PARTNER:
SOLUTION BRIEF

MENLO SECURITY

appgate

Menlo Cloud Security Platform Powered by an Isolation Core™ and Appgate Software-Defined Perimeter (SDP)

Defending Enterprise Access

The challenge

Enterprises need secure access to resources, applications, and workloads. However, some secular trends have increased IT security challenges and the urgency to adapt. First, applications are now deployed everywhere, with more internal apps deployed in the public cloud and outside of the corporate data center. Second, users are globally dispersed. The accelerated adoption of remote work means that users end up relying increasingly on BYOD smartphones, laptops, and other potentially risky or compromised devices to access corporate assets while transiting through insecure public Wi-Fi networks. Third, and more important, well-funded adversaries are more sophisticated with ransomware and other tactics, techniques, and procedures. To enable work-from-anywhere policies securely for a distributed workforce, with connectivity and security as a service from the cloud, enterprises are increasingly implementing a Secure Access Service Edge (SASE) framework.

These trends are driving the demand for secure access to business-critical applications and data as part of a broader movement to detach the corporate network from the data center. Legacy security technologies have largely failed to adapt to these trends, and more important, are expensive to scale and hinder cloud adoption.

Menlo Cloud Security Platform—Powered by an Isolation Core™

The Menlo Cloud Security Platform enables safe viewing of web content and documents by executing all active content in the cloud—away from the endpoint device—while providing a native and seamless user experience. Unlike legacy solutions, the Menlo Cloud Security Platform does not rely on a detect-and-respond approach, but rather on the assumption that all web content is risky and hosts potentially malicious content. This approach eliminates the need to make an "allow or block" determination based on coarse categorization and detailed analysis.

The Menlo Cloud Security Platform instead offers an option to "isolate" potentially risky or uncategorized websites. Once content is isolated, malware-free content is delivered safely and efficiently to the end user's browser, with no impact on user experience or productivity, and without requiring an endpoint agent or browser plug-ins. All active content such as JavaScript and Flash, whether good or bad, is fully executed and contained within the Menlo Security's cloud-based Isolation Core™. This eliminates the possibility of malware ever leaving the isolated web browsing session and infecting the endpoint. This approach restores 100 percent confidence in the security posture and enables security teams to empower worry-free and productive clicking, downloading, and browsing for end users.

The Menlo Cloud Security Platform also gives administrators the ability to set and enforce acceptable use policies to block malicious activity, including file uploads and downloads. Policies can be applied by user, group, file type, or website categorization to determine when content is blocked or rendered in “safe preview” mode.

Appgate SDP

Appgate SDP delivers industry-leading Zero Trust Network Access (ZTNA) to anything from anywhere by anyone. It requires users to be authenticated across a range of identity-centric and context-based parameters—such as role, time, date, location, and device posture—before allowing access to enterprise resources, thus preventing unsanctioned lateral movement.

Appgate SDP secures the network with a software-defined perimeter—a network security model that dynamically creates one-to-one network connections between the user and the resources accessed while leveraging user identity. It delivers the industry’s only identity-centric, network-enforced perimeter.

Menlo Cloud Security Platform Powered by an Isolation Core™ Combined with Appgate SDP

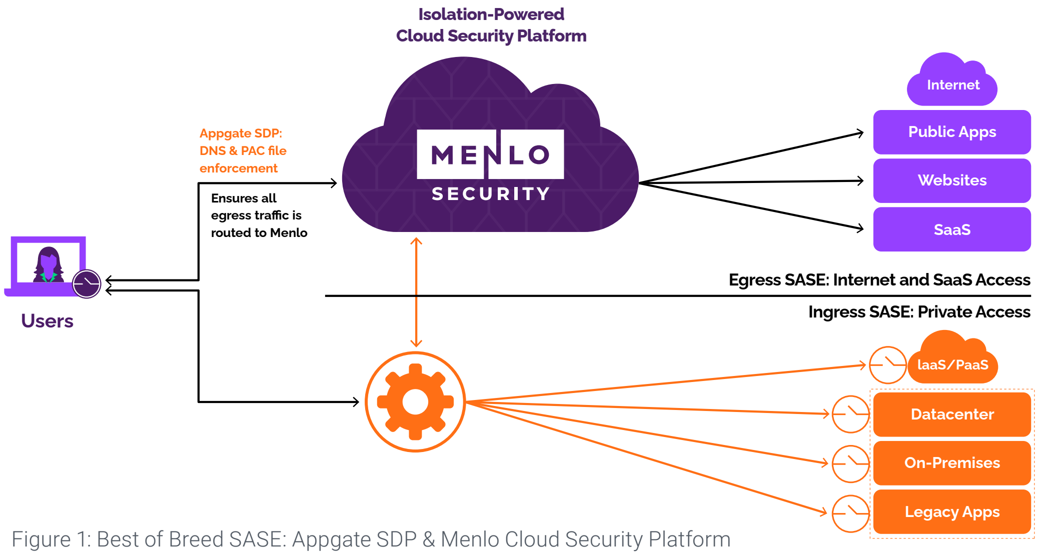

Figure 1: Best of Breed SASE: Appgate SDP & Menlo Cloud Security Platform

The Menlo Cloud Security Platform powered by an Isolation Core™ fuses with Appgate SDP to deliver a comprehensive SASE solution that safeguards access to Internet and cloud applications while providing private access to corporate applications.

The Menlo Cloud Security Platform controls and protects all Internet and SaaS access while the Appgate SDP protects all private access to corporate applications running in public or private clouds. The Appgate SDP provides DNS and the security policy file enforcement to ensure that all egress traffic is routed through the Menlo Cloud Security Platform and is isolated accordingly.

In addition, Appgate SDP securely delivers and enforces Menlo Security policies to all users based on policy and risk, ensuring that no user, attacker, or malware on a compromised device can disable, alter, or remove these settings.

With this integrated offering, enterprises can shift to a high-security SASE framework with industry-leading data and threat protection, allowing users to safely and securely browse the Internet and access SaaS applications and private enterprise resources with one seamless experience.

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.