Akamai Solution Brief

Akamai Workforce Protector (Formerly LayerX)

Secure human and AI agent interactions in the browser

Our workspace has changed

Work has moved to the interaction layer, fundamentally breaking traditional security models. As organizations rapidly adopt AI tools, copilots, and web-based workflows, the enterprise threat surface is expanding faster than ever before. Per Forrester, more than 70% of corporate work occurs within a browser,[1] as employees frequently execute business-critical tasks inside encrypted browser sessions, accessing SaaS apps, pasting sensitive data into public AI chatbots, and installing third-party extensions. Because this activity happens at the point of interaction, long before data touches the network, traditional proxies and legacy data loss prevention (DLP) tools cannot see it. This widening gap leaves organizations with no visibility into their most critical vulnerabilities, forcing them to navigate the risks of shadow AI (or even to block AI interactions altogether), and face compliance violations and data leakage without a reliable control point where work actually happens.

The Problem: Why secure access is harder than it seems

The in-session blind spot

Work has moved into AI tools, SaaS applications, and web environments where users and AI agents interact with sensitive data in real time. Legacy security architectures were not designed for this shift. Network controls, existing secure access service edge (SASE) tools, and security service edge (SSE) tools cannot inspect encrypted, dynamic application traffic effectively, and endpoint tools lack granular visibility into user behavior. This creates a massive in-session blind spot. Traditional DLP and proxies cannot see critical interactions — like copy-and-paste activity, screenshots, file transfers, and text input, because they occur inside the browser, long before the data ever touches the network.

The accelerating risk of shadow AI

AI adoption is accelerating faster than governance capabilities. Employees increasingly turn to unapproved generative AI tools, browser-based LLMs, and embedded AI assistants inside SaaS apps. Because this “shadow AI” activity is invisible to traditional security controls, employees frequently paste proprietary source code, customer records, and internal documents directly into unmanaged AI systems, creating silent compliance and intellectual property risks.

Key features

AI usage control
Secure every interaction of humans and AI agents. Apply real-time guardrails to control prompts, responses, and data copy/paste exactly at the point of intent.

AI usage governance
Discover shadow AI, embedded widgets, and unmanaged agentic workflows. Map your complete AI attack surface to enforce consistent enterprise compliance.

Zero Trust browser security
Securely transform any browser into a managed workspace. Instantly verify identity and device posture to govern access to SaaS and private apps without forcing a browser swap.

Extension governance
Automatically analyze risk scores, permissions, and behaviors to instantly block malicious third-party plug-ins using native ExtensionPedia intelligence.

Data loss prevention
Enforce session-level protection against unauthorized data movement across SaaS, web, and private apps, eliminating the visibility gaps of network perimeters.

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

Akamai Security

The third-party and BYOD challenge

Modern work happens outside tightly controlled corporate environments, but most security tools still depend on managed devices. Organizations struggle to enforce consistent security policies and secure third-party access for contractors, business process outsourcers, and bring-your-own-device (BYOD) users. Securing these unmanaged devices has traditionally required expensive deployments, which introduce friction and operational overhead.

The hidden threat of browser extensions

As the browser becomes the primary work interface, it also becomes the primary attack vector. Third-party browser extensions pose a significant and growing risk due to their elevated permissions and access to corporate identities, session cookies, and user input. A compromised or overprivileged extension can read keystrokes, access enterprise apps, or seamlessly exfiltrate data.

The lose-lose compromise of current tools

Enterprises have historically been forced into a lose-lose compromise: Legacy network security platforms offer low friction but suffer from critical blind spots, relying on blunt "allow" or "block" decisions that miss data leakage at the point of interaction. Conversely, full-stack enterprise browsers provide deeper visibility but demand a highly disruptive trade-off: forcing organizations to completely "rip and replace" the tools their employees already use. This introduces massive change management hurdles, privacy concerns, and fierce end-user resistance.

The Solution: Enterprise browser control. On any browser.

Akamai Workforce Protector (formerly LayerX) is pioneering true interaction security by delivering a frictionless browser extension that securely transforms any browser into a fully managed workspace. You gain the deep, end-to-end security of a dedicated workspace platform without ever forcing a browser swap or disrupting the user experience.

AI usage control

Built on this secure workspace foundation, Akamai Workforce Protector extends its real-time visibility to govern how employees, AI agents, and vendors interact with AI. To safely accelerate AI adoption, organizations need end-to-end governance for AI usage. Workforce Protector performs comprehensive shadow AI discovery across the web and captures full AI conversations. It applies real-time AI data security to text inputs, file attachments, and copy/paste operations directly at the browser. By inspecting and controlling data at the exact moment it is entered into AI tools, Workforce Protector prevents intellectual property loss and regulatory violations right at the source.

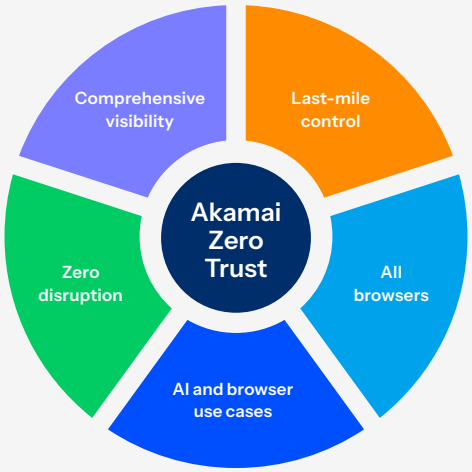
Securing the entire workspace surface

Workforce Protector establishes the browser as a secure, enterprise-controlled workspace for all daily tasks. It secures the entire interaction layer by delivering:

- **Browser-native DLP:** This monitors data in motion natively in the browser without relying on complex network decryption, such as utilizing file sandboxing to isolate and inspect sensitive uploads and downloads.

- **Automated compliance:** Workforce Protector features one-click automated enforcement of CIS Benchmarks across major browsers, ensuring continuous configuration compliance.
- **Unmanaged device support:** For BYOD and third-party contractors, the extension seamlessly enforces read-only sessions and watermarking without requiring heavy device management deployments.
- **Extension risk elimination:** A native extensions risk database automatically analyzes risk scores, behaviors, and permissions to instantly block malicious or overprivileged third-party browser plug-ins.

Take control of your interaction layer



Happy users. Happy security. Happy IT.

Workforce Protector delivers measurable security and architectural savings from the first hours of deployment, balancing robust protection with a frictionless end-user experience. Users maintain their preferred browsers and native workflows, with zero performance degradation or latency introduced into daily tasks. IT and security teams achieve unmatched time to value with rapid deployment that requires no complex network rerouting or downtime, hardware appliances, or proxy configurations.

To learn more about how Akamai Workforce Protector can safely accelerate your AI adoption without slowing down your business, visit akamai.com/akamai-workforce-protector.

© 2026 Akamai Technologies | Support |
| Published 07/26