The ultimate buyer's guide:

Cloud Secure Web Gateway

eBook

MENLO SECURITY

Contents

How users work today

The future of work will be more distributed

Workers will continue using corporate-issued and personal devices within the confines of the network and at places like home and coffee shops, which have less secure WiFi.

9/10

executives envision a hybrid model going forward[1]

20%

of employees fully remote[2]

Where work flows, threats go

80% of employees access the Internet for their job[3]

90% of breaches stem from the Internet[4]

75% of an employee's workday is spent in a browser[5]

Reliance on web-apps is growing

box Office 365

salesforce

Web threats: Sophisticated and successful

Attackers increasingly target users directly after researching them for better results. According to IT decisions makers[6]:

66%

of respondents identify ransomware as their top security concern

57%

consider phishing the biggest threat

52%

are most concerned about malware

[1] https://www.mckinsey.com/business-functions/organization/our-insights/what-executives-are-saying-about-the-future-of-hybrid-work

[2] https://www.weforum.org/agenda/2021/07/work-form-home-hybrid-working-covid-pandemic-us-office/

[3] https://www.statista.com/statistics/1114434/worldwide-adults-with-internet-access-employment/

[4] https://info.menlosecurity.com/Solving-Your-Trust-Issues-with-SASE_webinar.html

[5] https://cloud.google.com/blog/products/chrome-enterprise/chrome-is-helping-it-teams-support-cloud-first-workforce

[6] Enterprise Cybersecurity Plans in a Post-Pandemic World

Working habits are changing

and it's pushing the boundaries of legacy security.

Mobile and distributed users accessing data center applications, web apps, Software-as-a-Service (SaaS) platforms, and websites from outside the perimeter are now the rule, rather than the exception. Full of potential, these new working habits offer tremendous benefits for end-users and for business continuity. Ultimately though, as past and present collide, it creates security sticking points for organizations striving to balance productivity and security while continuing to use traditional on-premise security solutions.

At the beginning of the work-from-home boom, companies flipped on VPNs to backhaul Internet traffic to headquarters or centralized data centers in an attempt to provide secure access to corporate assets. Doing this added latency and sapped bandwidth—creating disruptive performance issues for workers expecting fast, seamless experiences whenever they logged in. As VPN concentrators began failing from the high volume of traffic, organizations defaulted to legacy secure web gateways (SWGs) to manage the expanding attack surface.

Strategically unsuited to protect skyrocketing Internet traffic volumes and remote work, legacy SWGs instead created inefficiencies and required organizations to deploy additional hardware that needed configuration and management.

Cloud data centers aren't helping

Even security and networking vendors are trying to quickly adapt only to uncover scalability and availability challenges. Many have opted to push virtualized remote access, security, and networking appliances into the public cloud, rather than reworking them into a unified cloud-native platform. When functions are compute-intensive, however, they can't run on a cloud provider's numerous content delivery network edge locations, which keeps security further from the already distributed users.

You need radical, not reactive

Legacy cybersecurity solutions use deterministic logic that decides whether websites are safe or not. This binary approach isn't reliable and can introduce security gaps depending on how it categorizes threats. Given the volume and sophistication of websites and malware, this reactive approach has run its course. Even sandboxing and newer artificial intelligence (AI) and machine learning (ML) techniques that vendors claim to automate away problems are fundamentally reactive as they still require human intervention and large amounts of threat data.

Cloud-based Secure Web Gateway:
A modern approach to securing users

Determining which SWG is right for you.

Not every SWG solution works in today's highly-distributed, work-from-anywhere environment. When considering a new SWG, a modern delivery model alone does not guarantee transformation. Instead, it must abandon the detect-and-remediate approach that typically results in threat actors finding new ways to evade detection, steal credentials or infect the endpoint, and spread laterally in the network.

Security should make work better, not worse.

Workers expect freedom while browsing, with access to sites like Facebook and YouTube for personal use. Yet legacy SWGs tend to use blanket Allow/Block policies that keep users from their chosen sites. Even more disruptive, these outdated practices also stop users from accessing a large range of "uncategorized" websites, which may be essential to the lines of business, but could be malicious. When either of these scenarios happen, it often results in an IT ticket—driving up IT costs and frustration for all parties. And in the end, this security doesn't provide protection assurances since users can simply bypass the blockades. For instance, if they are blocked from a website, they may try accessing it from another device where they may come into contact with malicious content that could steal their user credentials.

To maximize digital transformation efforts, consider a SWG which is purpose-built for cloud that can outsmart known, unknown, and future threats, while protecting productivity with these six features and benefits:

Cloud-scalable isolation
1

Secure Access Service Edge (SASE) Compatibility
2

Zero Trust
3

Future proof
4

Invisible security
5

Global and scalable security
6

1 Today's workforce needs a SWG with cloud-scalable isolation

Using a fundamentally different approach, SWGs built on top of cloud-scalable isolation deliver the capabilities enterprises need to achieve secure cloud transformation by ensuring security goes wherever work happens—neutralizing malware before it gets in.

Since it assumes that all web content is risky and poses a danger to the organization, it eliminates the need to make an allow-or-block determination based on traditional categorization, filters, and hard-to-maintain policies. And through a cloud-based platform, IT and security administrators have the ability to centrally configure security and access policies instantly, for every user, offering more granular controls. No matter how many users an organization might have, or how often needs change, isolation automatically scales to meet the needs of the company and its users.

Security end users won't notice

Smooth scrolling, no pixilation, no need to install agent or plug-ins—users operating within an isolation layer will never know a SWG is securing them.

Isolation makes the Internet safe, seamless, and effective for all workers. Stop sacrificing productivity for security—isolate instead.

2 Prepare for future architecture decisions with SASE compatibility

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."[7]

What is SASE? And, how does it improve security?

SASE tightly integrates software-defined wide area networking (SD-WAN) capabilities with network security functions such as secure web gateway (SWG), cloud access security broker (CASB), firewall-as-a-service (FWaaS), and zero trust network access (ZTNA). SASE also integrates with connectivity like 5G to create a framework that supports the dynamic secure access needs of modern organizations looking to secure modern work.

As SASE convergence continues to mature and evolve, organizations are coming to the realization that security, not connectivity, is the critical design point for future architecture decisions.

SASE security models help in several ways:

1. Easy implementation and delivery of security services using cloud-based infrastructure.
2. Minimizes the number of security products IT has to manage, update, and maintain by consolidating the security stack.
3. Removes trust assumptions and provides complete session protection.
4. Prevents unauthorized access and abuse of sensitive data.

Start with cloud-based SWG on your journey to SASE

The vast majority of enterprise SASE adoption will occur over several years, according to Gartner. However, the way we work and its effect on our computing environment and end users has already happened—meaning, most cannot afford to wait to fully adopt a SASE framework. Instead, a cloud-based SWG can be a more manageable starting point, while offering many of the same benefits and setting up for future SASE success. Because of this, when evaluating SWG options, be sure that it fits with your plan to adopt and upgrade to a SASE architecture.

Consider asking if the cloud-based SWG's framework ties in other components in the SASE stack so that you can achieve a unified approach. This includes the ability to integrate:

- Zero Trust Network Access (ZTNA)
- Cloud Access Security Broker (CASB)
- Remote Browser Isolation (RBI)
- Cloud DLP
- Cloud firewall capabilities

With deeper integrations, users can work productively without worrying about whether they are able to securely and seamlessly access the tools and information they need. All while IT teams have access to centralized management, policy creation, and visibility across SASE security components.

[7] Source:Gartner, "2021 Strategic Roadmap for SASE Convergence", Neil MacDonald, Nat Smith, Lawrence Orans, Joe Skorupa, 25 March 2021. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission

3 Zero Trust is a must

What is SASE? And, how does it improve security?

Zero Trust is one of Gartner's foundational elements for SASE. And, also a differentiator of cloud-based SWGs. Its value to the future of cybersecurity has never been as evident as it is now after the White House handed down an imperative to advance towards a Zero Trust approach. Now, as agencies continue to use cloud technology, they must do so in a way that they are able to prevent, detect, assess, and remediate cyber incidents.

The May 12, 2021 briefing clarifies that a Zero Trust approach works to protect against threats both inside and outside traditional network boundaries by eliminating implicit trust, and requires continuous verification from multiple sources to determine access and other system responses.[8] By doing so, it grants users full access, but only for the bare minimum of what they need to perform their job.

Key security for the hybrid workforce

While a Zero Trust approach has sweeping applications, it shines as an essential piece to the hybrid workforce puzzle. Given that Zero Trust considers everything untrusted—including, users, devices, network connections, and data—as workers move about, a consistent security posture follows.

When done right, cloud-based SWGs powered by isolation enables a Zero Trust approach that preserves the native browsing experience for users.

Eliminate the need to "find the bad"

While many vendors claim to have a Zero Trust approach, not all are equal. Be sure to examine how the vendor applies the architecture, and ensure that it:

- Eliminates the need to reactively "find bad" to prevent threats.
- Keeps users in a safe layer away from any potential opportunities for malware to sneak in.
- Operates bi-directionally so that both users and devices, as well as data are considered untrusted.

With deeper integrations, users can work productively without worrying about whether they are able to securely and seamlessly access the tools and information they need. All while IT teams have access to centralized management, policy creation, and visibility across SASE security components.

[8] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

4 Flexibility for what comes next

The future of global work is set to remain distributed, requiring vendors to modernize SWGs appropriately to support the new reality. There are several key factors to consider when choosing a SWG that is flexible enough to meet today's needs and overcome tomorrow's future challenges:

Future proof

While a Zero Trust approach has sweeping applications, it shines as an essential piece to the hybrid workforce puzzle. Given that Zero Trust considers everything untrusted—including, users, devices, network connections, and data—as workers move about, a consistent security posture follows.

Doesn't require rip and replace

A full move to the cloud doesn't happen overnight. Most journeys take years. Be sure that the SWG can work with existing security infrastructure and that when things change in the future, it won't require purchasing additional capabilities.

Secures all users no matter what.

Needing fast, secure, and reliable access will never change. But the people connecting, their locations and networks, and devices are likely to. SWGs should be able to scale up and down rapidly at the flip of a switch without requiring new hardware deployments—assuring enterprises that they're protected from web-based cyberthreats, and that granular access and compliance is consistent across all devices and locations.

Prepares for tomorrow's threats.

The world around us, our workplace, and future attacks are always ebbing and flowing. Cloud-based SWGs should break away from the detect-and-remediate approach and work to ensure that no matter what comes next, protection is there. With isolation and Zero Trust, threats can become increasingly sophisticated, and it will still proactively protect the same as it does today. All without relying on specific threat intel or updated signatures.

5 Invisible security built around the user

Adopting a modern, cloud-based SWG doesn't simply enhance security—it boosts productivity.

Achieve complete security confidence and a positive end-user experience with a modern SWG that offers:

Native, but safe browsing experience for users—Consider implementing a SWG that isolates and preserves the native browsing experience, rather than blocking access. Web browsers should continue to work as intended, without latency, and without requiring client installation or extra hardware. Additionally, users should still have access to common functionalities like completing forms, viewing/downloading documents safely, cutting, copy, pasting, and printing.

A protective layer around users—With a detect-and-remediate approach, by the time you identify an attack, a threat, or an indicator of an attack, the attackers might have already infected the endpoint or started spreading laterally. Rather than responding to the attacks after the fact, cloud SWGs should prevent them from reaching users in the first place. With isolation, users operate with an invisible, protective layer around them as they navigate the web, blocking known, existing, and unknown sophisticated future threats.

Look for web and document isolation features that include:

- ✓ Scalability for all users, not a subset of users.
- ✓ Remote cloud-based browsers that produce safe viewing environments for all active and risky content like JavaScript and Flash.
- ✓ Power-efficient rendering that doesn't use up CPU cycles.
- ✓ Discarding native web content in disposable containers using stateless web sessions.
- ✓ Granular policies to limit web interaction and document access based on file type and user.
- ✓ Safe viewing of documents in the cloud, away from the endpoint.
- ✓ Ability to provide safe, sanitized, high-fidelity original files with the support to print, search, copy/paste, and share on desktop and mobile devices.

A positive experience for all

A SWG's management experience is as important as the user experience. It should allow IT teams to:

Monitor all web traffic—Full inspection of encrypted and non-encrypted web traffic gives security teams visibility into communications between workers and the web-based tools they use, and provides details on threats targeting the organization.

Intelligently limit bandwidth usage—User/group policies allow organizations to intelligently apply bandwidth controls within browser sessions (e.g. limits the video playback resolution), but does not put limits on other aspects of the site, which would degrade the user experience.

6 Global and scalable security

Even full SASE software stacks aren't guaranteed to scale.

When evaluating SWGs, identify options built with a unified SASE software stack to ensure security and network functions share context.

Expanding security coverage to new places where employees work has long been a time-consuming and arduous process. It can take months to identify a vendor, execute a contract, provision hardware, and complete configurations. All the while, work remains open to malicious attacks.

Even as organizations move beyond the corporate datacenter, security roadblocks follow. Organizations, along with networking and security vendors, are finding that providing security everywhere work happens is often highly compute-intensive. With the dispersed nature of work and resources, they are constantly battling issues of latency, while still falling short of security goals.

To be truly global and scalable without degrading performance, today's SWGs have to rework everything into a unified cloud-native platform. And, it must support autoscaling with the least-latency-based routing so that connectivity can happen from anywhere, for all users, and on any device.

Security where your users are at the press of a button.

Users are not in the datacenter, so your security shouldn't be limited to its walls. Make sure that the SWG you choose moves security closer to the edge—where users are. Given that end users are the new perimeter, and workloads and users are in constant flux, coverage has to be elastic enough to scale globally without the same time-consuming process that security teams have previously endured.

Scale around the world through the cloud.

- No provisioning new hardware or virtual machines.
- No additional configurations.
- No new vendors.
- No new contracts.

An easy choice
to protect productivity and outsmart threats

As users, workplaces, and threats continue to change, choosing the right cloud SWG for your organization is an essential business decision. Menlo Security makes it easy.

The Menlo Security SWG powered by an Elastic Isolation Core™ converges all SWG capabilities into a single cloud native platform— including CASB, DLP, RBI, FWaaS, and Private Access—and provides extensible APIs and a single interface for policy management, reporting, and threat analytics.

As the only solution to deliver on the promise of SASE security, Menlo provides 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.

Say good-bye for good to Allow/Block

The Menlo Security SWG allows enterprises to employ an isolate or isolate/read-only policy for all users at all times, resulting in a truly proactive approach to security, as opposed to the reactive stance that organizations take by focusing on detection and remediation. 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.

Flexible deployment options

Menlo protects millions of users on our Cloud Security Platform. To ensure our SWG meets every organization's needs, we offer flexible deployment options, including hosted on-premises or delivered as a cloud service. And, we integrate with existing network infrastructure and support any device so that security fits seamlessly with your architecture and end users.

Eliminate threats completely with Menlo Security

Protect productivity and secure with a one-of-a-kind, isolation-powered security platform that is cloud native, elastic, and extensible.

menlosecurity.com

www.menlosecurity.com

(650) 614 1705 | ask@menlosecurity.com

© 2021 Menlo Security, All RIghts Reserved.

MENLO SECURITY