MENLO SECURITY

White Paper

Eliminate malware threats with zero trust.

Isolation-powered security provides full protection against email and Web based threats.

“It’s not if, but when.”

Unfortunately, that’s the view many organizations take about the inevitable failure of their cybersecurity defenses. They’re being forced to resign themselves to partial protection, because today’s security technology—which hasn’t changed much since the beginning of the Internet—is fundamentally flawed. It’s designed to identify threats and prevent them from reaching the network. But no product on the market can evaluate with 100% accuracy whether something from the Internet—including a file, an image, or a document—is safe.

Instead of trying to identify threats and scrambling to prevent them, what if you could:

Ensure secure cloud access for your employees without any risk to your organization?

Warn employees when they’ve fallen for a phishing attack?

Never again worry about malware, viruses, or ransomware?

Using a fundamentally different approach, Menlo Security eliminates threats from Malware completely, fully protecting 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 and removing the guesswork from security.

Zero Trust is a default deny approach that is fundamentally different from traditional cybersecurity.

Detect-and-prevent is a faulty strategy.

Cyberattacks are becoming more sophisticated, with increasingly targeted phishing scams in the form of emails that can trick even the most tech-savvy of employees into divulging the most secure information. According to Gartner, the accelerating adoption of cloud applications and an ever-mobile workforce have made the browser the most important productivity tool in the organization. At the same time, the clear majority of cyberattacks start with an email or the browser, targeting end users with bogus emails and infected attachments, websites, and downloadable documents. The risk of harm to organizations, employees, and customers continues to grow. But the security industry insists on the same old approach—detect and prevent.

Detect-and-prevent has reached its potential, and attackers have learned how to bypass it. According to Verizon, in 2018 there were 41,686 reported security incidents and 2,013 confirmed cybersecurity breaches. Worse: 68% of breaches took months or longer to detect. This means that the two primary defense methods—blocking an attack and then detecting a breach once it has occurred—are failing miserably.

68%

of breaches take months or longer to detect.

Verizon, 2018 Data Breach Investigation Report

The problem is getting worse.

There are already millions and even billions of malware attacks being created. As companies move to the cloud and adopt SaaS, users may now encounter attacks outside the safety of their corporate network. The cloud and SaaS break the hub-and-spoke architecture of the corporate network as users go directly to the Internet, bypassing network security and potentially costing organizations millions of dollars as a result of cybersecurity breaches.

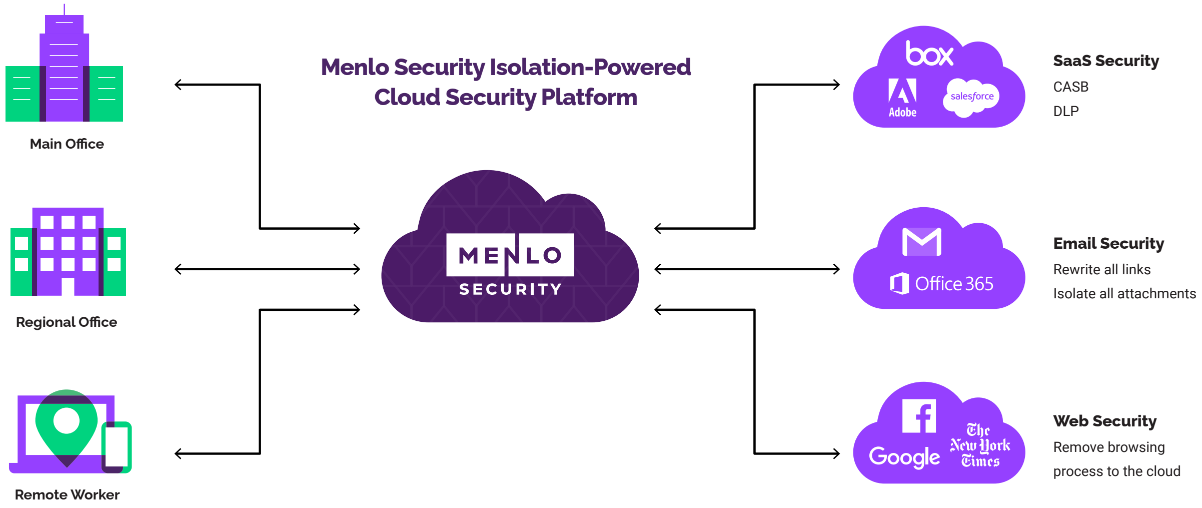
A global insurance company was experiencing web malware and phishing attacks and found that 80% percent of those issues were caused when employees accessed uncategorized websites. Infected devices required costly, time-consuming reimaging. While anti-phishing training for employees was somewhat helpful in addressing the attacks, many employees continued to click on infected links, leading to credential theft and malware infection.

The industry is trying to get better at detecting threats. There is a lot of focus on artificial intelligence (AI), and it does look promising. With the vast amounts of data processing required, only a machine can achieve the computational scale required. But true AI that is as good as human intelligence with machine scale is still years away. To address the growing and dangerous problem today, we need to fundamentally rethink the security paradigm.

Zero Trust enabled by Isolation, prevents 100% of all malware threats from email and web attacks.

Zero Trust: rethinking email and web security

As many cybersecurity experts continue to lose sleep over trying to perfect a faulty paradigm, Zero Trust has emerged as the best way to achieve the previously unthinkable: 100% safe email and web access. At Menlo Security, we achieve Zero Trust with the Menlo Security Isolation-powered Cloud Security Platform, which takes the browsing process off the desktop and moves it to the cloud, effectively creating an “air gap” between the Internet and enterprise networks. The content is cleaned and safely rendered from the cloud browser to the browser on the desktop, giving the user an experience identical to the one on the desktop. Any breaches or attacks are completely isolated away from the endpoint and user.



Isolation is a completely new way of thinking about security, as it separates an organization’s network from the Internet so that attackers can never gain a foothold in the working environment. Malware is literally barred from the endpoints. All email and web traffic moves through this isolation layer, where the content is visible but never downloaded to the endpoint. As a result, the Menlo Security Isolation-powered Cloud Security Platform allows companies to maintain control of security and apply a consistent, global policy to all their users.

The evolution of isolation

When isolation technology first emerged about a decade ago, it proved effective against cyberattacks, but it also ruined the user experience by making Internet browsing slow and clumsy. But as with any good idea, innovators improved it, making it viable for even the most demanding enterprise. For years, Menlo Security has worked to make isolation technology a pleasant and seamless browsing experience for a modern-day workforce that is increasingly using cloud-based applications.

> The Isolation Core™ is a completely new way to think about security. It separates your network from the Internet so that attackers can never gain a foothold in your environment.

Today our content-rendering technology, called Adaptive Clientless Rendering™ (ACR), has been perfected to the point where we provide a user experience identical to native browsing on the desktop. When a user sends a command to the local browser from their computer, the Menlo Security Isolation-powered Cloud Security Platform receives the command and opens the site in a browser in a remote container in the company’s cloud. The content is then replicated through ACR, which uses three different rendering methods to optimize the user experience.

The user can engage with the website without any active content on their computer. In other words, any malicious content on the website can never infect a laptop or other device. What's more, warnings are displayed on phishing sites, and then entry of credentials or uploading of files is blocked. As a result, employees can safely open emails and use cloud-based applications without fear of a cyberattack.

Take malware off the table.

The Menlo Security Isolation-powered Cloud Security Platform enables Zero Trust and eliminates 100% of all malware threats from email and web attacks and fully protecting productivity. Now organizations can offer a safe online experience, empowering users to work without worry while they keep the business moving forward.

Menlo Security transformed malware prevention for a global financial enterprise over a six-month period. This Fortune 100 company has one of the most advanced security operations in the world, with some of the most advanced cybersecurity products. Despite the millions of dollars they were spending on cybersecurity, phishing attacks and malware attacks were still occurring—until they moved to Menlo Security.

The Menlo Security Isolation-powered Cloud Platform provided 100% protection against:

1,089

phishing malware and malware links that bypassed defenses but were stopped by Menlo Security

8,541

known malware sites that were missed by existing security solutions but were blocked by Menlo Security

The Menlo Security Isolation-Core™ has tremendous benefits above and beyond protection from email and malware threats. For example, because email and web threats are eliminated, companies often experience a reduction in alerts of up to 90%. This frees up tremendous capacity for cybersecurity personnel, who are already difficult to find, hire, train, and retain. Zero-day threats are also eliminated. And unpatched systems are safe, so no fire drills are needed every time Microsoft or google releases a new patch.

It's time to rethink how you approach security. Menlo Security does not leave anything to chance. Our extensible security platform—built on a unique isolation core—is the only solution to deliver on the promise of cloud security by eliminating all online threats to enable organizations and their people to work without worry.

To find out more, contact us:

menlosecurity.com
1-877-255-9394
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.