Trend:

More organizations are using a Secure Internet Gateway for secure access.

What if you could provide workers with safe access to the internet – no matter what device they're using or where they're located, even if they aren't on the VPN? A Secure Internet Gateway (SIG) provides just that. No wonder it's gaining traction.

Cisco and ESG surveyed 450 cybersecurity professionals to understand technology consumption patterns and validate market trends. This security readout provides a unique look at the trends impacting remote and roaming user security.

How secure is your onramp to the internet?

In the face of expanding threats and growing numbers of remote workers, many IT professionals turn to more security tools, hoping it will all add up to better protection.

But that standalone, siloed approach is no longer effective at helping burdened security teams dig themselves out from constant alerts, and prioritize remediation efforts across distributed networks and branch offices.

Today, security leaders need to find ways to give users back their freedom while still protecting sensitive data. A Secure Internet Gateway (SIG) is a cloud-based security platform that delivers performance, flexibility, and security for users anywhere they access the internet or cloud apps.

What is a Secure Internet Gateway (SIG)?

A Secure Internet Gateway (SIG) acts as a secure onramp to the internet, providing safe access anywhere users go, even off the VPN. Before a user connects to any destination, a SIG delivers the first line of defense and inspection. Its policies can be tuned to specific devices, users, and locations, to protect and proxy communication between a user and any service – whether they are at the branch office, headquarters or roaming. Plus, it integrates with your existing security stack to extend protection beyond the perimeter.

Why SIG, and why now?

Hackers don't discriminate across industries or geographies. A startling 66% of organizations have experienced or are currently battling targeted attacks.[1] Every company is at risk – and security leaders know that traditional controls simply aren't working anymore.

Enter the Secure Internet Gateway. It protects against threats before they ever reach your network or endpoints. Instead of chasing attacks that are already inside the system, a SIG prevents them from getting in.

A SIG enables better protection, central management, and operational efficiency. 87% of organizations agree that SIG platforms would protect remote and branch offices and roaming users effectively[2] – something every business wants.

What's driving SIG adoption?

The need for a Secure Internet Gateway is driven by the growing need for better security efficacy, operational efficiency, and improved performance.

31%

to mitigate risk & improve security posture.[3]

26%

to enable policy management, configuration management, and reporting for security across all remote offices/branch offices and roaming users.[4]

25%

to achieve better performance and end-user satisfaction.[5]

A SIG keeps users safe anytime, anywhere

Networks are becoming decentralized. More people are using cloud-based apps and services to work on proprietary documents and data. That's why a SIG is particularly effective – it goes where IT can't, without restricting user access or freedom.

For distributed enterprises with remote workers and branch offices, a SIG is a huge asset. When workers are off the company network, logged into a personal or new device, or simply subverting the VPN, SIG still keeps them safe.

SIG and Remote and branch office: Better together

1 **Helps you discover and control SaaS apps**
Shadow IT – when employees use personal or unauthorized apps – is less scary when you have full visibility. Use a SIG that offers cloud application and blocking, like Cloud Access Security Brokers capabilities, to protect the use of data and applications in the cloud. Visibility gives you the power to intelligently manage cloud usage and make decisions rooted in data to optimize productivity, minimize expenses, and reduce risk.

2 **Integrates security functions for better management**
With a SIG, you reduce complexity, security alerts, and noise from multiple disparate systems to better secure users, devices, and apps across the business. By unifying your security stack across functions (SWG, firewall, CASB, DNS-layer) you gain centralized visibility. This makes SIG platforms ideal for organizations with large populations of branch offices and remote workers that need more effective protection, for all users and all networks, against malware.

3 **Doesn't interrupt users or their workflow**
A SIG doesn't stand in the way of worker productivity – in fact, it's just the opposite. It works automatically, so remote employees can get their jobs done, wherever they are, without worrying about slow or broken connections or performance issues. If implemented correctly, it should improve network performance and feel seamless to the end user.

5 things you need in a Security Internet Gateway solution

The benefits of a SIG are undeniable, but it's not enough to invest in just any solution. As you're evaluating options, make sure to choose one that will deliver on everything you need.

Look for these components

A Secure Internet Gateway should provide a combination of DNS-layer security plus web gateway, firewall, and CASB functionality – all in a unified platform. It should deliver the flexibility, integrations, threat intelligence, and speed required to secure internet use in any distributed organization.

With a SIG, you can deliver that secure onramp to the internet for your employees wherever they are, while gaining visibility, control, and protection – all the must-have's for modern security teams.

Make sure it provides these 5 things:

1 **Advanced visibility and enforcement.** Get a complete view into internet activity, no matter where your users are located, and block threats before they become attacks. This will help your users stay safe on any network, anytime, on any device.

2 **Centralized management.** With centralized management, strained resources are better able to manage policies, see trends, and defend against threats.

3 **Comprehensive threat protection.** Protect your users with comprehensive coverage over every protocol and port. No matter what threats are lurking, SIG keeps everyone safer.

4 **Proxy-based web traffic and file inspection.** A cloud-delivered full proxy deeply inspects and scans all web traffic for greater transparency, control, and protection from malware and other threats. Advanced content filtering helps with policy enforcement and compliance challenges.

5 **An open platform for integration with your existing stack.** The right SIG is built as an open platform that seamlessly integrates and shares intelligence with other systems, reducing overhead and improving incident investigations and remediation tasks. Organizations need a highly reliable solution when integrating key functions to prevent a choke point.

Sources:
1-5. ESG Research Insights Report, *The Rise of Direct Internet Access (DIA): Securing Remote Users and Branch Offices,* May 2019

Solution:

Cisco Umbrella

As your perimeter expands with more roaming employees and branch offices, so does your attack surface. Cisco Umbrella offers effective protection for your users, no matter where they are working. Now you can give your employees the freedom to work wherever and whenever they want without putting your business at risk.

Cisco and ESG surveyed 450 cybersecurity professionals to understand technology consumption patterns and validate market trends. Combined with exclusive threat data made available through Cisco Talos Intelligence Group, this security readout provides a unique look at the trends impacting remote and roaming user security.

When it comes to security, Umbrella has you covered

Cisco Umbrella is a cloud security platform that provides the first line of defense against virtual threats, wherever users go. Because it's built into the foundation of the internet, Umbrella delivers complete visibility into internet activity across all locations, devices, and users. It allows you to take a proactive stance against attackers, instead of chasing them down once they're already inside your system.

> "Umbrella enables us to allow branches to access the internet locally and securely instead of being backhauled to the datacenter."
>
> — **IT Director, Medium Enterprise Professional Services Company**

Umbrella uses the internet's infrastructure to deliver complete visibility into internet activity across all locations, devices, and users. It can help you see and block threats before they ever reach your network or endpoints, reducing the number of malware infections your team needs to review and respond to.

With Cisco Umbrella, you get 5 big advantages:

Complete visibility, complete threat protection.
See and protect on-the-go users, on all devices, in every location. Proactively block connections to malicious destinations at the DNS and IP layers.

Superior, predictive intelligence.
Uncover attacks before they infiltrate your system, with live threat intelligence, statistical and machine learning models, and human intelligence.

Smart integration.
Pair Umbrella with your existing security tools to make the most out of your investments. With an open platform and APIs, sharing data and extending protection is simplified.

Easy, quick deployment.
Since Cisco Umbrella is built in the cloud, there's no hardware to install, and no software to maintain. Now you can leverage your existing Cisco footprint – Cisco AnyConnect, Cisco routers, Meraki, SD-WAN and more – to provision thousands of network devices and laptops in minutes.

Fast, reliable infrastructure.
With Anycast routing, requests are transparently sent to the fastest datacenter available with automated failover. And with more than 800 peering partnerships with ISPs and CDNs, we resolve requests faster, boosting network performance.

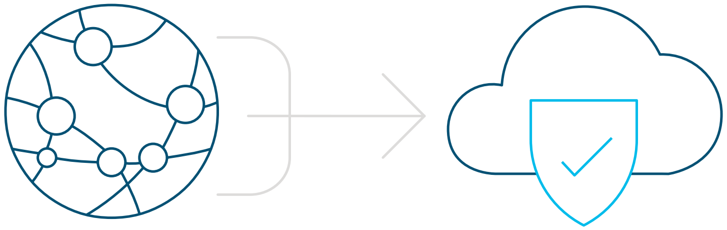
> "Umbrella gives us a consistent user experience across all locations globally. We have 40+ locations and users get the same experience regardless of location."
>
> — **Senior IT Manager, Large Enterprise Industrial Manufacturing Company**

Protection that's as seamless and flexible as today's work environments

Better security and performance for branch & remote workers

With the increasing adoption of SD-WAN, more and more offices and remote workers are connecting directly to the internet – creating a huge security risk. Cisco Umbrella enables you to secure your SD-WAN in minutes, protecting all devices, locations, and users, even if they're off VPN.

Simply point your DNS to the Umbrella global network to protect any device that joins your network. No added latency, and no hassle for your employees. You no longer have to worry when users roam, because your network will stay secure.



Expose Shadow IT once and for all

When you can see what's happening across your organization, you can take steps to protect it. Umbrella allows you to discover which SaaS apps are being used, who's using them, and what risks they pose to your organization. You'll gain full visibility into Shadow IT activity – and the ability to block apps and secure users, even when they're roaming.

> "I think Cisco Umbrella's biggest strength is providing clarity on what applications and services our clients are trying to connect with – and making it a simple process to approve or deny access to those services."
>
> — **Nick Currie, Network Administrator, ABN Group (VIC) PTY LTD**

A new approach means no more playing defense

Don’t wait for threats to strike first

As threat risks continue to escalate, Cisco Umbrella turns you into a proactive defender. It maps internet activity patterns and learns from past behavior, actively processing and enforcing more than 7 million unique malicious domains and IPs concurrently at the DNS layer. Every day, it adds 60,000+ new destinations to its block list. With this massive reach and volume, Umbrella allows you to identify, understand, and block threats even faster.

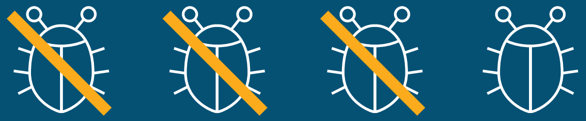
> “With Umbrella, the risk of security breaches is less likely and mitigated across our user base. The solution allowed us to utilize broadband internet local at the branch which improved internet access speeds without compromising security.”
>
> — **IT Director, Medium Enterprise Professional Services Company**

7million

unique malicious domains and IPs blocked daily.

In a recent survey

More than half of respondents saw a reduction in malware infections by 75% or more[1]

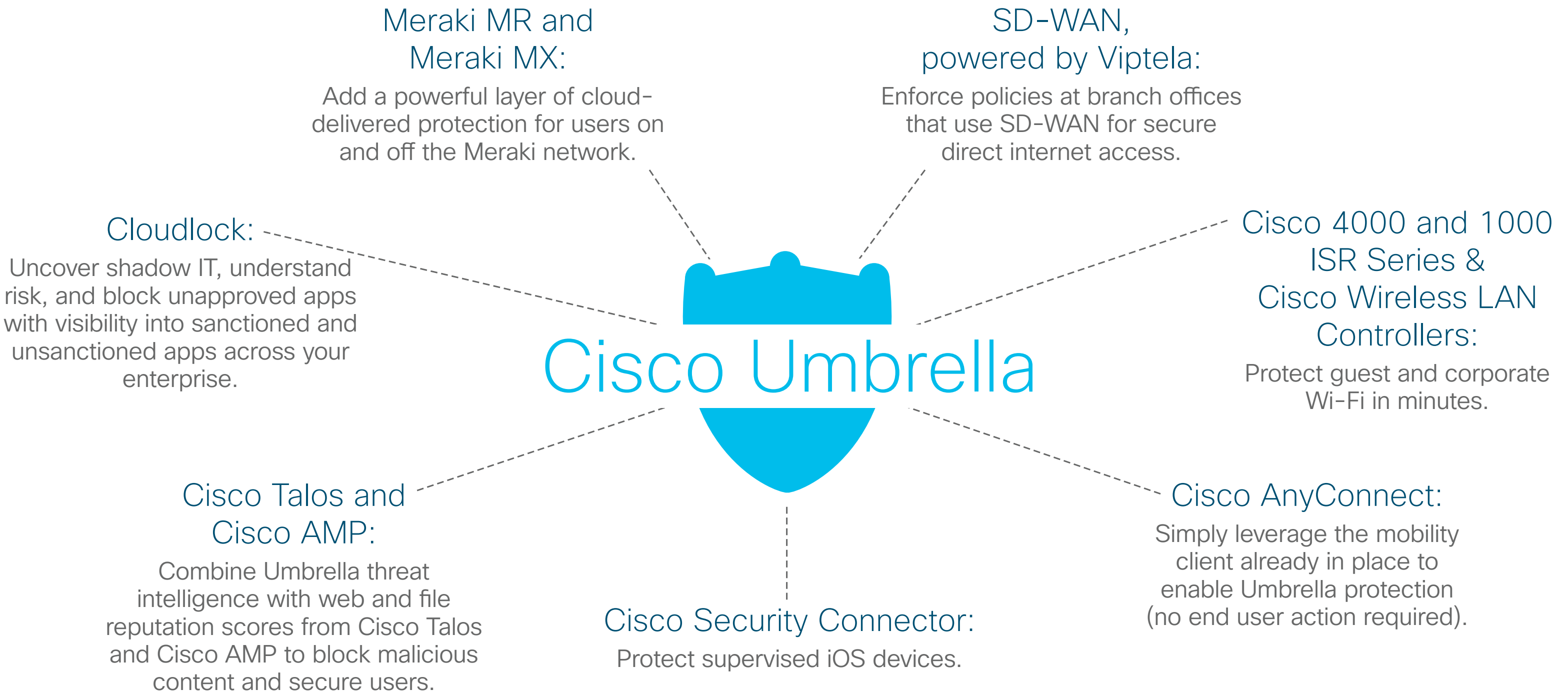


More than 2/3 of respondents stated that Umbrella helped to improve protection for remote workers and branch offices by 75%[1]

Discover the industry’s first Secure Internet Gateway

Cisco Umbrella provides a comprehensive SIG solution that protects every device on your network, whether managed or unmanaged – including mobile and Internet of Things (IoT) devices. Umbrella offers more effective protection for all of your office locations from a single platform, reducing the time, money, and resources previously required for deployment, configuration, and integration tasks.

Take advantage of the Cisco Security ecosystem.



Cisco Umbrella

Meraki MR and Meraki MX:
Add a powerful layer of cloud-delivered protection for users on and off the Meraki network.

SD-WAN, powered by Viptela:
Enforce policies at branch offices that use SD-WAN for secure direct internet access.

Cloudlock:
Uncover shadow IT, understand risk, and block unapproved apps with visibility into sanctioned and unsanctioned apps across your enterprise.

Cisco 4000 and 1000 ISR Series & Cisco Wireless LAN Controllers:
Protect guest and corporate Wi-Fi in minutes.

Cisco Talos and Cisco AMP:
Combine Umbrella threat intelligence with web and file reputation scores from Cisco Talos and Cisco AMP to block malicious content and secure users.

Cisco Security Connector:
Protect supervised iOS devices.

Cisco AnyConnect:
Simply leverage the mobility client already in place to enable Umbrella protection (no end user action required).

Source:
1. TechValidate survey of 195 users of Cisco Umbrella

Cisco Umbrella

Multiple, disparate tools with glitchy integrations. Siloed data. Hundreds of security alerts and thousands of incidents to investigate. As resources remain squeezed and the security skills gap widens, you need to prioritize your team's efforts. Where to begin?

If you're using traditional security tools and expecting them to scale across your SD-WAN, you'll likely run into trouble. The best approach is an integrated one that works with your stack, not against it.

Cisco Umbrella amplifies your existing investments with a bi-directional API that easily integrates with other systems and your Cisco security architecture. And it starts working in minutes. Simply point your DNS to Umbrella – and start protecting against malware, ransomware, DNS tunneling, and more.

Learn more about the top security trends

See full report ›

The Umbrella Advantage

180B
daily DNS requests
(over all ports and protocols)

800
partnerships with top ISPs and CDNs

90M
global daily active users

3,900
peering sessions

31
data centers across five continents

Don't take our word for it.
Try our world-class threat protection for 14 days.

Start free trial