Layer X

THE SECURE ENTERPRISE BROWSER EXTENSION

LayerX all-in-one, agentless security platform protects enterprises against the most critical GenAI, SaaS, Web, Identity and Data Leakage risks and threats, without any impact on the user experience.

The browser is the main work interface in most organizations, making it the main point of risk for most cyberattacks. However, legacy security solutions such as CASB, web gateways, and endpoint solutions are blind to most in-browser user activity and data, leaving organizations exposed. This is why you need a dedicated browser-based security solution to protect you against the emerging risks of the modern workplace.

GenAl Security

Map GenAl usage in the organization, discover 'Shadow' Al apps and restrict sharing sensitive data with LLMs

Browser Extension Protection

Discover all extensions installed in the organization, assess their risk, and block or disable risky extensions

Web/SaaS DLP & Insider Threat

Track all data that goes on webbased SaaS and file-sharing apps and enforce controls on file-based and file-less data

N

Zero-Hour Web Protection

Scan every code element in realtime to stop 0-hour web threats such as phishing, malware, web vulnerabilities and more

The LayerX Platform:

Delivered as an Enterprise Browser Extension, LayerX seamlessly integrates with any browser and IdP, enabling organizations to address their most critical use cases, including:

Shadow SaaS

Detect 'shadow' SaaS apps, enforce granular guardrails and block sensitive data from leaking through them

- <mark>8</mark>

Identity Protection

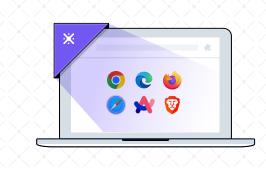
Protect organizational identities, prevent account takeover attacks and restrict activity by unsafe identities

Secure Access by BYOD/Contractors

Secure remote access from unmanaged devices and 3rd-party users with a single solution that covers all devices and employees

100% Enforcement with 0% Disruption

LayerX can be easily deployed, with no disruption to the user experience and no changes to existing software installations or network architecture. LayerX supports all common (and uncommon) web browsers, and integrates with IdP solutions, MDM solutions, and SIEM systems to fit in with your existing architecture



Don't Just Know About It. Fix It.

address their unique risks and threats

While many security tools only tell you about a problem but do not help you fix it, LayerX offers granular enforcement capabilities with a graphical rules wizard that enables security managers to easily define detailed security rules to

	and cond	nditions itions that wil	l trigger th	is policy			
ent ") Paste		~					
Conditions							
When the	Website	⊘ ∨ Username	Domain ⑦ ~	Not ends with	Gen-Al	Corporate Id	entities × v

Granular Enforcement Options

Gen Al Personal vs Corporate Accounts Usaae

tool usage breakda

Chat GPT

Co-Pilot

Claude

Gemini

Corporate Users

umber of sessions with pe

861

389

523

Personal Users

782

sonal and corporate account:

86

241

62

69

947 Total

851 Tota

764 Total

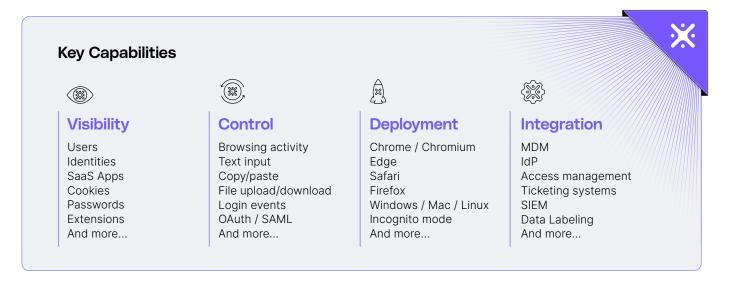
451 Total

Traditional security tools often force organizations to choose between allowing everything or blocking it all. LayerX, on the other hand, provides adaptive, risk-based enforcement options, enabling security teams to choose the level of enforcement they desire based on the risk profile without sacrificing productivity

Actions Actions triggered upon policy violation							
Security Profile							
Monitor	^						
Monitor Warn User							
Prevent With Bypass							
Prevent							
Redirect							

No Impact on the User Experience

LayerX is easily deployed to organizational endpoints without disrupting users' work. It does not add latency or require changes to user workflows, allowing for quick timeto-value with rapid adoption and no user friction



Layer×