Menlo Security

BRIEF

Zero Trust Internet

Secure Cloud Transformation powered by Isolation enables a Zero Trust mindset.

Benefits:

- Organizations prevent more malware by adding increased security to all traffic
- Security teams catch malware proactively rather than waiting for a breach
- Protects users from web- and email-based attacks
- Instantly follows Zero Trust policies explicitly and by design

Traditional Internet-Related Cybersecurity Is Inherently Flawed

Modern cybersecurity still acts as it did back when the industry was created, 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. The 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 until it has passed into the user environment.

Companies today are faced with this new paradigm: The Internet is changing rapidly and dramatically while malware increases in complexity and severity. To meet these new threats, the security industry has devised a new approach: Zero Trust security.

Zero Trust Internet

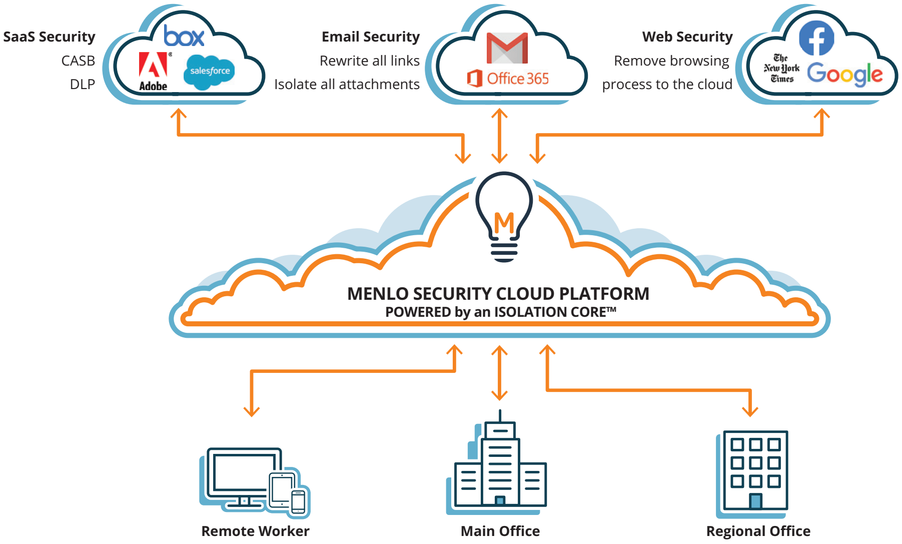
At the core of Zero Trust architectures lies the idea that no traffic should be trusted, even packets that originate from inside an organization. The Zero Trust Internet dictates that all browser-based Internet traffic should be treated as malicious, and web traffic should be isolated from endpoint devices. This new approach is comprehensive and removes many issues associated with detection-based security, yet it theoretically requires lots of management overhead.

Internet Isolation

Secure Cloud Transformation powered by Isolation enables the Zero Trust Internet by re-routing all web traffic through a cloud-based remote browser. It doesn't matter if the web content is good or bad, categorized or uncategorized. Internet isolation simply assumes everything is malicious and treats it as such. Basing 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. Internet isolation can scale as big as an organization's cloud, accommodating fluctuating workforces, business cycles, or traffic volume.

Traditional security architectures and philosophies don't work anymore; cybercrime is still growing despite the huge number of security tools in an organization's stack. Why is this the case? How can we stop it?

Zero Trust Internet Architecture



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 the future's security policies and demonstrates that the days of "patient zero" attacks and long breach-to-detection times are at an end.

Zero Trust security through secure cloud transformation 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. To find out more, visit menlosecurity.com or contact 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 Secure Cloud Transformation. The Menlo Security Cloud 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