AKAMAI-LÖSUNGSÜBERBLICK

Akamai Enterprise Application Access und Secure Enterprise Browser

Herkömmliche SSE-Lösungen (Secure Service Edge) versprechen umfassende Sicherheit, führen aber häufig zu fragmentiertem Schutz, komplexen Betriebsabläufen und umständlichen Nutzererlebnissen, die die Produktivität beeinträchtigen. Unternehmen müssen umfangreiche Richtlinien-Frameworks verwalten und Engpässe bei der Proxy-Performance bewältigen und haben bei alldem auch noch mit dem effektiven Schutz vor komplexen webbasierten Bedrohungen zu kämpfen.

Akamai Enterprise Application Access und Secure Enterprise Browser

Die Kombination aus Akamai Enterprise Application Access und Secure Enterprise Browser (powered by Seraphic) bietet einen fokussierten, leistungsstarken Ansatz, um die wichtigsten SSE-Anwendungsfälle zu unterstützen: sicheren Anwendungszugriff, Websicherheit und Datenschutz. Diese Kombination bietet Zero Trust Network Access (ZTNA) für private Unternehmensanwendungen sowie erweiterte Browsersicherheit für SaaS-Anwendungen und Internetzugriff – so ermöglicht sie zuverlässigen Schutz ohne die unvollständige Abdeckung herkömmlicher Plattformen.

Indem sich diese Lösung auf die zentralen Sicherheitsanforderungen konzentriert – anstatt zu versuchen, sämtliche Funktionen für jeden Anwendungsfall zu bedienen –, bietet sie überragende Performance, weniger Komplexität und geringere Gesamtbetriebskosten.

Wichtige Merkmale und Funktionen

Sicherer Zugriff (ZTNA für private Anwendungen)

- **Zugriffskontrolle für private Anwendungen**, die den breiten Netzwerkzugriff durch präzise, identitätsbasierte Berechtigungen für Unternehmensanwendungen ersetzen
- **Dynamische Richtliniendurchsetzung** basierend auf Nutzeridentität, Gerätestatus und Echtzeit-Risikobewertung
- **Integration von Identitätsanbietern**, um vorhandene Identitäts-Frameworks zu unterstützen und einen nahtlosen Zugriff auf private Anwendungen zu gewährleisten
- **Verhinderung von Datenverlust** (Data Loss Prevention) durch Echtzeit-Inhaltsanalyse und Durchsetzung von Richtlinien für private Anwendungen
- **Unterstützung privater Multicloud-Anwendungen** für sicheren Zugriff auf interne Anwendungen in hybriden und cloudnativen Umgebungen

Vorteile für Ihr Unternehmen

Erzielen Sie bessere SSE-Ergebnisse mit fokussierten Lösungen, die in bestimmten Anwendungsfällen glänzen, anstatt Kompromisse in mehreren Sicherheitsbereichen einzugehen. So erhalten Sie überragende Performance für Anwendungszugriff und Browsersicherheit und können die modernen Herausforderungen beim Datenschutz für verwaltete und nicht-verwaltete Geräte meistern.

Kontrollieren Sie die Datenweitergabe durch GenKI-Tools mit Echtzeittransparenz und -durchsetzung von Datenrichtlinien für ChatGPT, CoPilot und ähnliche Plattformen. So können Sie die Produktivität fördern, aber dabei Ihr geistiges Eigentum schützen und Compliance-Anforderungen erfüllen.

Beschleunigen Sie die Amortisierung mit vereinfachter Bereitstellung und Verwaltung im Vergleich zu vollständigen SSE-Implementierungen. Decken Sie dabei weiterhin die wichtigsten Anwendungsfälle ab, die die meisten SSE-Initiativen vorantreiben, darunter beispielsweise neue Governance-Anforderungen.

Optimieren Sie das Nutzererlebnis, indem Sie vorhandene Browser nutzen, anstatt Nutzer dazu zu zwingen, sich an neue Oberflächen, spezielle Browser oder eine verminderte Anwendungsperformance zu gewöhnen, wie es bei herkömmlichen SSE-Plattformen üblich ist.

Verringern Sie SEE-Komplexität und -Kosten, indem Sie zentrale Funktionen für sicheren Zugriff und Websicherheit über eine optimierte Architektur bereitstellen. So entfällt die Notwendigkeit einer umfassenden SSE-Plattformlizenzierung, umfassender Professional Services und einer kontinuierlichen, komplexen Verwaltung.

- **Clientloser und clientbasierter Zugriff**, der verschiedene Nutzerszenarien ohne die Komplexität eines VPN unterstützt
- **Performanceoptimierte Bereitstellung** über die globale Edge-Infrastruktur von Akamai

Internetsicherheit und Datenschutz (SaaS und Internetzugang)

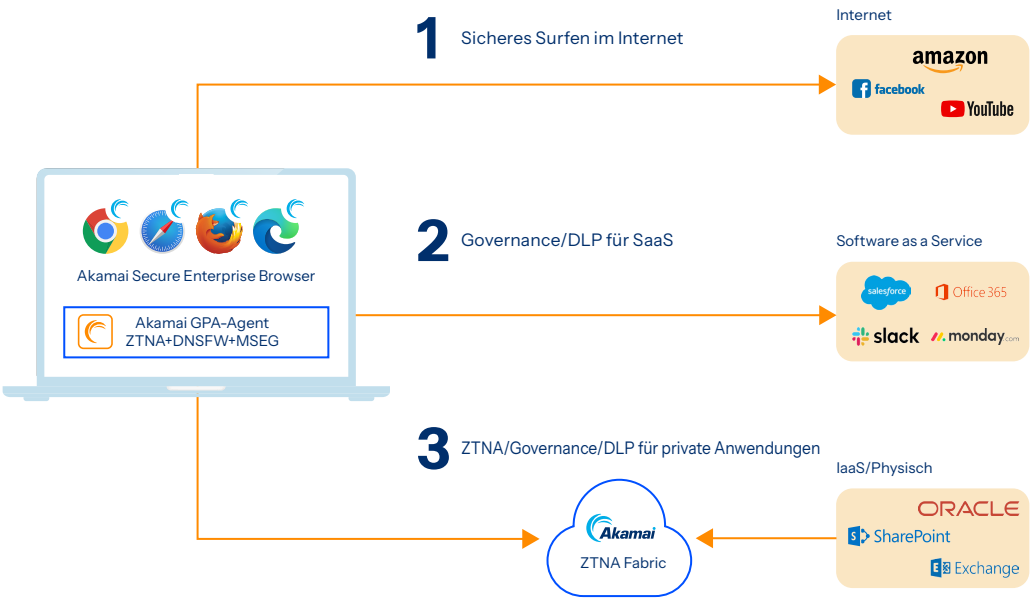
- **Zugriffskontrolle für SaaS-Anwendungen** mit gerätebasierter Richtliniendurchsetzung für Cloudanwendungen
- **Erweiterte Bedrohungsabwehr** zur verzögerungsfreien Erkennung von Zero-Day-Exploits und ausgeklügelten, webbasierten und identitätsbasierten Angriffen
- **Umfassende Data Loss Prevention** mit Echtzeit-Inhaltsanalyse, Datenmaskierung und Richtliniendurchsetzung über SaaS-Anwendungen, Webbrowsing und KI-LLMs hinweg
- **Browserunabhängige Sicherheit**, die jeden beliebigen Browser in einen sicheren Browser der Enterprise-Klasse für Internet- und SaaS-Zugriff verwandelt
- **Schutz auf Sitzungsebene**, einschließlich Identitätssicherheit und verschlüsselter Sitzungsverwaltung.
- **SaaS-Anwendungssicherheit** erweitert den Schutz auf moderne Tools zur Zusammenarbeit wie Slack, Teams und andere Cloudanwendungen.

Funktionen zum Ersetzen von SSE

- **Direkter SaaS- und Webschutz**, sodass keine separaten CASB-Lösungen erforderlich sind
- **Integrierte Bedrohungsabwehr**, die die SWG-Funktion (Secure Web Gateway) ersetzt
- **Browsernative Sicherheit**, die die Vorteile einer Remote-Browser-Isolierung bietet, ohne die Performance zu beeinträchtigen

Optimierte SSE-Architektur

Anstatt eine unflexible SSE-Plattform zu implementieren, erzielen Sie mit dieser Lösung überzeugende SSE-Ergebnisse, und zwar durch zwei optimierte Komponenten, die nahtlos zusammenarbeiten.



Netzwerksicherheit direkt an der Edge: Der Zero-Trust-Zugriff auf private Unternehmensanwendungen, die über die Akamai Connected Cloud bereitgestellt werden, beseitigt nicht nur die Netzwerksicherheitslücken, die SSE-Lösungen abdecken sollen, sondern bietet auch eine überragende Performance über global verteilte Points of Presence. Hierdurch werden die SWG- und ZTNA-Komponenten herkömmlicher SSE für den internen Anwendungszugriff ersetzt.

Datenschutz auf Browser-Ebene: Die erweiterte Browsersicherheit bietet umfassenden Schutz für SaaS-Anwendungen und Internetzugang, mit hervorragender Data Loss Prevention und Websicherheit direkt am Punkt der Nutzerinteraktion. Indem die Lösung den Browser schützt, über den Nutzer auf genehmigte SaaS-Anwendungen und allgemeine Internetinhalte zugreifen, entfällt nicht nur der Bedarf an herkömmlichen CASB-, SWG- und RBI-Lösungen, sondern es werden auch Performance und Nutzererlebnis verbessert.

Diese Architektur liefert die Kernwerte von SSE – sicheren Zugriff, Websicherheit und Datensicherheit – und beseitigt dabei gängige SSE-Herausforderungen wie Traffic-Backhaul, Performanceprobleme und komplexes Richtlinienmanagement.

Wenn Sie mehr über Akamai Enterprise Application Access und Secure Enterprise Browser (powered by Seraphic) erfahren möchten, wenden Sie sich an Ihren Akamai-Ansprechpartner oder senden Sie eine E-Mail an sales@akamai.com.