MENLO SECURITY

A Modern VPN Alternative for Secure Application Access

Overcome the limitations of Virtual Private Networks (VPNs) with Menlo Secure Application Access.

Solution Brief

In the past, secure remote access was required for off hours work and mobile users. Today, hybrid access and zero trust access are how we work. Remote access used to focus on enabling an email client to connect with a server through a Virtual Private Network (VPN) gateway. Many VPN gateways have been left behind because of the complexity, costs and recognition of the security risks that they cannot close. And users need access to all the applications they use while working–not just email.

Digital transformation and the rise of Software as a Service (SaaS) platforms has accelerated, as this new hybrid working model has evolved. Users, applications, data and endpoints are connected across the Internet and not necessarily private network infrastructure. VPN gateways offer little value in this model. Cloud VPNs and costly cloud-network services simply move the old "connect networks" model to the cloud. Supporting secure application access and enforcing zero trust policy enforcement can be dramatically improved with a modern approach.

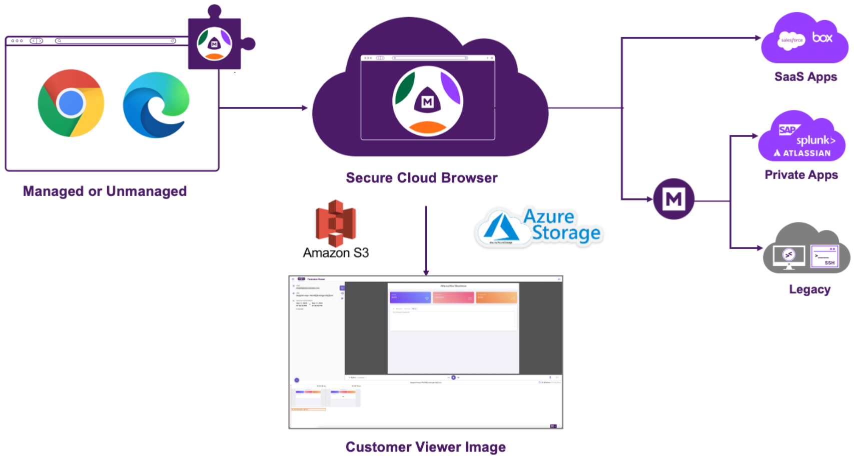
It has been years since the global pandemic laid bare the limitations of decades-old VPN technology. The massive expansion of utilization created scalability challenges which led to traffic bottlenecks. The resulting congestion at gateways led to latency and lag, causing poor user experiences. In addition, the quick shift to remote work forced some organizations to put certain critical applications on the internet in order to make them accessible to employees. Throwing applications into the DMZ was a risky move. While this made it possible for employees to access the applications necessary for their job functions, it also significantly increased the attack surface.

In addition, VPNs connect users to the entire network, rather than a specific application. In the absence of multi-factor authentication (MFA), which unfortunately continues to be common, a threat actor able to breach the VPN by stealing a users' credentials through a well-executed phishing campaign would then have what they need to access any business system without having to go through another authorization process. This is exactly the case for the Colonial Pipeline Co. ransomware attack. In May 2022, DarkSide, a hacker group, gained access to Colonial Pipeline's network through a compromised VPN password. They then used their access privileges to move laterally across the network's infrastructure to steal data and infected the company's network with ransomware. While Multi-Factor Authentication (MFA) would have been able to stop this attack, MFA can be circumvented, as we've seen with some recent attacks like MFA bypass. Additionally, due to the internet facing nature of VPNs, there are a consistent and primary target of threats.

Some VPNs have vulnerabilities beyond the general risk of extending network access when users really want applications access. Just in the first several months of 2024, Ivanti has had to disclose five major vulnerabilities in its Connect Secure VPN devices (CVE-2023-56805, CVE-2024-21887, CVE-2024-21893, CVE-2024-21888, CVE-2024-22024). Three of those vulnerabilities are actively being exploited, according to multiple threat intelligence sources, and, once breached, these vulnerabilities give threat actors unfettered access to entire corporate networks – including critical finance, HR and engineering systems. In addition, the encrypted nature of VPNs includes a lack of visibility into user's actions.

It's time for a modern solution

Security teams and enterprise architects have been searching for a VPN replacement. Many candidate solutions have proven to be complex, expensive, and have even introduced risk. Some approaches have provisioned access and elements of security, such as authentication and authorization, but they have degraded visibility. Secure Application Access from Menlo Security delivers simple, efficient and cost-effective secure access and zero trust policy enforcement.



Menlo Secure Application Access + Browsing Forensics

Menlo Secure Application Access combined with Menlo Browsing Forensics delivers secure remote access whiie preserving visibility into user sessions and transactions. Menlo Secure Application Access presents a dashboard of authorized applications to each user. Rather than opening up a network, Menlo provides application-by-application access and preserves network separation. Browsing Forensics enables visibility into TLS-encrypted web apps without the complexity or transport security tradeoffs of network-oriented approaches.

The combination of Secure Application Access and Browsing Forensics enables users to work anywhere with ease and within the constraints of a zero trust policy. Every user session retains the visibility required for incident response and compliance. Users simply launch applications from a dashboard that is delivered via a portal or a within browser extension.

Menlo Secure Application Access safeguards applications by using the Menlo Secure Cloud Browser to communicate with applications. Rather than accessing the origin server, users interact with the Menlo Secure Cloud Browser. The remote browser creates a rendered representation of the application and delivers content to the endpoint device within the user's local browser. In addition to providing access, the combination of the local browser and the cloud browser shields users from content-based attacks. The architecture also shields the application from malicious requests that might involve parameter tampering, web scraping, API abuse, and a host of other problems, because network separation is preserved and all requests are inspected by the AI-driven protections within the Menlo Cloud. Even in the event of endpoint compromise,, a threat actor cannot get direct access to issue requests to the server. All application requests are executed from the Menlo Secure Cloud Browser rather than the endpoint browser. To help protect against browser vulnerabilities, Menlo Secure Application Access:

- Enables organizations to hide applications from the internet while providing authorized access
- Provides access to a specific application, not to the network. In addition to protecting applications, such controls thwart lateral movement
- Prevents attacks based on unauthorized access
- Prevents attacks from protocol manipulation, session hijacking & cookie stealing

Further, Menlo Secure Application Access provides Sandboxing and AV Scanning for all content shared between the user and the application. In the event of a user uploading an infected file, Menlo Secure Application Access stops the file from infecting the application and other potential malicious activity.

To provide comprehensive protection for the valuable data these applications hold, Menlo Secure Application Access has additional layers of data security controls. These controls, which can be used to help with compliance, data leakage prevention, and more, include:

- Download/upload controls
- Read-only/read-write policies
- Watermarking of applications and documents
- Data redaction
- Copy/paste controls

The simplified architecture of Secure Application Access combined with Browser Forensics offers reduced time to deployment, improved security, and a better experience for both end users, admins, and infrastructure/network teams.

While a continuously increasing number of applications are being accessed via the browser, organizations might have legacy applications that still need to be accessed. To provide secure access to both browser and non-browser based applications, Menlo Security offers flexible deployment options.

The Menlo Security Client is available for legacy client-server applications, enabling access for end users while the organization works to migrate towards a modern application architecture.

Menlo Browsing Forensics delivers another groundbreaking attribute – visibility - including screen captures, user inputs and more. This visibility is particularly important when considering third party users, such as partners or contractors, or those involved in merger/acquisition activities. Security teams can leverage the information captured by Browsing Forensics to ensure access control models are being enforced, applications are being used appropriately and to monitor the activities of higher risk users, such as those on a watch list. Browsing Forensics efficiently provides that deep level of insight without any ambiguity.

With the combination of Secure Application Access and Browsing Forensics, enterprises can replace their VPNs while ensuring that employees and third parties can access only the content that they need while ensuring complete visibility of actions during the session.

Key Benefits

- Provide access to specific apps versus the entire network.
- Last-mile data protection including download/upload, read-only/read-write and copy/paste controls plus watermarking and data redaction
- Capture user sessions to validate that compliance requirements are being enforced, such as restricting access to applications to defined users and groups and adherence to data controls.
- Resolve security incidents quickly, with visibility of browser-based actions from which security analysts can derive intent.
- Quickly provision and deprovision access to applications without changing network topology or firewall rules.
- Zero touch and agentless deployment for browser-based applications and an agent for non browser-based applications.
- Leverage information you can use, not data you have to parse. Browsing Forensics automatically preserves a comprehensive record of web sessions and user interactions. Security analysts can now access the complete history of any browser session.

Traditional VPN infrastructure allowed organizations to keep operations running during the global pandemic, but also served to highlight new and ongoing security concerns and performance issues around this decades-old technology. Organizations need a simpler, more secure alternative. Menlo Secure Application Access and Browsing Forensics delivers the right solution given today's dispersed workforce.

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.