FAQ - Halo

Dizzion Halo FAQ

What is Dizzion Halo?

Dizzion Halo is a Secure Every Browser (SEB) solution that transforms everyday browsers into enterprise-grade security endpoints. It works silently in the background of the browsers your users already use. Built for ease of adoption, flexibility, visibility, and zero-trust enforcement, Halo secures browser environments without disrupting users or requiring additional applications.

Why do we call it Secure Every Browser and not Secure Enterprise Browser?

The tagline “Secure Every Browser” (SEB) is intentional. While Gartner and vendors like Island, Talon and others use SEB to mean “Secure Enterprise Browser,” Halo emphasizes Every Browser, not just “enterprise.” We focus on securing Chrome, Edge, Firefox, and Safari for all customers, from small & medium businesses to large enterprises. Another reason for using “Secure Every Browser” is to ensure Halo is recognized within the SEB category.

What is behind the name halo?

A halo is a glowing ring of light, often shown around something valuable or sacred - a symbol of protection, safety, and visibility.

- Halo represents a protective shield around every browser.
- It wraps enterprise-grade security around Chrome, Edge, Firefox, and Safari without changing how users work.
- It is a security layer that follows the browser everywhere, safeguarding SaaS, extensions, and data flows.

In short: Halo = a protective layer of security around the browsers people already use and trust.

Key issues addressed by Dizzion Halo

- SaaS & Shadow IT risks – employees install unvetted apps and extensions outside IT control
- Unmanaged extensions – lack of visibility into risky or malicious browser add-ons
- Data leakage & compliance – difficulty protecting sensitive data and meeting SOC 2, HIPAA, and PCI-DSS requirements
- Resource-constrained teams – small IT/security staff need simple, automated protection without added complexity
- Advanced threat gap – existing tools fail to detect zero-day and AI-driven browser attacks.

What functionality does Halo provide?

- Unknown threat detection (zero-day & AI-driven attacks)
- Zero-trust browser security controls
- Browser Extension discovery and risk scoring
- SaaS app visibility and shadow IT control
- Real-time data loss protection (copy/paste, downloads, filtering)
- Centralized policy management and compliance reporting
- Activity monitoring and user behavior visibility
- Cross-browser support (Chrome, Edge, Firefox, Safari)
- Cloud-delivered deployment with SAML, OAuth, and AD integration
- Optional sensor for unmanaged endpoint visibility and deeper policies

Who benefits from using Halo?

- Remote/hybrid staff and contractors, secure every browser (SEB) on any device, including managed and unmanaged (BYOD), reducing risk and simplifying rollout without extra tools.
- CISOs and security teams, stop unknown and zero-day browser threats before damage occurs, closing the gaps traditional tools miss.
- IT managers and CIOs, manage Chrome, Edge, Firefox and Safari from one console with unified policies, extension control, and rapid onboarding to cut overhead.
- Regulated industries (finance, healthcare, legal, SaaS), protect sensitive data and meet compliance (HIPAA, PCI, SOC2).
- SMBs with small IT teams, gain enterprise-level browser security that’s lightweight, automated, and easy to deploy without new infrastructure.
- Companies facing Shadow IT, discover and control risky extensions and SaaS apps to eliminate blind spots and prevent data leaks.

Key Use Cases

- Shadow IT & SaaS Governance – Discover SaaS usage, enforce app policies, control data flows.
- Extension Risk Management – Inventory browser extensions, score risk, block unsafe add-ons.
- BYOD & Unmanaged Devices – Apply security policies on personal or contractor devices.
- Real-Time Threat Detection – Stop phishing, malware, and risky downloads.
- Compliance & DLP – Block copy/paste, uploads, downloads, and hide sensitive information.
- Runs anywhere: as a standalone solution on any device or fully integrated with your DaaS and Cloud PC platforms.

Is Halo a browser, or does it work with an existing browser?

Halo is not a browser; it's a cloud-based security solution that integrates seamlessly with existing browsers. Unlike solutions like Island and Palo Alto, Halo enhances the security of browsers already deployed in your environment, whether in public or private clouds, without switching to a new browser.

Is Halo a standalone product, or is DaaS or Cloud PC required?

Halo is sold standalone as a lightweight Secure Every Browser (SEB) solution; DaaS and/or Cloud PC aren’t required to use Dizzion Halo. So Halo can be standalone and run within Dizzion DaaS or Cloud PC to extend secure access and compliance coverage to browser activity within Virtual Desktops and Apps.

What does the Halo user experience look like?

- Users need not learn a new browser: they can keep Chrome, Edge, Firefox, and Safari. There is no retraining or switching.
- Lightweight browser extension: Halo runs quietly in the background as a browser add-on. Most users won’t notice it unless a risky action is blocked.
- Minimal disruption: Day-to-day browsing feels the same. Policies kick in only when necessary (e.g., a blocked extension, denied upload, or warning page).
- Clear feedback: If a policy is enforced (e.g., blocking a download), users see a short, understandable notification rather than a cryptic error.
- Privacy separation – Admins can scope Halo to only corporate browsing, so personal use remains unaffected on BYOD device.

What does the Halo admin experience look like?

- Fast deployment: the extension can be installed manually from a secure download link (unavailable via public web stores). IT teams can also deploy it through existing tools such as GPO or standard software distribution systems.
- Single pane of glass – Centralized dashboard to configure policies and monitor activity via https://halo.difr.com
- Visibility without noise – Rich telemetry on extensions, SaaS use, and risky events, without overwhelming users with popups

How does the Halo extension work, and what data does it collect?

The Halo extension operates within each browser profile where it’s installed, connecting securely to our platform over a high-performance protocol. As users browse, each URL is seamlessly validated against configuration profiles and categorized to ensure compliance with security policies. Our extension checks every URL against threat protection feeds in real time to detect potential malware or phishing risks. Suppose a site matches a blocked category, is flagged by configuration settings, or is identified as a known malware or phishing source. In that case, Halo protects the user by blocking access to the site. The extension collects minimal, essential data such as URLs visited (for threat validation purposes) and the user's authentication status to enable this protection. This data is managed with strict privacy controls to maintain user confidentiality and compliance with data protection standards.

How do I install the Halo extension?

The Halo extension isn’t available in the public web stores but can be deployed using flexible options tailored to your organization’s needs. Distribution methods include user invites, Group Policy Objects (GPOs) for Windows, and Google Workspace for streamlined Chrome installations. Once deployed, the extension updates automatically, provided your organization's policies allow for auto-updates on Chrome and Edge. New versions are seamlessly installed within a few hours or upon the next browser restart, ensuring continuous protection without manual intervention.

How much network bandwidth is required to support Halo?

The Halo extension is highly efficient and uses minimal bandwidth. Even for intensive users (12-14 hours of browsing daily), it typically transfers only about 50 KB in a 24-hour period—significantly less than the bandwidth required to load a single web page. This ensures that Halo’s protection operates seamlessly without impacting network performance.

Which browsers are supported with Dizzion Halo?

Browser extensions for Google Chrome and Microsoft Edge are available, and Safari and Firefox are available soon.

Which Identity Providers are supported?

Halo supports Microsoft Entra ID, Google Workspace, and Microsoft Active Directory (Classic). Additional SAML2 and OAuth providers, such as Okta and Duo, can be added. Contact Dizzion for more information.

Can Dizzion Halo run in air-gapped or dark site deployments?

Dizzion Halo is a Cloud Service that cannot run within air-gapped deployments. The end-user device must have an internet connection.

Is Dizzion Halo a VDI / DaaS replacement?

No, not really, some Secure Enterprise Browser solutions, like Island, position themselves as VDI replacements — but it’s not that simple. It really comes down to the use case. Suppose customers only need access to SaaS applications. In that case, Dizzion Halo (and solutions like Island) can provide secure access as VDI/DaaS does, but at a lower cost. However, Halo and other SEB solutions are not the right fit for Windows applications since they require a managed Windows runtime. VDI, DaaS, and Cloud PC — collectively known as Virtual Desktops and Apps — provide access to secure Windows and SaaS applications. However, they require infrastructure to stream desktops and apps over a network. In this scenario, the endpoint browser can be secured using a Secure Every Browser solution like Halo.