Gaming Companies Protect and Control Their Data with an Enterprise Browser Extension

LayerX - The first fully-automated solution that enables gaming companies to secure and control all browsing activities, including GenAI, browser extensions, online apps and websites.

Gaming companies struggle to protect against data risks

Gaming companies encounter unique data risks. Safeguarding data is essential for protecting their revenue streams, intellectual property and user privacy. Manual processes, DLPs and other limited solutions cannot provide the robust protection gaming companies need in modern browsing environments.

The LayerX Enterprise Browser Extension automatically enforces DLP policies for any browsing activity

The LayerX Enterprise Browser Extension natively integrates with any browser to deliver continuous monitoring, risk analysis, and active policy enforcement on any event and user activity within the browsing session, including browser extensions, GenAI applications, insecure websites, and others. From its unique location in the browser, LayerX is ideally positioned to address gaming companies' unique data protection challenges in a seamless, cohesive manner.

LayerX data protection capabilities for gaming companies

GenAI DLP & Web DLP

- Governance and control over uploading or typing of sensitive data into GenAI tools, like ChatGPT
- DLP policies that prevent uploading, downloading and sharing sensitive data and files to insecure locations, including file-sharing sites, personal accounts, Skype, online chat apps like Whatsapp or Facebook Messenger, and others.
- Blocking of insecure applications.
- Ability to define sensitive data policies based on keywords, images, regex and other criteria.

Browser Extensions Protection

- Continuous scanning and analysis of browser extensions to identify ones that need to be removed.
- Monitoring of extension behavior to prevent access to sensitive data

Key Benefits

- **DLP across multiple websites and environments**
- **ChatGPT and GenAI app exposure mitigation**
- **Risky browser extension blocking and protection**
- **360 visibility into all browsing activity**
- **Simplifying IT and security team responsibilities**

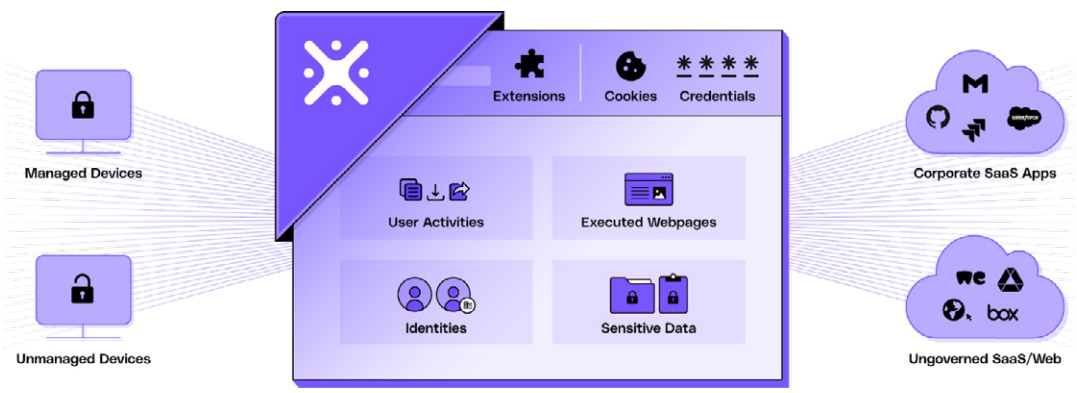
Monitoring and Logging

- Centralized dashboard of alerts. Includes the ability to send alerts to users before/instead of blocking and restricting activities.
- Granular monitoring and logging of all user activities, like visited sites and activities. Ability to monitor specific users or user groups.

LayerX Enterprise Browser Extension

LayerX Enterprise Browser Extension natively integrates with any browser, turning it into the most secure and manageable workspace, with no impact on the user experience. LayerX is the first solution that provides continuous monitoring, risk analysis, and real-time enforcement on any event and user activity in the browsing session.

Enterprises leverage these capabilities to secure their devices, identities, data, and SaaS apps from web-borne threats and browsing risks that endpoint and network solutions can't protect against. These include data leakage over the web, SaaS apps and GenAI tools, credential theft over phishing, account takeovers, discovery and disablement of malicious browser extensions, Shadow SaaS, and more.



LayerX Use Cases

LayerX enables security teams to monitor and reduce the attack surface of their browsers, enforce secure data usage across all web destinations, and protect against any type of attack delivered by a malicious web page

Browser Data Protection

- Web DLP
- GenAI/LLM DLP
- SaaS Discovery, DLP, and Protection
- BYOD DLP

Threat Prevention

- Zero-Hour Protection Against Browser-borne Threats
- Risky Browser Extensions Protection
- Browser Patch Management
- Identity Security Posture Management

Access Control

- Secure 3rd Party Access
- Secure Browser-based Authentication to SaaS and Web Apps
- BYOD Protection