Cisco Umbrella

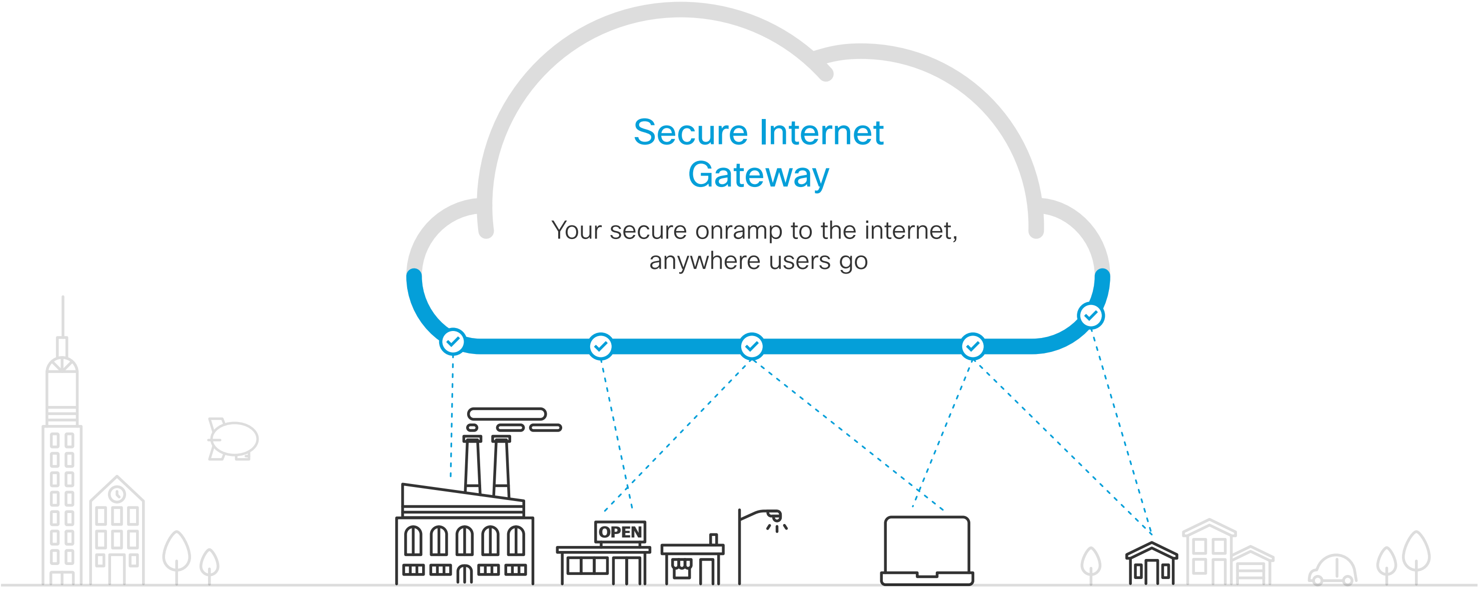
Buyer’s Guide: 10 things to look for in a Secure Internet Gateway

As networks become more decentralized and users connect directly to SaaS applications, security must also shift to the cloud. A new category of products is emerging to address these changes, the Secure Internet Gateway (SIG).

A SIG provides safe access to the internet anywhere users go, even when they are off the VPN. Before you connect to any destination, a SIG acts as your secure onramp to the internet and provides the first line of defense and inspection. Regardless of where users are located or what they’re trying to connect to, traffic goes through the SIG first. Once the traffic gets to the SIG cloud platform, there are different types of inspection and policy enforcement that can happen. As more security controls move to the cloud, a SIG provides a platform that future capabilities can be built upon.

Learn more

cs.co/SIGwhitepaper

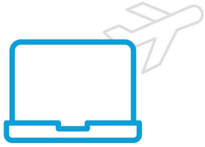


Secure Internet Gateway Capabilities

Here are the key capabilities buyers should look for in a SIG:

1 Visibility and enforcement everywhere

A SIG must provide a complete view into internet activity, anywhere users are located. A SIG protects users no matter what network they connect to – even when they are off the VPN.



Cisco Umbrella protects every device (managed or unmanaged) on your network – even mobile phones and Internet of Things (IoT) devices. Easily protect off-network laptops, using our integration with Cisco AnyConnect (no additional agents required) or a lightweight roaming client (cs.co/RoamingClient).

2 Cloud-delivered security platform

The benefits and capabilities that a SIG provides can only be achieved when the platform is entirely built and delivered via the cloud. A SIG must also provide a comprehensive, yet simple way to get all traffic to the cloud platform for analysis.

With Umbrella, there's no hardware to deploy or software to maintain, and it can scale to meet the needs of any organization. Umbrella uses DNS – a foundational component of how the internet works – as the main mechanism to get all internet requests to the cloud. Umbrella also has tight integration with Cisco endpoint and network products (AnyConnect, ISR, Wireless LAN Controllers, etc.) to make it even easier. Additionally, with the Cisco Security Connector app, you can use the Umbrella extension to protect supervised iOS 11 devices.

3 Protection against threats over all ports and protocols

With comprehensive coverage over every protocol and port, a SIG is able to protect against a broader range of attacks.

By using DNS, Umbrella stops threats over all ports and protocols – not just web ports 80 and 443 like a traditional web proxy. The DNS request becomes the very first point at which Umbrella enforces security, by determining whether the domain or IP is legitimate or malicious.

4 Proxy-based inspection of web traffic and files

A SIG must have a cloud proxy to be able to more deeply inspect web traffic, especially for requests to risky sites. The proxy should be built using the latest technology and offer the ability to inspect files using antivirus (AV) engines and behavioral sandboxing.

With the Umbrella intelligent proxy, only requests to risky domains (those hosting malicious and legitimate content) are proxied for deeper inspection – removing performance impacts felt by traditional proxies. Our proxy was built using a microservices architecture that automatically scales for better performance, and we check files against AV engines and Cisco Advanced Malware Protection file reputation services (http://cs.co/IntelligentProxy).

5 Open platform to integrate with your existing security stack

A SIG must be built as an open platform that can integrate and share intelligence and event data with other systems. To better defend against today's threats, you need the ability to share information automatically between systems, and a SIG should be able to extend protection beyond the perimeter and help amplify investments you've already made.

Umbrella was built with a bidirectional API to easily integrate with existing systems including security appliances, intelligence platforms or feeds, and custom, in-house tools. Using our API, you can send local intelligence into Umbrella and enforce it globally within minutes. You can also query our threat intelligence using the Cisco Umbrella Investigate API and enrich security event data in your SIEM or other systems.

6 Discovery and control for SaaS apps

Cloud Access Security Brokers (CASB) solutions protect the usage of data and applications in the cloud. A SIG should work together with a CASB to provide more comprehensive visibility and control of SaaS apps.

Umbrella works directly with Cisco Cloudlock to provide visibility into and to control the use of sanctioned and unsanctioned SaaS apps. For example, Cloudlock helps control data usage for sanctioned apps, and Umbrella can uncover unsanctioned SaaS apps being used by employees and can be used to prevent access to those apps if needed. Together, Umbrella and Cloudlock protect your users, data, and infrastructure wherever they are.

7 Live threat intelligence

A SIG stays one step ahead of traditional security methods by uncovering attacks before they are executed. A SIG accomplishes this by using live threat intelligence derived from global internet activity that's analyzed in real-time, with updates enforced within minutes. Not only does a SIG enforce protection based on this intelligence, but it should also enable you to access the intelligence though a web-based console or API.

Umbrella sees the relationships between malware, URLs, domains, IPs, and networks across the internet. Umbrella analyzes internet activity patterns from more than 120 billion DNS requests from 85 million users worldwide every day and automatically identifies infrastructure being staged for the next attack using a combination of statistical and machine learning models and human intelligence. Then, Umbrella proactively blocks your users from these threats before a connection is ever made or a file is ever downloaded.

8 Easy to deploy and manage

A SIG must provide a comprehensive, yet simple way to get all traffic to the cloud platform for analysis. And it should be done without requiring complex deployments with VPNs, GRE or IPSec tunnels, and PAC files. Deployment should be simple and ongoing management should be minimal.

Deploying Umbrella is quick and painless. It's as simple as changing a configuration on your network to start pointing DNS to the Umbrella global network, so you can start protecting users enterprise-wide in minutes.

Not convinced? Sign up for a free trial and see for yourself: signup.umbrella.com

If your organization has 1000+ users, you're qualified for the Umbrella Security Report, which provides a detailed post-trial analysis

9 Non-intrusive to users

A SIG keeps users protected without affecting how they get work done. Threats are blocked automatically without impacting connection speeds or device performance.

Umbrella is always on, always protecting, without action required from end users. They won't experience slow or broken connections with Umbrella or memory impacts on their devices. In fact, many even see performance improvements when accessing the internet.

10 Fast, reliable cloud infrastructure

Not only do you need protection everywhere, but it also has to be reliable. A SIG must not only be built in the cloud, but on cloud infrastructure that provides rock solid and fast service.

100% UPTIME

Umbrella is built on a global network of 25 datacenters co-located with the largest internet exchange points around the world and has maintained 100% uptime since launching in 2006. Umbrella uses Anycast routing – every data center announces the same IP address, so requests are transparently sent to the fastest available with automated failover. And, Umbrella has more than 500 peering partnerships with ISPs and CDNs that provide shortcuts between every network, which boosts internet connectivity.