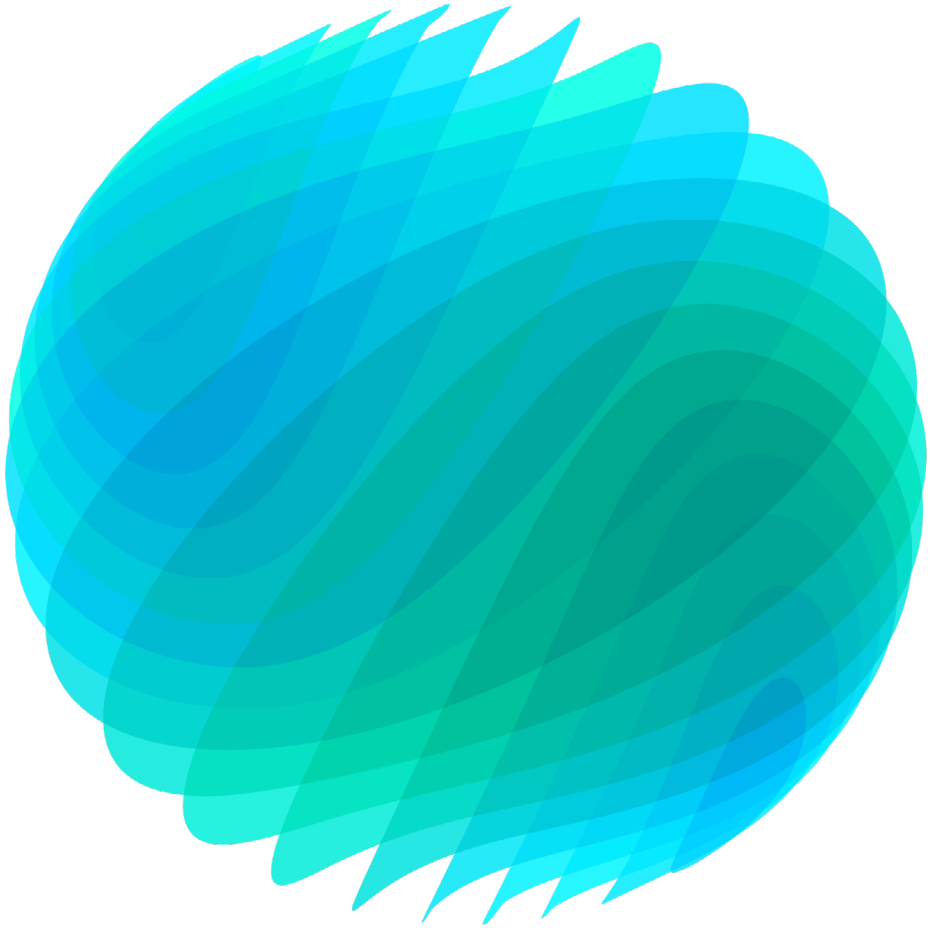
Deloitte.



Zero Trust in the Cloud: How Cloud Migration Can Create Opportunities for Cyber Security

Contributors: Timothy Li, Mason Evans, and Daniel Jones

MAKING AN IMPACT THAT MATTERS since 1845

Evolving demands on enterprise Information Technology (IT) have led to large advancements that fundamentally change how organizations do business or conduct their mission. The move to the cloud has led to more open access across the internet for employees and customers, but also increased the access points for threat actors. As recent cyber attacks have shown, shifts in IT capabilities have outpaced the cyber security capabilities and tools traditionally used to protect an organization's most sensitive assets. The migration to cloud and cloud-hosted services has been the biggest enabler to implementing Zero Trust strategies through new capabilities and system integrations. By leveraging software-defined infrastructure and cloud vendor services, organizations can be better positioned to plan their security implementation from the ground up to enable Zero Trust. Accelerated by new cyber executive orders and federal guidance, agencies are looking to rapidly adopt an agile and dynamic security foundation that is resilient to organizational change and flexible enough to meet the challenges faced by remote workforces, evolving threats, and technology trends.

What is Zero Trust?

Zero Trust is a strategic shift in how organizations approach implementing Cyber Security. Instead of another tool to purchase and administer, Zero Trust is a framework for integrating the disparate security practices an organization may already have and identifying the potential gaps. At its core, Zero Trust is an approach built upon the concept of 'least privilege' across users, workloads, data, networks, and devices. A strategic Zero Trust implementation shifts the balance of privileges away from open access to enable ease of use and towards a more granular method of protecting an organization's most sensitive assets with consistent, contextual, and automated decision-making.

Through our extensive work with clients across industries and government agencies, we have identified core capabilities for key target areas of Zero Trust which are needed for a mature implementation:

Zero Trust in Cloud Migration and Common Use Cases

Cloud migrations have had two major impacts on our cybersecurity clients. First, it has forced them to look at and understand how the cybersecurity capabilities they have in place today will work for new cloud use cases and evolve those capabilities for the cloud where they are found to be deficient. Second, cloud migration has unlocked new security capabilities available in the vendor marketplace to achieve security designs not possible in their existing data centers. We've seen a set of common Zero Trust use cases arise around remote access to cloud-hosted resources and privileged access. Each of these use cases or design patterns highlights some of the considerations we make across the pillars, and particular challenges when extending to a cloud environment. While some products may tackle one or two use cases, Deloitte's view is to take a strategic perspective on each use case end-to-end to focus on how the Cloud and Zero Trust considerations can impact each other and the overall approach.

Use Case 1: Remote access: End user accesses cloud-hosted application from home

Zero Trust Pillars that Use Case cuts across: Data, Device, Identity, Network, Telemetry and Analytics

Zero Trust Considerations:

- Can cloud-hosted identity systems correlate device or identity attributes (e.g. Device Geolocation, User Access Patterns) to dictate authentication decisions based on levels of trust (lower level of trust = lower level of access)?
- Can virtual and cloud networks apply and consume common access policies?
- Are common policies or Access Controls schemas applied to data/cloud data storage services to restrict access?
- Can you correlate identity and access event data in a common event manager across all cloud network service hubs and cloud application proxies for analytics and visibility?

Use Case 2: Privileged access: Cloud administrator needs to make configuration updates on cloud-native database

Zero Trust Pillars that Use Case cuts Across: Data, Device, Identity, Network, Telemetry and Analytics, Automation and Orchestration

Zero Trust Considerations:

- Can systems correlate user activity/behavior data as well as other attributes such as location from the cloud to detect anomalies in activity in real-time?
- Are common policies applied to restrict access to cloud resources and data?
- Can you enforce cloud service configurations to control misconfiguration?

But what does this mean to our Government clients?

Executives may find themselves asking "How does Zero Trust relate to other IT security transformation efforts and federal requirements I'm required to meet?" It is a frequent concern, as each new initiative may seem like an additional strain on already burdened resources. The goal of Zero Trust is to mature the processes put in place to meet existing needs, rather than to add new requirements. As more organizations move to architecture with hybrid Infrastructure-as-a-Service models and blended approaches of Platform-as-a-Service or Software-as-a-Service vendors integrated with on-premises datacenters, a model such as Zero Trust can help to bring all the IT growth into a cohesive structure. Initiatives such as HSPD-12 deployments, Continuous Diagnostics and Mitigation (CDM) monitoring, and National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) implementations all have their place as a piece of the overall Zero Trust architecture. Each of these initiatives are a milestone in the maturity of a Zero Trust capability, and by advancing those existing solutions to optimized levels organizations can further their overall goals.

The Bottom Line

In the move to the cloud, organizations see the realization of many technological leaps that help expand their ability to meet their mission. Yet as the distribution of organization IT moves to a shared model with cloud vendors, the responsibility for managing cyber risk remains firmly in the hands of organizational leadership. Vendors may provide a leading set of cyber security tools, but without a broad approach to cyber security such as Zero Trust, these tools can be ineffective at best and add unnecessary complication at worst. By taking a strategic perspective on each use case end-to-end, organizations can create a Zero Trust strategy that works across enterprise IT services that impact each other and the overall enterprise approach. A cohesive approach creates a clear-eyed path to bring the various cloud use cases together into a single integrated approach to meet an organization's mission.

Deloitte.