Contents

[SECURITY 2](#_Toc159324608)

[CONCEPT OF ZERO TRUST 2](#_Toc159324609)

[CLASSIC TRUSTED MODEL 2](#_Toc159324610)

[ZERO TRUST MODEL 2](#_Toc159324611)

[DEFENCE ON DEPTH 3](#_Toc159324612)

[COMPONENTS OF DEFENSE IN DEPTH 4](#_Toc159324613)

[MICROSOFT DEFENDER FOR CLOUD 5](#_Toc159324614)

[MICROSOFT SENTINEL 5](#_Toc159324615)

[SETTING UP AZURE SENTINELS 5](#_Toc159324616)

# SECURITY

# CONCEPT OF ZERO TRUST

* Before understanding Zero Trust Security Model/Principle. Let’s To understand the concept of classic Trusted Model

## CLASSIC TRUSTED MODEL

* In a typical classic security model ,especially when it comes to getting access to sensitive resources - is based on a concept - referred to as a trusted perimeter, or a trusted boundary for secure access.



* The classic example of a trusted perimeter or trust boundary is internal corporate network.
* Inside the corporate network at the corporate office, we've been able to restrict access to private or sensitive materials to entities or devices inside of that secure network.
* In other words, if you're on the internal corporate network, we have a higher level of trust to those sensitive resources.
* By comparison then - users and devices outside of that corporate network are non-trusted devices. The users, computers, and databases inside of our corporate network or our trusted perimeter are implicitly trusted, and anyone outside of that network is not trusted.



* For remote connection, in order to access our sensitive corporate resources we can set up a VPN client on that external work-from-home entity.
* VPN is simply an extension of that trusted perimeter or extending access to that internal corporate network.
* But, if we provide too much implicit trust to resources inside of a network, Just in case - if one of those internal users gets malware on their computer, well, it can cause havoc on that internal perimeter network because that implicitly trusted user may have too broad of a scope of access. Hence - for challenges like these, this is where the Zero Trust security model comes into play to effectively solve them.

## ZERO TRUST MODEL

* The foundation principle of Zero Trust in Azure is based on the concept of "**never trust, always verify**."
* It challenges the traditional security model that assumes trust once a user or device is inside the network perimeter. Instead, Zero Trust in Azure ensures that every access attempt is continuously verified and validated, regardless of the user's location or the network(trusted /untrusted network) they are connected to.

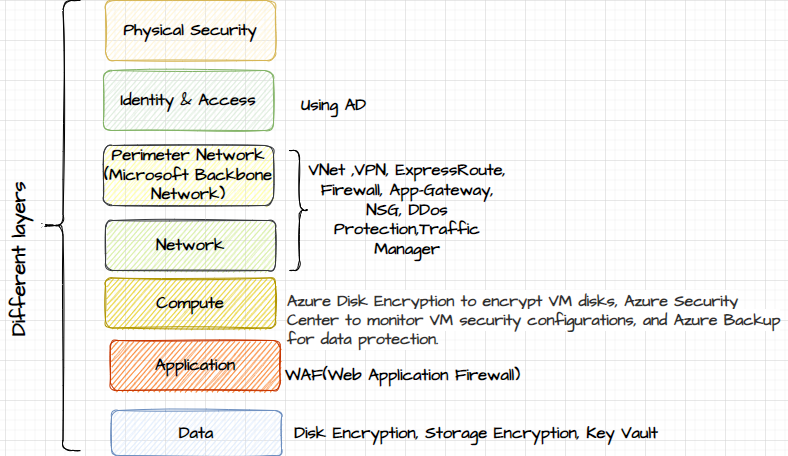
KEY FOUNDATION PRINCIPLES OF ZERO TRUST

* VERIFY EVERY ACCESS
  + Azure implements strong identity and access management practices, ensuring that every user and device attempting to access Azure resources is verified.
  + This involves multi-factor authentication (MFA) to confirm the user's identity and device health checks to assess the security posture.
* LEAST PRIVILEGE ACCESS
  + Azure enforces the principle of least privilege, which means that users are granted the minimum level of access required to perform their specific tasks.
  + This ensures that users only have access to the resources they need and minimizes the risk of unauthorized access.
* ASSUME BREACH
  + Zero Trust in Azure assumes that breaches can happen at any time. Therefore, Azure implements continuous monitoring and threat detection mechanisms to identify potential security incidents and respond to them promptly.
  + This proactive approach helps mitigate the impact of breaches and reduce the time to detect and respond to security threats.
* MICRO-SEGMENTATION
  + Azure supports network segmentation to create isolated environments within the Azure infrastructure. This allows organizations to separate resources into different subnets and control traffic flow between them using Network Security Groups (NSGs) and Azure Firewall.
  + Micro-segmentation reduces the attack surface and limits lateral movement within the network.
* DATA PROTECTION
  + Azure provides various data protection features, including encryption at rest and in transit, data classification, and access controls.
  + These measures help protect sensitive data from unauthorized access and ensure compliance with data privacy regulations.

*By adhering to these foundation principles, organizations can build a Zero Trust architecture in Azure that enhances the overall security of their cloud resources, mitigates the risks of unauthorized access and data breaches, and provides better protection for sensitive information.*

# DEFENCE ON DEPTH

* **Defense in depth in Azure refers to the implementation of multiple layers of security controls and measures to protect Azure resources, data, and applications.**
* Azure provides a comprehensive set of security services and features that can be utilized to establish a strong defense in depth strategy.



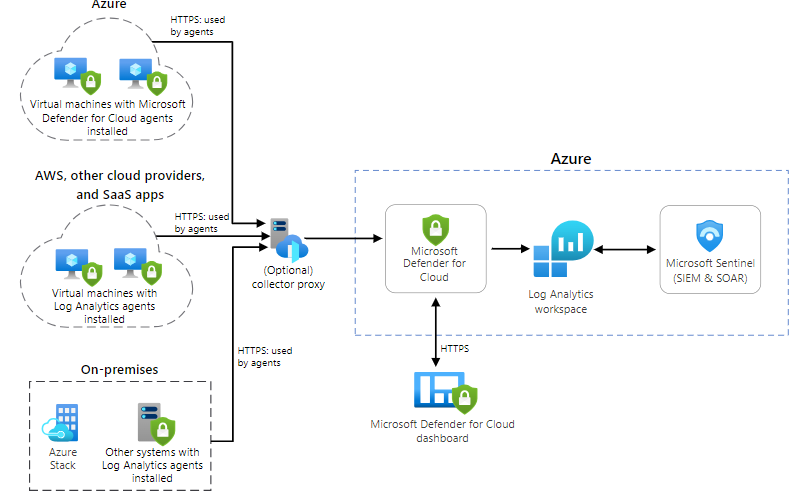
## COMPONENTS OF DEFENSE IN DEPTH

* IDENTITY AND ACCESS MANAGEMENT
  + Azure Active Directory (Azure AD) enables organizations to manage user identities, enforce strong authentication methods, and implement granular access control policies.
  + This helps ensure that only authorized users have access to Azure resources.
* NETWORK SECURITY
  + Azure Virtual Network (VNet) allows you to create isolated network environments within Azure.
  + You can implement Network Security Groups (NSGs), Azure Firewall, and Azure DDoS Protection to control inbound and outbound traffic, protect against network-based attacks, and mitigate distributed denial-of-service (DDoS) attacks.
* DATA ENCRYPTION
  + Azure offers various encryption capabilities to protect data at rest and in transit.
  + Azure Disk Encryption can be used to encrypt virtual machine disks, Azure Storage Service Encryption automatically encrypts data stored in Azure Storage, and Azure Key Vault provides a secure location to manage encryption keys and secrets.
* APPLICATION SECURITY
  + Azure provides services and tools to enhance application security, such as Azure Web Application Firewall (WAF) to protect web applications from common attacks, Azure Security Center to monitor and assess application security, and Azure Functions to securely run serverless applications.
* THREAT DETECTION AND MONITORING
  + Azure Security Center provides continuous monitoring and threat detection capabilities for Azure resources. It uses advanced analytics and machine learning to identify potential security threats, misconfigurations, and vulnerabilities. Azure Sentinel, a cloud-native security information and event management (SIEM) solution, helps organizations collect, analyze, and respond to security events across the Azure environment.
* INCIDENT RESPONSE AND RECOVERY
  + Azure provides features for incident response and recovery, such as Azure Backup for data protection and recovery, Azure Site Recovery for disaster recovery planning, and Azure Security Center's incident response capabilities to help organizations respond to and mitigate security incidents.

# MICROSOFT DEFENDER FOR CLOUD

* Microsoft Defender for Cloud is a cloud-based security solution provided by Microsoft.
* It is designed to help organizations detect and protect against advanced threats and potential breaches within their cloud and hybrid environments.
* It continually assessing the resources for security and provide recommendations to secure the Azure account.
* Based on the recommendations, we can implement certain steps to ensure that security is at the forefront
* We get a secure score to let us know - how secure our account is.

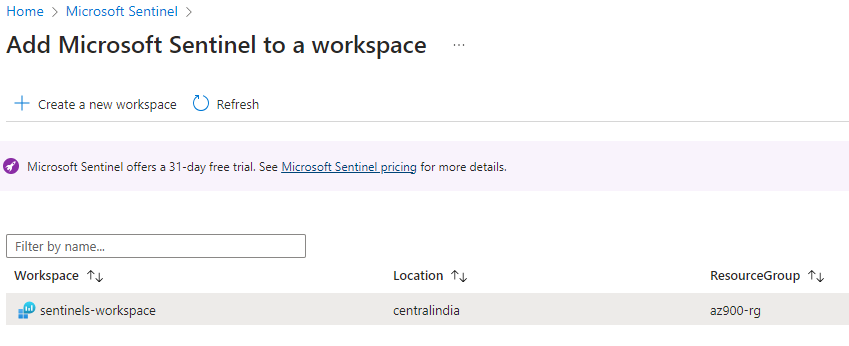
# MICROSOFT SENTINEL



* Microsoft Sentinel tool can be used for security information, event management, security orchestration, automation and response.
* When we host resources on a cloud platform, we can direct the logs to Log Analytics workspace. The logs can be for example, Azure Activity Log (for all the activities that are occurring in Azure account) or sign-in logs from AD.
* We can collect data not only from Azure based services but can also collect data from other third party services as well.
* **We can Microsoft Sentinel on top of the Log Analytics workspace which can look at the collected data from these different sources and detect any sort of threats**.
* Based on collected data it can provide data about the of threat patterns so that we can then respond and investigate threats.

## SETTING UP AZURE SENTINELS

1. Step 1: Create a Log Analytics Workspace
2. Step 2: Creating Azure Sentinels Service. Note – while creation itself it will ask for log analytics workspace.



* DATA CONNECTORS:
  + For the collection of data. Configuration 🡪 data connectors.
  + There are various connectors that allow us to collect data from various sources e.g. Azure Service and other third party services as well.
* ANALYTICS
  + Once the data is collected we can search for any sort of threat using in-built or custom rules from Analytics
  + Using Playbooks we can automate i.e. we automate the mitigation to the threats that are detected.

