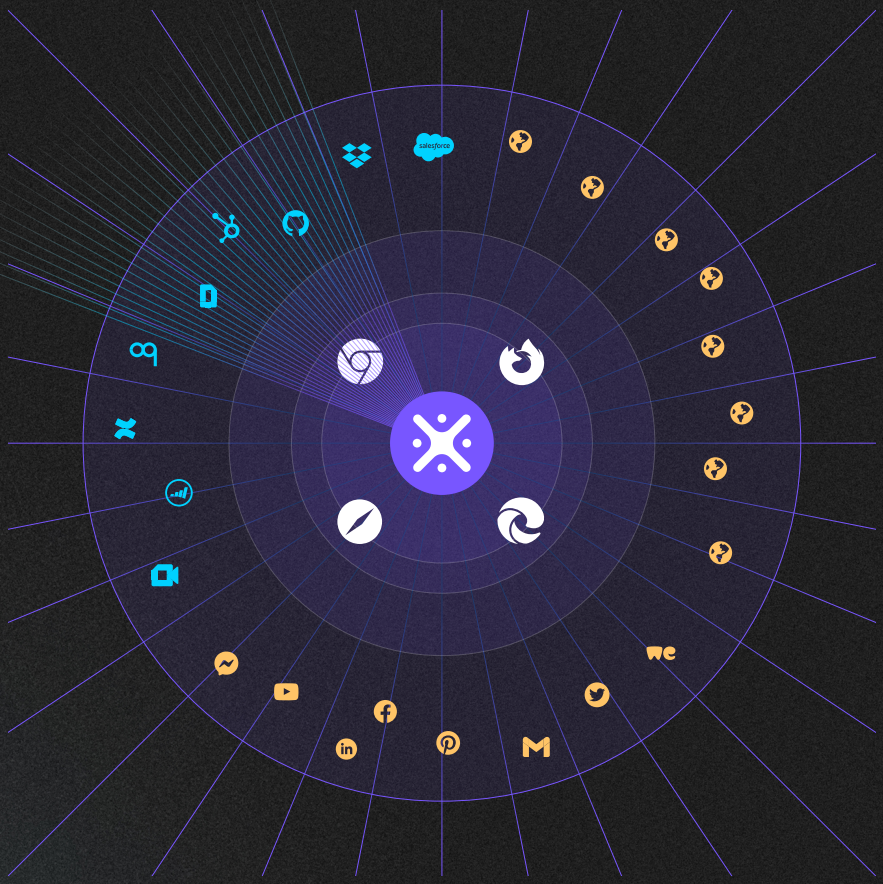
LayerX

LAYERX SECURE ENTERPRISE BROWSER EXTENSION

LayerX is an 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.

Solution Brief



INTRO:

LayerX Enterprise Browser Extension

The Threat Landscape of the Modern Workspace

The nature of the modern workspace has dramatically changed in just a few years: most business applications today are delivered as SaaS apps that can be accessed from anywhere, and host corporate data remotely. The enterprise workforce, as well, has undergone rapid evolution: most organizations today practice some form of hybrid work, utilizing a mix of internal employees and contractors. Finally, the rapid adoption of GenAI tools has introduced additional complexity with high productivity benefits alongside concerns over privacy and security.

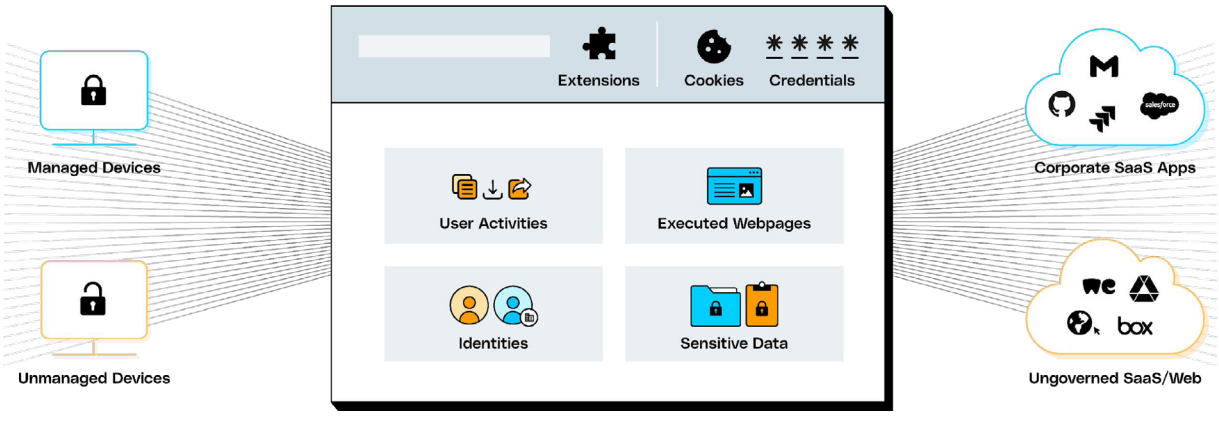
At the heart of this evolution sits the browser. As]business applications increasingly shift to a SaaS-based delivery model, the browser has become the main work interface for most employees in most organizations. Indeed, according to Forrester Research, 83% of employees believe they can perform most or all of their work through the browser.

Moreover, as the lines between corporate and non-corporate networks - and between work and personal devices - continue to blur, browsers are increasingly used as the main productivity platform for both professional and personal uses.

However, as the browser has become the main interface for work, it has also become the main point of risk for both users and organizations. The nature of the modern web exposes users to a myriad of browser-borne risks and threats, ranging from malicious web pages, web vulnerabilities and phishing attacks, to various forms of inadvertent or malicious data exposure via web, SaaS, or GenAI channels.

The problem, however, is that while the browser sits at the intersection of endpoint, network, data and identity security, no existing security solution (or combination of solutions) truly covers the browser against all forms of vulnerabilities, exploits, and data leakage that can occur within the browser.

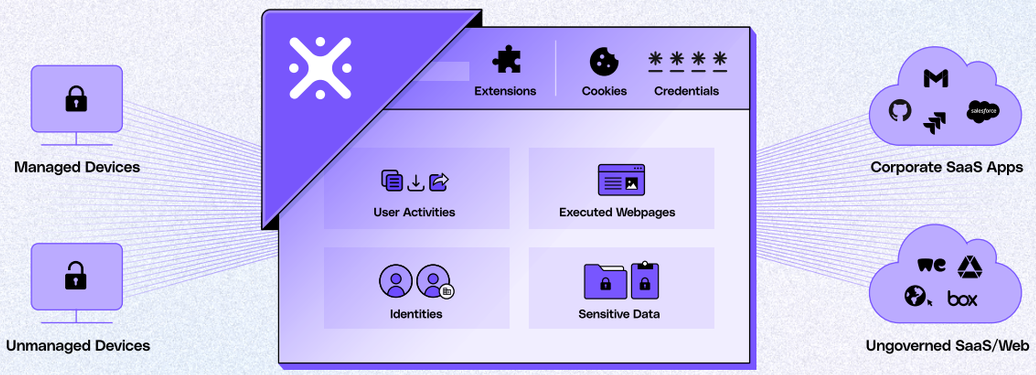
LayerX is an all-in-one, agentless security platform, delivered as a browser extension, that protects enterprises against the most critical GenAI, SaaS, Web, Identity, and Data Leakage risks and threats, without any impact on the user experience.



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.

Gen AI Security

Enable GenAI usage in the organization without worrying about GenAI data leakage

Web/SaaS DLP & Insider Threat

Block sensitive data from leaking through web and SaaS apps

Risky Browser Extensions Protection

Identify and block risky browser extensions that can steal user credentials

Secure Browsing

Defend against malicious websites, malware, phishing, credential theft, etc.

Shadow SaaS & SaaS Security

Detect all SaaS apps in the organizations and who's using them

Secure Access by BYOD/Contractors

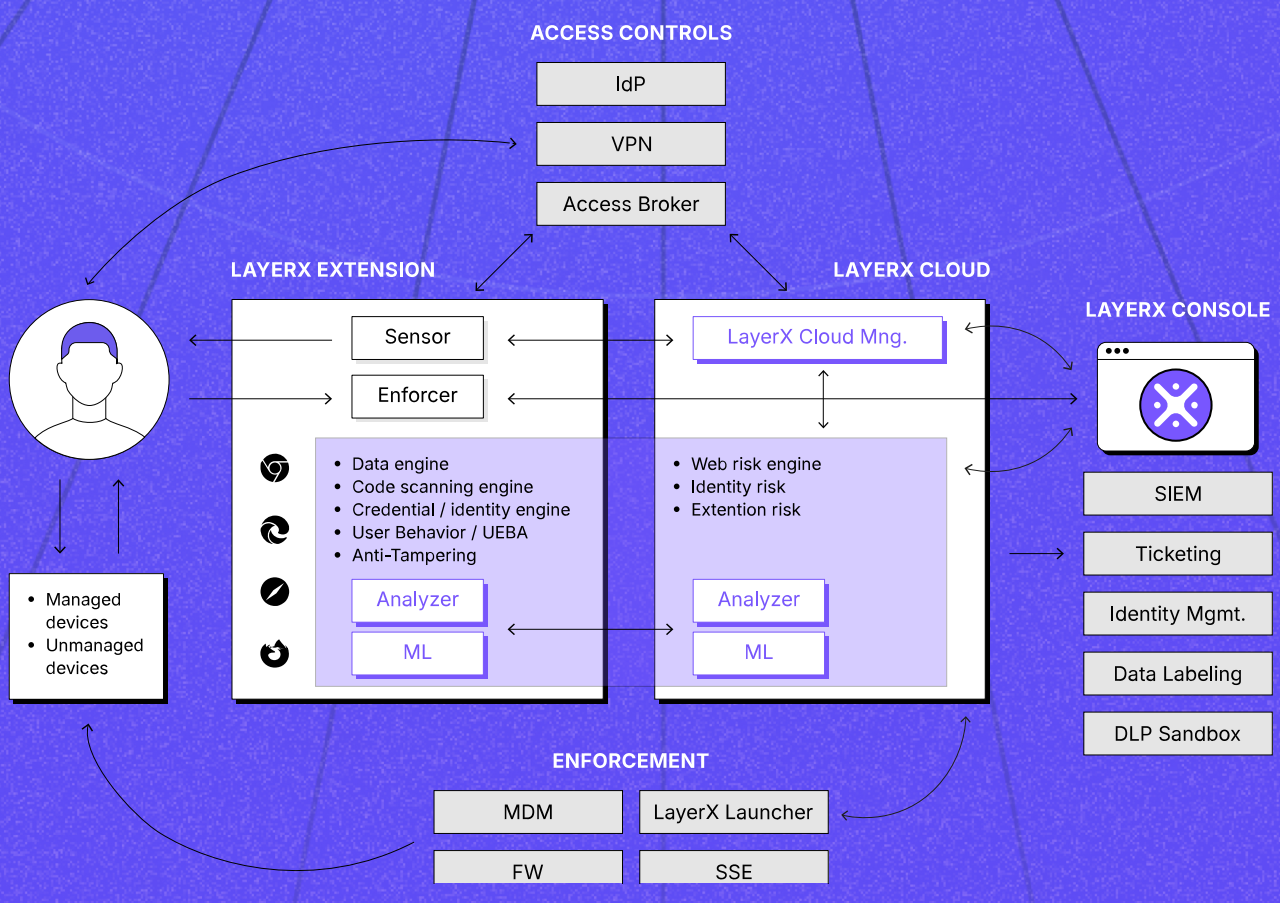
Secure remote access from unmanaged devices and 3-rd party users

Identity Protection

Secure against identity & passwords risks: password reuse, shared accounts & shadow identities

LayerX Architecture: How does it work?

LayerX analyzes web sessions at their utmost granular elements in order to prevent attacker-controlled webpages from performing malicious activities and users from putting enterprise resources at risk. All while preventing disruption of legitimate user interaction with websites, data and applications



The LayerX Platform Architecture

Extension

- **Deployed on each browser instance and profile.** For managed devices provides visibility into all non-corporate web destinations, and for unmanaged devices ensures secure access to corporate web resources.
- **Sensor:** Gathers browsing events: browser features, webpage behavior and user activity.
- **Enforcer:** Initiates browser actions and injects code to visited webpage to apply granular real time risk prevention without disrupting legitimate browsing activity.

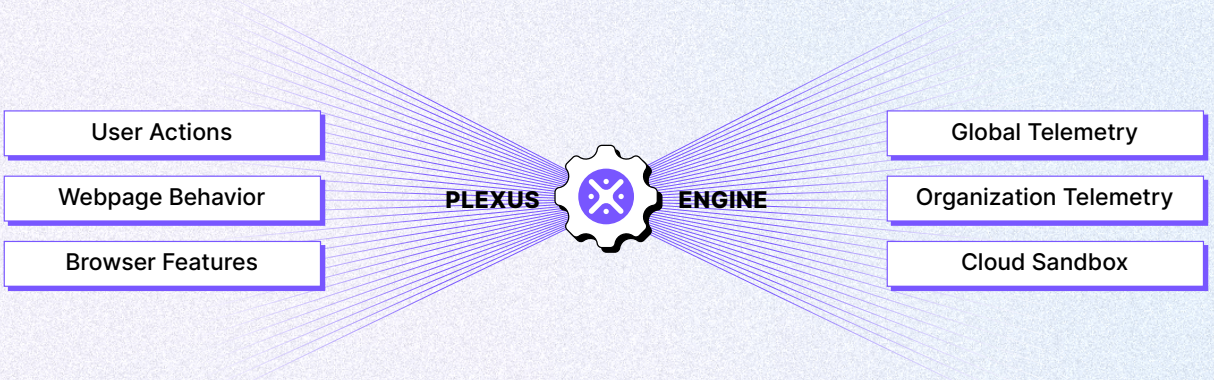
Plexus Engine

- **Extension Analyzer:** Analyzes all gathered events, assisted by enrichment feed from LayerX threat intel cloud to detect potential risks.
- **Cloud Analyzer:** Conducts on-demand enrichment based on LayerX data sources and global visibility and sends it to the extension. Increases precision with extended detection and response in the organizational level.

Cloud

- **Cloud Management:** Aggregates and processes of all Sensor-gathered events, making them available to the management console as well as passing conllustracjad policies to the Enforcer.
- **Management Console:** User interface for access and activity policy configuration, browser management, activity and usage tracking and creation of audit reports.

LayerX Plexus Engine: Deep Session Analysis

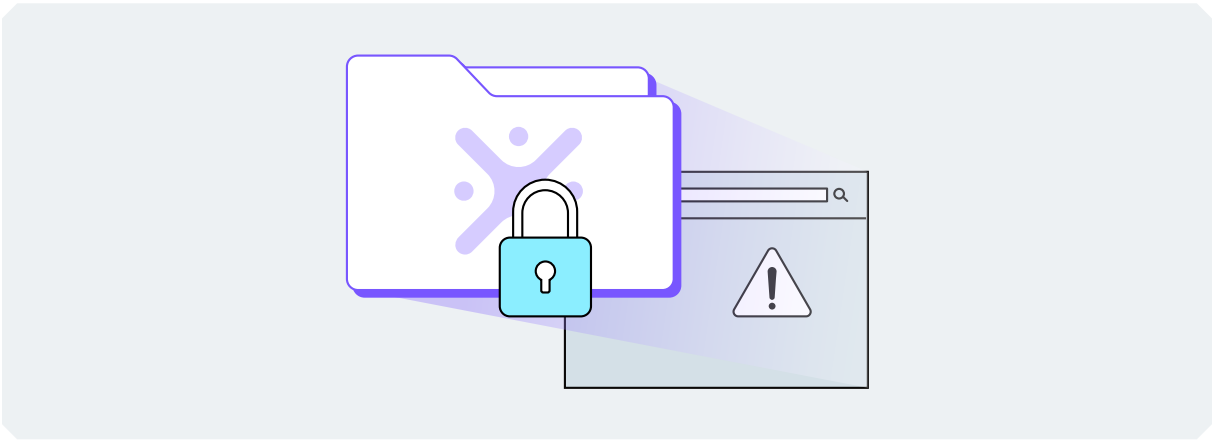


The LayerX Plexus Engine is the first purpose-built deep session analysis dual engine that operates both on the browser extension itself and in a centralized cloud service. Plexus monitors browser modifications, webpage behavior and user activities. All gathered events are analyzed in real-time and enriched by the LayerX Threat Intel cloud to reveal the risk context of every event, so protective action within the web session can be enforced.

By monitoring events at the application layer, LayerX Plexus is the first solution that goes beyond the hostname/URL level, the operational limitations of encrypted traffic analysis and API dependencies. These methods, implemented by Endpoint, Network and CASB solutions respectively, are too crude to effectively capture the wide range of granular events that comprise a modern web session, which limits their visibility and ability to protect against web-borne threats.

USE CASE #1:

Gen AI DLP



Overview

ChatGPT and other GenAI tools introduce a unique security challenge. While GenAI tools offer massive productivity benefits, users are also prone to unintentional exposure of sensitive corporate data - such as source code, customer PII, internal business data, etc. - to remote LLMs, where they might be exposed to third-parties and/or used for training of the AI models. This new risk is rapidly gaining momentum as the adoption of GenAI technologies spreads across the organization.

Gen AI DLP Challenges

For most organizations, banning GenAI tools altogether is out of the question due to its tremendous contribution to productivity. Enabling employees to use GenAI tools in a secure manner requires two capabilities:

- First, is to identify whether the data that the user inserts to GenAI tools is sensitive or not.
- Second, is to enforce controls over user actions to prevent potential exposure.

Both capabilities are challenging due to the extensive use of 'paste' as the default way to provide ChatGPT with raw data to work with.

Gen AI DLP Challenges

The key limitation of existing DLP products – endpoint and SaaS based alike - when attempting to resolve GenAI data exposure, is that their approach to data protection is file-based. As such, they acknowledge actions such as download, copy, open, and others. However, the standard way for most users to feed GenAI tools with data is by typing or copy/pasting it from existing texts. DLP products have limited to non-existing protection against pasting, making them an inefficient solution against this risk.

The LayerX Solution

Overview

The LayerX extension provides a comprehensive solution to All Gen AI Tools related data exposure. With its ability to identify every web destination and every user action in the browser, LayerX enables its users to configure Gen AI data protection policies to mitigate this risk. These policies identify an attempted insertion of sensitive data to Gen AI prompt and respond by either warning or blocking the attempt.

Monitored Events

- Text actions: text input, copy/paste
- File activities: file upload/download
- Application access
- User authentication
- Installed AI-enabled extensions

Sample Capabilities

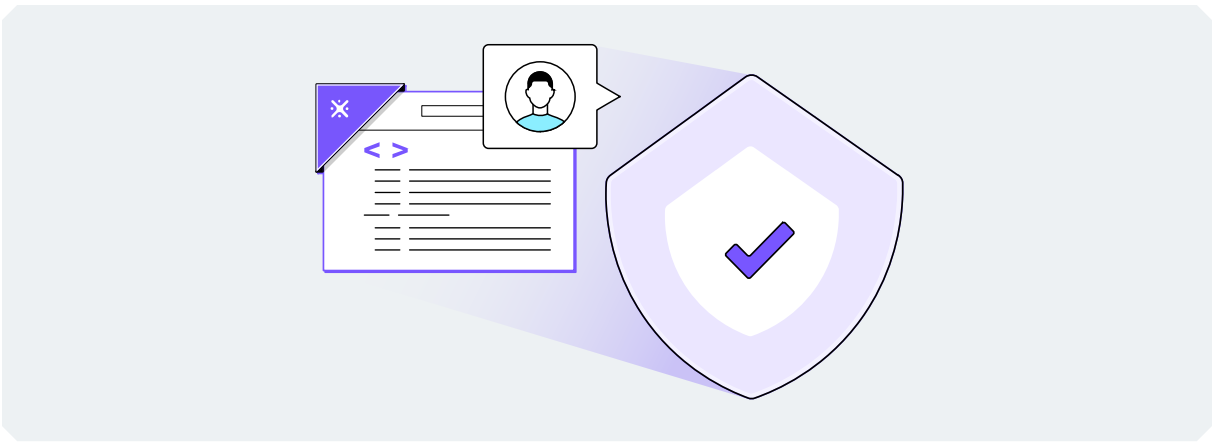
LayerX provides a wide range of GenAI data protection policies to adjust to organizations' different needs and enable them to assign different protection levels per users or groups. Balancing between these controls allows organizations to enjoy the benefits of GenAI tools without compromising security.

› **Examples of policies that organizations can define**

- Block access to non-sanctioned AI applications
- Prevent access to AI tools such as ChatGPT using non-corporate accounts (i.e., so users will be able to use only the sanctioned enterprise accounts and not their personal accounts that are used for LLM training)
- Prevent text functions such as text input or copy/pasting
- Preventing file upload of sensitive data (e.g., upload a file containing sensitive customer data for data analysis)
- Prevent/disable installation of AI-enabled browser extensions that extract user browsing data to unknown external LLMs

USE CASE #2:

Risky Browser Extension Protection



Overview

Malicious browser extensions have become a leading attack vector. Users are easily lured to download and install them, as they are often disguised as benign software distributed in legitimate marketplaces. Once installed on the browser, they can serve various purposes, most prominent of which are stealing browser credential data, such as passwords, cookies, and MFA tokens. By this, malicious extensions facilitate adversaries' ability to perform account takeover attacks.

Risky Browser Extension Protection Challenges

There are two core approaches that can be implemented against malicious extensions: either to prevent the initial download and installation of risky extensions, or to continuously scan the device to detect and disable unauthorized extensions. Neither of these capabilities are part of the core set of capabilities of existing MDM or endpoint security solutions.

Limitations of Existing Security Solutions

- **Active Directory**

  While it is possible to set up a Group Policy for each different browser that allows, blocks, or whitelists extensions, the policy setup process varies between the different browsers and can be very complicated for some.

- **EDR\EPP\NGAV**

  Theoretically, various endpoint protection products are ideal for guarding from malicious browser extensions. Unfortunately, these products don't include such extensions in the pool of threats they protect from.

The LayerX Solution

Overview

LayerX's extension automates the discovery of all risky extensions and provides real-time monitoring and protection against their malicious activities. LayerX enables its users to disable all the discovered extensions to neutralize any malicious action they might perform. Unlike existing solutions that trigger allow/block based on the extension ID alone, LayerX bases its decision on a far more granular analysis of the browser extension, including attributes such as their permissions, access, install type, last updated at, browser store, extension risk and many more.

Monitored Events

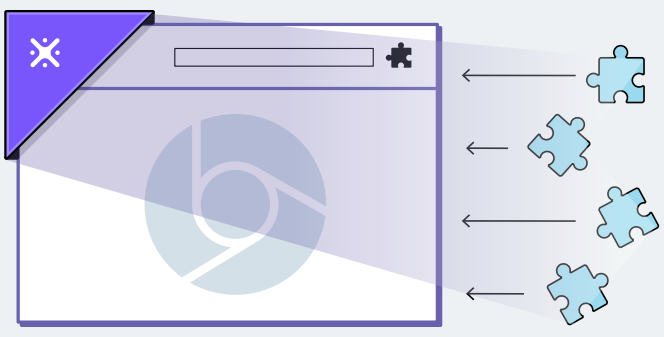
- Existing installed extensions
- Download and installation of new browser extensions
- Permissions allowed for each extension

Sample Capabilities

- Discover / audit all browser extensions across all browsers, devices, and users
- Evaluate and assess the risk for each browser extension, based on its permissions and other attributes such as source, installation type, number of download, etc.
- Define Granular enforcement based on risk (e.g., disable all AI-enabled browser extensions that have a 'High' or 'Critical' risk score)
- Configure policies to continuously scan your workforce's devices for newly installed browser extensions, determining whether they are allowed, and alerting IT and security teams if a risky extension is in place.
- Disable extensions' ability to extract credentials or other sensitive data from your workforce's browsers. These proactive policies ensure that even when malicious extensions are not yet removed, their ability to cause harm is disabled.
- Disable existing risky extensions completely, and/or prevent the installation of new risky extensions

USE CASE #3:

SaaS Discovery , DLP, and Protection



Overview

SaaS apps are the leading work interface in the modern enterprise. In practice, employees use two types of SaaS apps: sanctioned apps that are centrally managed by the organization and unsanctioned public apps that employees choose independently to assist them with their tasks. It's imperative for every organization to have full visibility into their workforce's usage of each type, ensure that sensitive data is not being exposed in them, and continuously monitor their security posture.

SaaS App Security Challenges

SaaS application security requires security and IT teams to be able to discover all applications in use, map all user accounts and identities, monitor account and identity activity, ensure that there are no stale or shadow users and protect sensitive data on these apps from illegitimate access and exfiltration. While this is partially achievable for sanctioned apps, it's out of scope for unsanctioned ones.

Limitations of Existing Security Solutions

› **Cloud Secure Access Brokers (CASB):**

Reactive Monitoring and Protection Only for Fully Sanctioned Apps

CASB solutions are, by design, limited in their protection coverage:

- **Business usage of Sanctioned Apps Only:** CASB protection applies only to fully sanctioned apps, i.e. enterprise apps that have a detailed API that provides the CASB with visibility and governance into user activities within the app. All other SaaS types, semi-sanctioned (enterprise apps with no API), federated sanctioned (a personal app that is used with an enterprise identity) and unsanctioned apps (personal app and identity) are beyond the scope of CASB protection. Moreover, CASB can't identify a personal usage in a sanctioned app. for example, if Google Drive is sanctioned but the user is using his personal Google Drive, the CASB won;t have a way to differentiate the personal use from the business one.
- **Reactive and Partial Protection Even for Sanctioned SaaS Apps:** CASB dependency on the protected apps' API creates a critical lack of consistency in the level of visibility between different apps. Another result of this dependency is that CASB activity policies for mitigating detected malicious activity are, by design, reactive and with limited ability to prevent such activity in real-time.

› **Network Solutions (Firewalls, SASE, Proxies, etc.):**

No Visibility Into User Activities With Accessed Apps Forward proxies have the ability of preventing access to both sanctioned and unsanctioned apps based on policies. However, they don't have any visibility into the actual activities performed by the logged user within the app it accesses. This means they are limited and can only determine whether to allow access to a given app or ban it altogether.

The LayerX Solution

Overview

LayerX monitors SaaS-related browsing events to discover all apps, users and identities within the SaaS environment, gain insights into each user's activity and behavioral patterns and prevent data theft/leakage.

LayerX is the first solution that delivers the same level of visibility and protection to all SaaS apps used by the enterprise's workforce, sanctioned, semi-sanctioned, federated sanctions and fully unsanctioned, securing your environment 'as is' with no need for an infrastructure change or requiring time-consuming configurations.

Monitored Events

LayerX leverages its visibility and enforcement capabilities on browsing events at the application layer to monitor the following events:

- SaaS application access
- User interaction and activity with SaaS applications
- Authentication details to each SaaS application, including the user account, identity and credentials used to access it
- OAuth permissions granted to SaaS applications
- Data submission
- File activity: Share/download/upload/view

By monitoring these events, LayerX creates a granular behavioral profile for every user, to detect any anomalies that indicate a potential risk, at the highest precision.

Sample Capabilities

The following capabilities are applied to both sanctioned and unsanctioned apps:

› **Auditing Reports:**

- Discovering all sanctioned and unsanctioned SaaS apps in use.
- Mapping each user account's activities, including their identity, login method, and usage patterns.
- Discovering 'shadow' identities (of non-corporate or non-SSO identities) used to access SaaS applications

› **Adaptive Activity Policies:**

- Alerting or blocking user access to the SaaS app upon detection of anomalous activity that may indicate an account compromise, malicious app activity or malicious data interaction.

› **SaaS Security Posture Management**

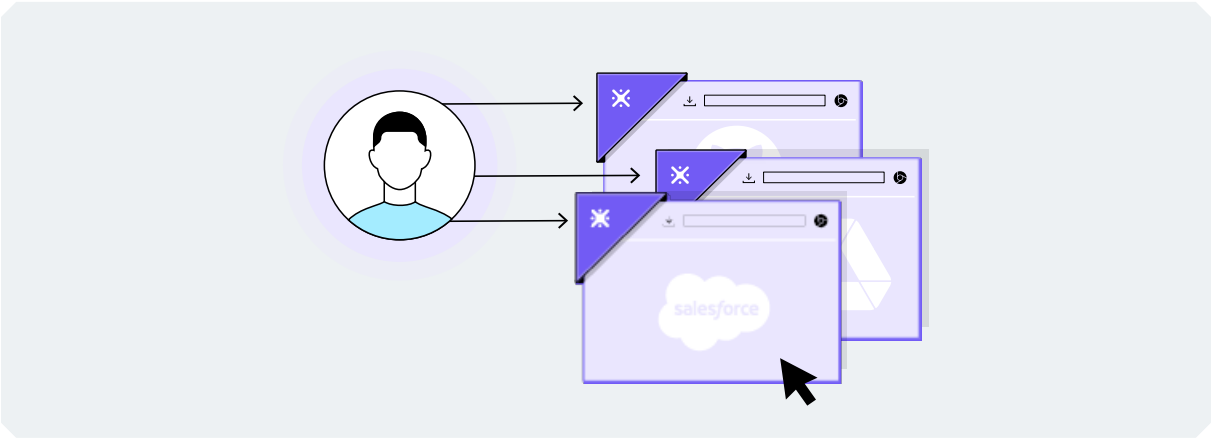
- Continuously monitoring applications, accounts, identities, and credentials to detect vulnerable accounts and account sharing and enhancing their security.

› **Data Protection Policies:**

- Enforcing SaaS security governance on SaaS accounts and identities, including password strength, restricting password re-use, shared accounts, requiring SSO on all corporate accounts, etc.
- Restricting activity on non-corporate SaaS applications, and/or restricting the data that can be uploaded to those applications
- Configuring policies to govern every data interaction between the user and the application (including copy, paste, upload, download, and submit) to prevent data loss through unauthorized or vulnerable applications.

USE CASE #4:

Identity Security Posture Management



Overview

User identities have become the most targeted attack surface today. Adversaries seek compromised credentials to gain access to corporate resources, with extreme focus on SaaS and web apps. To proactively confront these efforts, organizations must ensure that basic password hygiene is practiced and that their identity and security teams have the ability to easily identify and resolve weaknesses that make accounts more susceptible to compromise.

Identity Security Posture Management Challenges

While organizations typically have good visibility to corporate identities that go through their Identity Provider (IdP), SaaS applications often introduce two types of 'shadow' identities that do not go through the IdP:

- Non-corporate identities - by definition, these are non-corporate identities that do not pass through the IdP.
- Corporate identities not backed by SSO - corporate accounts that login to SaaS applications using a password, not backed by their corporate IdP.

While SSO-backed corporate accounts are subject to the authority of the IdP, which provides visibility, governance and control over those accounts, 'shadow' accounts are outside of the jurisdiction of the IdP, which cannot enforce control over them. The problem, however, is that in a SaaS-first environment, 'shadow' identities are often used to handle corporate data, but the organization is unable to have visibility or contorl over their actions.

Limitations of Existing Security Solutions

Cloud identity providers or federation servers can provide limited insight into users' security posture. However they were not built for this task. To gain comprehensive insight into a user's actual exposure to compromise, you need to manually assemble data from various places.

The LayerX Solution

Overview

The LayerX extension provides a single, centralized interface for viewing users' identity security posture, enabling identity and security teams to identify and prioritize the weaknesses that need to be resolved.

Monitored Events

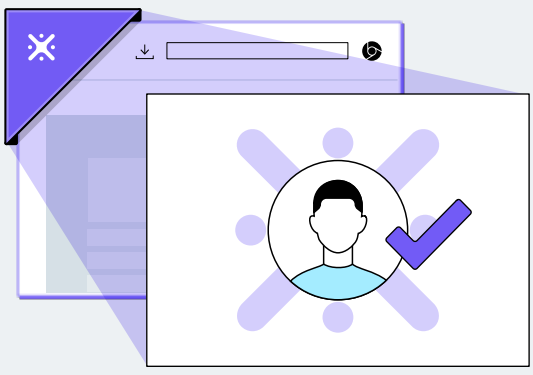
- User accounts and identities
- User profiles
- Credential usage
- Credential sharing (among multiple users)
- Password strength
- Password re-use
- OAuth permissions
- SSO status

Sample Capabilities

- Monitor for weaknesses in your identity posture, such as compromised or reused credentials.
- Discover 'shadow' or non-corporate identities that have access to your internal resources.
- Prevent access by non-SSO-backed corporate identities to SaaS website
- Identify potentially compromised user accounts
- Apply last-mile controls based on risk assessment (e.g., prevent access by users who have weak passwords until they change their passwords)
- Identify security governance gaps (weak passwords, reused passwords, shared accounts, etc.)
- Using LayerX as a mandatory authentication factor to eliminate account takeovers

USE CASE #5:

Web/SaaS DLP and Insider Threat Protection



Overview

Web-based file-sharing websites and SaaS applications are ubiquitous among users and organizations, making it the easiest and most convenient channel for inadvertent or purposeful leakage of data. Employees' web activities introduce two main risks to sensitive corporate data. The first is data uploading to ungoverned web destinations. The second is downloading data from corporate SaaS apps to unmanaged devices. In both cases, the result is the transfer of corporate data from its initial monitored and protected location, to a new location that is not subject to the corporate's data protection policies, putting it at risk of exposure.

Web DLP Security Challenges

Traditionally, data leakage protection was heavily focused on file activity at the endpoint level, where access to local applications could be controlled at the process level. However, the move to SaaS applications introduced new complexities:

- File upload to individual websites and/or SaaS applications, where in some contexts, such activity might be legitimate, and in other cases it may not (for example, logging in to a file-sharing application using the user's corporate identity vs. their perosnal identity).
- Non-file-based data activities, such as text input or copy/paste, which are not saved within local files (for example, copy/paste of sensitive data within Office365, from a user's corporate account to their personal account).

Limitations of Existing Solutions

Web-based data leakage is well beyond the scope of existing DLP solutions. This is mainly because they assume a level of control over the space where the data interaction takes place – the endpoint itself, a sanctioned app, and others. DLPs are insufficient if the risk involves either an unsanctioned app or an unmanaged endpoint.

› **Endpoint DLP**

Traditional DLP solutions scan files for tags or other identifiers that mark them as sensitive, so they can either block, warn, or audit when the file is copied, printed, printed, or opened in an insecure manner. For example, when copied to a USB drive, network share, RDP session, etc. However, they don't have the ability to discern between different web locations, materially limiting their ability to prevent upload to insecure web destinations.

› **CASB DLP**

SaaS DLP solutions, by design, are limited to monitor and control usage over sanctioned SaaS apps alone, to which they connect via API. Any user interaction with unsanctioned web destinations is beyond their scope of coverage.

The LayerX Solution

Overview

The LayerX extension provides a full-featured web DLP solution that enables data protection teams to configure policies to prevent, warn, or audit any download or upload activity that puts sensitive data at risk.

Monitored Events

- File upload/download
- Endpoint state (managed/unmanaged)
- Target SaaS application (sanctioned/unsanctioned)
- User data interactions
- Local file data labels (E.g., "Sensitive," "Confidential," "Partner," etc.)

Sample Capabilities

- Prevent copying files with sensitive data to external SaaS services (e.g., Google Drive, OneDrive, Dropbox, etc.)
- Prevent file sharing using unsanctioned file-sharing services
- Restrict login and activity on multi-tenant SaaS apps (e.g., Google Drive), and make sure that corporate data is uploaded only to corporate accounts
- Provide visibility and control on both managed and unmanaged devices, and make sure that 3rd-party contractors aren't leaking data

USE CASE #6:

Zero-Hour Protection Against Web Vulnerabilities

Overview

The recent years have witnessed a steep escalation in the volume and sophistication of attacks that lure users to malicious webpages. The basic malicious capabilities of the redirection chain and file download were replaced with fully-geared malicious SaaS applications that make use of modern web page capabilities. This attack vector transformation is forcing security stakeholders to reevaluate their traditional defense methods and seek more efficient protection.

Web Protection Challenges

Security and IT teams need to detect, prevent and respond to a wide range of web-based threats: credential access via phishing pages, downloading of malicious files, and malicious code execution. The existing tools within the standard security stack fall short in this sense.

Limitations of Existing Security Solutions

› **URL/DNS filtering:**

Extremely partial protection due to dependency on known network addresses. This method can be implemented on a web gateway/firewall as well as on the endpoint itself. It examines URLs or DNS queries and blocks them, based on threat intelligence feeds. The main limitation of this method is that in order to prevent access, the solutionmust know in advance that an address is malicious. This provides attackers with an ability to constantly change the address of their controlled webpages, resulting in the vast majority of malicious web pages being out of the protection scope.

› **Deep packet inspection and session emulation:**

Degraded user experience due to latency and inability to detect malicious webpages with emulation detection capabilities. This method attempts to complement the first by executing the requested webpage within an isolated environment to monitor its actual behavior and detect signs of malicious features. The main limitation of this method is that decrypting network packets takes time, which degrades the user experience and cannot be applied to all suspicious page requests, inevitably leading to partial protection. Moreover, the protection is partial even for the portion of web pages that do get inspected, due to malicious web pages' ability to detect that they are running in an emulated environment and respond by avoiding any activity that may be interpreted as malicious

The LayerX Solution

Overview

The LayerX browser provides the full lifecycle of browser protection, from proactive hardening of the browser's security posture to real-time detection and prevention of threats. LayerX monitors browser sessions at the application layer, gaining direct visibility into all browsing events at their post-decryption stage and enabling the analysis and enforcement of protective actions in real-time with no latency or impact on the user experience. LayerX can seamlessly modify the rendered web page to go beyond crude block/allow access and deliver granular enforcement that neutralizes the malicious aspects of the web page, rather than blocking access altogether. This is of critical importance when attackers mount their attack on an essentially legitimate page, such as when traversing the DOM structure of a banking app page. LayerX provides the highest level of security without degrading the user's browsing experience.

Monitored Events

LayerX leverages its visibility and enforcement into browsing events on the application layer and protects against phishing attacks and malicious web pages by monitoring the following events:

- Modify/create/remove of cookies, cache, downloads, passwords submission.
- History, form data.
- Modify the website's ability to use cookies, JavaScript and plugins.
- Page Interaction: Keyboard/track mouse/bind on input buttons/submit/paste/copy.
- Enable/disable 'do not track' privacy sandbox.
- Modify proxy settings.
- Allow/block Camera notifications, images, cookies, JavaScript, fullscreen, microphone, popups, location, automatic downloads.
- Browser version

Sample Capabilities

Enforcement of browser patching to prevent exploitation of known vulnerabilities

› **High Precision Threat Detection Without Relying on Prior Knowledge:**

- Detecting website activity that indicates malicious intention to trigger either alert or active enforcement policy.
- An independent ML engine that performs real-time analysis of each accessed web page with zero latency.

› **Real-time Granular Enforcement With Near-zero User Experience Impact:**

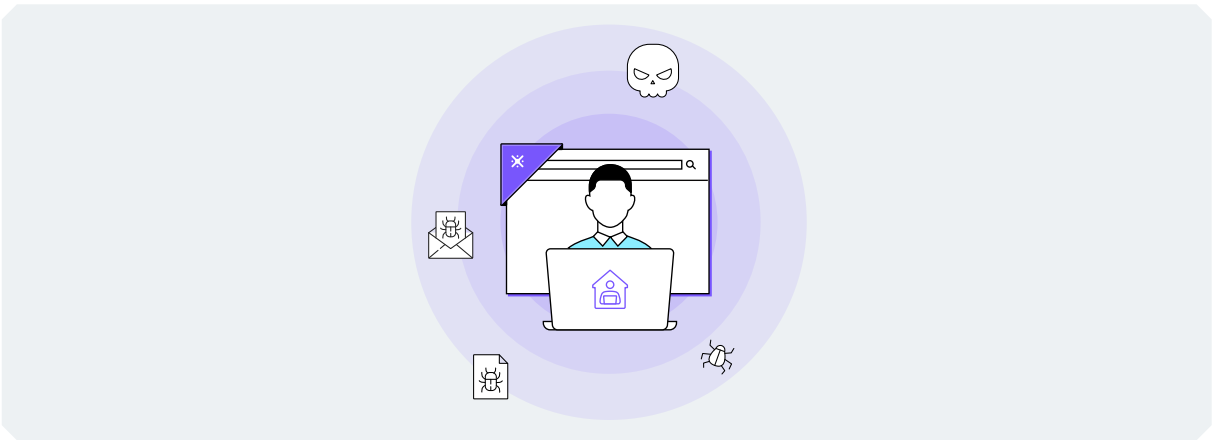
- Modifying any component within an accessed web page to pinpoint malicious activity and preventing its interaction with the browser.
- In the case of a legitimate page - enabling the user to continue browsing without interruption.
- Just-in-Time prompting to alert users prior to accessing risky web pages.
- Prevention of user access to malicious web pages by using URL filtering that is based on the most updated threat intelligence feeds.

› **Enhancing Protection of Email Security Solutions:**

- Replacing session emulation with continuous scanning of the behavior and actions of pages that were accessed via email links, across both corporate email and personal webmail, blocking any detected malicious activity in real-time.

USE CASE #7:

Secure Access to SaaS and Web Apps for Remote Employees, 3rd-Party Contractors, and BYOD Devices



Overview

The modern workplace has evolved beyond the traditional model of corporate devices behind a network perimeter. Modern organizational networks routinely include a combination of internal users within the network perimeter, corporate users working remotely, and external 3rd-party contractors. In addition, it includes a mix of managed and unmanaged devices, including employees' personal devices, which are allowed under BYOD policies. Therefore, to fully realize the productivity potential of its workforce, today's enterprise must enable access to both public and internal web applications from any user or device, regardless of their location and without downgrading the level of protection for sensitive data.

Secure Authentication Challenges

- **Remote and External Users:** All resources that reside in the public cloud are inherently exposed to malicious access via compromised credentials. To mitigate the risk, organizations must implement an 'assumed breach' approach, eliminating any implicit trust and enforcing continuous risk analysis and adaptive policies on all users' access and activity across their SaaS environment.
- **Unmanaged Devices and BYOD:** Unmanaged devices are typically more vulnerable to compromise by threat actors since organizations cannot enforce local endpoint security posture such as disk encryption or password policies, or mandate the usage of endpoint security solutions such as anti-virus, EDR/XDR, etc.

Limitations of Existing Security Solutions

Authentication

- **External SaaS Applications:** For users using external SaaS applications, authentication is a challenge since access is governed by the SaaS application itself. Corporate users using SSO-backed accounts will have authentication and access managed by the organizational IdP, but 'shadow' identities based on personal accounts or non-SSO corporate will not be visible to IdP services.
- **Internal SaaS Applications:** For internal SaaS applications, the organization can require access from within the internal network only. However, this typically requires users to log-in to the network via VPN or zero-trust access, adding latency and overhead to user access.

Enforcement

Unmanaged devices, by definition, lie outside the organizations' scope of control. Therefore, policies enforced by access management or MDM solutions will not be applicable for remote or external users on unmanaged devices. As a result, once users on unmanaged devices are granted access to SaaS applications, there are no controls on their activity within the SaaS application, data they extract from the application, or what they do with this data on their local endpoint.

The LayerX Solution

Overview

LayerX enables leveraging the browser as an additional authentication layer for accessing corporate SaaS apps, across both managed and unmanaged devices. LayerX can also enforce consistent and granular authorization policies across all SaaS apps to mitigate excessive access privileges and integrate with the cloud identity provider to require additional authentication or MFA verification when accessing sensitive resources. Enabling secure connection to SaaS apps through the users' browsers eliminates the need for costly and slow VPN connection and provides users with secure seamless access.

Monitored Events

LayerX leverages its visibility and enforcement capabilities on browsing events at the application layer to monitor the following events:

- **Authentication:** User logins to SaaS apps
- **Authorization:** Resource access (varies per specific app)
- **Device status:** Managed or unmanaged
- **User activity:** All user actions within the SaaS application
- **File activity:** File upload/download to/from the application
- **Data activity:** Text input, copy/paste, printing, etc.

Sample Capabilities

LayerX integrates with your cloud identity provider of choice to provide the following capabilities across both managed and unmanaged devices:

- Configure access policies that allow access to a SaaS app only through the LayerX extension (with LayerX acting as an additional authentication factor). No agents required and no interruption to the user's authentication flow.
- Enforcing least-privilege policies to allow access to SaaS applications or corporate resources.
- Trigger additional verification when risk is detected, based on LayerX's granular visibility of the user's activity within the app.
- Restrict user activities within the SaaS application on an unmanaged device, such as preventing file download to the unmanaged endpoint, preventing printing, adding watermarks to all screens, etc.
- Preventing any malicious device-website interaction that may be initiated by on-device malware.

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 provides continuous monitoring, risk analysis, and real-time enforcement on any event or user action 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 other solutions can't protect against.

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

GenAI Security
Map GenAI usage in the organization, discover 'Shadow' AI 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 web-based SaaS and file-sharing apps and enforce controls on file-based and file-less data

Zero-Hour Web Protection
Scan every code element in real-time 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

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