Cisco Secure Access

Hybrid work is here to stay

Protect users and resources anywhere work is done

Cisco Secure Access is a converged Security Service Edge (SSE) solution that is better for users, easier for IT, and safer for everyone. It enforces modern cybersecurity while providing a seamless and frictionless experience as users connect from anything to anywhere, via a common access method. This solution is a foundational element of Cisco's Secure Access Service Edge (SASE) architecture.

Cisco Secure Access simplifies IT operations through a single, cloud-managed console, unified client, AI-assisted centralized policy creation, and aggregated reporting. Extensive security capabilities converged in one solution (ZTNA, SWG, CASB, DLP, FWaaS, DNS security, RBI, DEM and more) mitigate risk by applying zero trust principles and enforcing granular security policies. Market leading Talos threat intelligence fuels unmatched threat blocking to reduce risk and speed investigations. AI application and API use is protected with app discovery, prompt and response DLP, hazardous use guardrails and blocking controls.

Benefits

- Deliver unified, seamless, and secure end user access to any app or port via any protocol.
- Simplify IT operations via a single console, simplified policy management and aggregated reporting.
- Reduce risk with advanced cybersecurity protection, zero trust principles and granular security policies.
- Secure the use of AI apps/APIs with discovery, reporting, DLP, machine learning guardrails, and blocking.
- Obtain visibility into cloud application usage, their risk levels and shadow IT operations.
- Proactively monitor the health of applications, connectivity and devices, pinpoint performance issues and quickly remediate.

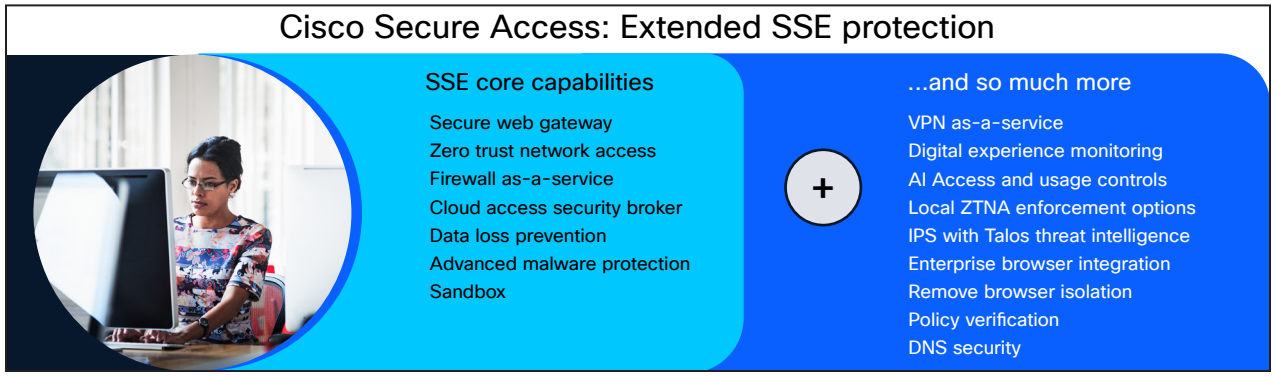

Figure 1. Cisco secure access

Cloud security that's better for users, easier for IT, and safer for everyone

Cisco Secure Access safeguards access to the web, cloud services, SaaS, and private applications. Leveraging least privileged principals, the solution dynamically authenticates users. It evaluates device posture with contextual insights to ensure security. Multiple sophisticated security layers protect your users and resources against wide-ranging cyberattacks such as malicious threats, data exfiltration, phishing, ransomware, and infected files. Dynamic user trust scores are maintained throughout sessions to highlight changes in the risk level per user.

Cisco Secure Access delivers industry-leading flexibility in how it secures access to all (not some) private applications. Client-based and clientless Zero Trust Network Access (ZTNA) seamlessly secures access to standard applications with least privileged access, from managed and unmanaged devices.

CASB functionality exposes shadow IT by detecting and reporting on cloud applications, including a wide variety of generative AI apps. Granular compliance and security policies can block inappropriate or high risk applications.

For AI applications DLP blocks uploads of sensitive data to prevent its leakage to unauthorized users, and it can also prevent the download of potentially unsafe content, such as AI-generated source code. Machine learning helps provide AI guardrails to protect against prompt injections, how-to-harm prompts, and toxic content.

Organizations of all types are undergoing a fundamental shift in how their users are accessing various resources. Employees, contractors and partners are now often located outside the corporate security perimeter and extensively utilize an expanding array of cloud-located applications and databases.

This leads to a suboptimal experience for hybrid workers, increased complexity for IT/security, and gaps in security. End-users are frustrated by a mix of connection methods and cumbersome security processes. IT/security teams struggle with too many security tools and disparate management portals. With cyberattacks increasing in frequency and sophistication and targeting an expanded threat surface, security risk rises. To surmount these challenges, organizations are adopting consolidated, cloud-based security in the form of Security Service Edge (SSE) solutions like Cisco Secure Access.

Cisco Secure Access incorporates all pertinent security modules in one cloud-delivered solution. Furthermore, a single dashboard simplifies IT/security management and lowers administration cost. AI Assistant automatically converts conversational, English phrases into security policies to save time and simplify policy administration.

Raising the SSE bar

Cisco Secure Access goes beyond the traditional approach taken by some other security vendors. Our cloud-delivered security is provided as a service and offers several critical advantages.

Cisco provides:

- Secure access to all applications including those involving non-standard protocols as well as those based on multi-channel and client-to-client architectures.
- Single unified management console across all security modules.
- A converged set of “best-of-breed” security capabilities that enable vendor consolidation, ensure consistent rulesets, and simplify administration tasks.
- Resilient cloud-native architecture provides easy scalability, up or down per business requirements, efficient single-pass processing for faster responses, and continual, rapid support of new features.
- Identity aware proxy design ensures apps and resources remain obscured from view to all but fully authorized users. Granular per app per user proxy connections provide complete traffic isolation and protect against resource discovery and lateral movement.
- Experience Insights monitors health and performance as users access applications and resources. Track endpoint, network connectivity, SaaS, and collaboration app performance levels.
- Flexibility to utilize standard HTTP2 with TLS or, where permitted, optionally take advantage of the standardized QUIC protocol that can achieve higher throughput HTTP3 connections with lower latency.

Get started today

Learn more about Cisco Secure Access.
Visit www.cisco.com/go/secure-access.

- Integration with Duo, Cisco SD-WAN, ISE, ThousandEyes, Cisco XDR, CSPM.
- Unique, high-performance integration for mobile device ZTNA with Apple, Samsung, and other Android devices.
- AI application discovery, reporting, control, DLP, usage guardrails, and threat protection.
- Integration with Chrome Enterprise to deliver local and cloud-based threat protection for managed/unmanaged devices accessing web-based applications and resources.
- Proactive policy testing to identify conflicts and unintended impacts before activation.

Security efficacy is paramount

Cisco Secure Access is backed by Cisco Talos, one of the largest and most trusted providers of cutting-edge security research globally. Talos' robust expert team of full-time researchers and data scientists, machine learning, and artificial intelligence sees what is happening across the threat landscape, acts on that data rapidly, and drives protection.

Package options

Cisco Secure Access is available as a full SSE solution, delivered in a single subscription, with a single policy set, and unified dashboard.

Alternatively, Secure Access offers various packages to suit specific needs: Cisco Secure Access for Government (FedRamp approved), DNS Defense for DNS-layer security, Secure Internet Access (SIA) to protect access to the internet and SaaS applications (includes DNS Defense capabilities), and Secure Private Access (SPA) to secure access to private applications. Each package comes in "Essentials" or "Advantage" configurations. See the package comparison guide to compare features across packages.

C45-5049803-01 09/25