Cisco Umbrella

Is SASE security right for you?

Tips for evaluating vendors and solutions

Cisco Umbrella

Meeting the challenge of security in the cloud

Today's savviest organizations have transitioned away from legacy, on-premise apps to cloud services that enable more flexibility and agility. Yet many continue to rely on traditional, on-premise network security.

A new approach is emerging, one that can connect and protect users anywhere they work. Secure Access Service Edge (SASE) consolidates critical network and security functions in a single cloud-delivered service—providing better protection and better performance with less complexity.

Many organizations start their SASE journey by adopting a consolidated set of security functionality that is delivered from a single cloud-based solution. This security-based checklist will help you determine if a SASE approach to security is right for you, what to look for in a vendor, and the key components that form an effective solution.

A quick SASE primer

SASE—pronounced "sassy"—was coined by Gartner in 2019, and is defined as the convergence of networking and security services into a single, cloud-delivered solution.

Cisco Umbrella

More people.
More locations.
More threats.

Distributed work has gone mainstream—supported by a growing number of devices, apps, and services. As the attack surface has expanded, security threats have become more sophisticated and persistent. IT teams are on the receiving end of a torrent of alerts, updates, and patches that are increasingly complex and difficult to keep up with.

You want to provide consistent, secure access to corporate resources without overburdening your teams or slowing down end users. If you're juggling multiple point solutions to connect and secure users at the edge, it's time to find out if a SASE approach to security is the answer for you.

Key questions

- Are more than 40% of your applications SaaS?
- Have you adopted a multi-cloud strategy?
- Are your end users dispersed across different locations?
- Do you plan to support a hybrid work model going forward?
- Do you use multiple consoles to administer security policies across all locations and users?

If you answered yes to any of these questions, your organization could benefit tremendously from adopting a SASE approach to security.

Cisco Umbrella

So you want to get SASE about security

Where should you start?

As the buzz around SASE has grown, many vendors have jumped into the space—but rising security risks and a changing workplace have upped the stakes. Not every vendor will deliver the performance and reliable architecture required to protect your organization and your employees.

One of your first objectives is finding a vendor with a comprehensive architecture and vision that helps you eliminate the complexity of managing multiple point solutions. Take the time to evaluate different vendors, reviewing capabilities and approaches. Look for one with a track record of delivering strong, secure access to users, no matter where they are.

What to look for in a vendor

- A proven track record of efficient security
- A simplified approach that includes Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), firewall, DNS security, remote browser isolation, DLP, sandboxing, XDR, and interactive threat intelligence—all from one dashboard
- A modern cloud infrastructure with high performance and reliability
- The ability to support a hybrid approach
- Flexible packaging that meets your specific needs today, and can easily scale to protect you in the future

Now it's time to find the right solution

The best solutions include a robust set of security services delivered from a reliable, high-performance cloud infrastructure. Look for the services you need now as well as the expertise and an extended feature set to handle future requirements. During your evaluation, look for the ability to deploy at your own pace, bridging the gap from where you are today to a full services-based model in the future. Keep this checklist handy to help you determine how offers compare.

Essential capabilities

Secure Web Gateway (SWG)	Log, decrypt, and inspect web traffic to gain complete visibility, leverage URL and application controls, and protect against malware.
Cloud Access Security Broker (CASB)	See which cloud apps are in use, view app details and risk information, and enforce specific controls to block risky apps and reduce Shadow IT.
Firewall-as-a-Service (FWaaS)	Deploy cloud-delivered firewalls to gain visibility and control of outbound internet traffic across all ports and protocols.
Domain Name System (DNS) security	Stop threats at the DNS layer over any port or protocol—before they establish a connection to an IP address and reach your network or endpoints.
Remote Browser Isolation (RBI)	Enable safe access to risky websites and apps without the threat of malware by isolating web traffic away from a user's endpoint.
Data Loss Prevention (DLP)	Discover and block sensitive data being transmitted to unwanted destinations; protect data from exfiltration and support compliance mandates.
Interactive Threat Intelligence	Get insight into malicious domains, IPs, and URLs, including real-time context on malware, phishing, botnets, trojans, and other threats.
Native global cloud architecture	Ensure reliability and speed with an architecture built for cloud—not adapted for it.

Cisco Umbrella

What do the experts say?

Major security analysts and industry experts all have their own view of the elements you should look for in a vendor that provides SASE security. Minor differences exist, but there is a common set of key items.

Key criteria	Cisco Umbrella delivers in each of these areas
Broad set of cloud-based services	✓
Simple deployment and maintenance	✓
High level of security effectiveness	✓
Strong infrastructure and performance	✓
Vision/roadmap for more consolidated services	✓

Cisco: the proven leader in cloud-native security

620 B

requests per day

73%

reduction in latency

500 M

authentication events every month

96%

threat detection rate[1]—the highest in the industry

Cisco Umbrella

Begin your SASE journey with proven protection and reliability from Cisco Umbrella

Cisco Umbrella is a core component of Cisco's SASE architecture, delivering multiple security functions in a single, cloud-delivered service. A solution that is simple, scalable, and flexible, Umbrella helps you develop a united and integrated defense that protects far beyond your corporate perimeter.

Every day, Umbrella delivers the most secure, most reliable, and fastest internet experience to more than 24,000 customers. By unifying multiple security solutions into a single service, Umbrella helps businesses embrace direct internet access, secure cloud applications, and extend protection to roaming users and branch offices.

Chat with an expert at Cisco to see how Cisco Umbrella can meet your SASE needs.

Contact us

1. *DNS-Layer Protection & Secure Web Gateway Security Efficacy Test*, AV-TEST, February 2020