MENLO SECURITY

Migrate from network security appliances to a cloud-based Secure Web Gateway (SWG).

As your users and application workloads move to the cloud, security architectures are adapting to provide complete, seamless protection with an isolation-powered Secure Web Gateway (SWG) on the journey to a fully converged Secure Access Service Edge (SASE) approach.

Solution Brief

Once considered a staple of enterprise security, on-premises web proxies are no longer fit to protect modern work.

The world has changed dramatically since this technology was first introduced, not only in terms of technological implications, but also in how knowledge workers operate today. Users, data, apps, and services are now highly distributed, utilizing services in offices, homes, data centers, and clouds to collaborate and get work done. Internet traffic volume has skyrocketed, with over 200 exabytes of traffic going over the Internet's backbone on a monthly basis. Protecting these rapidly increasing levels of traffic with traditional on-premises web proxies would require companies to deploy additional hardware, resulting in increased IT management and configuration. These physical appliances are expensive and not easily scaled to meet the distributed, mobile nature of work today.

Today's workforce needs fast, secure, and reliable Internet access.

Prior to the COVID-19 pandemic, roughly 20 percent of global employees worked from home occasionally, with an even smaller percentage working from home full time. Once the pandemic struck, forcing many organizations to disperse their workforces and quickly implement work-from-home policies, this percentage drastically changed.

After the pandemic struck, more than 70 percent of the workforce worked from home.[1]

[1] Pew Research Center

Allowing employees to work from anywhere has resulted in a tremendous advantage to organizations from a productivity standpoint; however, a majority of companies weren't prepared for the quick transition that took place. Prior to the pandemic, facilitating a work-from-home policy meant flipping on VPNs to backhaul Internet traffic to corporate headquarters or centralized data centers where security access policies could be applied. But following the work-from-home boom, VPN concentrators could not keep up with the traffic. As a band-aid solution, organizations rapidly deployed split-tunnel VPNs to offload traffic, but the process of acquiring more hardware and building secure local Internet breakouts for the distributed workforce has become costly and burdensome.

Given that the browser is considered the new office today, many organizations have allowed users to connect directly to the Internet without any security controls, dramatically increasing the company's risk posture.

Users spend 75 percent of their workday in a web browser.[2]

In addition to the browser now being considered as the office, cloud and SaaS applications have also seen rapid acceptance and dramatically increased use. The average company currently uses 651 SaaS apps, and for larger organizations that number multiplies exponentially.[3]

The pandemic created the perfect storm from a cyber-risk standpoint, since an expanded attack surface has resulted from the new technology deployed to assist remote workers and the high levels of Internet traffic. To address these challenges, organizations have had to rely on their legacy approaches to security. This legacy technology requires companies to install additional tools from multiple vendors in order to integrate with on-premises web proxies that manage access and controls—from firewalls and anti-virus engines, to data loss prevention (DLP) solutions for reporting and logging for SIEMs. Companies need to put all of these pieces together, creating immense complexity and management burdens from an IT perspective. With this increased complexity, gaps are introduced, and threat actors have taken notice.

[2] Google, "The future of enterprise: Your business, in the browser"

[3] Zylo, "Zylo's 2020 SaaS Management Benchmarks Report"

Online crimes reported to the FBI's IC3 unit have spiked 400 percent since the COVID-19 pandemic began.[4]

As today's modern business and remote workforces have moved to the cloud, the need for fast and secure access to the Internet and mission-critical SaaS applications to keep the business running is clear. It's become evident that legacy on-premises proxies are not equipped to secure the Internet or SaaS applications, or to provide DLP capabilities.

The Menlo Security Secure Web Gateway (SWG) powered by an Isolation Core™ protects productivity.

Using a fundamentally different approach, the Menlo Security Secure Web Gateway (SWG) powered by an Isolation Core™ delivers the capabilities enterprises need to secure work. Menlo Security converges all SWG capabilities into a single cloud-native platform—including CASB, DLP, RBI, Proxy, FWaaS, and Private Access—to provide extensible APIs and a single interface for policy management, reporting, and threat analytics. Additionally, it's the only solution to deliver on the promise of the Secure Access Service Edge (SASE)—by providing the most secure Zero Trust approach to preventing malicious attacks, by making security invisible to end users while they work online, and by removing the operational burden for security teams.

Benefits

✓ **Maintain productivity, with no agents or endpoints to manage.**

✓ **Use with desktop, laptop, and mobile devices.**

✓ **Retain the native end-user experience.**

✓ **Make efficient use of CPU/memory.**

[4] FBI, "2020 Internet Crime Report"

Delivered from a global elastic Cloud-as-a-Service, the Menlo Security SWG powered by an Isolation Core™ allows users to connect securely to the Internet from anywhere business takes them. Enterprises can be assured that they're protected from web-based cyberthreats, and granular access and compliance is ensured across all devices and locations. The Menlo Security SWG does this with unmatched performance and scale—allowing organizations to outsmart known and existing threats as well as unknown and future threats.

The Menlo Security Isolation Core™ assumes that all web content is risky and poses a danger to the organization.

This Zero Trust approach eliminates the need to make an allow-or-block determination based on coarse categorization, filters, and hard-to-explain policies. The Menlo Security SWG allows enterprises to employ an isolation-or-block policy instead, resulting in a truly preventive approach to security, as opposed to the reactive stance that organizations take by focusing on detection and response.

For content that is allowed, Menlo's Adaptive Clientless Rendering™ (ACR) technology efficiently delivers authorized content to the end user's browser with no impact on user experience or productivity, and with no need for special client software or plug-ins. The result is 100 percent confidence in the security posture for security teams, as well as worry-free and productive clicking, downloading, and browsing for end users.

To find out how Menlo Security can help you migrate from legacy on-premises web proxies to an SWG powered by an Isolation Core™, visit menlosecurity.com or contact us at ask@menlosecurity.com.

MENLO
SECURITY

To find out more, contact us:

menlosecurity.com
(650) 695-0695
ask@menlosecurity.com

About Menlo Security

Menlo Security enables organizations to eliminate threats and fully protect productivity with a one-of-a-kind, isolation-powered cloud security platform. It's the only solution to deliver on the promise of cloud security—by providing the most secure Zero Trust approach to preventing malicious attacks; by making security invisible to end users while they work online; and by removing the operational burden for security teams. Now organizations can offer a safe online experience, empowering users to work without worry while they keep the business moving forward.

© 2021 Menlo Security, All Rights Reserved.