



# Make Zero Trust Access Easy with Menlo Security

Complete Your Zero Trust Access Architecture and Enable Remote Users to Get Work Done—Without Network Rebuilds or a Firewall Refresh

## The Complicated World of Zero Trust

The zero trust model is designed to ensure that only authorized users can access applications, systems, and information without any notion of implicit trust. Every user, device, data, and network connection must be verified. Zero trust helps organizations move away from static, 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, partners, 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. Unfortunately, however, zero trust has been notoriously complex with legacy tools, which are 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 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.
- **Interruptions to productivity:** Certain policies and workflows may slow down employee processes. Employees and contractors need access to various applications for their day-to-day activities, and 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 apply zero trust principles to web traffic and interactions. If your zero trust architecture does not extend to the browser today, you do not have true zero trust. Additionally, modern workforces frequently consist of contractors and BYOD users, further highlighting the importance of and the need to apply zero trust principles 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 and third-party access
- Reduce the risk of cyber threats
- Increase visibility into user actions
- Ease deployment and management

## Zero Trust Access with Menlo Security

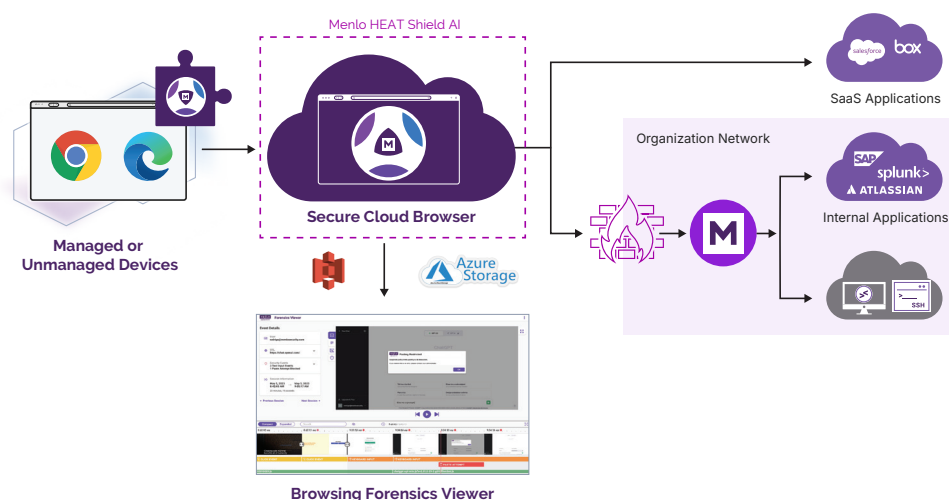
Menlo Secure Application Access makes zero trust access easy, reducing IT complexity and providing seamless and secure access to private and SaaS applications.

Access is granted only to the 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 fine-grained 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 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 additional hardware.
- 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. The Client uses the same interface for managing and monitoring access as the cloud version, and differentiated access to the same applications can be provided to different users or groups.



**Instead of directly accessing applications, users safely access a rendering of their applications in a portal or through an extension.**

Secure Application Access is built upon the Menlo Secure Cloud Browser, which creates a hardened digital twin of the user's local browser in the cloud. When a user requests access to an application, the request is replicated in the Secure Cloud Browser, protecting the servers and data from any threats that may be on the user's endpoint. This shields the app from potential problems, including parameter tampering, web scraping, API abuse, and more.

The Secure Cloud Browser also provides sandboxing and AV scanning for further protection. If a user uploads an infected file, the Secure Cloud Browser stops the file from infecting the application or carrying out other potentially malicious activities. The "clean" request is then sent to the application. The content that is returned from the server is processed the same way, and all active content is rendered in the Secure Cloud Browser, not in the user's local browser. That means that even in the rare case that a server is compromised, the threat is not spread to the user.

To provide even further protection, organizations can enable posture checks, both before and during access, which verify important device criteria like firewall status, OS version, and disk encryption. These checks integrate with CrowdStrike and enable endpoint posture checks that assess additional factors, such as the presence a CrowdStrike Zero Trust Assessment (ZTA) score.

With Menlo, organizations aren't forced to deploy a client for posture checks. Instead, organizations can leverage Managed Chrome to enable clientless posture checks, allowing IT to manage Chrome configurations and grant privileges based on the browser's posture.

To help ensure that zero trust is correctly implemented, organizations need increased visibility, which has long been impossible, as browsing sessions are notorious "blind spots" for security and IT teams. Menlo solves this problem with Browsing Forensics. As browsing sessions pass through the Secure Cloud Browser, Browsing Forensics can be enabled to record the sessions based on policy triggers, which can include specific applications, users, and groups, so that security, IT, compliance, and audit teams can finally see where users went and what they did while they were there.

## Benefits



Fine-grained and conditional **access policies**, such as read-only/read-write and upload/download.



Agentless, **easy deployment** of browser-based applications.



Only **clean, safe content** is delivered to the endpoint, while it safeguards your applications from malicious users or infected endpoints.



**Increased visibility** into end-user actions within applications.

## Make Zero Trust Access Easy

Menlo Security enables organizations to achieve zero trust access with a solution that is easy to deploy and easy on users, too. Enable partners, 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](https://www.menlosecurity.com) or email us at [ask@menlosecurity.com](mailto: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. © 2025 Menlo Security, All Rights Reserved.



Learn more: <https://www.menlosecurity.com>  
Contact us: [ask@menlosecurity.com](mailto:ask@menlosecurity.com)

