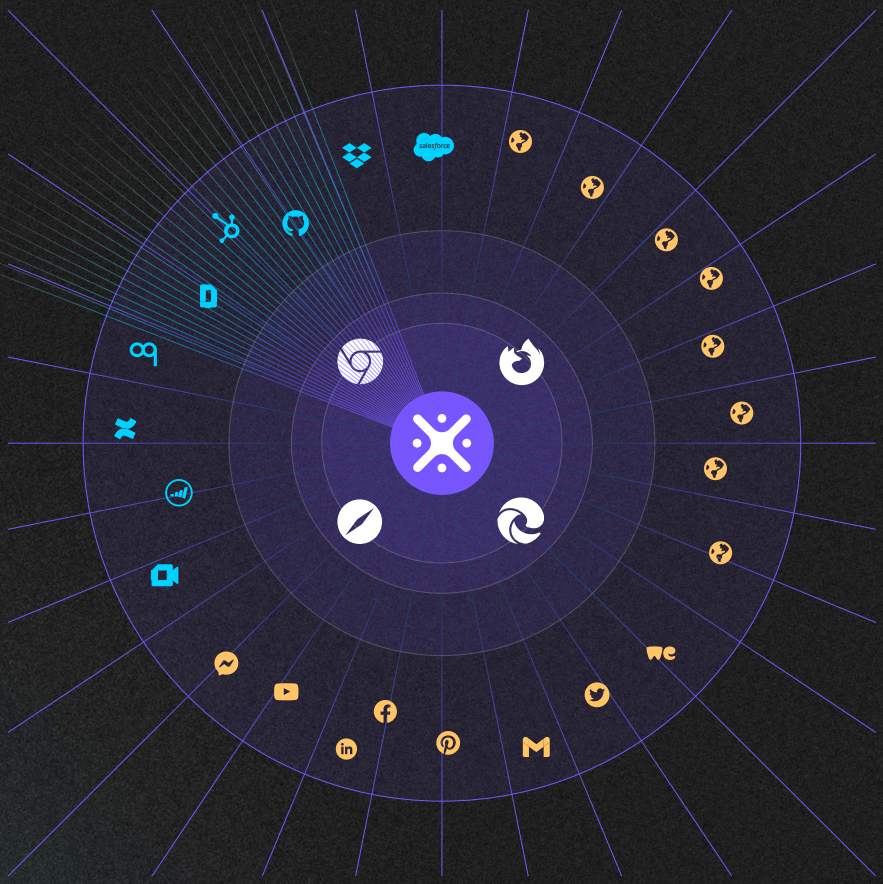
LayerX

LAYERX BROWSER SECURITY PLATFORM

Solution Brief



INTRO:

Layerx Browser Security Platform

The Browser Security Challenge

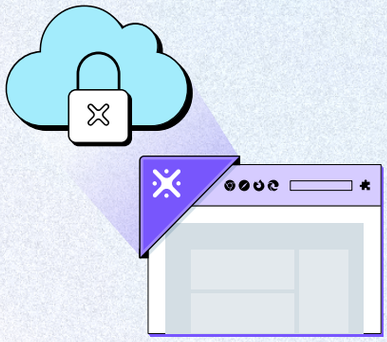
The browser has become the core workspace of the modern enterprise since it is the exclusive access interface to anything on the web, from managed SaaS applications to unsanctioned apps and websites. Moreover, the browser is a unique intersection point: between the on-premises environment and the web, as well as between partially controlled web assets, such as managed SaaS applications, and assets that are by-definition beyond the control of the enterprise's IT and security teams.

However, the browser threat landscape has far outpaced the security measures that were traditionally used to protect the enterprise from these web-borne threats and risks. Network-based solutions, for example, can no longer reliably prevent data exposure in SaaS or web apps, nor can they single out malicious web pages and block employees from accessing them. Endpoint protection products fail to prevent the prominent attack vector of installing malicious browser extensions on targeted devices. CASB solutions' protection is limited to sanctioned apps alone and so on and so forth.

The reason for this limited security scope is simple - the solutions in today's security stack were designed and built before the transformative evolution of web technology and the establishment of the browser's leading operational role in the modern enterprise. In addition, today's perimeter- less hybrid work environment has resulted in many enterprise resources being partially or completely out of IT and security teams' direct control. As a result, organizations today are exposed to a wide array of threats and risks that they lack means to mitigate.

When existing solutions cannot mitigate new security challenges, it's time to develop a new one that can help enterprises strengthen their security posture in the face of modern threats and risks.

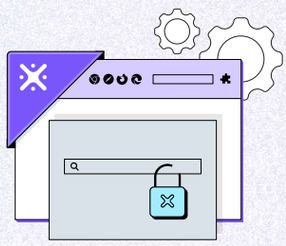
The LayerX Vision: Turn Any Browser Into the Most Secure and Manageable Workspace, While Maintaining Top User Experience, to Enable a True Cloud-first Strategy



The steep rise of browser usage and its prominent role in the modern enterprise calls for a re-evaluation of the entire security stack. As the main workspace and access point to enterprise resources, all browser-related risks should be addressed collectively in a single solution that fully monitors and governs browsing activity.

Comprehensively protecting the browser introduces an opportunity to regain lost control over enterprise resources and leverage all the production potential the web offers, while maintaining the highest level of security for enterprise data and resources. In that manner, a single browser security platform can remove both the security and management concerns that bar the way of full cloud migration, enabling enterprises to become truly cloud-first.

The LayerX Mission: A User-first Browser Security Platform



To turn this vision into reality, LayerX pioneers the only user-first browser security platform that is purpose-built to provide real-time high-resolution visibility and governance of user activities across all commercial browsers, while protecting from browser-related risks to enterprise data, applications and devices. The LayerX ability to identify both websites' and users' actions at the highest granularity enables the platform to single out only the activities that introduce risks and mitigate them.

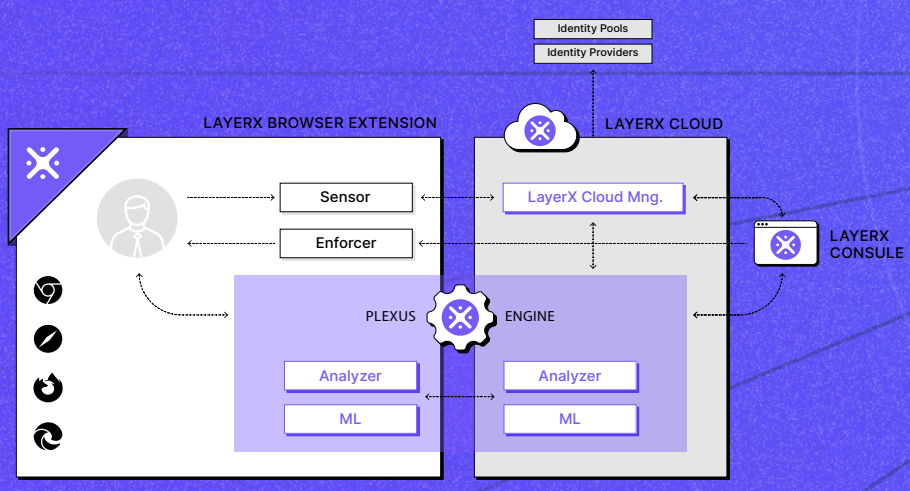
This enables the security team to confidently enforce secure usage but with near-zero impact on the user experience.

Granular visibility into user actions prevents the risk of data compromise and leakage. But LayerX also goes beyond and fundamentally changes the way enterprises manage their attack surface. The platform enables IT and security teams to easily grant secure, least-privileged access and a Zero Trust approach through access policies of the browser itself.

Being user-driven, the platform's protection is implemented at the browser's user profile/identity level, providing its full set of capabilities from anywhere users access the web, regardless of if their device is managed or not.

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.

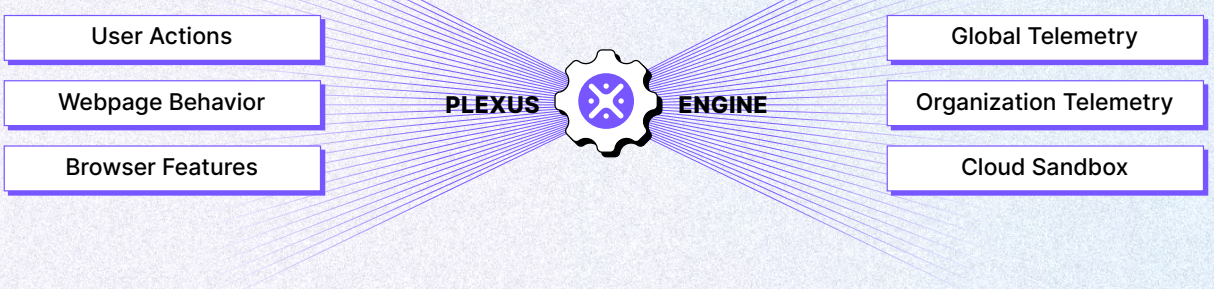
Plexus Engine

- **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 configurated 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 Cases

Overview

LayerX use cases address the three key aspects of browser security:

The browser itself - reducing the browser's attack surface to proactively prevent threat actors from compromising the host device or the data that resides within the browser application itself, like cookies, passwords and more.

The data users interact with via the browser - monitoring and governing users' activities on the browser across the wide array of sanctioned and unsanctioned SaaS apps and web destinations. This ensures that no corporate data is exposed while also detecting and blocking malicious activity related to account takeover.

Web pages used as an attack vector - detecting and preventing malicious activity of attacker-controlled web pages users visit through real-time ML-based analysis of their behavior and various web components.

USE CASE #1:

Web DLP

Overview

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 transit 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

The web is beyond the control and governance capabilities of the security team. Unlike internal SaaS or web apps, where visibility and rules can be applied, websites and other locations across the public Internet are not easily protected. Blocking employees from accessing the web destinations they desire is not an option due to the heavy disruption to productivity it entails.

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, 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
- Data copy/paste
- Endpoint state: managed/unmanaged
- Target app (sanctioned/unsanctioned)
- User data interactions

Capabilities

- Configuring data protection policies to control data upload from employees' managed devices to any app that is not included in the 'trusted apps' list.
- Configuring policies that detect that an organizational app is being accessed from an unmanaged device and controlling the ability to download data to it.
- Monitoring and profiling users' data interactions to detect deviations that might indicate a malicious insider's data exfiltration attempt. Such a deviation triggers a data control action to prevent either its download to an unmanaged device or its upload to an unsanctioned app.

USE CASE #2:

ChatGPT DLP

Overview

ChatGPT and other GenAI tools introduce a unique data protection challenge. Employees, in their attempt to increase productivity, are prone to unintentional pasting of sensitive information – source code, internal business data, etc. Each such paste exposes the pasted data, making it potentially available for anyone. This new risk is rapidly gaining momentum as the adoption of ChatGPT spreads wider across the organization.

ChatGPT DLP Challenges

For most organizations, banning ChatGPT altogether is out of the question due to its tremendous contribution to productivity. Enabling employees to use ChatGPT in a secure manner requires two capabilities. The first, is to identify whether the data that the user inserts to ChatGPT is sensitive or trivial. The second, is to enforce a protective control 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.

Limitations of Existing Security Solutions

The key limitation of existing DLP products – endpoint and SaaS based alike - when attempting to resolve ChatGPT-related data exposure risk, is that they are only built to protect files. As such, they acknowledge actions such as download, copy, open, and others. However, the standard way for most users to feed ChatGPT with data is by 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 ChatGPT-related data exposure. With its ability to identify every web destination and every user action in the browser, LayerX enables its users to configure ChatGPT data protection policies to mitigate this risk. These policies identify an attempted insertion of sensitive data to ChatGPT prompt and respond by either warning or blocking the attempt.

Monitored Events

- Text actions: paste, fill, type
- Accessed app
- Installed extensions

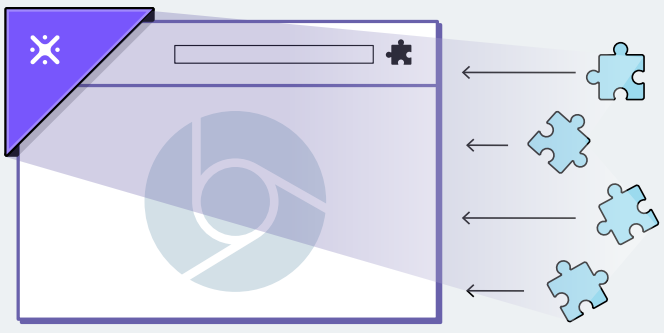
Capabilities

LayerX provides a wide range of ChatGPT 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 enables getting the best of ChatGPTs' benefits without compromising security.

	ChatGPT Action		
	Access	**Data Insertion (type, paste, fill)**	
		Any Input	Sensitive data Input Only
Block	No access is allowed	Chosen action is disabled	Chosen action is disabled for sensitive data input
Warn User	Access allowed but with a data exposure warning pop up	Chosen action is allowed but with a data exposure warning pop up	Chosen action is allowed for sensitive data input but with a data exposure warning pop up
Allow	Access is allowed	Chosen action is allowed	

USE CASE #3:

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

Theoretically there are two different approaches that can be implemented against malicious extensions. The first is to prevent their initial download and installation, and the second is to continuously scan the device to detect and disable unauthorized extensions. Neither of these capabilities are part of existing solutions' core set of capabilities.

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 name (contains 'AI'), permissions, install type, last updated at, browser store, extension risk and many more.

Monitored Events

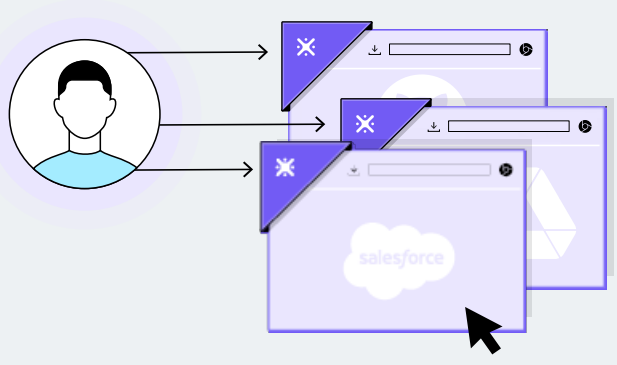
- Installed extensions

Capabilities

- Configuring 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.
- Disabling 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 the extension completely.

USE CASE #4:

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:

- App access
- App interaction
- 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.

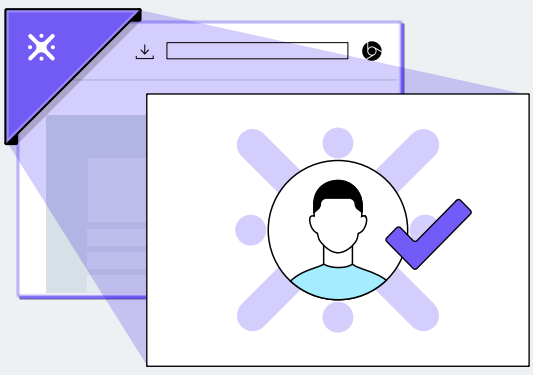
Capabilities

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.
- **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:**
  - 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. In addition, adjusting data protection policies for potentially risky or vulnerable user accounts.

USE CASE #5:

Secure Browser-based Authentication to SaaS and Web Apps



Overview

Ensuring secure authentication in your SaaS environment is of critical importance. Identify-based attacks that utilize compromised credentials for malicious access are becoming more ubiquitous, making it risky to implicitly trust authentication-based usernames and credentials alone. Even authenticated users should be authorized to ensure they access only the resources they need to reduce the potential impact of successful attack.

Secure Authentication Challenges

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.

Limitations of Existing Security Solutions

› **Authentication**

Cloud and Federation Identity Providers:

- Multi-factor Authentication (MFA): Adds another verification layer on top of the username and password as a means of additional proof that the credentials provider is a legitimate user. However, MFA solutions are hard to roll out due to workforce user-experience objections and are not widely used.
- Device Trust: Using the managed device as an authentication factor while requiring MFA when accessing from unmanaged devices. However, if the organization is not using an MFA solution, device-based protection is only capable of completely blocking access from unmanaged devices, which many organizations will decline since it contrasts their BYOD approach.

› **Authorization**

CASB

- Activity Policies: CASB solutions enable configuring and enforcing policies that control users' ability to access resources within a given app. The key limitation to this approach is the lack of centralized consistency between the different apps due to CASB's dependency on the protected apps' API.

The LayerX Solution

Overview

LayerX enables leveraging the browser as an additional, genuine, authentication factor 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)

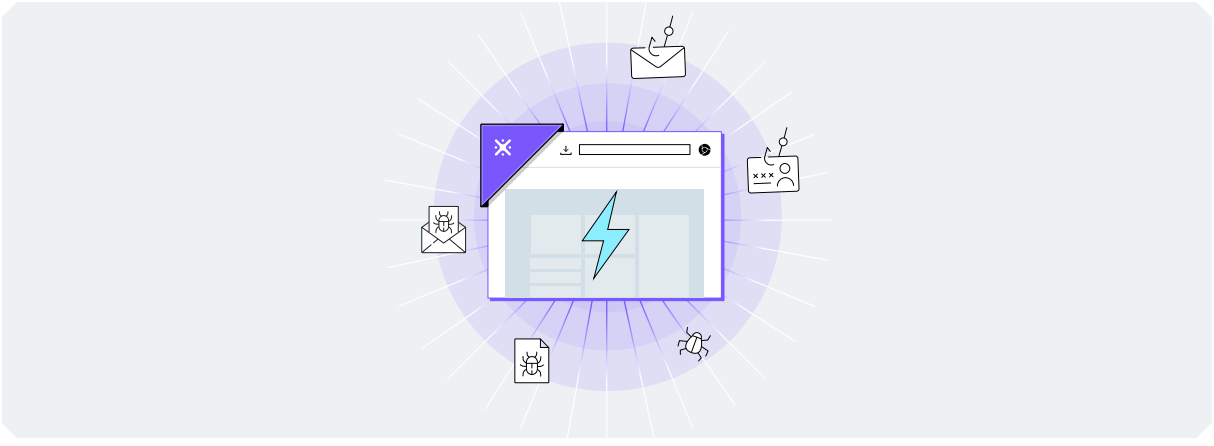
Capabilities

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

- Configuring 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.
- Configuring activity policies to enforce least privilege access policies for resources within the SaaS app itself.
- Trigger additional verification when risk is detected, based on LayerX's granular visibility of the user's activity within the app.

USE CASE #6:

Zero-Hour Protection Against Browser-borne Threats



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 apps that make use of modern web page capabilities. This attack vector transformation is forcing security stakeholders to re-evaluate 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 solution must 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

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:

BYOD Protection

Overview

The modern workplace has evolved beyond the traditional model of corporate devices behind a network perimeter. The use of personal devices by internal employees, has become the norm for many organizations.Therefore, to fully realize the productivity potential of its workforce, today's enterprise should have a way to enable access to both its public and internal web applications from any device, without degrading its security posture and the protection level of its sensitive data.

Unmanaged Devices Security Challenges

Unmanaged devices are, by definition, more vulnerable to being compromised by threat actors. A common attack pattern of a persistent threat actor is to target these devices in an attempt to install malicious browser extensions or other utilities and establish Man-in-the-Browser attacks that ultimately enable the attacker to access corporate web and SaaS resources. Moreover, the increasing BYOD trend in conjunction with the mass shift to working remotely have positioned unmanaged devices as the weakest link in the corporate's security stack. Realizing that, attackers are continuously targeting employees' devices as a beachhead to access the corporate resources. This applies equally to internal employees as well as external contractors.

Limitations of Existing Security Solutions

- **For Employee BYOD**

  Every solution that entails deploying corporate software on personal devices would encounter employee objection as it is experienced as a violation of their personal space and voids the BYOD concept from its actual meaning. There is no solution today that is able to successfully balance flexibility towards workforce's needs and security requirements, without having one coming at the expense of the other.

The LayerX Solution

Overview

LayerX preserves employees' operational needs while maintaining the highest level of security to the corporate's data. The LayerX extension doesn't require intrusive software installation on employees' machines since it merely extends the browser they are already using.

Monitored Events

- SaaS/web apps login,
- Resource interaction (file view/open/modify/download) within each app based on needs and context.

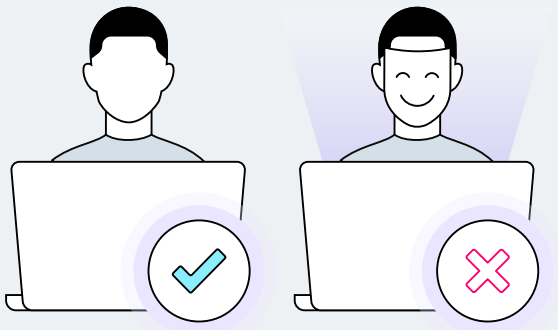
Capabilities

Data Security on Employees' Unmanaged Devices:

- Deploying the lightweight LayerX extension on top of the browsers in your employees' devices.
- Configuring dedicated activity policies to limit data downloads and storage on unmanaged devices to prevent data compromise due to on-device malware.
- Enforcing least-privilege policies to allow access to required corporate resources.
- Preventing any malicious device-website interaction that may be initiated by on-device malware.
- Discovering and assessing the security posture of all unmanaged devices that access resources.
- Enabling secure remote working by establishing a monitored and secure browser connection to organizational resources.

USE CASE #8:

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

To adequately assess, discover, and resolve an account's security posture, one needs visibility into various aspects. These include reused credentials, login behavior, shadow identities, and others. While some of these can be manually extracted from the Identity Provider in place, there's no way to get all of them in an automated, centralized manner.

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

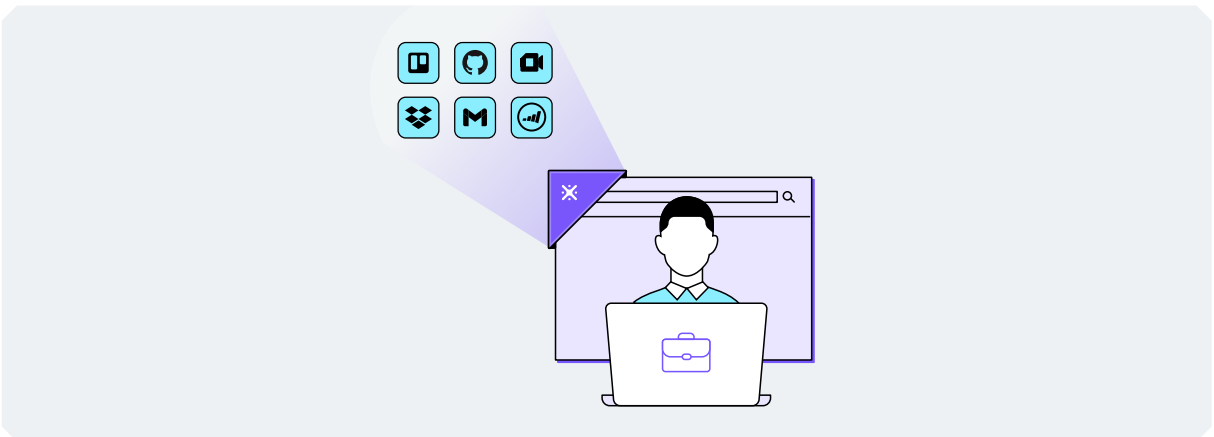
- Reused credentials
- User profiles
- Credential usage
- Apps login
- Account Sharing

Capabilities

- Monitoring for weaknesses in your identity posture, such as compromised or reused credentials.
- Discovering shadow or non-corporate identities that have access to your internal resources.
- Identifying potentially compromised user accounts, enabling the security team to take mitigation actions and reset their passwords. Detecting and blocking compromised users' malicious activity in real time.
- Using LayerX as a mandatory authentication factor to eliminate account takeovers.

USE CASE #9:

VDI and RBI Alternative



Overview

VDI and RBI have been used extensively by organizations in the past decade to provide their workforce with an alternative to being confined to one physical machine. In that manner, each employee has their own desktop image available via remote connection, which can be accessed anywhere, anytime.

VDI and RBI Security Challenges

It goes without saying that the security safeguards of the on-demand VDI and RBI desktops must at least equal the ones on the physical device. Moreover, these solutions introduce an additional attack surface - the connection itself. Unlike the device, access to the virtual desktop is done with a username and credentials which, if compromised, can provide an adversary with direct access.

Limitations of Existing Security Solutions - High Cost and Degraded User Experience

VDI and RBI solutions all suffer from the following issues:

- **High costs** - The initial setup and the maintenance of the infrastructure that's required to support multiple virtual desktops is extremely expensive.
- **Complex operations** - The ongoing operation entailed in having the inventory of desktop images available on demand for each user requires a skilled and dedicated workforce.
- **Slow user experience** - Delivered over an already overloaded network connection, VDI and RBI are infamous for degrading the user experience to a much slower speed and response than they are used to on the physical device.

The LayerX Solution

Overview

LayerX enables organizations to replace their costly and complex infrastructure with secure access straight from users' devices. This enables cutting TCO dramatically and meeting all the initial needs of VDI and RBI while materially reducing costs and enhancing the user experience.

Monitored Events

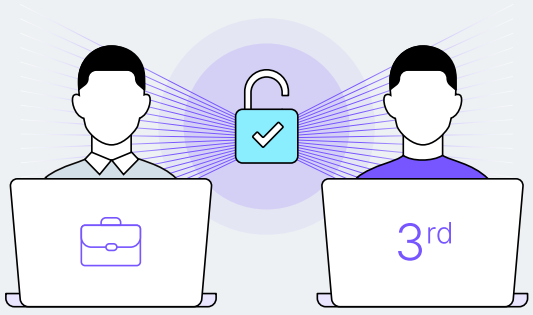
- Modify/create/remove of cookies, cache, downloads, passwords submission
- History, form data
- Modify the website's ability to use cookies, JavaScript and plugins
- Page Interaction: Keyboard/track mouse/bind on input buttons/submit/paste/copy
- Enable/disable 'do not track' privacy sandbox
- Modify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

Capabilities

- Configuring access policies to govern every user interaction with organizational data, preventing both unintentional data leakage as well as malicious adversary access.
- Eliminating the risk of an adversary compromising the VDI credentials since access is only enabled through the browser on the device.
- Scaling the number of users by adding them to existing data prevention and threat protection policies, eliminating the need to spawn a new desktop instance for any new user.
- Improving the user experience with direct access from the browser at the same speed as accessing any web location, while replacing the latency and lags that typically plague VDI.

USE CASE #10:

Secure 3rd Party Access



Overview

3rd party contractors are a core component of almost every organization's operational ecosystem. They can be found at all levels - from merely providing services to taking an active part in the organization's production. That way or the other, in order for them to deliver their full value, they often have to access mission critical apps and resources, making the ability to secure their access imperative.

3rd Party Access Security Challenges

The single fundamental challenge in securing 3rd party access is that the organization doesn't have any visibility and control over the devices they log in from. In a similar manner, there is no control from the organization's side over the 3rd party's credential security and hygiene. Adversaries often take advantage of this weakness and compromise either 3rd party devices or their access credentials for malicious initial access.

Limitations of Existing Security Solutions

The common enterprise approach today is to assign a managed device or provision a VDI to external contractors for accessing corporate resources. This approach is cumbersome for both the contractors and the corporate alike, as it materially degrades the speed and flexibility of the provided service.

The LayerX Solution

Overview

LayerX provides a seamless alternative that preserves 3rd party contractors' operational needs, while maintaining the highest level of security to the corporate's data with least-privileged access policies. The LayerX extension doesn't require intrusive software installation on the 3rd party device, since it merely requires then to sign in in order to have the LayerX extension enabled on the browser they are already using.

Monitored Events

- SaaS/web apps login
- Resource interaction (file view/open/modify/download) within each app based on its needs and context

Capabilities

Managed Browsers as Virtual Terminals:

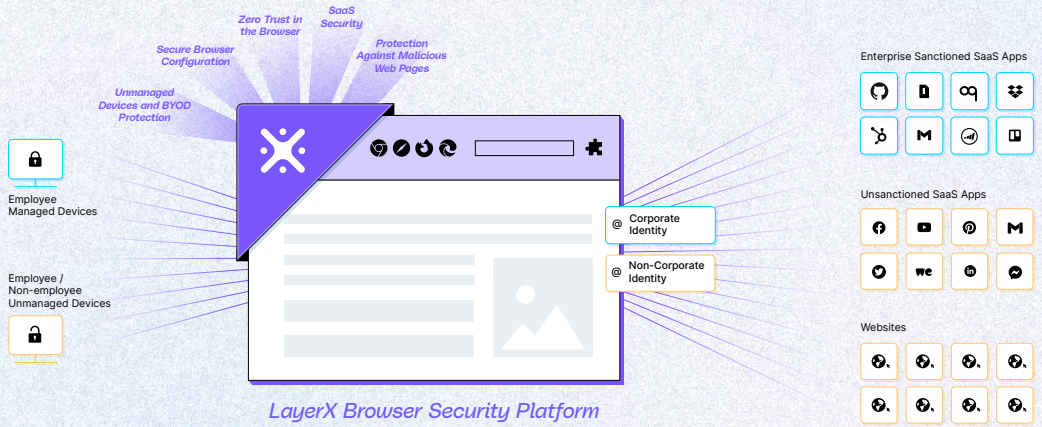
- Single-click onboarding/offboarding by allowing third party users to either sign in to or install a managed browser instance on one of their commercial browsers.
- Least privileged access policies to ensure your 3rd party contractors have access only to the data that they need, eliminating unnecessary exposure.
- Preventing malicious access by enforcing threat protection policies that monitor for behavior anomalies that indicate an account takeover,and responding with real-time access blocking.

About LayerX

LayerX provides a Browser Security Platform that's purpose-built to monitor, analyze, and protect against web-borne cyber threats and data risks. Delivered as a browser extension, LayerX natively integrates with any commercial browser, transforming it into the most secure and manageable workspace. Using LayerX, customers gain comprehensive protection against all threats that either target the browser directly or attempt to utilize it as a bridge to the organization's devices, apps, and data.

LayerX monitors every web-session at its most granular level to detect and disable risky activity at its utmost early stage with near-zero disruption to the user's browsing experience. With LayerX your workforce can securely browse anywhere.

Request Demo



KEY BENEFITS

Eliminate critical blind spots

Gain the most granular visibility into unsanctioned apps, shadow identities, 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.