Domain 12: Related Technologies & Strategies

Introduction

In this guidance, we have explored a range of topics relevant to cloud security, including organization management, identity and access management, security monitoring, network, workload, application, and data. In this section, we turn our attention to two overarching perspectives that influence many of these topics.

First, Zero Trust (ZT) is a strategic cybersecurity approach with the potential to comprehensively address both cyber and cloud security.

Second, Artificial Intelligence (AI), particularly through Large Language Models (LLMs), is rapidly revolutionizing many aspects of IT and security.

While these topics are discussed throughout the guidance, this section introduces their foundational concepts.

Learning Objectives

The learning objectives for this domain aim to provide readers with knowledge on:

- Discuss the benefits of integrating AI into threat and vulnerability management for cloud security.
- Explain the role of Artificial Intelligence in cloud security.
- Identify the key components of the Zero Trust cybersecurity approach.

12.1 Zero Trust

Historically, access to information resources (servers, databases, etc.) was segregated according to whether the user of those resources was “inside” or “outside” of the data center, with a firewall boundary separating the two. This was compared to an egg: hard shell, soft inside. Once inside the firewall perimeter, it was a lot easier to connect from one resource to another (known as a lateral move). The inside of the perimeter was a monolithic zone of trust.

ZT is a cybersecurity approach that rejects unfounded sources of trust. In other domains of this guidance, examples are given. In this section, we focus on general principles. Cloud Security Alliance (CSA) has a much more extensive body of knowledge that discusses how ZT can be implemented in organizations at large.

ZT does not start by identifying general attacks and controls, but by identifying the "protect surface": the data, applications, assets, and services (DAAS) that need protecting. From that perspective, it becomes much easier to identify the relevant attack surface that surrounds the protect surface, which helps promote more granular access controls.

12.1.1 Technical Objectives of Zero Trust

The technical objectives of ZT can all be used to improve cloud security.

- **Protective Framework:** ZT's core assumption is that an organization should not inherently trust any principle within or beyond its boundaries.
- **Simplified User Experience:** Zero Trust Architecture (ZTA) streamlines access by using a consistent model for all requests, eliminating complicated access controls and ensuring just-in-time authorization. Who are you? What resource do you need to access now? Here is the access for X time period.
- **Reduced Attack Surface:** ZTA implements strict access controls, continuous authentication, and least privilege principles across the entire network and infrastructure.
- **Reduce Complexity:** ZT reduces IT complexity by creating focused security perimeters around applications and identities, simplifying access control in hybrid, multi-cloud, and edge computing environments.
- **Enforce Principles of Least Privilege:** ZT ensures that users and programs have only the necessary privileges for their tasks, simplifying security management and improving user experience.
- **Improved Security Posture & Resilience:** A reduced attack surface improves the security posture, and makes it easier to recover from security incidents.
- **Improved Incident Containment & Management:** The micro-segmentation and continuous authorization for network access reduces the blast radius of a potential breach as it allows better control over the attacker's lateral movement.

12.1.2 Zero Trust Pillars & Maturity Model

ZT security principles are grouped into pillars that broadly align with our control domains as depicted in Table 1. They work in concert to provide thorough protections for key assets and resources. These pillars

and their respective capabilities and functions are described in the US CISA ZT Maturity Model (ZTMM)[58] and DoD ZT Reference Architecture[59] reference documents. While their depictions of the pillars differ, portions of their models are basically equivalent and fundamentally consistent.

The figure below shows the pillars (Identity, Devices, Networks, Applications and Workloads, Data) and cross-cutting capabilities (visibility, automation, governance) in the CISA ZTMM:

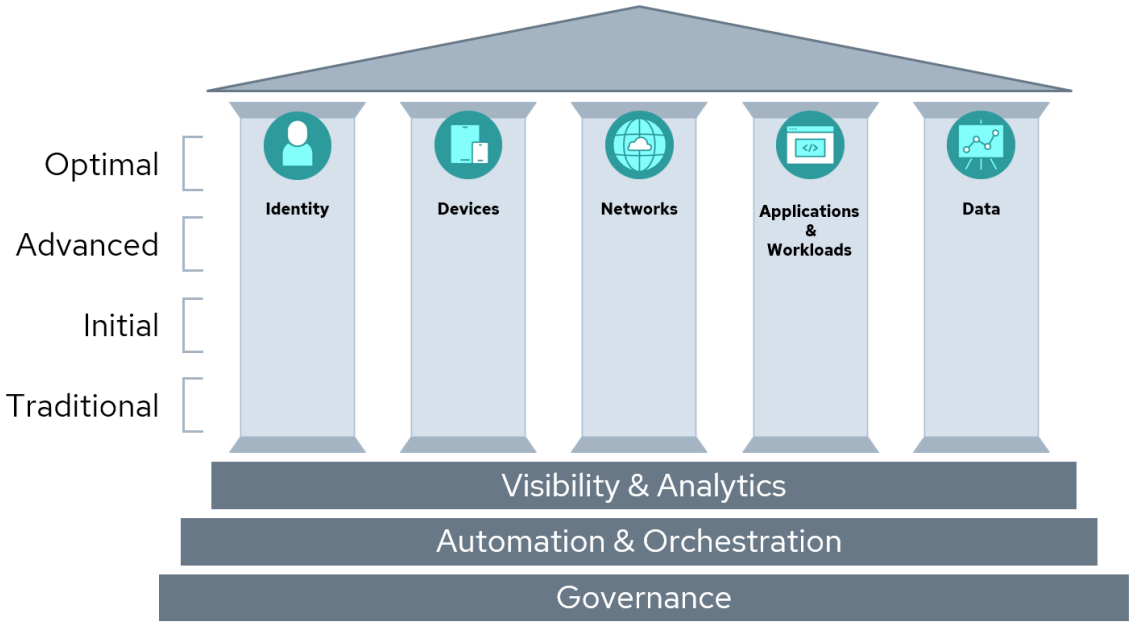

Figure 32: The CISA Zero Trust Maturity Model

- **Users/identities:** Securing, limiting, and enforcing access for persons, non-persons, and federated entities to DAAS, which encompasses the use of identity, credential, and access management capabilities, such as MFA.
- **Devices/endpoints:** Device security hygiene is an input to an access control decision.
- **Networks/environment:** In a ZT approach, networks are highly segregated.
- **Applications and workload**: Applications need protecting, but when compromised, can also be a source of malicious traffic.
- **Data:** Data, wherever stored, is an element to protect.
- **Visibility and analytics** Seeing all access behavior enables anomaly detection and dynamic adaption of security policies.
- **Automation and orchestration** Automate manual security processes to take policy-based actions across the enterprise quickly and at scale.

[58] CISA. (2023) Zero Trust Maturity Model
[59] DOD. (2022) Department of Defence (DOD) - Zero Trust Reference Architecture

- **Governance:** Governance ensures that business, risk, and IT perspectives are aligned. Governance helps to define ZTA policies.

The CISA ZTMM helps organizations enhance their ZT strategies as it outlines maturity stages – Traditional, Initial, Advanced, and Optimal – across the ZT pillars and capabilities. These maturity stages help organizations assess, plan, and implement the necessary measures to progress toward a more secure ZTA.

This maturity model has 4 stages:

1. **Traditional:** security controls are typically based on firewalls and static policies.
2. **Initial:** centralized identity management and device security is introduced. Networks start to be segmented.
3. **Advanced:** continuous and dynamic controls are implemented.
4. **Optimal:** Functions like identity management and network segregation are fully automated and adaptive.

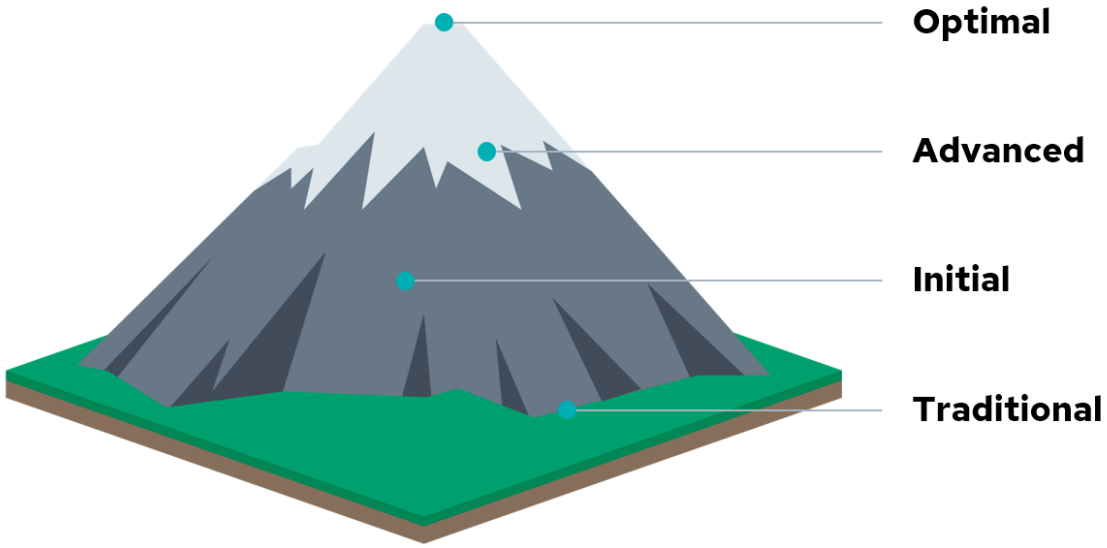

Figure 33: ZT Maturity Journey

12.1.3 Zero Trust & Cloud Security

The table on the following page summarizes ZT principles, mapping them to security domains for how these can be applied to mitigate risks and enhance an organization's overall cybersecurity posture.

Security Domain	Zero Trust Principle
Organizational Management	ZT as an enterprise security and connectivity strategy, best implemented with a ZT culture
Identity and Access Management	Continuous, phishing-resistant MFA with context-based authorization of users, devices, and access requests
Security Monitoring	Monitor everything; presume breaches, detect suspicious activity early and dynamically adjust access
Network	Micro-segmentation, ZT Network Architecture & Software-Defined Perimeter
Workload	ZT device and workload security and integrity verification, malware and data exfiltration monitoring , with ZT workload access controls
Application	Fine-grained, least privilege access authorization with separation of duties; limit user permissions to the minimum required data and functionality
Data	Classify, protect, and monitor data at rest, in transit, and in use with strict ZT data access controls

Table 4: CCSK Security Domains and Corresponding Zero Trust Principles

12.2 Artificial Intelligence

AI serves as both a cloud-hosted service and an emerging tool to bolster cloud security. While AI services are typically hosted in the cloud, it is important to note that on-premises hosting solutions are also available for certain applications. Additionally, AI presents a dual role in cloud security: it can be utilized to enhance cloud security measures, but it also poses a risk as an emerging attack tool. AI-powered algorithms have the capability to discover vulnerabilities, craft exploits, and execute sophisticated attacks, highlighting the importance of securing AI services and implementing robust security measures to defend against AI-driven threats.

12.2.1 Characteristics of AI Workloads

Arguably, the concept of AI is as old as computers are. Alan Turing introduced the "Imitation Game" in 1950 as a test of whether a machine could exhibit intelligent behavior.

Currently, the most popular AI technologies are based on neural networks, which are inspired by the human brain. These networks can run in the hundreds of Gigabytes or more. This gives rise to two different types of workloads: training and inference. Training often consumes massive amounts of training

data and millions of dollars of computing resources to create models that are used by inferencing. In a way, training creates applications, and an inference workload runs them.

Models are used to recognize and classify pictures and sounds, but can also be generative, creating new pictures, sounds, and texts.

A specific popular class of models are the LLMs, which embed language and world knowledge. These are foundational models, in that they can be applied to a wide variety of tasks.

12.1.2 How AI Intersects with Cloud Security

AI workloads are workloads like any other, although often bigger. They also ingest and store large amounts of data, which has its own security implications. Furthermore, they can be consumed as services, as applications, or as components of applications. Consequently, the security aspects of those are discussed in the relevant domains of this guidance.

Of specific relevance to mention is the use of AI as a cloud security defense or attack tool. Security products increasingly embed AI models for better detection and classification. At the same time, AI is being used to craft attacks.

AI workloads related to cloud security can be categorized into the following four areas.

1. **AI as a Service for consumption (full SaaS)**:
   In this model, AI is provided as a complete, ready-to-use service by the cloud provider. Offerings like Claude can leverage AI capabilities without having to build or train an organization's own models. This is ideal for organizations that want to quickly adopt AI without deep technical expertise.

    a. Security controls:
        - Only allow approved services
        - Upgrade for data privacy
        - Only allow approved data
        - Track prompts and results

2. **AI as a Service (PaaS/Foundation model hosting[60])**:
   The cloud provider offers the underlying infrastructure and tools to host and run AI models but leaves the model development and application building to the customer. AWS Bedrock is an example of this - it provides the foundation models and hosting environment, but customers create their own solutions built upon it. This gives organizations more control and customization.

    a. Security controls:
        - Secure training data
        - Secure the application's integration
        - Secure deployment environment

[60] In the context of AI as a service (AIaaS) within a platform as a service (PaaS) model, foundation model hosting involves offering infrastructure and resources optimized for deploying, running, and managing foundational AI models.

- Secure users and access
- Defend against adversarial attacks (examples - injection, jailbreak)

3. **Cloud as workload host for AI (Bring Your Own Model)**:
   In this scenario, organizations develop their own AI models from scratch or deploy off-the-shelf models (code) and simply use the cloud as the hosting environment. They are responsible for the entire AI lifecycle, from data preparation to model training to deployment. The cloud just provides the raw compute resources. This offers the most flexibility but requires the most in-house AI skills and has the same responsibilities as building an in-house application.

4. **AI-enhanced security tools**:
   In addition to the hosting options, AI is being embedded into various cloud security products to make them smarter and more effective. Think AI-powered threat detection, intelligent access control, automated policy enforcement, and so on. As AI matures, expect to see it enhance more traditional security solutions.

Figure 34: Use Cases Where AI Enhances Security Tools and Processes

Next Steps

1. Register on the CSA Exams website
    a. https://exams.cloudsecurityalliance.org/en/signup
2. Purchase a CCSK exam token
    a. https://exams.cloudsecurityalliance.org/en/tokens/select
3. Take the CCSK exam
    a. https://exams.cloudsecurityalliance.org/en/attempts/new
    b. You have two attempts to take the exam

Optional:

1. Get hands on training that is provider-specific for the CSPs you work with
    a. Check out our CCSK Hands On Labs here:
        i. https://cloudsecurityalliance.org/education/ccsk-plus
    b. Check our Self-paced and Instructor Led training here:
        i. https://cloudsecurityalliance.org/education/schedule
2. Advance your skills with additional CSA training:
    a. https://cloudsecurityalliance.org/education
3. Join the CCSK CSA Circle Community: Ask experts questions!
4. Share your success
    a. A certificate is provided at the end of any training option and the CCSK exam
    b. Share your digital badge with your network, which is available for CCSK certificate holders
    c. Provide feedback: there is a survey at the end of any training option and the CCSK exam

Note: More information can be found on the CCSK in the CCSK Prep Kit FAQ and on our CCSK landing page.