to websites and cloud applications. Exium has the unique ability to perform AI-powered Deep Packet Inspection (DPI) on SaaS/ cloud applications and website traffic to understand remote workers' activities, inspect data movement, and detect and stop threats.

Secure Internet Access 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.

With the use of CyberMesh, you can monitor behavior for web, apps and cloud services, set granular acceptable use policies, invoke adaptive policies based on app risk, user risk, activity, and data sensitivity, and provide real-time user coaching to safer alternatives and away from risky apps. Not only does this improve your security in the cloud, but it also improves user experiences by avoiding blanket bans on certain actions and devices. Granular controls and inline visibility delivered by CyberMesh helps contextualize user and data activity so adaptive policies can guide users while reducing risk and protecting data without interfering with legitimate work practices.

CyberMesh decodes thousands of apps and cloud services alongside web traffic to understand content and context for data and threat protection defenses. The new language is APIs built around JSON for apps, cloud services, and web sites. CyberMesh understands user, device, location, app, risk, instance, content, and activity for contextual policy controls, plus collecting rich metadata for analytics, investigations and machine learning.

## Why Exium Secure Internet Access

Exium's CyberMesh, which runs our SIA service, leverages 5G technology and is built on true cloud architecture. This gives our cloud security services advantages over legacy providers that built their tech years ago.

Delivered as a scalable SaaS platform from the world's largest security cloud, it eliminates legacy network security solutions to stop advanced attacks and prevent data loss with a comprehensive zero trust approach, offering:

**Best-in-class, consistent security for today's hybrid workforce**: When you move security to the cloud, all users, apps, devices, and locations get always-on threat protection based on identity and context. Your security policy goes everywhere your users go.

Furthermore, CyberMesh leverages the 5G trust model and hardware root of trust to deliver hardened security. 5G has evolved over generations of mobile technology. Mobile tech runs billions of device 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.

> *"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**

**Enhanced digital experience with zero infrastructure**: Direct-to-cloud architecture ensures a fast, seamless user experience. This eliminates backhauling, improves performance and user experience, and simplifies network administration—with no physical infrastructure, ever.

CyberMesh delivers Enhanced user experience through an integrated 5G acceleration & QoS and a single-pass networking + security architecture. 5G is all about speed and the digital experience. Most legacy providers deliver security and networking using separate offerings that are bolted together.

**Keeps pace with new attacks.** CyberMesh addresses a wide array of new and emerging threats, including cloud-enabled threats such as cloud phishing, cloud payload delivery, and callback communications. This requires the systematic advantage of decoding

apps and cloud services for content and context for advanced threat and data protection defenses, plus machine learning.

Cloud-enabled threats leverage trusted domains with valid certificates either passing through legacy defenses or being allow-listed to bypass defenses. Users can maliciously or accidentally transfer data between company and personal instances, or be phished for access credentials in these legacy environments.

**Leverages true cloud architecture performance and scale.** The CyberMesh solution is built around cloud-native microservices with fully integrated capabilities, not cloud-hosted separate legacy solutions, for true cloud performance and scale. Also, using a carrier grade private network optimized for access leveraging peering relationships with global and local cloud service providers is essential for worldwide availability and performance.

## Integrated, AI-powered security and data protection

Secure Internet Access includes a comprehensive suite of AI-powered security and data protection services to help you stop cyberattacks and data loss. As a fully cloud-delivered SaaS solution, you can add new capabilities without any additional hardware or lengthy deployment cycles. The top features and capabilities of Exium Secure Internet Access are:

| Top Features and Capabilities of Exium Secure Internet Access (SIA) | |
|---|---|
| ***Secure Access*** | Provide remote users with secure access to SaaS, cloud apps and web |
| ***Monitor and assesses individual actions*** | Achieve inline visibility for thousands of managed and unmanaged apps and cloud services, plus web traffic, and unify SWG+CASB+DLP critical capabilities into one platform. |
| ***Digital Experience Monitoring*** | Reduce IT operational overhead and speed up ticket resolution with a unified view of application, cloud path, and endpoint performance metrics for analysis and troubleshooting. Deliver an enhanced digital experience for accessing SaaS, cloud, and web applications with cloud edge-based network infrastructure, optimized for low latency and high capacity worldwide. Enforce bandwidth policies and prioritize business critical applications over recreational traffic. |
| ***Protection of data everywhere, Data Loss Prevention (DLP)*** | Follow and protect data everywhere it goes and ensure accurate and precise inspection with advanced measures like exact data match (EDM), fingerprinting, optical character recognition (OCR), and machine learning. |
| ***Cloud Secure Web Gateway (SWG), Content/ URL filtering*** | Block or limit website access by identifying malicious sites and automatically preventing web-based attacks.<br>Deliver a safe, fast web experience that eliminates ransomware, malware, and other advanced attacks with real-time, AI-powered analysis and content/ URL filtering. |
| ***Implementation of acceptable use policies*** | Incorporate a combination of traditional web filtering covering URL categories, custom categories, and dynamic page ratings for new sites with comprehensive cloud app usage ratings, risks, and acceptable use policies that cover both cloud and web. |

| | |
|---|---|
| ***DNS Security*** | Detect and block DNS queries against known and malicious destinations, data exfiltration attempts or DNS tunneling. |
| ***Cloud Access Security Broker (CASB)*** | Secure cloud apps with integrated CASB to protect data, stop threats, and ensure compliance across your SaaS and IaaS environments. Discover and control unknown cloud apps with Inline CASB. Prevent data exposure and ensure SaaS compliance. |
| ***Protection against threats*** | Protect against web and cloud-delivered malware and advanced threats including, ransomware, phishing, denial of service, and botnet infections in one easy to use cloud service. |
| ***Privacy and anonymity*** | Privacy and anonymity by masking your internet protocol (IP) address. |
| ***Granular control over applications*** | Get real-time, granular control of thousands of cloud apps including the shadow IT ones led by lines of business and users vs. IT. This enables you to stop the bad stuff from happening and safely enable the good. |
| ***Cloud Firewall & IPS*** | Extend industry-leading protection to all ports and protocols, and replace edge and branch firewalls with a cloud native platform. |

# Ready to secure SaaS and Web for your Hybrid Workforce?

Test Drive Here