An enterprise browser as a VDI alternative for browser-based work

For browser-based and SaaS work, an enterprise browser can stand in for VDI. Here's where Island Browser fits for MSP clients, and where a desktop still fits.

November 2026 | Jason Makevich, CISSP

For browser-based and SaaS work, an enterprise browser can stand in for VDI: Island presents Island Browser as an alternative to VDI that runs locally, with no brokers, servers or extra infrastructure. Apps that still need a full desktop can stay on a virtual desktop, reached through Island Browser's built-in RDP. Island Browser is part of Island for MSPs.

Can an enterprise browser replace VDI for browser-based work?

Yes, for work that happens in web and SaaS apps: Island Browser installs locally, takes its policy from Island's cloud console and gives people the apps they're authorized for, with no virtual desktop to set up. Island notes that Island Browser isn't a desktop virtualization platform, so the fit is browser work rather than full desktops.

Whichever way a client delivers remote work, NIST's guidance says every part of a remote access setup, including BYOD client devices, should be secured against expected threats identified through threat models. See NIST SP 800-46 Rev. 2.

What does Island Browser cover in place of VDI?

For browser-based work, Island Browser covers access, data protection and visibility in the browser itself.

- **Access from personal devices.** People install Island Browser, sign in with their work identity and get the apps they're authorized for, with no agents or MDM.
- **Data protection.** Island's last-mile controls cover copy and paste, downloads, printing and screenshots, and Island can redirect downloads to secure cloud storage, add watermarks and redact sensitive data on screen.
- **Visibility.** Island records work activity in detail for audits and incident response, and it can send that activity to SIEM and analytics platforms.
- **Compatibility.** Web apps that work in Chrome or Edge should generally work in Island Browser without compatibility testing, and IE Legacy Mode supports older web apps.

When do clients still need a virtual desktop?

Clients still need a virtual desktop for apps that don't run in a browser, and Island Browser supports RDP natively so people can reach those desktops from the same work browser. An Island Browser license includes built-in RDP, SSH and SMB clients, so the same work browser can reach remote desktops, servers and file shares.

How do people reach apps that need a full desktop?

People reach those apps through Island Browser's built-in RDP client, inside the same managed browser as their web apps. For private apps behind the client's firewall, the Island Private Access (IPA) add-on gives zero trust access without a VPN for those apps, through connectors that connect outbound to Island.

What do users notice when they move off VDI?

Users work in a local browser instead of a remote desktop: Island Browser installs locally and takes its policy from Island's cloud console. As of November 2026, Island lists Island Browser for computers, phones and tablets, so the same approach works across the devices people already have. It includes productivity tools such as a smart clipboard and an ad and tracker blocker, and its interface can carry the organization's branding, messages and notifications. On personal devices, personal browsing stays private while policy applies to work apps and sites.

How does Island Browser keep work files under control?

Island can redirect downloads to secure cloud storage, and an Island Browser license includes secure cloud storage for work files. Island's data protection is based on context, so data can move between approved work apps while leaks are blocked, for example allowing a paste into Salesforce but not into personal email.

What does this mean for contractors and remote teams?

Contractors install Island Browser on their own device and see only the apps they're provisioned for, without shipped laptops, imaging or virtual desktops. Access can change with context such as role, contractor status or project duration, and it's removed in one place when someone leaves.

See how MSPs give contractors secure access to client apps and how MSPs secure BYOD and unmanaged devices.

What does this look like for Island's customers?

Island's customer story says Eftsure, a B2B payment fraud prevention firm, saves more than $200,000 a year by replacing VDI with Island Browser and ended two-second delays that had slowed its fraud detection work. Island's customer story says Sonar, a software company of about 500 employees, decided against building a VDI environment and made Island Browser the required browser for its internal tools. Island also reports that Sonar no longer ships laptops to short-term and remote users.

Island's customer story says Landis+Gyr, a Swiss energy technology manufacturer, uses Island to give about 400 third-party contractors controlled access and eliminated two VDI platforms.

Where do the Island Extension and IslandOS fit?

On company-owned, managed computers, the Island Extension brings Island's controls into the browsers people already use. For company-owned computers where the work happens in Island, IslandOS runs Island Browser as the primary workspace on Scylos ZeroCore, and it fits SaaS-heavy users and aging Windows computers.

How do MSPs test it with a client?

An Island pilot can start with 1 to 5 users, and PORT1 helps set up the tenant, single sign-on, starter policies and a success checklist, then reviews the results with the partner. Partners get PORTER, PORT1's partner platform, for help along the way. For a move off VDI, the natural pilot group is users whose work is mostly in web and SaaS apps. See Island Browser for everything that's included.

Sources

- NIST SP 800-46 Rev. 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, NIST, July 2016

Book an Island demo