LayerX | CASE STUDY

LayerX Helps WCF Prevent Browser Security Threats: Phishing, Malicious Extensions, Web DLP and Password Reuse

WCF Insurance (WCF Insurance is the common brand mark and brand name for WCF Mutual Insurance Company, WCF National Insurance Company, and WCF Select Insurance Company. WCF.com/About-Us) provides property and casualty insurance to customers in the Western United States. As an insurance provider, the employees of WCF Insurance interact with sensitive data on a daily basis. Ensuring this data doesn't get exposed is a critical part of their integrity and commitment towards their customers. To live up to their high security standards, WCF's security team is continuously assessing their architecture to enhance protection and eliminate unprotected blind spots. In the course of this process, WCF identified four key browser security weaknesses that their previous solutions failed to adequately protect:

1 Safe Browsing: Preventing Phishing Attacks

The Challenge: Password Exposure

Phishing attacks are a leading password theft vector. They are commonly launched by sending employees a socially engineered email, which lures them to click an embedded link for various malicious purposes. Clicking the link redirects the user to an attacker-controlled page that requests the user to insert their password to log in. Once they do so, the attacker can obtain their password and use it for malicious access.

Limitation of Existing Solution: Limited Coverage and Downgraded Browsing Experience

The customer had a BEC solution that employed a Browser Isolation module for the execution of links embedded in the email messages. While this approach has gained some success in the prevention of malware execution, it failed to cover the full range of web-borne threats, such as phishing and other forms of password leakage. This was due to its inability to perform granular inspection of web content and activities. On top of that, using browser isolation significantly slowed down browsing speed, triggering continuous objections from WCF's employees.

> *"We were constantly getting complaints from employees that they were having trouble accessing online apps and couldn't get their work done. . We needed a way to better address the risk that didn't force employees to try working from their own personal devices or finding other, less secure, work arounds."*
>
> *- Cliff Frazier, CISO, WCF Insurance*

WCF INSURANCE

Industry
Insurance

Size
650 employees

Location
Utah, USA

Challenges

- Secure browsing
- Data leakage over the web
- Malicious browser extensions
- Password reuse

LayerX Solution

- **Phishing:** Granular activity policies to detect malicious web pages with behavioural analysis without relying on prior knowledge.
- **Web Data Leakage:** DLP policies to prevent users from uploading and pasting with no slow down or disruption of the user's browsing experience.
- **Malicious Extensions:** Risk-based policies that automatically discover and disable extensions that don't meet security requirements.
- **Password reuse:** detection and alerting whenever an employees reuse their work passwords for non-work purposes.

2 Preventing Data Leakage on the Web

The Challenge: Data Exposure on Legitimate Web Destinations

WCF employees surf various legitimate web locations, such as Gmail, Facebook, LinkedIn, and others. WCF attempted to use Remote Browser Isolation (RBI) to monitor and prevent data leakage to these sites. However, similar to the safe browsing challenge, the RBI slowed down the browsing experience to an unbearable level.

This left WCF with two unacceptable alternatives, One, block all traffic to personal web destinations. Two, let the traffic flow without any governance, creating a security concern for inadvertent data exposure and for these sites being abused by an attacker as a data exfiltration channel.

Limitation of Existing Solution: No Protection

The endpoint-oriented DLP solution in WCF's environment didn't cover web locations, nor were they able to identify pasting of sensitive data. DLPs were designed to protect files, not text.

3 Eliminating Malicious Extensions from Users' Browsers

The Challenge: Malicious Access to All Browser Data and Session Activity

Browser extensions have become a key component in attackers' toolkits. They deliver them either by socially engineering employees to download a seemingly benign extension from a web store, or by sideloading them to their machines without the user's knowledge or consent. Once installed, the malicious extension has direct access to all the browser's data and activities and can capture and exfiltrate them at will.

Limitation of Existing Solution: Unscalable Manual Blocklist

WCF attempted to mitigate the risk of malicious extensions with their existing Unified Endpoint Management (UEM) solution. They created a blocklist of extensions that are not allowed to be installed. However, this proved to be unscalable due to the large volume of new extensions users added over time. Manually maintaining the list proved to be too resource-consuming to be a sustainable policy. The end result was that extensions were installed on employees' browsers without monitoring of governance.

> *"It was impossible to track all the new extensions that were being published, but we knew we couldn't allow them all. We were spending an unacceptable amount of time managing and tracking extensions, but that didn't seem like the best use of our talent."*
>
> *- Cliff Frazier, CISO, WCF Insurance*

4 Preventing Password reuse

The Challenge: employees expose their work credentials via careless reuse.

Some of WCF employees tended to reuse their work username and password for logging in to various non-work apps. As these apps are susceptible to compromise, the reuse of work credentials exposes them to compromise as well and putting WCF SaaS resources at risk.

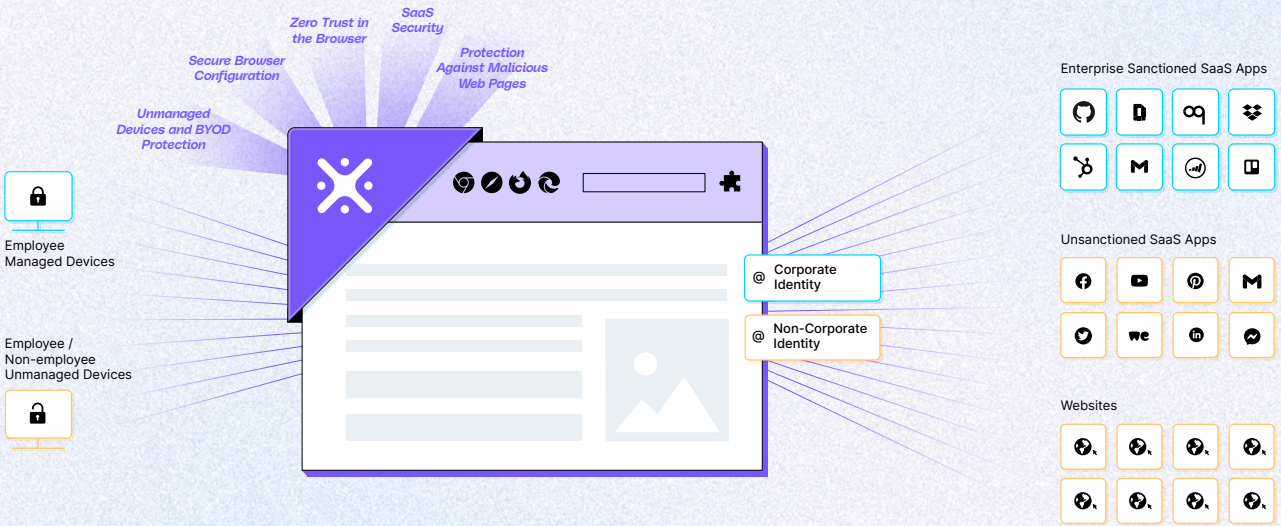
Limitation of Existing Solution: No Available Protection

WCF didn't have in their security stack any tool that could provide them with visibility into the credentials their employees are using when logging to non-work destinations. This was a complete blind spot.

LayerX Solution:
Secure Browser Extension

The LayerX Difference

LayerX provides an enterprise browser extension that natively integrates with all leading browsers to deliver continuous monitoring, risk analysis, and proactive policy enforcement on every event within a browser session. LayerX's risk engine granularly inspects both the execution of webpages as well as user activities in the browser to identify any anomalies or policy violations and respond with a preventative security action.



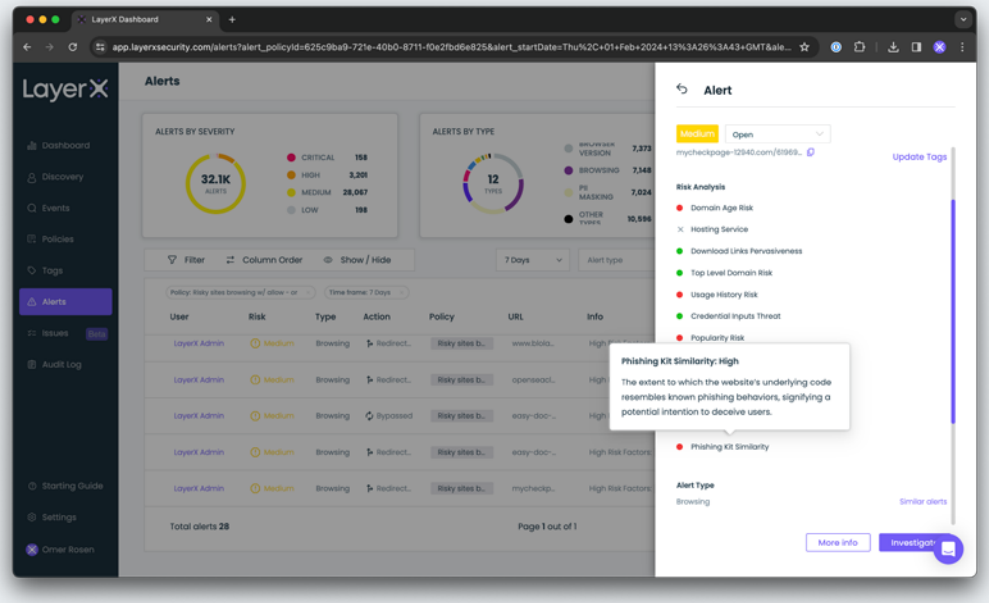
Rapid Deployment and Onboarding

The LayerX agentless secure browser extension was installed on all WCF's employees' browsers in a fast and seamless manner via a single group policy click. Once installed, the extension started its automatic discovery of all browser-related entities within WCF browsers' ecosystem, such as user accounts, applications, extensions, and many others. Once the discovery process was completed, the WCF security team set out to solve their four security challenges.

Phishing Protection: ML-based Detection of Malicious Pages Without Slowing Down the Session

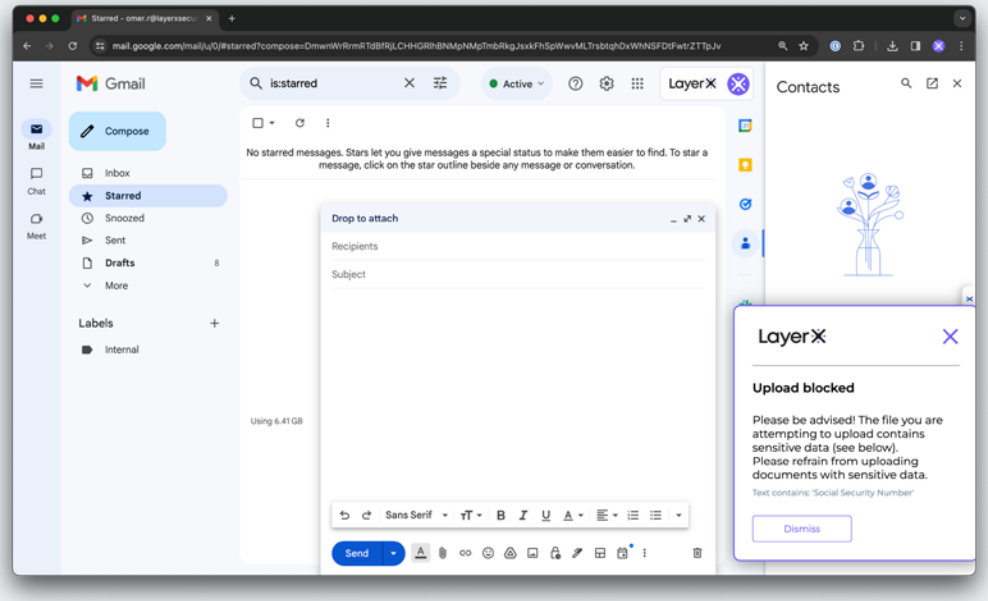
LayerX analyzes the gradual execution of the web page within the browser and applies various ML algorithms to detect any component that features a potential risk. This enabled LayerX to mitigate any web-borne threat, thanks to its ability to spot early indicators of malicious activity as they build up. Then, LayerX can disable them before any harm is done.

The WCF team configured a policy that granularly disables the page's malicious capability whenever such is detected. All of this is achieved within the live session itself, without any isolation or sandboxing to slow it down.



Web DLP: Prevent User Activity that Might Subject Data to Exposure Risk

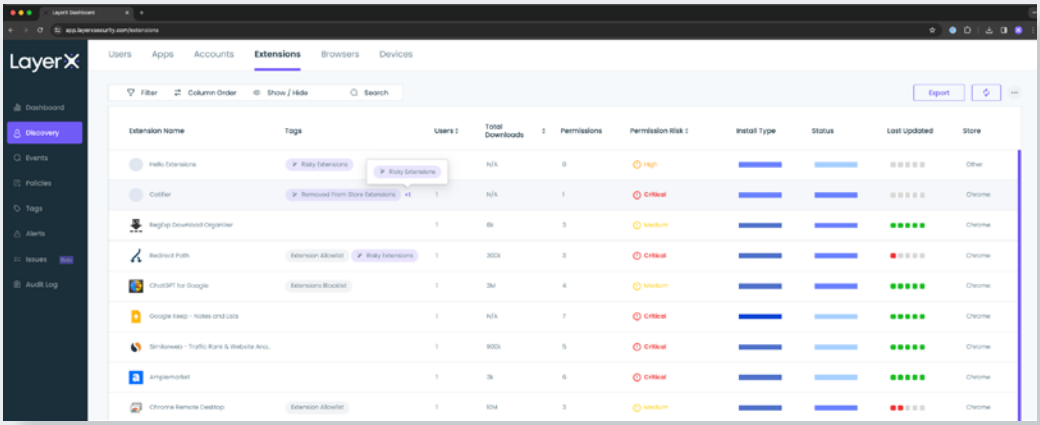
LayerX can identify all activities users perform in the browser down to the granular level of a mouse movement or a button click. The WCF team leveraged this capability to configure DLP policies that prevent users from uploading or pasting sensitive data to their personal web apps. LayerX architecture enables this capability to become an integral part of the browser, so the analysis and policy enforcement take place as part of the web session itself and without any disruption to the user's browsing experience.



Malicious Extensions: Automated Detection and Disablement

The LayerX extension has immediate visibility into all other extensions that reside on the browser. The LayerX risk engine analyzes the required permissions, installation method, publisher reputation, and other unique attributes for each discovered extension. It uses this information to reach a verdict on the extension's risk.

The WCF team used this capability to configure policies that alert whenever an extension with high permissions was being installed, and to disable any extension that LayerX flagged as critical risk. Once the policy was configured, LayerX applied it automatically to all the extensions in place, as well as to all extensions installed from that point onwards.



Password Reuse: Automated Detection and Alerting

LayerX has full visibility into all activities that take place within the browsing session, including what credentials are used when accessing or registering to a non-work app. With this visibility it was easy to configure policies that would either block the credentials reuse or trigger an alert whenever the work password was used for a non-work destination.

This enabled the WCF team to identify who are the employees that have been already practicing this insecure habit, as well proactively prevent it from happening in the future.

Conclusion:
A Single Solution that Delivers Automated Protection with Near-zero User Impact

The guidelines LayerX solution follows are automation and maintaining the user's browsing experience. In the context of WCF's security challenges, this can be achieved only by an extension that is integrated with the browser itself. On top of the visibility and enforcement within the web session, it also ensures that employees don't have to give up their browsing speed to get security. In this manner, LayerX enabled WCF to replace the partial protection it got from BEC, DLP, and UEM, with a single solution that's purpose built to solve any browser-related risks.

> *"LayerX is an all-in-one solution for our online browsing security issues. Whether it's protecting against phishing or malicious extensions or data leaks, LayerX ensures our employees can access anything they need without risking our customer and company data."*
>
> *- Cliff Frazier, CISO, WCF Insurance*