Keep every user secure and connected, in every cloud, with Cisco SASE

IT teams are under more pressure than ever before to keep their organizations secure, reduce operational costs, and make things simpler to manage.

But it's not easy when:

Applications extend across multiple clouds

Workforces and workspaces are hyper-distributed under hybrid work models

IT teams must rely on a patchwork of point solutions from many vendors

76% of IT teams say that remote workers are harder to secure.[1]

51% of organizations are having problems connecting workers to company resources.[2]

70% of IT leaders agree or strongly agree that managing a multi-vendor networking and security stack is too complex.[3]

Security and networking need a better path forward, together

Using yesterday's approaches to provide secure connectivity for today's hyper-distributed, dynamic environments is proving more costly.

There has been a dramatic rise in Internet traffic as organizations have continued to adopt cloud applications and storage, and run more workloads from the cloud.

Backhauling traffic to corporate data centers via expensive MPLS lines and VPNs and forcing it through security appliances before forwarding it on no longer makes sense.

With many people working anywhere, on any device—at home, on the go, at the branch or campus offices—networking and security teams must:

Security teams

Achieve a consistent approach to security, anywhere users work, with simpler solutions that ensure a seamless experience and eliminate gaps in coverage.

Increase security efficacy and mitigate the cyber risk posed by an expanding attack surface and vectors to assure regulatory compliance, by adopting new security models such as Zero Trust.

Reduce complexity and the risk of human error as security stacks evolve to support faster adoption of cloud infrastructure and software as a service (SaaS).

Network operations teams

Support an excellent hybrid workforce experience by ensuring optimal connectivity to any cloud and improving control of, and visibility into, the complete service delivery chain.

Resolve network performance issues driven by soaring Internet traffic and new traffic patterns that create bottlenecks in legacy network topologies and result in a poor user experience.

Reduce operational costs associated with providing secure connectivity between complex IT environments (public, private, and hybrid clouds), using SD-WAN with end-to-end traffic modelling for optimal routing.

Security and networking teams can't handle these challenges alone. They've got to come together to:

Control costs

Simplify operations

Keep their organization secure

SASE: Where IT worlds collide—and thrive

As work dynamics shift again, networking and security teams can't keep working in silos, reacting in parallel to the same problems. They need to be ready for the next disruption.

Secure access service edge (SASE) converges networking (SD-WAN), cloud-based security (CASB, FWaaS, SWG, and ZTNA), analytics, and insights into a single, cloud-based solution, delivered as a service, to provide optimal, secure connectivity from every user and device to every cloud:

SD-WAN

Centralized management
A centralized, highly visual dashboard that facilitates device configuration, network management, monitoring, and automation. Includes zero touch provisioning at the network edge.

Cloud network extension and middle mile optimization
Extensive cloud on-ramp integrations to enable seamless, automated connectivity with any site-to-cloud and site-to-site configuration. Includes optimized middle mile connectivity through SDCI and colocation integrations.

Application experience
The ability to monitor and validate the usability and performance of web applications. The detailed metrics and waterfalls show the sequential fetching and loading of web components to identify errors and bottlenecks and understand the impact on application performance.

Flexible and scalable infrastructure
A wide range of physical and virtual platforms that deliver high availability and throughput, multi-gigabit port options, 5G cellular links, and powerful encryption capabilities. Optimizes WAN traffic by dynamically selecting the most efficient WAN links that meet the service level requirements.

AI-enhanced troubleshooting
Robust AI/ML for optimizing network performance, automating routine manual tasks, and accelerating troubleshooting. Provides intelligent alerting, self-healing, and predictive internet rerouting capabilities.

Integrated security
Robust security capabilities that work hand-in-hand with cloud security to protect branches, home users, and cloud-based applications from infiltration.

Identity-based policy management
Micro-segmentation and identity-based policy management across multiple locations and domains.

Advanced insights
Enhanced visibility into application, internet, cloud, and SaaS environments with comprehensive, hop-by-hop analysis. Enables the isolation of fault domains and provides actionable insights to accelerate troubleshooting and minimize or eliminate the impact on users.

Cloud security

Zero Trust Network Access (ZTNA)
A security framework that mitigates unauthorized access, contains breaches, and reduces attackers' lateral movement across the network. ZTNA should be coupled with strong identity and access management to verify users' identity and establish device trust before granting access to authorized applications.

Secure Web Gateway (SWG)
A gateway that logs and inspects web traffic to provide full visibility, URL filtering and application control, and protection against malware.

Cloud-delivered firewall with Intrusion Prevention System (IPS)
Software-based, cloud-deployed services that help manage and inspect network traffic.

Cloud Access Security Broker (CASB)
Software that detects and reports on cloud applications in use across a network, exposing shadow IT and enabling risky SaaS apps and specific actions, like posts and uploads, to be blocked.

Data Loss Prevention (DLP)
Software that analyzes data in-line to provide visibility and control over sensitive data being pushed or pulled beyond the organization's network or cloud environment.

Remote Browser Isolation (RBI)
Software that isolates web traffic from user devices to mitigate the risk of browser-delivered threats.

DNS-layer security
Software that acts as the first line of defense against threats on the Internet, blocking malicious DNS requests before a connection to an IP address is even established. Strong DNS security can greatly reduce the number of threats a security team has to triage on a daily basis.

Threat Intelligence
Threat researchers, engineers, and data scientists who use telemetry and sophisticated systems to create accurate, rapid and actionable threat intelligence to identify emerging threats, discover new vulnerabilities, and interdict threats in the wild before they spread, with rule sets that support the tooling in your security stack.

How the SASE model evolved

Network as a service — Connect it

Security as a service — Secure it

Market convergence

Secure Access Service Edge (SASE)

Software-Defined Wide Area Network (SD-WAN)

Firewall as a Service (FWaaS)

Secure Web Gateway (SWG)

Cloud Access Secure Broker (CASB)

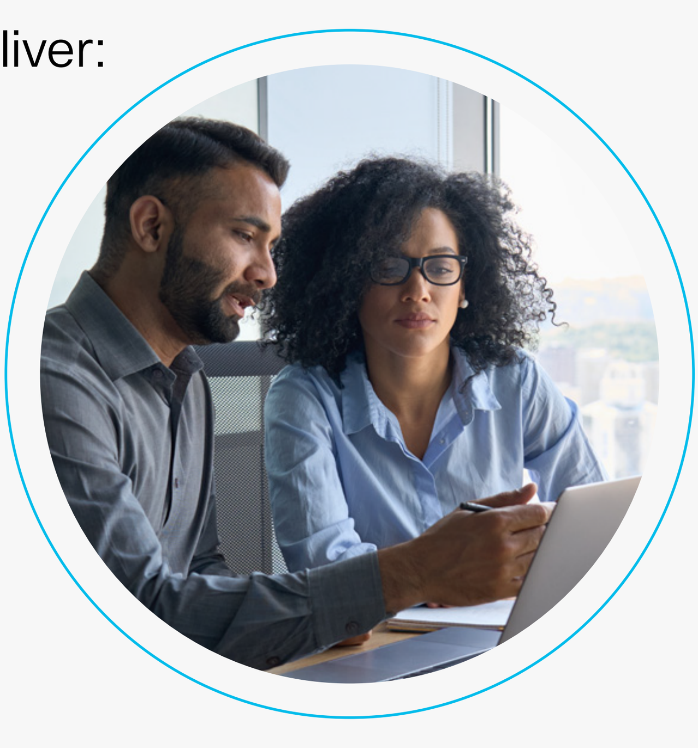
Zero Trust Network Access (ZTNA)

Cisco SASE enables you to deliver:

Dynamic
connectivity that's fast, flexible, and predictive

Secure
access across every point of service

Seamless
experiences from every user and device to every cloud



60% By 2025, at least 60% of enterprises will have explicit strategies and timelines for SASE adoption encompassing user, branch, and edge access, up from 10% in 2020.[4]

48% of companies interested in SASE will start with security, 31% will start with the network, and 21% plan to address security and networking simultaneously.[5]

34% of organizations are prioritizing solutions and services that provide integrated, cloud-based management of SD-WAN.[6]

Supporting today's use cases

Designed for today's hybrid work environments, SASE lets you minimize the complexity of managing more remote users, devices, applications, and data across multiple clouds—while minimizing risk in a changing and ever-expanding threat landscape.

Secure Edge

Connect your sites securely and seamlessly to applications and data anywhere.

Incorporates global points of presence (PoP), infrastructure as a service (IaaS), and colocation facilities.

Local traffic secured and forwarded to destination without first traveling to data center focal points.

Secure Remote Worker

Connect your users from off corporate network remote locations to applications and data anywhere.

Identity-based security – individuals, groups, office locations, devices, Internet of Things (IoT), and services.

Option to use client (AnyConnect) or client-less (VPN) for **user end-point security.**

Cisco's SASE solutions are based on open standards and support extensive APIs, enabling you to address immediate secure connectivity needs and business demands, while driving strategic transformation:

Reduce costs

75%

of customers were able to give their IT teams the ability to focus on cost savings.[7]

"...Thanks to Cisco SASE, our network topology is now optimized and centralized across all of our operations and IT offices, making it easier to manage data and incrementally save costs.

– Head of IT Enterprise, Vistara

Improve user experience

73%

Improvement in latency and traffic consistency (jitter).[8]

"...a tremendous improvement in speed, stability and bandwidth across all our operations utilizing Cisco SASE capabilities along with effective enablement towards our cloud strategy.

– Joel Marque, IT Director, Tamimi Markets

Minimize risk

85%

of customers were able to cut malware infections by half.[9]

"...Threats and exploits can't get through – Cisco SASE gives us confidence because we know that our users are protected when they're surfing the Internet on or off the network.

– Adam Kinsella, Product Owner, Qantas

Ready to learn more?

The best way to realize the full potential of SASE is by working with a single vendor who combines best-in-class networking, security, analytics and insights, with industry know-how and a vast partner and vendor ecosystem to offer the flexibility and investment protection you need to transition to the cloud your way, at your pace.

We own all the required building blocks for your SASE foundation today, including the cloud-managed tools, analytics, and insights you need to **deliver the unified experiences your users demand – whatever tomorrow brings.**

1. The State of Security 2021, Splunk 2. Future of Technology, Cisco 3. The Present and Future of Cloud SASE, Cisco, and Pulse 4. 2021 Strategic Roadmap for SASE Convergence, Gartner 5. SASE Trends: Plans Coalesce but Convergence Will Be Phased, ESG Research Report 6. 2022 Cisco Global Networking Trends Report: The Rise of Network as a Service 7. Techvalidate Customer Research 8. Miercom - Performance validation testing 9. Techvalidate Customer Research

Learn how Cisco and CDW can help transform your infrastructure and contact your account manager today.