Menlo Security

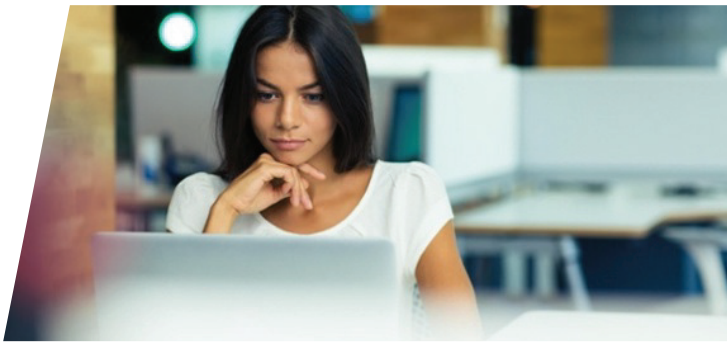
A LOOK AT MENLO SECURITY'S ELASTIC CLOUD

WHITE PAPER

OVERVIEW

Menlo Security set out years ago to transform cybersecurity by defining and building the first truly new approach in web and email security in two decades. We didn't want to create another tool to detect and stop a new type of cyberattack, or another filter to do a better job of denying users access to potentially dangerous websites. Instead, we envisioned a cloud-based platform built around a technology called browser isolation that could keep all web content from reaching users' devices. We focused on two core beliefs. First, we believe in the radical idea that all web content is potentially dangerous. Second, we believe that for companies and their users to employ an isolation platform, it must work without slowing down or negatively impacting user experience and workflow.

We believe that an isolation platform must work without slowing down or negatively impacting user experience and workflow.



That's exactly what the Menlo Security Isolation Platform (MSIP) does. Everything users do with their web browser—from searching the Internet to sending emails to downloading documents—is routed through MSIP, which executes the user's clicks and keystrokes in its cloud-based, isolated browser, and sends back safe visual components to be rendered in the user's web browser on their endpoint device. In other words, Menlo Security—not the enterprise or user—has to deal with the malware, phishing campaigns, and other malicious schemes intended for your unsuspecting users. Rather than infect endpoint devices and web browsers, user activity takes place in disposable virtual containers in the MSIP cloud platform—containers that are "shredded" and emptied at the end of each web session.

It's a simple idea that is rapidly gaining acceptance in the marketplace. According to Gartner, the number of enterprise companies using browser isolation techniques will rise from 1 percent today to 25 percent in 2022.

Yet there is nothing simple about building and operating a cloud-based isolation platform. MSIP is not just software running on a public cloud: It's a thoroughly modern architecture, purpose-built to ensure that users enjoy the same web experience and speed they've always enjoyed. Rather than tie the platform's performance to a Service Level Agreement (SLA) from a public cloud provider, Menlo Security guarantees a higher level of reliability and uptime typically provided only by telecommunications providers and Internet Service Providers (ISPs). Just as you would expect from an ISP like AT&T or Comcast, our service can never go down.

Global Scale, World-Class Redundancy

The Menlo Security Isolation Platform was built from the start to be a multi-tenant, cloud-based environment, able to support millions of concurrent users worldwide. The result is a platform that handles more than 100 million transactions per day with the performance, adaptability, and scalability required by today's enterprise customers. Menlo Security has delivered uptime greater than 99.995 percent. That's on par with large cloud providers, and much greater than the typical web application. Microsoft's SLA guarantees a 99.9 percent uptime for Office 365. That .095 delta between what MSIP has delivered and what is guaranteed in the Microsoft Office 365 SLA is the difference between around eight and a half hours of downtime a year for Microsoft, and around 26 minutes a year for MSIP. The bottom line: Even if a customer's cloud service failed, Menlo Security would still be able to isolate their users' web access and content.

Menlo Security also has scale and global reach. Since our start, we have focused on the needs of large, multinational companies. We now have more than 20 ISO 27001 and SOC2-certified data centers in a dozen of the runtime regions serviced by Amazon Web Services (AWS) around the world, including Northern California; Northern Virginia; Ireland; Frankfurt, Germany; Singapore; Tokyo, Japan; and Sydney, Australia. This geographic breadth allows us to provide anywhere, anytime service to end users, even if they are working remotely or traveling. We employ geo- and latency-based routing to ensure that users experience the lowest potential latency, always connecting them to the fastest point of ingress. We also build out local routing nodes in specific countries or locations to support key customers. While we are not dependent on AWS, we leverage many of its services, including Amazon Elastic Cloud Compute (EC2) and Virtual Private Cloud (VPC) to enable latency-based routing to the nearest region.

Since Menlo Security has targeted large multinational organizations from the start, we have also worked to provide a local experience no matter where users are in the world. If a business traveler shuts down their computer en route from San Francisco to Singapore, for example, they will receive content and restaurant suggestions for Singapore when they reach their destination and relaunch their browser.

Redundancy has been built into every level of the Menlo Security Isolation Platform, from the chips in our servers to the data centers in which they are housed. If there is a service outage in Tokyo, there is another data center ready and able to accept the load without hesitation. We provide transparent and automatic failover between data centers with 99.995% availability.

MSIP provides unlimited capacity elasticity via an automated process that lets customers add users within seconds. This sophisticated process leverages AWS's Auto Scaling to instantiate new instances, as well as other software components for load balancing. The Menlo Security platform was architected to scale horizontally, and includes management and performance analysis tools so customers can add or subtract resources as the load dictates. This means our customers do not need to do any capacity planning or maintain IT staff for handling changes as their web traffic rises or falls.

Secure by Design

MSIP also protects web traffic en route. Web requests normally make many random hops after they leave your organization, exposing your network to unidentified systems that process requests and potentially compromised destination servers that can connect to other sites used by cybercriminals to inject code and malicious traffic into your organization. With Menlo Security, however, users' web requests are routed directly to MSIP, eliminating these dangers.

All MSIP logs are encrypted in transit and cannot be deleted by any tenant. Administrative connections are secured via SHA2/TLS 1.2. Tenant administrative accounts reside in a protected, secured database. Password strength enforcement is strictly enforced on administrative accounts. Only Menlo Security's operations staff may enable tenant administrators. We deliver security updates on a continuous basis, so you are protected as soon as a patch is available.

Our cloud infrastructure allows us to deploy the latest security and feature updates without requiring downtime or any other impact on customers. We also conduct regular vulnerability assessments and penetration testing to ensure the safety of all MSIP components. We offer 24x7x365 support, and incidents are broadcast to multiple channels, including active pager duty.

Redundancy has been built into every level of our solution, from the chips in our servers to the data centers in which they are housed.

No Compromise to User Experience

At the end of the day, what matters most is the combination of enhanced security with no degradation of user experience. Efforts to use isolation technology in the past accomplished neither of these goals. Take virtual desktop infrastructure (VDI), for example. Hundreds of IT shops have tried to simplify and reduce the cost of deploying thousands of devices by running their workloads on centralized servers—ostensibly, also removing the security risks of letting each employee administer their own machine. The reality is frustrating for users, because of slowed network performance and an inferior user experience. Since users are essentially interacting with snapshots of their activity on their screens, they are unable to print to local printers, cut and paste content from one place to another, or see dynamic data on the web—from up-to-the-second stock prices to the most recent changes made to a shared online document.

Menlo Security has solved this problem by developing a patented technology called Adaptive Clientless Rendering (ACR). ACR allows us to safely deliver actual, dynamic web content to users by converting potentially malicious active content, such as Flash and JavaScript, to safe HTML5. Through ACR, we also eliminate any malware that may be hidden in the code used to generate fonts, images, and other website elements in a user's browser, thanks to a technology called Document Object Model (DOM) Mirroring. Using ACR's patented technology, DOM Mirroring mirrors the actual code produced by a web page, including the code used to generate fonts, images, and other web elements, and isolates the actual web code in MSIP disposable virtual containers. This strategy ensures that any malware masked by web page fonts, images, Cascading Style Sheets (CSS), and other web content is stopped in our cloud-based environment and disposed of, so it is never able to reach the user's browser and endpoint device. ACR then transmits the transformed active content and mirrored web code to the browser on the user's endpoint device for rendering, so the web page retains its dynamic nature, interactivity, and look and feel, without any malware or other malicious code. There is nothing in which malware and other web threats can hide. This process is all accomplished using a standard web browser, without additional clients, agents, or plug-ins.

Conclusion

Chances are, you'll be hearing about new entrants in the fast-growing market for isolation technology in the coming months and years. Menlo Security welcomes the competition and the further validation of our efforts as pioneers in this space. We are confident that our Isolation Platform, designed from top to bottom for today's cloud-focused economy, will continue at scale to protect our customers and their users from all web, email, and document threats, without forcing users to put up with a slower, degraded user experience.

There is nothing in which malware and other web threats can hide. This is all accomplished using a standard web browser, without additional clients, agents, or plug-ins.

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