Akamai-Lösungsüberblick

Akamai Workforce Protector (zuvor LayerX)

Schützen Sie Menschen und KI-Agenten im Browser

Unsere Arbeitsumgebung hat sich verändert

Die Arbeit hat sich auf die Interaktionsebene verlagert und damit die herkömmlichen Sicherheitsmodelle grundlegend durchbrochen. Da Unternehmen KI-Tools, Copiloten und webbasierte Workflows schnell einführen, wächst die Bedrohungslage für Unternehmen schneller als je zuvor. Laut Forrester findet mehr als 70 % der Unternehmensarbeit in einem Browser statt,[1] da Mitarbeiter häufig geschäftskritische Aufgaben in verschlüsselten Browsersitzungen ausführen, auf SaaS-Anwendungen zugreifen, sensible Daten in öffentliche KI-Chatbots einfügen und Erweiterungen von Drittanbietern installieren. Da diese Aktivität am Interaktionspunkt stattfindet, lange bevor Daten das Netzwerk erreichen, können herkömmliche Proxys und ältere DLP-Tools (Data Loss Prevention) sie nicht sehen. Durch diese zunehmende Lücke haben Unternehmen keinen Einblick in ihre wichtigsten Schwachstellen, sodass sie die Risiken von Shadow-KI (oder auch das vollständige Blockieren von KI-Interaktionen) sowie Compliance-Verstöße und Datenlecks ohne einen zuverlässigen Kontrollpunkt, an dem die Arbeit tatsächlich stattfindet, bewältigen müssen.

Das Problem: Warum sicherer Zugriff schwieriger ist, als es scheint

Der tote Winkel in der Sitzung

Arbeit hat sich in KI-Tools, SaaS-Anwendungen und Webumgebungen verlagert, in denen Nutzer und KI-Agenten in Echtzeit mit sensiblen Daten interagieren. Veraltete Sicherheitsarchitekturen wurden nicht für diese Änderung konzipiert. Netzwerkkontrollen, vorhandene SASE-Tools (Secure Access Service Edge) und SSE-Tools (Security Service Edge) können den verschlüsselten, dynamischen Anwendungstraffic nicht effektiv prüfen, und Endpunkttools bieten keine detaillierte Einsicht in das Nutzerverhalten. Dadurch entsteht ein massiver toter Winkel während der Sitzung. Herkömmliche DLP- und Proxys können kritische Interaktionen nicht erkennen, wie z. B. Kopieren und Einfügen, Screenshots, Dateiübertragungen und Texteingaben, da sie im Browser auftreten, lange bevor die Daten das Netzwerk erreichen.

Das zunehmende Risiko von Shadow-KI

Die Einführung von KI beschleunigt sich schneller als die Einführung von Governance-Funktionen. Mitarbeiter nutzen zunehmend nicht genehmigte generative KI-Tools, browserbasierte LLMs und eingebettete KI-Assistenten in SaaS-Anwendungen. Da diese „Shadow-KI"-Aktivität für herkömmliche Sicherheitskontrollen unsichtbar ist, fügen Mitarbeiter häufig proprietären Quellcode, Kundendatensätze und interne Dokumente direkt in nicht verwaltete KI-Systeme ein, was zu Risiken für Compliance und geistiges Eigentum führt.

Wichtige Merkmale

KI-Nutzungskontrolle
Sichern Sie jede Interaktion von Menschen und KI-Agenten. Wenden Sie Echtzeitrichtlinien an, um Eingaben, Antworten und Kopieren/Einfügen von Daten direkt am Interaktionspunkt zu kontrollieren.

Kontrolle der KI-Nutzung
Erkennen Sie Shadow-KI, eingebettete Widgets und nicht verwaltete agentische Workflows. Stellen Sie Ihre gesamte KI-Angriffsfläche dar, um eine konsistente Compliance im Unternehmen zu gewährleisten.

Zero-Trust-Browsersicherheit
Verwandeln Sie jeden kommerziellen Browser sicher in einen vollständig verwalteten Arbeitsbereich. Überprüfen Sie sofort die Identität und den Gerätestatus, um den Zugriff auf SaaS und private Anwendungen zu steuern, ohne dass ein Browserwechsel erforderlich ist.

Erweiterungs-Governance
Analysieren Sie automatisch Risikobewertungen, Berechtigungen und Verhalten, um schädliche Plug-ins von Drittanbietern mithilfe nativer ExtensionPedia-Intelligence sofort zu blockieren.

Data Loss Prevention
Setzen Sie den Schutz auf Sitzungsebene gegen unbefugte Datenbewegungen über SaaS, Web und private Anwendungen hinweg durch, wodurch Transparenzlücken am Netzwerkrand beseitigt werden.

[1] Forrester Research Inc., Digital Workplace And Employee Technology Survey, 2025, Mai 2025

Akamai Security

Die Herausforderung von Drittanbietern und BYOD

Moderne Arbeit findet außerhalb streng kontrollierter Unternehmensumgebungen statt, aber die meisten Sicherheitstools sind nach wie vor von verwalteten Geräten abhängig. Unternehmen haben Schwierigkeiten, einheitliche Sicherheitsrichtlinien durchzusetzen und den Zugriff Dritter für Auftragnehmer, Outsourcing-Anbieter von Geschäftsprozessen und BYOD-Nutzer (Bring Your Own Device) zu sichern. Die Sicherung dieser nicht verwalteten Geräte erfordert traditionell teure Bereitstellungen, die zu Belastungen und mehr Betriebsaufwand führen.

Die versteckte Bedrohung durch Browsererweiterungen

Wenn der Browser zur primären Arbeitsoberfläche wird, wird er auch zum primären Angriffsvektor. Browsererweiterungen von Drittanbietern stellen aufgrund ihrer erweiterten Berechtigungen und des Zugriffs auf Unternehmensidentitäten, Sitzungscookies und Nutzereingaben ein erhebliches und wachsendes Risiko dar. Eine kompromittierte oder überprivilegierte Erweiterung kann Tastenanschläge lesen, auf Unternehmensanwendungen zugreifen oder Daten nahtlos exportieren.

Der Lose-Lose-Kompromiss der aktuellen Tools

Unternehmen waren in der Vergangenheit zu einem Lose-Lose-Kompromiss gezwungen: Alte Netzwerksicherheitsplattformen bieten geringe Reibung, sind jedoch von kritischen Schwachstellen betroffen. Sie verlassen sich auf eine stumpfe „Zulassen“- oder „Blockieren“-Entscheidung, bei der Datenlecks am Interaktionspunkt übersehen werden. Im Gegensatz dazu bieten Full-Stack-Unternehmensbrowser eine bessere Transparenz, erfordern jedoch einen äußerst disruptiven Kompromiss: Unternehmen müssen die Tools, die ihre Mitarbeiter bereits verwenden, vollständig ersetzen. Dies führt zu massiven Hürden beim Änderungsmanagement, Bedenken hinsichtlich des Datenschutzes und einem hohen Widerstand der Endnutzer.

Die Lösung: Enterprise-Browser-Kontrolle. In jedem Browser.

Akamai Workforce Protector (früher LayerX) ist wegweisend für echte Interaktionssicherheit, indem eine reibungslose Browsererweiterung bereitgestellt wird, die jeden Browser sicher in einen vollständig verwalteten Arbeitsbereich verwandelt. Sie erhalten die umfassende Ende-zu-Ende-Sicherheit einer dedizierten Arbeitsplattform, ohne einen Browsertausch zu erzwingen oder das Nutzererlebnis zu beeinträchtigen.

KI-Nutzungskontrolle

Akamai Workforce Protector basiert auf dieser Grundlage eines sicheren Arbeitsbereichs und erweitert seine Echtzeittransparenz, um zu bestimmen, wie Mitarbeiter, KI-Agenten und Anbieter mit KI interagieren. Um die Einführung von KI sicher zu beschleunigen, benötigen Unternehmen Ende-zu-Ende-Governance für die Nutzung von KI. Workforce Protector führt eine umfassende Erkennung von Shadow-KI im gesamten Internet durch und erfasst vollständige KI-Gespräche. Er wendet die Echtzeit-KI-Datensicherheit auf Texteingaben, Dateianhänge und Kopier-/Einfügevorgänge direkt im Browser an. Workforce Protector überprüft und kontrolliert Daten genau zum Zeitpunkt der Eingabe in KI-Tools und verhindert so den Verlust geistigen Eigentums und Verstöße gegen gesetzliche Bestimmungen direkt an der Quelle.

Schutz der gesamten Arbeitsumgebung

Workforce Protector stellt den Browser als sicheren, unternehmensgesteuerten Arbeitsbereich für alle täglichen Aufgaben bereit. Er sichert die gesamte Interaktionsebene, indem er folgende Funktionen bereitstellt:

- **Browsernatives DLP:** Diese Funktion überwacht Daten nativ im Browser, ohne sich auf eine komplexe Netzwerkentschlüsselung verlassen zu müssen, wie z. B. Datei-Sandboxing, um sensible Uploads und Downloads zu isolieren und zu untersuchen.

- **Automatisierte Compliance:** Workforce Protector ermöglicht die automatisierte Durchsetzung von CIS-Benchmarks mit nur einem Klick für alle gängigen Browser und sorgt so für kontinuierliche Konfigurationskonformität.
- **Unterstützung für nicht verwaltete Geräte:** Für BYOD und Drittanbieter setzt die Erweiterung nahtlos schreibgeschützte Sitzungen und Wasserzeichen durch, ohne dass umfangreiche Bereitstellungen zur Geräteverwaltung erforderlich sind.
- **Eliminierung von Erweiterungsrisiken:** Eine native Erweiterungsrisikodatenbank analysiert automatisch Risikobewertung, Verhalten und Berechtigungen, um schädliche oder überprivilegierte Browser-Plug-ins von Drittanbietern sofort zu blockieren.

Übernehmen Sie die Kontrolle über Ihre Interaktionsebene

Zufriedene Nutzer. Zufriedenes Sicherheitsteam. Zufriedene IT.

Workforce Protector liefert sofort bei Bereitstellung messbare Vorteile bei Sicherheit und Architektur, indem er robuste Schutzmaßnahmen und gleichzeitig ein reibungsloses Endnutzererlebnis ermöglicht. Nutzer können ihre bevorzugten Browser und nativen Workflows beibehalten, ohne dass bei täglichen Aufgaben Performanceeinbußen oder Latenzen auftreten. IT- und Sicherheitsteams erreichen unübertroffene Wertschöpfung mit einer schnellen Bereitstellung, die kein komplexes Netzwerkrouting oder Ausfallzeiten, Hardware-Appliances oder Proxy-Konfigurationen erfordert.

Weitere Informationen darüber, wie Akamai Workforce Protector Ihre KI-Einführung sicher beschleunigen kann, ohne Ihren Betrieb zu beeinträchtigen, finden Sie unter akamai.com/akamai-workforce-protector.

© 2026 Akamai Technologies | Support |
| Veröffentlicht: Juli 2026