Customer Story

WCF Prevented Security Threats

Akamai Workforce Protector (formerly LayerX) helped stop phishing, malicious extensions, web DLP, and password reuse challenges

Prevented phishing attacks

Eliminated malicious extensions

Deployed and onboarded seamlessly

WCF Insurance 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 toward 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 key browser security weaknesses that their previous solutions failed to adequately protect.

Safe browsing: Preventing phishing attacks

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 asks the user to insert their password to log in. Once they do so, the attacker can obtain the password and use it for malicious access.

Although legacy browser isolation tools prevented basic malware execution, they failed to mitigate broader web-borne threats such as phishing and credential theft. This was due to the tools' 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.

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

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

WCF INSURANCE

Location
Utah, United States
wcf.com

Industry
Financial Services

Solution
Security

Product
Akamai Workforce Protector

Akamai Security

Preventing data leakage

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 site abuse by an attacker as a data exfiltration channel.

The endpoint-oriented data loss prevention (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.

Workforce Protector can identify all activities that 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. Workforce Protector 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.

Eliminating malicious extensions

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.

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-intensive to be a sustainable policy. The end result was that extensions were installed on employees' browsers without monitoring or governance.

The Workforce Protector extension has immediate visibility into all other extensions that reside on the browser. The 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 Workforce Protector flagged as critical risk. Once the policy was configured, Workforce Protector applied it automatically to all the extensions in place, as well as to all extensions installed from that point onward.



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

Preventing password reuse

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

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

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

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

Rapid deployment and onboarding

Workforce Protector's agentless secure browser extension was installed on all WCF employee 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 security challenges.

A single solution that delivers automated protection with near-zero user impact

The guidelines that Workforce Protector follows are automated and maintain 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, Workforce Protector enabled WCF to replace the partial protection it got from business email compromise (BEC), DLP, and UEM with a single solution that's purpose-built to solve any browser-related risks.

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

> **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**

WCF INSURANCE

With over 100 years of service, WCF Insurance is an innovative commercial insurance provider that serves the Western United States. Their daily commitment revolves around supporting the individuals who drive community growth, including businesses they insure, valued agency partners, dedicated employees, and the non-profit organizations they champion. WCF Insurance's unwavering mission is to provide an excellent insurance experience while fostering positive change through ongoing commitment to the communities they serve.

© 2026 Akamai Technologies | Support |
| Published 11/26