CASE STUDY

Spin.ai

Outbrain: Taking Control of Extension Security

Overview

Outbrain standardized on Chrome Enterprise to benefit from the ease of working in the cloud, the browser's built-in security, and easy management, control, and visibility. To further strengthen security, particularly around browser extension controls, Outbrain paired Chrome Enterprise and its extension risk assessment and workflow tools with Spin.AI. This resulted in a faster, more streamlined process for assessing the risks of browser extensions.

Strengthening Security for a Cloud-First Company

- Outbrain chose Chrome Enterprise as the foundation for its cloud-first approach, teaming the browser with Google Workspace and taking advantage of built-in Chrome security.
- To tap the security benefits of Chrome Enterprise, Outbrain creates policies for app and extension use with Chrome Enterprise Core, and also manages automatic updates.
- Outbrain pairs Spin.AI with Chrome Enterprise Core for extension risk assessment to improve security decision making.
- The combination of Chrome Enterprise and Spin.AI has accelerated the development of extension policies and other user guardrails to keep the company secure.

> *"We definitely have fewer worries about browser security now," Naraine says. "We know that Spin.AI and Chrome Enterprise updates are doing their job in the background, so we're not constantly concerned that a user is installing something malicious. We can set it and forget it."*
>
> Travis Naraine, IT Infrastructure Engineer, Outbrain

Outbrain

About Outbrain

Outbrain (Nasdaq: OB) is a leading technology platform that drives business results by engaging people across the Open Internet.

Industry

Technology

Location

Global

Products Used

- SpinOne (including backup and recovery, archive, SSPM, risk assessment, DLP, and ransomware detection and response)
- Google Chrome Enterprise

Easy Management and More Visibility for an Enterprise Browser

IT leaders are always looking for ways to improve their organization's security posture. With employees working in the cloud, the browser became a focal point for strengthening security, leading Outbrain to Chrome Enterprise.

Outbrain had already standardized on Chrome Enterprise as a linchpin of its cloud-first strategy – especially valuable with a hybrid workforce around the world. The security team zeroed in on browser extensions as a common security gap that needed to be closed.

"People like to use browser extensions to improve their productivity and to access the tools and features they need to do their jobs," says Travis Naraine, IT Infrastructure Engineer for Outbrain. "That's great, but we know there are malicious extensions available online. We needed a way to enable employees to install Chrome Enterprise extensions, but to choose the ones that are safe to use."

The process of vetting, testing, and blocking extensions was manual, explains Harel Shaked, Director of IT Services and Support for Outbrain.

"Once we learned about risky extensions, we would block them," Shaked says. "But we didn't have the visibility to see which extensions and apps were already in our environment." The process was reactive instead of proactive, raising concerns over missed opportunities to detect and block risky extensions.
As Shaked and Naraine explored backup solutions for another security project, they came across Spin.AI's SpinOne platform. It met their needs for SaaS backup, as well as ransomware detection and response, as well as shared data monitoring, including SaaS Security Posture Management (SSPM). SSPM had several points in its favor, including features for app and browser extension risk assessment and reassessment, and the ability to easily integrate with Chrome Enterprise.

"We like to stay with single vendors where possible," Naraine says. Outbrain employees use Google Workspace with Chrome Enterprise. "And if we go outside of Google, we want solutions that are tightly integrated with our Google tech stack."

Outbrain uses Chrome Enterprise extension risk assessment, powered by Spin.AI, to generate risk scores that assist in decisions about allowing or blocking extensions. In addition, with Chrome Enterprise Core's extension workflow, Outbrain employees can submit extension requests for IT and security teams to review and allow or deny use of the extensions. The automated process saves significant time compared with manual reviews.
The SpinOne platform helps Outbrain's security and IT teams test and assess extensions for use in the company. The testing and assessments help IT maintain security.

"The policies and the Spin.AI solution created an environment that nudged users to think about anything they were installing–extensions but other apps as well," Naraine says.

Chrome Enterprise makes management and control easy, enforcing policies for the browser and extensions with less complexity. Outbrain even creates its own internal Chrome extensions.

"At Outbrain we develop in-house extensions for Chrome for tasks like inspecting widgets within the company," Naraine says. "Since Chrome Enterprise is the browser we support company-wide, the extensions we develop have to maintain the security of the browser."

In addition to setting browser policies through the Google Admin console, Naraine and Shaked can manage automatic updates to ensure their employees are using the newest version of Chrome with the latest security patches to reduce Outbrain's exposure to vulnerabilities.

About Spin.AI: Spin.AI is an innovative provider of SaaS security solutions for mission-critical SaaS apps (Microsoft 365, Google Workspace, Salesforce, and Slack). Our all-in-one SpinOne platform helps organizations mitigate risk, save time, reduce downtime, and improve compliance.

☎ 1 888-883-2993   @ info@spin.ai   www.spin.ai