MENLO SECURITY

Put the security into SASE.

Overcome legacy networking and security limitations to deliver on Zero Trust with an isolation-powered Secure Web Gateway (SWG).

Solution Brief

Today's distributed world needs a new security architecture.

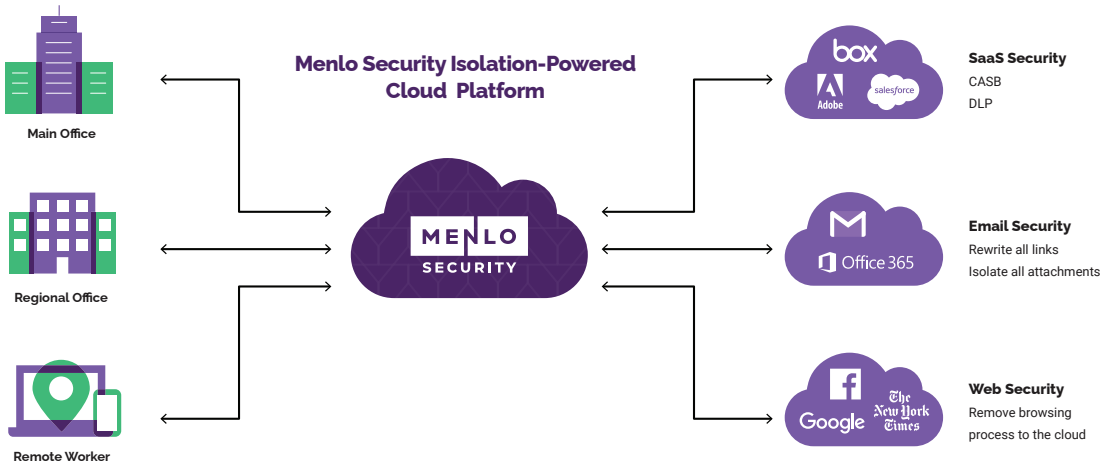
[1]Menlo Security,
"The Future of IT Network Security"

Users, data, apps, and services are now highly distributed, utilizing services in offices, homes, data centers, and clouds to collaborate and get work done. Traditional network and network security infrastructure was built for the old hub-and-spoke model—requiring traffic to be backhauled to the data center where it can be monitored and secured through policies. The latency and bandwidth issues of this legacy approach causes slow performance and limits the productivity of employees slow performance and limit productivity—unacceptable conditions for the modern, competitive business environment.

An overwhelming majority of IT decision makers agree that security needs to support the user experience.[1]

The distributed workforce needs direct, secure Internet access.

Employees today need fast, reliable, and secure access to the tools and information they need to keep business running—wherever they log in from and no matter the underlying infrastructure. However, building a secure local Internet breakout for each user is architecturally impossible. Physical appliances are expensive and not easily scaled to meet the distributed, mobile nature of work today. As a result, many organizations simply allow users to connect directly to the Internet without any security controls, but this puts them (and the organization) at great risk. Malicious actors know this, of course, and are using email and the web as attack vectors with malware, ransomware, and phishing campaigns that target the end device.



A growing percentage of organizations (86 percent) were compromised by at least one attack in 2020.[2]

Once endpoints are compromised, malicious hackers can then spread to the rest of the network, including branch offices, cloud accounts, and the data center.

As Secure Access Service Edge (SASE) convergence continues to mature and evolve, it becomes more evident that security, not connectivity, becomes the critical design point for future architecture decisions. Increased security is needed because:

- More user work is performed off the enterprise network than on the enterprise network.
- More workloads are running in an Infrastructure as a Service (IaaS) platform than in the enterprise data center.
- More applications are consumed via SaaS than from enterprise infrastructure.
- More sensitive data is located outside of the enterprise data center in cloud services than inside.
- More user traffic is destined for public cloud services than the enterprise data center.
- More traffic from branch offices is heading to public clouds than the enterprise data center.

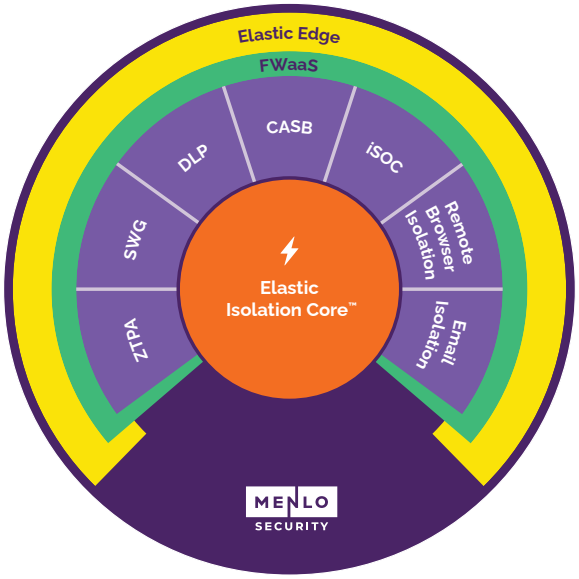
[2] CyberEdge Group, "2021 Cyberthreat Defense Report"

The Menlo Security Secure Web Gateway (SWG) powered by an Isolation Core™ is the most effective approach to eliminate malware as organizations move to a SASE-based architecture.

Menlo Security gives organizations a single framework from which to deliver security and networking services through the cloud to connect distributed users, devices, branch offices, apps, and Software-as-a-Service (SaaS) platforms—regardless of physical location. This allows users to work productively without worrying about whether they are able to securely and seamlessly access the tools and information they need. Menlo Security eliminates threats from malware completely, fully protecting productivity with a one-of-a-kind, isolation-powered Secure Web Gateway (SWG). It's the only solution to deliver on the promise of SASE 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.

[3] Gartner, "2021 Strategic Roadmap for SASE Convergence", Neil MacDonald, Nat Smith, Lawrence Orans, Joe Skorupa, 25 March 2021.

According to Gartner®, "By 2025, at least 60% of enterprises will have explicit strategies and timelines for SASE adoption encompassing user, branch and edge access, up from 10% in 2020."[3]



The Menlo Security SWG powered by an Isolation Core™ ensures that SASE security can be scaled infinitely to reflect organizational growth, dynamic demand, and security needs.

This single framework allows organizations to build their SASE capabilities as they mature through their networking and network security journey. This includes the ability to integrate Zero Trust Network Access (ZTNA), Cloud Access Security Broker (CASB), Secure Web Gateway (SWG), Web Application and API Protection as a Service (WAAPaaS), DNS Security, remote browser isolation, SD-WAN, Cloud DLP, and cloud firewall capabilities directly from Menlo or one of our solution providers.

Benefits

Secure work wherever users do business.

Take a pragmatic, step-by-step approach to implementing SASE capabilities.

Reduce IT overhead typically required to secure remote work.

Completely eliminate malware and other web-based threats without sacrificing user experience.

The multi-cloud world requires users to connect directly to the Internet, SaaS platforms, and other cloud services, but traditional security solutions were built for monolithic applications and the hub-and-spoke networking model. Menlo Security doesn't leave anything to chance. Our extensible security platform—built on a unique Isolation Core™—is the only solution to deliver on the promise of SASE security by:

- Providing the most secure Zero Trust approach to preventing malicious attacks by isolating all Internet traffic.
- Making security invisible to end users while they safely browse, share files, and use email, SaaS, or private applications.
- Removing the operational burden for security operations teams so they can focus on other issues.

Zero Trust principles are at the heart of the SASE convergence journey, and isolation-powered security is at the heart of enabling Zero Trust in the SASE security journey,

To find out how Menlo Security can provide your organization with protection against cyberattacks while giving secure Internet access worldwide, 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.