Island

# The Enterprise Browser Buyers Guide

# Table of contents

# Introduction

> By 2030, enterprise browsers will be the core platform for delivering workforce productivity and security software on managed and unmanaged devices for a seamless hybrid work experience.
>
> Gartner®

The most commonly used enterprise application today isn't Office 365 or Salesforce. It's the browser. Ever since work went online, data moved to the cloud, and software became a service, the browser has been at the center of the modern workspace.

Yet, the browser isn't even an enterprise application. It was meant for shopping, streaming, and socializing. It was built to serve advertisers and their consumers, not organizations and their employees.

Which is why working on a consumer browser today means surrounding it with agents, proxies, gateways–an endless stack of security and IT solutions–just to get it to cooperate with the enterprise. The result is a stack that's too complex, fragile, and costly to manage. And an end user experience full of delays, disruptions, and frustrations.

**But what if the browser was designed for the enterprise?**

This is the enterprise browser. The ideal enterprise workspace that naturally embeds the core security, IT, and productivity needs of the organization into the familiar, Chromium browsing experience end-users love. An enterprise browser helps CISOs deliver a truly secure-by-design work environment for their organization. It helps CIOs provide a dramatically simpler, more efficient, and cost-effective platform for application delivery and enablement. And it provides end users with a faster, smoother work experience, productivity-boosting features, and enhanced privacy.

This guide will introduce you to the enterprise browser and provide you with the necessary context and key considerations to help make an informed decision on whether an enterprise browser is right for your organization. By the end of this guide, you'll know why the enterprise browser exists, what value it delivers, which use cases it addresses, how it compares to alternative options, and where to go next in your journey.

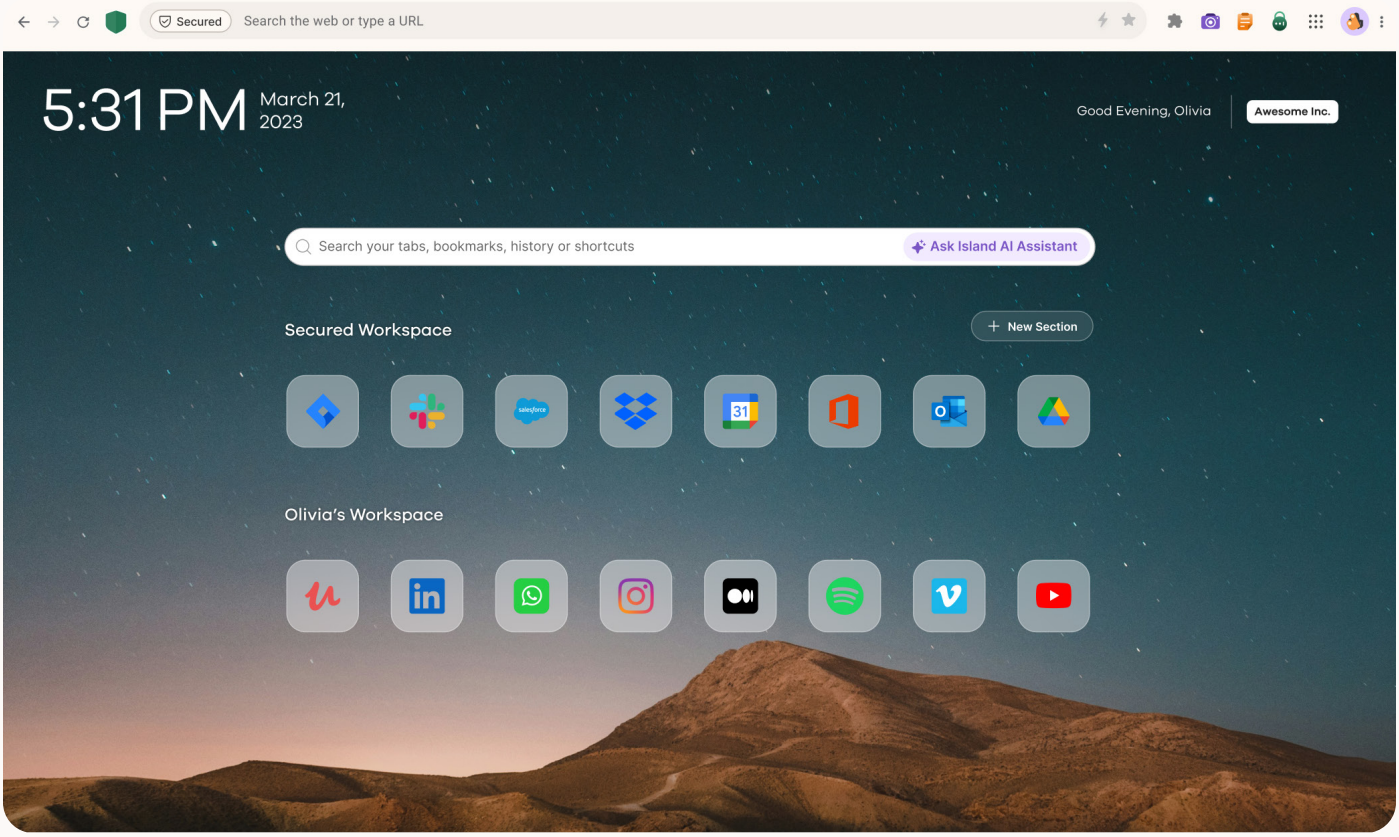
*Gartner, Emerging Tech: Security — The Future of Enterprise Browsers, Dan Ayoub, Evgeny Mirolyubov, Max Taggett, Dave Messett, 14 April 2023. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.*

# What is an enterprise browser?

The web browsers most people use today like Google Chrome or Microsoft Edge were designed for the widest possible user community, and optimized for personal use. An enterprise browser was designed specifically for the workplace, and optimized to serve the enterprise needs of the organization. It does so by taking the core security, IT, and productivity capabilities that typically surround the browser, and naturally embedding them into the browser itself.

The result is a browser experience optimized for end users, coupled with an admin console optimized for IT and security teams.

At its core, an enterprise browser is built on the Chromium browser engine–the same technology that powers Chrome, Edge, Brave, and other popular consumer browsers. By using Chromium, an enterprise browser can deliver the smooth, familiar user experience users expect, while ensuring 100% compatibility with SaaS and web applications right out of the box.



# What are the benefits of an enterprise browser?

Because the enterprise browser is at the center of enterprise work, its impact can be felt by many different stakeholders across the organization, from security admins to end users.

## The CIO

- **Efficiency and Cost Savings**
  First and foremost, an enterprise browser dramatically simplifies your IT infrastructure and security stack. Many of the security tools, endpoint agents, and IT solutions needed to secure and enable the enterprise are now embedded in the browser or are no longer needed in many cases. Which means the cost and effort involved in licensing, deploying, maintaining, and supporting all the infrastructure is brought to an absolute minimum.

- **Application Provisioning**
  With an enterprise browser, users access all the applications they're entitled to–SaaS, web applications, and even non-web apps via SSH or RDP. It's the ideal access point for application virtualization platforms to connect users to traditional "thick" applications without requiring a desktop installation. This way, new apps can be introduced simply, and new users can onboard by just logging in and getting to work.

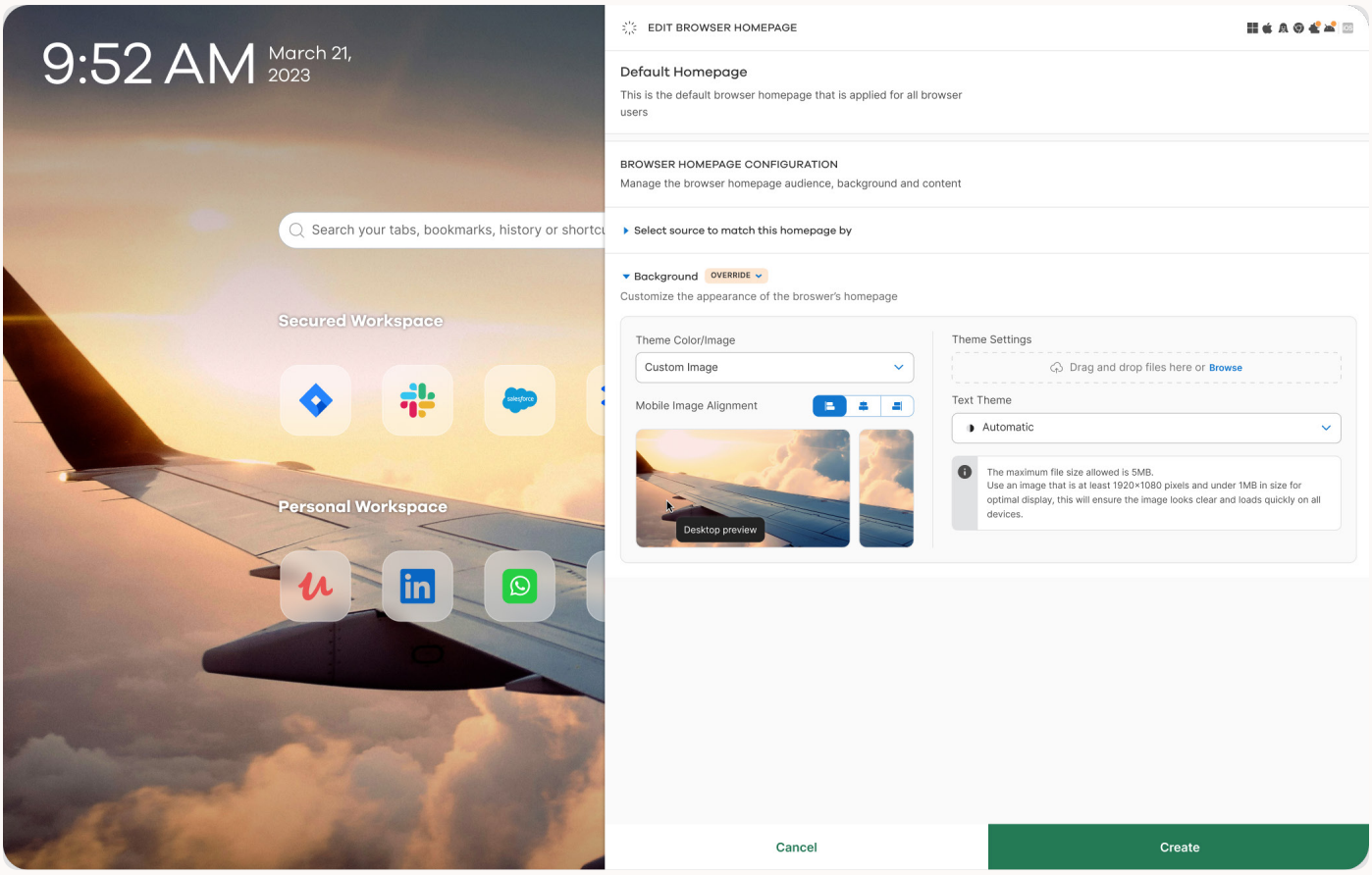
- **Digital Experience**
  An enterprise browser provides analytics on application usage, performance, and workflow insights. This data can be used to optimize application spend, identify and remediate performance issues, and inform IT strategy to maximize business value. Unlike alternative solutions that require application-side integrations or additional agents on the endpoint, an enterprise browser naturally collects these analytics across every application interaction.

**94%**

of contractor VDI costs were eliminated at a global pharmaceutical company.

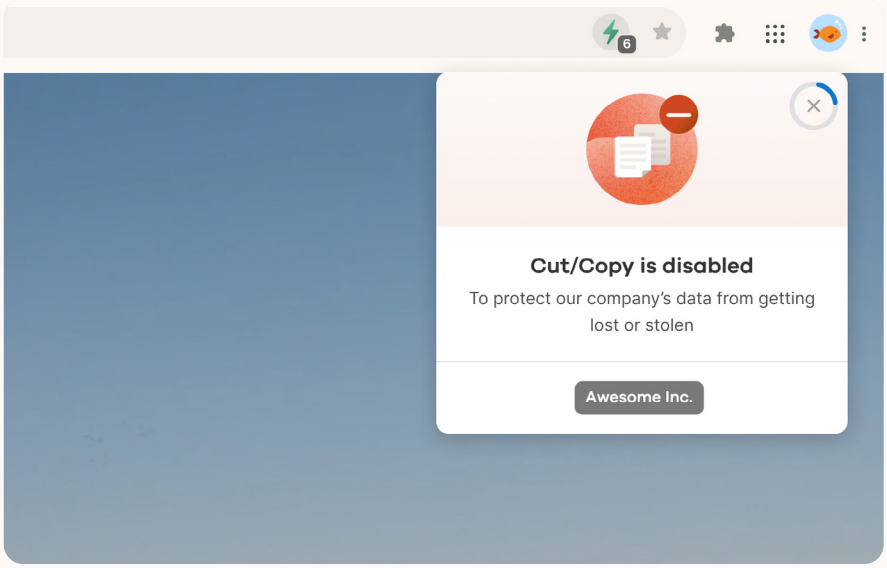
- **Remote Access**
  an enterprise browser can enable remote access for a hybrid workforce with employees outside the corporate office. Many organizations use an enterprise browser to reduce the need for traditional VPN or virtual desktop infrastructure (VDI) while empowering employees to access their applications from anywhere. An enterprise browser can be easily deployed to personal devices to enable BYOD initiatives as well.

- **Employee Awareness and Education**
  As the daily workspace for most users, an enterprise browser can enable employee awareness and education. It can deliver contextual messaging within the browser, onboard new users, activate new applications, and help users understand active IT policies. And with the ability to brand it as your own, the enterprise browser can ensure your organization is consistently represented across the workspace.



## The CISO

- **Data protections**
  Work's widespread shift to SaaS and internal web apps inside a consumer browser has made data protection more challenging than ever. With no control over browser activity itself, legacy approaches have taken a "blunt instrument" approach, securing data while disrupting work and driving up cost and complexity in the process.




An enterprise browser, however, builds dynamic data protections into the browser itself, enabling you to build policies that prevent data leakage without disrupting organizational workflows. Its DLP controls protect sensitive data from being improperly downloaded or uploaded before it leaves or enters the browser. Robust policies govern the exact context in copy/paste, screenshots, printing, or saving can be executed, so data can move freely between work applications while keeping it from leaking to undesired destinations.

- **Visibility**
  An enterprise browser offers unprecedented visibility into all browser activity in a way that simply wasn't possible before. Most legacy security tools offer visibility via network traffic inspection by decrypting SSL traffic. An enterprise browser offers visibility into browser behavior without any unnatural network traffic manipulation. Security teams can see the applications in use, monitor specific clicks, keystrokes, or workflows within an application, and connect actions to the user's identity. And unlike legacy approaches, organizations can choose what and how to monitor, enabling them to keep personal browsing private.

**3 min**

to open and close a phishing attempt investigation by The Bank of Marion. Previously took several hours.

- **Zero trust security**
  An enterprise browser can be used to implement a zero trust security framework across a wide range of deployment scenarios:
  - User identity is verified with IdP integration and multi-factor authentication.
  - Device posture is checked to verify the device meets security standards.
  - Network and geolocation are examined to see where the request is coming from.

  All of these elements are continuously evaluated with every access request, making it easy to implement and enforce robust zero trust security policies across all browser activity.

- **Safe Browsing**
  An enterprise browser comes embedded with powerful security tools that protect all browser activity from the myriad of web-born threats, regardless of device or network. Malware is detected and blocked before ever reaching the endpoint. Phishing attacks are stopped before credentials are compromised. Unsafe or inappropriate sites are blocked from access. Sophisticated attack vectors are neutralized by isolating key browser components and protecting local browser data stores. And with robust event data at their disposal, security teams can respond to incidents and resolve investigations in minutes instead of hours or days.

- **Password protections**
  An enterprise browser offers several key advantages over consumer browsers to help protect, manage, and govern passwords.
  - An enterprise browser naturally protects from phishing attacks, password exfiltration, or password interception through local malware like keyloggers.
  - An enterprise browser provides an integrated password manager that's optimized for enterprise use.
  - An enterprise browser can be used to implement privileged access management (PAM) workflows where users can authenticate with credentials assigned to them, without ever seeing the password. This is especially useful in situations where several employees need access to a shared company account, such as social media platforms.

## The End-User

- **Access**
  An enterprise browser creates the ideal workspace for users to quickly access all work applications and resources in a natural, familiar interface. By integrating with enterprise identity providers, a user simply logs in to the browser and automatically accesses all the applications and links they need based on their identity, role, or job function. Single sign-on enablement makes access frictionless. Newly deployed applications automatically show up in the browser. Streamlined access to external applications and resources is done via integrated privileged access management and password management. And native SSH and RDP delivers access to user workflows outside of web and SaaS.

- **Productivity**
  Consumer browsers are optimized for personal convenience, advertising, consumer workflows like online shopping and social media. By contrast, an enterprise browser is designed to optimize for the workplace. It is tied to your enterprise identity (rather than a personal account), with built-in ad blocking to remove distractions and speed up browsing, and integrated tools to speed up common workflows. This includes a smart clipboard manager, an AI assistant, password manager, and PDF editor. An enterprise browser also integrates with enterprise cloud storage to streamline downloads and uploads. And instead of having to manage a collection of extensions and external productivity tools, the IT team simply deploys and configures everything inside the browser itself.

- **Automations**
  An enterprise browser delivers a significant productivity boost with powerful workflow automations. Users who carry out repetitive tasks, like customer success teams responding to client requests or managing ticketing systems, can speed up their daily workflow with smart automations. For example, client details can be automatically added to the clipboard manager for instant access and ticketing systems can be pre-filled with common responses based on the context of the user and their activity. And since these automations are native to the enterprise browser, they can be applied anywhere–regardless of whether the underlying application supports it.

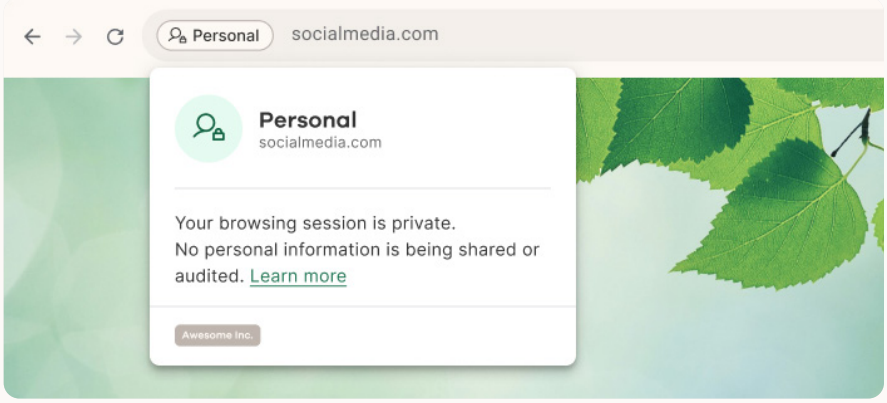
- **Education and awareness**
  An enterprise browser delivers helpful, context-based feedback to

**80%**

Faster point-of-sale system launch by a national retailer, saving 40 seconds on each launch.

users as they navigate through their workflows. For example, users will be notified why an action was prevented as the result of an IT or security policy in place. Users may also get a notification educating them on their organization's data security policies when they arrive at an application with sensitive data, which minimizes frustration and maximizes transparency. Users can even request exceptions when their work requires going outside the typical IT policy framework. Their request would go directly to their service desk and they'd get a response in minutes, all without leaving the enterprise browser.

- **Privacy**
  An enterprise browser can apply policy based on the context of the user's browser activity, making it possible to separate between work and personal browsing. Unlike legacy solutions that decrypt and monitor all activity on the device, an enterprise browser finally makes it possible to log only the applications, sites, and activities related to work–while ignoring everything else. A simple indicator shows users whether their browser activity is being monitored on every page they navigate to. By making it possible to respect personal privacy at work, an enterprise browser fosters a sense of mutual trust between the user and employer.




- **Performance**
  An enterprise browser is optimized for speed and responsiveness even more so than a consumer browser. For example, it minimizes unnecessary network requests by blocking ads and trackers. It also eliminates the performance delays and disruptions caused by added layers of abstraction between the user and their work as with desktop virtualization and remote browser isolation. Which means working on an enterprise browser feels identical to working on a consumer browser–just noticeably faster.

# Common use cases for an enterprise browser

Secure SaaS and Web Access | VDI Reduction | Zero Trust Workflow | BPO and Third-Party Access

Data Loss Prevention | Mergers, Acquisitions, and Divestitures | BYOD Programs | Incident Response and Resiliency

## Solve the SaaS data leakage problem

The shift to SaaS and web applications means critical data and workflows move through a consumer browser that offers very little in terms of security and data controls. This forces organizations to surround the browser with tools in an attempt to prevent data leakage and protect their applications. With an enterprise browser, the critical data inside SaaS and web apps are secure by design. Organizations have a closed-loop system where security and access policies can be implemented across any SaaS or web app. So data remains fundamentally secure, without relying on complex network controls, app-specific APIs, or inefficient solutions outside the browser.

Key Capabilities:

- Access management with IdP integration that supports granular controls to protect specific pages, workflows, and data across any application.

  ***Example: an enterprise browser adds the ability to protect legacy in-house web applications with MFA security, without modifying the application source code.***

- Data protection policies to govern how data can move between or outside of applications.

  ***Example: an enterprise browser offers controls to protect customer records from being copied and pasted to a personal email.***

- Conditional access policies to ensure that a device meets the organization's requirements before accessing critical SaaS applications.

  ***Example: an enterprise browser continuously checks the device posture for patch level, disk encryption status, and an active endpoint protection agent.***

## Radically reduce VDI

Many organizations turned to virtual desktop infrastructure (VDI) solutions to provide browser access to critical applications for off-premises users. This adds significant cost, complexity, and end-user frustration. An enterprise browser is a modern alternative that delivers all the security, visibility, and remote access capabilities without any of the drawbacks of VDI. Switching to an enterprise browser can greatly reduce the reliance on VDI, delivering dramatic cost savings and a radically improved user experience.

---

Key Capabilities:

- Data segregation and application isolation between an enterprise browser and the device it's running on to provide deployment flexibility with robust security.

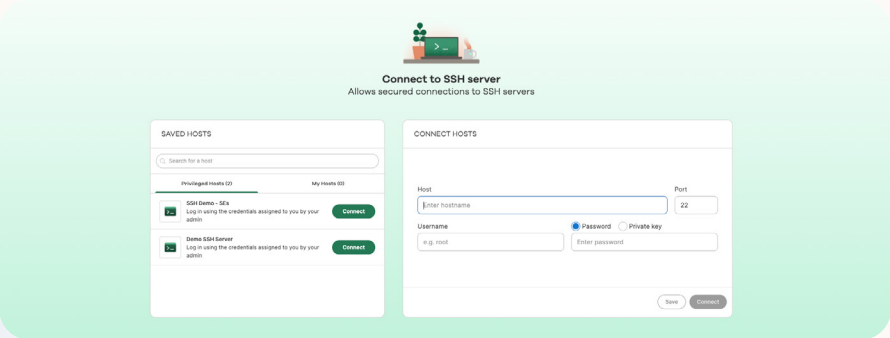
  ***Example: an enterprise browser offers the ability to prevent data from being saved, downloaded, or copy/pasted from an enterprise application when operating on an unmanaged device.***

- Remote access capabilities to support a hybrid or remote workforce.

  ***Example: an enterprise browser offers the ability to make a secure network connection to private to internal enterprise resources without requiring an external VPN client.***

- Broad application support and native user experience.

  ***Example: an enterprise browser supports web applications, SSH access, and RDP sessions to support the widest possible range of business workflows, all without requiring the inherent performance penalties of virtualization.***



## Extend zero trust throughout the workflow

Zero trust is an essential security paradigm that moves away from static network perimeters to focus on user identity, device posture, and least-privilege resource access. When applied consistently, this approach dramatically reduces risk across many categories of cybersecurity threats. Consumer browsers, however, don't cooperate with a zero trust framework, causing security checks to be performed externally by agents on the endpoint or network infrastructure. An enterprise browser will play an active role in embedding zero trust practices into the browser itself - where the majority of application and data access flows–creating an end-to-end zero trust work experience.

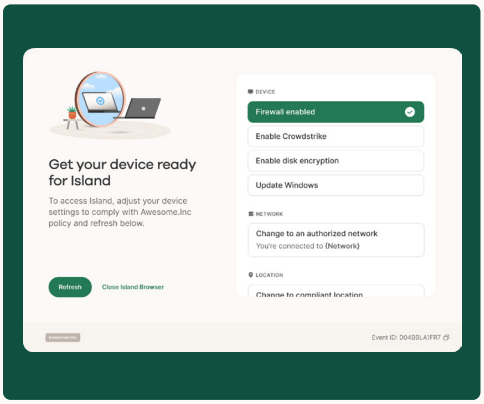
---

Key Capabilities:

- Verify user identity through an enterprise Identity Provider (IdP) with multi-factor authentication support.

  ***Example: an enterprise browser offers native integration with your IdP and offer configurable settings to invoke additional MFA challenges when accessing sensitive applications.***

- Device assessment to determine if the device being used meets security requirements.




***Example: an enterprise browser detects the security configurations of the device it's running on, including OS patch level, disk encryption status, active MDM and EDR agents, network connection, and geo-location.***

- Integrated zero trust network access for secure connectivity to private applications.

  ***Example: an enterprise browser establishes a ZTNA connection to a private application only after validating the user identity, device posture, and access authorizations for that application.***

## Provide safe, simple, BPO and Third-Party Access in minutes

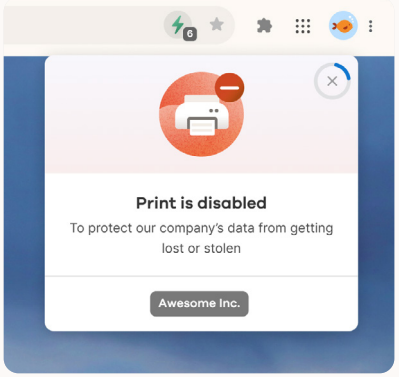
As organizations supplement their employee workforce with contractors or business process outsourcers (BPOs), the challenge for efficient and secure access compounds. This is often addressed by provisioning managed laptops or virtual desktops. The hardware route adds cost and serious delays, particularly when contracted workers are in foreign countries. The virtual route also adds cost and complexity, with the added burden of a sub-par user experience and higher administrative overhead. An enterprise browser enables contractors to simply log in and get to work using their existing hardware while giving the organization full control over access, data security, and visibility. And unlike VDI, there's no performance penalty for users.

Key Capabilities:

- Self-guided installation on any device, without interfering with existing management agents.

  ***Example: a contractor can install an enterprise browser on their laptop that's managed by their contracting firm without requiring an IT support ticket.***

- Application and data boundaries to prevent leakage of sensitive data.




***Example: a contractor working through an enterprise browser can access only the applications required for their work remit, and no data can leave the browser through copy and paste, screenshots, printing, or downloading to their desktop.***

- Integrated zero trust network access for secure connectivity to private applications.

  ***Example: a contractor can access an internal application on a private network through an enterprise browser without requiring any additional network configurations or agents installed on their device.***

## Build data loss prevention into the workplace

Today's work happens outside the office, from unmanaged devices and networks, and with an ever-expanding set of SaaS and web applications. It's a work environment that legacy DLP platforms simply weren't designed for. An enterprise browser builds data loss protection capabilities into the workspace (the browser) itself, delivering a more effective, and efficient way to protect data in today's modern workplace.

Key Capabilities:

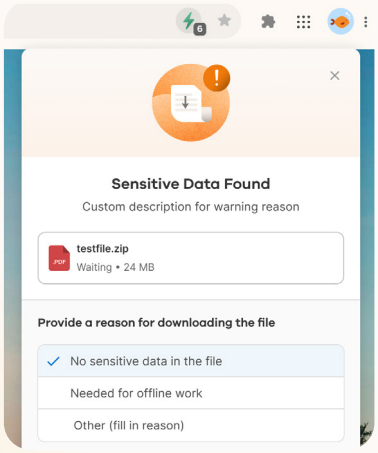
- Application and data boundaries keep sensitive data within defined enterprise applications and prevent leakage across all means of egress.

  ***Example: employees working with sensitive financial records can move data between several applications used for financial reporting. An enterprise browser stops that data from moving into a personal email or downloaded to their desktop.***

- Data masking hides sensitive data from view on a page until it's needed.

  ***Example: personal contact information is redacted on screen for customer support staff, but they can selectively unmask that data if needed to resolve an issue. An enterprise browser logs each unmasking event and the user who viewed it for auditing purposes.***

- DLP detectors flag sensitive data to stop leakage, regardless of which application it originates from.



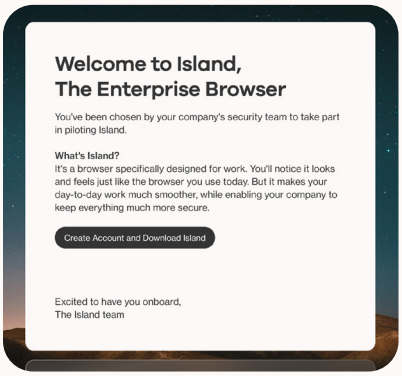

***Example: an enterprise browser will detect any attempt at downloading files containing credit card numbers or social security numbers to prevent leakage and alert on the event for internal review.***

## Do mergers, acquisitions, and divestitures without interrupting work

Successfully merging together the IT systems of two organizations can take months, even years. This can create unwelcome friction and extended work stoppages following a merger or acquisition, precisely at the moment where efficient communication and data sharing is most critical. With an enterprise browser, lines of communication and application access can be opened from day one, hour one. Employees of the acquired company can launch an enterprise browser on their laptop and immediately access the applications, resources, and communication tools they need to interface with their new colleagues. The same is true for divestitures: an enterprise browser enables you to gracefully separate business units while maintaining access until the final divestiture is complete.

Key Capabilities:

- Rapid deployment of an enterprise browser to existing laptops or mobile devices.




***Example: On day one of an acquisition, employees get an email with a link to download an enterprise browser and login with their credentials. This step takes only minutes and does not require hands-on IT support or provisioning of new equipment for employees.***

- Extend access through an enterprise browser with consistent IT and security policies.

  ***Example: Employees can access all the applications and resources from the acquiring organization before infrastructure changes are completed, with IT and security policies enforced through the enterprise browser.***

- Provide access across disparate networks without VPN or infrastructure changes.

  ***Example: Employees who need access to private or internal applications can connect through an enterprise browser with integrated ZTNA before any changes to the network infrastructure are completed.***

## Deliver a safe, viable BYOD initiative

Implementing a BYOD initiative that satisfies business requirements, meets IT and security needs, and is practical enough to be adopted by employees is a challenge that's gone unsolved for more than a decade. Mobile device management (MDM) solutions can satisfy the business and IT requirements, but often require users to give up an uncomfortable amount of control over their personal devices. VDI solutions offer better segmentation between work and personal use, but come at a steep cost and impair the user experience. An enterprise browser, however, balances the needs of all three constituencies with an elegant solution that is lower cost, easy to administer, and delivers a natural user experience while preserving the user's independent control over the personal device.

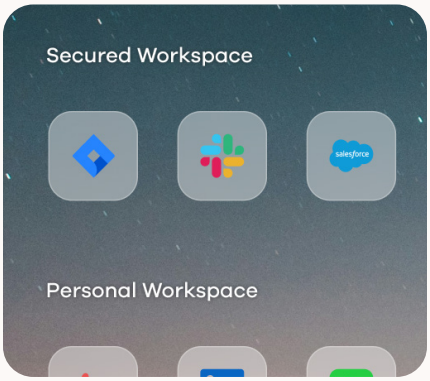
---

Key Capabilities:

- Simple self-service onboarding with a familiar workflow.

  ***Example: Anyone who's installed a browser can install an enterprise browser on their personal device. There are no unfamiliar steps requiring certificate installation or device profiles like with MDM.***

- Full separation between work and personal content.




***Example: All work activity happens within the enterprise browser and it's configured to prevent any data or documents from moving outside the browser. When work is complete, the employee simply closes the enterprise browser.***

- Remote de-provisioning when the BYOD device is no longer needed for work.

  ***Example: When an employee leaves the organization, or if they want to trade in their device, IT staff can remotely terminate all access to the enterprise browser on that device. Since no data was ever saved to the device itself, there's nothing to clean up and there's no need for hands-on de-provisioning.***

## Keep business going during security incidents and IT shutdowns

During a cybersecurity incident response, IT teams may need to shut down endpoints and disable network segments to contain the threat. Employees are typically forced to work on other devices, or stop working altogether until the threat is eliminated, causing intolerable delays and stoppages to the flow of business. An enterprise browser offers a compelling solution for this scenario with self-service installation on personal devices or other alternative hardware. Using an enterprise browser, staff can instantly access critical communications tools and business applications while their regular IT systems are down, ensuring business continues as usual, no matter how severe the incident is.

Key Capabilities:

- Quick self-service installation to a wide range of devices.

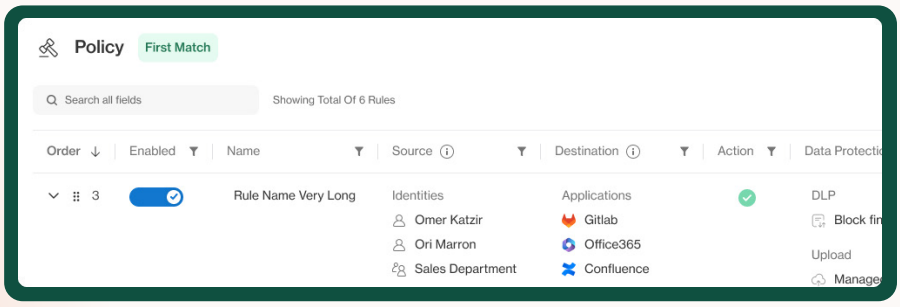
  ***Example: During an incident, staff need to quickly set up an alternative workstation. An enterprise browser is easy to download and install without requiring IT assistance.***

- Dynamic policies that step up security controls based on device posture.

  ***Example: While staff are using alternate devices during an incident, an enterprise browser detects the device posture and automatically applies the appropriate security controls to prevent data leakage.***

- Centralized management to efficiently manage access during an incident.

  ***Example: The centralized management capabilities of an enterprise browser make it possible to gradually expand access and restore business services.***



# The industry experts' perspective

## Gartner, Emerging Tech: Security — The Future of Enterprise Browsers

*Published 14 April 2023*

Gartner

***"By 2026, 25% of enterprises will be using managed browsers or extensions, up from less than 10% today."***

***"By 2030, enterprise browsers will be the core platform for delivering workforce productivity and security software on managed and unmanaged devices for a seamless hybrid work experience."***

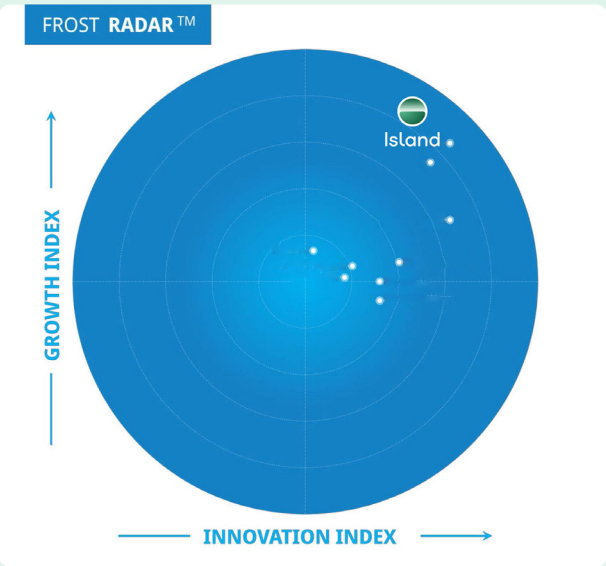
***"By 2030, the browser will become a platform from which enterprises can distribute software, collect intelligence, control access and securely enable remote work."***

*Gartner, Emerging Tech: Security — The Future of Enterprise Browsers, Dan Ayoub, Evgeny Mirolyubov, Max Taggett, Dave Messett, 14 April 2023. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.*

## Frost & Sullivan Radar

*Published December 2023*

FROST & SULLIVAN




## Omdia Market Radar for Browser Security 2023

*Published August 21, 2023*

OMDIA

***"An enterprise browser thus comes with all the security policies required for protecting an organization, such as completely blocking access to dangerous or inappropriate sites, as well as imposing limitations on access rights."***

# Enterprise browser vendors

## Island

Island is the pioneer and market leader of the enterprise browser market. It has the largest user base and the widest set of enterprise browser capabilities

**Headquarters:** Dallas, TX, USA
**Founded in:** 2020
**Website:** island.io
**Customer Reviews:** Gartner Peer Insights

## TALON

Talon was a fast follower to Island. In 2023, Palo Alto Networks acquired Talon to complement their Prisma SASE product line. Their product positioning is focused on using Talon for unmanaged devices to steer traffic through Prisma.

**Headquarters:** Tel Aviv, Israel (Palo Alto Networks is Santa Clara, CA, USA)
**Founded in:** 2021 (Palo Alto Networks, 2005)
**Website:** talon-sec.com (paloaltonetworks.com)

## citrix

Citrix is best known for their desktop virtualization solutions. In 2023 they rebranded the Citrix Workspace Browser as the Citrix Enterprise Browser. The depth of capabilities for the Citrix Enterprise Browser is more modest and largely depends on interactions with other Citrix services.

**Headquarters:** Fort Lauderdale, FL, USA
**Founded in:** 1989
**Website:** citrix.com

## MAMMOTH CYBER

Mammoth Cyber, previously known as AppAegis, recently rebranded their zero trust security solution as the Mammoth Enterprise Browser. Their product focus is exclusive to security use cases, narrower than other enterprise browser vendors.

**Headquarters:** Palo Alto, CA, USA
**Founded in:** 2019
**Website:** mammothcyber.com

## SURF

Surf is a recent enterprise browser startup. They describe their product as “The Zero Trust Enterprise Browser” and focus exclusively on security use cases. As a seed-stage startup, their actual customer deployments are unknown.

**Headquarters:** New York, NY, USA
**Founded in:** 2022
**Website:** surf.security

# Alternatives to an enterprise browser

There are several products on the market today that address similar use cases as an enterprise browser. Some of these are legacy products that pre-date the introduction of enterprise browsers, while others are newer products that are often positioned alongside enterprise browsers.

## Browser extensions

Several vendors offer browser extensions that can be installed within a consumer browser to add enterprise security and management features. Confusingly, some vendors market these as enterprise browsers, though the distinction between an extension and a true enterprise browser is important.

**Strengths:**

- Low friction deployment that integrates into the end users' existing browser
- User experience remains largely unchanged compared to a regular consumer browser
- The lightweight development and infrastructure requirements of a browser extension allows vendors to offer these products at relatively low cost

**Weaknesses:**

- Extensions are limited in their capabilities by the extension framework as defined by the consumer browser vendors. These frameworks change from time to time, so there's a risk that existing features and functionality would be negatively impacted with future extension framework changes.
- Deploying and managing browser extensions requires a separate device management platform, like an MDM or UEM. Extensions are not recommended for unmanaged deployments like BYOD or third-party contractors, BPOs, etc.
- Security protections are limited. Extensions cannot protect against local attack vectors like malware on a device that hijacks cookies, cache, keystrokes, or passwords. Extensions are also limited in their ability to interact with the underlying OS, so they're not able to provide full zero trust security with deep device and network inspection.
- Browser extensions are not available for mobile devices, so an environment with a mix of desktop and mobile devices will require multiple solutions.

**Example Vendors:**

ERMES
Ermes Browser Security

LayerX
LayerX Security

SAVVY
Savvy Security

SERAPHIC
Seraphic Security

# Remote browser isolation

Remote browser isolation (RBI) is a technology that predates the introduction of enterprise browsers. These solutions are squarely focused on security use cases, mainly protecting against malware or malicious web content. As the name implies, these products host a browser environment on a remote host where web pages are rendered and then streamed back to the user as a video stream.

**Strengths:**

- RBI offers full isolation between the web content and the endpoint device. Only the visual content of a webpage is delivered to the endpoint.
- Malware or malicious web content is contained within the remote environment so the local endpoint is protected.
- RBI may be useful for specific use cases like threat research where malware encounters are expected.

**Weaknesses:**

- RBI creates an unnatural user experience that adds latency with the extra layer of remote browser rendering. Rendering issues and web application compatibility issues are more common as well.
- RBI solutions try to offset the user experience weakness described above by selectively choosing only some web destinations to send to the remote environment. This is done through web classification and risk scoring. The problem with this approach is that it assumes classification will be 100% accurate; any time malicious content is falsely classified as safe it defeats the purpose of RBI.
- RBI requires substantial infrastructure and bandwidth to host and stream the remote browser environment, so costs are high relative to the value it offers.

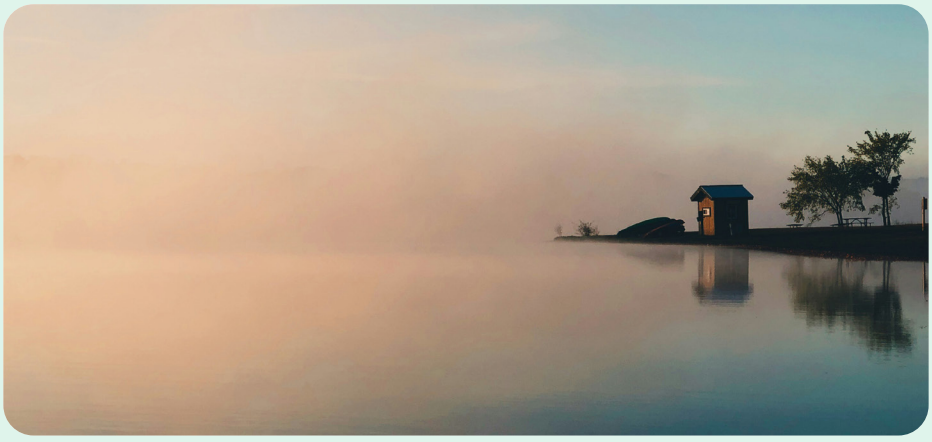
**Example Vendors:**

AUTHENTIC8
Authentic8

CLOUDFLARE
Cloudflare

GARRISON
Garrison

MENLO SECURITY
Menlo Security



# The enterprise browser deployment experience

Deployments usually start with one or two use cases and expand from there. By default, it's already a fully functional browser, which means you can easily deploy it to users first and build out policies and configurations in parallel. This speeds up deployment as well as value - delivering impact in just days instead of months.

## 1

**Connect the enterprise browser with your identity provider for user authentication**

An enterprise browser supports all common providers and offer both SAML and SCIM support.

## 2

**Deploy the enterprise browser to your users**

You can push the installer through device management tools (like InTune or Jamf) or by a self-service download link. Just download, install, and that's it.

## 3

**Launch the enterprise browser and import settings**

Users log in via your IdP then simply import their personal settings and bookmarks.

## 4

**Start building policies**

Choose a group of users and a few key applications and start building policies that align with your workflow. Then repeat with more workflows or use cases.

# User Experience

A key motivation for adopting an enterprise browser is its natural user experience. Because it's powered by the Chromium browser engine like Google Chrome and Microsoft Edge, users enjoy a familiar user experience. Users gain easy access to work applications while experiencing faster browsing and ad blocking. No complicated and slow VPN or VDI sessions are required.

**Enterprise browser deployment**
Installation is done in moments via device management tools or by self-guided installation. The whole process is no more complex than installing a consumer browser.

**Improved user productivity**
An enterprise browser offers productivity boosting tools that help accelerate and streamline user workflows. These can include generative AI tools, workflow automations and secure cloud storage capabilities.

**Enterprise identity and SSO**
By integrating with the enterprise identity provider the user is greeted with a familiar login flow. Once logged in, they will automatically see their application entitlements and can access apps and resources simply via SSO.

**Enterprise branding and messaging**
An enterprise browser makes it possible to apply company branding and tailored messaging to reflect the organization's identity. For example, in a blocked navigation or data protection event, users will receive a notification featuring company-specific branding and messaging explaining what happened, why, and what to do next.

**Native browser experience**
An enterprise browser delivers the natural, smooth browser experience that users are familiar with. The navigation and shortcuts are nearly identical, all extensions are 100% compatible, and everything renders exactly as it would on a consumer browser.

# Common Questions About an Enterprise Browser

| | |
|---|---|
| **Do I need to test all my applications for compatibility?** | All leading enterprise browsers are based on the Chromium rendering engine, the same as Chrome, Edge, Brave, and other browsers. This means that any application that works with Chrome or Edge will work with an enterprise browser, and the page rendering is identical. |
| **Can I use an enterprise browser with legacy applications that require Internet Explorer?** | Some enterprise browsers offer an IE Legacy Mode that swaps out the Chromium rendering engine to use the IE engine that's still bundled with the Windows OS. Be sure to ask your enterprise browser vendor if they offer this capability. |
| **Does an enterprise browser introduce any performance penalties?** | An enterprise browser offers the same performance as a consumer browser for all web applications and web browsing. In many situations, you'll actually see a performance improvement over consumer browsers if the enterprise browser offers ad and tracker blocking. Be sure to ask your enterprise browser vendor if they offer this capability. |
| **How does an enterprise browser compare to VDI/DaaS streamed through a browser?** | Virtual desktops are often used to fill a similar role as an enterprise browser. There are some significant differences between the two technologies to consider: VDI requires substantial infrastructure investments in terms of servers, networking, and virtualization software. Even when cloud hosted, the service cost reflects the large infrastructure requirement. VDI also puts a burden on users, with session interruptions, visual artifacts, or delays in application performance, creating a real tax on user productivity. For most organizations, shifting SaaS and web workloads out of VDI and into an enterprise browser will deliver significant cost savings and a dramatically better user experience. |
| **Can an enterprise browser work within my security service edge (SSE) environment?** | An enterprise browser can happily coexist within an SSE environment, and this is not uncommon today. Or, an enterprise browser can be used as an alternative to SSE. Moving the enforcement layer from the network to the browser offers several advantages. An enterprise browser offers complete flexibility in deployment. They can be used on managed or unmanaged devices and don't require routing and inspecting network traffic. |

| | |
|---|---|
| | This flexibility applies to applications as well: an enterprise browser does its management and inspection in the browser, so there's no requirement for application-specific API integration |
| **Do I need a VPN to use an enterprise browser?** | An enterprise browser will use whatever network connection is available on the endpoint. It can use a VPN, ZTNA, or proxy connection from another vendor without conflict. Some enterprise browser vendors offer integrated ZTNA that's built-in to the browser to streamline access to internal or private applications. Be sure to ask your enterprise browser vendor if they offer this capability. |
| **Can I use an enterprise browser on an unmanaged or personal (BYOD) device?** | Yes. All the management capabilities of an enterprise browser are delivered directly through the browser so it can be deployed on any device, whether it's managed or unmanaged. This also offers flexibility in deployment where the enterprise browser is managed by one organization and the device is managed by another–for example, clients working with a BPO. |
| **Can I use an enterprise browser on a mobile device?** | Yes. Several enterprise browser vendors offer both desktop and mobile versions. Be sure to ask your enterprise browser vendor if they offer this capability. |
| **Does an enterprise browser record all user web activity? What about user privacy?** | Activity logging and auditing is an important capability for an enterprise browser, but it is configured in a way to balance the needs of the organization and the user's privacy. An enterprise browser supports flexible logging controls that record activity within critical application workflows while anonymizing (or ignoring) strictly personal web destinations. Some enterprise browsers also offer a user-facing indicator that will show the user whether their activity is being monitored. Be sure to ask your enterprise browser vendor if they offer this capability. |

# Questions to Ask Any Enterprise Browser Vendor

Not all enterprise browsers offer the same functionality. The list of questions below will help identify which features to consider when choosing the right vendor for you.

| Question: | What to consider: |
|---|---|
| How many customers do you have of a similar size and industry to my organization? | There are many small vendors offering some version of an enterprise browser. Building a browser is relatively easy, but building an enterprise browser with all the supporting services, customer support resources, and global scalability is not. Many enterprise browser vendors have not moved beyond the startup company phase and lack the resources and experience with supporting large, global enterprise customers across a diverse range of industries. |
| Does the enterprise browser offer integrated zero trust network access? | Some vendors make marketing claims for zero trust access, but don't offer the full technology layers required to connect users to private applications or networks. These vendors may require you to purchase additional products or integrate with other vendors to deliver ZTNA through their enterprise browser. |
| Is the enterprise browser available on mobile devices? | Building an enterprise browser as a mobile application for iOS and Android requires a separate development effort from desktop versions. Some vendors shortcut this step and leave mobile devices unsupported, or offer a significantly reduced feature set for mobile. |
| Can I customize the user experience to align with my company branding and messaging? | The user experience is essential for a successful enterprise browser deployment. Many vendors in this space are oriented exclusively around security requirements and leave the all-important user experience as a secondary priority or ignore it altogether. |
| Do you offer both a standalone enterprise browser and browser extension to manage and secure the consumer browsers in my environment? | Several vendors offer only one of these deployment models. In most organizations, there will always be a mix of browsers in use so it's essential to find a vendor who can support both an enterprise browser as a standalone application and a browser extension, with integrated backend management controls. |