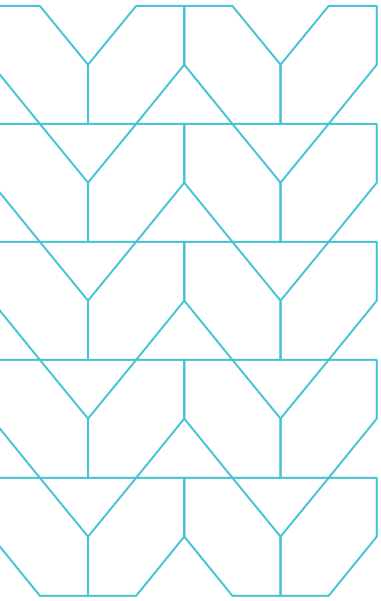
MENLO SECURITY

Make zero trust access easy with Menlo Security

Complete your zero-trust access architecture and enable remote users to get work done, all without requiring network rebuilds or a firewall refresh.

Solution Brief



The complicated world of zero trust

The zero trust model is designed to ensure that only authorized users can access applications, systems, and information. Every user, device, data, and network connection must be verified. Zero trust helps organizations move away from static, traditional perimeter-based security to a framework that focuses on users, assets, and resources. This change is necessary now more than ever with remote work, as employees and contractors need to access applications for their job no matter where they work or what device they use.

For over a decade, organizations have been trying to understand how to deploy zero trust within their organizations, however zero trust has been notoriously complex and often limited in deployment. These challenges include:

- **Complex Implementation:** To start a zero trust deployment, security and IT teams need to understand where data lives within their organization. Such data inventories can be especially difficult as data has moved outside of private data centers with the explosion of SaaS. Additionally, the increase in the bring your own device (BYOD) use case adds further to the complexity.
- **High Cost:** To map where data lives and continue with a traditional zero trust project, an infrastructure rebuild may be required and can be costly.
- **Interrupt Productivity:** Certain policies and workflows may slow down employee processes. Employees and contractors need access to various applications for their day-to-day, however, inefficient or incorrect access policies can slow down productivity and lead to employee resistance.

As an increasing number of applications become accessible through the browser, organizations need to implement zero trust to web traffic and interactions. If your zero trust architecture does not extend to the browser, you do not have true zero trust. Additionally, modern workforces frequently consist of contractors and bring your own device (BYOD) users, further highlighting the importance and need to implement zero trust to application access.

The key to implementing zero trust to application access

Organizations need a solution that reduces the cost and complexity of traditional technology, while protecting against evasive threats that target your browser-based applications. A solution should:

- **Support remote access**
- **Enable BYOD**
- **Reduce the risk of cyber threats**
- **Increase visibility into user actions**
- **Easy deployment and management**

Zero trust access with Menlo Security

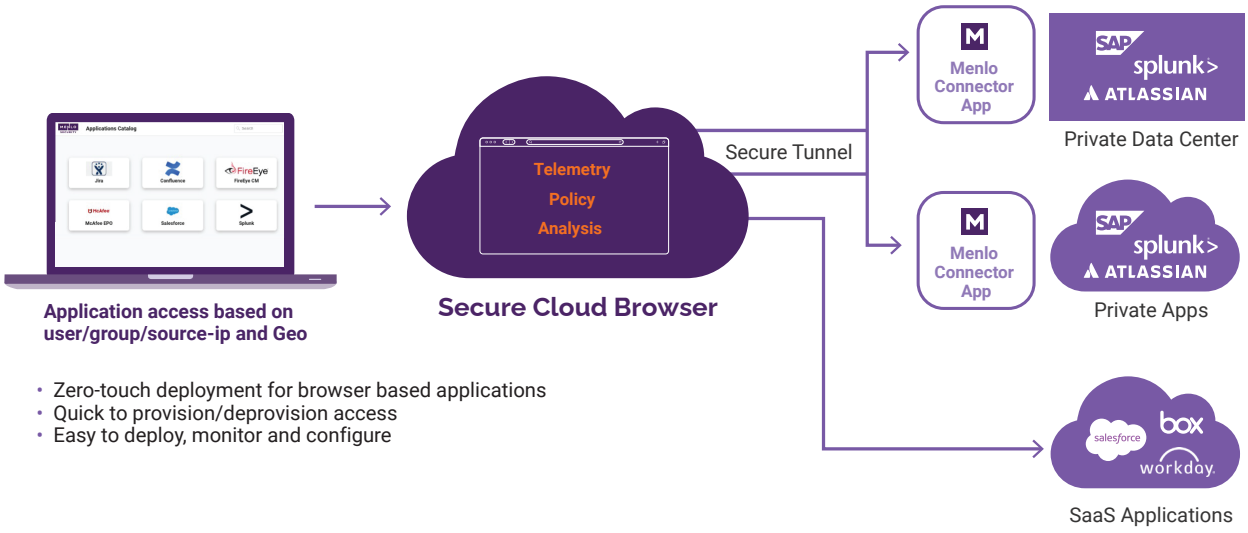
Menlo Secure Application Access makes zero trust access easy, helping reduce IT complexity while continuing to provide seamless and secure access to private and SaaS applications.

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.

To easily support remote access and/or BYOD users, Menlo Secure Application Access has zero touch and agentless deployment for browser-based applications. This agent-free, easy deployment helps organizations:

- Quickly provision and deprovision access to different applications. This can be done for users in a very secure manner without changing network topology or firewall rules.
- Provide secure access with lower cost and maintenance because there's no need for hardware, enabling BYOD.
- Scale quickly with organizational needs because secure access can be deployed within minutes.

For non browser-based applications, the Menlo Security Client can be installed. 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.



- Zero-touch deployment for browser based applications
- Quick to provision/deprovision access
- Easy to deploy, monitor and configure

To protect organizations from web threats, rather than access the original application, the Menlo Secure Cloud Browser creates a rendered image of the application on the endpoint device directly in the user's browser. There is no inherent trust of web traffic and interactions. As a result, this shields the application from 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 HTTP headers, content, and the application. Instead, all malicious activity is executed 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 help ensure zero trust is correctly implemented, organizations need increased visibility. Menlo Browsing Forensics can help organizations identify blind spots and continuously ensure only authorized access to applications with a comprehensive record of user interactions with web applications. These forensic archives are based on policy triggers such as users accessing private and sensitive applications. Each recorded session has a Menlo Forensics Log entry that includes supporting data of the event and one-click access to the recording.

Key Benefits

- **Granular and conditional access policies like Read-only/Read-write and Upload/Download**
- **Agentless and easy deployment for browser-based applications**
- **Deliver only clean, safe content to the endpoint, while safeguarding your application from malicious users or infected endpoints**
- **Increased visibility into end-user action within applications**

Make zero trust access easy

Menlo Security enables organizations to achieve zero trust access that is easy to deploy and easier on users, too. Enable contractors and BYOD users to get work done while continuously enforcing zero trust access policies, defending against web threats, and protecting data down to the last mile.

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.