ZERO TRUST ACCESS

BYOD SECURITY

VDI REDUCTION

VPN REPLACEMENT

Menlo Secure Application Access

Accelerate Zero Trust Initiatives as You Protect Mission-Critical Applications and Data

Legacy network-based application access technologies are clearly aging in the face of major trends in IT consumption, as illustrated by the realities facing today's enterprises:

- The need for zero trust in light of dramatic workplace changes following the pandemic
- The fact that legacy technologies like VPNs and VDI often deliver poor user experiences, limit security visibility into traffic, and can be cumbersome to deploy on unmanaged devices
- The fast pace of application migration to web-based access has made the web browser the primary access technology
- The increasing sophistication of web-borne threats, which leverage AI and DevOps methods to morph and spread rapidly

Menlo Secure Application Access provides policy-driven access to internal and web-based applications and data for managed and unmanaged devices. Permitted applications and websites are presented in user-friendly tiles or lists via a web portal or browser extension. Legacy, non-web-based apps can be accessed via a client, which offers additional access and security controls. Secure access to internal and internet web properties is assured by the Menlo Secure Cloud Browser. Instead of directly accessing enterprise or SaaS applications, users connect through the Secure Cloud Browser. This prevents compromised endpoints from attempting data exfiltration from enterprise applications, and prevents malicious content from a compromised server from exploiting the endpoint.

SOLUTION BRIEF

Zero Trust Access

Your Challenges

First, consider the core principles of zero trust, which include:

- User and device verification and authentication
- Least-privileged access
- Continuous monitoring and re-verification

As digital transformation progressed, more applications moved to the cloud, hybrid work became the norm, and zero trust **network** access (ZTNA) became the security standard. But today, zero trust principles mandate that nothing be trusted—regardless of location—with the focus on granting user access only to the applications users require. ZTNA has evolved to zero trust access (ZTA).

In fact, some zero trust offerings completely fail to secure the web browser, which has become the primary mechanism for accessing the applications most users need to do their jobs.

The Menlo Solution

Unlike other zero trust access offerings on the market, Menlo Secure Application Access is easy to deploy, easy to manage, and is delivered through an easy-to-use management console. Menlo Secure Application Access, combined with the Menlo Secure Cloud Browser, provides comprehensive zero trust access, with the following capabilities:

- Internal applications can be hidden, with access to them granted on a least-privileged basis
- Least-privileged access permissions are limited by user, group, location, and application, with controls that are specific to each application
- All web requests are executed in the Secure Cloud Browser, isolating web servers and browsers from threats and minimizing attack surfaces
- Bidirectional last-mile data loss prevention (DLP) can detect sensitive data and block downloads from internal applications as well as block uploads to the internet
- Internal applications can be secured from attacks from unmanaged devices; users of such devices can be prevented from uploading potentially infected files
- Intuitive, centralized management reduces the management burden

ZTNA design and deployment can be complex, with many offerings on the market requiring some form of heavyweight client, complex network changes, or both. In contrast, Menlo Secure Application Access can be delivered with zero-touch deployment simply by providing a URL, username, and password to users.

Secure Access for BYOD Users

Your Challenges

Zero trust requires validation of processes and methods, including those required for authentication, verification, and data protection. Many such methods require heavyweight clients, which must be installed and configured on the endpoint. This can be difficult or impossible in user groups that include:

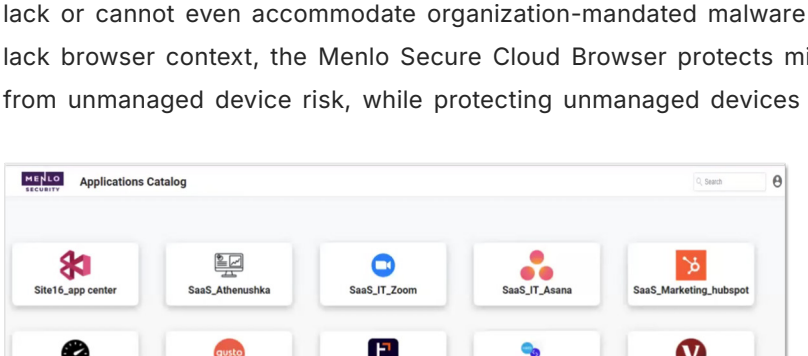
- Contractors and partners
- Users associated with mergers and acquisitions
- Employees who are permitted to bring their own device (BYOD)

Often, business needs require users in these groups to access internal web-based applications, such as SAP, Oracle, or Confluence, as well as managed and secured public SaaS applications, like Salesforce. Access to such resources must be controlled and secured to prevent data loss.

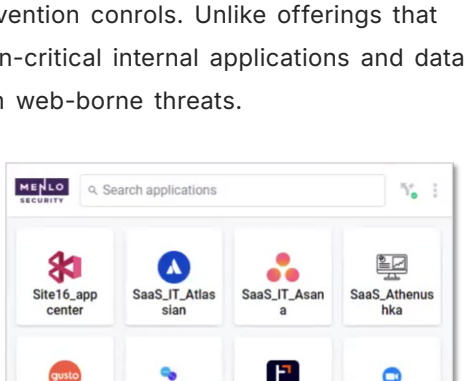
The Menlo Solution

Secure Application Access enables organizations to extend zero trust access to unmanaged users and devices quickly and easily, with access only to specified applications. Unlike most offerings on the market, which require client deployment, network configuration, or infrastructure changes, Menlo offers a fully zero-touch deployment method, requiring only a URL, username, and password.

All Secure Application Access methods direct web traffic through the Menlo Secure Cloud Browser. Unmanaged devices carry a higher risk of data loss, as they usually lack organizational data protection controls. Menlo Last-Mile DLP can prevent data loss from internal web apps, and reduce the risk of exfiltration from unmanaged devices. Further, internal applications risk infection from unmanaged devices, which often lack or cannot even accommodate organization-mandated malware prevention conrols. Unlike offerings that lack browser context, the Menlo Secure Cloud Browser protects mission-critical internal applications and data from unmanaged device risk, while protecting unmanaged devices from web-borne threats.



Zero-Touch Application Access
Menlo Web Portal



Single-Touch Application Access
Menlo Enterprise Extension

VDI Reduction

Your Challenges

Virtual Desktop Infrastructure (VDI) emerged as an approach leveraging virtualization to reduce desktop costs. VDI vendors developed protocols to deliver desktop sessions over the LAN. Arguably, VDI tools were not originally intended for remote work, even if VDI protocols offered encryption. VDI solutions generally do not offer integrated VPN capabilities to secure remote access, so IT teams rely on VPNs to secure VDI access. Moving VDI LAN-friendly protocols to the WAN and pushing them through VPNs tends to deliver a poor end-user experience.

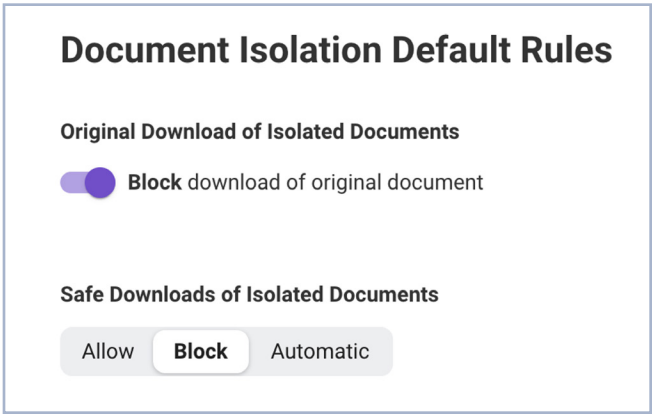
Other VDI disadvantages include:

- High deployment cost, reported to be well over $1000/user
- Complexity, due to the fact that VDI requires many infrastructure components and associated software, complicating support and troubleshooting
- VDI's method of converting web pages to pixels, then transporting them via RDP, HDX, or another proprietary VDI protocol, which requires open firewall ports, is outdated and inefficient when compared to HTTP/S and HTML
- Poor remote user experience, due to the fact that VDI protocols were not designed for the higher-latency environments presented by remote work

The Menlo Solution

Many apps served by VDI have evolved to web access. With Menlo Secure Application Access, you can replace VDI instances with secure web usage for managed and unmanaged devices.

A risk scenario illustrates the benefit of browser security relative to VDI.



File and Archive Security
Note that all downloads to endpoint can be disabled

In the first scenario, a user starts a VDI session. An email arrives with a link to a password-protected file and its password, along with the message, *It's the contract we need to get signed.* The user clicks the link and the file downloads; unbeknownst to the user, the file is infected. The user double-clicks on the file and enters the password, infecting the user's VDI instance. Because internal network traffic is assumed safe, the malware is free to roam the enterprise network.

In the second scenario, VDI is replaced with Menlo Security, which protects browser sessions. An email arrives with a link to a password-protected file and its password, along with the message, *It's the contract we need to get signed*. Once again, the user clicks the link. Menlo protects the user and the enterprise in one of two ways:

- The suspicious website hosting the malicious file is blocked. There is no download.
- If the website is permitted, the file is downloaded to the Menlo Secure Cloud Browser, which prompts the user for the password. The malware in the file is identified, and the download is blocked.

Migrating web apps from VDI to Menlo Secure Application Access delivers a secure and enhanced user experience, especially for remote users, combined with the potential for significantly reduced costs.

VPN Replacement and the Evolution to Zero Trust Access

Your Challenges

- VPNs can't deliver least-privileged zero trust, as they typically give users access to a broad network segment with many applications.
- VPN vulnerabilities, because they provide network-level access and are exposed to the internet, can create unacceptable risk.
- The very nature of encrypted VPN communications prevents the session visibility needed for reporting, auditing, breach investigations, and forensics.
- It can be extremely difficult to add guests, such as contractors or even team members from an acquired organization, particularly if MFA is required. VPN clients can be difficult to install on unmanaged devices due to interoperability challenges. And, while MFA has modernized toward mobile apps rather than hardware tokens, the latter is still common in many organizations, adding to the distribution challenge.

The Menlo Solution

- Rather than opening a full network or network segment, Secure Application Access can remove enterprise web servers from the DMZ, and embed them in their own network microsegments
- In contrast to VPNs, which lack browser context, Secure Application Access includes web usage controls, such as copy/paste limitations and last-mile DLP features, including watermarking and data redaction
- Unlike wire encryption provided by VPNs, all Secure Application Access user traffic can be logged and recorded with Menlo Browsing Forensics; advancing from VPN to a solution offering browser context enables faster incident analysis and response
- Like VPN clients, the Menlo Security Client offers device posture checks
- Unlike VPN clients, only permitted applications are visible in the Menlo Security Client

SSN	GENDER	BIRTH DATE
172-32-1176	M	1958/04/21
514-14-8905	F	1944/12/22
213-46-8915	F	1958/04/21
524-02-7657	M	1962/03/25
489-36-8350	M	1964/09/06
514-30-2668	F	1986/05/27
505-88-5714	F	1963/09/23
690-05-5315	M	1969/10/02

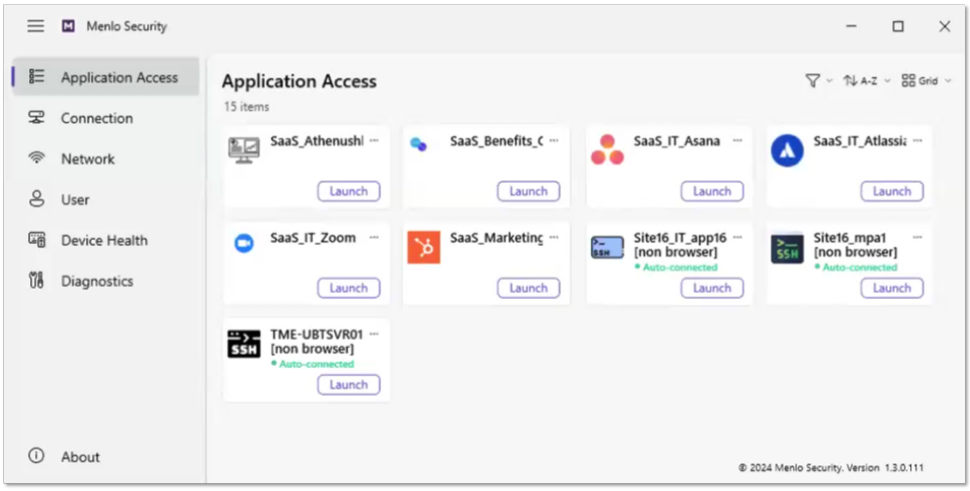
Visible Social Security Numbers

SSN	GENDER	BIRTH DATE	MAIDE
XXX-XX-XXXX	M	1958/04/21	Sr
XXX-XX-XXXX	F	1944/12/22	Am
XXX-XX-XXXX	F	1958/04/21	Pir
XXX-XX-XXXX	M	1962/03/25	H
XXX-XX-XXXX	M	1964/09/06	Po
XXX-XX-XXXX	F	1986/05/27	Nich

Redacted Social Security Numbers

SOLUTION BRIEF

Menlo Secure Application Access

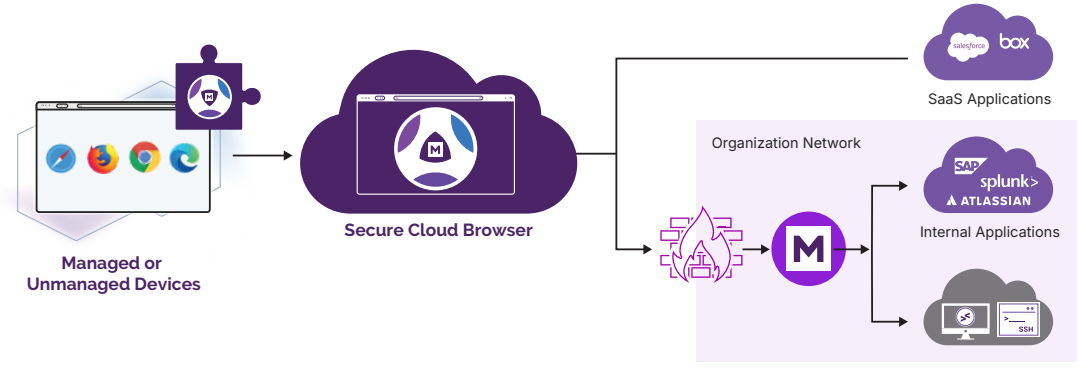


Menlo Security Client showing permitted applications

Simplify and Accelerate Zero Trust Access

With users spending most of their day using web browsers, organizations need a secure access solution that works on managed and unmanaged devices, as well as on any web browser. Menlo Secure Application Access is a modern solution that can replace cumbersome and dated VDI and VPN infrastructure. Secure Application Access speeds zero trust rollouts, while providing security for users with unmanaged devices.

Find out more at menlosecurity.com/saa



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.

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