Menlo Security

WHITE PAPER

Isolation Core™: A Part of the Modern Cloud Security Architecture

Integrate the Menlo Security Cloud Platform powered by an Isolation Core™ in your security stack to stop email- and web-based attacks without negatively impacting user experience or productivity.

Cyberattacks are a worldwide threat, and every person, government, and organization connected to the Internet needs to be aware of them. Reports indicate that the volume of cyberattacks around the world is expected to increase significantly—especially as business users continue to rely more and more on web apps, Software as a Service (SaaS) platforms, and powerful media-rich websites to conduct day-to-day responsibilities. While attack volume has always been a challenge for individuals, nations, and organizations, it is not the real problem: The increasing sophistication of the attacks is the most damaging.

> Cyberattacks today may be surgical, targeting specific payloads and even specific individual victims.

Cyberattacks today may be surgical, targeting specific payloads and even specific individual victims. Attacks are able to evade detection—avoiding anti-virus (AV) and anti-malware software, and going into sleep or stealth mode to remain undetected when placed in a sandbox. They are also able to elude detection if exfiltrating data. Many attacks have gone fileless, meaning they are not utilizing any files or executables, making them almost invisible to standard AV and other detection tools, and virtually unstoppable before they can launch their malicious payloads. Cyberattacks are also becoming easier to launch. The meteoric rise in the number and deployment of "as-a-service" attack methods, such as ransomware as a service, means that even novice attackers can afford and leverage sophisticated code to launch dangerous, profitable attacks.

Today's Cybersecurity Frameworks

There is no lack of existing cybersecurity frameworks available today. These frameworks provide best practices to guide organizations on how to secure their networks and data. They also provide guidance on how to best protect an organization's users from the latest threats and cyberattacks.

Menlo Security's new approach to web and email security alleviates the need to limit employee web access, even for uncategorized websites.

Most existing cybersecurity frameworks leverage similar methods and techniques for network, user, and data protection, especially for web and email security. The only differentiators between many published security frameworks are the success and follow-through of the deployment and the strength of the organization's security team in deploying, enforcing, and maintaining the framework.

However, some security frameworks are not feasible for deployment, and others, while stressing security, sacrifice convenience and the user experience. An example of this trade-off is evident with addressing web and email security. Several cybersecurity frameworks suggest that in order to attain optimum web security, users should be compelled to use two separate web browsers: One would disable all plug-ins and unnecessary scripting as well as enforce limited functionality for web browsing, while the other web browser would be configured with plug-ins, scripting, and more. The first browser would be used only to access sensitive websites, such as websites for business, banking, and so on. The second browser would be used for general web access.

While this concept has been around for some time, it is not a practical or effective approach to solving the issue of web malware and email-based attacks. For instance, it is almost certain that users would become confused about when to use which web browser for business or personal use, leaving the organization open to attack and defeating the purpose of the separate browser approach. Also, help desk calls would likely increase because of the confusion about which browser to use and when. Finally, supporting two browsers for two different use cases would be costly and time-consuming, not to mention that it would severely impact user experience and productivity. The most important reason, however, is the simple fact that most business is conducted over email and on the web. Users need secure and ubiquitous access to powerful web-based tools to conduct business—and these advanced features can't be throttled back without seriously impacting users' ability to do their job.

There are now other, more viable techniques to protect organizations and users from web and email attacks.

Web Browsers Are Vulnerable

While web browsers are becoming more sophisticated, and developers are adding more features and capabilities to make web browsing safer and more secure for users, attackers can still exploit many areas of exposure and even vulnerabilities. Many studies show that most cyberattacks begin on the web. Reports have also shown that many common websites accessed by users daily are running vulnerable code on their web servers, making them ripe for attack or hijacking. In addition, while a user may be initializing a single request on a web page, the website they are accessing can be connecting to an average of 25 different "background sites." Background sites are the websites that may be fetching the latest viral video from a content-delivery server or grabbing advertisements from an ad-delivery network. These actions are all behind the scenes, unseen by the user, and mainly invisible to current malware protection solutions such as anti-virus and web filtering offerings. Yet, a background site that is delivering malware-infested code or active content can still infect a user's device. The level of sophistication and maliciousness of web-borne malware, combined with the deviousness of attackers, continue to make web browsing as treacherous as ever for users, their organizations, and their data.

> The Isolation Core™ is a fresh, new approach to an ever-growing, ever-complex challenge organizations face today that cannot be adequately addressed by the existing detection approach to security. Isolation is part of today's security stack.

Isolation Core™

What if the execution of the actual website code occurred away from a user's device?

That's the fundamental approach of the Menlo Security Cloud Platform powered by an Isolation Core™.

Instead of making the choice between running all web functions—fetch, execute, and render—in the web browser on a user's device, Menlo Security contains the fetch and execute functions remotely in a cloud environment. That leaves the rendering, and all the functionality that goes along with it, to run in the user's web browser. The rendered web page (either via an email link or web browsing) looks and feels exactly the same as the actual web page—because it IS the web page, only there is no malware risk. All executables are handled in the cloud-based remote browser. It doesn't matter if the web code is or isn't infested with malware, or if the web page contains active content—JavaScript, Flash, and so on—that is or isn't serving as a platform for malware, because the Menlo Security Cloud Platform with an Isolation Core™ doesn't try to determine whether the code is good or bad. The same is true for any email link. There's no need to determine if links are malicious. They can all be isolated, effectively stopping users from falling victim. Unlike current malware protection solutions, Menlo does not need to make a "good" versus "bad" or "allow" versus "deny" decision. The Menlo Security Cloud Platform with an Isolation Core™ is agnostic: It treats all web code as if it were bad and isolates it.

Menlo Security has pioneered an approach that cleanly combines web and email security into a single, cohesive secure cloud platform powered by isolation. Built from the ground up as a multi-tenant platform, the solution leverages the elasticity of the cloud to deliver a scalable, 100 percent safe web environment without compromising the user experience.

Enabling the Zero Trust Internet

Thousands of organizations have eliminated web- and email-based malware by implementing the Menlo Security Cloud Platform with an Isolation Core™. But while providing users with ubiquitous and secure web access without impacting the native experience is the main benefit, it's not the only benefit of isolation. Using isolation to enable a Zero Trust Internet approach to cybersecurity also radically reduces IT operational expenses—a key benefit in today's agile, budget-conscious environment. The traditional detect-and-respond approach that relies on website categorization and threat intelligence causes an explosion of help desk requests resulting from false positives. In addition, infected devices take time and resources to reimage. Taken together, a Zero Trust Internet approach powered by the Menlo Security Cloud Platform with an Isolation Core™ can save enterprises millions of dollars in IT costs—all the while reducing the risk of being impacted by a devastating cybersecurity attack.

Many decisions today come down to cost efficiency. However, with the Menlo Security Cloud Platform, you get the best of both worlds: a more robust cybersecurity posture and a reduction in IT costs.

To find out how Menlo Security can help protect your company against cyberattacks, contact us at ask@menlosecurity.com or vist 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