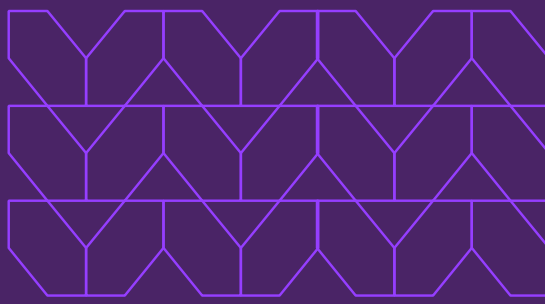
MENLO SECURITY

Data Sheet

Enable seamless access to enterpise applications for employees or third parties without compromising security

Menlo Private Access (MPA) leverages an elastic Isolation Core™ to grant safe access to an enterprise's private or cloud applications without requiring VPN clients or other agents.

The new normal has spread users, devices, applications, and data away from a centralized data center and out to thousands of distributed locations, including remote offices, factory floors, worksites, dining room tables, and coffee shops across the globe. The move to the cloud has mitigated many of the challenges associated with expanding accessibility, but an enterprise's private and SaaS applications presents a different challenge. How can organizations provide distributed employees and third parties with the unhindered access to internal web apps, data, and other enterprise resources they need to do their jobs without severely expanding the surface area for attackers to target?



Three things to know:

Organizations struggle to secure access for employees and third parties to web, SaaS, and private applications, especially with today's remote workforce.

A Zero Trust approach applies the principles of "never trust, always verify" and eschews the legacy approach of being overly permissive, which can give attackers or malicious insiders access to things that need to be protected.

Menlo Private Access (MPA) enables organizations to deploy Zero Trust Network Access (ZTNA) across their entire user base, making it easy to access private and SaaS applications while ensuring the highest level of security using Menlo's Isolation Core™.

An isolation-based approach to application access

A new approach to network security is needed to overcome the critical flaws of legacy web app security tools and the common exploits of attackers. This new approach must be rooted in Zero Trust, the notion that a user is not trusted unless their identity is extensively verified. This can be done effectively and efficiently through cloud-delivered security services.

Menlo Private Access (MPA) provides fast, seamless access to enterprise applications isolating all traffic to and from private web applications. Rather than accessing the original application, Menlo Private Access leverages reverse isolation capabilities to create a rendered image of the application on the endpoint device directly in the user's browser. As a result, Menlo's Isolation Core™ shields the application from parameter tampering, web scraping, API abuse, and a host of other problems not addressed by other Zero Trust Network Access (ZTNA) solutions.

Menlo Private Access provides additional security controls, e.g., read-only/download/upload controls, AV/sandboxing, and DLP scanning.

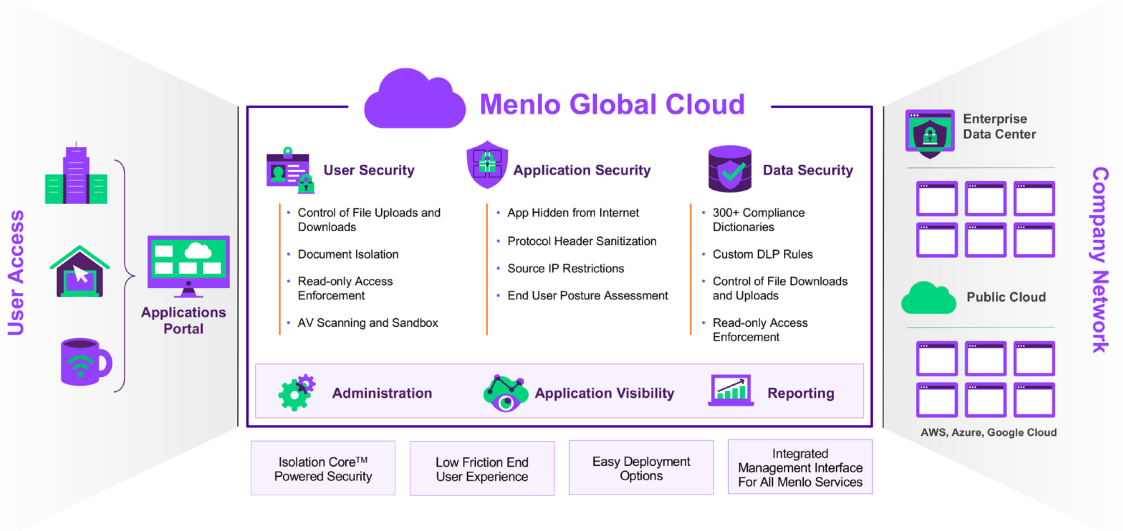


Figure 1: Private and SaaS applications are the new entry point into the network. MPA provides secure access for users to the data and information needed throughout the company network, ensuring that user, application, and data security requirements are met.

Enabling secure access to private applications from unmanaged devices

Menlo Private Access allows organizations to grant user-level access to highly distributed employees or third parties (partners, contractors, and customers), without exposing internal networks to untrusted entities and kept hidden from direct visibility on the public Internet. This provides a touch-free clientless deployment for private browser-based applications while improving the flexibilty, agility, and scalability of application access. Menlo's unique approach to clientless access coupled with its Isolation Core™ reduces IT complexity while continuing to provide seamless and secure access to private applications.

Menlo Private Access provides clientless, isolation-based secure access to private browser-based applications. MPA is quick to deploy, with no certifcate changes and no DNS record creation, and it's easy to manage through a single management pane.

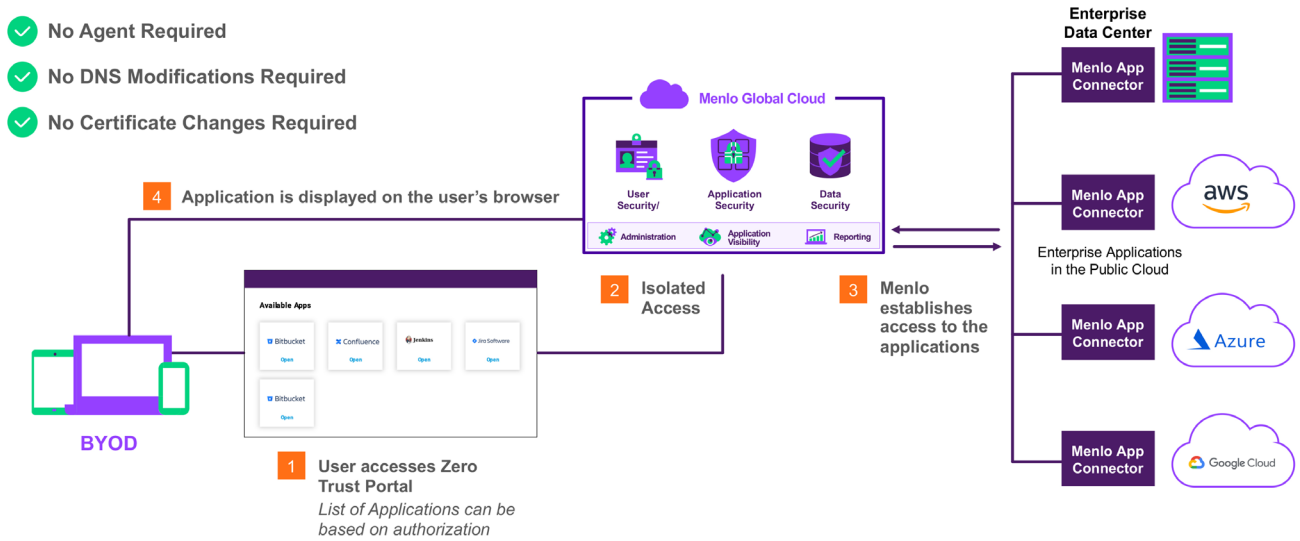


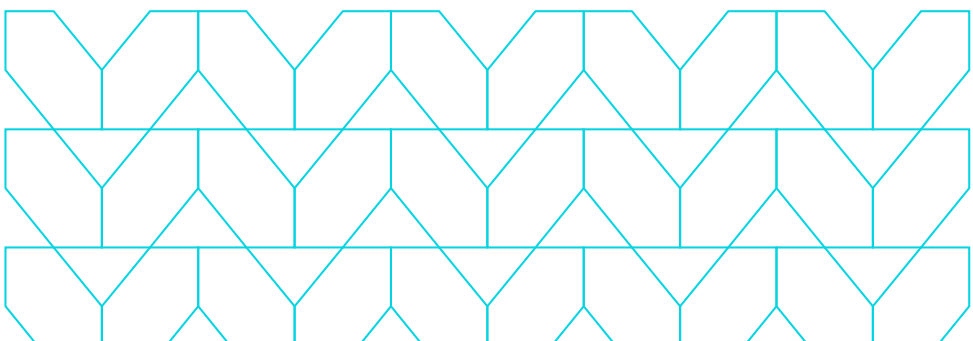
Figure 2: Zero Trust Network Access through browser session without requiring agent.

Legacy web app security tools fall short

Traditional web app security tools such as virtual desktop infrastructures (VDIs) and virtual private networks (VPNs) have traditionally been used to provide secure connections between remote users and mission-critical applications. However, the huge increase in remote workers resulting from digital and cloud transformation—as well as work-from-home mandates caused by the Covid-19 global pandemic—have shown the limitations of VPNs and VDIs, creating major bottlenecks that have significantly impacted application performance and user productivity. Organizations have gotten around this problem by using split tunneling or exposing application traffic altogether, neither of which is a good option.

Even when deployed properly, web app security tools are extremely vulnerable to hackers and malicious insiders exposing traffic to enterprising threat actors who use phishing, drive-by, and zero-day attacks to steal credentials and gain access to users' devices. Organizations have overcome these pitfalls by coupling their existing security tools with ZTNA solutions like MPA to help shore up the failings of their existing VPN and VDI solutions and provide access to only the applications that users need, all through a clientless approach.

Menlo Private Access provides secure and authenticated access to the configured application itself, not to the network. Applications are not exposed to the Internet, and access to all applications is encrypted and secured by isolation.



Feature	Benefits
Zero Trust Access to Private Applications	Easily provide access to apps that users need for their job functions, regardless of the network they are using.
	Secure access to applications for third parties, for contractors, or from BYOD devices.
Zero Touch Deployment	Simple agentless options to suit organizational needs. • Quick to deploy, quick to install and onboard users • No certs need to be imported • No public DNS record needs to be created
	Built on Menlo's elastic edge to ensure easy rollout to users globally, which scales dynamically based on usage.
Security Based on Isolation Core™	MPA is built on the Menlo Isolation Core™, which ties enhanced security directly into application access.
	Beyond allowing full application access polices, allows for granular application access such as read-only or preventing uploads/downloads within applications.
	Integrates directly with Menlo Security SWG and over 300 compliance dictionaries to ensure better security outcomes for the organization by eliminating threats.
Centralized Management	Define granular access policy per group or individual to access specific private applications.
	Provide a single management interface for all aspects of configuration and reporting across all Menlo Security Cloud Services.
	Save time and effort in configuration and ongoing management.

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 enables organizations to eliminate threats and fully protect productivity with a one-of-a-kind, isolation-powered cloud security platform. It's the only solution to deliver on the promise of cloud security—by providing the most secure Zero Trust approach to preventing malicious attacks; by making security invisible to end users while they work online; and by removing the operational burden for security teams. Now organizations can offer a safe online experience, empowering users to work without worry while they keep the business moving forward.