Menlo Security

ISOLATION: A PART OF THE MODERN SECURITY ARCHITECTURE

WHITEPAPER

ISOLATION: A PART OF THE MODERN SECURITY ARCHITECTURE

Introduction

Cyberattacks are a worldwide issue, and every person, government, and organization connected to the Internet needs to be aware of it. Reports indicate that the volume of cyberattacks around the world is expected to increase significantly. Most attacks leverage the ubiquitous web for proliferation. While attack volume has always been a challenge for individuals, nations, and organizations, it is not the real problem: The increasing quality of the attacks is the most damaging.

While cyberattack volumes are growing, unfortunately, attack quality is also getting exponentially better. Cyberattacks today may be surgical, targeting specific payloads and even specific individual victims. Attacks are becoming more sophisticated and able to evade detection—avoiding anti-virus (AV) and anti-malware software, and going stealth 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. As cyberattacks increase in volume and sophistication, they are also becoming increasingly 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.

Almost hand in hand with the increase in cyberattack volume and sophistication, email has become the chosen delivery mechanism for cyberattacks. Email is, after all, still the most-used business communication means. Most attacks are now driven by phishing operations and even more targeted spear-phishing campaigns.

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.

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 pleasure, 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 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 could negatively affect user productivity.

There are now other, more viable techniques to protect organizations and users from web and email attacks. To best appreciate these methods, it can help to understand how a web browser works.

Web Browser Inner Workings

On a computing device such as a laptop, various components enable the web experience on the device: operating system components, application components, and web browser components. Diving deeper into the browser components, three core functions deliver a web page to a web browser on a user’s device: fetch, execute, and render.

When a user clicks on a web link in an email or a document, or accesses a web page in any fashion, their web browser fetches a data stream that comprises the content from the web page, which is code that has been served from web servers. The fetched data stream includes the fonts, images, and active content, such as JavaScript and Adobe Flash, that make up the web page. The fetched data is then executed on a user’s device in their web browser. Execution transforms the data stream from bits into content, such as video, music, advertisements, and more. The web browser renders the pixels, delivering the content in the viewable and interactive format of a web page for the user on their device.

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 and their device. The level of sophistication and maliciousness of web-borne malware, combined with the deviousness of attackers, continues to make web browsing as treacherous as ever for users, their organizations, and their data.

A NEW APPROACH

Isolation

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

That's the fundamental approach of Menlo Security's web browser isolation.

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 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 Menlo Security Isolation Platform. 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 platform doesn't try to detect good from bad. Unlike current malware protection solutions, Menlo's isolation platform does not need to make a "good" versus "bad" or "allow" versus "deny" decision. The Menlo Security Isolation Platform 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 security, email security, and phishing and awareness training into a single, cohesive platform. Built from the ground up as a multi-tenant platform, the Menlo Security Isolation Platform leverages the elasticity of the cloud to deliver a scalable, 100 percent safe web environment, without compromising the user experience. Menlo Security's isolation solution addresses credential theft, zero-day attacks, ransomware, and malvertising, as well as secures personal email and helps organizations meet compliance regulations.

A Customer's Isolation Journey

A large, global insurance company was experiencing web malware and phishing attacks. Eighty percent of web malware infections were caused by employees accessing uncategorized websites. Infected devices would require costly, time-consuming reimaging. Anti-phishing training for employees was somewhat helpful in addressing phishing attacks. But some employees would continue to click on phishing links, leading to credential theft and malware infection

Limiting employee web access wasn't a solution the company wished to implement, because it would negatively affect user productivity while causing an explosion in help desk requests. However, left without other options and facing increasing infections, potential data breaches, and increasing reimaging costs, the company took a draconian measure: They stopped user access to any website that was uncategorized. This created the "perfect storm" the company had feared it would, as user productivity plummeted and help desk calls and tickets skyrocketed.

Frustrated, and with productivity negatively impacted, many users decided to circumvent the new security measures. This situation left the company in even more dangerous waters, as users began taking security into their own hands.

After hearing and then learning about isolation and the Menlo Security Isolation Platform, the company tried it out. They initiated a proof-of-concept (PoC) deployment, and found that Menlo Security's new approach to web security alleviated the need for them to limit employee web access, even for uncategorized websites.

After the company agreed that isolation seemed like the perfect approach to addressing their employee web and malware challenges, cost efficiency would be the determining factor in acquiring the Menlo Security Isolation Platform. And cost justification came down to a simple equation: Weighing the costs of fast-rising and significant time and resource hits the company was incurring for employee device remediation, including device reimaging, responding to nonstop help desk requests, lowered employee productivity, as well as the good chance of still being infected and potentially facing a data breach as employees dodge complex and difficult security mechanisms, against obtaining and deploying the cloud-based Menlo Security Isolation Platform. In the end, the company's costs decreased by deploying the Menlo isolation solution.

PHASE 01
Isolate Risky Websites

The company took a phased approach to isolation. The first step was to isolate risky websites in the Menlo Security cloud-based isolation platform, which immediately eliminated web malware infections. This action alone was particularly helpful to the company, as many uncategorized websites were risky. The isolation of risky websites, especially uncategorized websites, enabled the company to allow employees access to uncategorized websites again, increasing user productivity and satisfaction while decreasing the number of help desk requests, especially for website recategorization.

PHASE 02

Isolate All Email Links

As their second step, the company isolated all links in emails, alleviating malware infections from employees clicking inadvertently or unconsciously on web links in emails—even after being trained not to. The theft of user credentials and other information entered into web forms also ceased, as the company was now able to render web pages in “read-only” format with the Menlo Security Isolation Platform. Plus, visibility into what employees clicked on and the web pages they accessed improved.

PHASE 03

Isolate All Websites

For the last step, the company decided to isolate all websites that employees accessed, initially for high-value internal targets, then for all employees. This ensured complete protection and elimination of infections via web malware.

Conclusion

Isolation 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.

This is one company’s story of how they found that isolation was the best, most cost-effective way to stop an onslaught of help desk requests, increase employee satisfaction with security, and maintain a known, user-accepted experience, while putting an end to web and email attacks, including phishing, credential theft, ransomware, and more. Employee productivity went up, help desk requests went down, user experience was normalized and even enhanced, and employees and their devices were once again safe—all because of isolation. Isolation became an important piece in their modern security architecture.

Menlo
Security

About Menlo Security

Menlo Security protects organizations from cyber-attacks by seeking to eliminate the threat of malware from the web, documents, and email. Menlo Security's cloud-based Isolation Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. Menlo Security is trusted by major global businesses, including Fortune 500 companies and financial services institutions, and backed by General Catalyst, Sutter Hill Ventures, Engineering Capital, Osage University Partners, American Express Ventures, Ericsson Ventures, HSBC, and JP Morgan Chase. Menlo Security is headquartered in Palo Alto, California.

2300 Geng Rd., Ste. 200
Palo Alto, CA 94303
Tel: 650 614 1705
info@menlosecurity.com

menlosecurity.com