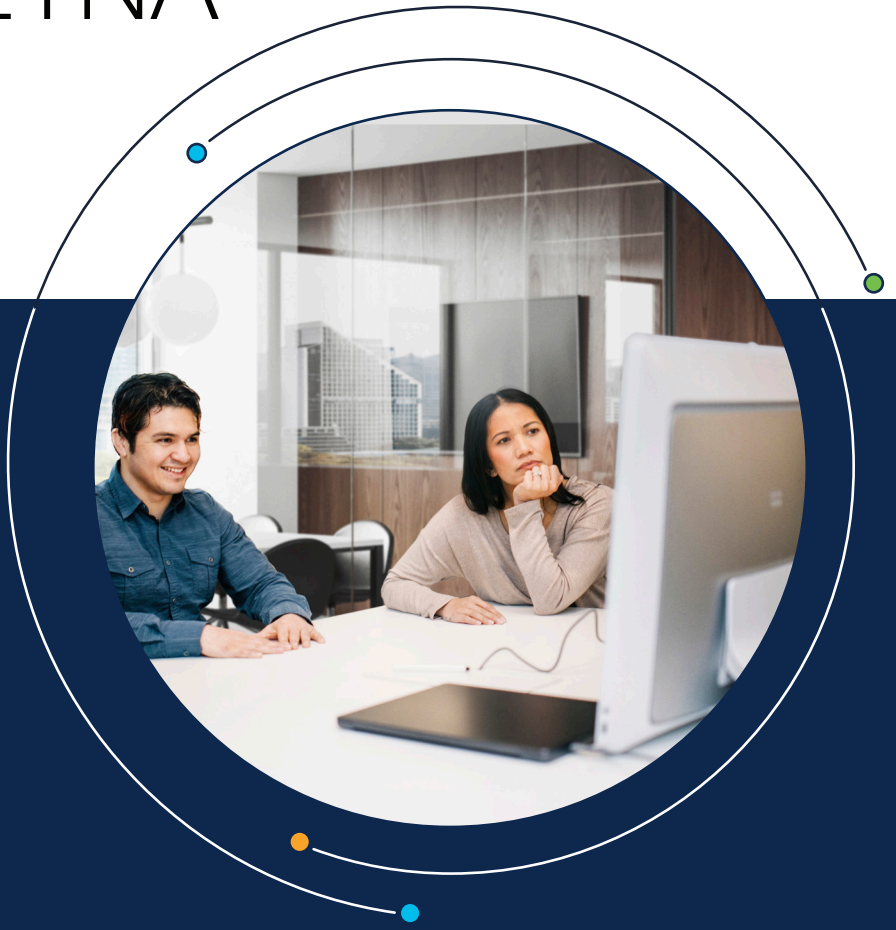
Accelerate Your Azure Journey with Cisco Secure Access and Universal ZTNA

Connect your users to Azure apps



Executive summary

Enable your workforce to securely connect to your Azure apps – from anywhere – with Cisco and Microsoft's identity-first approach.

Today, most enterprises are living in the cloud. Simultaneously, your users (employees at branch offices, remote and hybrid workers, road warriors, and contractors) must connect to apps and services everywhere. They need seamless and secure connectivity – that just works.

But efficiently achieving the promise of zero trust is complicated by two factors:

1. Difficulty supporting access to apps across cloud-native, custom, and legacy domains, and
2. Identity-based attacks that undermine the very the promise of zero trust

Implement Zero Trust your way

Together, Cisco® and Microsoft lead the industry in taking an identity-centric approach to security. Built for the real world, our Universal Zero Trust Network Access (ZTNA) solution features Cisco Secure Access, our identity-first Cisco Security Service Edge (SSE) capability, plus Cisco Identity Intelligence (CII). The solution delivers zero trust access with the power of its Microsoft Azure and Entra ID integrations. Cisco's Identity Intelligence aggregates and correlates events across Entra ID, plus third-party identity providers like ServiceNow, Salesforce, and more.

Key outcomes

1. **Accelerated secure connectivity to your Azure workloads**. Security and IT teams can efficiently manage cloud-delivered security, as Cisco's Resource Connectors for Azure reduce ZTNA configuration from days to hours.
2. **Simplified management + better security outcomes**. Your team gains efficiencies and closes security gaps with our unified manager, unified policy construct, and unified client for internet security plus ZTNA + VPN as a Service (VPNaaS) application access.
3. **Zero trust project risks are minimized**, as only Cisco delivers Secure Access Resource Connectors for Azure, with both clientless ZTNA plus a single-client for ZTNA + VPNaaS and internet access security.

Differentiators to Securely Accelerate your Azure Journey

- **Seamless Application Access:** Only Cisco and Microsoft take an identity-first approach. Combining Microsoft Entra ID with Cisco's ZTNA and Cisco Identity Intelligence aggregates and correlates identity-based threats across all your identity providers. Only Cisco Secure Access supports all versions of Microsoft Entra ID, protecting investments in your existing identity infrastructure.
  - **Access to all apps, not just some:** Secure, transparent connectivity to cloud-native, custom, and legacy applications hosted in Azure, the multicloud, and on-premises.
  - **Zero trust on your timeline.** Dual VPNaaS and ZTNA capability enables migration to ZTNA at your own pace, with VPN fallback and unified connectivity to your legacy applications that are suited for ZTNA.
  - **Happier users.** With unified ZTNA + VPNaaS, users connect to more applications, faster. **Users transparently connect to all required resources, without having to know, manage, or think about the underlying connection method**.
  - **MFA support for special situations**. When you want to compliment Microsoft MFA in special situations, such as supporting Linux systems, we can help. Cisco's solution can authenticate users against Entra ID, and our MFA complements Microsoft Entra ID and supports Entra ID External Authentication Methods (EAM), plus Microsoft Intune.
- **Data Protection:** Secure Access' Data Loss Prevention (DLP) integrates with Azure Storage, and other Microsoft services, to ensure compliance and mitigate data exfiltration risk, as well as protecting against loss of critical Azure keys and secrets. Also, Cisco DLP uniquely enables granular ingress and egress control of Generative-AI developed and reviewed code, both via API and Web.
  - **#1 in Threat Defense.** In recent independent laboratory testing by Miercom, Cisco Secure Access threat defense outperformed SSE offerings from Zscaler, Palo Alto Networks, and Netskope.

  - **Full SSE Protection.** Cisco delivers fully integrated SSE security capability, with unified Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), DLP, DNS-layer security, ZTNA + VPNaaS, and Remote Browser Isolation (RBI), operating under a single policy construct, with a single manager, and a single client, to protect against advanced threats and data loss while simplifying connectivity.

- **Performance and Resilience:** Cisco's MASQUE/Quick UDP Internet Connections (QUIC) protocols delivers a consistent ZTNA app access user experience, without reconnection, even as roaming users move between networks.
- **Differentiated mobile support:** Only Cisco has been first to market with Apple and Samsung for advanced protocol support on mobile devices, enhancing user's ZTNA experience everywhere they roam.

Return on investment

- **Cisco customers achieved a 231% return on investment** with our cloud-delivered security, according to Total Economic Impact research performed by Forrester Consulting. In this study, Forrester independently interviewed Cisco customers.
- **CIOs maximize every dollar of their Azure investment**—accelerating your cloud journey and supporting your mission with seamless application access that enhances user productivity.
- **CISOs can proceed with confidence** that their cloud-delivered security posture reduces risk and meets compliance requirements with an integrated, identity-centric SSE solution.

Securely Access all your Cloud and Legacy Apps

Identity-Centric Integration: Microsoft Entra ID forms the foundation of your Zero Trust approach, and Cisco's Universal ZTNA solution layers in both Secure Access SSE and Cisco Identity Intelligence to mitigate identity attacks by aggregating and correlating events across multiple additional identity providers, including ServiceNow and Salesforce. Further, Cisco's approach includes integrated ZTNA and VPNaaS, plus the full suite of SSE capabilities (CASB, DLP, RBI, Firewall as a Service [FWaaS], Intrusion Prevention System (IPS), DNS-layer security, and more).

- **Unified Policy and Visibility:** From a single manager, control:
  - Internet access threat defense
  - ZTNA + VPNaaS
  - Data Loss Prevention (DLP) and CASB
- **Flexible App Access Migration:** Where required, you can start with VPNaaS and transition to ZTNA as your cloud adoption matures, ensuring a controlled progression that aligns with your strategic roadmap.

Next steps

Experience for yourself secure, identity-first connectivity for Azure workloads and beyond. **Visit the Cisco Secure Access for Azure Resource Center, and contact us today.** Together, Cisco and Microsoft will help you strengthen your security posture, delight your users, and accelerate your cloud journey.

C22-4938751-00 03/25