LayerX | CASE STUDY

LayerX Helps MediaTek Protect Against Web and AI Data Leakage, Insider Threats, and Browser Extension Risks

Introduction

MediaTek Inc. is a Taiwanese fabless semiconductor company that designs and manufactures a range of semiconductor products, providing chips for wireless communications, high-definition television, handheld mobile devices, navigation systems, consumer multimedia products and digital subscriber line services as well as optical disc drives.

As a company that designs chips in the highly competitive semiconductor industry, they are constantly concerned about data leakage of sensitive information, chip design, trade secrets, etc., from the company. While they already have a dedicated DLP team and a full stack of network, application and end-point security tools that protect against data leakage, existing security tools still have some blind spots that MediaTek wants to cover to ensure an even higher level of protection.

Most users consume GenAI tools, Web/SaaS apps and extensions via the browser, making the web browser the main point risk for data leakage. Existing security solutions fail to protect the last mile of user activity due to which MediaTek has identified the browser as a unique threat surface that requires dedicated protection. They want to give employees freedom and flexibility to use web applications and browser extensions to get their jobs done effectively and efficiently, while managing the security risks of any inadvertent data leakage through these apps.

MEDIATEK

Industry
Semiconductor

Size
20,000+

Location
Global presence

Challenges

- Preventing data exfiltration across websites and SaaS apps
- Detection and control over unauthorized usage of shadow GenAI tools
- Managing employees' usage of browser extensions while blocking malicious ones

LayerX Solution

- **Web DLP:** Visibility into browser sessions and user activity at a granular level to prevent users from uploading or pasting sensitive data to ungoverned SaaS/Web applications
- **GenAI DLP:** Blocking unauthorized GenAI apps while ensuring continued productivity by enabling the use of internal GenAI tools through continuous monitoring and preventing sensitive information exfiltration
- **Browser Extensions Protection:** Allowing the use of legitimate browser extensions and blocking malicious ones

Protecting from Insider Threats and Data Exfiltration on Web and SaaS Applications

Challenge : Data Exposure on Web Destinations

Web channels are the easiest channel for insider threats and inadvertent data leakage. Similar to GenAI applications, employees can expose sensitive information intentionally and accidentally across various websites and SaaS applications. Employees may copy and paste sensitive data and upload files to ungoverned SaaS and Web apps using non-corporate identities. This could include risky sites like online drives, file-sharing SaaS apps, web messaging tools, etc, which are crucial for day-to-day work.

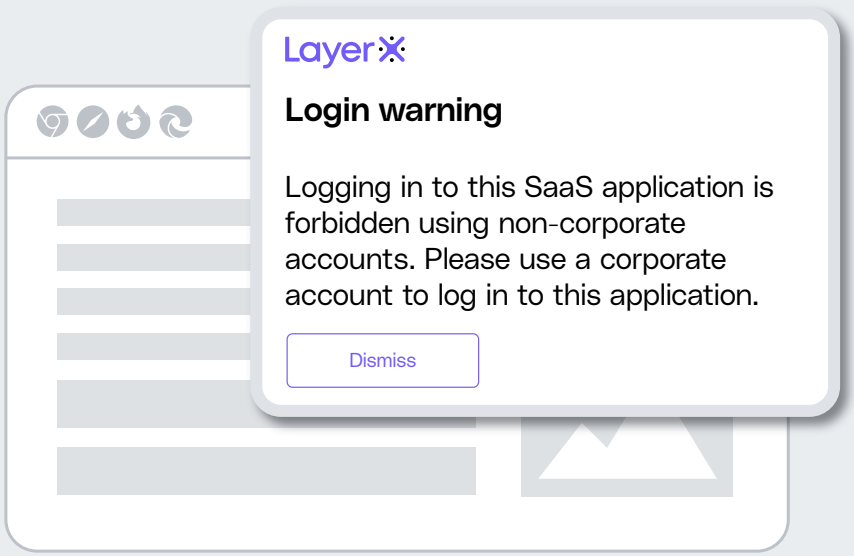
Existing DLP solutions are file-centric and fail to protect data-in-motion, leaving organizations blind and exposed to sensitive data leakage. Without full control and oversight, organizations are left vulnerable to data leaks, which can happen unnoticed through these channels.

Due to the sensitive nature of their data, MediaTek is highly concerned about data leakage. However, Mediatek's employees are highly-skilled knowledge workers that need (and demand) web access for their everyday work. This means that Mediatek can't just block off web access. Rather, they need a solution that covers web DLP without impacting the user experience.

LayerX Solution : Web DLP to Prevent Data Exposure Risk

LayerX provides complete visibility into all websites and SaaS apps, tracking where your data is going and who is using it. It also restricts copying data or files with sensitive information to external SaaS apps and unsanctioned file-sharing services through granular last-mile enforcement. We also provide detailed information about where the data was copied from, the browser tab-titles for the source and to which destination it was pasted which gives MediaTek full visibility into their employees actions. The MediaTek team leveraged this capability to provide full browsing context with identity awareness and cross-identity controls to DLP logic, restricting login to
web/SaaS file-sharing tools using non-corporate accounts, and ensuring sensitive corporate data can be accessed only by verified corporate users.

> *"LayerX gives us real-time eyes and control over every click and upload. Securing the web has never been this seamless, but LayerX made it happen."*



Preventing Unauthorized GenAI Tool Usage and Detecting 'Shadow' AI tools

Challenge: Employees Inadvertently Leaking Sensitive Data to GenAI Tools

Preventing unauthorized use of GenAI tools has become an industry-wide problem, especially to companies like Mediatek due to the highly secretive nature of the semiconductor industry. The widespread use and convenience of AI-driven tools and lack of awareness result in employees unknowingly sharing proprietary and confidential information while seeking assistance, developing code or generating content.

As a leading provider of semiconductor chip designs, Mediatek is concerned about any exposure of their chip designs to external sources. Shadow GenAI tools are hazardous as any data shared with them is stored/processed outside the organization, used for LLM training, etc., exposing highly confidential and proprietary data. This compromises the organization's security posture and exposes 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 tools. While they can enforce file-centric data transfer restrictions, the main issue arises when there is file-less data activity like copy/paste, text input, etc. This means that despite efforts to secure data, there was a gap in effectively monitoring and controlling how employees interact with AI tools.

While some organizations block GenAI altogether, Mediatek recognizes the productivity advantages of GenAI tools and how they can enable businesses more efficiently and productively. While Mediatek has built their own AI tools for this, they need to block all GenAI activity from unauthorized and shadow AI applications. They also wanted to monitor and control all data that goes into their GenAI tools so that employees can use them seamlessly to drive productivity and innovation while preventing sensitive data leakage.

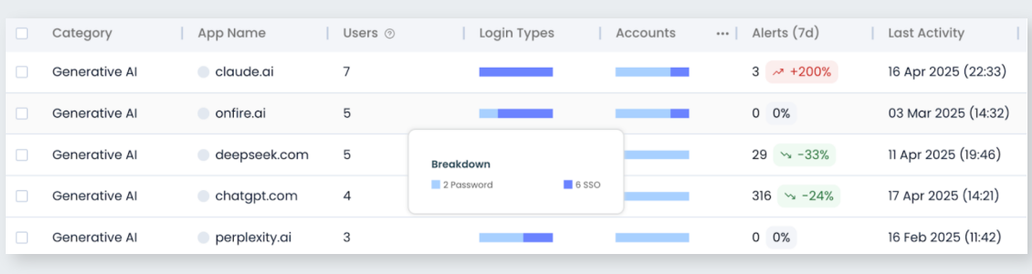
The LayerX Solution: GenAI Discovery and Prevent GenAI Data Leakage

LayerX offers comprehensive visibility into GenAI application usage by deploying directly as a browser extension. It monitors user actions such as browsing activity, login attempts, data input, and file uploads, identifying which tools are accessed, by whom, and through which accounts (corporate or SSO or personal). This enables organizations to detect unauthorized data sharing and enforce policies to block 'shadow' AI applications.

LayerX permits organizations to enforce last-mile controls on all shadow GenAI tools and SaaS applications, directly within the browser. Organizations can define tailored security policies with a range of enforcement options, ranging from monitoring only, to warning users with customizable messages, to masking sensitive data, to completely blocking their actions. By leveraging advanced algorithms and real-time analysis, LayerX detects and prevents typing, copy/paste or sharing files with sensitive data, ensuring 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 Mediatek team deployed LayerX on the browser to block access to shadow AI tools and secure employee interaction with their own GenAI tools without compromising security.

> *"LayerX made it possible for us to embrace GenAI securely - seeing, managing, and protecting every interaction at the browser level. Deploying LayerX was a game-changer as we now empower innovation without ever worrying about data leakage to shadow AI tools."*



Eliminating Malicious Extensions from Users' Browsers

Challenge : Allowing Browser Extensions While Blocking the Malicious Ones

Browser extensions have become a key component in attackers' toolkits. Attackers use social engineering or silent sideloading to install malicious extensions that gain full access to browser data. Once installed, malicious extensions have direct access to all the browser's data and activities, making it possible for the attacker to exfiltrate them at will.

Existing tools offer little visibility into extension activity and rely on manual blocklists, making it difficult to detect threats in real time. As an "open" organization that is attuned to its employees, Mediatek did not want to block all extensions. However, managing extension whitelists manually is very resource-intensive. This is why companies like Mediatek look for automated processes that allow safe, productivity- boosting extensions—while blocking malicious ones.

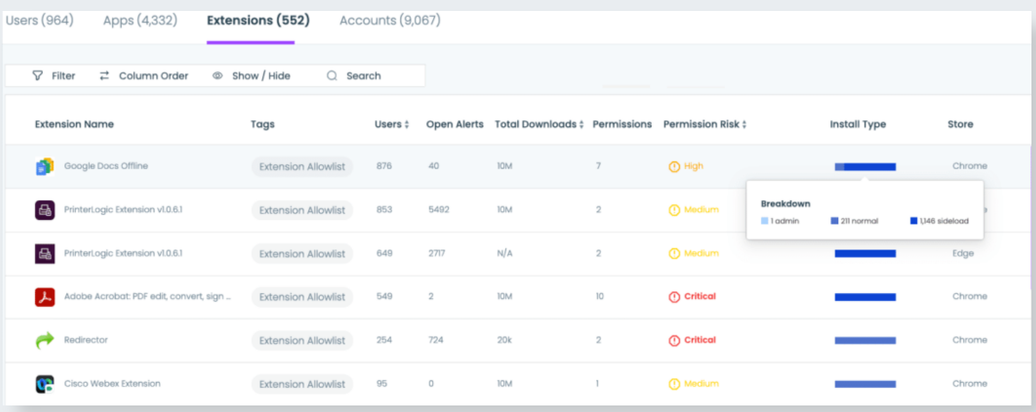
LayerX Solution: Automated Detection and Disablement of Malicious Extensions

LayerX, has full visibility into all the extensions that reside on the browser. It identifies risky browser extensions using a comprehensive risk scoring approach that combines risk factors such as permission scope and extension reputation.

The Mediatek team used this capability to manage employee use of browser extensions across the organization. They configured policies that alerted whenever an extension with high permissions was being installed and disabled any extension that LayerX flagged as critical risk.

Once the policy was configured, LayerX automatically applied it to all the existing extensions.

> *"LayerX's automated extension control saved us countless IT hours and shut down a major attack vector. We empower innovation while automatically blocking any extension that could put us at risk."*



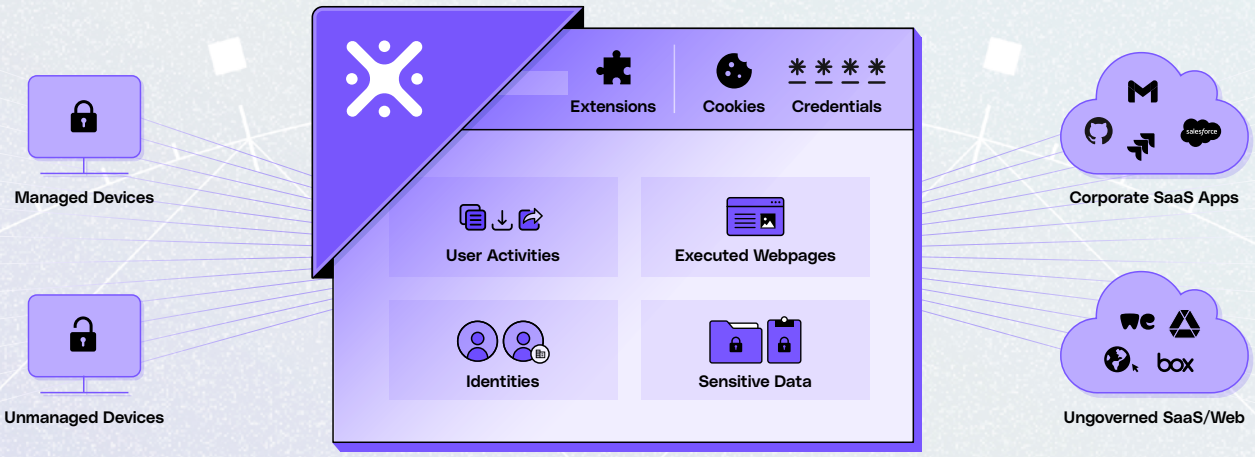
Conclusion:

Protect More, Restrict Less: A Security Solution that Drives Employee Productivity

The LayerX Enterprise Browser Extension provides a security solution that supports MediaTek'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, allowing 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 MediaTeks' working methods, further supporting the security organization as a business enabler that boosts employee productivity.

> *"With LayerX, we get the best of both worlds - protecting against Web and AI data leakage, without worrying about disruption to the user experience or workflow."*



One Platform for ALL Browsing Risks and Web-Borne Threats

The All-in-One AI & Browser Security Platform

LayerX agentless AI & browser security platform protects enterprises against the most critical AI, SaaS, web and data leakage risks across any browser, application, device and identity, with no impact on user experience

Integrates with All Commercial, AI and Enterprise Browsers

The LayerX Security Platform

Delivered as an Enterprise Browser Extension, LayerX offers the most comprehensive visibility and enforcement capabilities over AI and Browsing risks, including:

AI Usage Security

GenAI DLP
Prevent leakage of sensitive data on AI tools

AI Browsers Protection
Protect AI browsers against attack and exploitation

Shadow AI Discovery
Discover and enforce security guardrails on all AI apps

AI Access Control
Restrict user access to unsanctioned AI tools or accounts

AI Misuse Prevention
Protect against prompt injection, compliance violations, and more

AI Response Validation
Ensure AI response validity and data security

Enterprise Browser Security

Web/SaaS DLP & Insider Threat
Prevent data leakage across all web channels

Browser Extension Management
Detect and block risky browser extensions on any browser

Shadow SaaS & SaaS Security
Discover 'shadow' SaaS and enforce Saas security controls

Safe Browsing
Protect all browsing activity against web exploits

SaaS Identity Protection
Discover and secure corporate and personal SaaS identities

AI Browsers Protection
Protect AI browsers against attack and exploitation