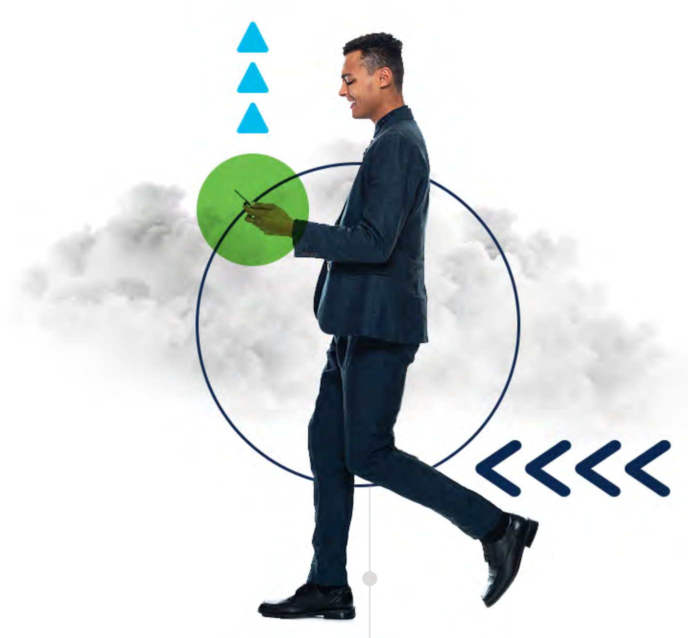
Cisco Umbrella

The traditional SWG is out – what's taking its place?

Secure web gateways are crucial to protecting your organization from web-based threats, but are traditional SWGs still up to the challenge?

Explore the ins and outs of today's evolving security landscape – and how a modern, cloud-delivered secure web gateway can fit into your infrastructure.



What challenges is your SWG facing?

Out Traditional, on-premises, appliance-based SWGs are starting to show their age.

- **Increased complexity** – Pieced together from multiple point solutions
- **Low scalability** – Unable to secure every location and user
- **Incomplete visibility** – Can't track threats across all web traffic and apps
- **Inconsistent protection** – Varying degrees of security and policy enforcement across locations and users

In The time has come for a modern SWG – one that can keep up with today's evolving trends.

- **Cloud-based SaaS apps** are increasingly used to drive productivity – today's SWG protects users from the risks that can come from using unauthorized apps.
- **Direct internet access** offers improved performance for remote and branch workers – with 79% of orgs shifting to DIA, the modern SWG ensures these users are protected everywhere.[1]
- **Encrypted traffic** ensures users are better protected from threats – today's SWG decrypts this traffic without putting a strain on hardware or performance.

Is your org satisfied with your SWG?

Out Even though most organizations are already using a secure web gateway, the many challenges and downsides of traditional SWGs are leaving them dissatisfied with the results.

84% of organizations currently have an SWG deployed.[2]

<10% of SWG users are very satisfied with their SWG.[2]

In Today's SWG offers significant upgrades, providing a new caliber of protection – and a new level of user satisfaction.

Unifying security and networking functionality, the modern SWG is delivered as part of a multifunction cloud service. As a result, it can offer:

- Granular control and visibility – available from a single console
- Robust threat intelligence shared across security services
- Enriched context on threats – and the ability to sandbox them as needed
- Automated protection – for fewer threats and fewer alerts to manage

What features does your SWG need?

Out Although they do offer some basic security capabilities, traditional SWGs are increasingly seen as limited in the features and functionality they offer.

These limitations include:

- Limited protection against evasive malware and advanced threats
- Difficulties protecting users off network
- Susceptibility to shadow IT
- Inability to inspect encrypted web traffic
- Complex tunnel management

67% of cybersecurity experts believe their org will replace proxies on corporate networks with cloud-based alternatives.[3]

In The modern SWG builds on the core functionality of the SWG with advanced architecture and networking integration features.

- Full URL logging and reporting
- Multilevel content control
- Antivirus/malware scanning
- Full or selective decryption
- File sandboxing
- Application visibility and granular control
- Tenant restrictions
- Multiple traffic redirection methods

+

Scalable cloud-native architecture for rapid deployment, simple configuration, optimal performance, and immediate scalability

Automated SD-WAN integration to efficiently route and secure all web traffic across every location using DIA

Efficient container and microservices format for faster development and greater service flexibility

Is your SWG on the outs?

As you consider your current SWG, ask yourself:

- Do you find it difficult to detect and block multiple threats?
- Is scaling protection across every location and user a challenge?
- Do you struggle to secure SaaS apps, DIA, and encrypted traffic?
- Is your SWG impacting user performance?
- Are you juggling multiple point security systems?

If you find yourself answering yes to these questions, it may be time to say out with the old and in with a new, more modern SWG.

Learn how to take your SWG from out to in.

Read ebook

References

1. ESG Survey Results, Market Dynamics Impacting Remote and Roaming User Security Requirements, January 2019.
2. ESG Survey Results, Transitioning Network Security Controls to the Cloud: The Emergence of Elastic Cloud Gateways, May 2020
3. ESG Report, The Rise of Direct Internet Access (DIA): Securing Remote Users and Branch Offices, May 2019

Cisco Umbrella