

Security Where You Need It Most

Protecting everything but the browser
isn't enough

ENTERPRISE BROWSER VS. OBSIDIAN SECURITY

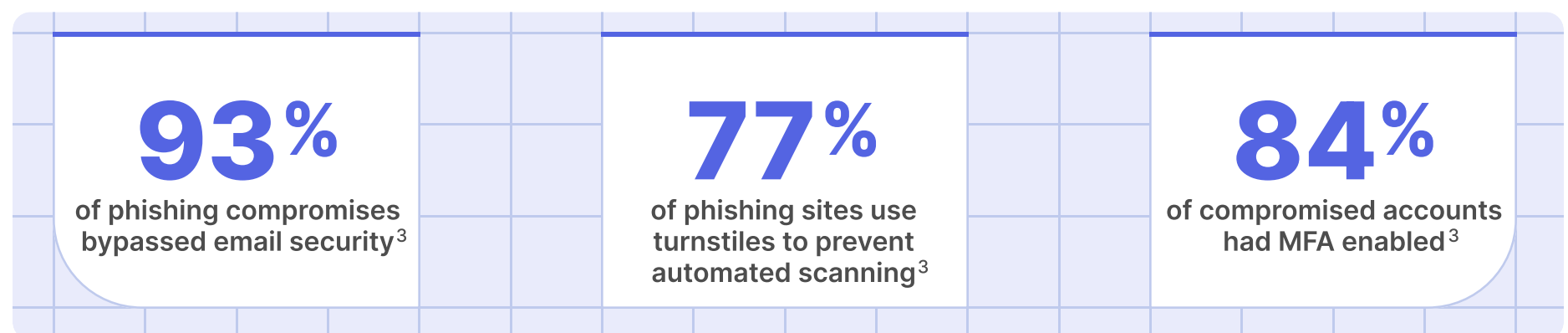
Browsers Are Where We Work

You can't get away with protecting everything but the browser—it's where your employees spend around 75%¹ of their time accessing business-critical SaaS applications, checking email, trying new GenAI tools, and much, much more. Despite the crucial role the browser plays, it represents a gap for many existing security tools, mainly because these tools were built to defend the places where we used to work (like the endpoint).

Security in 2025 and beyond requires a new focus.

Advanced Identity-Based Attacks Are Harder to Stop

We all know that email gateways aren't 100% foolproof. The use of adversary-in-the-middle (AiTM) techniques have grown in popularity due to their ability to sneak malicious links past spam filters using tactics like turnstiles to prevent automated scanning. In one month of 2024, Microsoft reported there were over 35,000 AiTM incidents.²



Manually tuning email security rules to stop these attacks not only results in more work, but leads to either too much legitimate content being blocked, or allows too much spam to pass through. It also relies on teams to be notified of every new toolkit attackers use; security professionals must then create new models and rules to stamp them out. It really becomes a high-stress and expensive game of whack-a-mole.

Shadow AI and SaaS Applications Hide Risk

The proliferation of AI tools like ChatGPT makes it difficult to monitor and secure sensitive and proprietary data; 10% of GenAI prompts contain corporate IP.⁴ Just this year, the Chinese AI assistant, DeepSeek, made headlines by becoming the most-downloaded free app in the U.S. on Apple's App Store.⁵ Just as quickly, researchers quickly exposed flaws in the application's security, demonstrating how to access a large database of sensitive data without proper authentication.⁶

SOURCES

¹ Forrester

² Microsoft Digital Defense Report (2024)

³ Obsidian Security

5-20+AI tools used on average
by employees³**44%**of AI apps are not
federated behind an IdP³**55%**of AI apps are connected
to core apps and data³

SaaS too has grown the attack surface. Because employees can easily procure and integrate applications with just a credit card and email address, security and IT often lack visibility into all the apps in the corporate environment. Despite this, security teams are still challenged with securing every tool employees are using—especially those connected to core systems and data. Unfortunately, finding and controlling every SaaS app before data is leaked is easier said than done.

Just scanning emails to discover unauthorized SaaS and AI applications result in false positives and missed apps. And relying on network whitelists can't stop teams from using unauthorized SaaS tenants hooked up to corporate data.

Existing Solutions Are Not Enough

Security teams need to bring policies and detections to where these applications and attacks are unfolding—the browser. It is where credentials are phished, threats become ransomware, and unauthorized applications are accessed.

However, legacy solutions like CASBs (Cloud Access Security Brokers), SWGs (Secure Web Gateways), and EDRs (Endpoint Detection and Response) have significant blind spots when it comes to browser security. CASBs only secure sanctioned applications and lack context, while SWGs typically rely on static URL filtering or known malicious indicators. EDRs miss most in-browser threats unless an attacker drops traditional malware onto the endpoint.

So what tool is best to close the gap and add new layers to your security perimeter?

SOURCES

⁴CSO Online⁵CNBC⁶Forbes

What Are Enterprise Browsers?

Enterprise Browsers are deployed as a standalone, specialized solution that replaces popular browsers like Google Chrome to control web activities. In practice, they act as policy enforcement tools, designed to prevent data loss and control the access to the corporate environment.

✓ The Good

- **Extend Zero Trust**
Security teams no longer have to rely on endpoint agents, web portals, or VPNs to cover the last mile.
- **Data Loss Prevention**
IT teams can define and enforce security policies to prevent unauthorized data exfiltration through web downloads and clipboard activity.

⚠ The Bad

- **User Friction**
Stopping teams from using familiar browsers disrupts workflows and forces users to adopt new habits, creating resistance.
- **Slow Performance**
Enterprise Browsers may lag behind commercial browsers in security patches and usability updates, leaving gaps in protection and functionality.
- **Compatibility Issues**
Website functionality can break on custom browsers, hindering performance and even delaying critical tasks.
- **Business Exception**
It is impossible to enforce company-wide standards for only using an enterprise browser—especially with BYOD policies.

Make Any Browser You Use Safe For Business with Obsidian Security

While in-browser protection is a needed layer of defense, Enterprise Browsers introduce unique challenges and gaps that security teams must balance before deployment.

Obsidian Security offers an added defensive layer at the browser level without the headache of a new deployment. This lightweight, easy-to-install, and privacy-sensitive browser extension uses less computing power than a single tab and provides immediate value and security by ensuring organizations and people are protected in real-time.

What You Get

Once deployed, your browser of choice will be protected by real-time detection and prevention threat models informed by the largest repository of real-world SaaS breaches. Deeply inspecting website content enables accurate, out-of-the-box detections of common, as well as never-before-seen, AiTM phishing kits without the need to push new updates.

Plus, security teams discover 50% more Shadow GenAI applications on average compared to just relying on email scanning. This added visibility improves the security and management of business data by preventing the usage of unapproved SaaS and AI applications.



Stop Identity-Based Attacks

100% success detecting and blocking phishing kits and AiTM proxy toolsets like Evilginx by deeply inspecting webpage visuals and content paired with custom phishing detection rules that go beyond traditional indicators like IPs, domains, or URL reputation.



Minimize False Positives

Browser attestation enriches activity logs with a unique identifier, attesting if the activity came from a trusted, managed browser; this reduces false positives, identifies additional threats, and aids in incident response.



Manage Shadow AI and SaaS

Create a real-time inventory of every SaaS and AI tool employees are using in your environment and optionally block access to specific applications like ChatGPT. Additionally, see all unknown, high-risk browser plugins or extensions that access browser history, cookies, and other sensitive data.



Broad Support

Support for all versions of Windows, macOS, and Linux, as well as all active versions of Chrome, Firefox, and Edge (v91+) with immediate compatibility for new browser versions.



Secure, High Performance, and Private










Operates in a protected sandbox without system access and does not monitor personal accounts. All analysis occurs locally, and network traffic is not recorded, proxied, or sent to Obsidian.

“After rolling out Obsidian’s browser extension to over 8,000 users, we caught a real phishing attempt almost immediately. This was a great catch, and the whole process has been super easy and smooth for our team.”

Chief Information Security Officer
Global Financial Services & Asset Management Company

Obsidian Security vs Enterprise Browser

Get faster time to value by removing the complexity of deploying an agent or custom browser. Security teams also avoid technical and organizational adoption challenges like user preferences, network tunneling, latency issues, and application problems caused by SSL/TLS certificate pinning.

	 OBSIDIAN	Enterprise Browser
Security Coverage Across Broad Browser-base	 Chrome, Firefox, and Edge	 Standalone browser
Light Friction & Adoption	 No setup or training needed—employees keep using their current browser	 Requires employee training, strict browser controls, and is often skipped on exec and engineer devices due to friction and valid exceptions
No Impact on Performance or Speed	 Use the same browser you prefer with no user impact	 Use more RAM and CPU and webpages may not be compatible
Light IT Maintenance	 The extension automatically updates itself, no experts needed	 Requires ongoing involvement for policy enforcement, updates, provisioning

Shift Left with Browser-Level Protection from Obsidian

While organizations have traditionally defended endpoints, data centers, and cloud infrastructure, critical business operations and sensitive data now flow through hundreds of SaaS applications—accessed through the browser. And, with attackers using AiTM kits to target employees, deploying Obsidian Security alongside tools like email security will provide the best coverage.

[Request a Demo](#)