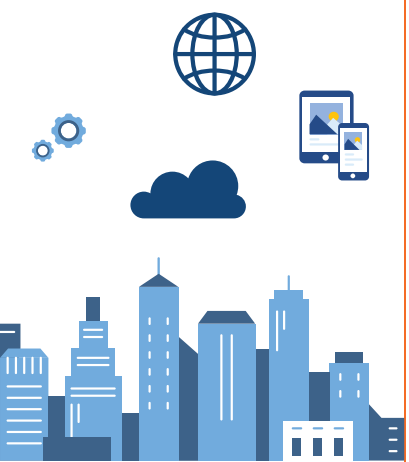
CipherCloud Zero Trust Remote Access Solution

At a Glance

- Founded in 2010 and Headquartered in Silicon Valley
- Over 10 years providing advanced cloud security and data protection solutions
- 23 granted and pending CASB and cloud security patents
- **Investors:** Andreessen Horowitz, Transamerica Ventures, Delta Partners, Deutsche Telekom.

Customers

- Trusted by enterprises of all sizes
- Across every region and geography
- Representing nearly every vertical including:
  - Banking and Financial Services
  - Healthcare and Pharmaceutical
  - Manufacturing
  - Energy
  - Technology
  - Telecommunications
  - Education
  - Government



Solution Overview

Today's distributed workforce requires secure, uninterrupted access to data and applications, regardless of applications infrastructure or hosting parameters. CipherCloud's Zero Trust Remote Access solution enables secure and controlled access to internal applications anywhere, anytime, from any user device, while reducing the risk of data exposure from unauthorized users or compromised devices.

Built to support today's Zero Trust Network Access (ZTNA) "least privileged" strategy, CipherCloud Zero Trust Remote Access creates software-defined perimeters that enforce identity and context-aware access policies for applications and resources residing in hybrid IT environments – including public clouds and private data centers. Delivered as part of its integrated Secure Access Service Edge (SASE+) platform, CipherCloud enables today's practitioners to ensure context-aware, data-centric access across enterprise applications from any device and location.

CipherCloud ZTNA benefits include:

- Granular, identity-driven access controls for applications access
- Applications-centric access, solving excessive VPN "implicit trust" challenges
- A data-centric, context aware approach to optimize information protection
- Agile and scalable deployments to accelerate business transformation
- Full application cloaking to prevent discovery on the public Internet
- Visibility and access into legacy applications in conjunction with IAM and MFA
- Consistent user experience across SaaS and private applications deployments

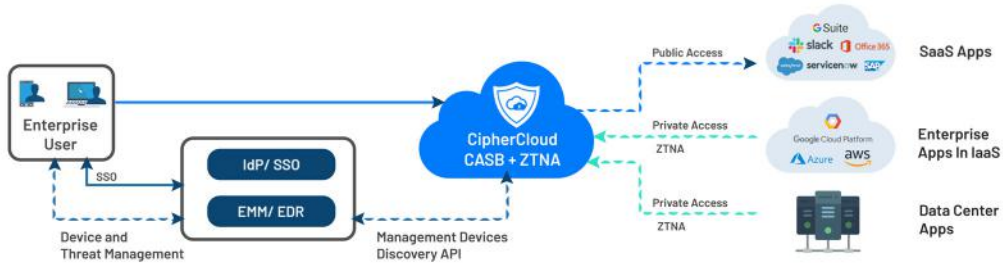
CipherCloud Zero Trust Remote Access Deployment

CipherCloud Zero Trust Remote Access facilitates agentless access from endpoint devices to private enterprise applications running in hybrid IT environments. This enables frictionless deployment, without requiring additional software installation by end-users while securing access for any device - whether the device is managed or unmanaged.

Additional benefits include:

- Microsegmentation: Through abstraction of access mechanisms, CipherCloud Zero Trust Remote Access isolates application access from network access, preventing potential data breaches driven by over-entitlement of services and thwarting lateral movement by threats within private networks.
- Full application cloaking: By eliminating the need to expose inbound firewall ports for applications access, and preventing the exposure of internal applications to theInternet - CipherCloud reduces the risk of data exposure and secures organizations from external threats and DDoS attacks.

CipherCloud ZTNA can be deployed both in standalone modes and in conjunction with the CipherCloud CASB+ solution for cloud security and data protection, and is directly supported via integration with leading network security, identity and threat protection solutions, enabling a powerful best-of-breed and out-of-the-box approach to a Zero Trust Network Access (ZTNA) strategy.



CipherCloud Zero Trust Remote Access Differentiators

Unified policy enforcement

CipherCloud's centralized policy enforcement enables a unified and consistent cloud security approach, providing extensive coverage and governance for applications access in multi-cloud and multiple datacenter environments.

Agentless deployment

CipherCloud does not require agents to be installed by end users, securing applications' access for unmanaged and personal devices in a seamless fashion. Agentless access is extended to HTTP/S, RDP, and SSH applications, among many others.

Advanced data security

CipherCloud extends CASB+ cloud security, data protection and threat protection controls to private applications, including DLP content inspection, malware scanning, encryption and enterprise DRM, delivering end-to-end Zero Trust security, ensuring that sensitive information is protected across the enterprise environment.

Deep visibility and monitoring

CipherCloud integrates with popular Security Information and Event Management (SIEM) tools, allowing organizations to analyze the network logs and deliver complete visibility into application and user activity to prevent potential threats.

User Anomaly Detection with UEBA

CipherCloud User and Entity Behavior Analytics (UEBA), backed by powerful Machine Learning, performs real-time monitoring of user interactions to identify anomalous activities to unearth emerging threats. Related anomaly detection includes monitoring of persistent login attempts by an unauthorized user, higher-than-normal login attempts from the same user, or abnormally large download volumes, among others.

Zero Trust Adaptive Access Control, with IAM integration

Contextual access policies defined by CipherCloud's Adaptive Access Control integrate with Microsoft Active Directory and SSO solutions - including Okta, Ping and Thales, to enable Zero Trust access and invoke strong authentication for granular control over applications access and usage. This further reduces user friction and establishes fine-grain access control for login activities carried out over SaaS, IaaS and private applications.

Endpoint Security Posture Management

Used in concert with the CipherCloud CASB+ platform, CipherCloud enables context-aware management of devices connecting to the cloud, from any remote location. This allows retrieval of endpoint device posture using digital certificates or integration with MDM/EMM solutions, as well as adaptive access control policies that can be enforced based on device posture (managed or unmanaged), OS, location, device compliance, IP risk, etc.

Establishing SASE Foundation

CipherCloud CipherCloud Zero-Trust Remote Access combines with the industry-leading Cloud Access Security Broker (CASB+), Data Protection and Secure Web Proxy (SWP) solutions to establish a strong foundation for Secure Access Service Edge (SASE) methodologies, enabling centralized "Zero Trust" access control. Zero-Trust Remote Access enables organizations to rapidly define unified policies to secure all of their enterprise applications and data across SaaS, IaaS, and on-prem environments, facilitating ongoing SASE process adoption.

For more information on CipherCloud ZTNA visit:

https://www.ciphercloud.com/ciphercloud-zero-trust-network-access/

Awards

About CipherCloud

CipherCloud delivers the market's leading approach to integrated CASB, SASE, and Data Privacy, addressing the full scope of customer requirements across cloud access, discovery, monitoring, data protection, policy enforcement and compliance. CipherCloud CASB+ has been named SC Magazine Cloud Security Product of the Year, Overall Leader in the CASB market by KuppingerCole, and a Visionary by Gartner, while counting numerous global 1000 companies among its rapidly growing customer base. CipherCloud is backed by Andreessen Horowitz, Transamerica Ventures, Delta Partners and DTCP, the venture arm of Deutsche Telekom. For more information, visit **www.ciphercloud.com** and follow us on **Twitter @ciphercloud.**

CipherCloud

Headquarters

CipherCloud
4353 North 1 Street,
Suite 100, San Jose CA 95 134,
USA

+1 855-5CIPHER
(+1 855-524-7437)

info@ciphercloud.com