SEAMLESS AND SECURE CONTRACTOR ACCESS TO ORGANIZATIONAL SAAS AND WEB APPLICATIONS

Enable third parties to interact with your internal resources in an easy and protected manner with browser-based access and activity policies.

THE CHALLENGE:

Contractor Access From Unmanaged Devices Is An Exposed Attack Surface

The enterprise environment today is a far more complex entity than it was a decade ago. One of the key factors that challenges the traditional enterprise boundaries is the extensive presence of third party contractors who access organizational SaaS apps for various purposes. While there is a high degree of variance between different types of contractors, there is a common feature all of them share. They all access your sensitive resources from devices you don't manage and are not bound to the security practices you enforce in your environment. This could easily become a security risk, as was demonstrated in numerous attacks.

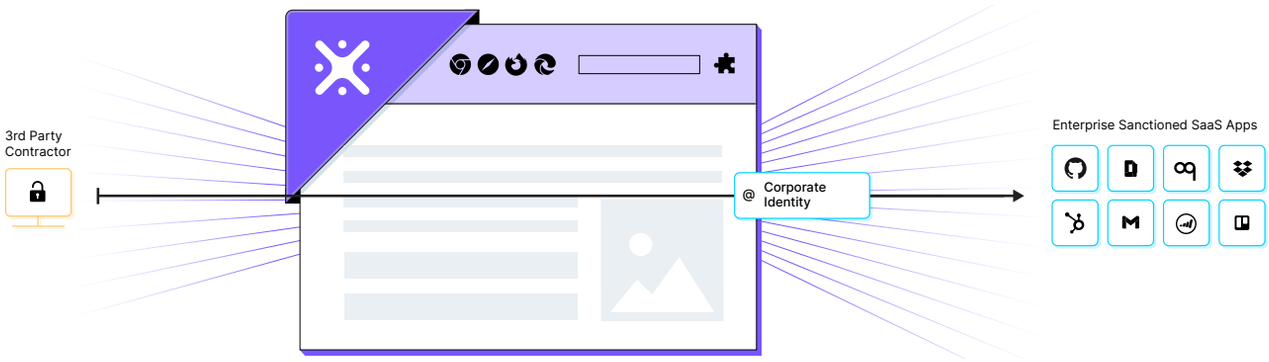
Today, most organizations address this challenge by requiring contractors to access their resources via VPN connection. However, while VPNs increase the security of the remote session itself, they don't mitigate the risks that can arise from a compromised contractor's device. In that case, the VPN might even provide a false sense of security. The security team would trust it to protect the session from hijacking without even considering the option that it's already under the adversary's control.

The fact is that unmanaged devices are a black box. But banning them altogether and allowing access only from corporate devices is not practical. Therefore, organizations today have no other choice than to accept them as an exposed attack surface that requires significant monitoring efforts. If any attempt to leverage it for malicious access is detected, they act accordingly. This is not a sustainable situation. There's a need for a security solution to solve this challenge at its root.

THE SOLUTION:

LayerX Browser Security Platform

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 the earliest stage with near-zero disruption to the user's browsing experience. With LayerX your workforce can securely browse anywhere.



LayerX For Secure Contractor Access

LayerX enables you to provide your contractors with seamless, secure access to your organizational resources with a few simple steps:

- Assign the contractor a user profile in any of the commercial browsers the company is using, with the LayerX extension installed on it.
- Let the contractor user sign into the newly created browser profile to get the extension deployed on its browser.
- In the LayerX management console, configure a policy that requires the contractor to log in via the LayerX extension to allow access to the app.
- Optional: In the policy, add the specific resources within the app that the contractor is entitled to interact with, as well as the permission levels (view only, download, etc.).
- Optional: In the policy, add the risk factors that will block access upon suspected account takeover.

Following these steps, the contractor's access is now fully secured. LayerX's risk engine will ensure that the contractor will only be able to access its target resources when the conditions in the policy are met. Moreover, LayerX continuously analyzes the contractor's activity while interacting with the app and blocks the session if any risk appears. This eliminates the 'black box' risk described earlier, rendering full transparency into the contractor's entire activity.

LayerX Core Use Cases for Contractor Access

Data Loss Prevention

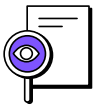
LayerX policies prevent insecure use of your sensitive files, such as downloading to unmanaged devices or sharing with unknown destinations.

Supply Chain Attacks Protection

LayerX continuously monitors the contractor's activity in your apps to detect any anomalous activities, which might indicate an adversary using the contractor's compromised credentials.

Zero Trust in the Browser

LayerX enables you to incorporate third party access in your overall Zero Trust implementation, making them no different than your internal workforce's.



Visibility and Auditing

LayerX provides granular visibility into all work-related activities the contractor performs throughout the connection with your SaaS and web resources.

Preventing Account Takeovers and Identity Theft

LayerX enforces browser-based zero trust access, eliminating the ability to conduct account takeover attacks via cookie or password theft.