Menlo Security

WHITE PAPER

Zero Trust Internet Is the Answer for 100% Email and Web Security

Internet Isolation Provides Superior Protection against Cyberattacks

How many times have you heard the phrase, "It's not if, but when"? The saying can easily be applied to the inevitable failure of a company's cybersecurity defenses, and it's surprising how widely accepted this view is. Cybersecurity defenses are designed to identify threats and then prevent them. This strategy is imperfect, however, because there is no product on the market today that can evaluate with 100 percent accuracy whether something from the Internet—including a file, an image, or a document—is safe. So the industry standard is to accept that your cybersecurity sometimes fails, and you need to ensure that you can detect and remediate the breach as quickly as possible.

What if there was another way?

- What if you could separate your enterprise network from the public web while still allowing employees to have seamless access to the Internet?
- What if you could warn employees that they were on a phishing site when they've fallen for a real phishing attack?
- What if you never had to worry about malware, viruses, or ransomware being downloaded?

All of these "what if" questions can be a reality with the Zero Trust Internet. This is a default deny approach that is fundamentally different from the way traditional cybersecurity products work. Today's products categorize Internet content and websites as being either malicious or safe, and this approach is known to fail. Internet isolation enables the Zero Trust Internet and takes the guesswork out of security by assuming that all Internet content and websites are malicious.

Internet isolation is the technology that delivers the Zero Trust Internet by separating an enterprise network from the public web, while still allowing users to access the Internet seamlessly. The solution removes the viewing of email attachments and web browsing from the desktop and moves it

Zero Trust Internet is a default deny approach that is fundamentally different from the way cybersecurity products work.

to the cloud. By isolating Internet content in the cloud, users are protected from malware, ransomware, and phishing attacks that bypass legacy defenses, thereby eliminating the most prolific sources of breaches.

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 and critical information. According to Gartner, the accelerating adoption of cloud applications and an ever-mobile workforce have made the browser the most important productivity tool by far. 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 does not appear to have an end in sight. Yet the security industry insists on the same old approach—detect and prevent.

68%

of breaches take months or longer to detect.

Detect and Prevent Is a Faulty Strategy

The "detect and prevent" approach has reached its potential, and attackers have learned how to bypass this defense method. Verizon reported that in 2018, there were 41,686 reported security incidents and 2,013 confirmed cybersecurity breaches. What's more appalling is that studies have shown that 68 percent of breaches take 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.

The industry is trying to innovate and 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.

The problem gets worse as companies move to the cloud and adopt software as a service (SaaS). There are already millions and even billions of malware attacks being created, and users may now encounter them outside the safety of their corporate network on the Internet. The cloud and SaaS literally 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.

Let's take the experience of a large, global insurance company as an example. They were experiencing web malware and phishing attacks and found that 80 percent of those issues were caused by employees accessing 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.

To address this growing and dangerous problem, we need to fundamentally rethink the security paradigm.

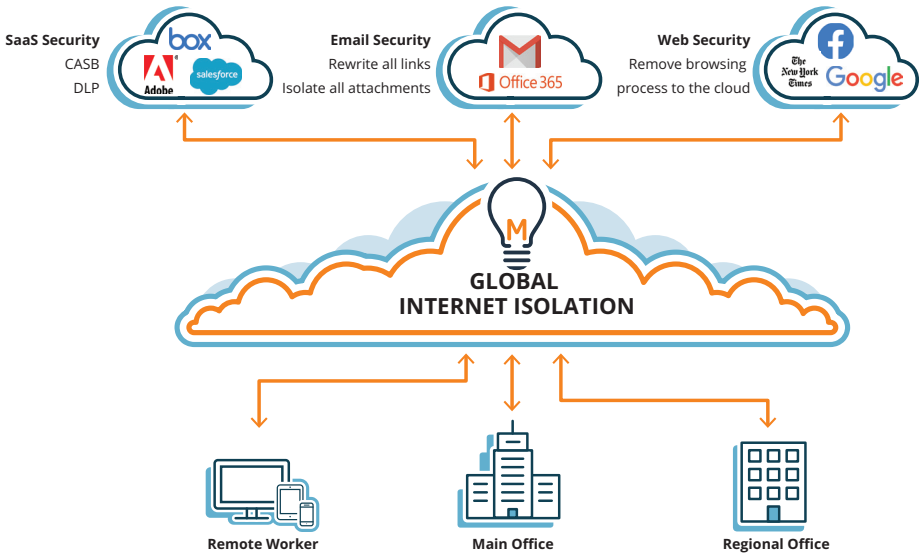
Zero Trust Internet: Rethinking Email and Web Security

As many cybersecurity experts continue to lose sleep over trying to perfect a faulty paradigm, the Zero Trust Internet has emerged as the best way to achieve the previously unthinkable: 100 percent safe email and web access. This is achieved through Internet isolation, which removes the browsing process from the desktop and moves it to the cloud, effectively creating an "air gap" between the Internet and enterprise networks. Content is cleaned and safely rendered from the cloud browser to the browser on the desktop, so the user experience is the same as if they were browsing from their own desktop. Any breaches or attacks are completely isolated away from the endpoint and user. The user is literally isolated from the threat.

Internet 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 workplace 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, Internet isolation allows companies to maintain control of security and apply a consistent, global policy to all their users.

Internet isolation is a completely new way of thinking about security. It separates your network from the Internet so that attackers can never gain a foothold in your environment.

Zero Trust Internet Architecture



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

Today our content rendering technology, called Adaptive Client Rendering (ACR), has been perfected to the point where we provide a user experience that is no different from native browsing on the desktop. When a user sends a command to the local browser from their computer, the isolation cloud 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. The experience is the same as if browsing from the desktop browser, and the result is that employees can safely open emails and utilize cloud-based applications without fear of a cyberattack.

Internet Isolation Prevents 100% of Email and Web Attacks

Today we can say, without hesitation, that the Internet isolation platform we have developed for our customers to achieve a Zero Trust Internet prevents 100 percent of all malware threats from email and web attacks.

Zero Trust Internet prevents 100 percent of all malware threats from email and web attacks.

The clear benefit of moving to a Zero Trust Internet is demonstrated by how we helped one of our enterprise-level global financial clients over a six-month period. This Fortune 100 customer 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 the Zero Trust Internet. Internet isolation has prevented the following:

- 1,089 phishing malware and malware links that bypassed defenses but were stopped by Internet isolation.
- 8,541 known malware sites that were missed by existing security but were blocked by Internet isolation.

Internet isolation 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 percent. This frees up tremendous capacity for cybersecurity personnel, who are already difficult to find, hire, train, and retain. Zero-day threats are also eliminated. Unpatched systems are also safe, so no fire drills are needed every time Microsoft or another company releases a new patch.

Cybersecurity is always evolving, and it is time to rethink how we approach security. The standard detect-and-prevent approach is not working, and as an industry, we have already accepted the fact that it will fail. The industry needs something different, and that something is the Zero Trust Internet. The best way to protect your organization from today's threats is to isolate your endpoints from the Internet. It's a radical and completely logical concept, and it makes much more sense than to keep doing what isn't working.

To learn more, visit menlosecurity.com or email ask@menlosecurity.com.

About Menlo Security

Menlo Security protects organizations from cyberattacks by eliminating the threat of malware from the web, documents, and email. Menlo Security has helped hundreds of Global 2000 companies and major government agencies achieve Zero Trust Internet. The company's cloud-based Internet Isolation Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. The company was named a Visionary in the Gartner Magic Quadrant for the Secure Web Gateway.

Contact us
menlosecurity.com
(650) 614-1705
ask@menlosecurity.com