Cisco Umbrella

Is your organization ready for

the next level in threat protection?

Securing the cloud has never been more critical. Which means now may be the time to consider migrating from your DNS-layer security solution to a secure internet gateway (SIG) package.

SIG:

The next level in cloud-based security and protection

SIG consolidates critical security functions into a single, cloud-delivered service, making it easy to protect your users, apps and data – both on and off your network.

Is it time to move to SIG?

This checklist can help you decide if your current DNS-layer solution sufficiently meets your security needs, or if now may be time to upgrade to a SIG package.

	yes	no
Could you benefit from a more granular level of network visibility than your current DNS-layer protection offers? Cisco Umbrella SIG, as part of a SASE architecture, lets you easily view all of the apps currently running across your entire network – and see precisely who's using them – to enhance user and data security.	○	○
Do you need greater oversight over large groups of end users dispersed across many different locations? Cisco Umbrella SIG makes it easy to deploy and manage your security environment over thousands of remote sites. You can customize and assign security policies based on the level of protection and visibility needed – all from one consolidated dashboard.	○	○
Do you need full URL visibility? Cisco Umbrella SIG provides a cloud-based full proxy that can log and inspect all of your web traffic for greater transparency, control, and protection. Filter content by category – or even specific URLs – to block destinations that violate company policies or compliance regulations.	○	○
Do you currently use Cisco AnyConnect along with DNS-layer security? If you're already using AnyConnect, Cisco makes it easy to add secure web gateway (SWG) functionality to see and inspect all of your web connections. Unlike DNS-layer protection, Cisco's web proxy sees and inspects all files and the full URLs to offer you a higher level of control.	○	○
Does your organization rely heavily on SaaS applications? The cloud access security broker (CASB) in Cisco Umbrella SIG allows you to control which SaaS applications individual users or groups can access.	○	○
Is your organization regularly handling high volumes of sensitive data? Cisco Umbrella SIG data loss prevention (DLP) analyzes data in-line to provide better visibility and control over your outbound web traffic, blocking sensitive data from leaving your organization.	○	○
Do you need to control your Internet bandwidth by site, category, or user? Cisco Umbrella SIG lets you control which types or categories of websites end users can access. It's easy to monitor which websites are most bandwidth-intensive so you can then block problem content, freeing up bandwidth and improving overall network performance.	○	○

What's the verdict?

If you answered "yes" to any of the above questions, consider an upgrade to the Cisco Umbrella **Secure Internet Gateway (SIG) Essentials package.**

DNS-layer security **only** vs. SIG

AV-TEST recently evaluated the efficacy of DNS-layer security solutions against secure web gateway packages from five leading vendors. See how Cisco Umbrella SIG performed versus its DNS-layer offering – and how both stacked up against the competition.

Get the report

Cisco Umbrella