Island

The Enterprise Browser Buyer's Guide

Introduction

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 wasn't built for the enterprise.

It was meant for shopping, streaming, and socializing. It was designed to serve advertisers and their consumers, not organizations and their employees.

That's why working on a consumer browser today means surrounding it with an army of security and IT solutions in order to satisfy even the most basic enterprise needs and security requirements. The result is a stack of agents, proxies, and gateways that's too complex, too fragile, and too costly to manage — and an end user experience that's full of delays, disruptions, and frustrations.

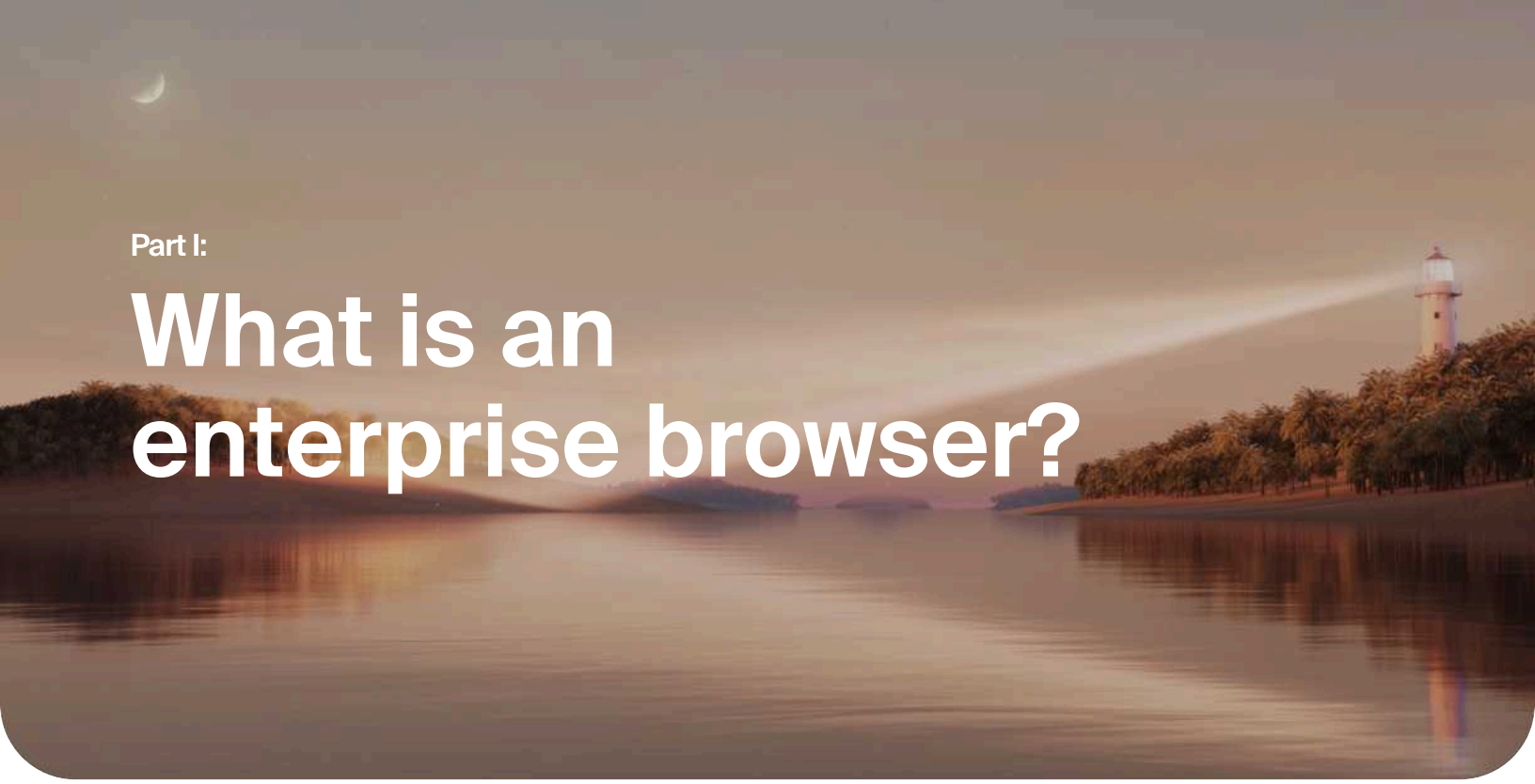
Now ask yourself: What if the browser was designed for the enterprise?

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 know and love.

An enterprise browser helps:

- CISOs deliver a truly secure-by-design work environment for their organization while combining capabilities traditionally delivered by multiple solutions into a single streamlined platform.
- CIOs provide their tech teams with a dramatically simpler, more efficient, and cost-effective platform for application delivery and enablement.
- End users with a faster, smoother work experience, productivity-boosting features, and enhanced privacy.

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



Part I:

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 and recreational use. An enterprise browser, though, is designed specifically for the workplace and optimized to serve organizations. It places the browser at the center of business work with security, IT, and productivity capabilities all baked into the experience.

The experience is both familiar and streamlined for end users. For administrators, it's a single unified experience that spans every type of device and user profile in the enterprise. The enterprise browser is able to go both broad and deep, keeping it simple and intuitive for business teams while allowing IT and security teams to precisely configure it to meet their specific requirements and use cases.

At its core, an enterprise browser is built on the Chromium browser engine, the same technology that powers Google Chrome, Microsoft Edge, ChatGPT Atlas, and other popular consumer browsers. By using Chromium, an enterprise browser can deliver the browser experience everyone expects 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 is felt by stakeholders across the whole organization, from security admins to end users. Here are the different benefits that CIOs, CISOs, and end users enjoy with an enterprise browser.

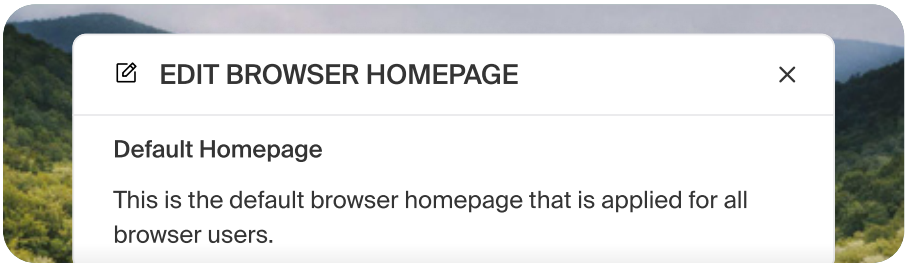
- **Efficiency and cost savings:** Many of the security tools, endpoint agents, and IT solutions currently needed to secure and enable the enterprise either come embedded in the enterprise browser or are just simply no longer needed. This dramatically simplifies your IT infrastructure and security stack, minimizing and streamlining the cost and effort involved in licensing, deploying, maintaining, and supporting all the infrastructure.

- **Application provisioning:** With an enterprise browser, users have access to everything they need at their fingertips, including SaaS, web applications, non-web desktop apps, generative artificial intelligence, and private apps. Instead of juggling a collection of extensions and external productivity tools, the IT team simply deploys and configures everything inside the browser itself – so it's simple to onboard users to new apps and services. Island also has fully integrated SSH, RDP, and SMB clients.

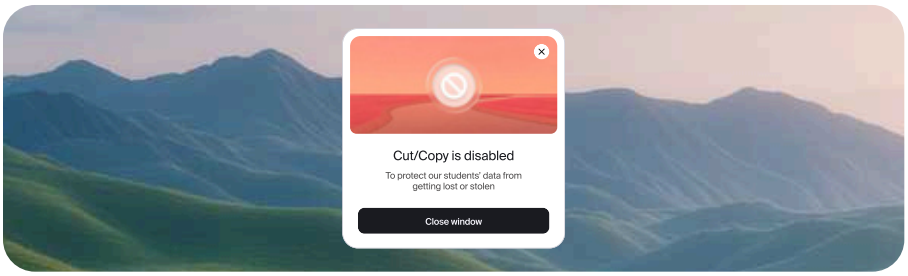
- **Deep insight:** An enterprise browser provides analytics on application usage, performance, and workflow insights. Island automatically identifies connectivity disruptions, service outages, network slowdowns, and more. Because Island controls the presentation layer, it's also able to easily monitor the real end-user experience, including application and device performance, without application-side integrations or additional agents.

- **Remote access:** Many organizations use an enterprise browser to reduce the need for traditional VPN or virtual desktop infrastructure (VDI). It's ideal for hybrid and remote workforces because employees can access their applications from anywhere, and the enterprise browser is easily deployed to personal devices to enable BYOD initiatives as well.

- **The modern workspace:** It's not just *an* enterprise browser, it is *your* enterprise browser. Island can be fully branded with your organization name, logo, color scheme, and brand identity. It is the ideal way to deliver company communications, such as blog posts, employee surveys, and urgent notifications.



- **Data protections:** With no control over browser activity itself, securing SaaS and internal web apps in a consumer browser forces a “blunt instrument” approach to protecting data, 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 data protection controls protect sensitive data from being improperly downloaded or uploaded before it leaves or enters the browser. Robust policies govern copy/paste, screenshots, printing, sharing, saving, or uploading, 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 without any unnatural network traffic manipulation (while most legacy security tools can offer visibility only by breaking and inspecting SSL traffic).

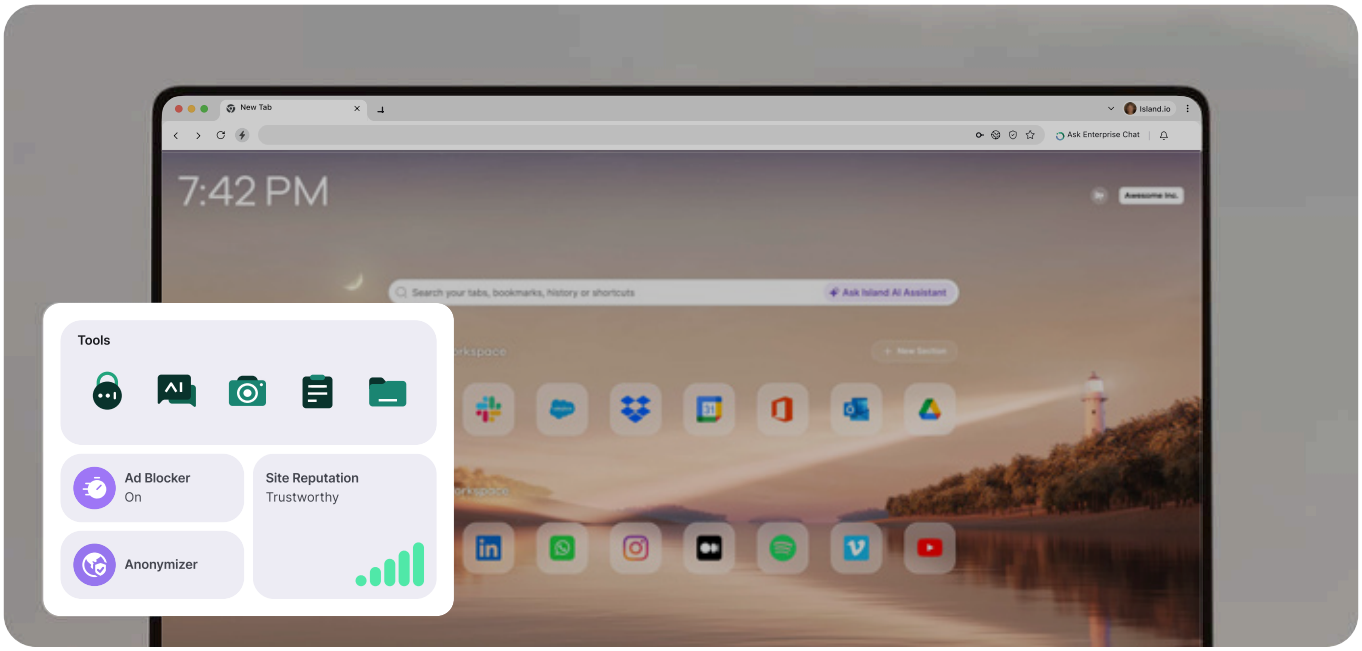
  Security teams can see the applications in use, monitor specific clicks, keystrokes, or workflows within an application, and connect actions to the user's identity. And, unlike legacy approaches, organizations can choose what to monitor and how, enabling them to keep personal browsing private.

- **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 and resolve incidents in minutes.

- **Password protections:** A password manager is built into — not bolted onto — the enterprise browser and inherently protects against phishing attacks, password exfiltration, or password interception for every session for every user on every device.
    - Because credentials are shared only on the network layer and never exposed in the DOM, this safeguard is particularly effective for distributed or hybrid workforces.
    - An enterprise browser can implement privileged access management (PAM) workflows where users can authenticate with credentials assigned to them, without ever seeing the password. This is especially useful, for example, in situations where several employees need access to a shared company account, such as social media platforms.



The end user

- **Access:** In the enterprise browser, a user simply logs in to the browser with single sign-on and automatically accesses all the applications and links they need based on their identity, role, or job function. Newly-deployed applications show up automatically, and native SSH and RDP deliver access to user workflows outside of web and SaaS.

- **Productivity:** Because an enterprise browser is designed for the workplace, it comes with built-in ad blocking to remove distractions and speed up browsing, and integrated tools to speed up common workflows. It also integrates with enterprise cloud storage to streamline downloads and uploads.

- **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, or ticketing systems can be pre-filled with common responses based on the context of the user and their activity — regardless of the underlying application's own automation features.

- **Education and awareness:** An enterprise browser automatically gives helpful, context-based feedback, like notifying users why an action was prevented due to an IT or security policy. When they access sensitive data, a popup notification can remind them of your organization's data security policies. If work requires going outside the policy framework, an exception request goes directly to the service desk to be granted within minutes — without ever leaving the enterprise browser environment.

- **Privacy:** Work and personal browsing are kept separate through context-based browser activity policies. A simple indicator shows users whether their browser activity is being monitored on every page they navigate to.

- **Performance:** An enterprise browser is optimized for speed and responsiveness by, for example, blocking ads and trackers to minimize unnecessary network requests. 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.

The enterprise browser deployment experience

Deploying or updating enterprise software is typically a slow, complex, and intricate process filled with training sessions and on-premises support that can consume several days or even weeks.

By contrast, an enterprise browser downloads and installs in a handful of minutes (and is fully functioning within hours) through a shockingly simple four-step deployment process:

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

An enterprise browser supports all common providers, including Okta, Microsoft Entra ID, and Google Workspace, and offers 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

Upon launching, users login via your IdP. Then import their settings or bookmarks from their previous browser.

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, such as contractor access, safe browsing, zero trust network access, and more.

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

The user experience

Because the enterprise browser is powered by the same Chromium browser engine that drives consumer browsers like Google Chrome and Microsoft Edge, users instantly understand that this is the same experience — only better. They have easy access to all apps and resources needed for their work, browsing is faster and smoother, and there are no VPNs or VDI sessions needed to access internal apps.

Enterprise browser deployment

Installation is done in moments via device management tools or by self-guided download and installation steps, just like installing a consumer browser.

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.

Native browser experience

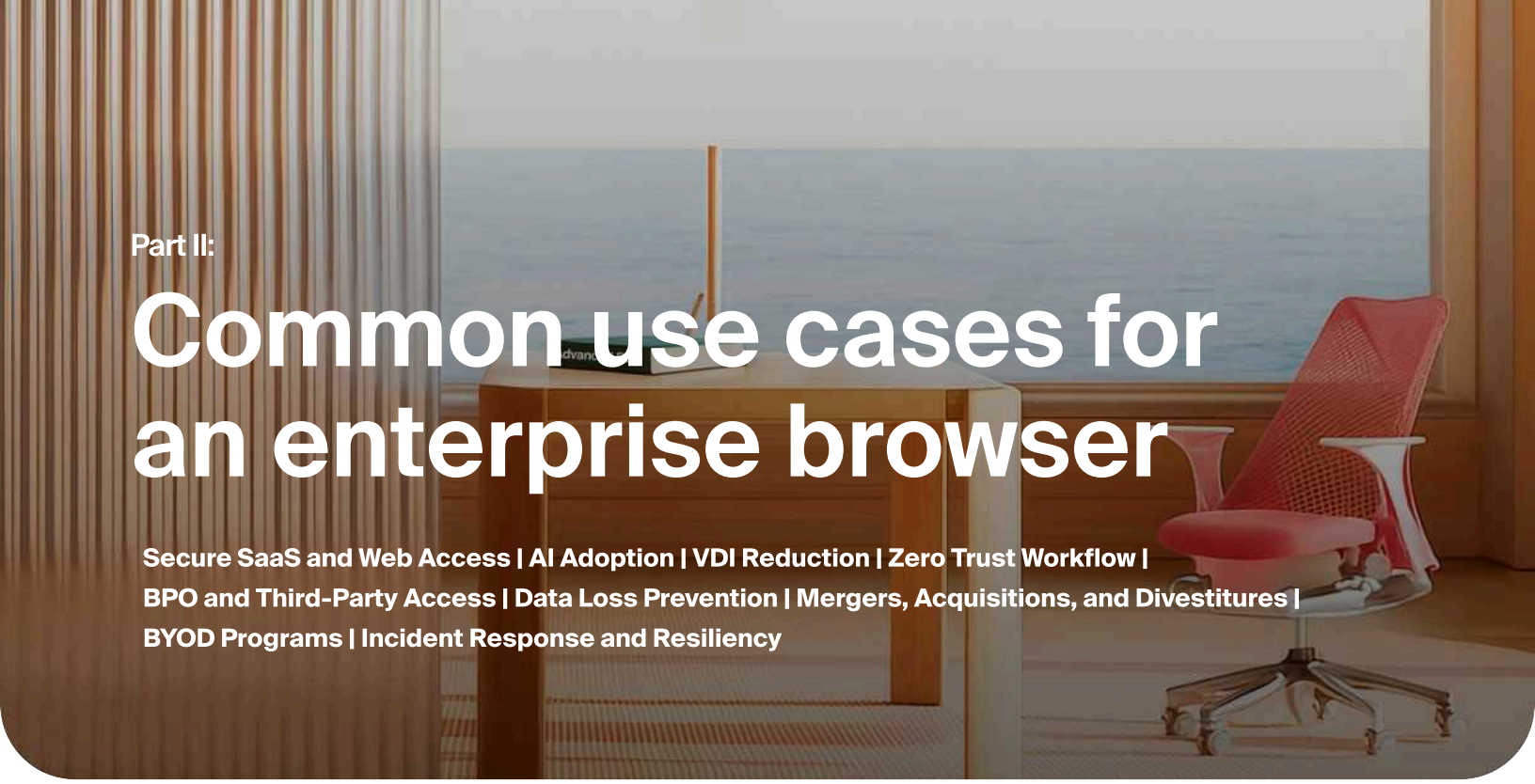
An enterprise browser delivers the natural, smooth browser experience that users are familiar with. The navigation and shortcuts are nearly identical, all extensions are 100% compatible, and everything renders exactly as it would on a consumer browser.

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 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 and why, and what to do next.



Part II:

Common use cases for an enterprise browser

Secure SaaS and Web Access | AI Adoption | VDI Reduction | Zero Trust Workflow | BPO and Third-Party Access | Data Loss Prevention | Mergers, Acquisitions, and Divestitures | BYOD Programs | Incident Response and Resiliency

Because most work takes place in the browser, enterprise browsers can address a large number of use cases. Oftentimes, organizations start with one urgent use case and adopt additional use cases over time. Here are the most common enterprise browser use cases:

Solve the SaaS data leakage problem

The shift to SaaS and web applications for a wide range of businesses means critical data and workflows often move through consumer browsers that offer 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.

The enterprise browser gives your organization:

- 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.

Say "yes" to AI

Generative AI tools like ChatGPT, Claude, and specialized AI platforms offer transformative potential for employee productivity and efficiency. However, the risk of inadvertently sharing sensitive data with unapproved AI platforms has caused many enterprises to block AI tools entirely.

Instead of preventing employees from pursuing AI's potential productivity gains, an enterprise browser solves this dilemma by enabling organizations to embrace AI innovation while maintaining organization-defined protections, policies, and compliance. Companies can choose which AI platforms are approved for use with company data (while blocking others), automatically prevent sensitive data from being shared with unapproved AI tools, and maintain comprehensive audit trails of all AI interactions.

The enterprise browser gives your organization:

- Centralized visibility and governance of AI tool usage across the organization.

  Example: an enterprise browser provides security teams with a dashboard showing all AI platforms being accessed by workers, distinguishing between approved tools (like organization-sanctioned AI platforms) and unapproved tools (like personal ChatGPT accounts), with the ability to set policies for each.

- Data protection policies that prevent sensitive data from being shared with unapproved AI platforms.

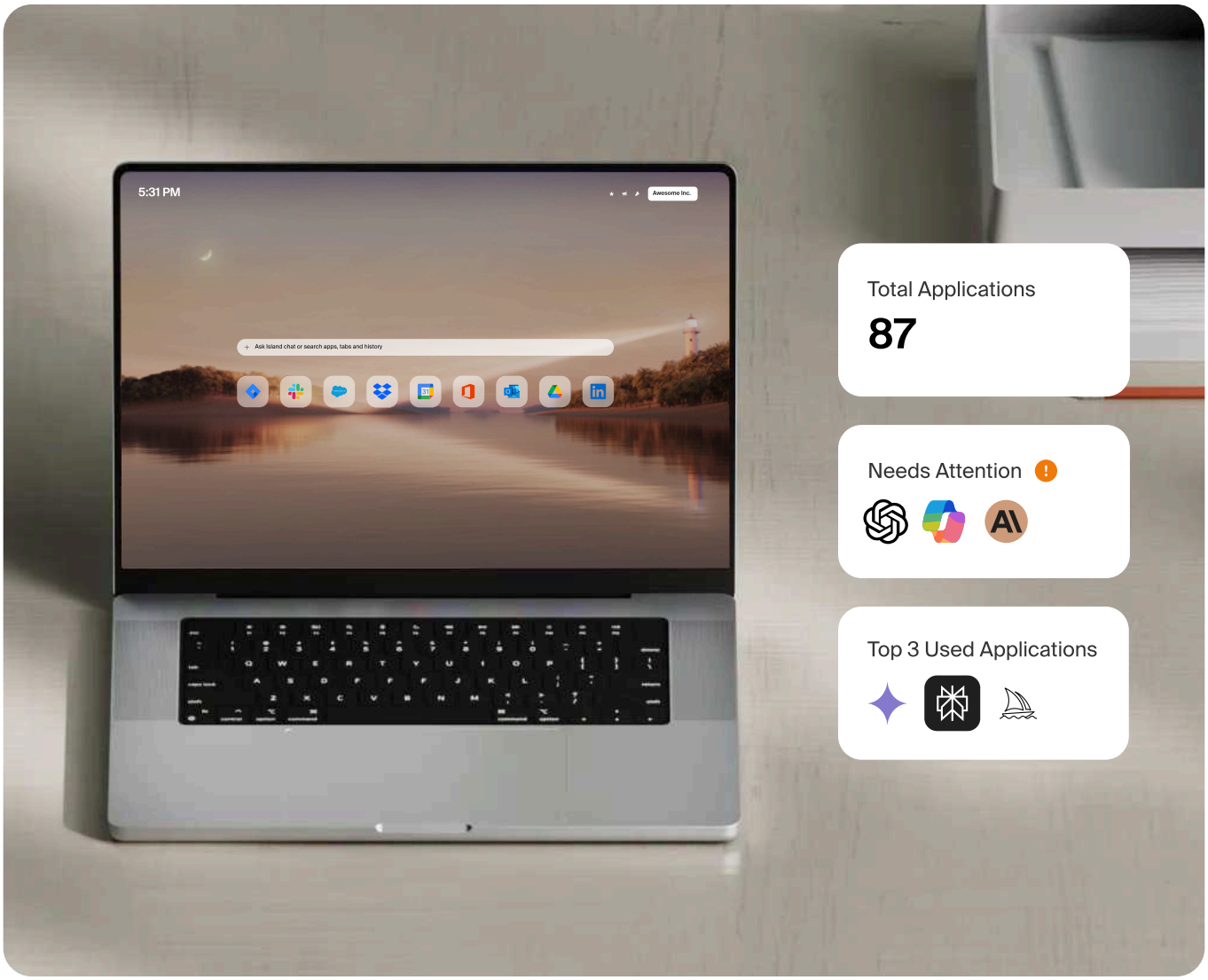
  Example: when an employee attempts to paste sensitive customer information into a consumer AI chat interface, an enterprise browser gives you the option to block the action, warn the user about the policy violation, or automatically redact the sensitive data while allowing the question to proceed.

- Graceful redirection from unsanctioned to approved AI tools.

  Example: When an employee navigates to a public AI platform, an enterprise browser can display a message explaining the organization's AI policy and automatically redirect them to the company's approved AI assistant that has proper data handling agreements and compliance measures in place.

- Complete audit trails for compliance and training.

  Example: An enterprise browser logs all interactions with AI platforms, including what prompts were submitted and what data was accessed, creating a comprehensive audit trail for compliance reviews and surfacing training opportunities for guidance on appropriate AI usage.



Radically reduce VDI

Many organizations use virtual desktop infrastructure (VDI) solutions to provide browser access to critical applications for off-premises users, carrying 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 VDI's drawbacks.

The enterprise browser gives your organization:

- 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, copy/pasted, etc. 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 apps or internal 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.

- Background services that can be used to govern non-web desktop applications.

  Example: some enterprise browsers install a background service that extends data protection and file controls to desktop applications such as Microsoft Office.

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 embed zero trust capabilities into the browser itself — where the majority of application and data access happens — creating an end-to-end zero trust work experience.

The enterprise browser gives your organization:

- Verified user identity through an enterprise identity provider (IdP) with multi-factor authentication support.

  Example: an enterprise browser offers native integration with your IdP and offers 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), they often end up provisioning managed laptops or virtual desktops.

The hardware route adds cost and serious delays, particularly when contracted workers are in foreign countries. Virtual desktop infrastructure 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.

The enterprise browser gives your organization:

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

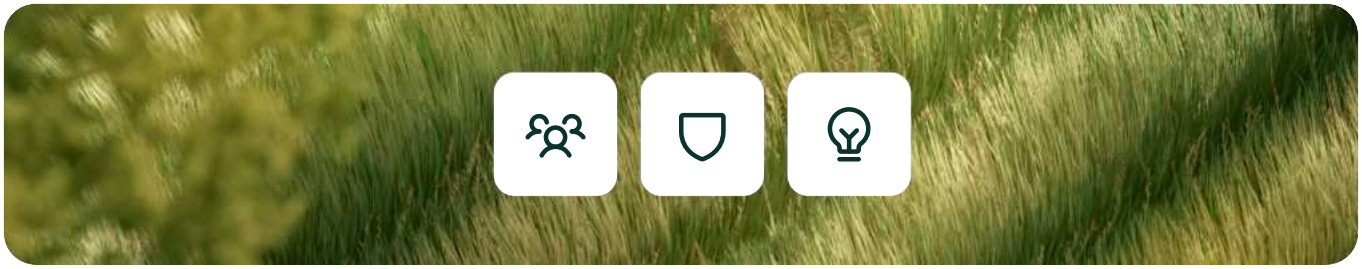
  Example: a contractor can install an enterprise browser on their laptop that's managed by their contracting firm without requiring an IT support ticket.

- 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.

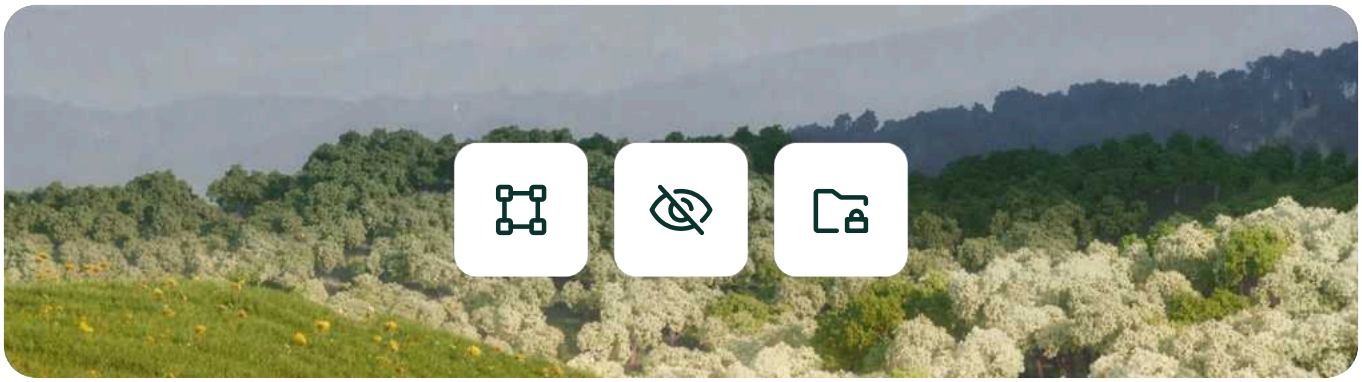


Build data loss prevention into the workplace

The traditional workplace could rely on well-defined boundaries across endpoints, network, and applications. Today's work, though, happens outside the office, often on 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 center of the workspace (a.k.a. the browser) itself, delivering a more effective, more efficient way to protect data in today's modern workplace.



The enterprise browser gives your organization:

- Application and data boundaries that 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 to hide 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 flagging 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

Merging together the IT systems of two organizations is a major undertaking that can take months or even years, while causing major friction and work stoppages. During a merger or acquisition, though, this is precisely 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.

The enterprise browser gives your organization:

- 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.

- 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.

- Access across disparate networks without VPN or infrastructure changes.

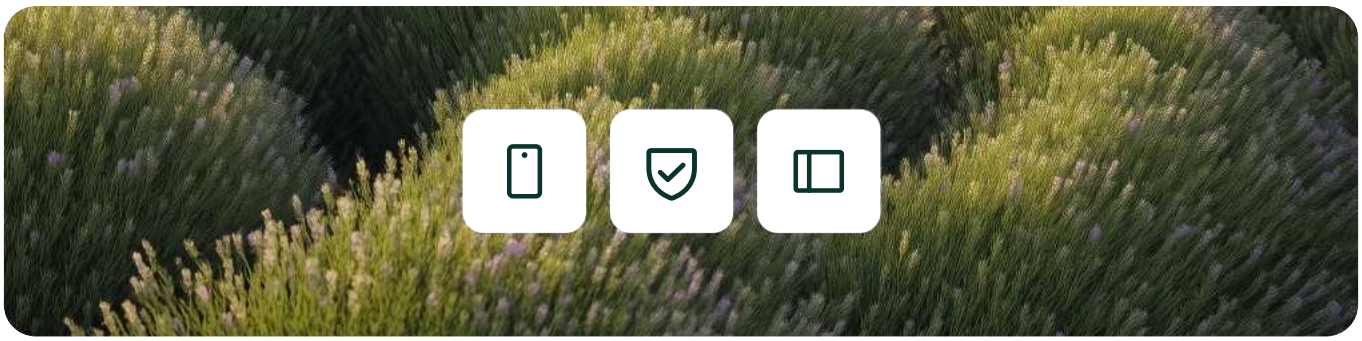
  Example: employees who need access to private or internal applications can connect through an enterprise browser with integrated ZTNA before any changes to the network infrastructure are completed.

Deliver a safe, viable BYOD initiative

A universal challenge that's gone unsolved for over a decade: finding a BYOD initiative that satisfies business requirements, meets IT and security needs, and is practical enough to be adopted by employees.

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.



The enterprise browser gives your organization:

- 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: the enterprise browser keeps track of work and personal contexts, allowing users to move data between work apps, but preventing them from moving corporate data and resources to a personal website, such as their personal email.

- 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 often forced to work on other devices, or simply stop working altogether until the threat is eliminated.

With an enterprise browser, though, security staff can instantly access critical communications tools and business applications while their regular IT systems are down (and everyone else carries on with business as usual, no matter how severe the incident is).

The enterprise browser gives your organization:

- 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.

Part III:

The industry experts' perspective

Gartner, Innovation Insight: Secure Enterprise Browsers

Published 1 April 2025

Gartner

> ***"By 2028, 25% of organizations will augment existing secure remote access and endpoint security tools by deploying at least one secure enterprise browser technology to address specific gaps."***

Gartner, Innovation Insight: Secure Enterprise Browsers, Evgeny Mirolyubov, Max Taggett, John Watts, 1 April 2025

Frost & Sullivan, Frost Radar: Zero Trust Browser Security, 2025

Published November 2025

FROST & SULLIVAN

> ***"The browser is rapidly becoming the central hub of enterprise activity, evolving into the new endpoint for both productivity and threat risk. Enterprise browsers and browser extensions are eclipsing legacy tools like VPNs, virtual desktop infrastructure (VDI), and proxy-based secure web gateways (SWGs), offering clientless and user-friendly secure application access."***

Frost & Sullivan, Frost Radar : Zero Trust Browser Security 2025, Swetha Krishnamoorthi, November 2025

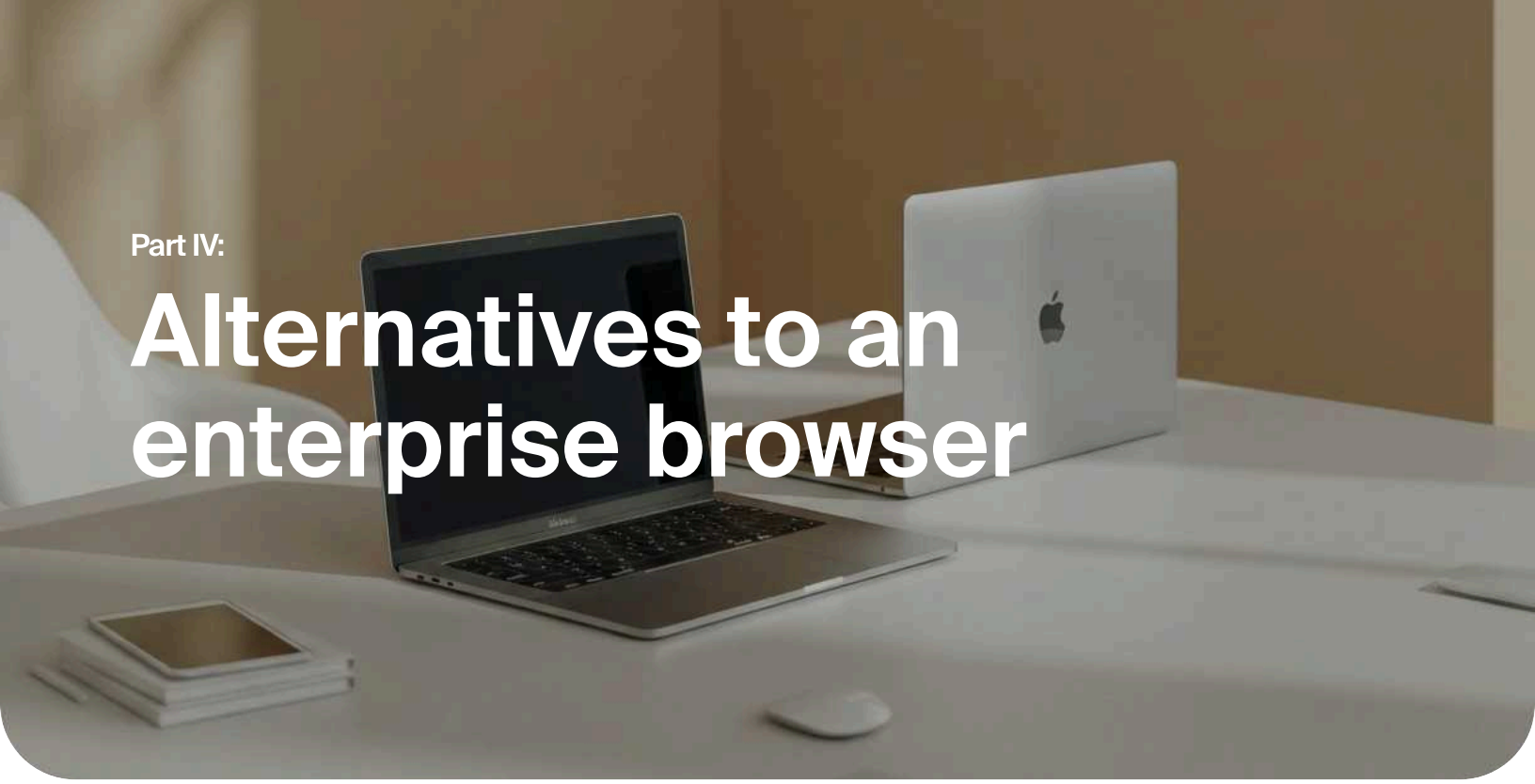
GigaOm, Radar for Secure Enterprise Browsing v2

Published 14 August 2025

GIGAOM

> ***"Secure enterprise browsing solutions can improve security posture while also simplifying the technology stack. Integrating security functions into the most widely used application ensures that end users do not experience additional friction introduced by other security products. This is an appealing proposition, so we expect the adoption of enterprise browsers to increase considerably over the next few years."***

GigaOm, Radar for Secure Enterprise Browsing v2, Andrew Green, 14 August 2025



Part IV:

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.

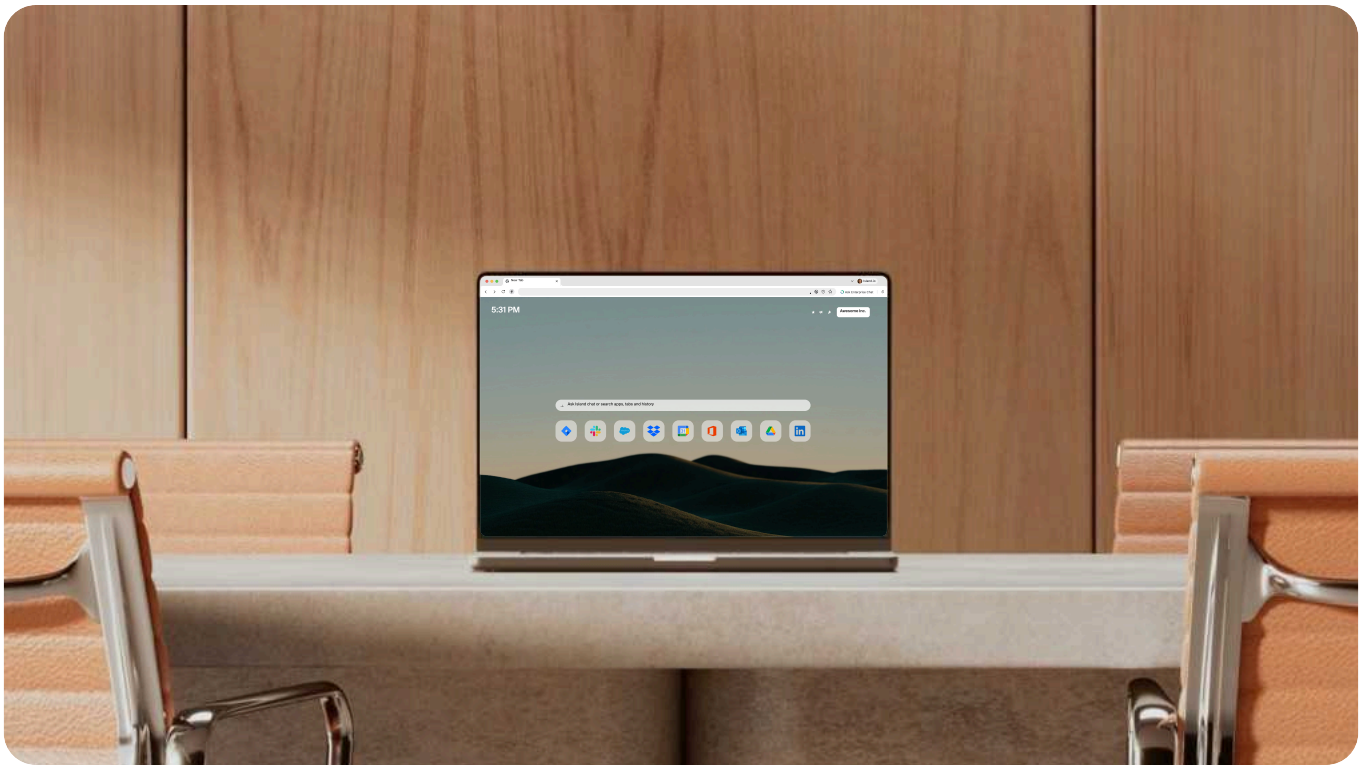
Weaknesses:

- Extension capabilities are limited by the extension framework as defined by the consumer browser. These frameworks change from time to time, so there's a risk that existing features and functionality could change or disappear unexpectedly.

- 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.
- Example browser extension vendors are not available for mobile devices, so an environment with a mix of desktop and mobile devices will require multiple solutions.

There are some scenarios where browser extensions are the right choice (see the section Deployment Model Considerations). That said, most organizations will eventually need some capability that is only achievable as part of the browser itself. A hybrid deployment can provide the best of both worlds, but requires a vendor that offers both a browser extension and full browser.

Example consumer browser extension security vendors: LayerX Security, 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 that 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.

While some RBI providers market their solutions as enterprise browsers, RBI is a tool with a smaller scope and limitations to the end user experience. In fact, many of the attack vectors addressed by RBI can also be mitigated with local isolation and intelligently disabling certain high-risk browser APIs, which is much less complex and provides a better end user experience.

RBI vendors include Authentic8, Cloudflare, Garrison, and Menlo Security

Virtual desktop infrastructure (VDI)

Virtual desktops are often used to fulfill similar objectives as an enterprise browser. Namely, to extend access to applications and resources with security controls and centralized management.

VDI long-predates the enterprise browser and was popularized in an era when most enterprise applications were standalone applications installed on the desktop. As SaaS trends shift more and more workflows to the browser, VDI can still play a role by using a browser within the virtualized environment. But this use case presents some significant drawbacks.

Strengths:

- Complete isolation between work and personal environments with full control over the virtual desktop.
- Centralized management and patching of virtual desktop images simplifies IT operations.
- Can support legacy desktop applications that require full installation to the desktop.
- Provides a consistent work environment regardless of the physical device being used.

Weaknesses:

- VDI requires substantial infrastructure investments in terms of servers, networking, virtualization software, and all the corresponding administrative costs to host and maintain these systems. Several vendors now offer desktop virtualization as a service (sometimes called Desktop-as-a-Service or DaaS). This shifts some of the burden off the customer in exchange for a higher price point.

- Managing and maintaining a virtualized desktop environment (whether on-premise or hosted) requires substantial IT staffing. The virtual desktops must be configured, patched, and managed, similar to managing physical endpoints. Help desk staff are burdened with onboarding new users and assisting with troubleshooting issues with virtual sessions or connectivity.

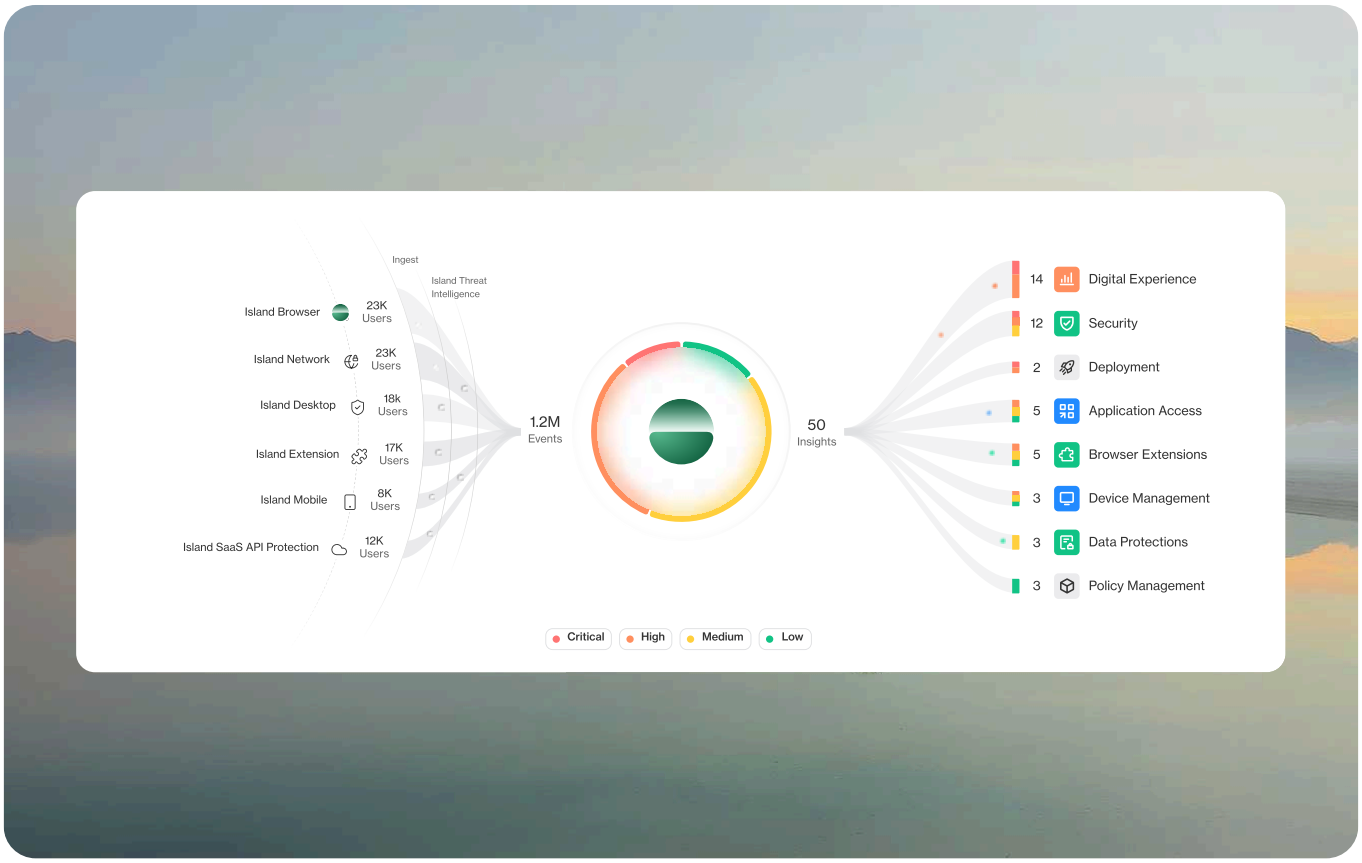
- In an ideal environment with fast networks, low latency, and untaxed virtualization servers, the user experience is acceptable. In practice, it's more common that one (or all) of these factors are less than ideal. Session interruptions, visual artifacts, or delays in application performance create 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. Some enterprise browsers like Island include a background service that can extend controls to desktop apps, allowing these organizations to shift even non-web applications out of VDI.

VDI vendors include Citrix, Omnissa, Microsoft, and Amazon

Security service edge (SSE)

Security service edge (SSE) is a collection of technologies that aim to provide security and access controls over the network and all upstream applications. This was popularized when IT and cybersecurity teams started managing highly distributed environments with applications moving to the cloud and users moving off the corporate network. SSE operates primarily at the network layer, so it can provide access controls, security, and data protections for web and desktop apps. An enterprise browser can happily coexist within an SSE environment, and this is not uncommon today. Or, an enterprise browser can be used to achieve the same objectives and serve as an alternative to SSE.



Strengths:

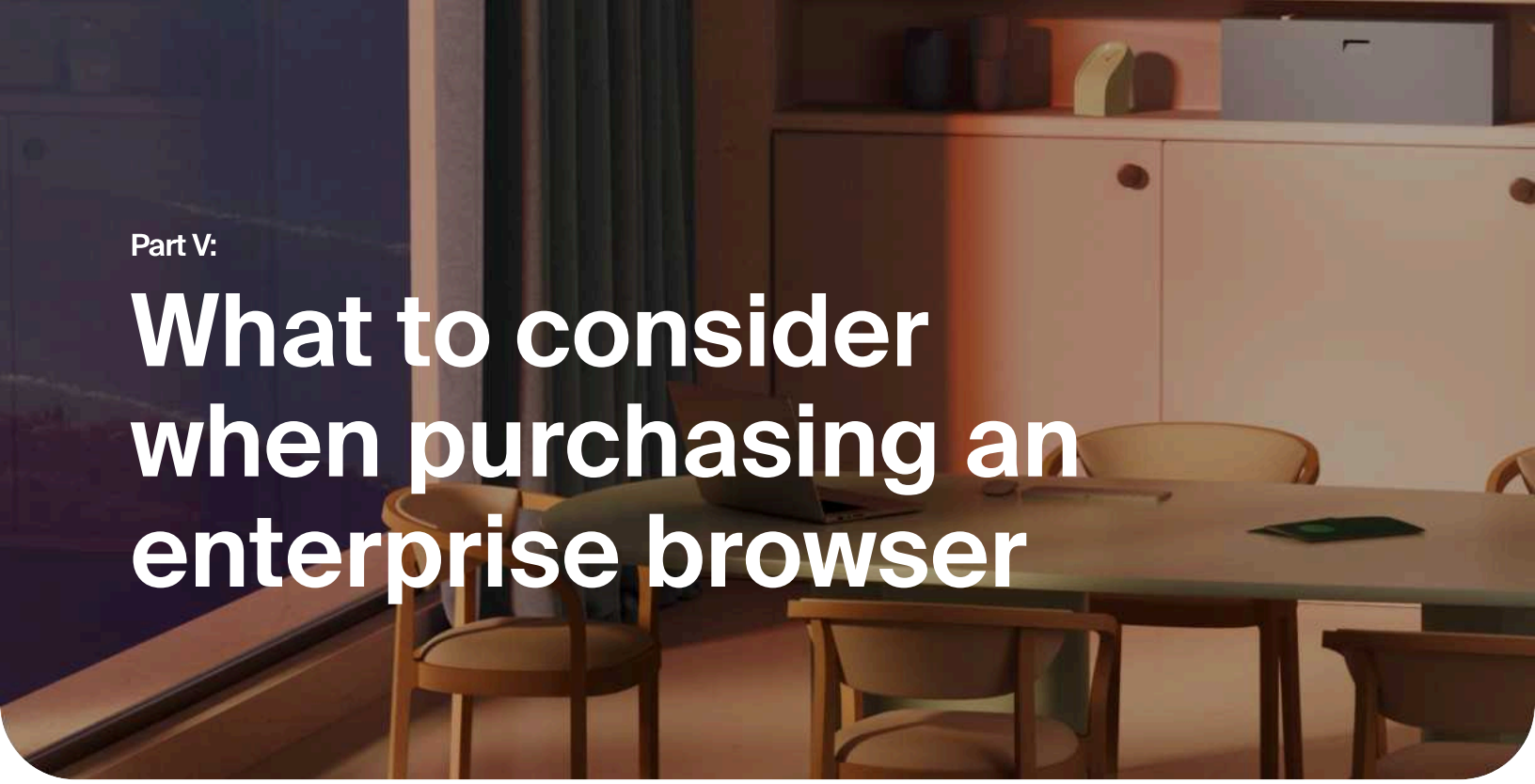
- Works regardless of which browser or desktop client is used, providing consistent security policies across all web access.
- Provides network-level visibility and control over all traffic flowing through the organization.
- Based heavily on the popularity of zero trust network access (ZTNA) as a VPN replacement, and many organizations adopt the other internet protections — secure web gateways, data loss prevention, cloud access security brokers, etc. — as a secondary use case.

Weaknesses:

- SSE requires redirecting network traffic and breaking open SSL encrypted traffic to inspect the contents before re-encrypting and sending it along to its destination. Not only does this include additional hops, which increases latency, but often prevents the use of new network protocols, such as QUIC, and drastically increases the administrative burden.
- While some SSE vendors offer limited support for unmanaged devices, in practice they leave gaps in coverage particularly for devices outside the organization's direct control, such as contractor or BPO devices.
- Services that use certificate pinning, which includes many services commonly used by enterprises, cannot be inspected. Some services can be configured to ignore certificate pinning, but this adds another layer of configuration complexity.
- Requires routing all traffic through the SSE service, which can create single points of failure and dependency on the vendor's infrastructure.
- Because of their reliance on network-layer enforcement, SSE solutions do not support last mile controls, such as governing how and where a user can copy and paste data.

By moving the enforcement layer from the network to the browser itself, an enterprise browser offers an alternative approach that eliminates the need for SSL decryption, provides universal deployment flexibility across any device type or deployment model (including managed devices, unmanaged BYOD, and third-party devices), and offers consistent controls on any device, on any network.

SSE vendors include Palo Alto Networks, Zscaler, Netskope



Part V:

What to consider when purchasing an enterprise browser

Enterprise browsers address a large number of scenarios, can be deployed in many different circumstances, and serve many different types of users. Making the right choice requires careful consideration of your organization's current needs and future plans. Here are the key factors to evaluate when purchasing an enterprise browser.

Use-case planning

As outlined earlier in this guide, enterprise browsers can address many different use cases. Most organizations begin their enterprise browser journey with a single, well-defined use case. For example, many start with third-party contractor access or BYOD programs.

However, the most successful enterprise browser deployments rarely stop there. Organizations typically expand to additional use cases over time, often culminating in deploying the enterprise browser across the entire company as their primary enterprise workspace.

When evaluating enterprise browser vendors, consider your future trajectory alongside your immediate needs. Some enterprise browser companies focus exclusively on security use cases with limited productivity capabilities or workflow automation.

Look for an enterprise browser that can grow with your organization, including the productivity tools, automation capabilities, and user experience enhancements that make it viable as a long-term workspace solution.

Deployment model considerations

The deployment model you choose will significantly impact the value you derive from an enterprise browser. A comprehensive enterprise browser strategy should account for various deployment scenarios, platforms, and use cases.

Platform coverage

To serve as an effective workspace, enterprise browsers must be available across all major platforms your organization uses. This includes:

- **Desktop platforms:** Windows, macOS, and Linux.
- **Mobile devices:** iOS, iPadOS, Android, and ChromeOS, and it should be available in both the Apple App Store and the Google Play Store.
- **Specialized environments:** If your organization uses secure endpoint operating systems, such as IGEL or other locked-down environments, verify that the enterprise browser supports these deployments.

Browser extension capabilities

While enterprise browsers in the purest sense are standalone Chromium-based browsers, some vendors offer browser extensions that work within consumer browsers like Chrome or Edge. Though extensions have inherent limitations compared to full browsers (see the Alternatives to an enterprise browser section), there are scenarios where they provide value.

- **Phased rollout strategy:** Organizations adopting full enterprise browsers may use browser extensions as part of a gradual transition. This allows users to experience browser-based controls while continuing to use their familiar consumer browser. Over time, users become comfortable with the governance model and can transition smoothly to the full enterprise browser.
- **Hybrid approach:** Some organizations allow employees to use consumer browsers for general work but require the full enterprise browser when advanced capabilities or stricter controls are needed. For example, a browser extension might provide in-browser data loss prevention for everyday work, but when a user needs to share a password with another user without allowing the recipient to view the password, they must switch to the full browser. In this scenario, the browser extension can provide a seamless redirect, launching the full browser with a single click.

- **Emerging browser adoption:** Companies may also want to allow users to adopt new browser technology, such as AI-enabled browsers like ChatGPT Atlas. In these cases, a browser extension can be used to allow users to adopt these browsers while limiting the data or company resources that are exposed to them.

Endpoint capabilities

Enterprise browsers were built because the majority of work happens inside the browser due to the prevalence of web and SaaS applications. However, most organizations still rely on some desktop applications, such as Microsoft Office, Adobe Creative Suite, development tools, and legacy applications.

If you deploy an enterprise browser with controls that only function inside the browser, you'll need a separate solution, such as an endpoint protection platform, to secure desktop applications. This creates the burden of managing multiple licenses, separate management consoles, and disparate policy frameworks, increasing both cost and complexity.

Some enterprise browsers include a background service that installs alongside the browser and interfaces with the operating system. This service can extend policies and controls beyond the browser itself, enabling organizations to enforce data protection policies, application access controls, and file management rules across both web and desktop applications from a single platform.

This unified approach simplifies administration, reduces costs, and ensures consistent policy enforcement regardless of whether users are working in a SaaS application or a desktop program.

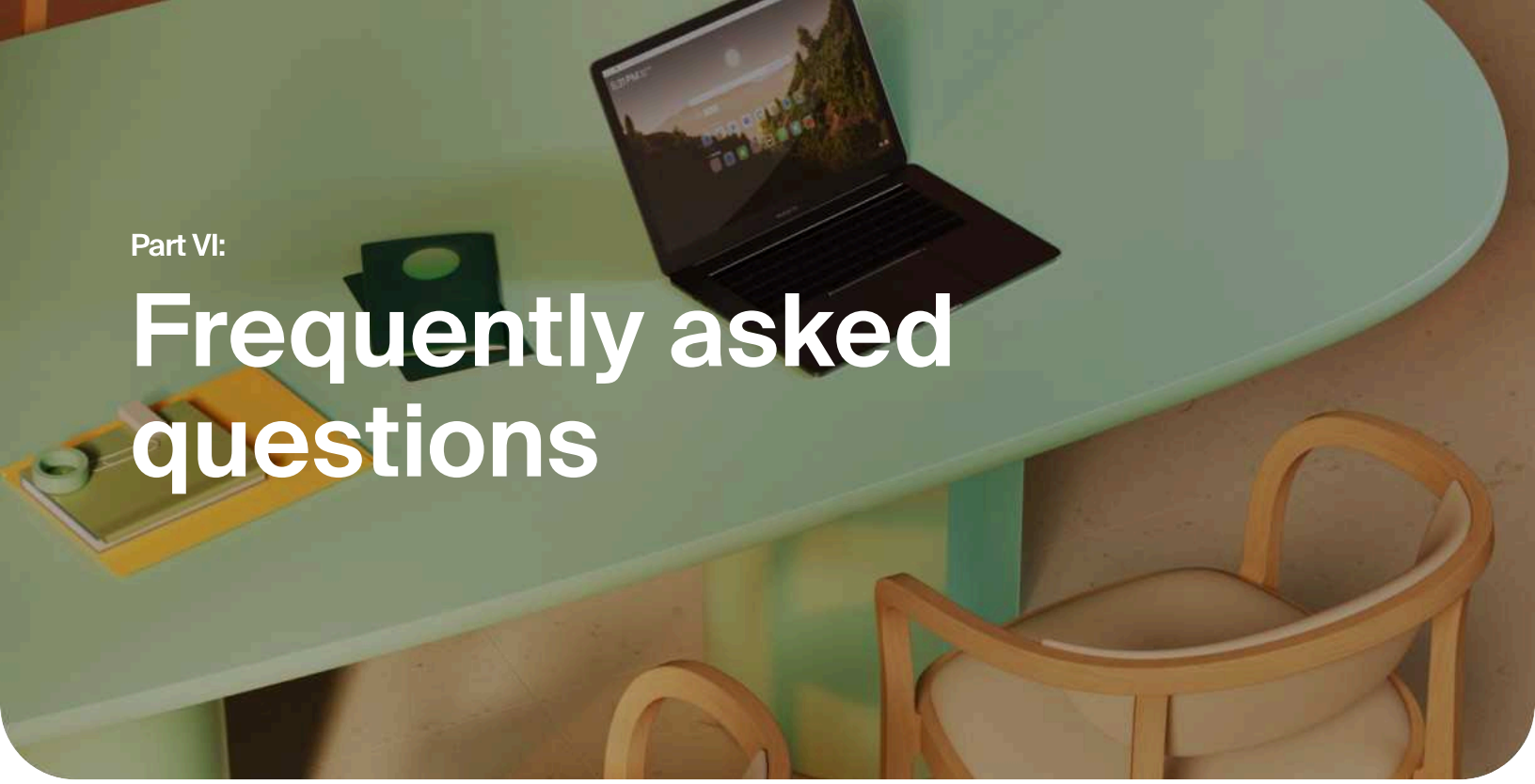
Choosing the right deployment model

Just as with use case planning, it's essential to consider your organization's future needs when deciding on a deployment model. Your initial use case may be well-served by a browser extension, but if you plan to roll out the enterprise browser as your primary workspace in the future, you'll want the additional capabilities of a full browser deployment.

Similarly, if your organization relies on desktop applications like Microsoft Office, Slack desktop clients, or specialized industry software, you should prioritize vendors that offer endpoint controls beyond the browser.

The strongest enterprise browser vendors support all these deployment models — not just technically, but in their licensing approach as well. Pricing should be based on users, not deployment method. Whether users access the browser extension, full browser, or both across multiple devices, they should be covered under a single, simple license.

This flexibility ensures you can start with the deployment model that fits your immediate needs and evolve smoothly without changing vendors.



Part VI:

Frequently asked questions

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.

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 to achieve the same objectives and serve 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 to use a proxy or 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, for clients working with a BPO.

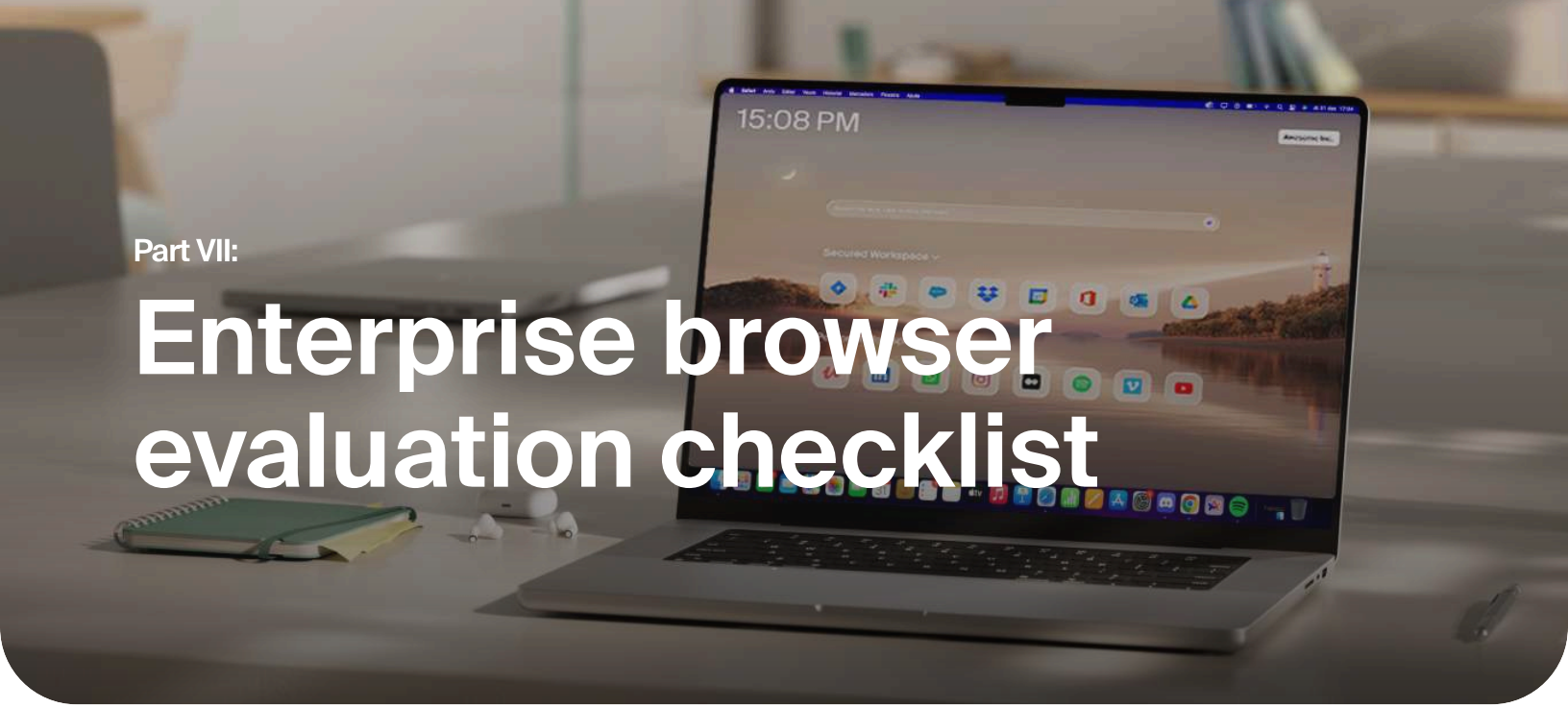
Can I use an enterprise browser on a mobile device?

Yes — but only on some. 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.



Part VII:

Enterprise browser evaluation checklist

When getting ready to evaluate an enterprise browser, here are the important capabilities and integrations to be looking for:

1 General questions

- Is the enterprise browser available on mobile?
- Can you customize the user experience to align with my company branding and messaging?
- Does the vendor offer both a standalone enterprise browser and a browser extension?
- Is the enterprise browser a standalone product, or does it require other solutions, such as an SSE platform, to achieve the same outcomes?

2 Browser capabilities

- Data loss prevention
- Application access controls
- Zero trust network access
- URL filtering and content categorization controls
- Password manager
- Privileged access management
- Browser extension management
- Audit logging and analytics
- Application automations
- Digital employee experience monitoring
- Cloud access security broker
- Managed homepage
- Company communications
- AI assistant
- AI protection

3 Browser integrations

- Identity provider
- SIEM
- Approval workflow (ex. ServiceNow)
- User cloud storage (ex. Microsoft OneDrive, Box, Google Drive)
- System storage (ex. AWS S3, Azure, Snowflake)
- ZTNA
- Sensitivity labels (ex. Azure Information Protection)
- VDI (ex. Citrix, Azure Virtual Desktop, Microsoft RDS, Amazon AppStream)
- Anti-malware (ex. Crowdstrike)
- Large language models
- Bring-your-own-key for password manager vault

Island

Island is the ideal environment for enterprise work. Its Enterprise Platform embeds core modern work requirements like enterprise AI, secure access, and data protection into the workspace itself. With it, organizations see, control, and protect work activity while delivering a smooth, simple, AI-powered experience across any user, anywhere. Leading enterprises use Island to embrace AI, enable BYOD, reduce VDI spend, and recover from disasters. Island is backed by Coatue Management, Insight Partners, and Sequoia Capital.

Learn more at island.io ↪

Thinking an enterprise browser could be right for your organization? Take your next step here.

Schedule a demo ↪