# General Security & Network Security

Shailendra Chauhan

Microsoft MVP, Technical Consultant and Corporate Trainer

# Agenda

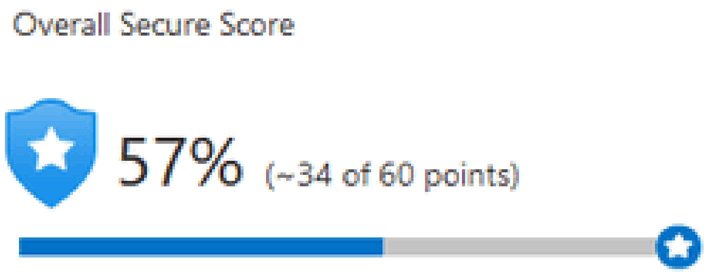
- Azure Security Center
- Secure Score
- Azure Sentinel
- Key Vault
- Azure Dedicated Hosts
- Network Security Groups (NSG)
- Defense in depth
- Azure Firewall
- Azure DDoS protection

# Azure Security Center

- Monitor security settings across on-premises and cloud workloads.
- Automatically apply required security settings to new resources as they come online.
- Provide security recommendations that are based on your current configurations, resources, and networks.
- Use machine learning to detect and block malware from being installed on your virtual machines (VMs) and other resources.
- Provide just-in-time access control for network ports to reduces your attack surface by ensuring that the network only allows traffic from verified source.

# Secure Score

- Secure score is based on the percentage of security controls that you satisfy.
- The more security controls you satisfy, the higher secure score you receive.
- Secure score report on the current state of your organization's security posture.
- Secure score improve your security posture by providing discoverability, visibility, guidance, and control.

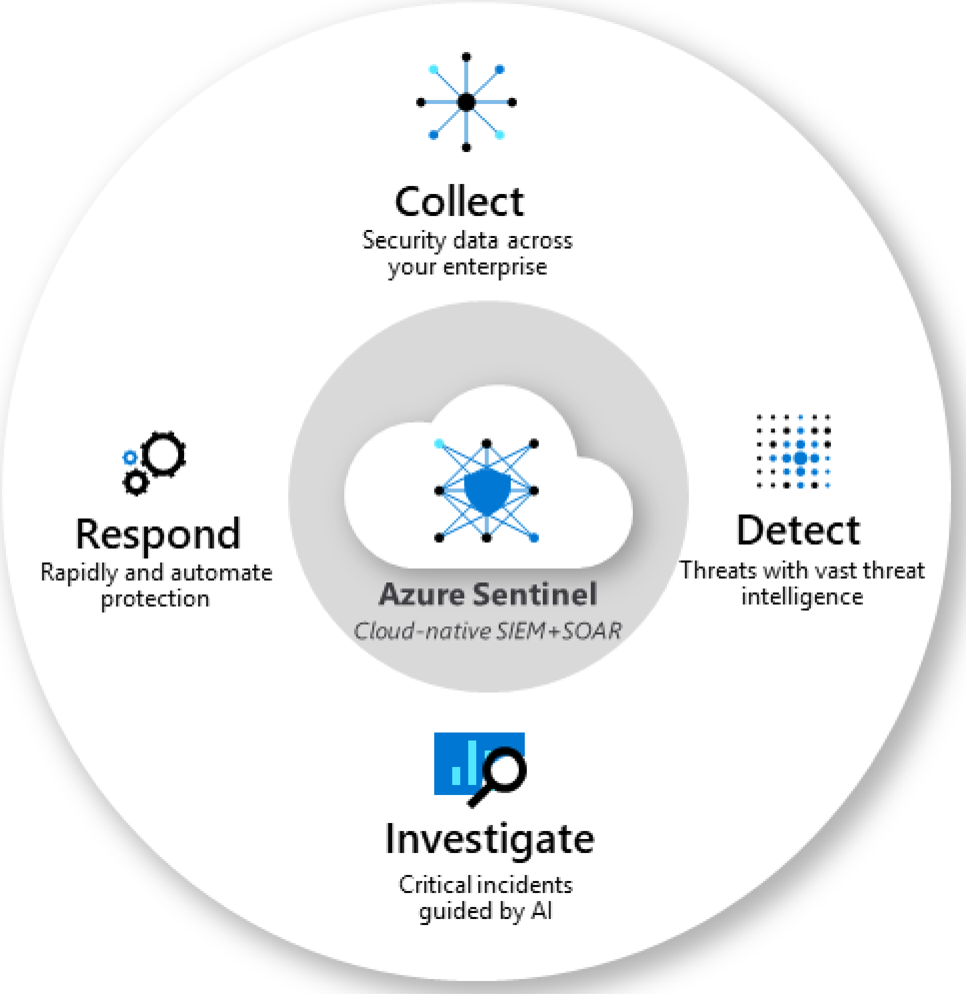


Overall Secure Score

57% (~34 of 60 points)

# Azure Sentinel

- A scalable, cloud-native, security information event management (SIEM) system.
- Provides intelligent security analytics for your entire enterprise.
- Provide a single solution for alert detection, threat visibility, proactive hunting, and threat response

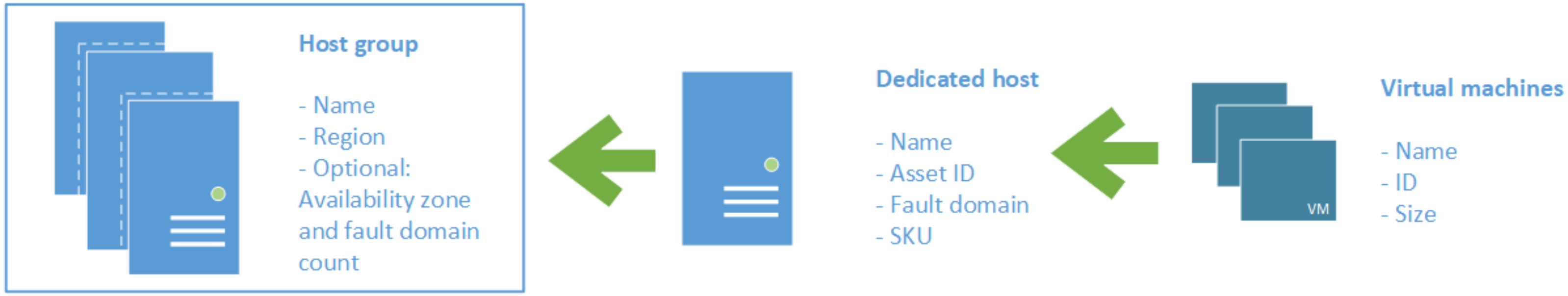

Collect
Security data across your enterprise
Respond
Rapidly and automate protection
Azure Sentinel
Cloud-native SIEM+SOAR
Detect
Threats with vast threat intelligence
Investigate
Critical incidents guided by AI

# Azure Key Vault

- A centralized cloud service for storing an application's secrets in a single, central location.
- Azure Key Vault is a safe place to store passwords, connection strings, access codes, and certificate keys
- Fully managed by Azure, so you don’t have to worry about the underlying infrastructure.

# Azure Dedicated Host

- On Azure, virtual machines (VMs) run on shared hardware that Microsoft manages.
- Azure Dedicated Host provides dedicated physical servers to host your Azure VMs for Windows and Linux.
- You're charged per dedicated host, independent of how many virtual machines you deploy to it.
- A *host group* is a collection of dedicated hosts.

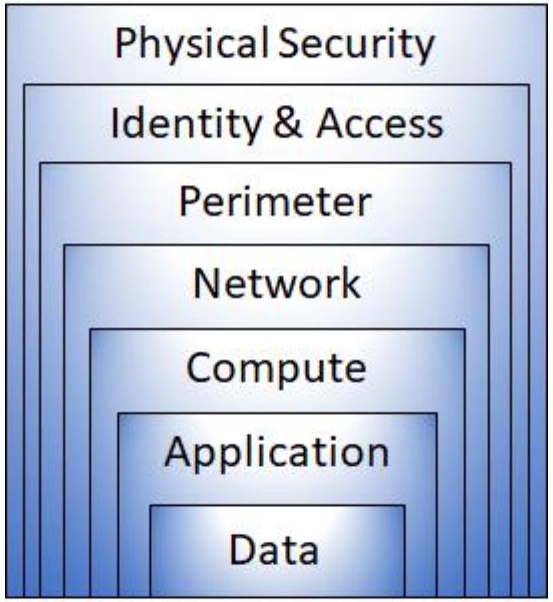


# Network Security Group

- A network security group enables you to filter network traffic to and from Azure resources within an Azure virtual network.
- NSGs works like an internal firewall.
- An NSG can contain multiple inbound and outbound security rules that enable you to filter traffic to and from resources by source and destination IP address, port, and protocol.

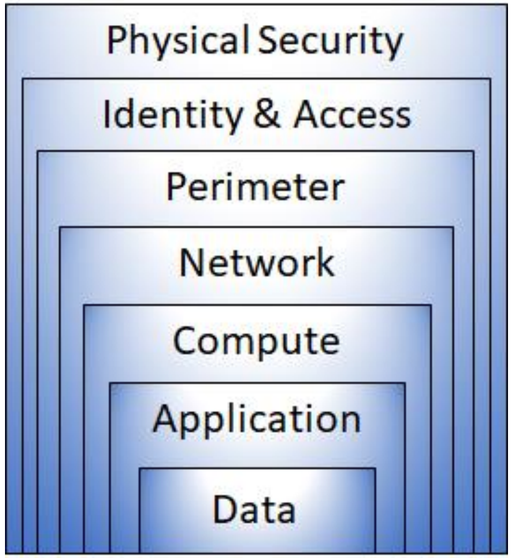
# Defense in depth

- Protect information and prevent it from being stolen by those who aren't authorized to access it.
- These layers provide a guideline for you to help make security configuration decisions in all of the layers of your applications.



# Layers of defense in depth

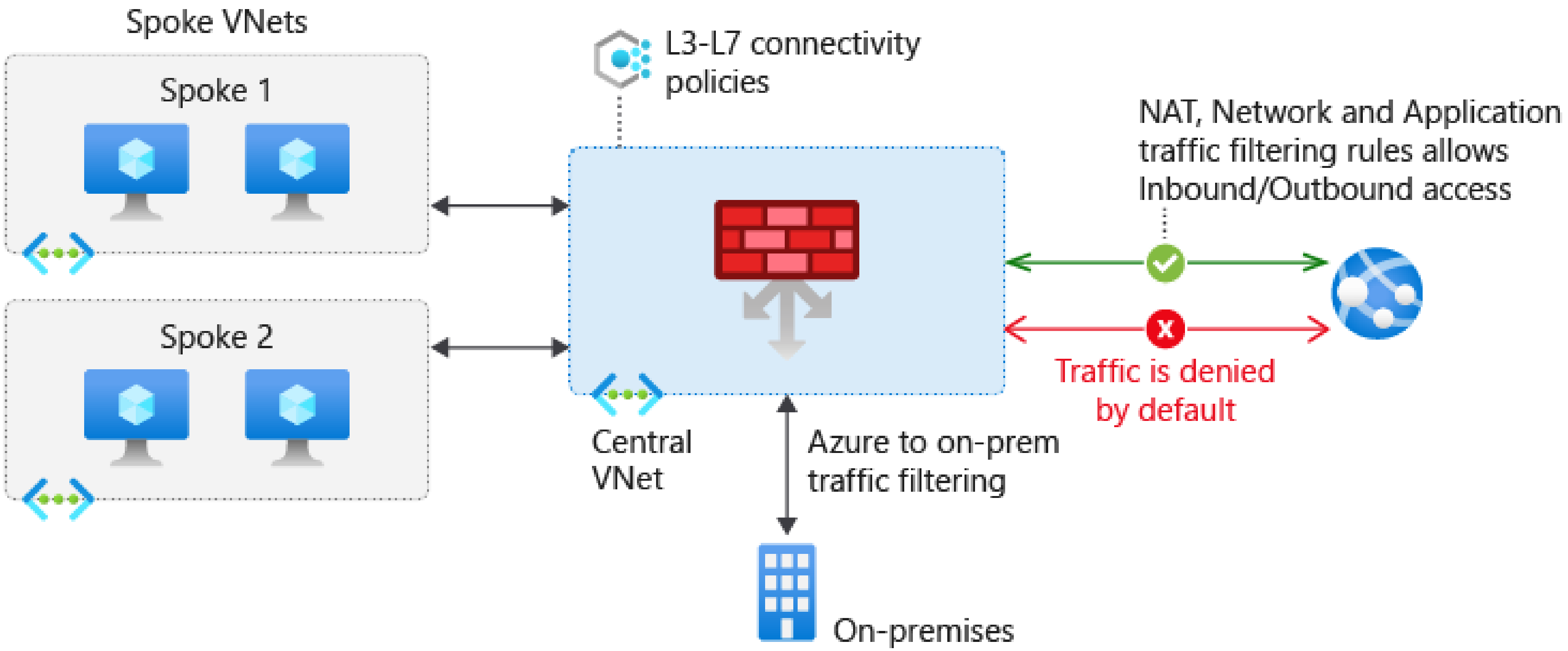
- The ***physical security* layer** is the first line of defense to protect computing hardware in the datacenter.
- The ***identity and access* layer** controls access to infrastructure and change control.
- The ***perimeter* layer** uses distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.
- The ***network* layer** limits communication between resources through segmentation and access controls.
- The ***compute* layer** secures access to virtual machines.
- The ***application* layer** helps ensure that applications are secure and free of security vulnerabilities.
- The ***data* layer** controls access to business and customer data that you need to protect.



DotNetTricks

# Azure Firewall

- A managed, cloud-based network security service that protect resources in your Azure virtual networks.



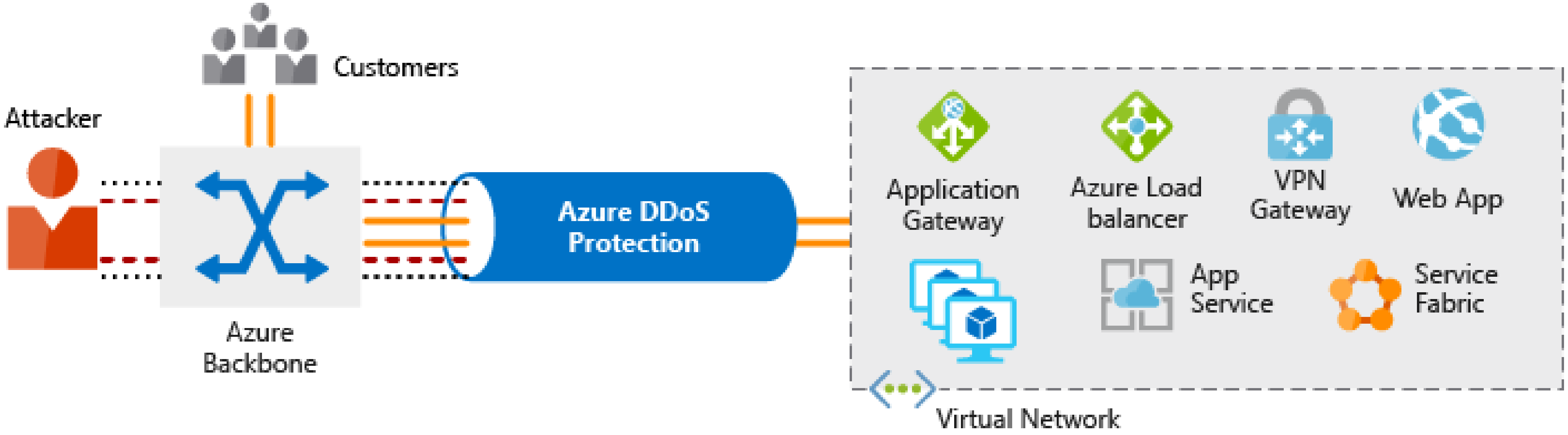
Spoke VNets
Spoke 1
Spoke 2
L3-L7 connectivity policies
NAT, Network and Application traffic filtering rules allows Inbound/Outbound access
Traffic is denied by default
Central VNet
Azure to on-prem traffic filtering
On-premises

# DDoS Atacks - Distributed Denial of Service

- DDoS attack attempts to crush or exhaust an application's resources and making the application slow or unresponsive.
- DDoS attacks can target any resource that's publicly reachable through the internet, including websites.

# Azure DDoS Protection

- Azure DDoS Protection identifies the attacker's attempt to overwhelm the network and blocks further traffic from them, ensuring that traffic never reaches Azure resources.


Customers
Attacker
Azure Backbone
Azure DDoS Protection
Application Gateway
Azure Load balancer
VPN Gateway
Web App
App Service
Service Fabric
Virtual Network