Cisco Secure Access

Frequently asked questions

Q: What is Cisco Secure Access?

A. A Security Service Edge (SSE) solution that provides secure access to both private and cloud-based resources. SSE solutions help organizations provide secure connectivity for hybrid workforces, while protecting corporate resources from cyberattacks and data loss. Cisco Secure Access unifies multiple security functions into a cloud service to protect users, infrastructure, and data from threats. More details here.

Q: What is driving the adoption of SSE solutions?

A. Organizations of all sizes are looking to improve their security posture while providing a better user experience and simplifying their security infrastructure and administrative tasks. Converged, cloud-based SSE solutions reduce hardware, licensing, deployment, and maintenance costs while providing improved security and immediate scalability.

Q: Does Cisco Secure Access provide security and controls for the internet and SaaS apps?

A. Yes, it provides a full proxy (SWG), Cloud access security broker (CASB), sandbox for new or suspicious files, AI powered advanced threat protection, multimode data loss prevention (DLP), remote browser isolation (RBI), digital experience monitoring (DEM), control and protection for the use of AI, and more.

Q: Does Cisco Secure Access provide protected connections to private applications (on-premise, or in the cloud/IaaS)?

A. Yes, it provides both client-based and clientless private access. Zero trust network access (ZTNA) and VPNaaS are available to protect all private applications with a unique set of security controls that enable a streamlined user experience and simplified IT administration.

Q: Does Cisco Secure Access include clients/agents?

A. Cisco has optimized deployment to include just one single agent (Cisco Secure Client) that handles both secure private access and secure internet access. Cisco Secure Access also has a set of clientless security features for devices/users without a client installed.

Q: Does Secure Access include digital experience monitoring (DEM) capabilities?

A. Yes, it allows administrators to monitor health and performance of endpoints, applications, and network connectivity as users access resources. Operators can optimize user productivity, simplify troubleshooting, and accelerate incident resolution with AI assisted problem visibility. A deep set of device and session details on the user's end-to-end experience, enable the IT/help desk staff to rapidly resolve issues.

Q: How does Cisco Secure Access leverage artificial intelligence (AI)?

A. **Automation:** An AI assistant is used to automate policy creation and testing. It can also help identify and troubleshoot user connectivity issues.

Security: Artificial intelligence is utilized to detect advanced threats to shorten the investigation and remediation process

Control and Security of AI use: Secure Access can identify over 700 AI applications and APIs. It can block the usage of specific AI tools and perform DLP functions to both AI inputs (prompts) and output (e.g. code) to block the sharing or loss of sensitive data.

Q: How does Cisco Secure Access compare with other SSE solutions?

A. Cisco has a unique architecture and set of functionality included in a single SSE subscription, console, and agent. Cisco Secure Access takes an identity first approach to SSE which results in a higher level of protection across the full spectrum of users and device types. It has been recognized as a leader in SSE overall and for many of the individual components within the solution including zero trust network access (ZTNA) and secure web gateway (SWG). More details here.

Q: How does SSE relate to the Secure Access Service Edge (SASE) concept?

A. SASE is the combination of security (a set of SSE functionality) and networking (a set of SD-WAN functionality). Cisco Secure Access is an SSE solution that is integrated with both Cisco Catalyst SD-WAN and Cisco Meraki SD-WAN to provide full, single-vendor SASE. Cisco Secure Access can also be used with other third-party SD-WAN solutions to effectively deliver a dual-vendor SASE approach.

Q: What is the underlying infrastructure/ architecture of Secure Access?

A. Cisco Secure Access utilizes both hyperscaler-based and Cisco managed POPs to provide flexibility, coverage and control across the globe. Cisco utilizes an innovative set of technologies including MASQUE, QUIC, VPP, and ECMP to deliver a modern and secure SSE solution with high-performance.

Q: Why do organizations select Cisco Secure Access over other SSE solutions?

A. Breath of functionality, security efficacy, integrations with both other Cisco security offerings and third-party solutions, price, plus unique ZTNA and identity intelligence capabilities. They also like the built-in flexibility to easily expand into a variety of market leading, full SASE options.

Q: How is Cisco Secure Access priced and packaged?

A. Cisco Secure Access is priced by user. There is an Essentials package that includes the majority of capabilities and an Advantage package that includes an extended set of functions. Organizations can purchase separate user counts for Secure Internet Access (SIA) and Secure Private Access (SPA) to meet their specific needs. For more information please visit here.

Q: What has been the experience and learnings from existing Secure Access customers?

A. Customers have provided detailed feedback on this solution in a variety of case studies covering different use cases. Key highlights include the ease of deployment, simplified management process in the areas of policy, visibility & troubleshooting, and overall security effectiveness across both private and Internet/SaaS access. For more information see these customer stories.

P2004141007 12/24