Consulting Firms Regain Data Protection with an Enterprise Browser Extension

LayerX – The first solution that enables consulting firms to enforce DLP policies on employee access to and activity with customers' confidential data

Consulting firms' security teams struggle to guard data confidentiality

Data protection challenges that consulting firms encounter are essentially different from those of any other vertical. Customers' confidential data typically resides, and is sometimes even created, in their own environments. This hyper-centralization eliminates the option of using a standard DLP solution to tag these files or an SSE-based CASB to monitor employees' activities with this data.

The LayerX Enterprise Browser Extension enforces DLP policies even in customer environments

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. From its unique location in the browser, LayerX is ideally positioned to address consulting firms' unique data protection challenges in a seamless, cohesive manner.

LayerX data protection capabilities for consulting firms

Environment-agnostic DLP

- DLP policies that identify and scan data files in the browser and can thus be enforced equally across data rooms that belong to different customers.
- Governance and control over uploading or typing of sensitive data to GenAI tools such as Chat GPT.

Visibility and mapping of user activity

- Automated mapping of every app and web destination employees access, while alerting or blocking sites that might put data at risk.
- Accurate monitoring of time spent in each customer's environment, enhancing transparency of hourly charging.
- Compliance with any auditing requirements mandated by customers' vertical-specific regulations.

Key Benefits

- **Zero impact on browsing speed**
- **DLP across multiple environments**
- **ChatGPT exposure mitigation**
- **Rapid installation on users' browsers**
- **360 visibility into all browsing activity**

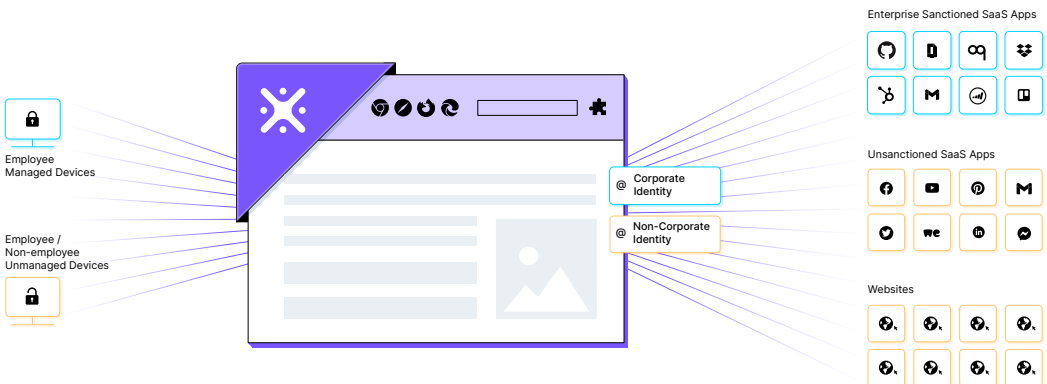
Access control

- Full mitigation of the malpractice of using the same password for different customers' data rooms.
- Enforcement of policies that follow up any password reuse attempt with either alerts or proactive prevention.
- Hardening access authentication requirements to prevent account takeover.

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