AKAMAI SOLUTION BRIEF

Akamai Enterprise Application Access & Secure Enterprise Browser

Traditional Secure Service Edge (SSE) solutions promise comprehensive security but often result in fragmented protection, operational complexity, and user friction that hamper productivity. Organizations find themselves managing extensive policy frameworks and proxy performance bottlenecks while struggling to effectively protect against sophisticated web-based threats.

Akamai Enterprise Application Access and Secure Enterprise Browser

The combination of Akamai Enterprise Application Access and Secure Enterprise Browser, powered by Seraphic, address the most critical SSE use cases — secure application access, web security, and data protection — with a focused, high-performance approach. This combination delivers Zero Trust Network Access (ZTNA) for private enterprise applications plus advanced browser security for SaaS applications and internet access, providing robust protection without the coverage gaps of traditional platforms.

By focusing on core security requirements, rather than attempting to be everything to everyone, this solution delivers superior performance, reduced complexity, and lower total cost of ownership.

Key features and capabilities

Secure access (ZTNA for private applications)

- **Private application access control**, replacing broad network access with granular, identity-based permissions for enterprise applications.
- **Dynamic policy enforcement** based on user identity, device posture, and real-time risk assessment.
- **Identity provider integration**, supporting existing enterprise identity frameworks for seamless private application access.
- **Data loss prevention** with real-time content analysis and policy enforcement for private applications.
- **Multicloud private application support** provides secure access to internal applications across hybrid and cloud native environments.

Benefits for your business

Achieve better SSE outcomes with focused solutions that excel at specific use cases rather than compromise across multiple security domains, delivering superior performance for application access, browser security, and modern data protection challenges for managed and unmanaged devices.

Control data sharing through generative AI tools with real-time visibility and data policy enforcement for ChatGPT, Copilot, and similar platforms, enabling productivity while protecting intellectual property and meeting compliance requirements.

Accelerate time-to-value with simplified deployment and management, compared to full SSE implementations, while still addressing the core use cases that drive most SSE initiatives, including emerging governance requirements.

Minimize user friction by leveraging any existing browser rather than forcing users to adapt to new interfaces, specialized browsers, or degraded application performance common with traditional SSE platforms.

Reduce SSE complexity and costs by delivering core secure access and web security capabilities through a streamlined architecture that eliminates the need for comprehensive SSE platform licensing, extensive professional services, and ongoing management complexity.

- **Clientless and client-based access** supporting diverse user scenarios without VPN complexity.
- **Performance-optimized delivery** through Akamai's global edge infrastructure.

Web security & data protection (SaaS and internet access)

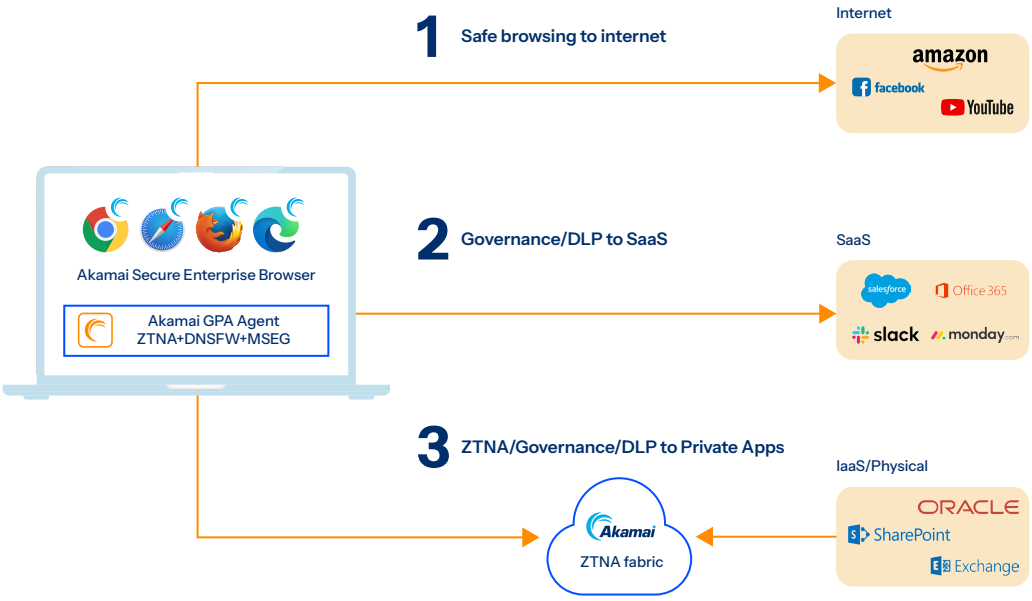
- **SaaS application access control** with device posture-based policy enforcement for cloud applications.
- **Advanced threat prevention**, stopping zero-day exploits and sophisticated web-based and identity-focused attacks without detection lag.
- **Comprehensive data loss prevention** with real-time content analysis, sensitive data masking, and policy enforcement across SaaS applications, web browsing, and AI LLMs.
- **Browser-agnostic security**, transforming any browser into an enterprise-grade secure browser for internet and SaaS access.
- **Session-level protection**, including identity security and encrypted session management.
- **SaaS application security** extends protection to modern collaboration tools like Slack, Teams, and other cloud applications.

SSE replacement capabilities

- **Direct SaaS and web protection**, eliminating the need for separate CASB solutions.
- **Integrated threat prevention**, replacing secure web gateway functionality.
- **Browser-native security**, delivering remote browser isolation benefits without performance overhead.

Streamlined SSE architecture

Rather than implementing an inflexible SSE platform, this solution delivers SSE outcomes through two optimized components that work seamlessly together.



Edge-delivered network security: Zero Trust access to private enterprise applications, delivered from Akamai Connected Cloud, eliminates the network security gaps that SSE solutions address, while providing superior performance through globally distributed points of presence. This replaces the secure web gateway and ZTNA components of traditional SSE for internal application access.

Browser-level data protection: Advanced browser security provides comprehensive protection for SaaS applications and internet access, delivering superior data loss prevention and web security directly at the point of user interaction. By securing the browser, where users access both sanctioned SaaS applications and general internet content, this approach eliminates the need for traditional CASB, SWG, and RBI solutions while providing better performance and user experience.

This architecture delivers the core values of SSE — secure access, web protection, and data security — while eliminating common SSE challenges like backhauling traffic, performance degradation, and complex policy management.

To find out more about Akamai Enterprise Application Access and Secure Enterprise Browser, powered by Seraphic, contact your Akamai representative or email sales@akamai.com.