keep aware

Guide

The Buyer's Guide to Browser Extension Management

Browser extensions have become indispensable productivity tools, from password managers and note-taking apps to specialized workflow integrations. But as browsers have evolved into the primary workspace for employees, extensions have also become a significant, and often overlooked, security risk. Each extension represents third-party code running inside the browser, potentially with deep access to sensitive data, credentials, and system functions.

This document outlines the scope of the extension management challenge, how Keep Aware addresses it, and how it compares to other solutions in the market.

The Problem: Extension Management in the Enterprise

1. **Unmanaged third-party code:**
   Extensions often operate with powerful permissions, and if malicious or poorly developed, they can be exploited to compromise employees and company data.
2. **Data exfiltration & credential theft:**
   Extensions may access sensitive information directly from web pages, forms, clipboards, or downloaded files.
3. **Permissions:**
   Malicious add-ons can monitor browsing behavior and inject content, enabling phishing or ad-based attacks.
4. **Shadow IT and outdated tools:**
   Employees can install unapproved or outdated extensions without IT oversight, creating security blind spots.
5. **Compromised trusted extensions:**
   Even legitimate, widely used extensions can become threats if a developer account is hacked or an update is weaponized.

Organizations need more than just a static policy to manage this risk. They require full visibility into installed extensions, real-time prevention controls, and the ability to detect and respond to suspicious activity instantly.

Keep Aware's Approach to Extension Risk Management

Keep Aware employs a browser-native, real-time approach to managing extension risk without compromising the user experience.

Key Capabilities:

- **Cross-browser visibility:** See all installed extensions across Chrome, Edge, and other major browsers.
- **Centralized policy enforcement:** Instantly block or restrict risky extensions in real time across the entire organization.
- **Behavioral detection & response:** Identify suspicious activity as it happens and take immediate action.
- **Seamless deployment:** Works with existing browsers, no need to replace them or reconfigure core infrastructure.
- **Unified control:** Manage extension security through a single platform, reducing administrative complexity.

By running where employees work, directly in the browser, Keep Aware serves as the last line of defense, stopping credential theft, malicious code execution, and unauthorized data transfers before they succeed.

Comparison of Extension Management Approaches

Security teams can control extensions in several ways, each with tradeoffs. Policies enforce rules but detect little. Endpoint tools reveal known risks but lack real-time reach. Enterprise browsers block threats but demand full adoption. Security extensions combine visibility, prevention, and detection across environments.

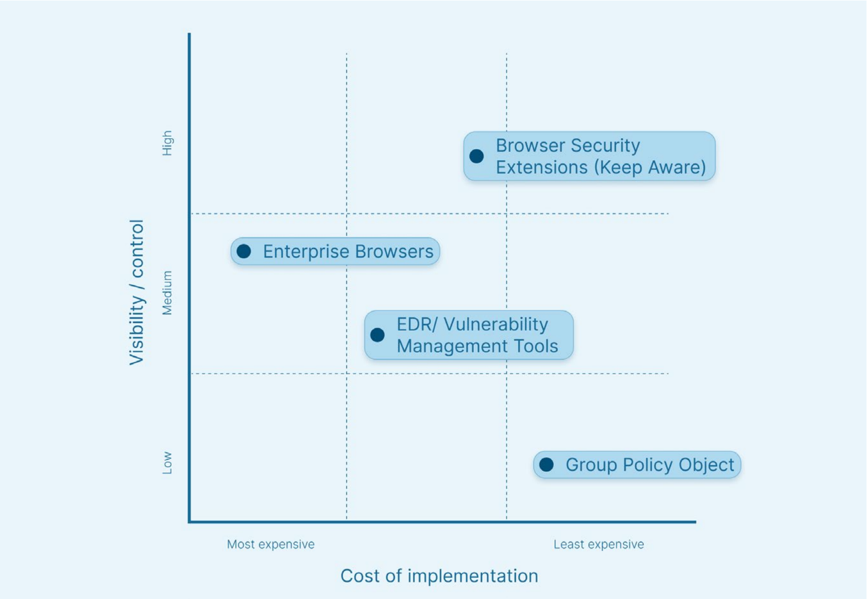


Figure 1: Comparison of controls and costs of extension management approaches

Policy-Based Controls (GPO, MDM, and Browser Admin Consoles)

Tools like Group Policy Objects (GPO), mobile device management (MDM) solutions, and native browser consoles offer basic visibility into which extensions are installed and can block specific ones based on pre-approved lists. However, they lack real-time behavioral monitoring, meaning malicious activity can go undetected. These solutions are typically limited to a single browser type, forcing IT teams to manage multiple policies for mixed-browser environments.

Endpoint-Based Tools (EDR, Vulnerability Scanners)

EDR platforms and vulnerability scanners can uncover some extension-related risks through device audits and scans. While they can detect known vulnerabilities, they generally cannot prevent risky extensions from being installed or stop malicious activity as it occurs. Their detection is often periodic rather than continuous, delaying response times. The benefit is that they leverage existing endpoint agents, making deployment relatively easy.

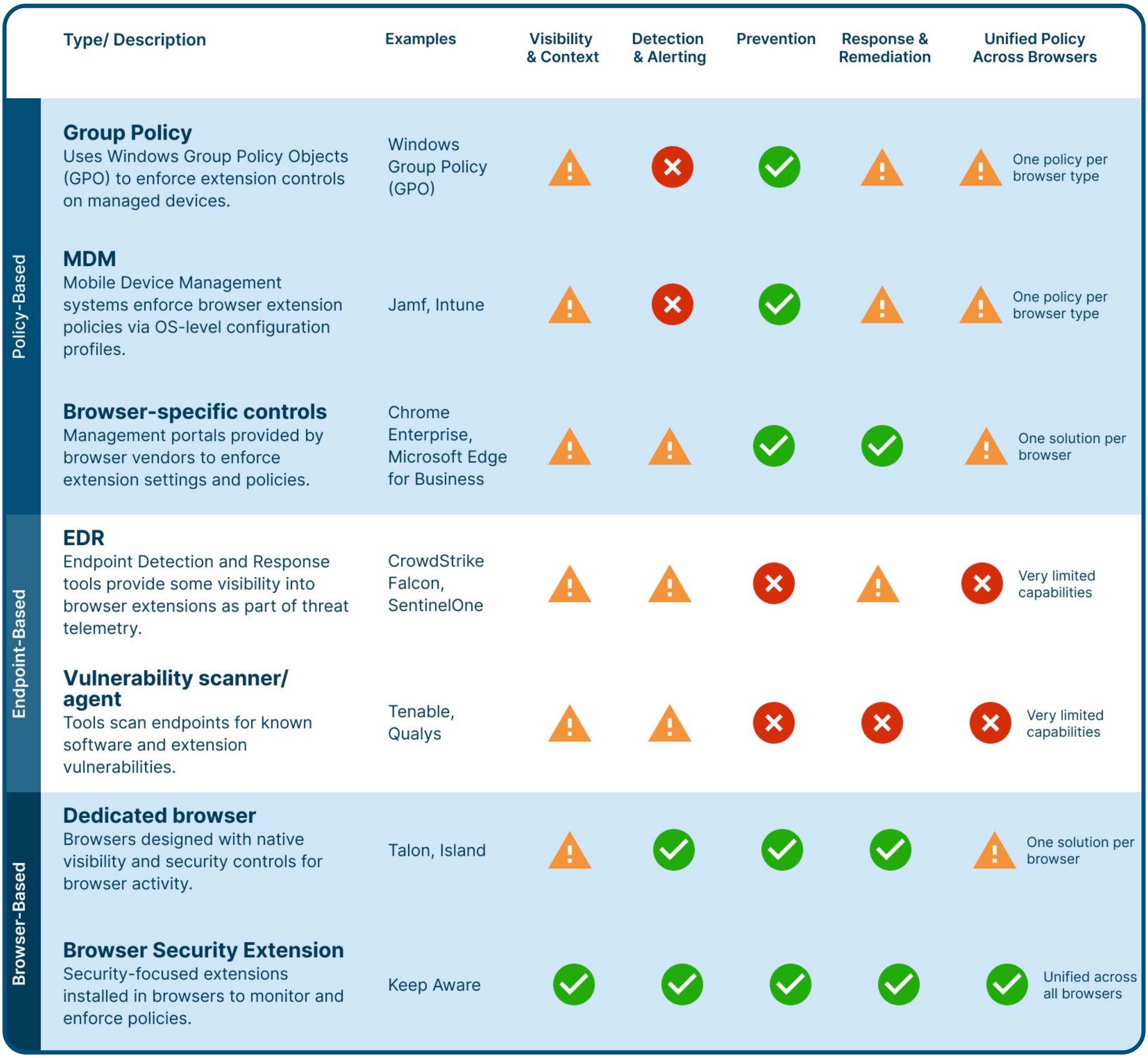
Dedicated Enterprise Browsers

Enterprise browsers offer strong prevention and policy enforcement, with deep visibility into activity within their own browser ecosystem. They can block unapproved extensions outright and detect certain suspicious behaviors. However, these advantages only apply if every user adopts the enterprise browser, a significant hurdle in organizations with established browser preferences. Deploying a new browser also adds operational and training challenges.

Browser Security Extensions (Keep Aware)

Keep Aware’s security extension model delivers comprehensive visibility, prevention, and real-time detection across all major browsers without requiring a browser replacement. It continuously monitors for risky or malicious extension activity and can block threats instantly. Centralized controls apply across the organization, regardless of browser type. Deployment is lightweight and seamless, installing directly into existing browsers without impacting user workflows.

Even if your organization isn’t able to adopt a purpose-built solution today, the comparison chart below can help you identify where your existing stack provides meaningful coverage and where critical gaps may exist.



	Type/ Description	Examples	Visibility & Context	Detection & Alerting	Prevention	Response & Remediation	Unified Policy Across Browsers
Policy-Based	**Group Policy** Uses Windows Group Policy Objects (GPO) to enforce extension controls on managed devices.	Windows Group Policy (GPO)	⚠	✕	✓	⚠	⚠ One policy per browser type
	MDM Mobile Device Management systems enforce browser extension policies via OS-level configuration profiles.	Jamf, Intune	⚠	✕	✓	⚠	⚠ One policy per browser type
	Browser-specific controls Management portals provided by browser vendors to enforce extension settings and policies.	Chrome Enterprise, Microsoft Edge for Business	⚠	⚠	✓	✓	⚠ One solution per browser
Endpoint-Based	**EDR** Endpoint Detection and Response tools provide some visibility into browser extensions as part of threat telemetry.	CrowdStrike Falcon, SentinelOne	⚠	⚠	✕	⚠	✕ Very limited capabilities
	Vulnerability scanner/ agent Tools scan endpoints for known software and extension vulnerabilities.	Tenable, Qualys	⚠	⚠	✕	✕	✕ Very limited capabilities
Browser-Based	**Dedicated browser** Browsers designed with native visibility and security controls for browser activity.	Talon, Island	⚠	✓	✓	✓	⚠ One solution per browser
	Browser Security Extension Security-focused extensions installed in browsers to monitor and enforce policies.	Keep Aware	✓	✓	✓	✓	✓ Unified across all browsers

This table compares browser extension management methods, showing that browser-based solutions offer the most comprehensive and unified protection across key security functions.

Conclusion

Browser extensions enhance productivity but introduce significant, often hidden, security risks if left unmanaged. Traditional approaches, whether policy-based, endpoint-driven, or tied to a dedicated enterprise browser, each address part of the problem but fall short in coverage, visibility and context, detection speed, or ease of deployment.

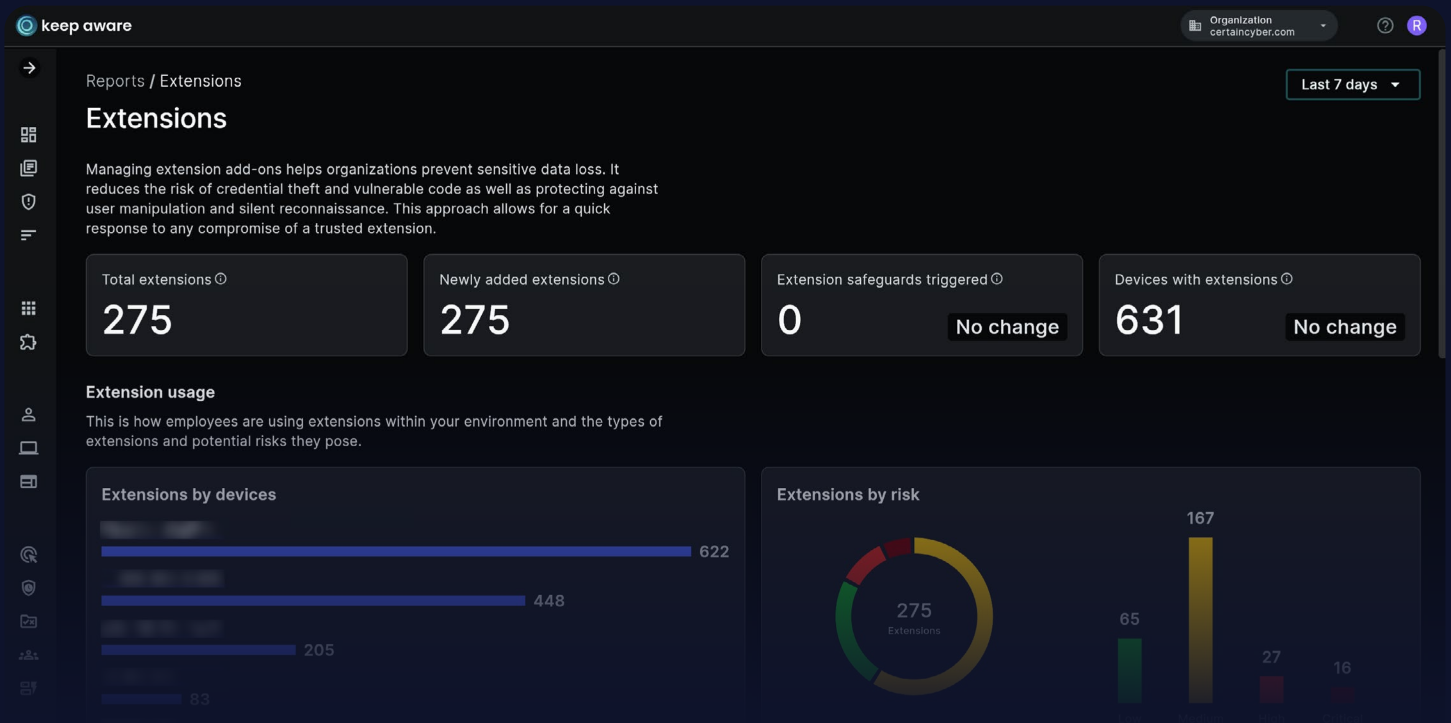
Keep Aware fills these gaps by delivering full visibility, real-time prevention, and active behavioral monitoring across all browsers, all without forcing a browser change. This enables CISOs and security teams to manage extension risk effectively and protect sensitive data.

S

Shield browsers from malicious extensions

Request a Demo

Risky browser extensions leave your organization vulnerable.
Keep Aware ensures only safe extensions are in use.



keep aware

Organization
certaincyber.com

Reports / Extensions

Last 7 days

Extensions

Managing extension add-ons helps organizations prevent sensitive data loss. It reduces the risk of credential theft and vulnerable code as well as protecting against user manipulation and silent reconnaissance. This approach allows for a quick response to any compromise of a trusted extension.

Total extensions ⓘ
275

Newly added extensions ⓘ
275

Extension safeguards triggered ⓘ
0
No change

Devices with extensions ⓘ
631
No change

Extension usage

This is how employees are using extensions within your environment and the types of extensions and potential risks they pose.