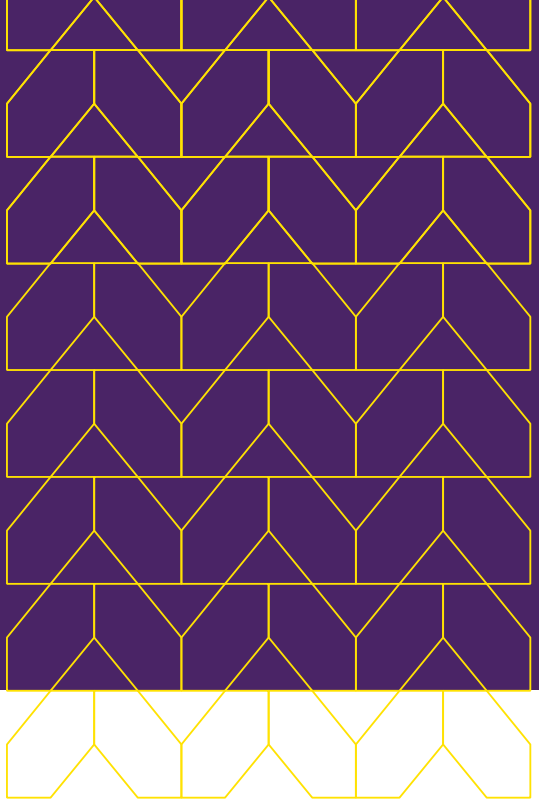
MENLO SECURITY



Secure the everywhere workforce.

Protect distributed, remote users from malicious threats on the Internet wherever business takes them.

Solution Brief

The way we work is constantly changing—users today are more distributed and more remote than ever before.

1. Verizon Data Breach Investigations Report

The days of everyone working from corporate headquarters are over. Employees today are spread out in branch offices, home offices, customer sites, coffee shops, and hotel rooms—yet they still expect the same working experience as if they were in the office. Malicious actors know this, of course, and have adapted their threat techniques for today's highly distributed workforce—using spearphishing, watering holes, and drive-by attacks to infect remote devices outside the network perimeter.

According to the Verizon Data Breach Investigations Report, 94 percent of malware is delivered via email, and phishing attacks account for more than 80 percent of reported security incidents.[1]

From there, they can spread laterally from device to device and eventually make their way to high-profile targets inside the network. In order to enable business agility and compete in today's highly competitive world, organizations need to ensure that remote workers are able to securely access the tools and information they need to do their jobs—wherever business takes them.

Traditional cybersecurity approaches were built for the perimeter.

Organizations have traditionally focused on building hardened perimeter defenses around the data center and corporate headquarters where most users worked—but the perimeter has largely evaporated over the past several years as users, applications, and data have migrated to the cloud. Unfortunately, enterprise security hasn't kept up, and it continues to rely on an outdated and irrelevant detect-and-respond approach to cybersecurity.

Digital and cloud transformation coupled with work from anywhere policies require a new way of protecting remote workers from malicious threats on the Internet.

Benefits

Secure work anywhere employees do business.

Reduce IT complexity and overhead by moving security to the cloud.

Expand to new markets and geographic regions without having to worry about security.

The Menlo Security Cloud Platform powered by an Isolation Core™ enables Zero Trust.

Zero Trust means that no traffic should be trusted, even packets that originate from inside the organization. Instead, all browser-based Internet traffic should be treated as malicious, and web traffic should be isolated from endpoint devices. Menlo Security takes an isolation approach to Zero Trust that eliminates the flaws with detection-based security. Zero Trust powered by isolation allows organizations to completely outsmart malware and other web-based threats, giving employees worry-free, secure access to the tools and information they need to keep the business running.

Menlo Security powered by an Isolation Core™ enables Zero Trust by routing all web traffic through a cloud-based remote browser before delivering only safe content to the endpoint. It doesn't matter if the web content is good or bad, categorized or uncategorized, because our isolation-powered platform assumes that all content is malicious and treats it accordingly.

Menlo Security's Cloud Platform is incredibly agile—scaling to be as large as the organization's cloud while accommodating fluctuating workforces, customer needs, and traffic volume without requiring complex configuration or clients deployed on endpoint devices.

At Menlo Security, our cloud-based platform isolates web content using our proprietary Isolation Core™ technology. It offers remote users a 100 percent safe way to view web and email content that doesn't diminish productivity or the user experience.

This Zero Trust approach, combined with the scale and coverage of the cloud, allows Menlo's isolation-powered platform to protect remote users from major threats like phishing, ransomware, and malvertising head-on. It also secures corporate and personal email and makes it easier for companies to achieve compliance—all without reducing functionality or the user experience.

Completely eliminate malware and other web-based threats.

As work moves from the data center to the edge of the network, organizations need a new cybersecurity approach based on Zero Trust. The Menlo Security Cloud Platform powered by an Isolation Core™ prevents malware and other web-based attacks from accessing the endpoint without hindering application access or productivity. This allows employees to access the tools and information they need wherever busines takes them.

To find out how Menlo Security can help you protect productivity and enable the business, visit menlosecurity.com or contact 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.