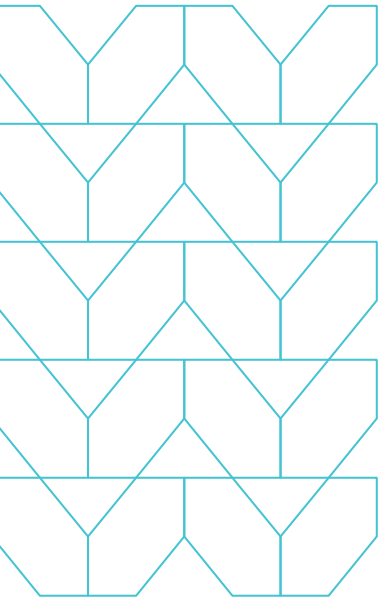
MENLO SECURITY

Modernize Virtual Desktop Infrastructure (VDI) with Secure Enterprise Browser Solution

Menlo Security offers a more efficient and secure solution, enabling organizations to address workforce accessibility concerns while reducing cost.

Solution Brief

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 do 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 detect and respond don't result in a successful attack
- **Converged:** Solution capabilities need to support multiple security needs, including email, web, and DLP
- **High performance:** Security and IT teams need to ensure that security delivers a seamless user experience

The disadvantages of VDI with the modern workforce

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

However, as browser-based applications became increasingly popular, VDI no longer provided these advantages. While many organizations still use VDI systems, security and IT teams have voiced their frustrations, propelling a shift to more advanced, flexible, and cost-effective approaches.

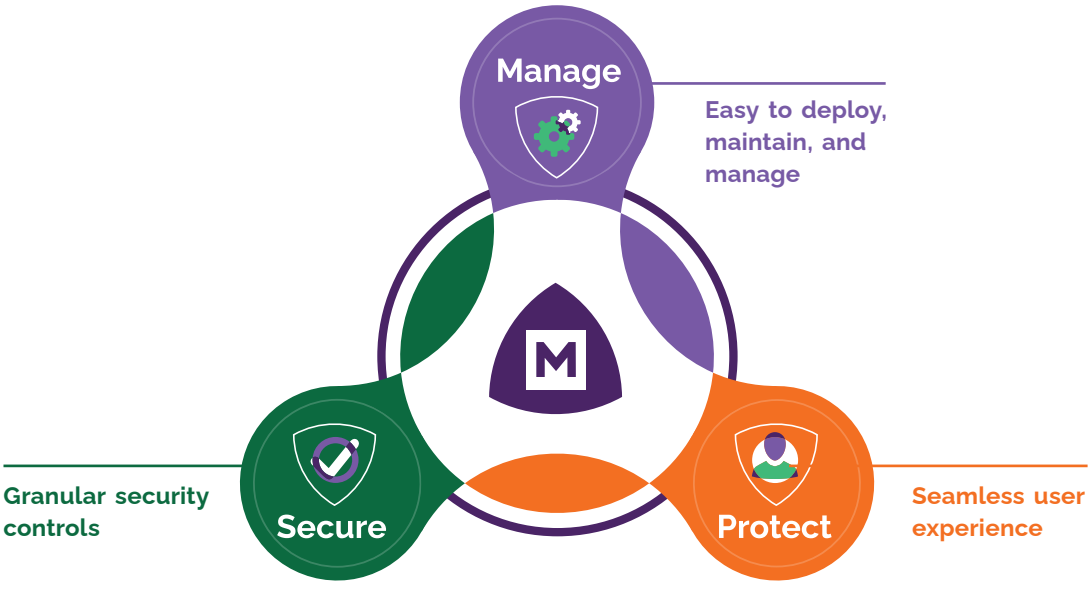
The disadvantages of VDI with the modern workforce:

- **Costly and resource intensive:** VDI requires a large upfront investment, reported to be between $1,000 to $4,000[1] per user. Along with the high license cost, there are expenses for hardware, software, storage, computing resources, bandwidth, and ongoing maintenance.
- **Complexity:** VDI deployment involves many different components, making troubleshooting and upkeep harder and more 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 utilized 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 poor, depending on the remote location, endpoint resources, and network connectivity. Often, these issues are difficult to resolve.

[1] Source: https://www.networkcomputing.com/data-centers/calculating-true-cost-vdi

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 web applications and legacy applications. At the core of Secure Application Access is the Menlo Secure Cloud Browser, which fetches and delivers the content to users. This helps shield the applications from parameter tampering, web scraping, API abuse, and a host of other problems not addressed by VDI.

Secure Application Access enables organizations to secure applications with:

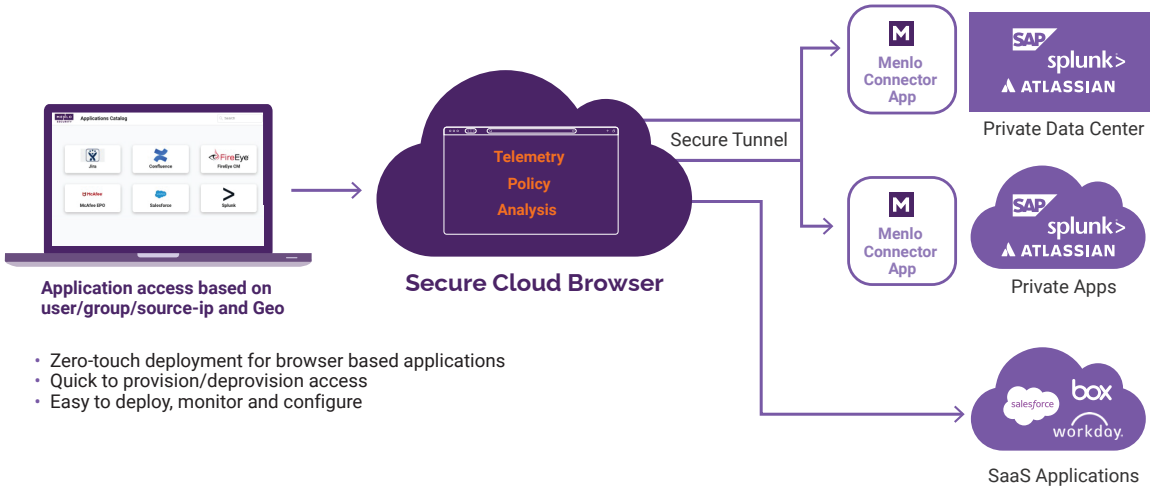
- Protection against malicious users
- Access based on user/group, source IP, and location
- Posture check
- Inspection and blocking of uploads

Secure Application Access enables organizations to secure data with granular DLP controls. These controls enable security and IT teams to provide application access to contractors without the worry of data leakage, and they include:

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

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

- A clientless and zero-touch deployment for browser-based applications
- One pane for configuring and monitoring all your applications
- Easy provisioning and deprovisioning of applications to users



Menlo Secure Application Access provides employees and contractors with secure connectivity to private applications, including web applications and legacy applications. At the core of Secure Application Access is the Menlo Secure Cloud Browser, which fetches and delivers the content to users. This helps shield the applications from parameter tampering, web scraping, API abuse, and a host of other problems not addressed by VDI.

Benefits

Granular security benefits, protecting applications from infected endpoints

Easy to deploy, monitor, and configure

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 the Zero Trust approach from Menlo Security to securing access to applications, organizations can ensure 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.

MENLO SECURITY

To find out more, contact us:

menlosecurity.com

(650) 695-0695

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.

© 2024 Menlo Security, All Rights Reserved.