LayerX | CASE STUDY

LayerX Helps Similarweb Enhance, Consolidate, and Simplify Protection Against Web-Borne Threats and Vulnerabilities

Similarweb is a digital intelligence platform that provides comprehensive analytics and data on websites and mobile apps. Similarweb helps businesses understand web traffic, user engagement, and competitive benchmarks by offering insights into visitor demographics, traffic sources, and keyword performance. This makes it a valuable tool for digital marketers, SEO professionals, business analysts and more.

Similarweb has identified the browser as a unique threat surface that requires dedicated protection. The company aimed to comprehensively understand and gain insight into its threat profile, pinpoint risk factors, and formulate an appropriate remediation strategy to address browser-borne risks and threats.

similarweb

Industry
Data

Size
1200 employees

Location
Worldwide

Challenges

- Detection of sensitive information inadvertently leaked into GenAI tools such as ChatGPT
- Identifying potentially malicious activities from phishing or high-risk websites
- Detecting shadows SaaS, unsafe browser extensions and potential data loss during employee off-boarding process
- Address and remediate web browser vulnerabilities to ensure governance and adherence to security regulations

LayerX Solution

- **Gen AI DLP:** Enabling the monitoring and prevention of sensitive information exfiltration, while ensuring continued productivity
- **Safe Browsing:** Identifying and blocking malicious attacks while educating employees on security practices
- **Shadow SaaS and Malicious Extensions Protection:** Providing enhanced visibility into browser sessions to prevent shadow accounts or use of unauthorized extensions, including when offboarding employees
- **Enforcing Browser Updates:** Notify and prompt users to update their browsers to ensure compliance with browser update policies

1 Eliminating Browser Blind Spots

The Challenge: Identify Threats at the Point of Risk and Eliminate Security Blind Spots

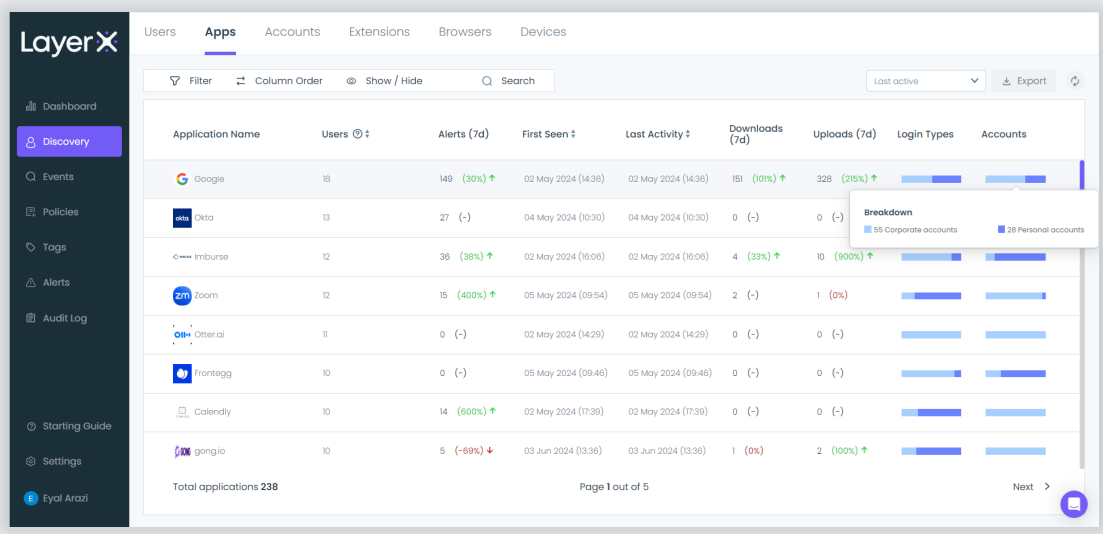
Similarweb is covered by all standard cybersecurity tools and protections, as a modern organization with an extensive information security team. Nonetheless, the Similarweb security team recognized that the browser is a unique blind spot for traditional network and endpoint security tools, and that while 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 the post-COVID hybrid-work world. Moreover, the browser is frequently invoked as part of the authentication for non-browser external applications, making it a critical focal point for identity security. As a result, Similarweb looked for a dedicated security solution that would lock-down their browsers, give them visibility into user activity and data that pass though the browser, and identify areas of risk.

> *"Visibility is essential; however, gathering insights from tools outside the browser can be time-consuming and even challenging. LayerX addresses this gap simply and effectively."*
>
> *Tomer Maman, CISO of Similarweb*

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

LayerX helped Similarweb address this problem by providing complete visibility to browser activity and data, including users, accounts, identities, and applications, thereby enabling Similarweb to define their browser-based security perimeter, understand their risk profile, and identify potential risks that need remediation.



2 Preventing Data Leakage to Gen AI tools

The Challenge: Employees Inadvertently Leaking Sensitive Data to Gen AI Tools

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 while seeking assistance, developing code, or generating content. This unintentional data sharing can compromise the organization's security posture and expose it to legal and compliance risks. At the same time, organizations aspire to enable the use of ChatGPT and similar tools to drive productivity and innovation.

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 some organizations block GenAI altogether, Similarweb recognizes the productivity advantages of GenerativeAI tools and how they enable business requirements. Yet, without a robust solution, organizations remain vulnerable to unintentional data breaches.

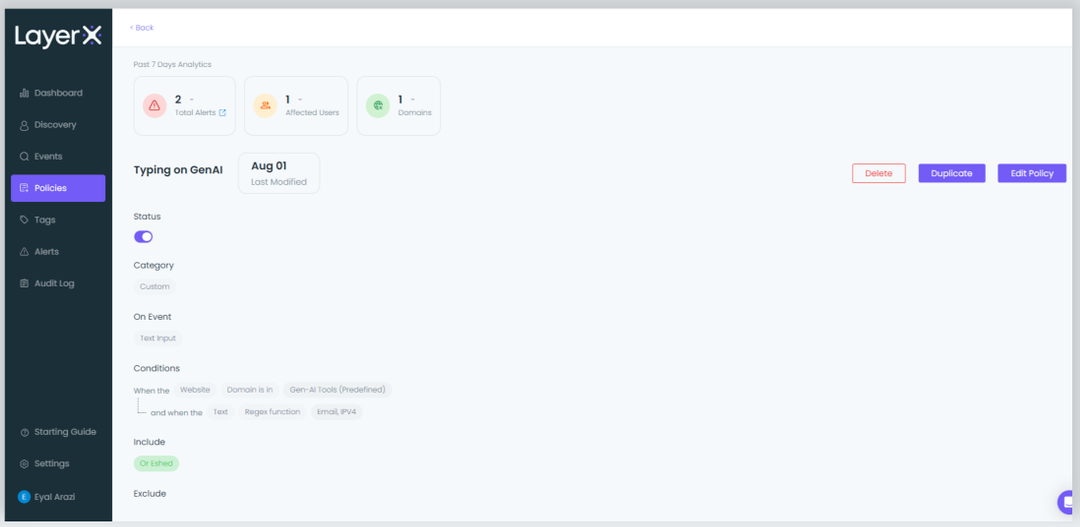
The LayerX Solution: Gen AI DLP: Productivity and Security

LayerX Gen AI DLP 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 ChatGPT 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.

The Similarweb team deployed LayerX on the browser to secure employee interactions with Generative AI tools and allow employees to use AI tools without compromising security.

> *"When we enable secure AI tools such as ChatGPT, the security organization becomes a business enabler. We're an innovative organization and LayerX ensures we continue to enable business agility and productivity while maintaining security."*
>
> *Tomer Maman, CISO of Similarweb*



3 Ensuring Safe Browsing and Preventing Malicious Attacks

The Challenge: Attackers Using Malicious Tactics to Access Data and Systems

The browser has become the main workspace in many enterprises. As a result, it is also one of the most critical points of risk since so much user activity and data go through it.

Attackers frequently target organizations with malicious websites and phishing attacks in an attempt to initiate account takeover attacks or data leakage. These schemes can take many forms, including phishing websites that mimic legitimate ones, malicious browser extensions that steal sensitive information, and more. This exposure can lead to significant financial, reputational, and legal consequences for organizations.

Recognizing this, the Similarweb team sought to consolidate their various browser security tools, streamline protection into a single flow (with a single discernable user journey), and achieve as much security coverage as possible directly at the point of risk.

The LayerX Solution: Safe Browsing and Malicious Activity Detection

LayerX provides comprehensive browser security capabilities that prevent malicious activities.

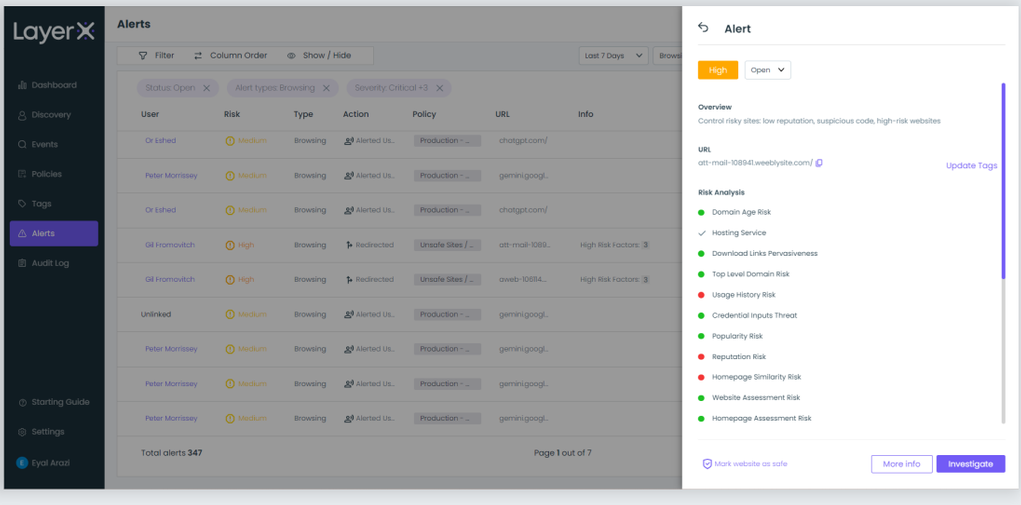
LayerX provides robust visibility into browsing activities, helping security managers understand their threat profile and monitor for potential browsing risks. Moreover, it helps simplify the security process by consolidating multiple tools and protections into a single platform, allowing for comprehensive coverage and tracking of browsing risks and threats.

LayerX blocks access to phishing sites and adversary-controlled web pages using advanced URL filtering and real-time page behavior analysis. In addition, LayerX scans every web page to disable phishing and social engineering attempts, even the most sophisticated ones. LayerX also ensures browsers are always patched and updated while preventing malware downloads from web pages. Finally, LayerX continuously monitors browsing sessions for immediate detection and prevention of malicious activities.

By providing multiple layers of protection, both at the preventative user level, as well as active protection against malicious sites, LayerX helps reduce the organization's attack surface and protect the point of risk.

LayerX's agility and user-centric design mean that employees are protected without interrupting or slowing down work, thereby maintaining the user experience and reducing workforce friction.

> *"Engaging with employees is fundamental in our line of work. LayerX explains to the employees why blocking a website or browser extension makes sense and is necessary for their security, harnessing them to become a part of the process."*
>
> *Tomer Maman, CISO of Similarweb*



Conclusion:
A Security Solution That Transforms Security Into a Business Enabler

LayerX provides a security solution that supports Similarweb's strategic security objectives: supporting the business goals and needs. LayerX provides visibility that allows the security organization to prevent malicious activities, allow innovation and productivity through tools like GenAI, secure web browsing, prevent shadow SaaS and more.

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 Similarweb's working methods, further supporting the security organization as a business enabler.

> *"LayerX provides a comprehensive solution, helping us secure even the most innovative user activities on the browser."*
>
> *Tomer Maman, CISO of Similarweb*