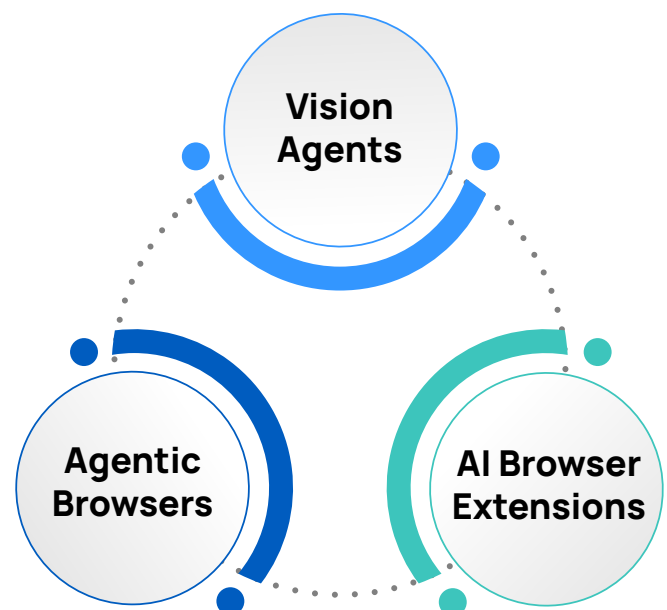# sonet.io

Vision Agents vs. Agentic Browsers vs. Browser Extensions: A Comparison Guide

AI-assisted browsing tools are emerging fast, from agentic browsers that navigate the web autonomously to lightweight AI plug-ins that add automation to existing browsers. Each promises convenience and efficiency, but their security and control models vary widely.
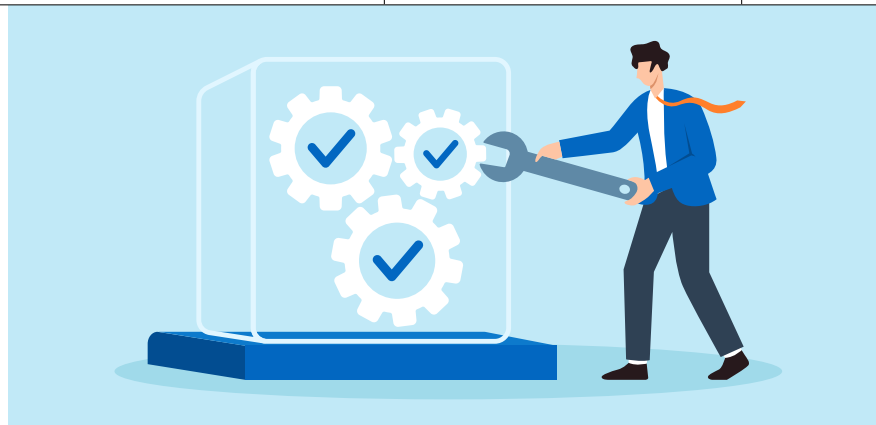
This guide compares three approaches, Vision Agents, Agentic Browsers, and AI Browser Extensions, to help IT and security leaders understand how each handles automation, governance, and enterprise control.

Comparing Three Approaches

Vision Agents

Agentic Browsers

AI Browser Extensions

Architecture and Control

	Vision Agents	Agentic Browsers	AI Browser Extensions
Execution model	Run inside a secure, Sonet-controlled browser workspace and can execute hundreds of Vision Agents in parallel. Workflows run autonomously with full isolation, continuous policy enforcement, and no dependency on local browser resources.	Designed for single-user, human-in-the-loop browsing. Actions typically occur sequentially, and the architecture is not built for large-scale parallel automation.	Built for enhancing an individual user's session inside browsers. Extensions operate within a single browser instance and cannot run large numbers of autonomous agents in parallel.
Control boundary	Fully contained within the enterprise browser workspace, with identity, access, and policy enforcement applied centrally.	Operate outside enterprise management, often using local storage or cloud APIs with user credentials.	Operate locally in the user's browser session, often with minimal isolation from the endpoint or network.
Integration approach	Do not require open internet access. Vision Agents run entirely inside the Sonet-controlled workspace and interact with enterprise applications without exposing sessions to the public web. No APIs or MCPs required, and no outbound access to external sites is required for automation.	Require open internet access to interpret, navigate, and act on websites. Even when restricted to allowed domains, the browser relies on external content, scripts, and page rendering, which increases exposure and risk.	Depends on the host browser's ability to reach external sites. Extensions need internet access to retrieve data, load content, and run automation tasks, and cannot function in a fully restricted or offline environment.

Security and Isolation

	Vision Agents	Agentic Browsers	AI Browser Extensions
Isolation level	Full session isolation within the Sonet workspace. No data touches the endpoint.	Limited isolation. Vulnerable to prompt injection, session hijacking, and token reuse.	Runs in the user's browser context with full access to local cookies, cached data, and sometimes clipboard contents. When active, they are also susceptible to prompt injection and malicious page behaviors.
Data protection	Built-in DLP, watermarking, and clipboard controls applied to all agent sessions. Vision Agents do not require open internet access, so data never leaves the controlled workspace and cannot be exfiltrated through the public web.	No enterprise-grade DLP or session controls. Agents operate on live internet pages and can expose or transmit sensitive data during tasks. Security research shows they can be manipulated into leaking data through prompt injection and malicious page content.	Extensions can access and transmit page content, cookies, cached data, and clipboard information. When active, they have the same data exposure risks seen in agentic browsers.
Credential handling	Uses enterprise SSO for identity and authentication for agent actions.	OAuth tokens often stored in plaintext or without encryption.	May store or transmit user credentials insecurely depending on extension permissions.

Governance and Policy Control

	Vision Agents	Agentic Browsers	AI Browser Extensions
Administrative oversight	Centralized control through enterprise policy. Admins define what apps and actions each Vision Agent can access.	Minimal policy support. Often managed through user-level settings or experimental features.	Controlled at the browser or extension level, with no enterprise policy inheritance.
Identity and access	Integrated with corporate IdPs (Okta and Entra ID). Agents inherit least-privilege policies.	Limited or no SSO integration. Users authenticate directly to external services.	Usually relies on the logged-in browser account, not enterprise identity.
Compliance alignment	Designed for regulated environments where actions must be logged, recorded, and approved. Vision Agents run inside a completely private stack, so critical enterprise data stays contained and does not leak to external services.	Limited or no built-in compliance features. Activity occurs in a consumer-oriented browser that cannot guarantee containment or verifiable session evidence.	No consistent recordkeeping or centralized control. Extensions may send data to third-party services and cannot provide reliable compliance assurance.

Observability and Auditability

	Vision Agents	Agentic Browsers	AI Browser Extensions
Session recording	Every session is recorded with event-level detail, including a step-by-step activity trail with screenshots and the logical steps the agent performed. All evidence is captured inside the private workspace for audit and playback.	No integrated session recording or replay capability. Activity occurs inside a consumer browser with no reliable way to capture actions for review or compliance.	Browser activity may be logged locally but does not include a structured activity trail, screenshots, or agent reasoning steps. No centralized or tamper-proof record is available.
Event visibility	Centralized dashboard for all event logs and sessions. Exportable to SIEM for full traceability.	No standardized telemetry or audit events. Visibility depends on vendor API access.	Minimal observability. Limited to browser console or developer logs.
Incident response	Admins can terminate agent sessions instantly.	No enterprise kill switch or live session control.	No real-time response capability; incidents rely on browser settings.

Enterprise Readiness

|	Vision Agents	Agentic Browsers	AI Browser Extensions
Deployment	SaaS-based. No endpoint software or extensions required.	Requires installing and managing an alternative browser.	Installed manually by users via browser Web Store or local packages.
Scalability	Scales securely across thousands of AI agents with centralized policies.	Lacks centralized management and version control for large deployments.	Difficult to manage across distributed users and versions.
Use cases	Secure automation across Windows, web, and legacy apps.	Consumer research and general web exploration.	Lightweight task automation for individuals.
Maturity	Enterprise-ready with zero trust controls, compliance, and audit.	Early-stage technology with unresolved security and governance challenges.	Mature browser ecosystem, but limited for enterprise-scale AI automation.

The Modern Alternative

For IT and security leaders exploring AI-assisted automation, Sonet Vision Agents provide a secure and governed path forward. Unlike Agentic Browsers or Browser Extensions, Vision Agents operate entirely inside a controlled browser workspace with full session isolation, centralized policy enforcement, and complete observability.

They enable automation across legacy and modern applications while maintaining the same zero trust and compliance standards that protect human users today.

Everything you need, nothing you don't.

- **Secure automation across all applications**
- **Centralized policy and audit visibility**
- **No APIs, no extensions, no new attack surface**
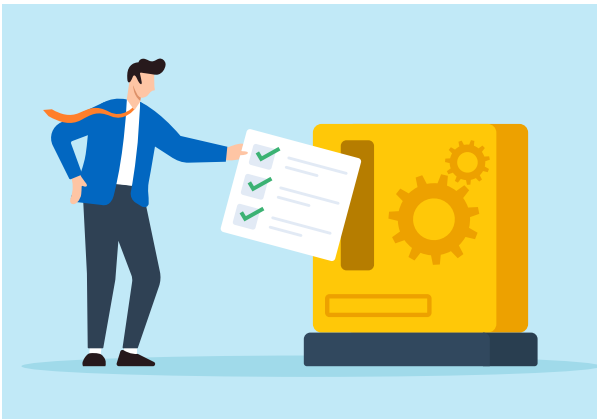
Schedule a Demo:
To see Sonet.io in action.

Talk to Our Team

sonet.io

Secure Workspaces for Humans and AI

sales@sonet.io

Find us online at **sonet.io**

3031 Tisch Way, 110 Plaza West
San Jose, CA 95128