CipherCloud Zero Trust Network Access (ZTNA)

Solution Brief

ZTNA Business Benefits

- ### Moving from network-centric access to application-centric access

  The traditional castle-and-moat approach to IT security is now widely spurned for creating excessive implicit trust, thereby leaving sensitive internal resources vulnerable to anyone capable of gaining access to the involved network, system or application.

  To help address this evolution, and support today's widely distributed and mobile-device enabled environments, Zero Trust Network Access (ZTNA) strategy prescribes a micro segmentation approach to better shield private applications within software-defined perimeters and provide "least privilege" access to authorized users, reducing any related risk of exposure based on lateral movement.

- ### Decouple users from devices

  To execute this technique, ZTNA utilizes adaptive, identity and context-aware access policies, enforcing separate user-centric and device-centric controls when doling out access to specific applications. These granular user access controls are defined by multiple attributes including user role, type and location, along with contextual information related to the connecting device's security posture, which is verified with acceptable security standards before providing access.

- ### Make the applications invisible, yet accessible

  With ZTNA in place, enterprises are thereby no longer required to open inbound firewall ports to support external connections, in essence creating a darknet with full application cloaking that ultimately prevents the discovery of applications on the public Internet. This allows employees and external partners or third-party contractors to securely access applications with greater ease to collaborate, irrespective of the device they use (managed or unmanaged) or the location from which they are connecting.

- ### Secure legacy applications

  Importantly, ZTNA extends the same security benefits associated with cutting-edge, cloud-based SaaS applications and web services to legacy applications, improving an organization's overall security posture. Integration with multi-factor authentication and identity solutions further supplements authentication control checks, ensuring that access is properly authorized and secured. ZTNA's central monitoring approach also provide deep visibility into legacy applications, detecting unusual user activity and preventing threats.

- **Provide consistent user experience**
  Today's end users expect SaaS-like uninterrupted connectivity while accessing private applications and ZTNA delivers on this model. ZTNA allows organizations to host applications at multiple strategic locations, avoiding the inconveniences and performance hits introduced by use of VPNs while preventing traffic backhaul to centralized data centers for access to internal resources. This reduces network latency and bandwidth issues introduced due to thousands of remote workers connecting via VPNs and provides a consistent user experience for accessing applications, whether hosted in private data centers or in public clouds.

- **Enable agile, scalable deployments**
  The flexibility of applications access introduced by ZTNA ultimately allows organizations to transform and scale their business operations at a far more rapid pace, without incurring the risk of exposing internal applications to the public Internet. The increased availability of applications hosted across multiple data centers also makes the remote work experience seamless. Additionally, phasing out complex legacy infrastructures lowers OPEX and TCO.

CipherCloud ZTNA Overview

The current "cloud everything" world, propelled by the requirement to unlock digital transformation and support rapid expansion of the remote workforce, has accelerated the need for seamless, flexible and low latency access to data and applications for collaboration. As organizations focus increasingly on decoupling their business-critical applications from private data centers and hosting these resources across multiple, distributed cloud servers such as AWS, Microsoft Azure, GCP, and Rackspace, they are specifically challenged to enable secure access to internal applications all while reducing the risk of data exposure from unauthorized users or compromised devices.

While VPNs have traditionally served to govern remote access, their excessive "implicit trust" far too often permits full network access to any user with valid login keys, creating the risk of unseen compromise and data theft. Additionally, VPNs neither possess application awareness nor are they designed to meet the expanding requirements of today's distributed organizations - resulting in bandwidth, connectivity and infrastructure scaling issues for remote workers connecting from remote locations.

To address this challenge, CipherCloud's Zero Trust Network Access (ZTNA) solution fully embraces the principle of "least privilege" to create software-defined perimeters and enforce adaptive, identity and context-aware policies when providing access to applications and resources residing in hybrid IT environments – including public clouds and private data centers.

Delivered as part of its integrated cloud and data security platform, also consisting of the CipherCloud CASB+ solution, ZTNA enables today's enterprise practitioners to dictate Zero Trust access across enterprise applications and data from any device and location – facilitating secure, flexible, and scalable remote workforce deployments.

CipherCloud ZTNA Solution

Gartner defines ZTNA as "products and services that create an identity and context-based, logical-access boundary encompassing a user and an application or set of applications". CipherCloud embraces this concept of ZTNA closely to provide secure access to private applications running in IaaS clouds or private data centers. CipherCloud's ZTNA framework binds application access to user identity and the context in which that specific application is being accessed. That context may also include various attributes such as geolocation, device type, OS type, and time of day.

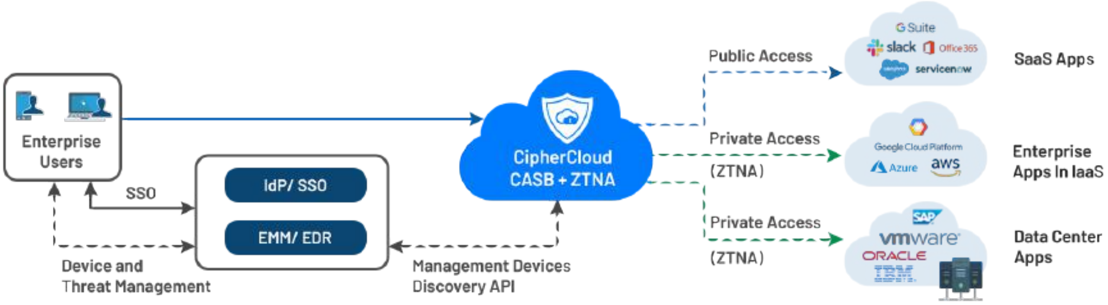

Fig. CipherCloud ZTNA Deployment

CipherCloud ZTNA facilitates agentless access from endpoint devices to private enterprise applications running in hybrid IT environments. Connector software deployed on the on-premise network hosting the private application opens a connection to CipherCloud's hosted ZTNA service, establishing a secure tunnel. Any users initiating a connection to the private applications in this manner are then authenticated and verified by ZTNA through an enterprise Identity and Access Management (IAM) service and, if granted access, connected to the applications via the established secure tunnel.

This agentless approach offers CipherCloud customers frictionless ZTNA deployment without the impact of any additional software installation on the end-user device while securing access for any device - whether managed or unmanaged. Additional benefits include:

- Microsegmentation: Through the abstraction of access mechanism, CipherCloud ZTNA isolates application access from network access, preventing data breaches due to over-entitlement of services and thwarting lateral movement by threats within the private network.
- Full application cloaking: Eliminating the need to open inbound firewall ports for applications access, and preventing the exposure of internal applications to the Internet - reducing the risk of data exposure, and securing organizations from external threats and DDoS attacks.

CipherCloud ZTNA can be deployed both in conjunction with CASB+ and in standalone modes and is directly supported via partnership with leading network security, identity and threat protection providers, enabling best-of-breed integration to offer powerful out-of-the-box Zero Trust Network Access (ZTNA) controls.

Establishing the foundation for SASE

CipherCloud's data-centric Secure Access Service Edge (SASE) approach represents the future of cloud access architecture - focused on reducing the complexity of siloed security measures through the convergence of network and security point solutions into a unified, global cloud-native service.

Our array of integrated SASE capabilities are highly identity and context-driven, relying on the identity of the entity at the source of the connection (user, device, branch office, IoT device, edge computing location) to provide access to cloud services, irrespective of user location. This consolidation of networking, network security, and cloud security enables a 360-degree security solution that goes to the edge and follows the data back to the cloud.

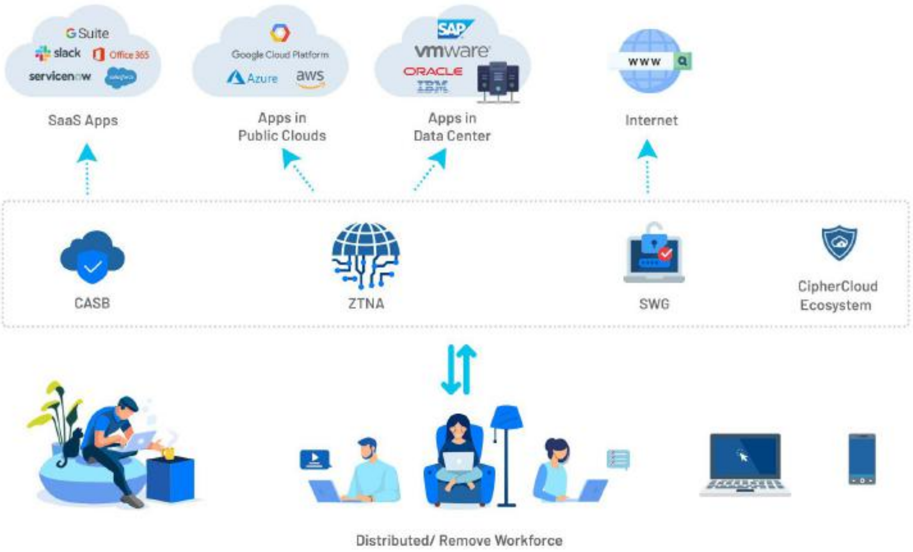

Fig. CipherCloud Integrated Ecosystem

CipherCloud combines ZTNA with its industry-leading CASB+ solution, Secure Web Gateway (SWG), and Cloud Security Posture Management (CSPM) capabilities to establish a strong foundation for Secure Access Service Edge (SASE) and enable centralized "Zero Trust" access control.

This integrated security platform capability directly allows enterprises to extend existing SaaS security controls offered by CASB+ to private applications, whether an ERP system or an intranet site behind the enterprise firewall - enabling centralized security oversight and control for all of their enterprise applications across SaaS, IaaS, and on-premise deployments.

Key processes supported by CipherCloud ZTNA include:

- Defining unified DLP policies to protect sensitive content downloaded to personal devices from private applications hosted on AWS or SaaS applications such as Office 365.

- Extending cloud antivirus, antimalware (AVAM) protection to private applications to detect and block malware -infected files from getting uploaded to the system.

The CipherCloud Difference

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

- ### Agentless deployment
  CipherCloud ZTNA does not require agents to be installed on user devices, securing applications' access from unmanaged and personal devices in a most seamless fashion. The agentless access is extended to HTTP/S, RDP, SSH and more applications.

- ### End-to-end security
  CipherCloud extends CASB+ 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 the sensitive information is protected across the enterprise deployment.

- ### 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 machine-learning powered UEBA performs real-time monitoring of user activity to identify anomalous activities that could signal an ongoing cyberattack in the ZTNA environment. Examples of anomalies include persistent login attempts by an unauthorized user, a higher than a normal number of logins from the same user, or an abnormally large number of downloads.

- ### Zero Trust Adaptive Access Control, with IAM integration
  The contextual access policies defined by CipherCloud's Adaptive Access Control integrates with Microsoft Active Directory and SSO solutions - Okta, Ping and Thales, to enable Zero Trust access to private applications and enables enterprise with strong authentication options and granular control over applications access and usage. This aids in the reduction of user friction and establishes fine-grain access control for login activities carried out over SaaS, IaaS and private applications.

- ### Endpoint Security Posture Management
  CipherCloud CASB+ enables context-aware management of devices connecting to the cloud from any remote location. CipherCloud allows retrieval of endpoint device posture using digital certificates or integration with MDM/EMM solutions, and adaptive access control policies can be enforced based on the device context - device type (managed or unmanaged), OS, location, device compliance, IP risk, etc.

Summary

The continued expansion of the distributed workforce and related cybersecurity risks clearly demands newer methodologies and tighter controls to prevent the exposure of sensitive applications and data. CipherCloud's advanced, integrated security platform, including ZTNA, addresses today's critical cloud visibility, security and governance challenges via leading edge data protection and access control, to facilitate secure remote access and collaboration.

CipherCloud's advanced approach to ZTNA fully engages the principle of "least privilege" to offer context appropriate access to nearly any application hosted on-premise or in the cloud. This integrated strategy, combining the strengths of CipherCloud CASB+ and proven ZTNA solutions capabilities, enables today's practitioners to isolate business critical applications through micro-segmentation and dictate Zero Trust access across enterprise applications and data from any device and location.

For more information or to schedule a ZTNA demo, contact sales@ciphercloud.com or
visit : **www.ciphercloud.com/contact-us.**

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**.