Definitive Guide™ to *Secure Browsers*

How to protect your organization with consistent security for any user, device, location, and app

Emily Matthews

FOREWORD BY:
Ofer Ben-Noon

Compliments of:

paloalto®
NETWORKS

About Palo Alto Networks

Palo Alto Networks is the world's cybersecurity leader. We innovate to outpace cyberthreats, so organizations can embrace technology with confidence. We provide next-gen cybersecurity to thousands of customers globally, across all sectors. Our best-in-class cybersecurity platforms and services are backed by industry-leading threat intelligence and strengthened by state-of-the-art automation. Whether deploying our products to enable the Zero Trust Enterprise, responding to a security incident, or partnering to deliver better security outcomes through a world-class partner ecosystem, we're committed to helping ensure each day is safer than the one before. It's what makes us the cybersecurity partner of choice.

At Palo Alto Networks, we're committed to bringing together the very best people in service of our mission, so we're also proud to be the cybersecurity workplace of choice, recognized among Newsweek's Most Loved Workplaces (2023, 2022, 2021), with a score of 100 on the Disability Equality Index (2023, 2022), and HRC Best Places for LGBTQ+ Equality (2022). For more information, visit www.paloaltonetworks.com.

Definitive Guide™ to *Secure Browsers*

How to protect your organization with consistent security for any user, device, location, and app

Emily Matthews

Foreword by Ofer Ben-Noon
SASE CTO, Palo Alto Networks

CYBEREDGE
PRESS℠

Definitive Guide™ to Secure Browsers

Published by:
CyberEdge Group, LLC
1997 Annapolis Exchange Parkway
Suite 300
Annapolis, MD 21401
(800) 327-8711
www.cyberedgegroup.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on CyberEdge Group research and marketing consulting services, or to create a custom *Definitive Guide* book for your organization, contact our sales department at 800-327-8711 or info@cyberedgegroup.com.

ISBN: 978-1-948939-40-9 (Paperback)
ISBN: 978-1-948939-39-3 (eBook)

Printed in the United States of America.

10 9 8 7 6 5 4 3 2

Publisher's Acknowledgements

CyberEdge Group thanks the following individuals for their respective contributions:

Editor: Susan Shuttleworth
Graphic Design: Colleen R. Abel
Palto Alto Networks Contributors: Nicole Morero and Peyton Padfield

Table of Contents

Foreword

The transition to hybrid work models and cloud-based operations puts browser-based work under the spotlight. This megatrend also widens the gap between network and endpoint security created by traditional security approaches. Browsers expose an expansive attack surface. They are positioned in the last mile, where workers interact with data, and users rely on them to do most of their work. This situation makes consumer web browsers a favored attack vector.

The *Definitive Guide™ to Secure Browsers* illustrates the importance of adapting to hybrid work and cloud computing. It will help you better understand the ripple effect of this new model on existing security strategies and the need to unlock the power of the browser to secure the modern workspace.

Secure browsers offer a strategic approach, leveraging the unique position of the browser to secure work where it happens. They provide built-in advanced security to proactively protect enterprise assets, which are exposed when users access SaaS and web applications and handle sensitive data in the browser.

The Definitive Guide explains why secure browsers offer unparalleled, frictionless security that bolsters organizations' defenses and meets the needs of workers in a web-first world. It also provides details about the security enhancements that come with SASE integration and other capabilities. For instance, you will see how SASE integration elevates data security in SaaS solutions, private web apps, and unmanaged and managed devices. This means that even if a device is compromised, the data will be protected. When secure browsers have native integration with a SASE platform, the protective reach of SASE extends beyond managed devices. You gain consistent visibility, control, and security across all users, apps, and devices.

The guide not only describes how an integrated SASE solution enhances security without impacting the user experience. It also reviews how integrations with other security solutions enable secure browsers to optimize and extend their capabilities.

The guide also offers an in-depth review of secure browsers' roles and functions and guidance for implementing them. Organization-wide support is critical. It can help you select the right solution, navigate the road to adoption, and optimize deployment.

Your IT and security teams face a changing and expanding enterprise footprint. At the same time, they must adapt to a threat landscape that continues to evolve and grow in scale and complexity. To meet these challenges, you need a modern cybersecurity plan for today's hybrid work and cloud operations environment, that includes secure browsers. The good news is that secure browsers are accessible, can be implemented at scale quickly and without disrupting operations, and extend advanced security to all users everywhere, using any device or web application.

Ofer Ben-Noon
SASE CTO, Palo Alto Networks

Introduction

The rapid rise of SaaS and web applications as a de facto business standard, the explosion of artificial intelligence (AI), and the paradigm shift in how we work have brought unprecedented efficiencies and operational enhancements. Like any major changes, these also expanded the attack surface and made it more complex.

While IT and security teams benefit from these technological advancements, they must also grapple with this broad array of new and existing vulnerabilities that pose significant challenges to maintaining a secure environment. Organizations need to embrace change while simultaneously adopting new strategies to mitigate negative effects in order to succeed and thrive.

Forward-looking enterprises were quick to see that this new environment exponentially expanded their attack surface and took swift action to protect it. The solution that previously offered the most effective protection for today's modern work environment was the enterprise browser. The solution that now offers the most effective protection is the secure browser, which builds upon the standard enterprise browser with advanced security capabilities. With work moving from secure networks to browser-based solutions that traverse public networks, secure browsers are uniquely positioned to enable secure access while protecting enterprises' data, systems, apps, and other critical resources.

This guide provides a detailed review of secure browsers. It will give you a foundational understanding of enterprise browsers and introduce secure browsers, as well as help you determine how best to select the solution that's right for you and successfully implement it.

Chapters at a Glance

Chapter 1, "Adapting to the Explosion of the Hybrid Workforce," reviews the rise of the hybrid workforce and how enterprise browsers can secure their remote workspaces.

Chapter 2, “Overcoming the Limitations of Current Security Approaches,” surveys the technology and deployment models being used and explains the security deficiencies that enterprise browsers can correct.

Chapter 3, “Introducing Secure Browsers,” provides a brief summary of enterprise browser solutions and introduces the secure browser. It also goes into detail about the secure browser with benefits and case studies that demonstrate its value.

Chapter 4, “Selecting the Right Secure Browser,” covers key features and capabilities to look for when evaluating secure browser solutions and includes an assessment checklist.

Chapter 5, “Integrating Secure Browsers into Your Tech Stack,” covers the core integrations that you should consider when reviewing secure browsers and why these integrations are important.

Chapter 6, “Getting Started,” offers tips and best practices for rolling out a secure browser solution to avoid user objections and ensure a smooth deployment.

Helpful Icons

TIP

Tips provide practical advice that you can apply in your own organization.

DON'T FORGET

When you see this icon, take note as the related content contains key information that you won’t want to forget.

CAUTION

Proceed with caution because if you don’t it may prove costly to you and your organization.

TECH TALK

Content associated with this icon is more technical in nature and is intended for IT practitioners.

ON THE WEB

Want to learn more? Follow the corresponding URL to discover additional content available on the web.

Chapter 1

Adapting to the Explosion of the Hybrid Workforce

In this chapter

- Learn how digital transformation has impacted the workplace
- Read about the risks posed by SaaS solutions, consumer-grade browsers, and unmanaged devices
- Understand why today's work environment requires a modern, browser-based security strategy that leverages the power of SASE

Digital transformation has fundamentally changed the way we work. The conventional centralized, hierarchical corporation with a monolithic workforce made up of full-time, office-bound employees is a thing of the past.

The precipitous rise in reliance on SaaS and increase in hybrid workers, who split work time between remote locations and traditional offices, has spotlighted the browser. It serves as the primary workspace and central productivity hub, enabling millions around the world to work seamlessly from multiple devices and apps. This paradigm shift necessitates a reevaluation of traditional security architectures because the browser is now a prime target for attackers. IT security systems and practices that were conceived to protect traditional brick-and-mortar operations did not emphasize browser protection and aren’t suited for the digital workplace.

The modern work environment requires a browser-focused approach to security – one built from the ground up for today's web-centric businesses and decentralized workforces. When integrated with a secure access service edge (SASE) solution, an enterprise browser can deliver enhanced network security services to managed and unmanaged devices in minutes, creating a secure workspace for all users, regardless of location, device, and app.

Rise of the Hybrid Workforce

The Internet has all but eliminated traditional barriers to remote communications, collaboration, and contracting. Today's digital businesses have a global pool of resources at their disposal. They can pick and choose the right employees, vendors, and partners for the right jobs at the right time.

The modern business is lean and nimble. It uses contractors and freelancers to reduce overhead, fill skills gaps, and increase business agility. It also uses outsourcers to contain expenses and focus internal resources on core competencies. And modern businesses leverage a global network of partners and suppliers to ensure goods and services are delivered on time and at the right price.

These organizations now include a virtual workplace where employees are no longer confined to corporate offices. Some work exclusively remotely, and others are hybrid. In the digital era, companies optimize business performance, improve employee satisfaction, and increase retention by giving staff the flexibility to work from any location and any device.

DON'T FORGET

According to the "Microsoft Digital Defense Report 2023," 80-90% of all successful ransomware compromises originate through unmanaged devices.

The primacy of SaaS solutions and web apps

Today, nearly all businesses are fueled by the Internet and powered by the cloud. Software-as-a-service (SaaS) solutions and web apps make it easy to support hybrid work models, leverage global suppliers and distribution partners, utilize contractors and outsourcers, and unleash productivity for on-the-go knowledge workers, field-service employees, and frontline staff.

DON'T FORGET

According to Productiv's "2023 State of SaaS Series," the average number of web/SaaS applications used by organizations has increased 32% since 2021. Many organizations have also moved internal line-of-business applications to the cloud to streamline operations and increase business agility. Most new companies rely solely on cloud-based business apps and SaaS solutions.

An outdated security model

Traditional perimeter-based security models, as well as virtual desktop infrastructure (VDI) and virtual private networks (VPNs), aren't suitable for modern IT environments. These approaches do not offer sufficient defenses, particularly data loss prevention, to secure work done in browsers.

Today, many organizations maintain confidential business data and personally identifiable information (PII) in SaaS solutions beyond the secure confines of the enterprise network. And employees, contractors, and vendors, whether working in a corporate office or remotely, often access critical IT systems and sensitive web apps using unmanaged devices that afford corporate IT organizations very little visibility and control.

SaaS solutions, web apps, and unmanaged devices are favorite targets for threat actors. Adversaries routinely exploit their inherent security vulnerabilities, as well as poor cyber-hygiene practices, to steal confidential data, spread malware, and carry out damaging attacks such as ransomware and distributed denial-of-service (DDoS).

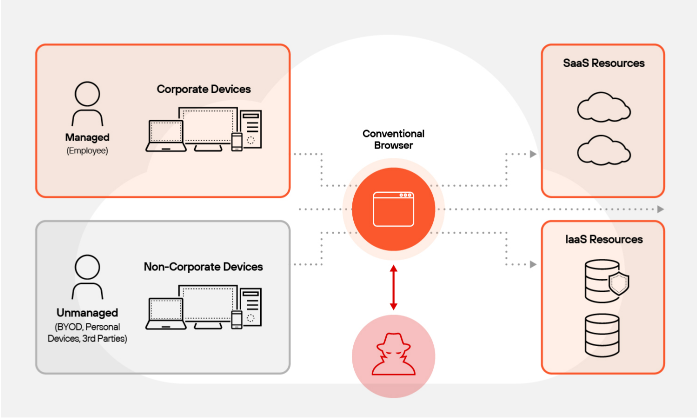

Figure 1-1: Today's diverse and distributed workforces use browsers to access an enterprise's data and applications.

Consumer browser risks

The browser is essentially an unlocked door for entry into the modern world of web applications and cloud-based solutions. It is where today's corporate users spend most of their working hours conducting business and engaging customers, colleagues, and partners.

DON'T FORGET

A 2024 Omdia study, "The State of Security in the Modern Organization," found:

- ☑ A 50% increase in web/SaaS app use is expected over the next 24 months, with 100+ apps already in use by study participants
- ☑ 85% of the daily work is taking place in a web browser

However, most organizations have little visibility into or control over their users' browser activities. Users can visit unsafe websites and succumb to malware, phishing attacks, and other threats without their employer's knowledge.

Unmanaged device risks

Employees, contractors, freelancers, business partners, and IT support vendors routinely access enterprise applications and IT systems using unmanaged devices — untrusted endpoints beyond the purview of corporate IT. Savvy threat actors can exploit poorly secured, unmanaged desktops, laptops, and mobile devices to steal confidential data, spread malware, and orchestrate advanced attacks.

Unfortunately, security teams often encounter resistance when they attempt to bring unmanaged devices into the fold. Many employees are concerned about their privacy and are reluctant to install potentially invasive corporate software on their personal devices. And many third-party vendors are unwilling to install their customers' security software on their endpoints or hand over endpoint administrative privileges to an outside organization.

DON'T FORGET

Unmanaged and poorly managed devices account for the bulk of security incidents.

> ☑ 68% of organizations that experienced accidental data leakage reported that these incidents ONLY occurred on poorly managed and unmanaged devices
>
> ☑ 89% of attacks were launched from unmanaged and poorly managed devices compared to 12% on managed devices

Source: Internal Palo Alto Networks research.

Managed device risks

Although managed devices are more secure than unmanaged ones, they still pose security risks that are not well addressed by current security solutions. One of the biggest risks is insufficient visibility by traditional endpoint and network-based security solutions into user activities in the browser, including the use of unsanctioned SaaS applications. This lack of visibility increases the browser's potential to act as an entry point for malware or allow leaks of sensitive data.

Transforming the Browser into a Secure Workspace

The browser is uniquely situated to serve as the first line of defense for the modern work environment. By directly embedding rich security capabilities with an enterprise browser, corporate IT and security professionals can gain deep visibility into and control over user behavior.

Using an enterprise browser protects data in SaaS solutions, private web apps, and unmanaged and managed devices. Even if a device is compromised, the impact on the organization is minimized because the data is protected against malware, theft, and abuse. A browser-based solution also boosts productivity, reduces complexity, and cuts costs.

Chapter 2

Overcoming the Limitations of Current Security Approaches

In this chapter

- Discover operational and usability challenges of legacy solutions
- Understand the limitations of traditional approaches, such as RBI, VDI, and DaaS
- Learn why enterprise browsers are the solution to overcoming these inefficiencies

Businesses have used various approaches to secure work, mitigate risks posed by unmanaged devices, provide secure access for remote workers, and defend against web-based attacks and risky websites. These approaches include virtual desktop infrastructure (VDI), virtual private networks (VPNs), desktop-as-a-service (DaaS), and remote browser isolation (RBI) solutions. Some organizations even resort to supplying contractors with corporate laptops.

In this chapter, we'll take a look at each of these approaches and explain some of their operational challenges and usability concerns.

VDI and DaaS

Some organizations use VDI or DaaS solutions to secure remote workers and support access from personally owned devices. With these solutions, desktop instances on servers are hosted in corporate data centers or the cloud, and business-critical apps and data reside on protected servers rather than unmanaged endpoints.

However, eventually, the session is connected to the unmanaged endpoint by video streaming. At this point, it can be manipulated to initiate a cyberattack. Additionally, malware on the unmanaged device can use screen recording or keyloggers to exfiltrate data or even take over a VDI session. And once you have malware on the server, the entire network is exposed.

VDI solutions' limitations also include scaling difficulties and high costs. Bandwidth constraints and latency issues can negatively impact the user experience.

CAUTION

While some security is built into VDI and DaaS, each has vulnerabilities. A commonly cited issue is weak default session policies that control what is allowed during the VDI or DaaS session. Unfortunately, because patching VDI and DaaS deployments can be complex, IT teams tend to prioritize patching traditional endpoints. This leaves the weak defaults in place, allowing vulnerabilities in VDI and DaaS to persist. Performance and compatibility limitations have also created issues for admins and users.

VPN

VPN solutions were originally intended to protect on-premises infrastructure and applications. Some companies still use VPNs to extend trusted enterprise networks to remote users on managed devices. While this approach worked well when applications were hosted primarily in corporate data centers, it’s not best suited for protecting SaaS applications or web applications running in public clouds.

With a legacy VPN solution, all traffic destined for the cloud is backhauled to the corporate data center. This approach can introduce latency, degrade application performance, and impair the user experience.

VPN solutions can be more difficult to administer and maintain than cloud-based systems. Legacy VPNs can also introduce security vulnerabilities. If an attacker gains VPN access, they also gain unfettered access to your entire corporate network.

RBI

RBI solutions are deployed to secure managed devices against threats originating in risky websites. With RBI technology, unsanctioned SaaS solutions and untrusted web pages are rendered on a remote server in the cloud and displayed on the user’s endpoint via pixel-streaming technology or other methods.

RBI solutions defend against web-based malware and data theft by completely isolating the user's browsing session from their device. However, this isolation causes latency, user experience issues (e.g., poor rendering), high bandwidth consumption, and drives up costs. In contrast, an enterprise browser provides a better experience with local, user-centric isolation that permits users to log into a secured browser account the same way they would with a personal browser.

CAUTION ⚠

While RBI solutions can help mitigate risk, they are often difficult to administer. Their deployment requires time-consuming manual labor. Similar to VDI and DaaS, RBI can introduce network latency that impacts the user experience.

Supplying Corporate Laptops

Some businesses opt to issue sanctioned corporate laptops to remote workers, including third parties and workers being integrated following a merger or acquisition. This approach ensures the devices run operating systems, security tools, and applications vetted by the corporate security team. However, a complementary solution is still required to protect remote work using browsers and the last mile of data loss prevention.

Supplying corporate laptops introduces significant administrative overhead, cost, and complexity. Onboarding and offboarding users and tracking and managing devices is a manual proposition that diverts valuable IT resources from more important tasks.

CAUTION ⚠

Procuring, setting up, and shipping corporate laptops can take weeks (or even months), delaying full productivity for new users or third parties. Once they receive their new machines, users may need some time to familiarize themselves with a new operating system or security tools.

Finally, some third parties may refuse to use a corporate laptop. It's unreasonable to expect contractors and service providers, who may work with dozens of different businesses, to have a special laptop just for your company. (Put yourself in their shoes and think about what life would be like if you had to use a dedicated laptop for each of your customers.)

A Better Way

Distributed workforces, cloud-based services, and web apps require a fresh approach to security. Hybrid workforces and direct-to-app architectures need a unified SASE solution to replace legacy security architectures that have become obsolete.

DON'T FORGET

According to Omdia's "The State of Security in the Modern Organization," 95% of organizations reported a security incident originating in the browser.

An enterprise browser, which can be used alongside or in place of a consumer browser, provides IT and security teams with comprehensive visibility into and control over web applications and user actions. In the next chapter, we'll look into this approach in more detail.

Chapter 3

Introducing Secure Browsers

In this chapter

- Learn why a browser-based approach to security is ideal for the modern work environment
- Understand how secure browsers elevate security compared to enterprise browsers
- Uncover the benefits of secure browser solutions
- Explore use cases for secure browsers that demonstrate their value

Modern business practices require a fresh approach to security — one that's conceived for an era of distributed workforces and ubiquitous use of cloud and web-based applications. The gateway to web and SaaS applications, the browser is uniquely positioned to serve as a critical first line of defense. Enterprise browsers secure managed and unmanaged devices and protect web-centric organizations against malicious attacks and data theft while providing a frictionless user experience.

Enterprise Browsers for a Web-first Work World

Until recently, the browser market was fragmented, with software giants like Google and Microsoft competing head-to-head with distinct designs and features for Chrome and Internet Explorer. There was no straightforward and cost-effective way for an independent software vendor (ISV) to create a browser-based security solution that addressed a large swath of the market.

Early browser-based security products failed to gain traction. ISVs were always playing catch up, trying to support multiple browsers and keep pace with new releases and functionality. Vendors didn't have the capacity to develop, test, and maintain their applications against vast combinations of browsers, devices, and operating systems.

We saw this change in January 2020 when Microsoft dropped its proprietary browser engine and introduced a Chromium-based version of its browser (Edge). Chromium is a popular open-source browser project spearheaded by Google. Microsoft's adoption helped drive industry consensus and standardization around Chromium, breaking down barriers for enterprise browser solutions.

Enterprise browser solutions raised this category to a new level, eliminating security gaps found in consumer browsers. With an enterprise browser, you can begin to create a secure, web-based workspace that controls access to sensitive corporate data across SaaS, web, and private applications.

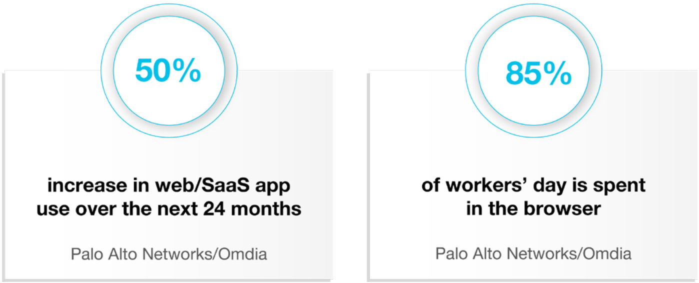

Figure 3-1: The browser is now the primary workspace and the most-used application in the world.

What Is an Enterprise Browser?

Enterprise browsers are Internet browsers that are centrally managed by an organization, as opposed to consumer browsers like Firefox, Safari, or Chrome, which individual users manage. Enterprise browsers are typically used to secure access to business applications from unmanaged devices used by remote/hybrid workers and third parties. They are increasingly being used as a complete replacement for consumer browsers. Enterprise browsers provide security, last-mile DLP, and visibility in the browser, offering detailed content and context-based controls.

TECH TALK

Mobile versions of enterprise browsers are gaining traction. They are being used as alternative to traditional mobile security solutions, which are viewed as too expensive and overly intrusive to end users, such as those that can wipe a personal phone completely.

With an enterprise browser, you get enhanced security compared to consumer-grade browsers and the ability to manage browser functions while ensuring a seamless browsing experience for employees. Purpose-built for business environments, enterprise browsers typically give you full visibility into and control over all web services and user actions according to policy. You can also block unsafe or unapproved activity and require additional authentication for highly sensitive activities. Standard enterprise browsers, however, may not be the most secure option for completely securing the browser-based workspace.

Standard Enterprise Browsers May Not Provide Adequate Security

While some enterprise browsers are more secure than consumer-grade browsers, they may not be adequate in securing the browser-based workspace against the most advanced phishing attacks and malware.

Some enterprise browser solutions use commodity-grade security solutions that rely on outdated technology. These enterprise browsers may be unable to detect modern phishing techniques, such as AI-generated and SaaS-hosted phishing attacks. Because they do not leverage threat intelligence from a vast pool of data, it is difficult for them to detect new and unique cyber threats.

Combining a lack of threat intelligence and commodity-grade security with the use of outdated malware detection methods, the standard enterprise browser is unable to adequately secure the web-based workspace.

Introducing the Secure Browser

The secure browser provides all of the same features of a standard enterprise browser, including full visibility and access control, a seamless experience for users, blocking unsafe activity, requiring additional authentication, content, and context-based controls, and last-mile DLP. But on top of these key features of an enterprise browser, the secure browser has advanced AI-powered security capabilities to protect the browser-based workspace against sophisticated phishing attacks and advanced malware.

In the modern web-based workspace, phishing attacks and malware are becoming increasingly sophisticated. Modern phishing attacks are using Generative AI to create new variants at a massive scale, and hiding behind SaaS apps to evade detection. Advanced malware is also using AI-based code generation to evade standard signature-based anti-malware engines.

The secure browser addresses these modern cyber threats with advanced AI-powered anti-phishing and anti-malware capabilities, further securing the workspace on the browser for any device, managed and unmanaged.

Secure Browsers Are Better with SASE

A SASE-native secure browser solution leverages cloud-delivered security services, browser-based data protection, and embedded advanced security features to efficiently reduce the attack surface by extending SASE to any device in minutes. It provides a secure workspace that protects sensitive data across SaaS, web, and private applications. It features a unified management console to administer all of the devices used by today's hybrid workforces. As part of a SASE solution, a secure browser gives IT and security teams comprehensive visibility into and control over web applications and user actions.

Secure Browser Benefits

Adopting secure browsers helps you realize business value across your organization—for everyone from IT and security teams to business units and end users.

The primary benefits of secure browsers are related to reducing risk, reducing costs, and increasing productivity. Secure browsers help lower your company's risk profile with security and data protection features that bolster your security posture. Compared to standard enterprise browsers, secure browsers provide best-in-class security. They also provide insights to IT and security operations center (SOC) teams.

To enhance security, secure browsers:

- ☑ Extend protection to unmanaged endpoints
- ☑ Leverage threat intelligence pooled from a vast amount of data
- ☑ Block the most advanced phishing attempts and access to malicious domains and unapproved sites
- ☑ Use advanced malware prevention engines to block new and unknown malware variants
- ☑ Prevent account takeover with credential protection and conditional access enforcement
- ☑ Offer deep visibility into browser activities for security, forensics, and regulatory compliance
- ☑ Use advanced URL filtering to protect against the most advanced web-based threats, such as malicious code, screen scrapers, spyware, new and unique malicious URLs, AI-generated and SaaS-hosted phishing attacks, and keylogging
- ☑ Isolate browser processes to protect systems from advanced threats, such as sophisticated malware and advanced phishing techniques
- ☑ Employ anti-tampering to prevent authorized changes to applications or services
- ☑ Reduce the attack surface by minimizing browsers' exposure to threats such as macros, scripts, and injection techniques
- ☑ Provide full control and protection for extensions
- ☑ Deliver a familiar user experience that keeps users from trying to bypass security

CAUTION

According to Omdia's "The State of Security in the Modern Organization," in the last 12 months, an alarming 95% of organizations reported a security incident originating in consumer browsers, initiated by a file download, phishing, and more. In 2023 alone, consumer browsers reported 345 vulnerabilities, with a whopping 210 of those being high-impact.

Data protection

Approaches taken by secure browsers to protect data:

- ☑ Secure data across the last mile with granular, policy-based controls, including compliance enforcement
- ☑ Control access to sensitive information based on security factors such as device posture, geolocation, and network connection
- ☑ Provide deep and broad DLP capabilities through a vast number of data classifiers
- ☑ Enforce continuous device posture checks to strictly control access
- ☑ Integrate just-in-time multi-factor authentication (MFA)
- ☑ Enable privileged access controls
- ☑ Use granular encryption for file transfers and downloads from corporate applications
- ☑ Block file downloads and uploads based on content and source sensitivity levels
- ☑ Restrict screenshotting, sharing via collaboration tools, copying and pasting, and printing
- ☑ Limit what users can do in the browser using account-based login restrictions

ON THE WEB

Common Vulnerabilities and Exposures (CVEs) in the browser open the door for malicious attacks and data theft. According to CVEdetails.com, as of May 2024, the major browsers had the following number of CVEs.

- Chrome — 3,677
- Firefox — 3,215
- Safari — 1,445
- Edge — 1,240

Visibility and control

IT and SOC teams leverage secure browser capabilities to:

☑ Support unified device management to rapidly onboard users and provide access to resources

☑ Monitor users' activity to discover and eliminate shadow IT

☑ Provide details about installed extensions, such as version, last update time, developer information, privacy policy, risk assessments, and permissions, to enable better control

☑ Centralize browser management with a dashboard for configuring access, policies, settings, and extensions

☑ Give security teams a comprehensive view of web activities across the organization with incident monitoring, selected session recording, and audit trails

☑ Allow easy logging and control of all events for threat hunting, forensics, and DLP

When you use an secure browser, you can also expect to see business and operational benefits centered around cost savings and productivity.

Cost savings

Secure browsers deliver immediate cost savings by allowing IT and security teams to:

☑ Reduce administrative expense and complexity

☑ Achieve significant total cost of ownership (TCO) savings vs. traditional solutions

- ☑ Avoid the capital, operational, and lost-productivity expenses associated with supplying corporate laptops to employees or third parties
- ☑ Eliminate or reduce the need for VPN, VDI/DaaS, and RBI solutions that are difficult and costly to administer and burden the help desk

Productivity and user experience

Secure browsers increase productivity and deliver delightful user experiences by helping IT and security teams:

- ☑ Onboard new users and respond to new business requirements quickly and easily
- ☑ Enable users to hit the ground running and become productive on day one
- ☑ Avoid inefficient, drawn-out processes like supplying corporate-sanctioned laptops or deploying special-purpose client software
- ☑ Eliminate latency by shifting security to endpoints
- ☑ Deliver maximum uptime with a fully distributed infrastructure

TECH TALK

Secure browsers give users the flexibility to seamlessly navigate between provisioned apps and work portals without having to sign in multiple times in the browser and opening the door for malicious attack

Use Cases Demonstrate Secure Browsers' Value

Secure browsers create a secure workspace on any device—managed or unmanaged. Deploying secure browsers allows you to consistently deliver frictionless and highly secure access to SaaS, web, and private applications and data. You can quickly address new and dynamic scenarios with highly flexible controls for data, access, and identity directly in the browser.

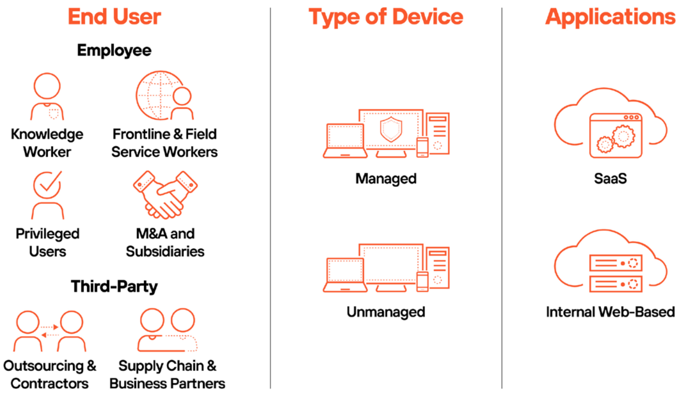

Figure 3-2: Secure browsers bring security everywhere users need to work, and IT teams need control.

Top use cases for contractors and BYOD

Access for third-party contractors, agencies, and business partners

Give non-employees secure access to SaaS and private apps from any device in minutes while meeting governance requirements, preventing unauthorized application access and data leakage, and blocking malware.

VDI and DaaS alternative

Deliver a high-performance experience and enhanced security with streamlined, secure access to web applications from any device. Increase worker satisfaction and productivity while reducing cost and complexity for the IT and security teams.

Securely enable BYOD policies

Allow employees and temporary workers to use their personally owned devices without compromising security. Secure BYOD will boost user satisfaction and productivity, cut onboarding times, and stop the spread of malware.

Facilitation of M&A and subsidiary operations

Apply uniform web security policies across heterogeneous organizations quickly and easily to improve governance, protect data and assets, and overcome corporate consolidation, integration, and spin-off challenges.

Cutting-edge use cases on any managed or unmanaged device

Secure encrypted traffic

Protect encrypted traffic such as QUIC and Microsoft 365 SLA, which is not inspected, logged, or reported on when using traditional security tools.

Last-mile data controls

Enable zero trust policy controls over work done in the browser, controlling actions such as screen sharing, printing, and downloading.

GenAI tools

Provide IT and security teams with deep visibility and tight control over all GenAI SaaS and web applications, including ChatGPT, enabling secure use of GenAI tools across the organization.

Privileged users

Protect the integrity and confidentiality of sensitive data, ensuring that access privileges are not stolen or abused and data is not accidentally tampered with.

Insider threats

Prevent both accidental and intentional data leakage by users without hindering productivity with highly granular last-mile data protections based on content and context, data sharing restrictions, and complete audit trails.

Now’s the Time for Secure Browsers

The adoption of secure browsers is exploding, driven by the powerful capabilities of these solutions and the shift in workstyles to hybrid models. Read on to learn about the features you should look for and evaluate when choosing a secure browser solution.

Chapter 4

Selecting the Right Secure Browser

In this chapter

- Learn what to look for when evaluating secure browsers
- Identify key product features and capabilities to consider
- Understand critical administrative functions and tech stack integration requirements

Not all secure browser solutions are alike. When evaluating a solution, you need to consider the product's core capabilities, administrative functions, convenience, and usability features, as well as the strengths and weaknesses of the vendor. Let's dig into each of these categories.

Security Features and Capabilities

Secure browsers should include an extensive collection of built-in security controls and data protection functionality to provide a secure environment. Key security features and capabilities to look for include:

Threat protection

Advanced security capabilities defend against sophisticated attacks and safeguard data with protections against internal and external threats like data exfiltration, credential and cookie theft, account takeovers, and man-in-the-middle attacks. Additional features to look for include:

- ☑ Ability to isolate enterprise apps and the browser from untrusted endpoints
- ☑ Last-mile data, identity, and access controls on selected apps, per policy
- ☑ Zero trust policies extended across selected actions and apps, with app and user context
- ☑ Extension controls
- ☑ Integration with a threat intelligence database with data pooled from a vast amount of events
- ☑ AI-powered, multi-layered anti-phishing prevention
- ☑ Advanced malware protection
- ☑ Anti-tampering protection
- ☑ Private app and SSH/RDP access controls
- ☑ Identity and privileged access controls with inline restrictions

DON'T FORGET

According to Omdia's "The State of Security in the Modern Organization," approximately 90% of organizations that had employees and contractors access corporate apps from personal devices. The prevalent use of personal devices is a serious challenge for security teams. They must strengthen security policies and tools to secure data on these unprotected endpoints.

Web and SaaS app filtering

A secure browser should have granular controls for web and app filtering to control the content accessible on networks. These controls prevent browsers from loading potentially malicious code. Look for secure browsers that:

- ☑ Allow or block access or login to individual URLs and web pages based on content categories and applications
- ☑ Manage which SaaS applications employees can access, preventing shadow IT
- ☑ Offer safe browsing based on a URL's reputation

DON'T FORGET

Businesses of all sizes are moving toward more robust security solutions—such as zero trust, secure service edge (SSE), and secure access service edge (SASE)—that provide greater visibility of network activity. Additionally, this transition helps organizations to better understand the vulnerabilities, threats, and practices associated with traditional remote access.

Data loss prevention (DLP)

Secure browser solutions should prevent data exfiltration and defend against insider threats with capabilities that extend to the last mile. DLP features to look for include granular, policy-based controls to manage users' engagement with URLs and applications by:

- ☑ Suppressing file download/upload capabilities
- ☑ Blocking copying/pasting of sensitive information into risky or uncategorized websites and apps
- ☑ Preventing printing of specific web pages or files from the browser
- ☑ Specifying which printers, such as home machines, can and cannot be used
- ☑ Disallowing screenshots, screen sharing, and video recording
- ☑ Restricting camera and microphone access by certain websites and apps
- ☑ Adding watermarks to sensitive files or any selected web app
- ☑ Hiding or disabling specific web page components
- ☑ Masking sensitive data automatically, according to user, device posture, and web application
- ☑ Encrypting files downloaded to an endpoint

Device management

A secure browser should offer device management functions that facilitate IT and security operations activities, including incident response. Capabilities needed to support these efforts include:

- ☑ Maintaining a full inventory of every device where the secure browser is installed
- ☑ Enabling immediate revocation of access for any device that's lost, stolen, or compromised
- ☑ Providing device posture assessment
- ☑ Granting access based on endpoint attributes like underlying operating system, patch version, and installed security software (e.g., EPP and EDR)

Usability and Convenience Features

No secure browser can be effective without providing a good user experience. The best solutions create a user-first workspace that makes it easy to work from any location and device. At a minimum, a secure browser solution should provide the following.

As organizations prioritize agility and productivity, the adoption of a SASE-native secure browser is instrumental to ensuring secure and efficient access to resources in the ever-connected world.

Frictionless onboarding

Leading secure browser solutions make it easy to onboard new users and manage software distributions and updates using your existing device management platform or a simple email.

Familiarity

To provide the same look and feel that users are familiar with, a secure browser should be based on Chromium. This platform ensures a seamless transition from a consumer-grade browser, like Chrome or Edge, by providing the same user interface, bookmarks, extensions, and rendering of web pages.

Seamless logon

Secure browsers should seamlessly integrate with identity providers (IdPs) and Active Directory to enable single sign-on (SSO) and reduce password fatigue and user frustration.

Consistent experience across devices

You should be able to use a secure browser to synchronize user profiles across devices. The browser should deliver a consistent experience whether users are working in the office, from home using their own devices, or on the go using a mobile device.

Convenience and productivity

An secure browser solution should support shortcuts and bookmark/setting import functions to improve usability and streamline adoption. It should deliver a high app performance and a smooth user experience that maximizes employee productivity and doesn't cause any delay or latency.

TIP

Secure browsers that are simple to distribute, install, upgrade, use, and don't burden help desk teams have far greater adoption rates and significantly fewer workaround attempts.

Centralized Administrative Features and Capabilities

Secure browsers should have a complete set of administrative tools that make it easy for IT and security operations teams to distribute and update new releases, onboard and offboard users, provision and manage user privileges, monitor and track user activity, and take advantage of existing IT systems and practices. To provide the best experience for end users and administrators, the solution should feature single-pane-of-glass management across browser deployments. Following are several of the main features and capabilities to consider.

Unified management

Secure browser solutions should empower administrators to define and enforce security policies at scale. To achieve this, the best secure browsers are part of a unified SASE solution rather than a standalone tool. Beyond SASE integration, platform-oriented secure browser solutions should offer features such as:

- ☑ Easily configure granular, policies based on user, device posture, location, time, or network
- ☑ Flexibility and ease of use when setting policies
- ☑ The ability to apply policies across users without creating friction
- ☑ A policy engine that lets you set policies once and apply them on any type of device (computer and mobile)
- ☑ An integrated experience as users are automatically "bumped" from their personal browser to the secure browser for applications that require higher levels of protection

TECH TALK

It is important to look at the policy engine's scalability and ease of use as usage grows to include more use cases and users.

Visibility and analytics

Administrative tools should be included with a secure browser solution to provide data for analyzing user behavior and to make it easier to identify potential security issues in real time. Capabilities to look for include:

- ☑ Built-in reports and dashboards that provide high-level and granular views into users' browser activities
- ☑ Web audit trails and session recordings to support forensics and compliance requirements
- ☑ Metrics reflecting users' digital experiences, such as page load and idle times, and CPU and RAM usage

Software distribution and deployment methodologies

Look for a secure browser solution that supports multiple software distribution and deployment options to help ensure compatibility with your incumbent endpoint software and configuration management tools. This compatibility will streamline onboarding and minimize support requirements. A best-of-breed secure browser solution can be:

- ☑ Managed using third-party software distribution tools and methodologies such as Microsoft System Center Configuration Manager (SCCM) and Microsoft Group Policy Objects (GPOs), as well as unified endpoint management (UEM) and mobile device management (MDM) tools
- ☑ Easily deployed via email invitations with no admin privileges required, which is especially important for outside users such as contractors, freelancers, and home-based workers, who often use unmanaged devices beyond the purview of corporate IT

Integration with your existing tech stack

Leading secure browser solutions are designed to help you protect and extend previous investments and reduce adoption barriers. More on this in the next chapter.

Choosing a Vendor

The vendor you choose is as important as the secure browser itself. Look for a vendor that:

- ☑ Provides the level of technical support that your team needs
- ☑ Comes highly recommended in independent reviews by industry experts, including customers and analysts
- ☑ Offers a secure browser that is part of a unified SASE solution

Security Features and Capabilities	
Threat protection	❑
Web and SaaS app filtering	❑
Data loss prevention (DLP)	❑
Device management	❑
Usability and Convenience Features	
Frictionless onboarding	❑
Familiar look and feel	❑
Seamless logon	❑
Consistent experience across devices	❑
Convenience and productivity	❑
Centralized Administrative Features and Capabilities	
Unified management	❑
Visibility and analytics	❑
Software distribution and deployment methodologies	❑
Integration with your existing tech stack	❑
Vendor	
Complete platform-based solution	❑
Support for managed and unmanaged devices	❑
Robust technical support	❑
Strategic partnerships	❑
Positive reviews by customers and industry analysts	❑

Table 4-1: Use this feature checklist to evaluate secure browser products and compare vendors.

Chapter 5

Integrating Secure Browsers into Your Tech Stack

In this chapter

- Understand how secure browsers integrate with other elements of your IT stack
- Find out how a SASE-native secure browser can augment your existing security tools and strengthen your security postures
- Learn how a SASE-native secure browser enhances visibility into security incidents and IT assets

Secure browsers are designed to integrate with other security applications and services. As shown in Figure 5-1, these include identity management and directory services, endpoint protection solutions, zero trust network access solutions, and SIEM and SOAR platforms.

These integrations, coupled with a secure browser that is part of a unified SASE solution, optimize security and IT operations. You get all the benefits of a secure browser, extended value that comes from integrated solutions, and, most importantly, streamlined and secure access for users from any device or location.

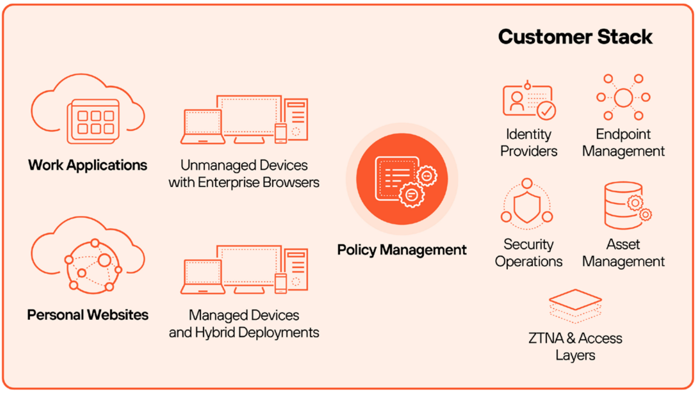

Figure 5-1: A secure browser should integrate with your technology stack.

SASE

Native integration of a secure browser with a SASE platform extends SASE's protective reach beyond managed devices, bringing consistent visibility, control, and security to web applications on any device. With native integration, you can deploy granular security measures for browser-based work on any device. This means that you not only enhance security in the browser but also dramatically simplify operations by monitoring all devices, branches, apps, and IT infrastructure from a single management system.

Integrating your secure browser with SASE gives you unparalleled, frictionless security that:

- ☑ Increases IT and business agility by easily extending SASE protection to managed and unmanaged devices in minutes
- ☑ Stops threats to components ranging from the app to the browser on the fly
- ☑ Unifies visibility across managed and unmanaged devices for comprehensive oversight

Identity Providers

Browser integrations with identity providers streamline user authentication and strengthen access control. These integrations are essential, as they provide a secure and efficient browsing experience throughout your environment.

Leading secure browsers integrate with products from popular identity providers, such as Azure Active Directory, Okta, and PingID. This allows secure browsers to provide conditional access controls and single sign-on (SSO) functionality.

Conditional access controls

Integrations with identity providers bring conditional access controls to secure browsers. With conditional access controls, you can require all users, or just named users, to use the secure browser to access specific web applications and services.

TECH TALK

Integration with identity providers ensures that access to specified SaaS and web apps from any other browser, including consumer-grade browsers like Chrome or Edge, is blocked.

You can also use conditional access controls to enforce security policies based on factors like user identity, device health, location, and resource sensitivity. By integrating with identity providers, secure browsers can leverage conditional access capabilities to prevent unauthorized users from accessing sensitive resources.

Single sign-on (SSO)

SSO, enabled through integrations with identity providers, allows users to authenticate to websites and all their enterprise applications securely using just one set of credentials.

Adding SSO functionality to secure browsers reduces password fatigue and frustration. It also increases users' productivity by reducing time spent dealing with multiple passwords. IT and security teams benefit because SSO improves security posture by minimizing the number of parties receiving users' credentials.

Endpoint Protection Solutions

Endpoint protection integrations safeguard data and defend against attacks by preventing users from downloading malicious files and blocking access to nefarious websites. These integrations help you better manage and secure user interactions across all endpoints.

Third-party endpoint protection products enhance security and control with:

- ☑ Automated endpoint detection and response (EDR)
- ☑ Extended detection and response (XDR)
- ☑ Threat intelligence feeds and platforms
- ☑ Antivirus and anti-malware software
- ☑ Intrusion detection systems (IDS) and intrusion prevention systems (IPS)

Security Operations Solutions

Secure browsers integrated with SIEM and SOAR solutions can forward security event messages and alerts to these platforms. This provides real-time threat detection, automates threat responses, and enables holistic monitoring and forensics.

SIEM and SOAR integrations also help SecOps teams streamline investigations and accelerate discoveries and responses by collecting and analyzing secure browser events, along with events from other network and security solutions and IT infrastructure.

TECH TALK

Integrating secure browsers with SIEM and SOAR solutions allow them to support threat analysis and incident response while avoiding the complexity of decrypting and inspecting SSL traffic in networks.

In addition, integrating SIEM and SOAR platforms with secure browsers helps you:

- ☑ Provide a centralized view of security operations across managed and unmanaged devices
- ☑ Deliver security analytics for all users
- ☑ Expedite incident response across all endpoints

Asset Management Systems

By providing integrations with IT network and system management solutions, IT teams can leverage the browser to simplify tedious remote systems management functions like distributing updates and patches and tracking devices connected to the network. Integrations with systems like IT asset management (ITAM) platforms allow IT teams to manage endpoint inventory and usage data without requiring users to install ITAM agent software.

TIP

You can use a secure browser to give IT staff the information and access they need and avoid user resistance to having "intrusive" software installed on their BYO laptops and mobile devices.

Some secure browser solutions can eliminate the need for intrusive agent software by supplying device configuration information and posture metadata (e.g., installed operating system, patch version, and security software) to an asset management platform. With this approach, corporate IT organizations can maintain asset information for both managed and unmanaged devices from a single ITAM platform.

This functionality also makes it faster and easier for IT and security teams to manage access controls. For example, the visibility and access provided with a secure browser allow these teams to adjust access privileges based on changing requirements. Asset management can also be used to immediately revoke access for any device that's lost, stolen, or compromised.

DON'T FORGET

According to Omdia's "The State of Security in the Modern Organization," more than 50% of organizations reported a lack of confidence in their ability to address security issues in unmanaged/poorly managed devices. And more than 30% found that threats on unmanaged/poorly managed devices had a higher financial and business impact compared to all other security incidents.

Zero Trust Network Access Solutions

Zero Trust Network Access (ZTNA) solution integration has become a must-have for most secure browser users. Similar to an identity provider integration, a ZTNA integration prevents users from accessing enterprise applications and services with consumer browsers by verifying that traffic originates from the secure browser.

However, secure browser integration with ZTNA solutions goes further, providing secure access to private, browser-based apps and resources hosted in the cloud or on-premises.

Delivering ZTNA as part of a secure browser simplifies deployment and ongoing management for zero trust access and fortifies network security by enforcing three core principles:

1. Ongoing, deep security inspection of all application traffic, including allowed connections, to help prevent threats like zero-day attacks
2. Elimination of access by default, requiring administrators to enable access to a resource using a policy rule explicitly
3. Continuous trust verification, even after access to the app is granted, to monitor and verify all changes to device posture in real time

Chapter 6

Getting Started

In this chapter

- Understand how to identify and prioritize secure browser use cases and user groups
- Identify ways to minimize user objections and overcome adoption barriers
- Learn how to deploy secure browsers effectively across your business

Most secure browsers are easy to deploy. You can distribute and install them with minimal impact on your help desk or support teams by using your existing device management solutions or a simple email invitation.

The best way to roll out secure browsers is in a phased fashion to minimize risk. Many organizations first deploy a secure browser to address a specific business scenario, like providing secure access to unmanaged bring-your-own (BYO) devices.

Once IT and security leaders become familiar with secure browsers and acknowledge their value, they often expand deployments to other user communities and use cases, making incremental adjustments along the way.

Plan Your Rollout

Start by identifying and prioritizing where and how secure browsers can add value to your business. Some organizations deploy secure browsers or extensions reactively, such as after a security breach. Others deploy them proactively, such as to enable secure access for contractors or as part of a larger initiative like a corporate acquisition.

Chapter 3 describes common use cases for deploying secure browsers to secure managed and unmanaged devices. To identify and prioritize use cases, talk to line-of-business managers to understand their end users' browsing practices, the types of devices they use, and the applications they require to perform their jobs.

TIP

Here are a few questions you can ask line of business managers to help uncover use cases.

- ☑ Do employees often work from home or the road?
- ☑ Do they use their own laptops or mobile phones for work?
- ☑ Do they use SaaS solutions and private web apps in their work?
- ☑ Does the business group use freelancers, contract workers, or outsourcers?
- ☑ What percentage of work is done in the browser?
- ☑ Do they use many web apps to run the business?

Use this information to determine which business units and users pose the greatest security risk and will benefit most from a secure browser.

Avoid User Objections

Secure browsers don't have a learning curve since they are designed using the same framework as Chrome and other commercial browsers with additional security measures built in. However, most users are upset by the change, making it difficult to persuade them to adopt a new approach. Make sure your users understand why the company is moving to an secure browser.

It is important to explain the risks that consumer-grade browsers present and how their exploitation causes big problems, not just for the business but for users as well. Beyond the risks, make sure to point out the superior user experience and improved productivity they could gain in comparison to other security solutions used in the company. When users understand how secure browsers can help reduce these risks without impacting their workflows, they typically put objections aside.

Make it real

Describing real-world scenarios to users helps reinforce the personal and professional impacts of cyber risk. Examples can illustrate the kinds of troubles that arise from inadequate browser security, like malware infecting their system or compromised credentials, locking them out of their applications.

Take the devil out of the details

You can also calm users by describing exactly when and how the secure browser will be rolled out.

Describe the new changes, when they will take effect, and how users will be impacted – and be specific. Providing an FAQ list is a great way to alleviate user concerns and avoid trouble tickets and complaints proactively. It also will help you think through the rollout process from the user's perspective and identify any hitches that may have been missed or additional steps that can make it smoother for them.

Be ready for questions AND complaints

To be prepared to counter user objections and turn naysayers into supporters, be ready to answer the following questions:

- ☑ Will the secure browser slow down my computer and impact other applications?
- ☑ Will the secure browser on my computer or mobile device monitor my activity or collect my personal data?
- ☑ What happens if I try to access a business application using my regular browser?
- ☑ Can I still use my regular browser to access personal applications and browse the web at work?

It would also be helpful to frame the answers in the context of your organization and different lines of business where applicable. Remember, facts tell, and stories sell. Turn users' questions into an opportunity to win their support.

Deploy in Stages

As with any other major IT initiative, it is best to deploy secure browsers in phases. A phased deployment minimizes risks, disruptions, and support burdens. By deploying in stages, you can identify and address potential issues or challenges and make necessary adjustments before rolling out the solution across the entire enterprise.

Prepare users for the change

Start talking to users about what's coming well in advance of the secure browser deployment. The previous section provided some proven techniques to help with this.

Secure browser deployment at a glance

Below, I've outlined the deployment process at a very high level to give you a sense of what it entails. As you can see, it's pretty straightforward and does not require heavy lifting for admins or end users.

- ☑ Identify the applications and user groups whose access will be restricted to secure browsers
- ☑ Integrate the secure browser with the identity provider
- ☑ Identify unmanaged devices (there are a number of tools that can automate this)
- ☑ Ensure the use of identity provider on unmanaged devices
- ☑ Provide user training
- ☑ Send users an invitation to set up the secure browser on their system

☑ Monitor adoption and follow up with users who do not set up their secure browser

☑ Be responsive to users who are asking about issues or concerns, and be quick to address any that surface

Start with a proof of concept

TIP

Start with a proof of concept (PoC) or pilot program involving a friendly group of users to validate the solution and work out the kinks. Have your users test out all the basic features and functions of the secure browser before configuring security policies.

Be sure to have a structured process for soliciting and capturing feedback. When input has been collected, categorize and prioritize it. I recommend addressing only the most pressing issues, as more are likely to surface as the full-scale rollout is underway. It will be faster and easier to make changes in bulk rather than piecemeal.

Quick wins

Upon the successful conclusion of the PoC or pilot, identify one or two high-priority use cases that can serve as quick wins. These early deployments can provide tangible benefits and help demonstrate the solution's value to key stakeholders and leadership. For instance, select a group of users with BYO devices or some friendly third parties for an initial rollout.

After you have a couple of quick wins, you can confidently roll out the secure browser to other business units and user communities to address other use cases and strengthen your company’s overall security posture.

These wins can also be added to your user communication mix. As noted previously, sharing real-world stories helps reduce users’ resistance and allay their fears.

CAUTION

Once you implement security policies, users may not be able to fall back to a consumer browser if something goes wrong, depending on how you set up your configuration. Identify the mission-critical use cases and include them in sandbox testing. Key areas to focus on are:

- ☑ Integrations with identity provider
- ☑ Performance on active devices (e.g., iOS and Android)
- ☑ Deployment model – manual or using mobile device management (MDM) and enterprise mobility management (EMM) solutions

Next Steps

In this book, I presented the new paradigm of web-first work, explained the limitations of current security approaches, and introduced the concept of secure browsers. I also delved into the process of selecting an appropriate solution and integrating it into your existing tech stack. Finally, I've provided guidance on getting started with secure browsers and extensions.

I hope you keep this book handy to reference as you use secure browsers to enhance your organization's security posture in the face of evolving browser-based threats.

The journey to secure browsing is ongoing, but with the right tools and understanding, you will be well prepared to face these challenges head-on.

paloalto® NETWORKS
CYBERSECURITY PARTNER OF CHOICE
It's time to fight AI with AI.
Predict cyberthreats and stop them in real time with Precision AI™ by Palo Alto Networks.
Learn more at paloaltonetworks.com/precision-ai-security

Are you confident in the security of your hybrid workforce and their use of web applications? The Definitive Guide to Secure Browsers shows how you can protect them.

The majority of users do most of their work through a web browser and often from personal devices, but traditional security systems were not designed to protect this attack surface. Secure browsers provide consistent visibility, control, and security to web applications on any device. When natively integrated with SASE, secure browsers can extend it to any device in minutes.

- Secure browsers – learn why a browser-based approach to security is ideal for the modern work environment.
- SASE-native secure browser solution – see why SASE integration enhances overall security and reduces complexity.
- Data protection – find out how you can restrict access to sensitive information based on specific security factors.
- Visibility and control – centralize browser management with a dashboard for configuring access, policies, settings, and extensions.
- Integration with your tech stack – review key secure browser integrations and why they are important.
- Requirements – understand how to select the right secure browser, identify optimal use cases, overcome user objections, and deploy them effectively.

About the Author

Emily Matthews is a renowned expert in the cybersecurity market. With over 20 years of experience, she has crafted insightful content that aids decision-makers and practitioners in comprehending cybersecurity solutions and services from a wide range of providers, including Fortune 500 giants and innovative startups.

CYBEREDGE PRESS℠

Not for resale

ISBN 978-1-948939-39-3

9 781948 939393 >