LayerX

DATA PROTECTION AND SECURE USAGE OF GENERATIVE AI

ChatGPT's Data Protection Blind Spots and How LayerX Can Solve Them

In the short time since their inception, ChatGPT and other generative AI platforms have rightfully gained the reputation of ultimate productivity boosters. However, the very same technology can expose sensitive corporate data. A recent incident, in which Samsung software engineers pasted proprietary code into ChatGPT, clearly demonstrates that this tool can easily become a potential data leakage channel.

LayerX Browser Security Platform (delivered as an enterprise browser extension) is the only solution that can enable your workforce to fully realize the productivity potential of ChatGPT and other generative AI platforms while mitigating any exposure risk to your sensitive data, by preventing employees from typing/pasting of your sensitive data to ChatGPT.

The ChatGPT data protection challenge

Whenever an employee pastes or types text into generative AI tools such as ChatGPT, the text is no longer controlled by the corporate's data protection tools and policies. It doesn't matter if the text was copied from a traditional data file, an online doc, or another source. That, in fact, is the problem. Traditional security solutions are all file-oriented, and cannot address data rich interactions over the browser.

When employees submit customer data, code or company sensitive information, the organization gets exposed to compliance, privacy and intellectual property risks.

How LayerX enables secure usage of ChatGPT and other generative AI tools

LayerX browser security platform provides continuous monitoring, risk analysis, and real-time protection of browser sessions. Delivered as a browser extension, LayerX has granular visibility into every event that takes place within the session.

In the context of protecting sensitive data from being uploaded to ChatGPT, LayerX leverages this visibility to single out attempted text insertion events, such as 'paste' and 'type', within the ChatGPT tab. If the text's content in the 'paste' event violates the corporate data protection policies, LayerX will prevent the action altogether.

LayerX Capabilities:

- Prevent data pasting/submission.
- Detect sensitive data type (based on regex) in data submissions, and conditional blocking/restricting.
- Warn-user mode - don't block, but add "safe use" guidelines to ChatGPT.
- Full site blocking.
- Require user consent/justification to use a generative AI tool.
- Detect and disable ChatGPT-like browser extensions.

These capabilities are conditional on users/groups/roles, identities, geo-location, data type, devices and more.

For more details - contact us at info@layerxsecurity.com

KEY BENEFITS

Eliminate critical blind spots

Gain the most granular visibility into unsanctioned apps, shadow identities, DNS over HTTPS, SaaS apps and dynamic websites.

Real-time protection

Enforce access & activity policies to restrict browsing activities that expose your apps, devices, and data to compromise.

High-precision risk detection

Multilayered AI analysis of every user activity and web session flags anomalies that can indicate risk in the browser session.

Unified browser management

Manage and configure your workforce's browsers from a single, centralized interface.

Bring your own browser

Enable your users to keep on using their browser of choice for both work and personal use.

Rapid deployment

Deploy across your entire environment and integrate with browser management tools and identity providers in a single click.

WHAT ARE YOUR CHALLENGES?

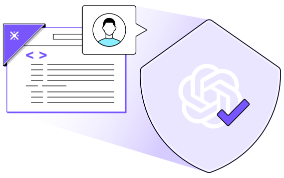
From preventing the simplest to execute yet hardest to detect web-borne attacks, through providing monitoring and governance on users' activities on the browser, and up to reducing the browsers' attack surface - whatever your challenges are – LayerX has got you covered

Web DLP

Prevent exposure of internal data in ungoverned websites and applications

- Prevention of insecure uploads
- Malicious insider protection
- Governance of data download to unmanaged devices

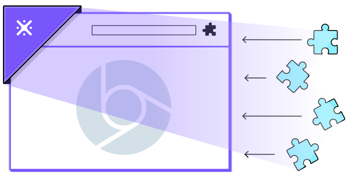
ChatGPT DLP



Mitigate any exposure risk to your sensitive data on ChatGPT and other GenAI tools

- Sensitive data paste prevention
- GenAI browser extension disablement

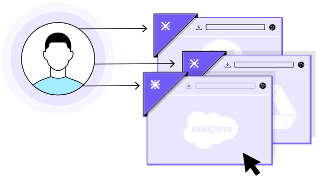
Risky Browser Extensions Protection



Block malicious or risky extensions to protect passwords, cookies, identities, and other browser-stored data from compromise

- Risky extensions detection
- Disabling the malicious extension downloading

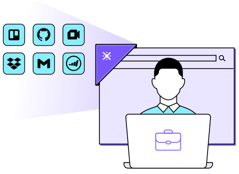
SaaS Discovery, DLP, and Protection



Eliminate shadow SaaS, prevent data leakage, and harden apps' security posture across all your sanctioned and unsanctioned SaaS and web apps

- Shadow SaaS discovery
- User account activity monitoring
- SaaS DLP
- User account security posture management

VDI and RBI Alternative



Replace costly and complex infrastructure with secure access from your users' devices

- Secure access from the browser
- Prevention of malicious access attempts
- No infrastructure costs
- Seamless user experience

Secure 3rd Party Access

Provide your external contractors with seamless access to your resources without compromising security requirements

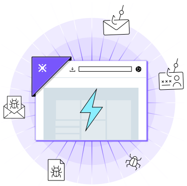
- Least-privilege access policies
- Seamless onboarding\offboarding
- Real-time malicious access blocking

BYOD Protection

Enable your workforce to securely access internal resources from unmanaged devices

- Least-privilege access policies
- Protection against on-device malware
- Security posture assessment for unmanaged devices

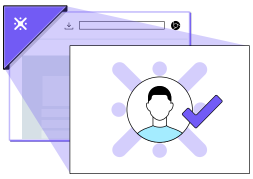
Zero-Hour Protection Against Browser-borne Threats



Gain real-time protection against all web-based attacked that couldn't be prevented before

- Browser patch management
- Phishing\social engineering pages detection
- Malicious web page activity disablement
- URL filtering
- User alerts when accessing risky web pages

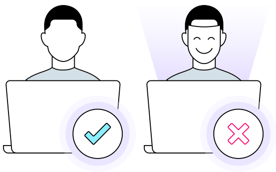
Secure Browser-based Authentication to SaaS and Web Apps



Enforce secure access to your SaaS resources without requiring VPNs or other dedicated networking infrastructure for both managed and unmanaged devices

- VPN alternative
- SaaS IdP integration
- Seamless and rapid rollout
- Least-privileged authorization policie

Identity Security Posture Management



Identify and mitigate identity weaknesses and block account takeover activities

- Identity weaknesses detection
- Shadow identities discovery
- Compromised credentials discovery
- Authentication hardening

About LayerX

LayerX is the user-first browser security platform that turns any commercial browser into the most protected and manageable workspace, with near-zero user impact, empowering hybrid enterprises to drive a true cloud-first strategy. LayerX is the pioneer of AI-based high-resolution monitoring, risk analysis and control of all users' browser activities to enable the enterprise workforce to access any web resource from any device while ensuring protection from the wide range of web-borne risks. Led by seasoned veterans of IDF cyber units and the cybersecurity industry, LayerX is reshaping the way cybersecurity is practiced and managed by making the browser a key pillar in enterprise cybersecurity.