MENLO SECURITY

A Zero Trust approach results in zero compromise.

Outsmart threats and protect productivity with a Zero Trust approach powered by the Menlo Security Isolation Core.™

Solution Brief

Modern enterprises need modern approaches to security.

1. Okta, "The State of Zero Trust Security in Global Organizations."

The way we work is changing. Monolithic applications now live in the cloud, are made up of tens or hundreds of microservices, and are accessed by highly distributed mobile users. Threat actors are aware of the landscape and are taking advantage of it. Companies today are faced with this new paradigm: Internet access and usage is changing rapidly, while techniques tied to delivering malware increase in complexity and severity. As a response, a growing number of organizations are taking a Zero Trust approach to securing their network.

60 percent of organizations in North America (and 40 percent globally) are currently working on Zero Trust projects.[1]

A simple and effective approach to protect work is needed.

Unfortunately, current approaches to cybersecurity haven't evolved fast enough to match new cyberthreats, and security professionals are relying on antiquated solutions such as sandboxing, whitelists, and URL filtering to detect malware before it activates in the user's environment. This approach worked in the early years of the Internet, when websites were mainly static and malware was clunky, basic, and easily detectable. Today, web pages serve up rich, dynamic content hosted on distributed servers scattered across the web. A staggering array of entry points and third-party web elements coupled with web apps and Software-as-a-Service (SaaS) technologies have changed the way people access the Internet. Modern users require continuous, 24/7 direct connections wherever work takes them.

The remarkable changes in the Internet's makeup have come at a cost: Malware has evolved in terms of both complexity and prevalence. It's extremely easy for a threat actor today to spin up a new, specialized threat for only a few hundred dollars, creating a cost-efficient, targeted attack. Hackers can then bombard a target with multiple attacks and variations until a piece of malware gets through. In addition to malware scaling, hackers have made technological advances to evade the security industry's latest detection methods.

Modern malware, for example, can detect if it's activated in a sandbox and subsequently delay its payload.

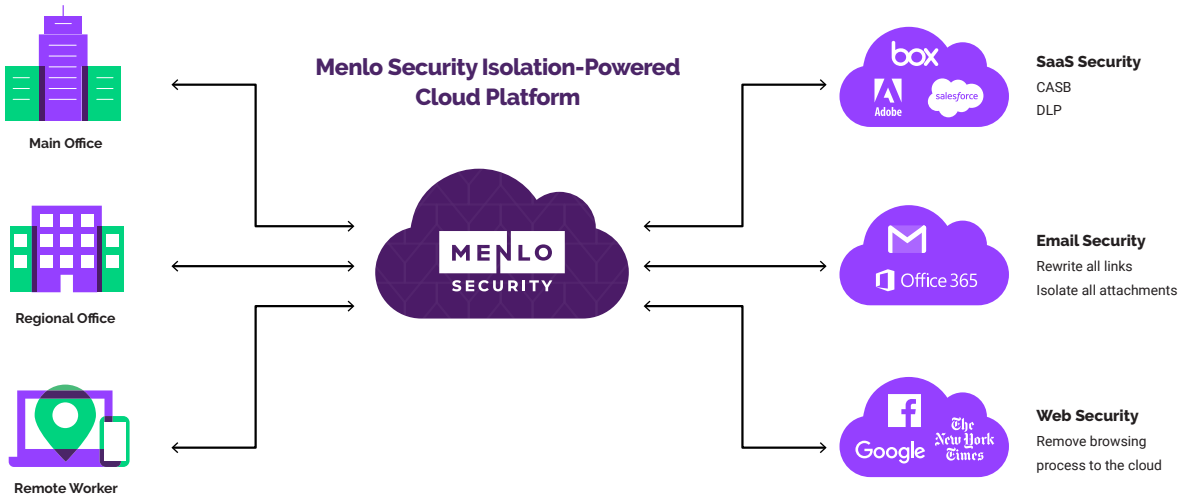
Benefits

- **Protect users from web- and email-based attacks.**
- **Open up more of the Internet for users without hindering productivity.**
- **Implement and scale Zero Trust security quickly and seamlessly across your organization.**

The Menlo Security Isolation-Powered Cloud Platform enables Zero Trust.

Menlo Security's Zero Trust approach is based on the notion that no traffic should be trusted, even packets that originate from inside the organization. This innovative approach is comprehensive and removes many issues associated with detection-based security Menlo Security has developed an approach that relies on isolation-powered cloud security. This enables an effective Zero Trust approach that isolates all web content—including sites, videos, and documents from employee endpoints.

Implementing the isolation platform in the cloud also makes it incredibly scalable and agile. IT teams don't have to configure hardware, and companies don't need to pay for additional software or machines. This approach can scale as big as an organization's cloud, accommodating fluctuating workforces, business cycles, or traffic volume.



Traditional security architectures and strategies don't work anymore; cybercrime is still growing despite the huge number of security tools available for an organization's stack. Zero Trust powered by Internet isolation is the answer.

Completely eliminate malware and other web-based threats.

By implementing the Menlo Security Cloud Platform powered by an Isolation Core™—and utilizing a Zero Trust Internet framework—an organization can proactively prevent all forms of browser-based malware. This tandem solution forms the backbone of cutting-edge security policies and demonstrates that the days of "patient zero" attacks and long breach-to-detection times are at an end. Zero Trust is the security stack of the future, allowing IT teams to overcome the cleverness and ingenuity of even the most malicious hackers. Its fundamentally different default-deny approach to web security stands against even the most complex malware by isolating every packet.

Discover how you can protect productivity and enable business to be conducted safely without deterring progress. We're ready to answer your questions 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.