Customer Story

AGG Protected Its Sensitive Data

Akamai Workforce Protector (formerly LayerX) helped identify web-borne threats without blocking employee use of generative AI tools and browser extensions

Protected browser extensions

Unblocked GenAI security

Achieved granular visibility

Arnall Golden Gregory (AGG) LLP is a law firm headquartered in Atlanta that provides legal services to mid-market and global businesses across the finance, healthcare, regulatory, real estate, and international trade sectors.

As a successful law firm, AGG's employees need to be able to access online data sources, from legal research and reference websites to document management and writing apps to communication tools. These online websites and SaaS applications allow lawyers and other employees to provide the most updated, comprehensive, accurate, and reliable legal services to their clients, in the most efficient manner. This ability translates directly into billable hours for the firm and contributes to the firm's brand management. In addition, AGG is subject to regulatory requirements.

AGG identified the browser as a unique threat surface that requires dedicated protection. At the same time, the firm realized that employee access to websites and tools was foundational to its success. AGG aimed to prevent browser-based malicious activity and data leakage. At the same time, it gave employees the flexibility to securely use their preferred productivity tools.

Protecting against malicious extensions

Malicious browser extensions have become a key component in attackers' toolkits. They deliver them either by socially engineering employees to download a seemingly benign extension from a web store or by sideloading them to their machines without the user's knowledge or consent. Once installed, the malicious extension has excessive permissions that provide direct access to all the browser's data and activities. The attacker can now capture and exfiltrate them at will.

AGG sought a solution to manage browser extensions downloaded and used by employees. AGG understood the extensions' productivity value, especially for employees who engage in tasks that require heavy research and document management. Extensions can help with citations, organizing legal research, saving online resources directly into case files, and more. This optimizes productivity, translating directly into the firm's profitability.

Arnall Golden Gregory LLP

Location
Atlanta, Georgia
agg.com

Industry
Business Services

Solution
Security

Product
Akamai Workforce Protector

Akamai Security

At the same time, AGG also realized some extensions are malicious and need to be blocked. The firm was looking for a solution to help it differentiate between the two types of extensions, allow the use of reliable extensions, and automatically prevent the download of malicious ones and disabling extensions that were already in use.

Automated detection and blocking malicious extensions

The Akamai Workforce Protector browser extension has immediate visibility into all other extensions that reside on the browser. The Workforce Protector risk engine analyzes the required permissions, installation method, publisher reputation, and other unique attributes for each discovered extension. It uses this information to reach a verdict on the extension's risk.

The AGG team used this capability to manage employee use of browser extensions across the entire firm. They configured policies that alerted whenever an extension with high permissions was being installed and disabled any extension that Workforce Protector flagged as critical risk. Workforce Protector applied these policies automatically to all the extensions in place, as well as to all extensions installed from that point onward.

Unblocking GenAI apps for employee use

Preventing GenAI data leakage has become an industry-wide problem. The widespread use and convenience of AI-driven tools, and lack of awareness, means employees may unknowingly share proprietary or confidential information, like customer information or internal strategies, while seeking assistance or generating content. This unintentional data sharing can compromise the organization's security posture and expose it to legal and compliance risks.

Traditional security measures such as firewalls, DLP tools, and employee training programs are not fully equipped to handle the unique risks posed by AI-driven communication tools. This means that despite efforts to secure data, there was a gap in effectively monitoring and controlling how employees interact with AI systems.

While AGG wanted to enable ChatGPT and similar AI tools to drive innovation, the firm could not accept the compliance and legal risks of unmonitored data leakage. Therefore, the law firm was forced to block employee access to ChatGPT and similar GenAI tools — until AGG discovered Workforce Protector.

GenAI security and productivity

Workforce Protector GenAI Security is a specialized DLP solution designed to address the unique challenges posed by the use of AI-driven tools like ChatGPT. Workforce Protector GenAI DLP monitors and controls data exchanges within GenAI-app interactions.

By leveraging advanced algorithms and real-time analysis, Workforce Protector detects and prevents typing or sharing of sensitive information, ensuring that confidential information is not exposed. This proactive approach enables organizations to benefit from the productivity capabilities of AI while maintaining stringent data security standards.

By deploying Workforce Protector, the AGG team was able to provide employees with access to ChatGPT and GenAI tools. Workforce Protector provided visibility and governance, ensuring there is no data leakage and allowing AGG's employees to use AI tools at will without compromising security, business confidentiality, or client privacy.



We were looking for a dedicated solution to help us manage browser extensions, and then we found LayerX [now Akamai Workforce Protector]. It solved our malicious extension problem, and then went beyond and solved all of our browser-related security challenges.

Daniel Lehman
CIO, Arnall Golden Gregory LLP

Identifying web-borne zero-hour threats

AGG is covered by all standard cybersecurity tools and protections, as a modern organization with an updated information security team. The AGG security team recognized the browser as a critical blind spot. Although operating at the intersection of **endpoint**, network, data, and identity security, web browsers lacked comprehensive protection from traditional security tools.

This is particularly a problem now that the browser is the main work interface for many employees, especially in professional services sectors. AGG looked for a dedicated security solution that would identify areas of risk from **CVEs** and zero-hour threats, and block them before they cause harm.

360-degree visibility into browser activity and risks

Workforce Protector helped AGG address this problem by continuously monitoring browsing sessions to detect any early sign of malicious activity. Protection ranges from zero-hour detection, disabling phishing pages, protecting against traditional browser exploits, preventing malware download threats, and more.

Because Workforce Protector operates directly on the browser, it can prevent users from interacting with malicious web pages or downloading harmful content through URL filtering, real-time analysis of page behavior, scanning, and browser patching. As a result, AGG did not need to completely block specific websites. Instead, it was able to operate at a granular level to reduce the risk. This turned the security team into business facilitators rather than restrictors.

Data exposure on legitimate web destinations

Similar to GenAI applications, employees can also expose sensitive information — whether intentionally or accidentally — across various websites and SaaS applications. Employees might be copying and pasting sensitive data, uploading files, or sharing information on ungoverned SaaS and web applications. Without full control and oversight, organizations are left vulnerable to data leaks, which can happen unnoticed through these channels.

For law firms, risky sites and apps might include case management platforms, online drives, signature tools, legal research platforms, and more. Yet these sites are also crucial for day-to-day attorney work. AGG needed the ability to ensure that employees were not exposing client and organizational secrets without blocking use altogether.

Web DLP to prevent data exposure risk

Workforce Protector can identify all activities users perform in the browser down to the granular level of a mouse movement or a button click. The AGG team leveraged this capability to configure DLP policies that prevent users from uploading or pasting sensitive data to insecure web apps. Workforce Protector architecture enables this capability to become an integral part of the browser, so the analysis and policy enforcement take place as part of the web session itself and without any disruption to the user's browsing experience.



LayerX [now Akamai Workforce Protector] has allowed us to open up GenAI tools like ChatGPT to employees. These applications were previously blocked. With LayerX, we can now enjoy the productivity and innovation benefits GenAI brings to the information and professional services sector.

Daniel Lehman
CIO, Arnall Golden Gregory LLP

Unblock restrictions and drive employee productivity

The Akamai Workforce Protector enterprise browser extension provides a security solution that supports AGG's strategic security objective: driving employee productivity through permissive use of online resources. Workforce Protector provides visibility that allows the security organization to prevent malicious activities and data exfiltration, allow innovation and productivity through secure use of GenAI, browser extensions, and online apps and tools.

Workforce Protector works with any browser and allows for easy installation across devices, making it straightforward for the security team to use. This agility supports AGG's working methods, further supporting the security organization as a business enabler.

"Akamai Workforce Protector is a comprehensive security solution, which not only does not prevent, but actually extends, what employees can do online. For a law firm, this is a significant competitive advantage," concluded Daniel Lehman, CIO at Arnall Golden Gregory LLP.

Arnall Golden Gregory LLP

Arnall Golden Gregory (AGG), an Am Law 200 law firm with more than 200 attorneys in Atlanta and Washington, D.C., takes a "business sensibility" approach when advising clients. AGG provides industry knowledge, attention to detail, transparency, and value to help businesses and individuals achieve their definition of success. AGG's transaction, litigation, regulatory, and privacy counselors serve clients in healthcare, real estate, retail, litigation and other dispute resolution, business transactions, fintech/payment systems, technology, global commerce/global mobility, life sciences, economic development, public finance, logistics and transportation, government investigations, and government contracts.

© 2026 Akamai Technologies | Support |
| Published 11/26