An Enterprise Browser for the Digital Business

Secure any web application, for any user, working from any location, using any device

Overview

SaaS solutions, cloud-based services, and hybrid work models fundamentally change the way businesses operate, creating new opportunities for threat actors and new challenges for corporate IT and security organizations. Today's enterprise is awash in unmanaged and untrusted devices—endpoints over which the business has little visibility and control. Home-based workers, contractors, IT support vendors, and business partners routinely access enterprise applications and systems using their own endpoints, exposing the business to malware and data exfiltration. Most security and IT teams simply have no way to validate the posture of an outside device accessing an enterprise resource. Many businesses resort to supplying remote employees and contractors with corporate laptops—a costly and drawn-out approach that squanders resources and delays onboarding.

Forward-looking enterprise security and IT leaders are turning to a new breed of browser-based solutions to secure unmanaged and untrusted devices, and protect today's web-centric businesses against malicious attacks and data theft. Specifically designed for the era of hybrid workforces and web applications, new Enterprise browsers transform the browser into a secure workspace by embedding rich security functionality directly into the browser.

The browser is the gateway to the world of web applications and SaaS solutions, and the logical place to implement fine-grained security controls. With an Enterprise Browser, any authorized business user can seamlessly access any website or web app, using any device, from any location, without posing security risks.

Enterprise Browsers are the perfect solution for extending corporate web apps and services to unmanaged devices and untrusted endpoints. They overcome the inherent cost constraints and adoption barriers associated with securing outside endpoints, defending against data exfiltration and malware spread without requiring intrusive endpoint software or Windows administrative privileges. With an Enterprise Browser, corporate IT and security organizations can easily verify any endpoint's posture before granting users access to enterprise systems and data.

This paper reviews the key features, functions, and benefits of Enterprise Browsers in general, and Talon's Enterprise Browser in particular. It describes what an Enterprise Browser is, why it is required, and why the concept is now poised for success.

Introduction

Enterprises are adopting cloud-based services and SaaS solutions to accelerate the pace of business and simplify operations. Digital transformation has reshaped the way businesses deliver and access applications, exposing the business to new attack vectors and threats.

Traditional perimeter-based security architectures, conceived to defend trusted enterprise network borders and protect conventional on-premises infrastructure and applications, aren't well suited for the digital era. In today's world, enterprises develop and deploy line-of-business applications in public clouds beyond the secure confines of the enterprise network. And hybrid workforces access SaaS solutions and internal web apps from home, as well as the office, using both company-owned and employee-owned devices, often bypassing the trusted enterprise network altogether. Unmanaged and untrusted devices expose the business to ransomware and other damaging malware. And to make matters worse, business groups and individual employees often sign up for public SaaS solutions without corporate IT involvement, subjecting the enterprise to additional security risks.

Source: CVE Details (May 2023)

Consumer browsers are laden with CVEs

Cyberattacks and data breaches can disrupt business-critical IT systems, impair revenues, damage a company's reputation, and lead to costly compliance fines, legal settlements, and recovery expenses. In fact, the average total cost of a data breach is now $4.35 million.[1]

[1] IBM Security Cost of a Data Breach Report 2022

Threat actors are continuously honing their skills, looking for new ways to penetrate systems, steal data, and wreak havoc. Poorly secured web apps, unsanctioned SaaS solutions, unvetted devices, and remote users are easy prey for clever threat actors. And if that's not bad enough, consumer browsers like Chrome and Safari are laden with CVEs (Common Vulnerabilities and Exposures) and are susceptible to tracking, malicious toolbars, and nefarious plugins. Threat actors routinely exploit consumer-browser vulnerabilities to steal confidential data, install ransomware and other types of malware, and orchestrate attacks.

A Browser-Based Approach to Security for the Digital Era

Digital transformation requires a fresh approach to cybersecurity. An approach specifically conceived for the era of hybrid workplaces, SaaS solutions, and web apps. The browser is uniquely positioned to serve as a critical first line-of-defense for today's web-centric, borderless enterprises.

The browser is the entryway to the world of web applications and SaaS solutions, and the new workspace for modern business users. It is where users spend most of their working hours, conducting business and engaging customers, colleagues, and partners. By embedding rich security capabilities directly into the browser, you can give enterprise IT and security professionals deep visibility and tight control over end-user behavior, and help secure data and defend against web-borne attacks.

What is an Enterprise Browser?

An Enterprise Browser is a hardened web browser, purpose-built for enterprise deployment and operation, that delivers previously unachievable security functionality. It provides granular controls and auditing capabilities for all web services, improving visibility and governance, while optimizing the user experience. An Enterprise Browser provides meaningful risk reduction, instant cost savings, and greater IT agility.

Unlike its consumer counterpart, an Enterprise Browser is designed with a security-first mindset. It includes built-in functionality to protect against malware, phishing, account takeover, man-in-the middle attacks and other modern threats. It helps enterprises safeguard infrastructure, protect confidential data, and mitigate risk as part of a defense-in-depth, Zero Trust security strategy.

Securing Unmanaged and Untrusted Endpoints

An Enterprise Browser provides secure access for unmanaged and untrusted devices without requiring admin privileges on the device or raising end-user data privacy concerns. Today's hybrid workers often use their own devices from home, the road, or the office. Most employees are concerned about data privacy and reluctant to install potentially invasive corporate software on their personal devices. No employee wants their employer accessing their personal data or controlling their home computer or personal laptop. Trade unions, regulators, and human resources organizations are all rallying behind employees, advocating for rules and policies to protect user privacy. An Enterprise Browser alleviates privacy concerns and eliminates objections by providing strong security without taking full control of the user's device or gaining access to the user's personal applications or data.

An Enterprise Browser also overcomes the challenges associated with extending corporate IT services and infrastructure to business partners and support vendors. Many enterprises open their networks and line-of-business applications to third parties like contractors, IT support providers, suppliers, sales channels, and other business partners over which they have limited visibility and control. Unmanaged and untrusted partner devices open the door for threat actors and malware. But most third parties are unwilling to install unsanctioned security software on their endpoints or hand over endpoint administrative privileges to an outside organization. As a result, some enterprises go as far as furnishing vendors and contractors with dedicated laptops—a costly approach that often impairs end-user satisfaction (nobody wants an extra laptop) and hinders adoption. An Enterprise Browser overcomes these challenges by defending against data exfiltration and malware spread without requiring special endpoint security software or Windows admin access.

Why an Enterprise Browser?

Over the years businesses have used a variety of technologies to secure remote workers and defend against internet-originated attacks, including virtual private networking (VPN), virtual desktop infrastructure (VDI), and remote browser isolation (RBI) solutions.

VPN Solutions Aren't Suited for Cloud Apps and Web Services

Most businesses use VPN solutions to securely extend trusted enterprise networks to remote workers. VPNs rely on special-purpose software clients that are notoriously difficult to roll out, use, and support. Worse still, VPNs were conceived to protect on-premises infrastructure and aren't well suited for securing web apps; all cloud-destined traffic is backhauled to the corporate data center, which adds latency and hampers performance. Furthermore, VPNs provide "all or nothing" access to corporate resources; they don't provide granular access controls. Finally, VPN solutions often introduce new security risks by adding entry points to the network and opening the door for lateral movement from unmanaged devices.

VDI and DaaS Solutions Degrade Performance and Usability

Some businesses use Virtual Desktop Infrastructure (VDI) or Desktop as a Service (DaaS) solutions to secure remote workers and provide support for employee-owned devices. VDI solutions strengthen security by hosting desktop instances on centralized servers in corporate data centers or in the cloud. With a VDI approach, business-critical applications and data reside on protected servers, not on the users' unmanaged endpoints. VDI solutions can be difficult and expensive to size and scale, and are prone to deliver poor user experiences.

RBI Solutions Impair User Experience and Satisfaction

Some businesses use remote browser isolation (RBI) solutions to sandbox browser activity and defend against web-borne malware and zero-day exploits. RBI solutions isolate web traffic, but don't provide deep visibility or tight control over user activity. With RBI technology, untrusted webpages are typically rendered on an isolated server in the cloud and displayed on the user's endpoint via pixel-streaming technology or other methods. RBI solutions prevent malware spread, but they are inherently costly and inefficient. Remote rendering introduces network latency, impairs performance, and produces a suboptimal user experience. So much so that many organizations only use RBI solutions to protect extremely sensitive business applications that pose legal or compliance risks.

Enterprise Browsers overcome the fundamental performance, cost, and UX constraints of traditional VPN, VDI, and RBI solutions by embedding advanced security functionality directly into the browser and delivering a responsive, native user experience. They defend modern web applications against insider and external attacks, and protect data privacy without impairing user satisfaction, hindering worker productivity, or overly complicating operations. And they augment the native security capabilities of SaaS solutions, providing full visibility and control of user behavior, and preventing data exfiltration.

Why Now?

Until recently the browser market was fragmented, with industry heavyweights like Google and Microsoft competing head-to-head with distinct designs and features. There was no straightforward and cost-effective way for a vendor to create a browser-based security solution that addressed a large swath of the market. Early browser-based security solutions failed to gain traction because vendors were always playing catch up, trying to support multiple browsers and keep pace with new browser releases and functionality. Vendors simply did not have the wherewithal to develop, test, and maintain their applications against vast combinations of browsers, devices, and operating systems.

That all changed in January 2020, when Microsoft dropped its proprietary browser engine and aligned with Google, introducing a Chromium-based version of Edge. Chromium is a popular open-source browser project spearheaded by Google. Microsoft's adoption has helped drive industry consensus and standardization around Chromium, breaking down barriers for Enterprise Browser developers like Talon, transforming the browser into a platform for innovation. With Chromium, developers can focus on delivering value-added, differentiated capabilities like enterprise-grade security functionality, knowing their applications will run on a wide variety of endpoints and operating systems, and deliver a consistent user experience.

Enterprise Browser vendors can leverage Chromium to accelerate time to market, broaden product appeal, and reduce development cost and complexity. Chromium provides easy portability and extensibility, a rich feature set, a familiar user experience, and the full backing of a large open-source community and partner ecosystem.

What is the Talon Enterprise Browser?

The Talon Enterprise Browser is a hardened Chromium-based browser, infused with advanced security capabilities, specifically conceived to protect modern web applications and hybrid workforces. It delivers measurable risk reduction, immediate cost savings, and greater IT agility and end-user productivity.

Unlike alternative VPN, VDI, and RBI approaches, Talon's browser

- Is easy and cost-effective to deploy, administer, and support, and requires no admin privileges
- Provides secure access to SaaS solutions and internal web apps running in public or private clouds
- Delivers a responsive, native user experience
- Supports a wide variety of endpoints and operating systems, including employee-owned and company-managed devices
- Addresses a wide range of users including employees, contractors, business partners, and third-party IT service providers
- Secures office-based workers, home-based workers, and mobile users

Why Talon's Enterprise Browser

Talon's Enterprise Browser brings enterprise-grade security capabilities to the browser, turning a liability into an asset. The solution overcomes the fundamental performance, manageability, and usability constraints of VPN, VDI, and RBI technologies, providing strong security without introducing latency, impairing user experience, or overburdening the help desk.

The Talon Enterprise Browser provides:

Comprehensive visibility of all browser activities

- **Leverage built-in reports and dashboards:** Gain a full picture of browser activity for SaaS and web applications across the enterprise.
- **Deep insights for IT and security teams:** Capture full web audit trails, session recordings for forensic investigations and compliance, and control the depth of monitoring to ensure privacy.
- **Integration with external systems:** Leverage browser telemetry to improve the capabilities of your existing security stack, including SIEM and XDR platforms.

Native security built into the browser

- **Security by design:** Protect users at the exact point where they interact with corporate applications and data: the browser.
- **Protect against malware and phishing:** Multi-layered approach for phishing protection and built-in file scanning to stop infected file uploads and downloads.
- **Reduce browser, extension, and device risks:** Prevent account takeover and man-in-the-middle attacks, manage extensions, and disable vulnerable components.

Full control of all browser activity

- **Granular controls:** Set policy scope based on user, device posture, location, time, or network.
- **Last mile control of your data:** Prevent sensitive files from being uploaded, downloaded, or stored on endpoints, mask data for compliance reasons, and control clipboard, printing, and screenshots.
- **Zero Trust controls for web applications:** Assess device posture and apply conditional access controls, set up MFA and just-in-time privileges, and lock devices when left unattended.

Unmatched productivity, no matter where your users are

- **Seamless SSO integration:** Integrate existing Identity Provider (IdP) or Active Directory groups for easy, secure user sign-on.
- **Simplify work across devices:** Synchronize profiles across multiple devices to empower workers across managed, unmanaged, and mobile devices.
- **Rich productivity features:** Personalized home screen shortcuts, intuitive clipboard manager, and importing of browser bookmarks and settings make transitioning to Talon easy.

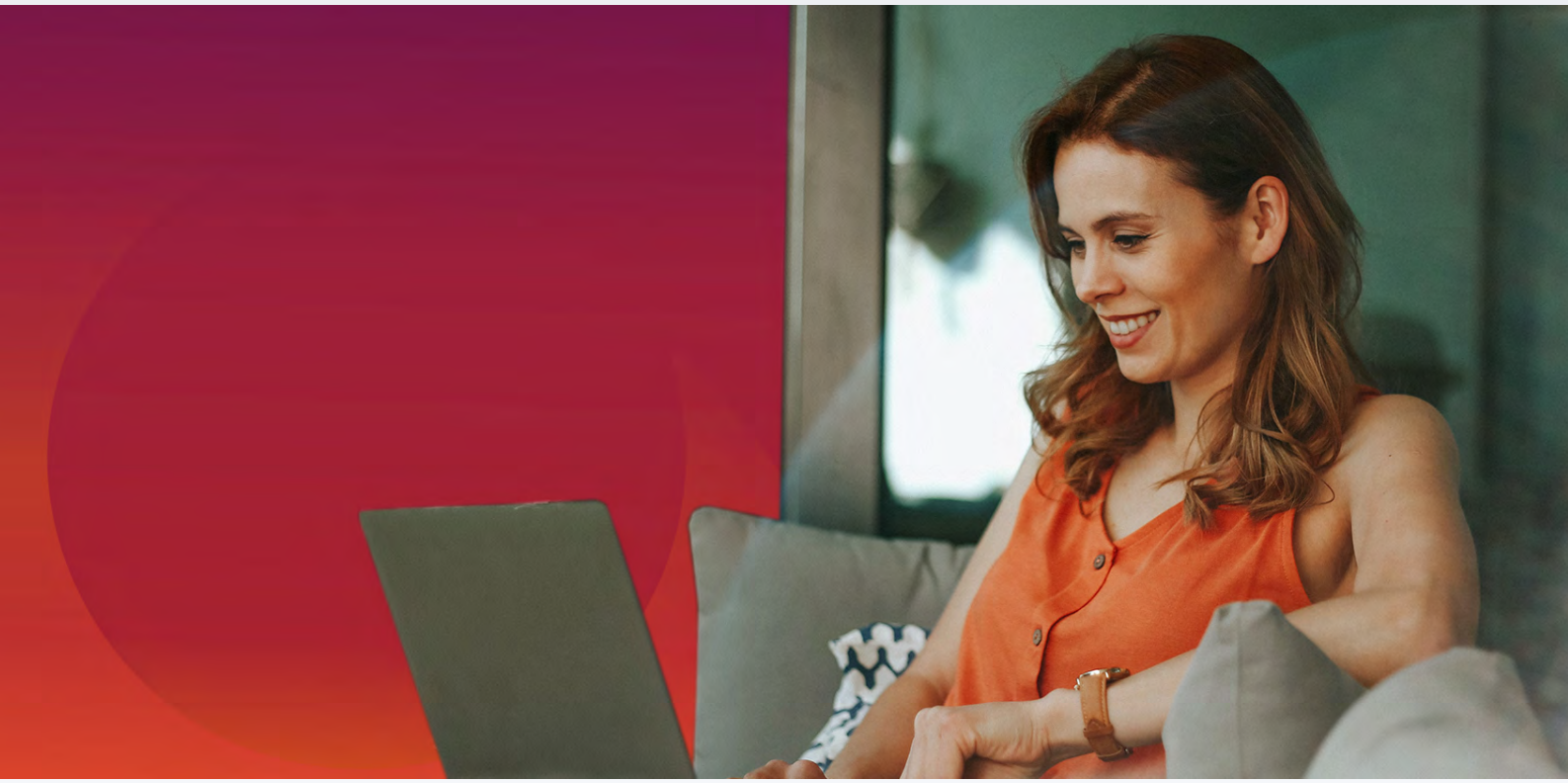
Superior end-user experience for any worker

- **Ultra familiar user experiences:** Built on Chromium – the same user interface, rendering, and extensions your workers know and love.
- **Enable device and OS choice:** Users are empowered to work from any location on any device they choose, all while remaining secure.
- **Onboarding made simple:** Workers get started in minutes rather than weeks, with no admin privileges required.

Talon Enterprise Browser Use Cases

The Talon Enterprise Browser supports a wide variety of applications and use cases, including:

- **Third-party support vendors, contractors, and business partners.** Securely extend internal web apps and browser-based admin consoles to non-employees. Improve governance, prevent unauthorized application access and data leakage, and block malware.
- **VDI and DaaS alternative.** Provide a secure workspace for team members that your end users will love for a fraction of the cost of VDI or DaaS solutions.
- **BYOD and unmanaged devices.** Allow employees to use their own devices at home, the office, or the road without compromising security. Improve user satisfaction and productivity, prevent data exfiltration, and defend against malware spread.
- **M&A and subsidiary operations.** Institute uniform web security policies across heterogeneous organizations—quickly and easily. Improve governance, protect data and assets, and overcome corporate consolidation, integration, and assimilation challenges.
- **Customer care and contact centers.** Safely extend internal web apps to outsourcers and home-based agents. Improve governance, quickly onboard and offboard users, and prevent data theft and malware spread.
- **Simple, seamless, safe browsing.** Provide a secure alternative to consumer browsers, without the drawbacks of RBI solutions. Ensure superior user satisfaction with a responsive, native browsing experience.



Summary and Next Steps

SaaS solutions and web apps are revolutionizing the workplace, and complicating life for corporate IT and security leaders. Conventional VDI solutions and RBI products can degrade application performance, frustrate users, and stall digital transformation initiatives.

Enterprise browsers are built from the ground up with hybrid workforces, unmanaged devices, and web services in mind. They help IT and security teams improve visibility and control without complicating operations or impairing the user experience.

Talon offers the industry's first Enterprise Browser. The Talon Enterprise Browser secures any web application, for any user, working from any location, using any device. To learn how the Talon Enterprise Browser can help your business reduce risk, cut costs, and improve IT agility and worker productivity book a demo today.

About Talon

Talon Cyber Security transforms the browser into a secure workspace with the market's most complete enterprise browser security portfolio, which includes the award-winning Talon Enterprise Browser, Talon Extension, and Talon Mobile. With Talon, IT and security teams benefit from deep visibility and tight control over all SaaS and web applications, enabling them to secure any user, in any location, on any device. Talon was named the Most Innovative Startup of 2022 at the prestigious RSA Conference Innovation Sandbox Contest. For more information, visit Talon at talon-sec.com, or connect on LinkedIn.