



THE ENTERPRISE BROWSER EXTENSION

Solution Brief



INTRO:

LayerX Enterprise Browser Extension

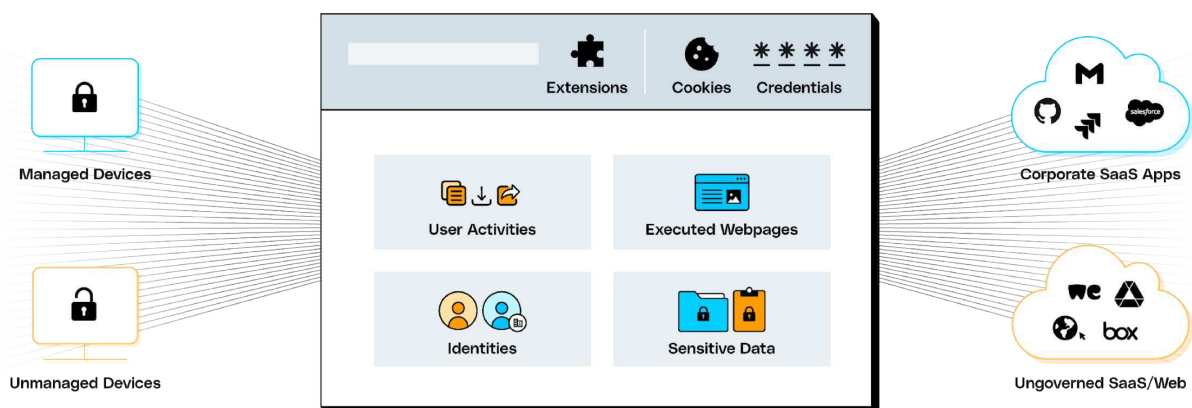
The Browser Security Challenge

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.

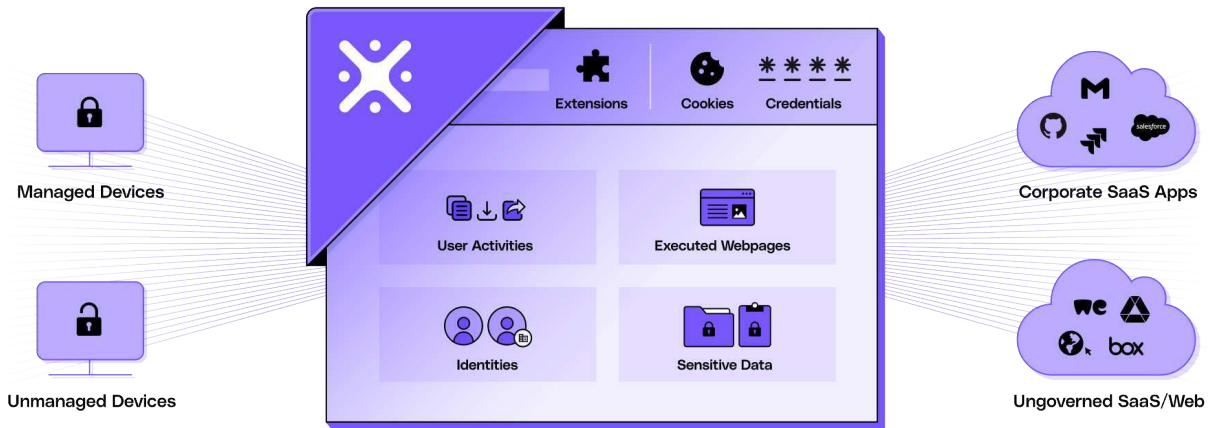
When existing solutions cannot mitigate new security challenges, it's time to develop a new one that can help enterprises strengthen their security posture in the face of modern threats and risks.



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.



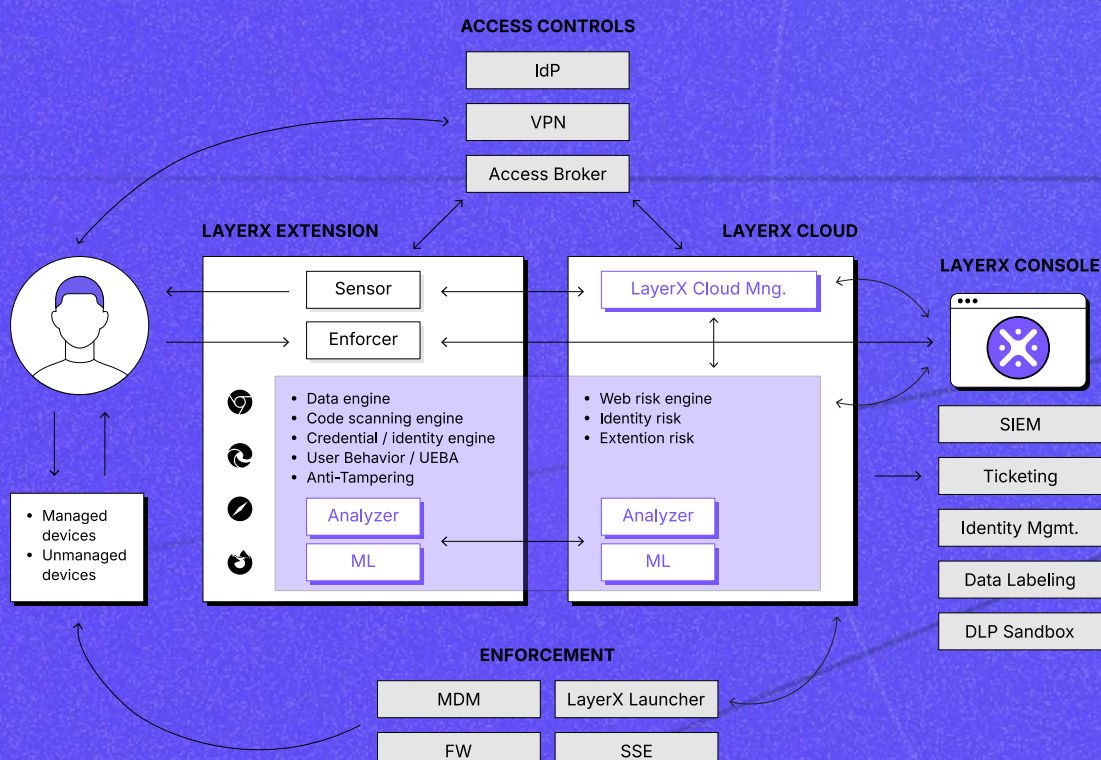
LayerX Use Cases

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

 <p>Gen AI Security</p> <p>Enable GenAI Usage in the organization without worrying about GenAI data leakage</p>	 <p>Web/SaaS DLP & Insider Threat</p> <p>Block sensitive data from leaking through web and SaaS apps</p>	 <p>Risky Browser Extensions Protection</p> <p>Identify and block risky browser extensions that can steal user credentials</p>	 <p>Secure Browsing</p> <p>Defend against malicious websites, malware, phishing, credential theft etc.</p>
 <p>Shadow SaaS & SaaS Security</p> <p>Detect all SaaS apps in the organization and who's using them</p>	 <p>Secure Access by BYOD/Contractors</p> <p>Secure remote access from unmanaged devices and 3rd-party users</p>	 <p>Identity Protection</p> <p>Secure against identity & passwords risk: password reuse, share accounts & shadow identities</p>	

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 configured 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

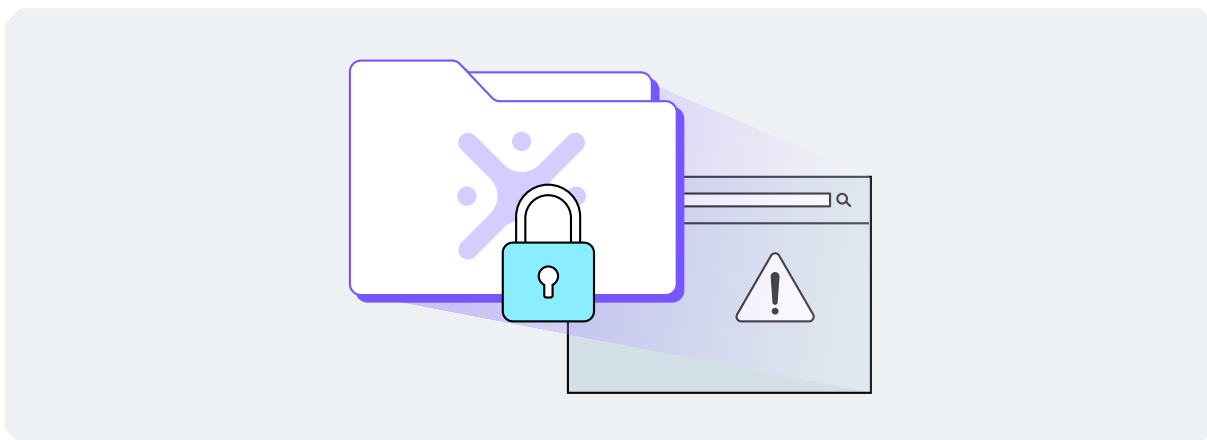


The LayerX Plexus Engine is the first purpose-built deep session analysis dual engine that operates both on the browser extension itself and in a centralized cloud service. Plexus monitors browser modifications, webpage behavior and user activities. All gathered events are analyzed in real-time and enriched 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:

Web/SaaS DLP & Insider Threat



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:

Gen AI Security



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.

Gen AI 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 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: paste, fill, type
- Accessed app
- Installed extensions

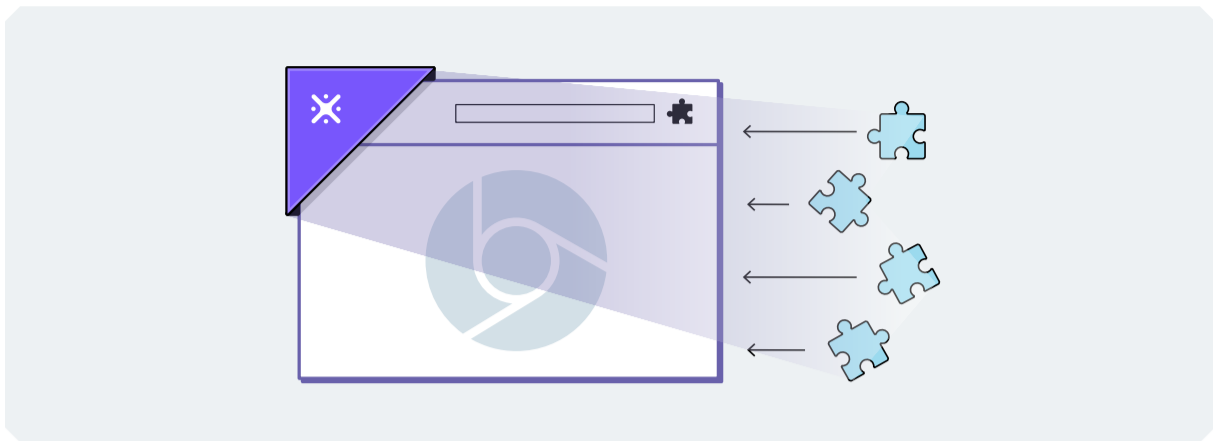
Capabilities

LayerX provides a wide range of Gen AI 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.

Gen AI 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

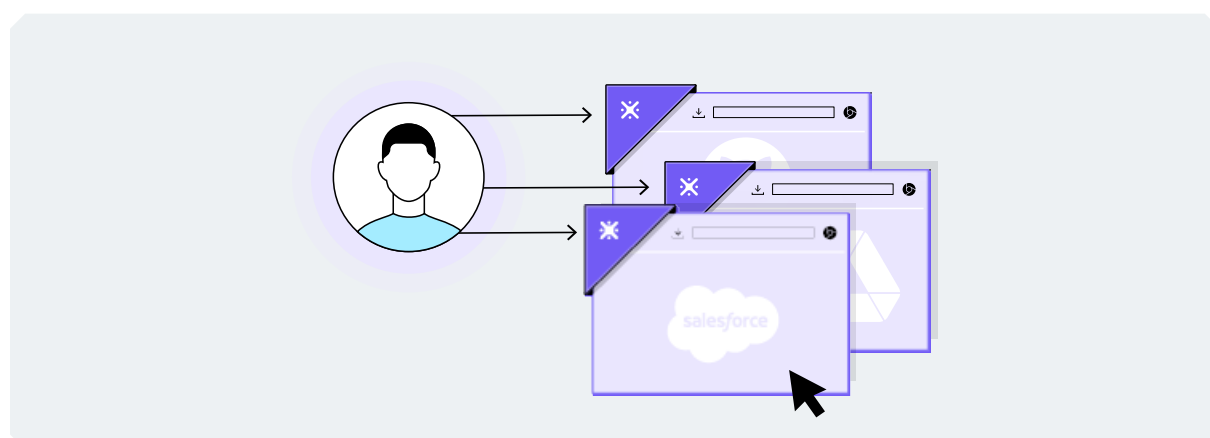
- Installed extensions

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:

Shadow SaaS & SaaS Security



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: Safe Browsing



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-gearred 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

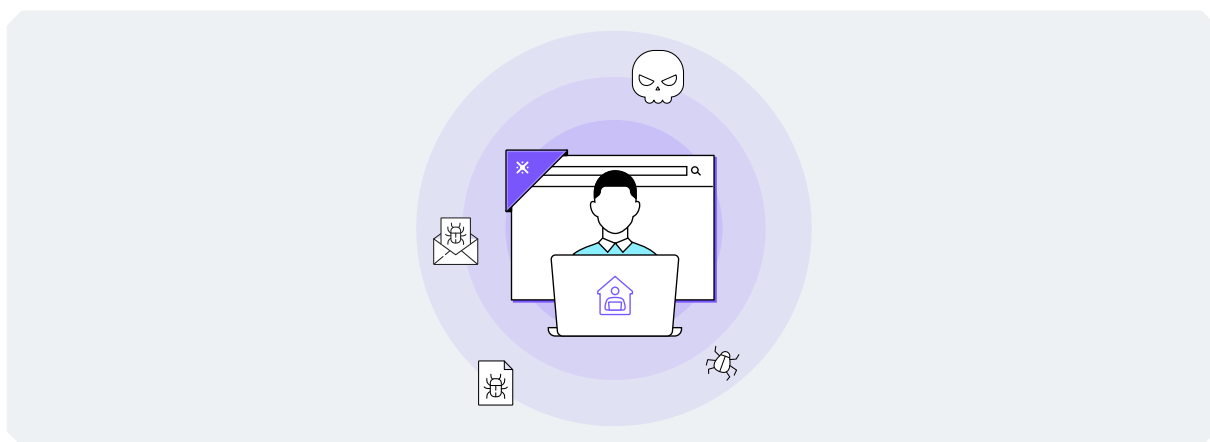
Capabilities

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 #6:

Secure Access by BYOD/Contractors



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.

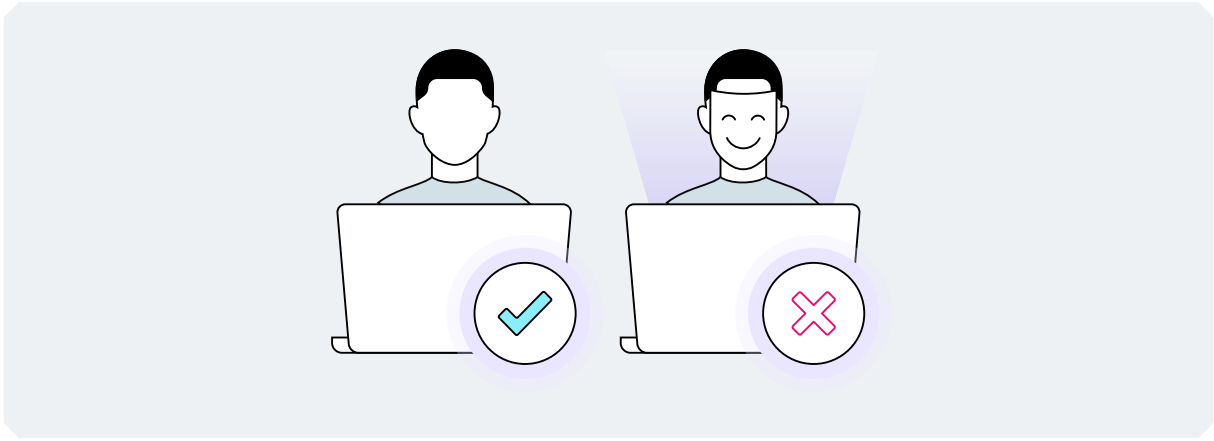
Capabilities

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 #7:

Identity Protection



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.