Data Sheet

Enable seamless access to enterprise applications for employees and partners without compromising security

Menlo Secure Application Access enables least-privileged access on a resource by resource basis, supporting access and application protection for both private and SaaS applications.

Providing employees and business partners with secure access to applications and data has proven more difficult as threat actors escalate their tactics. Hybrid work has made the situation even harder to manage. Legacy network architectures do not effectively extend beyond the systems that an enterprise controls, and layer-3 VPNs provide network access but can encourage lateral movement by threat actors. Enterprises need a zero trust solution that works everywhere, for managed and unmanaged devices.

Three things to know:

90% Of Fortune 500 companies were using applications with a zero-day vulnerability in the month of October 2023.

72% of applications provide access to unauthorized features.

66% of applications can be compromised by injecting code in HTTP headers or payloads.

Traditional secure access tools, such as virtual desktop infrastructure (VDIs) and remote-access 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 —have shown the limitations of VPNs and VDI. Performance bottlenecks have significantly impacted application performance and user productivity. Organizations have gotten around problems by using split tunneling or exposing web applications directly to the Internet. These workarounds are neither productive nor secure.

Exposed to the Internet, web applications are extremely vulnerable to hackers. Phishing, drive-by, and zero-day attacks make the situation worse. Hackers steal credentials and can gain access to enterprise networks and data.

Menlo Secure Application Access

Menlo Secure Application Access enables least-privileged access on a resource by resource basis. It supports access and application protection for both private and SaaS applications. Data security and information leakage protection works hand-in-hand with easy-to-manage access control. Menlo Secure Application Access ensures secure application access while simultaneously protecting the associated intellectual property and application data when you provide secure intranet access to contractors or provide access from a native RDP or SSH client. When you deploy Menlo Secure Application Access, you also protect your data and protect your application from infected endpoints.

Delivering the safest path to accessing enterprise private and SaaS applications

Menlo Secure Application Access supports access to private applications and keeps them hidden from direct visibility on the public Internet, helping protect the organization from exposure to internet-born threats, such as DDoS, code injection, and SQL injection. With Menlo Security, organizations do not have to sacrifice security or usability.

Additionally, access is granted only to specific applications that are necessary for a user's job function, not the whole network. The zero trust principles are built into the foundation of Menlo Secure Application Access, enabling both granular and conditional access policies to even highly distributed employees or third parties. Organizations can define access by users, groups, source IPs, and geographies. For non-browser based policies, organizations can enable a posture check of an endpoint before a user can gain access to an application.

Continuously enforce policy and safeguard applications, users and data

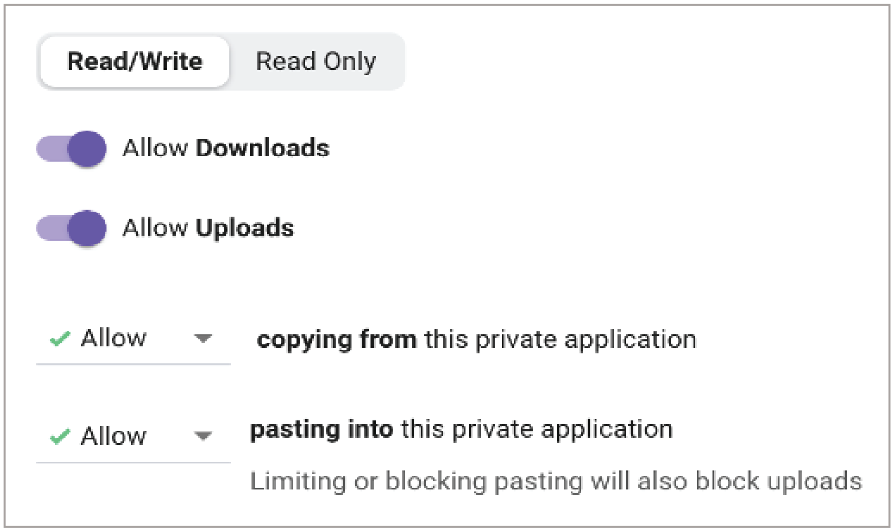
In addition to hiding applications from the Internet, Secure Application Access protects against the threat of an infected endpoint or an insider seeking to elevate privileges. Secure Application Access safeguards applications from evasive threats by using the Menlo Secure Cloud Browser to communicate between the local browser and application. Secure Application Access protects against attacks that employ:

- **HTTP header manipulation**
- **HTTP request smuggling**
- **Server-side request forgery**
- **And other protocol or payload manipulations**

Rather than access the original application, the Menlo Secure Cloud Browser creates a rendered representation of the application on the endpoint device directly in the user's browser. The content rendering provides access, while shielding the user from content-based attacks and shielding the application from malicious requests that might involve parameter tampering, web scraping, API abuse, and a host of other problems. Even if the endpoint somehow gets compromised, the threat actor cannot get direct access to issue requests to the server. Instead, all requests execute in the Menlo Secure Cloud Browser instead of the endpoint browser. Additionally, Menlo Secure Application Access provides Sandboxing and AV Scanning for all the content that is shared between the user and the application. If a user uploads an infected file, Menlo Secure Application Access stops the file from infecting the application and other potential malicious activity.

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

- **Download/upload**
- **Read-only/read-write**
- **Watermarking**
- **Data redaction**
- **Copy/paste**



● Allow **Downloads**

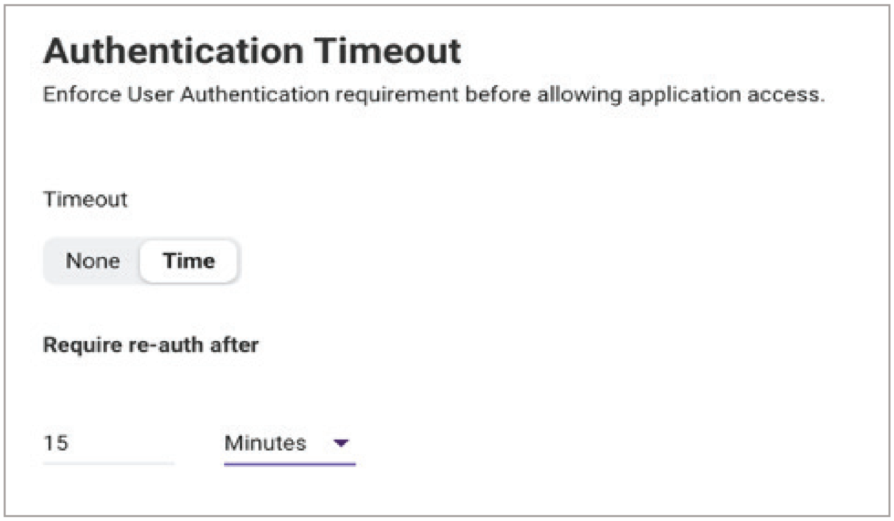
● Allow **Uploads**

✓ Allow ▾ **copying from** this private application

✓ Allow ▾ **pasting into** this private application

Limiting or blocking pasting will also block uploads

For more sensitive applications, Menlo Secure Application Access enables administrators to set a policy for shorter authentication timeouts.



Authentication Timeout

Enforce User Authentication requirement before allowing application access.

Timeout

Require re-auth after

15 Minutes ▾

Gain unmatched speed and scale for any application from any device and from any location

Menlo Secure Application Access offers flexible deployment options and solves the latency and scalability problems of traditional tools. Enterprises can choose a clientless deployment, use the Menlo browser extension or adopt the Menlo Zero Trust Client to secure access to public SaaS applications, internal web applications, and legacy client-server applications.

Menlo supports zero-touch and agentless deployment for browser-based applications and an agent for non browser-based applications. For browser-based applications, no DNS records are needed, there's no need to import certificates, and no agent is required. The agentless deployment helps organizations:

- Quickly provisioning and deprovisioning access to different applications without changing network topology or firewall rules
- Provide secure access with lower cost and maintenance
- Scale quickly with organizational needs
- Reduce IT complexity

The Menlo Security Client can be installed to provision access for non-browser applications. It uses the same interface for managing and monitoring. Different access to the same application can be provided to different users. With the Client, application access can be constrained by device posture as well. If configured, an end-user can access an application only if the minimum posture requirements are met.

Key capabilities:

Enterprise Extension:

Easily deploy the Menlo Enterprise Extension to provide users authorized access on unmanaged devices without installing any software on the endpoint.

Secure Access to Applications:

Menlo Security enables private applications to be hidden from the internet while still being accessible to authorized users, helping reduce the attack surface without impacting business operations. Access is only provided to configured users or groups to specified applications, preventing unauthorized access and lateral movement.

Protection Against Compromised Endpoints:

Rather than the browser accessing the application directly, a secure cloud browser fetches the data from the application and renders presentation of the application on the endpoint device directly in the user's browser. As a result, this shields the application from parameter tampering, web scraping, API abuse, and a host of other problems. Menlo Security provides sandboxing and AV Scanning for all the content that is shared between the user and the application. If a user uploads an infected file, Secure Application Access stops the file from infecting the application and other potential malicious activity.

Browser-Based Vulnerability Protection:

Attack techniques such as cookie and header manipulation, session hijacking are protected against because the endpoint is not interacting with the browser-based application directly. Menlo's Secure Cloud Browser is inherently secure, that means even if the endpoint gets compromised, the threat actor cannot get direct access to HTTP headers, content, and the application.

Granular Data Security:

Layers of granular security controls protect access to the data that applications hold. These controls include download/upload, read-only/read-write, watermarking, data redaction and copy/paste. Additionally, DLP controls can be applied to uploads for compliance and downloads for data leakage prevention.

Flexible Deployment:

Flexible deployment is delivered for private and SaaS applications. Zero touch and agentless deployment for browser based applications and an agent for non browser based applications.

Easy to Manage:

Simplify the onboarding and offboarding process with easy to manage policies.

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.