THE RISE OF HYBRID
SECURE WEB GATEWAY (SWG)

Overview

Malware infections are one of the most dreaded prospects companies face these days. Almost daily we hear about yet another business falling victim to an attack, it seems no one is immune to the enterprise of cybercrime.

A common way malware reaches the organizational network is of course the Internet. This endless gateway to knowledge is an essential tool for today's employees. Unfortunately, it also constitutes an endless attack surface. An unsuspecting visit to a compromised website can easily become the vehicle by which malware can compromise an employee's device. From there, the entire corporate network is at risk, and the potential damage is immense. While this scenario is by no means new, the magnitude, sophistication, and devastation of today's breaches are unprecedented.

The most common security solution for combating Internet-borne malware is the Secure Web Gateway (SWG). Traditionally offered as on-prem appliances, SWG solutions have been migrating to the cloud. But which SWG solution is the right one for you?

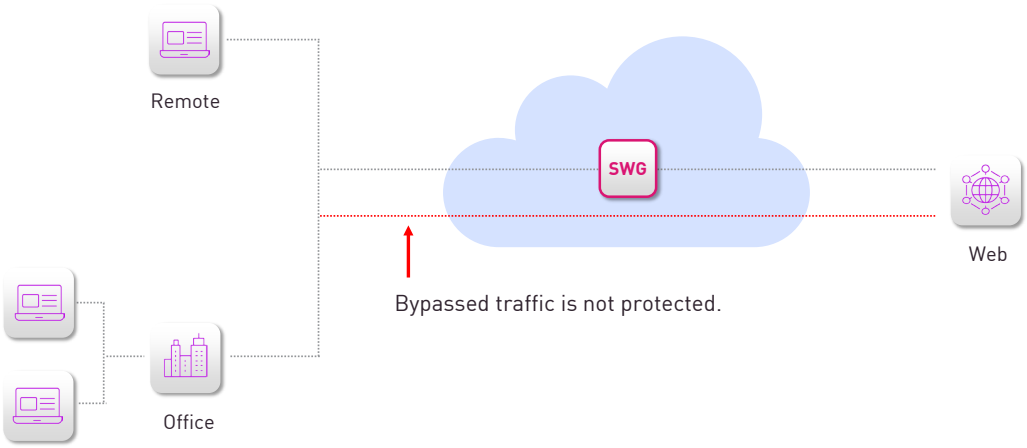
The SWG Dilemma

A cloud-based SWG might seem like the obvious choice. Delivered as a SaaS, it means there are no on-premise deployments, no ongoing maintenance of appliances (software updates, security patches, etc.), a centralized management system and better cross-company visibility into security events. The downside of a cloud-based SWG, however, is that all traffic needs to be routed through it.

For a unified solution that combines remote access (ZTNA, VPN) with a SWG, and possibly other security services, this means all traffic, including web browsing, must pass through the secure remote access tunnel. This can cause congestion and affect performance of critical internal business applications.

In order to avoid this, many companies bypass part of, or all, web traffic from the secure tunnel and send it directly to the Internet (also called split tunneling). What this means is that the bypassed traffic will not be routed through the cloud service and will therefore not be protected by the SWG, leaving an exposed attack surface.

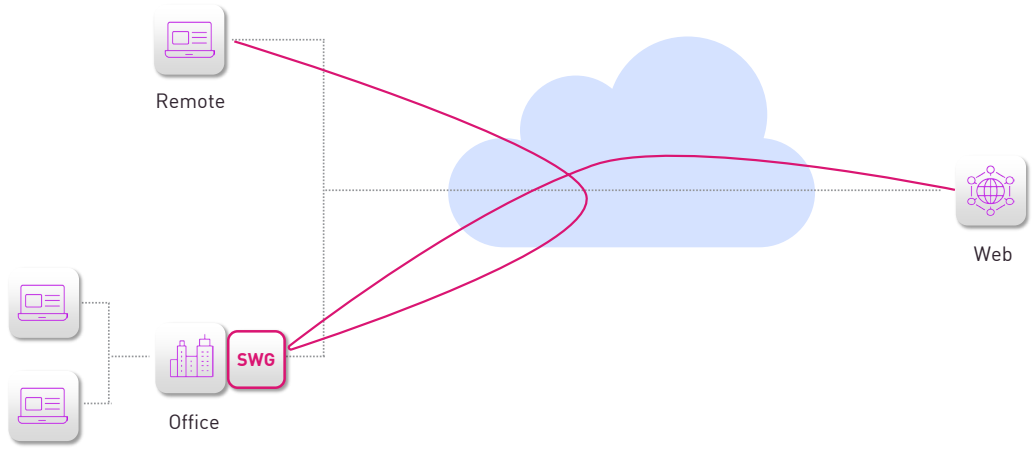
Cloud-based SWG



An additional downside of cloud-based SWGs is that they perform SSL decryption in an uncontrolled environment, essentially performing a man-in-the-middle attack in a potentially insecure datacenter and/or unknown geographic location.

On-prem SWG solutions don't suffer from this blind spot as all traffic is scanned locally, regardless of where it is forwarded to. They do, however, have their drawbacks. Besides the time, cost and effort needed to deploy, manage and maintain them, they require backhauling remote user traffic through an on-prem office or other location where the SWG is deployed. This creates the "trombone effect" which adds latency, impacting user experience and productivity.

On-Prem SWG

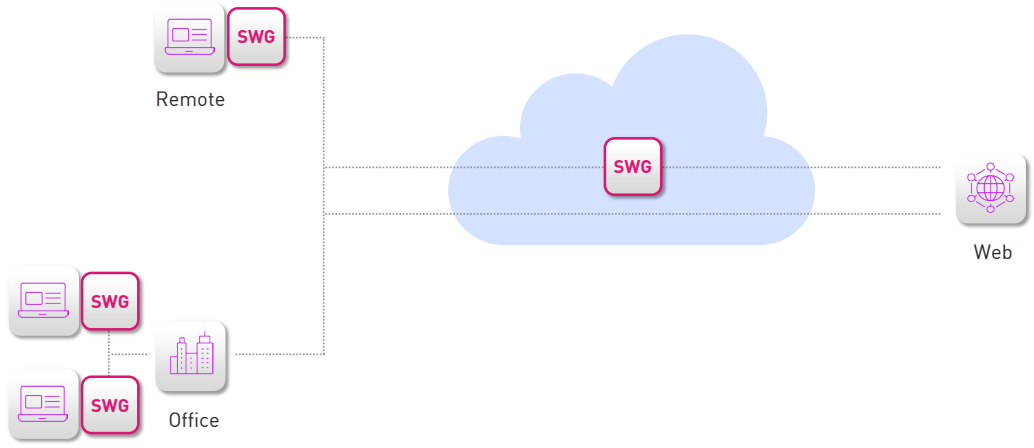


These downsides of on-prem solutions are fueling the SaaS revolution and cloud-first strategy many companies are adopting. But with the shortcomings of cloud-based SWGs, it seems there is no perfect option, just a more tolerable compromise.

Both cloud-based and on-prem SWG implementations have significant shortcomings. There's a need for a better way to deploy SWG.

Introducing Hybrid SWG

Hybrid SWG combines the advantages of cloud-based and on-prem SWGs. It consists of a cloud-based SWG which works in concert with a device-based SWG agent.



Device-Side SWG

Instead of deploying stand-alone SWG appliances in office locations, the SWG agent is deployed on the employee's device itself. This means employees are always protected, no matter where they connect from — office, home, coffee shop or anywhere else — without the need to backhaul traffic through an on-prem location.

It also means employees are protected even when not connected to the corporate network or when traffic is bypassed (split tunnel). The device-side SWG doesn't require any on-prem hardware or VM installations. The agent is easily deployed on employee devices and is centrally managed across the entire workforce. Additionally, SSL inspection is performed on the device itself, without the need to decrypt traffic at a remote, uncontrolled location.

Cloud-Side SWG

The cloud-side SWG provides all the benefits of a cloud-based SaaS solution, it requires no hardware deployment or maintenance and is managed via a single-pane-of-glass console. It is an additional layer of protection for traffic passing through the corporate network. It enables enforcement of consistent, network-wide policies which do not depend on specific user or group definitions. For example, blocking access to known malicious sites. When defined on the cloud-side SWG, this rule will always be applied regardless of the device-side SWG settings.

The cloud-side SWG enables organizations to apply stricter policies for when users are "at work" (i.e. connected to the corporate network). For example, blocking access to social networks (e.g. Facebook) to improve productivity, or blocking access to gambling or hate websites to reduce the risk of employee misconduct and possible liability for the organization. It also enables public WiFi protection by encrypting all communication between the user device to the cloud SWG.

The cloud-side SWG also provides protection in cases where the device-side SWG is not used. This can be due to a specific organization's preference, for example, or due to an unsupported device. As long as a user is connected to the corporate network, they are protected. Organizations can also choose not to work with the cloud-side SWG and only use the client-side SWG. Hybrid SWG provides complete flexibility in deploying either option or both in tandem.

Hybrid SWG—The Best of All Worlds

Hybrid SWG is a unique offering from Harmony SASE. It is the result of feedback from IT professionals across the industry about the limitations of existing SWG solutions and the pain points they create for them.

It eliminates all the major drawbacks traditional cloud SWGs and on-prem appliance SWGs suffer from, and enables organizations to benefit from a higher level of security, improved compliance, better performance and simplified operations.

Harmony SASE's Hybrid SWG advantages:

- Protects user traffic, even when not connected to the corporate network
- Protects bypassed traffic (split tunneling)
- Managed from a single-pane-of-glass (both device and cloud SWG instances)
- No decryption of traffic outside the user's device
- Enables secure and fast direct-to-Internet connectivity
- Flexible policy settings (e.g. "at work")
- Flexible deployment models (device and/or cloud-side)
- Enables multiple networks deployments with network-specific SWG policies
- No on-prem deployment, management or maintenance
- Secures public WiFi connections

Harmony SASE 's Hybrid SWG puts an end to the SWG dilemma and delivers a solution that doesn't require organizations to compromise on security or performance and is simple to deploy and manage. It can be deployed as a stand-alone solution or as part of Harmony SASE 's converged network security platform which includes additional services such as ZTNA and FWaaS.

SWG Deployment Comparison

	On-prem SWG	Cloud SWG	Hybrid SWG
No on-prem appliance deployment and maintenance	✗	✓	✓
Avoids backhauling remote user traffic	✗	✓	✓
Centrally managed from a single console	✗	✓	✓
Direct-to-website connection	✓	✗	✓
Protects bypassed traffic (split tunnel)	✓	✗	✓
Performs SSL decryption in trusted location	✓	✗	✓
Protects users when no connected to the corporate network	✗	✗	✓
Differentiated policies for "at work" vs "off work"	✗	✗	✓

Meet Harmony SASE

2x Faster Internet Access | Full Mesh Private Access | Secure SD-WAN

Offering a game-changing alternative, Harmony SASE delivers 2x faster internet security combined with full mesh Zero Trust Access and optimized SD-WAN performance— all with an emphasis on ease-of-use and streamlined management.

Combining innovative on-device and cloud- delivered network protections, Harmony SASE offers a local browsing experience with tighter security and privacy, and an identity-centric zero trust access policy that accommodates everyone: employees, BYOD and third parties. Its SD-WAN solution unifies industry-leading threat prevention with optimized connectivity, automated steering for over 10,000 applications and seamless link failover for uninterrupted web conferencing.

Harmony SASE enables any business to build a secure corporate network over a private global backbone in less than an hour. The service is managed from a unified console and is backed by an award-winning global support team that has you covered 24/7.

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391

www.checkpoint.com