MENLO SECURITY

SOLUTION BRIEF

Modernize Virtual Desktop Infrastructure (VDI) with Menlo Secure Application Access

Address Workforce Accessibility Concerns While Reducing Cost

The Needs of the Modern Workforce

In today's world, organizations need to provide access to applications for a variety of individuals, remote employees, short-term contractors, and others. These employees and third parties need safe and reliable access to applications no matter where they choose to work. However, security and IT teams also need to make sure that the sensitive data used within these applications does not get into the wrong hands or onto untrusted devices. To be truly effective, security for the modern workforce must be:

- **Scalable:** Organizations need to be able to support rapid changes in user traffic, regardless of location
- **Zero trust:** Technology architecture needs to be set up to ensure that the pitfalls of legacy detect-and-response tools don't result in a successful attack
- **Converged:** Solution capabilities need to support multiple security needs, including email and web, and offer last-mile DLP capabilities
- **High performance:** Security and IT teams need to ensure that an application access solution delivers a seamless user experience

The Disadvantages of VDI for the Modern Workforce

Remote desktops, thin-client computing, and VDI changed the way businesses operated in the 1990s and 2000s. VDI offered advantages over traditional workstations and desktop hardware, offering improved security, flexibility, and cost savings, because it allowed many employees to use less expensive machines to do their work. VDI helped support remote workers due to the fact that it could substitute or complement remote access VPNs and provide a virtualized work environment.

However, as browser-based applications have proliferated, VDI no longer provides these advantages, while its drawbacks have become increasingly obvious. Even so, many organizations still use VDI systems, compelling security and IT teams to voice their frustrations and prompting a shift to a more advanced, flexible, and cost-effective approach.

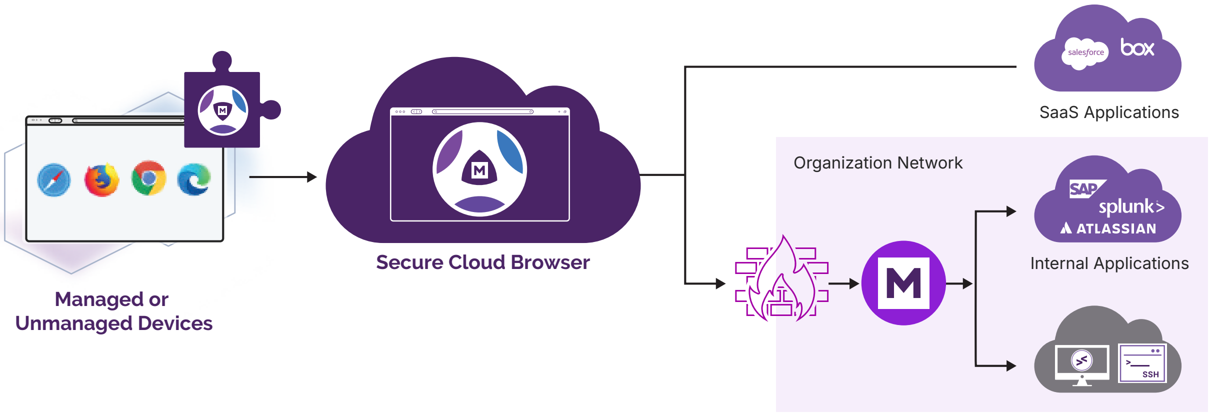
VDI Disadvantages

- **Costly and resource intensive:** VDI requires a large upfront investment and ongoing costs, reported to be between $1,000 and $4,000 per user. Along with the high license cost, there are expenses for hardware, software, storage, computing resources, bandwidth, and ongoing maintenance.
- **High complexity:** VDI deployment involves many different components, making troubleshooting and upkeep difficult and complex.
- **Security concerns:** VDI has been the target of attacks on public-facing servers, and has provided a mechanism for threat actors to move laterally within organizations. While the protocols have matured and now utilize modern authentication and transport security, these servers are just one more system that needs to be patched and monitored for threat activity. Highly evasive threats have used VDI systems to establish a persistent presence and execute a breach.
- **Poor user experience:** The user experience associated with VDI can be suboptimal, depending on the remote location, endpoint resources, and network connectivity.

Menlo Secure Application Access

Menlo Secure Application Access makes zero trust access easy, offering a more cost-effective and secure path to applications.

Menlo Secure Application Access provides employees and contractors with secure connectivity to private applications, including both web and legacy applications. At the core of Secure Application Access is the Menlo Secure Cloud Browser, which is positioned between the user’s endpoint and internal apps and data. This positioning helps shield the applications from parameter tampering, web scraping, API abuse, and a host of other problems not addressed by VDI.



Instead of directly accessing applications, users safely access a rendering of their applications in a portal or through an extension.

Menlo Secure Application Access enables organizations to apply zero trust principles to application access with:

- Protection against malicious users
- Access based on user/group, source IP, and location
- Posture check
- Inspection and blocking of uploads

Secure Application Access enables organizations to secure data with fine-grained, last-mile DLP controls. These controls enable security and IT teams to provide application access to partners, contractors, and remote workers, without the worry of data leakage. These controls include:

- Read-only/read-write, upload/download, and copy/paste controls
- DLP restrictions for uploads and downloads
- Watermarking
- Data redaction

Secure Application Access enables organizations to reduce costs with flexible and easy deployment options. Instead of the significant cost of VDI, organizations can enable secure access from any browser on any device, with:

- A clientless and zero-touch deployment for browser-based applications
- An easy-to-use management console for configuring and monitoring all applications
- A simplified yet secure architecture that reduces latency and cost

Benefits

Robust security benefits, protecting applications from infected endpoints.

Easy to deploy, monitor, and configure.

5–10X reduction in costs.

Simplify Zero Trust Access

As organizations navigate the changing landscape of VDI, it's clear that traditional approaches no longer suit the needs of the modern workforce. Menlo Security enables organizations to secure their applications and secure their data while reducing cost.

With our zero trust approach to securing access to applications, Menlo Security helps organizations ensure that users and data are safeguarded, while delivering a seamless user experience.

To learn more about securing the ways people work, visit menlosecurity.com or email us at ask@menlosecurity.com.

About Menlo Security

Menlo Security eliminates evasive threats and protects productivity with the Menlo Secure Cloud Browser. Menlo delivers on the promise of cloud-based security—enabling zero trust access that is simple to deploy. The Menlo Secure Cloud Browser prevents attacks and makes cyber defenses invisible to end users while they work online, reducing the operational burden on security teams.

Menlo protects your users and secures access to applications, providing a complete enterprise browser solution. With Menlo, you can deploy browser security policies in a single click, secure SaaS and private application access, and protect enterprise data down to the last mile. Secure your digital transformation with trusted and proven cyber defenses, on any browser.

Work without worry and move business forward with Menlo Security. © 2025 Menlo Security, All Rights Reserved.

MENLO SECURITY

Learn more: https://www.menlosecurity.com
Contact us: ask@menlosecurity.com