LayerX

PROTECTION FROM WEB-BORNE THREATS STARTS WITH A BROWSER SECURITY PLATFORM

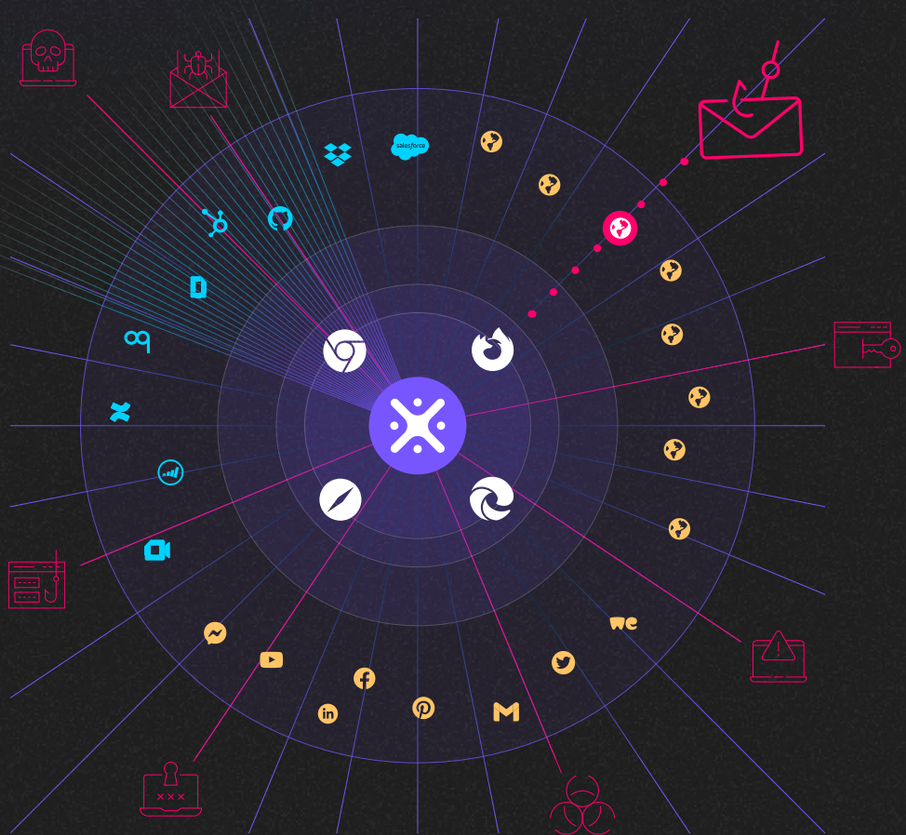
HOW CAN SECURITY TEAMS ADDRESS THE ADVANCED WEB-BASED THREAT LANDSCAPE?

Cyber security is about constantly adapting to changes that occur in two dimensions – the attack surface of the environment you need to protect and the threat landscape your environment faces.

In the modern corporate IT environment, the browser has long ago ceased to be a mere 'application'. It is now the most prominent work interface, connecting the workforce to managed resources, devices to the web, and the on-prem environment to the cloud one. This critical placement inevitably results in a steep increase in the number of threats that adversaries target the browser with.

To launch attacks on the browser, adversaries leverage its core functionality – rendering and executing web pages for users to access. Today's web pages are far more dynamic and sophisticated objects than their predecessors from a decade ago. This advantageous capability also has a dark side – these web pages can easily turn into an attacking tool that easily bypasses the corporate's defenses and runs on workforce's devices, turning the browser into a unique attack surface that must be addressed. Moreover, on top of being an **attack surface** that is targeted to compromise the data it stores, the browser is also the ultimate **attack vector** for malicious access to corporate SaaS and web applications through account takeover and use of compromised credentials.

All of this adds up to a simple insight: in the same manner the endpoint, network, and cloud require dedicated protection mechanisms, so does the browser. And in today's threat landscape it's nothing less than a critical necessity.

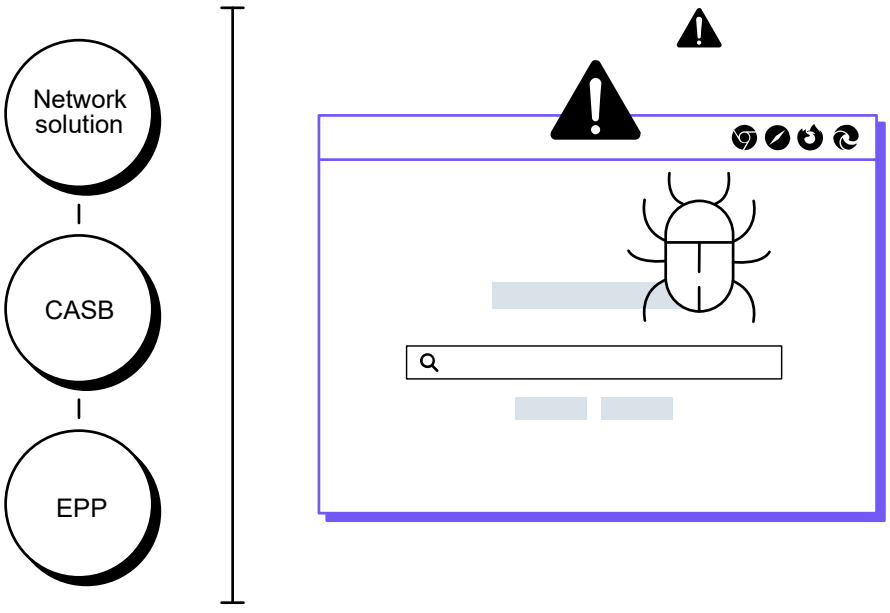


THE CHALLENGE:

YOU CAN'T PROTECT AGAINST WEB-BORNE RISKS FROM OUTSIDE THE BROWSER

Historically, security teams addressed various browser-related cyber threats and data loss risks with a patchwork of various solutions that were not natively built for protecting web sessions. For example, a network solution that analyzes web traffic to prevent access to malicious websites couldn't detect over 40% of today's adversaries-controlled web pages, because it can't analyze the actual, post-decryption web session. A CASB solution doesn't have any monitoring and threat detection capabilities for unsanctioned applications and other non-corporate web destinations. An Endpoint Protection Platform (EPP) doesn't have visibility into the installment of browser extensions, and so on and so forth. As you can see, a siloed approach that doesn't focus on web session protection results in a multi-product patchwork that's hard to manage. It also contains overlaps and blind spots that put your applications, devices, and data at risk.

The realization that sound **protection to web-borne risk can only come from within the browser itself** is the driver behind the design and building of a **Browser Security Platform**.

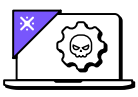


BROWSER SECURITY PLATFORM: THE FUTURE OF SECURE WEB BROWSING

Browser Security Platform is an emerging security solution category that's purpose-built to continuously monitor, analyze, and apply real-time security controls on browser sessions. Browser Security Platform differs from all the formerly used solutions in its visibility into the browser's application layer, where the actual web pages are rendered and built.

Browser agnostic

There are various commercial browsers that are used today by the organization's workforce. All of them are used as the main interface with the web. The common practice within most corporations is to delegate the choice of which browser to use to each employee. This creates a versatile browser ecosystem that varies from environment to environment. Hence, the initial prerequisite of Browser Security Platform is its ability to equally support any browser it might encounter.



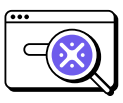
Converged

Browser Security Platform accommodates a wide range of management, visibility, and security capabilities and addresses risk and threat scenarios that vary greatly. It should harness its ability to analyze the post-decrypted web session to provide visibility into all web and SaaS activities, detect and prevent web-borne attacks in real time, prevent unintentional data loss, and enable the IT team to easily monitor and govern the corporate browsers' attack surface.

Comprehensive

A key feature in Browser Security Platform is its ability to address all aspects of the browser security:

- **The browser itself - Reducing the browser's attack surface** to prevent threat actors from utilizing it to compromise the host device or the data that resides within the browser application itself, such as cookies, passwords, etc.
- **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 to ensure that no corporate data is exposed. In addition, detecting and blocking account takeover malicious activity.
- **The web page that is used as an attack vector - Detecting and preventing malicious activity of attacker-controlled web pages** that users visit by real-time ML-based analysis of the behavior of its various components.



Deep web session inspection

While other security solutions operate on network packets, running processes, executable files or SaaS API, **Browser Security Platform provides real-time monitoring, risk analysis and proactive protection on the actual, post-decryption web session itself.** This capability is essential. It is the foundation of the platform's capabilities. First, monitoring the multitude of granular events that make up the assembly and rendering of the web page by the browser. Then, immediately pinpointing and neutralizing any indication of risk potential.

User-centric

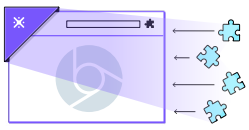
The browser is simultaneously the corporate's key working interface and an extremely personal application, making the maintenance of a seamless user experience and preservation of user privacy a far more critical necessity than in any other security solution.

Implementing this in practice dictates that Browser Security Platform must be able to abide by the following:

- Mitigate browsing related risks with minimal disruption of the session itself.
- Ensure that the web session monitoring it performs doesn't violate users' privacy and doesn't disclose personal information.

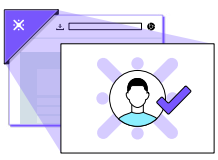
THE CORE CAPABILITIES OF BROWSER SECURITY PLATFORM

Browser Security Platform's architecture is made of three core components. A sensor that continuously monitors all web session events and user activities, a risk engine that analyzes each event to disclose the potential risk it introduces, and a policy enforcement mechanism that leverages the risk engine's output to block malicious activity and ensure that any risk to the device, data, or applications is removed. This architecture enables the browser security platform to provide the following capabilities:



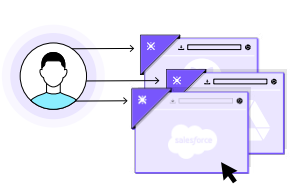
Secure browser configuration and attack surface reduction

A centralized interface for configuration and governance of all browsers in the corporate environment, enforcing software updates and security patches, as well as preventing installation of unauthorized browser extensions.



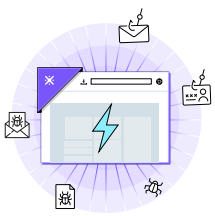
Zero trust in the browser

Can either enforce a standalone authentication and authorization mechanism or integrate with cloud-based identity providers (Okta, Azure AD, etc.). This becomes a consistent and granular alternative to CASB solutions and enables implementing Zero Trust authorization policies within the SaaS app itself.



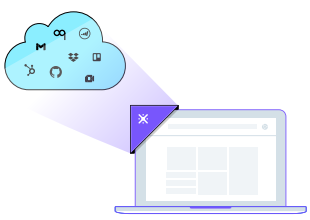
360° SaaS and web security

Continuous monitoring, analysis and active policy enforcement on all users' activities across all the sanctioned apps, unsanctioned apps, and other web destinations the corporate's workforce accesses from managed and unmanaged devices alike.



Protection from browser-borne attacks, phishing webpages and malicious websites

Detection and mitigation of risky actions from malicious web pages: from phishing-based credential theft to drive-by download of malicious files, by utilizing real-time analysis of the web page build up in the browser.



Protect unmanaged devices and BYOD

Enabling the internal workforce and external contractors to interact with corporate SaaS resources in a secure manner. Access becomes possible only through Browser Security Platform that enforces least-privileged access policies for authenticated users.

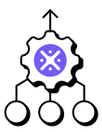
While these are the core features of Browser Security Platform, its architecture enables it to adapt and respond to any future web-based risks. Since, by definition, every web page is executed on the browser, the ability to monitor and control this execution from within the browser places Browser Security Platform at the ideal place to detect and mitigate any upcoming evolution of web-based risks.

THE BENEFITS OF BROWSER SECURITY PLATFORM

The main purpose of Browser Security Platform is to act as a transparent security layer that enables the corporate workforce to fully leverage the full potential of the web. Browser Security Platform is active across managed SaaS apps and the extremely wide range of unsanctioned SaaS and web apps that today's employees can choose from. Here are some of the benefits Browser Security Platform provides:

Flexibility

Empowers users to access any SaaS or web app from any managed or unmanaged device so they can perform their tasks. People work best when choosing their tools of choice out of the tremendous wealth of productivity tools. Browser Security Platform enables them to do so in a secure manner.



Consolidation

Instead of employing multiple disparate security controls that require manual orchestration and management, Browser Security Platform provides a single, unified interface that addresses every possible risk scenario that involves the browser, reduces operational costs, and saves precious time by automating browser-related security tasks.

Regained control

While the on-prem environment and sanctioned apps are fully managed and governed by the corporate's IT team, unsanctioned apps and other websites are, by definition, out of bounds. However, Browser Security Platform enables the security team to fully overcome this challenge by protecting the interface from these uncontrolled and unmanaged resources, which in practice provides full control.

Consistency

The basic requirement for an efficient security strategy is to apply it equally across the attack surface. In the same manner that all endpoints in your environment are subject to a consistent level of malware protection, Browser Security Platform provides all web and SaaS applications that your workforce accesses the same level of visibility, monitoring and threat prevention.

Cloud-first

Organizations are concerned about placing their sensitive data in the public internet with only a username and password to protect it from malicious access. This is one of the main obstacles that bars organizations from migrating their operations to the cloud. Browser Security Platform is the missing security link that addresses these concerns and drives forward a true cloud-first strategy.

WHAT IS NOT BROWSER SECURITY PLATFORM?

As an evolving category, the concept of Browser Security Platform is not always well understood by both security stakeholders and solution vendors alike. The driver behind the emergence of Browser Security Platform is the realization that the browser is at the most critical intersection point between the on-prem and the cloud environment, and as such should become the key pillar of the modern corporate security stack. However, there are various misconceptions that focus on mere portions of Browser Security Platform, rather than on the holistic paradigm shift it delivers. Below are some examples of common mistakes regarding the nature of this new product category.

Not a virtual machine for web-pages emulation

The concept of emulating the execution of incoming files in a secure environment to check if they are malicious or benign is more than a decade old. Network-based solutions resort to this approach due to their limited capabilities to detect if a web page is malicious or not based on network traffic alone. Browser Security Platform doesn't need this approach since it has real-time visibility, risk analysis, and enforcement capabilities on the live web page itself.

Does not only enhance endpoint protection solutions

Endpoint Protection Platforms (EPP\EDR\NGAV) are tasked with detecting and preventing the execution of malicious files and processes. While Browser Security Platform can indeed prevent the download of malicious executables from an attacker-controlled web page, this capability should be viewed as part of the focus on preventing web page malicious activity, rather than an additional malware protection layer.

Not a replacement to the leading commercial browsers

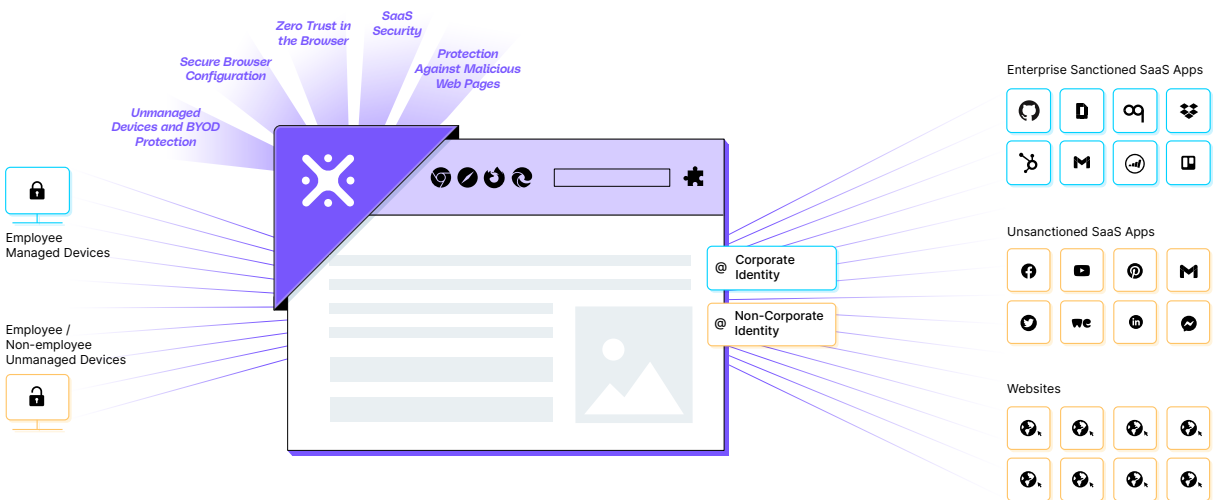
The modern browser is an extremely efficient productivity tool, built and designed over years to become the ultimate interface to consume information, interact with web destinations and SaaS apps and provide seamless user experience. The role of Browser Security Platform is to act as a native security layer on top of this experience, not replace it.

LAYERX BROWSER SECURITY PLATFORM: FULL PROTECTION FROM WEB-BORNE RISKS

The journey to protect your environment from web-borne risks and threats has started long ago, and you're already allocating budgets to that purpose through either your endpoint, network, or cloud protection projects.

In terms of budget, there is nothing new here – you've already been investing in the prevention of phishing attacks, downloading of malicious files, and protection of the sensitive data in your SaaS apps. The question you should explore is where you see the most urgent gaps. They might be the partial visibility you have across unsanctioned applications or the failure from preventing your employees from accessing malicious web pages. You're the expert in what your environment needs the most. As we've shown earlier, there are a multitude of protection challenges for the browser.

LayerX is the leading Browser Security Platform that is available for purchase and deployment today. It provides the full array of browser security capabilities to keep your environment safe from web-borne risks.



LAYERX MEETS THE KEY REQUIREMENTS OF BROWSER SECURITY ARCHITECTURE

As an evolving category, the concept of Browser Security Platform is not always well understood by both security stakeholders and solution vendors alike. The driver behind the emergence of Browser Security Platform is the realization that the browser is at the most critical intersection point between the on-prem and the cloud environment, and as such should become the key pillar of the modern corporate security stack. However, there are various misconceptions that focus on mere portions of Browser Security Platform, rather than on the holistic paradigm shift it delivers. Below are some examples of common mistakes regarding the nature of this new product category.

Browser-agnostic

Delivered as an extension and compatible with all the leading commercial browsers, LayerX provides full protection from web-borne risks and threats regardless of the browser ecosystem in the protected environment. Moreover, being an extension and not a standalone app, LayerX deployment is rapid and seamless, and can be distributed across all workforce browsers in mere minutes.

Converged

LayerX management console enables its users to perform the entire range of monitoring, management, auditing, and threat prevention activities that can only be performed from a security solution that is natively integrated with the browser application itself. Based on their specific needs and risk prioritizations, LayerX users can gradually build their browser protection journey, starting with the functionalities they need the most.

Comprehensive

LayerX delivers real-time protection against the wide range of web-borne threats – phishing attacks, installment of malicious browser extensions, downloading of malicious files, browser exploits, account takeover-derived access to data files, malicious access to SaaS and web resources from compromised unmanaged devices, and any other threat that either targets the browser directly or attempts to utilize it as a compromise vector to the hosting device or corporate app.

Deep web session inspection

LayerX monitors and analyzes each web session with its sensors in the browsers it protects. With its innovative web analysis technology, LayerX has granular, code-level insight into all the microevents that comprise the assembly and rendering of the web page in the browser. Utilizing two parallel risk engines, one in the browser extension that performs local risk analysis and one in the cloud that supports its peer with app, group, and corporate behavioral context, LayerX can leverage this granular visibility to realize high-precision detection and prevent web risks and threats.

User-centric

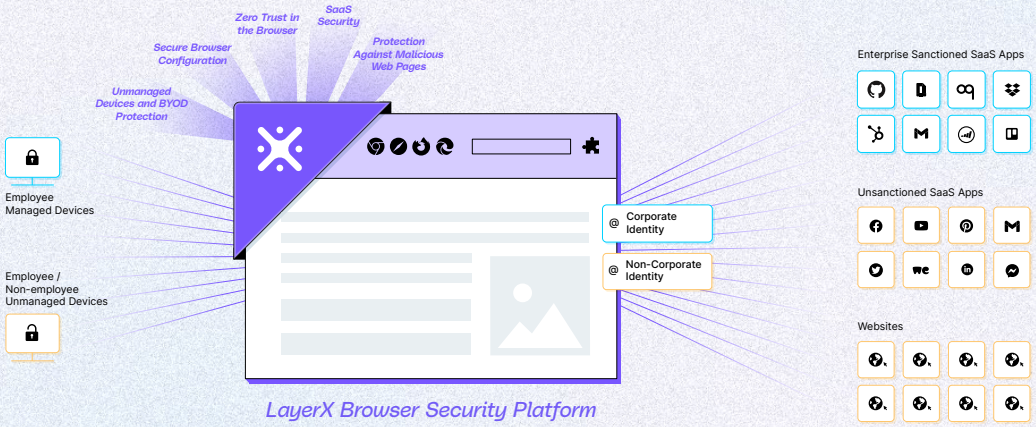
LayerX is built and designed as a user-first Browser Security Platform. First and foremost, as an extension it doesn't require users to change anything in their working routine. Moreover, its ability to detect, prevent and remove threats in a granular manner enables it to protect users without disrupting their browsing experience. Finally, it provides security stakeholders with the flexibility to determine, based on their internal corporate privacy policies, the exposure level of users' information in the browser. If needed, it can limit the data exporting from the browser's extension so no private data ever leaves the user's device.

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, DNS over HTTPS, SaaS apps, and dynamic websites.

Real-time protection

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

High-precision risk detection

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

Unified browser management

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

Bring your own browser

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

Rapid deployment

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