Zero Trust Network Access

The New Standard in Cloud Security for Hybrid and Multi-Cloud

Hybrid Applications Present New Security Challenges

The public cloud has become the next-generation datacenter for enterprises, but few enterprises are prepared for the complexity cloud migration creates. Much of industry focus has been on the applications that have migrated to the cloud, yet key corporate services such as LDAP and databases containing sensitive information have often stayed on-premises for data gravity or compliance reasons. This dependency on on-prem resources turns even a cloud-native application into a hybrid application.

Because misconfiguration of a cloud VPC has the potential to expose the corporate network to malware or other attacks, connections from the cloud back to the enterprise need to be carefully designed and continuously monitored. VPNs, the traditional workhorses of remote connectivity, were designed to connect sites together at the network level and assume that both of the sites are trusted. But should IT and Infosec consider the cloud trusted? Are the business unit user who controls the VPC and the cloud service provider are just a typo away from allowing malware to ride the VPN connection back into the enterprise? Is there a better way?

What About Zero Trust?

Zero Trust has existed as a term since 2010. And now, ten years later, companies are still struggling with its implementation. Why is this?

Zero Trust's core tenet of "never trust, always verify" encourages adopters to ditch security based on network topology and IP addresses in favor of security with stronger trust factors, such as identity. It makes a lot of sense - the network infrastructure is not to be trusted. Yet traditional network security enforcement (VLAN segmentation, ACLs, IDPS and UTM) is implemented by the routers and firewalls that make up the network infrastructure. As it turns out, many of the network security vendors promoting so-called "Zero Trust" solutions have integrated them into the infrastructure! This logical inconsistency has created serious confusion, which has slowed enterprise adoption of Zero Trust.

The truth is, the cloud has dramatically changed the enterprise computing and networking. Companies need new tools and new security best practices to fit the new reality.

Zentera Zero Trust Network Access

- Works on any public or private cloud, and on any on-premises environment
- Mutual authentication and end-to-end TLS 1.3 encryption
- Micro-segmentation blocks north-south and east-west threat movements
- Overlay fabric deploys without touching existing network and security infrastructure
- Granular protection down to the app and container level

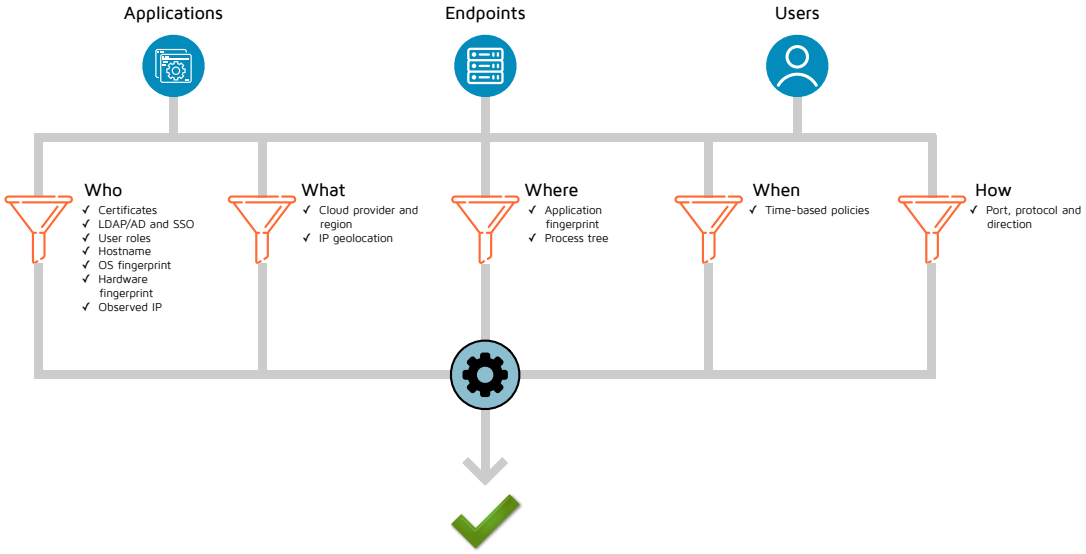
Cloud Migration	Jumphost Alternative
Database Replication	On-Prem Service Access

zentera™

Zentera ZCA: Zero Trust Network Access for the Hybrid and Multi-Cloud

Zentera Cloud Access (ZCA) creates Zero Trust Network Access (ZTNA), which is a dedicated point-to-point connection between applications with full Zero Trust security. Zentera ZTNA is completely decoupled from the existing network and security infrastructure, an deploys as a proxy, either in the endpoints or as a gateway. It carries application traffic in an encrypted overlay tunnel, connecting without touching the existing enterprise routers and firewalls.

ZTNA authenticates users, endpoints, and applications with a combination of certificate-based identity and identity providers as well as application and endpoint fingerprints constructed from metadata. ZTNA connectivity is always on-demand, created only when needed and restricted policy to specific applications and services. There is no "always on" connection, and access granted to one application can't be abused by other applications.



Individual VMs, applications, and even containerized micro-services can be cloaked from the physical network and micro-segmented, and powerful monitoring and logging provides complete visibility and observability over application traffic. These capabilities minimize the attack surface, improve visibility, and significantly reduce the risk when connecting back to the corporate network, compared to legacy VPN.