

LayerX Helps AGG LLP Protect Their Sensitive Data from Web-Borne Threats Without Blocking Employee Use of GenAI Tools, Browser Extensions and Other Productivity Tools

Arnall Golden Gregory (AGG) LLP is a law firm headquartered in Atlanta, Georgia 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, they realized that employee access to websites and tools was foundational to their success. The firm aimed to protect against malicious activity targeting the browser and data leakage from the browser, while giving employees freedom and flexibility to use their tools of choice and get their jobs done - effectively and efficiently.

1 Protecting Against Malicious Extensions

The Challenge: Allowing the Use of Browser Extensions While Blocking 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 were looking for a solution to manage browser extensions that were downloaded and in use 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.

At the same time, AGG also realized some extensions are malicious and need to be blocked. They were looking for a solution to help them 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.

Industry

Size

Location

Law firm

400 employees

US

Challenges

- Managing employees’ usage of browser extensions while blocking malicious ones
- Allowing secure use of GenAI tools to drive employee productivity, while preventing data leakage risks
- Protecting against zero-day threats and ensuring safe browsing
- Preventing data exfiltration across websites and SaaS apps

LayerX Solution

- Browser Extensions Protection:** Allowing use of legitimate browser extensions and blocking malicious ones
- GenAI Security:** Unblocking GenAI applications to drive productivity while protecting against sensitive data exfiltration
- Zero-Hour Protection Against Browser-borne Threats:** real-time prevention of zero-hour phishing and social engineering, to ensure safe browsing
- Web DLP:** Visibility into user activity at a granular level to prevent users from uploading or pasting sensitive data to ungoverned SaaS/Web applications

The LayerX Solution: Malicious Extensions: Automated Detection and Blocking

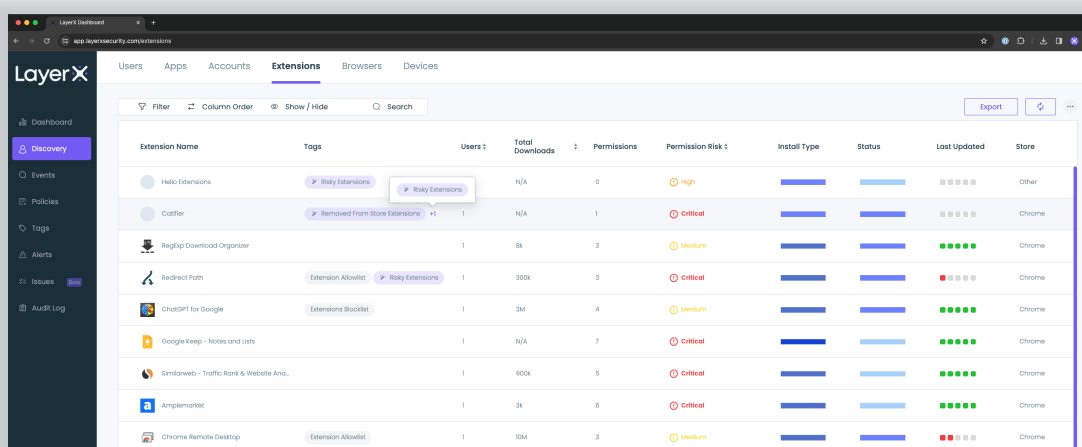
The LayerX browser extension has immediate visibility into all other extensions that reside on the browser. The LayerX risk engine analyzes the required permissions, installation method, publisher reputation, and other unique attributes for each discovered extension. It uses this information to reach 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 LayerX flagged as critical risk. LayerX applied these policies automatically to all the extensions in place, as well as to all extensions installed from that point onwards.



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

Daniel Lehman, Director Of Technology at Arnall Golden Gregory LLP



Extension Name	Tags	Users	Total Downloads	Permissions	Permission Risk	Install Type	Status	Last Updated	Store
Hero Extensions	Risky Extensions		N/A	0	High				Other
Catfish	Removed From Store Extensions	1	N/A	1	Critical				Chrome
RegUp Download Organizer		1	8k	3	Medium				Chrome
Redirect Path	Extension Allowlist	1	30k	3	Critical				Chrome
ChatGPT for Google	Extensions Blocklist	1	3M	4	Medium				Chrome
Google Keep - Notes and Lists		1	N/A	7	Critical				Chrome
Simulweb - Traffic Rank & Website Ana...		1	90k	5	Critical				Chrome
Anglemarket		1	3k	6	Critical				Chrome
Chrome Remote Desktop	Extension Allowlist	1	10M	3	Medium				Chrome

2

Preventing Data Leakage to Gen AI tools

The Challenge: 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.

Therefore, while AGG aspired to enable the use of ChatGPT and similar tools to drive productivity and innovation, they could not take upon themselves the legal and compliance risk of data leakage. Therefore, they were forced to block employee access to ChatGPT and similar GenAI tools - until they discovered LayerX.

The LayerX Solution: Gen AI Security: Productivity and Security

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

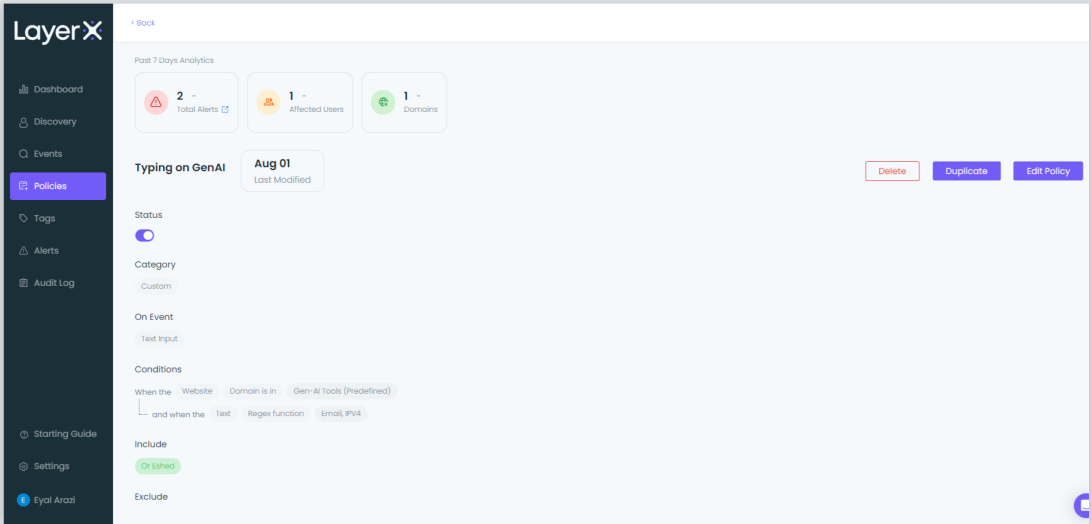
By leveraging advanced algorithms and real-time analysis, LayerX detects and prevents typing or sharing of sensitive information, ensuring that confidential information is not exposed. This proactive approach enables organizations to benefit from the productivity capabilities of AI while maintaining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

By deploying LayerX, the AGG team was able to provide employees with access to ChatGPT and GenAI tools. LayerX 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.



“LayerX 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, Director Of Technology at Arnall Golden Gregory LLP



3

Ensuring Safe Browsing and Safeguarding from Web-borne Threats

The Challenge: 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. Nonetheless, the AGG security team recognized that the browser is a unique blind spot for traditional network and endpoint security tools, and that while the browser sits at the intersection of endpoint, network, data and identity security, it wasn't getting full coverage by any of those 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.

The LayerX Solution: 360-degree Visibility into Browser Activity and Risks

LayerX helped AGG address this problem by continuously monitoring browsing sessions to detect any early sign of malicious activity. Protection ranges from 0-hour detection, disabling phishing pages, protecting against traditional browser exploits, preventing malware download threats, and more.

Because Layer X 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, they were able to operate at a granular level to reduce the risk. This turned the security team into business facilitators rather than restrictors.

The screenshot displays the LayerX Alerts interface. On the left is a sidebar with navigation options: Dashboard, Discovery, Events, Policies, Tags, Alerts (selected), Audit Log, Starting Guide, Settings, and Final Alert. The main area shows a table of alerts with columns: User, Risk, Type, Action, Policy, URL, and Info. The table lists several alerts for users like 'Or Eshed', 'Peter Morrissey', and 'Gil Fromavitch', with risks ranging from Medium to High. A summary at the bottom indicates 'Total alerts 347' and 'Page 1 out of 7'.

On the right, a detailed 'Alert' view is shown for a specific alert. It includes an 'Overview' section with a description: 'Control risky sites: low reputation, suspicious code, high-risk websites'. Below this is the 'URL' field: 'att-mail-108941weeblysite.com/'. The 'Risk Analysis' section lists various risk factors with status indicators: Domain Age Risk (green), Hosting Service (green), Download Links Pervasiveness (green), Top Level Domain Risk (green), Usage History Risk (red), Credential Inputs Threat (green), Popularity Risk (green), Reputation Risk (green), Homepage Similarity Risk (red), Website Assessment Risk (green), and Homepage Assessment Risk (green). At the bottom, there are buttons for 'Mark website as safe', 'More info', and 'Investigate'.

4

Protecting from Online Data Exfiltration

The Challenge: 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.

The LayerX Solution: Web DLP to Prevent Data Exposure Risk

LayerX 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. LayerX 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.

Extension Name	Tags	Users	Total Downloads	Permissions	Permission Risk	Install Type	Status	Last Updated	Store
Hello Extensions	Risky Extensions		N/A	0	High				Other
Coffler	Removed From Store Extensions	1	N/A	1	Critical				Chrome
RegUp Download Organizer		1	8k	3	Medium				Chrome
Redirect Path	Extension Allowed	1	30k	3	Critical				Chrome
ChatGPT for Google	Extensions Blocked	1	3M	4	Medium				Chrome
Google Keep - Notes and Lists		1	N/A	7	Critical				Chrome
Similarweb - Traffic Rank & Website Anal.		1	90k	5	Critical				Chrome
Anglemarket		1	2k	6	Critical				Chrome
Chrome Remote Desktop	Extension Allowed	1	10M	3	Medium				Chrome

Conclusion:

A Security Solution That Unblocks Restrictions and Drives Employee Productivity

The LayerX Enterprise Browser Extension provides a security solution that supports AGG's strategic security objectives: driving employee productivity through permissive use of online resources. LayerX 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.

LayerX makes it easy for the security team to utilize, by working with any browser and allowing for easy installation across devices. This agility supports AGG's working methods, further supporting the security organization as a business enabler.



"LayerX 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."

Daniel Lehman, Director Of Technology at Arnall Golden Gregory LLP

