**PROTECT AGAINST SECURITY THREADS**

Hi, and welcome to this module on general security and network security in Azure. In this module, you'll learn about how :

* Azure can help you protect the workloads that you run in both the Cloud and in your On-premises data center.
* You will also learn about the Azure services you can use to help ensure that your network is safe, secure, and trusted.
* More specifically, after completing this module, you will know the concepts of how to strengthen your security posture and protect against threats by using Azure Security Center,
* Collect and act on security data from many different sources by using Azure Sentinel, store and access sensitive information such as passwords and encryption key securely in Azure Key Vault.
* Manage dedicated physical servers to host your Azure VMs for Windows and Linux by using Azure Dedicated Host.
* Identify the layers that make up a defense-in-depth strategy.
* Explain how Azure firewall enables you to control what traffic is allowed on the network.
* Configure network security groups to filter network traffic to and from Azure resources within a Microsoft Azure Virtual Network, and
* Explain how Azure DDoS Protection helps protect your Azure resources from DDoS attacks.

Let's dive right into our case study. To demonstrate this, we are going to use our case study to give you an opportunity to apply the concepts you'll learn. Tailwind Traders operates retail hardware stores across the globe and online. It specializes in competitive pricing, fast shipping, and a large range of items. It's looking at Cloud technologies to improve business operations and support growth into new markets. By moving to the Cloud, the company plans to enhance its shopping experience to further differentiate itself from competitors. Tailwind Traders runs a mix of workloads on Azure and in its Data Center. The company needs to ensure that all of its systems meet a minimum level of security and that its information is protected from attacks. The company also needs a way to collect and act on security events from across its digital state.

Let's explore how Tailwind Traders can use some of the tools and features in Azure as part of its overall security strategy. In this lesson, you'll learn about some of the security tools that can help keep your infrastructure and data safe when you work in the Cloud.

Security is a small word for a significant concept. There are so many factors to consider in order to protect your applications and your data. How does Azure help you protect workloads that you run in the Cloud and in your On-premises Data Center? After completing this lesson, you'll be able :

1. to know the concepts of how to strengthen your security posture and protect against threats by using Azure Security Center,
2. Collect and act on security data from many different sources by using Azure Sentinel,
3. Store and access sensitive information such as passwords and encryption keys securely in Azure Key Vault,
4. Manage dedicated physical servers to host your Azure VMs for Windows and Linux by using Azure Dedicated Host.

----------------------------------------------------------------------------------------------------------------------------------------------------------

**Protect against security threats by using Azure Security Center**

Tailwind traders is broadening its use of Azure services. It still has on-premises workloads with current security-related configuration, best practices, and business procedures. How does the company ensure that all of its systems meet a minimum level of security and that its information is protected from attacks? Many Azure services include built-in security features. Tools on Azure can also help Tailwind traders with this requirement. Let's start by looking at Azure Security Center.

**Azure Security Center is a monitoring service that provides visibility of your security posture across all of your services, both on Azure and on-premises**. The term security posture refers to cybersecurity policies and controls, as well as how well you can predict, prevent, and respond to security threats.

A screenshot of a computer

Description automatically generated

**Security centers can :**

1. **Monitor security settings across on-premises and cloud workloads**.
2. **Automatically apply** required security settings to new resources as they come online.
3. **Provide security recommendations** that are based on your current configurations, resources, and networks.
4. **Continuously monitor** your resources and perform automatic security assessments to identify potential vulnerabilities before those vulnerabilities can be exploited.
5. **Use machine learning** to detect and block Malware from being installed on your virtual machines and other resources. You can also use adaptive application controls to define rules that list allowed applications to ensure that only applications you allow can run.
6. **Detect attack** and analyze potential inbound attacks and investigate threats and any post-breach activity that might have occurred, and
7. Provide **just-in-time access control** for network ports. Doing so reduces your attack surface by ensuring that the network only allows traffic that you require at the time that you need it to.

Tailwind traders can use Security Center to get a detailed analysis of different components in its environment. Because the companies’ resources are analyzed against the security controls of any governance policies it has assigned, it can view its overall regulatory compliance from a security perspective all from one place. Here's an example of what you might see in Azure Security Center.

A screenshot of a computer

Description automatically generated Let's say the Tailwind traders must comply with the payment card, industries data security standard. This report shows that the company has the resources that it needs to remediate. In the resource security hygiene section, Tailwind traders can see the health of its resources from a security perspective. To help prioritize remediation actions, recommendations are categorized as low, medium, and high. Let's now take a look at how secure score is implemented. Secure score is a measurement of an organization's security posture.

A secure score is based on security controls or groups of related security recommendations. Your score is based on the percentage of security controls that you satisfy. The more security controls you satisfy, the higher the score you receive. Your score improves when you remediate all of the recommendations for a single resource within a control. In this example from the Azure portal, we can see the portal showing a score of 57 percent or 34 out of 60 points. Following the secure score, recommendations can help protect your organization from threats. From a centralized dashboard and Azure Security Center, organizations can monitor and work on the security of their Azure resources like identities, Data, apps, devices, and Infrastructure. Secure score helps you report on the current state of your organization's security posture. Improve your security posture by providing discoverability, visibility, guidance, and control, and compare benchmarks and established key performance [inaudible].

Security Center also includes Advanced Cloud defense capabilities for Virtual Machines, network security, and file integrity. Let's look at how some of these capabilities apply to Tailwind traders.

* **Just in time VM access**, Tailwind traders will configure just-in-time access to VMs. This access blocks traffic by default to specific network ports of virtual machines but allows traffic for a specified time when an administrator requests and approves it.
* **Adaptive application controls**. Tailwind traders can control which applications are allowed to run on its virtual machines. In the background, Security Center uses machine learning to look at the processes running on a virtual machine. It creates exceptional rules for each resource group that holds the virtual machines and provides recommendations. This process provides alerts that inform the company about unauthorized applications that are running on its VMs.
* **Adaptive network hardening**. Security Center can monitor the internet traffic patterns of the VMs and compare those patterns with the company's current network security group settings or NSG settings. From there, the security center can make recommendations on whether the NSGs should be locked down further and provide remediation steps.
* **File integrity monitoring**. Tailwind traders can also configure the monitoring of changes to important files on both Windows and Linux, registry settings, applications, and other aspects that might indicate a security attack.

As you can see, Tailwind traders can use Security Center to get a centralized view of all of its security alerts. From there, the company can dismiss false alerts, investigate them further, remediate alerts manually, or use an automated response with a workflow automation.

* This workflow automation uses Azure Logic Apps and Security Center Connectors.
* The Logic App can be triggered by a threat detection alert or biosecurity center recommendation filtered by name or by severity.
* You can then configure the logic App to run an action, such as sending an email or posting a message to a Microsoft Teams channel.

----------------------------------------------------------------------------------------------------------------------------------------------------------

**Detect and respond to security threats by using Azure Sentinel**

Security management on a large scale can benefit from a dedicated security information and event management, or a SIEM system. Security Information and Event Management (SIEM System)

A SIEM system aggregate security data from many different sources as long as those sources support an open standard logging format. It also provides capabilities for threat detection and response. Azure sentinel is Microsofts cloud based SIEM system, it uses intelligence security analytics and threat analysis.

Azure sentinel enables you to :

* **collect cloud data** at scale across all users, devices, applications and infrastructure both on premises and from multiple clouds.
* **Detect (threats)** previously undetected threats while minimizing false positives by using Microsoft's Comprehensive Analytics and Threat Intelligence.
* **Investigate threats** with artificial intelligence and examine suspicious activities at scale. Tapping into years of cybersecurity experience from Microsoft.
* **Respond to incidents** rapidly by utilizing, built in orchestration and automation of common tasks.

Let's go back to the tailwind traders case study. In this instance, Tailwind decides to explore the capabilities of Azure Sentinel.

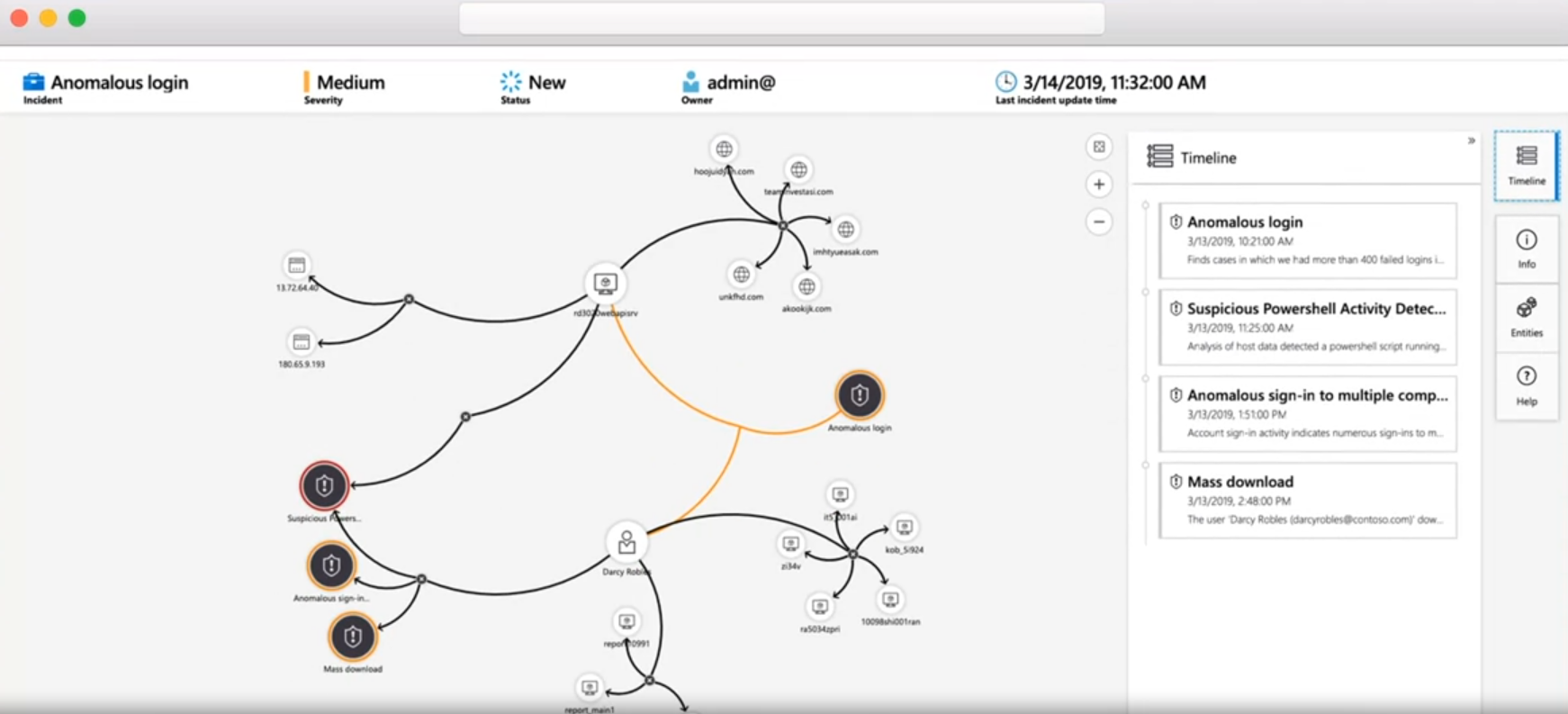
First, the company identifies and connects its data sources. Azure Sentinel supports a number of data sources, which it can analyze for security events. These connections are handled by built in connectors are industry standard log formats and API’s.

* **Connect Microsoft Solutions**, Connectors provide real time integration for services like Microsoft Threat Protection Solutions. Microsoft 365 sources, including office 365 , Azure Active Directory and Windows Defender Firewall
* **Connect other servies and solutions**, Connectors are available for common non-Microsoft services and solutions, including AWS Cloud Trail, Citrix Analytics, Sophos, Extra Firewall, VM Ware Carbon Black Cloud and Okta SSO.
* **Connect industry-standard data sources,** Azure sentinel supports data from other sources that use the common of informal messaging standard. SIS Log Arrest API.

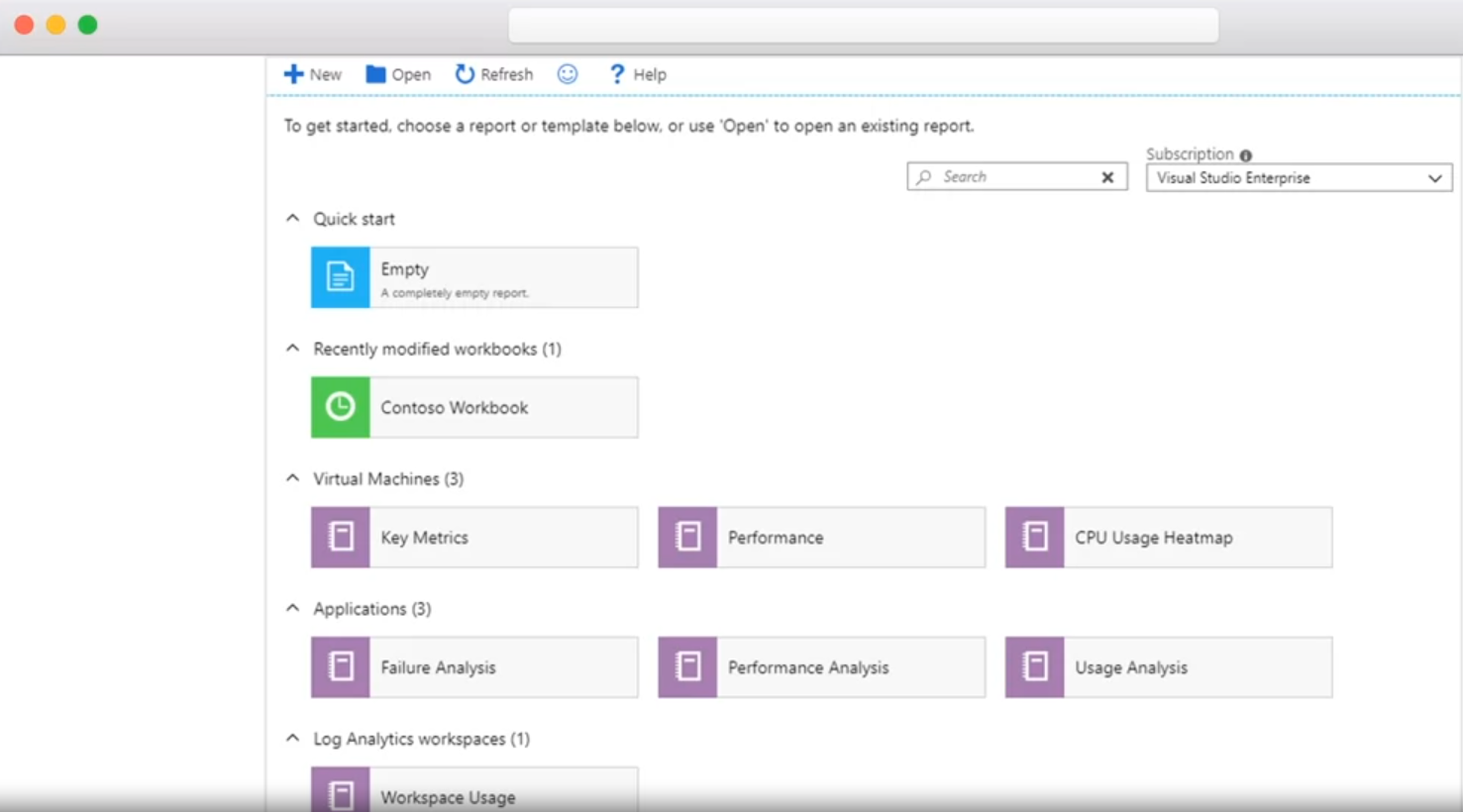
Tailwind traders needs to be notified when something suspicious occurs, it decides to use both built in analytics and custom rules to detect threats.

1. **Built in analytics** use templates designed by Microsoft's team of security experts and analysts. They're based on unknown threats, common attack vectors and escalation chains for suspicious activity. These templates can be customized and search across the environment for any activity that looks suspicious. Some templates use machine learning behavioral analytics that are based on Microsoft proprietary algorithms.
2. **Custom analytics** are rules that you create to search for specific criteria within your environment. You can preview the number of results that the query would generate based on past log events and set a schedule for the query to run.

You can also set an alert threshold when Azure Sentinel detect suspicious events, tailwind traders can investigate specific alerts are incidents. **Incidents are a group of related alerts**. This is what an investigation graph looks like in Azure Sentinel.



With the investigation graph, the company can review information from entities directly connected to the alert and see common exploration queries to help guide the investigation. You can also use Azure monitor workbooks to automate responses to threats.



Workbooks can run manually or automatically. When a rule triggers an alert, for example, it can set an alert that looks for malicious IP addresses that access the network and create a workbook that does the following steps. When the alert is triggered,

* it **opens a ticket** in the IT ticketing system.
* Then it **sends a message** to the Security Operations channel, In Microsoft teams or slack to make sure the security analysts are aware of the incident.
* Next, it **sends all of the information** in the alert to the senior network admin and to the security admin.
* The email message includes two user option buttons, **block or ignore**. When an admin chooses to block the IP address is blocked in the firewall, and the user is disabled in azure Active directory. When an admin chooses to ignore, the alert is closed in Azure Sentinel, and the incident is closed in the IT ticketing system, The workbook continues to run after it receives a response from the admins.

---------------------------------------------------------------------------------------------------------------------------------------------------------

**Store and manage secrets by using Azure Key Vault**

Let's take a look at how Azure Key Vault is used to store and manage secrets. Once again, we will use an example from our Tailwind Traders case study.

As Tailwind Traders builds its workloads in the cloud, it needs to carefully handle sensitive information such as passwords, encryption keys, and certificates. This information needs to be available for an application to function, but it might allow an unauthorized person access to application data.

**Azure Key Vault is a centralized cloud service for storing an application secret in a single central location.** It provides secure access to sensitive information by providing access control and logging capabilities. Now that we know what Azure Key Vault is, let's take a look at what Azure Key Vault can do.

Azure Key Vault can help you :

* **Manage secrets**. You can use Key Vault to securely store and tightly control access to tokens, passwords, certificates, API keys, and other secrets.
* A screenshot of a computer

  Description automatically generated**Manage encryption keys**, you could use Key Vault as a key management solution. Key Vault makes it easier to create and control the encryption keys that are used to encrypt your data.
* **Manage SSL/TLS certificates**, Key Vault enables you to provision, manage, and deploy your public and private secure sockets layer, transport layer security, or SSL/TLS certificates for both your Azure resources and your internal resources.
* **Store secrets backed by hardware security modules or HSMs**. These secrets and keys can be protected either by software or by FIPS 140-2 level 2 validated HSMs.

A screenshot of a computer

Description automatically generated

Here's an example that shows us certificates used for testing Key Vault. You'll add a secret key vault later in this module.

The benefits of using Key Vault include :

* **Centralized application secrets**. Centralizing the storage for your applications secrets enables you to control their distribution and reduces the chances that secrets are accidentally leaked.
* **Securely stores secrets and keys**. Azure uses industry standard algorithms, key lengths, and HSMs. Access to Key Vault requires proper authentication and authorization.
* **Access monitoring and access control**. By using Key Vault, you can monitor and control access to your application secrets.
* **Simplified administration of application secrets**. Key Vault makes it easier to enroll and renew certificates from public certificate authorities, RCAs. You can also scale up and replicate content within regions and use standard certificate management tools.
* **Integration with other Azure services**. You can integrate key vault with storage accounts, container registries, event hubs, and many more Azure services. These services can then securely reference the secrets stored in Key Vault.

----------------------------------------------------------------------------------------------------------------------------------------------------------

**Exercise - Manage a password in Azure Key Vault**

Click on the link below to start the exercise:

<https://docs.microsoft.com/en-us/learn/modules/protect-against-security-threats-azure/5-manage-password-key-vault>

<https://learn.microsoft.com/en-us/training/paths/azure-fundamentals-describe-azure-architecture-services/>

In this exercise, you add a password to Azure Key Vault. A password is an example of sensitive information that you need to protect. You then read the password from Azure Key Vault to verify that the password is accessible.

In practice, there are several ways to add secrets to and read secrets from Key Vault. You can use the Azure portal, the Azure CLI, or Azure PowerShell. By using your favorite programming language, your applications can also securely access the secrets that they need.

Here, you create a secret in Key Vault by using the Azure portal. You then access the secret from the portal and from the Azure CLI in Azure Cloud Shell.

The Azure CLI is a way to work with Azure resources from the command line or from scripts. Cloud Shell is a browser-based shell experience to manage and develop Azure resources. Think of Cloud Shell as an interactive console that runs in the cloud.

---------------------------------------------------------------------------------------------------------------------------------------------------------

**Host your Azure virtual machines on dedicated physical servers by Using Azure Dedicated Host**

On Azure, VMs run on shared hardware that Microsoft manages. Although the underlying hardware is shared, your VM workloads are isolated from workloads that other Azure customers run. However, some organizations must follow regulatory compliance that requires them to be the only customer using the physical machine that hosts their virtual machines. To facilitate this requirement, Azure dedicated host provides dedicated physical servers that will host your Azure VMs for Windows and Linux.

A diagram of a server

Description automatically generatedHere's a diagram that shows how virtual machines relate to dedicated hosts and host groups.

* **A dedicated host is mapped to a physical server in an Azure datacenter.**

Azure Dedicated Host provides dedicated physical servers to host an organizations Azure VMs for Windows and Linux, and

* **A host group is a collection of dedicated hosts**.

Now that we know that a dedicated host is mapped to a physical server in an Azure datacenter, let's take a look at some of the benefits of using Azure dedicated host.

Azure dedicated host gives you:

* **visibility** into and control over the server infrastructure that's running your Azure VMs.
* Helps **address compliance requirements** by deploying your workloads on an isolated server.
* **Custom configurations,** Let’s you choose the number of processors, server capabilities, VM series, and VM sizes within the same host.

After a dedicated host is provisioned, Azure assigns it to the physical server in Microsoft's cloud datacenter.

* For high availability, you can **provision multiple hosts** in a host group and deploy your virtual machines across this group.
* VMs and dedicated hosts can also take advantage of **maintenance control**.
* 35 Day window, This feature enables you to control when regular maintenance updates occur within a 35-day rolling window.

You're charged per dedicated host independent of how many virtual machines you deploy to it. The host price is based on the VM family, type, or hardware size and region.

Software licensing, storage, and network usage are billed separately from the host And VMs.

Congratulations, you have completed this lesson on how to protect against security threats on Azure. You learned how to use Azure Security Center to strengthen your security posture and protect against threats. You learned how to collect and act on security data from many different sources by using Azure Sentinel. We looked at how to store and access sensitive information such as passwords and encryption key securely in Azure Key Vault. We also covered how you can manage dedicated physical servers to host your Azure VMs for Windows and Linux by using Azure dedicated host.

----------------------------------------------------------------------------------------------------------------------------------------------------------

1. With Azure Security Center, you can define a list of allowed applications to ensure that only applications you allow can run. Azure Security Center can also detect and block malware from being installed on your VMs.
2. Azure Key Vault is a centralized cloud service for storing your applications' secrets in a single, central location. It provides secure access to sensitive information by providing access control and logging capabilities.
3. By default, virtual machines (VMs) on Azure run on shared hardware that's managed by Microsoft. Although the underlying hardware is shared, VM workloads are isolated from workloads being run by other Azure customers. However, some organizations must follow regulatory compliance that requires them to be the only customer using the physical machine that hosts their virtual machines. Azure
4. Secure score is based on security controls, or groups of related security recommendations. Your score is based on the percentage of security controls that you satisfy. The more security controls you satisfy, the higher the score you receive.
5. Azure Sentinel is Microsoft's cloud based SIEM solution. Azure Sentinel enables you to collect cloud data at scale. It can collect data across all users, devices, applications, and infrastructure, both on-premises and from multiple clouds. It can be used to detect previously undetected threats and minimize false positives by using Microsoft's analytics and threat intelligence.
6. Azure Security Center is a monitoring service that provides visibility of your security posture across all your services on Azure and on-premises.
7. Azure Sentinel is Microsoft's cloud based SIEM solution and can combine and report on security data from different sources.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

A screenshot of a computer security center

Description automatically generatedA screenshot of a computer error

Description automatically generated

A screenshot of a computer

Description automatically generated

----------------------------------------------------------------------------------------------------------------------------------------------------------

**SECURE NETWORK CONNECTIVITY ON MICROSOFT AZURE**

Welcome to this lesson on Secure Network Connectivity on Azure. This is an important topic. Every application and service, whether On-premises, or in the cloud, needs to be designed with security in mind. There's too much at risk. For example, a denial-of-service attack might prevent customers from reaching your website or services and block you from doing business. Or, your website might be defaced, causing damage to your reputation. A data breach would be even worse, because it can ruin hard earned trust, while causing significant personal and financial harm. Let's go back to our case study on Tailwind Traders, a fictitious home improvement retailer that operates retail hardware stores across the globe, and online. #

Tailwind Traders specializes in competitive pricing, fast shipping, and a large range of items. It's looking at cloud technologies to improve business operations, and support growth into new markets. By moving to the cloud, the company plans to enhance its shopping experience to further differentiate itself from competitors.

As Tailwind Traders moves to the cloud, it needs to evaluate its:

* **Security needs**, before it can deploy a single line of code to production.
* **Network configuration and network traffic,** Although security must be considered at every layer in the company's applications, all the way from the physical service to the application data, some factors relate specifically to the **network configuration** and **network traffic** of cloud-based workloads.
* **Network security capabilities,** In this lesson, you'll focus on the network security capabilities in Azure, and review how they help you secure your solutions in the cloud, based on your business needs.

After completing this lesson, you'll be able to identify :

* **Defense in depth strategy,** the layers that make up a defense in depth strategy.
* **Control traffic with Azure firewall,** Explain how Azure Firewall enables you to control what traffic is allowed on the network.
* **Configure network security groups** to filter network traffic to and from Azure resources within a Microsoft Azure virtual network.
* Explain how Azure DDoS protection helps protect your Azure resources from DDoS attacks.

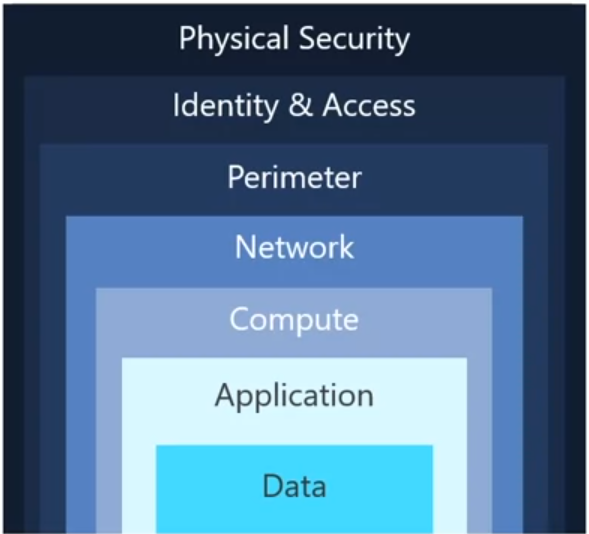
---------------------------------------------------------------------------------------------------------------------------------------------------------

**What is defense in depth?**

Tailwind Traders currently runs its work clothes on premises in its data center. **Running on premises means that the company is responsible for all aspects of security,** from physical access to buildings all the way down to how data travels in and out of the network. The company wants to know how its current defense in depth strategy compares to running in the cloud.

The objective of defense and depth is to protect information and prevent it from being stolen by those who aren't authorized to access it. A defense and death strategy uses a series of mechanisms to slow the advance of an attack that aims at acquiring unauthorized access to data**. Each layer provides protection**, so that if one layer is breached, a subsequent layer is already in place to prevent further exposure. This approach removes reliance on any single layer of protection. It slows down an attack and provides alert telemetry that security teams can act upon either automatically or manually..

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



These layers provide a guideline for you to help make security configuration decisions in all of the layers of your applications. Azure provides security tools and features at every level of the defense and death concept. Let's take a closer look at each layer.

1. Physically securing access to buildings and controlling access to computing hardware within the data center, are the first line of defense. With physical security, the intent is to provide physical safeguards against access to assets. Thes safeguards ensure that other layers can be bypassed and last or theft is handled appropriately. Microsoft uses various physical security mechanisms in its cloud data centers.
2. At the identity and access layer. It's important to control access to infrastructure and change control. Use single sign on (SSO), multi factor authentication and ordered events and changes. The identity and access layers is all about ensuring that identities are secure, access is granted only to what's needed and sign and events and changes are logged. We will cover identity and access and details in another module
3. At the perimeter layer. It's important to use DDoS protection to filter large scale attacks before they can affect the availability of a system for users. Use perimeter firewalls to identify an alert on malicious attacks against your network. At the network perimeter, it's about protecting from network-based attacks against your resources. Identifying these attacks, eliminating their impact and alerting you when they happen are important ways to keep your network secure
4. At the network layer. It's important to limit communication between resources, deny by default, restrict inbound Internet access and limit outbound access where appropriate and implement secure connectivity to on premises networks. At this layer, the focuses on limiting the network connectivity across all your resources to allow only what's required. By limiting this communication, you reduce the risk of an attack spreading to other systems in your network.
5. At the compute layer, it's important to secure access to virtual machines and implement in point protection on devices and keep systems patched and current. Malware unpatched systems and improperly secured systems open your environment to attacks. The focus in this layer is on making sure that your computer resources are secure and that you have the proper controls in place to minimize security issues
6. At application layer. It's important to ensure that applications are secure and free of vulnerabilities, storing sensitive application secrets in a secure storage medium, makes security a design requirement for all application development. Integrating security into the application development lifecycle helps reduce the number of vulnerabilities introduced in cold. Every development team should ensure that its applications are secure by default. In almost all cases, **Attackers are after data :**
   1. Stored in a database,
   2. Stored on disk inside virtual machines
   3. Stored in software as a service application (SaaS), such as Office 365 and managed through cloud storage.
   4. **Managed through cloud storage**, those who store and control access to data are responsible for ensuring that it's properly secured. Often, regulatory requirements dictate the controls and processes that must be in place to ensure the confidentiality, integrity and availability of the data. We will cover privacy compliance and data protection standards on azure in detail in another module.
7. Your security posture is your organization's ability to protect from and respond to security threats. The common principles used to define a security posture. Are confidentiality, integrity and availability, known collectively as CIA (Confidentiality, Integrity and Availability).
   1. **Confidentiality** uses the principle of least privilege, which means restricting access to information only to individuals explicitly granted access and only the level that they need to perform their work. This information includes protection of user passwords, email content and access levels to applications and underlying infrastructure.
   2. **Integrity** prevents unauthorized changes to information at rest when it's stored and in transit when it's being transferred from one place to another, including from a local computer to the cloud. A common approach used in data transmission is for the sender to create a unique fingerprint off the data by using a one-way hashing algorithm. The hash is sent to the receiver along with the data. The receiver Recalculates the data is hash and compares it to the original to ensure that the data wasn't lost or modified in transit
   3. **Availability** ensures that services are functioning and can be accessed only by authorized users. Denial of service attacks are designed to degrade the availability of a system affecting its users.

----------------------------------------------------------------------------------------------------------------------------------------------------------

**Protect virtual networks by using Azure Firewall**

**A Firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules**. You can create firewall rules that specify ranges of IP addresses. Only clients granted IP addresses from within those ranges are allowed to access the destination server. Firewall rules can also include specific network protocol and port information.

Tailwind Traders currently runs Firewall appliances, which combine hardware and software to protect its on-premises network. These firewall appliances require a monthly licensing fee to operate, and they require IT staff to perform routine maintenance. As Tailwind Traders move to the cloud, the IT manager wants to know what Azure services can protect both the company's cloud networks and it's on-premises networks.

**Azure Firewall is a managed cloud-based network security service that helps protect resources in your Azure virtual networks. A virtual network is similar to a traditional network that you'd operate in your own data center. It's a fundamental building block for your private network that enables virtual machines and other compute resources to securely communicate with each other, the internet and on-premises networks.** This diagram shows a basic Azure Firewall implementation.

A computer screen shot of a computer

Description automatically generated

Azure Firewall is a Stateful Firewall. A Stateful Firewall analyzes the complete context of a network connection, not just an individual package of network traffic. Azure Firewall features high availability and unrestricted cloud scalability. Azure Firewall provides :

* **Central location for connectivity policies,** A central location to create, enforce and log application and network connectivity policies across subscriptions and virtual networks.
* **Static public IP address,** It uses a static, unchanging public IP address for your virtual and network resources, which enables outside Firewalls to identify traffic coming from your virtual network. The service is integrated with Azure Monitor to enable logging and analytics.

Azure Firewall provides many features including :

* built-in high availability,
* unrestricted cloud scalability,
* inbound and outbound filtering rules,
* inbound destination network address translation or DNAT support, and
* Azure Monitor logging.

You typically deploy Azure Firewall on a central virtual network to control general network access. With Azure Firewall, you can :

* Configure application rules that define fully qualified domain names or FQDNs that can be accessed from a subnet.
* Network rules that define source, address, protocol, destination port, and destination address.
* Network address translation, also known as NAT, rules that define destination IP addresses and ports to translate inbound requests.

Azure Application Gateway also provides a firewall that's called the Web Application Firewall or WAF. WAF provides centralized inbound protection for your web applications against common exploits and vulnerabilities. Azure front door and Azure Content Delivery Network, or CDN, also provides WAF services.

---------------------------------------------------------------------------------------------------------------------------------------------------------

**Protect from DDoS attacks by using Azure DDoS Protection**

any large company can be the target of a large-scale network attack. Attackers might flood your network to make a statement simply for the challenge. Tailwind traders is no exception. as Tailwind traders moves to the cloud, it wants to understand how Azure can prevent DDoS and other attacks. Now you learn how Azure DDoS protection standard service tear helps protect your Azure resources from DDoS attacks.

First, let's define what a DDoS attack is.

* **DDoS attack attempts to overwhelm and exhaust and applications resources,** making the application slow or unresponsive to legitimate users.
* DDoS attacks can target any resource that's publically reachable through the Internet, including websites.

As your DDoS Protection standard, helps protect your azure resources from DDoS attacks. When you combine DDoS protection with recommended application design practices, you help provide a defense against DDoS attacks. DDos protection uses the scale and elasticity of Microsoft's global network to bring DDoS mitigation capacity to every Azure region. The DDoS Protection Service helps protect your azure applications by analyzing and discarding DDoS traffic at the azure network edge, before it can affect your services availability. This diagram shows network traffic flowing into Azure from both customers and an attacker.

A diagram of a computer network

Description automatically generated

DDoS Protection identifies the attacker's attempt to overwhelm the network and blocks further traffic from them, ensuring that traffic never reaches as your resources. Legitimate traffic from customers still flows into azure without any interruption of service details.

DDoS protection can also help you :

* **Help manage your cloud consumption**. When you run on premises, you have a fixed number of computer resources, but in the cloud, **elastic computing means that you can automatically scale out your deployment to meet demand**. A cleverly designed DDoS attack can cause you to increase your resource allocation, which incurs unneeded expense details.
* **Ensure network load reflects usage**, Protection standards helps ensure that the network load you process reflects customer usage.
* **Credit for costs in DDoS attack,** you can also receive credit for any costs accrued for scaled out resources during DDoS attack.

There are several service tiers available to DDoS protection.

1. **The basic service** here is automatically enabled for free as part of your azure subscription. It ensures that azure infrastructure itself is not affected during a large-scale DDoS attack.
2. **The standard service** here provides additional mitigation capabilities that are tuned specifically to Azure virtual network resources. DDoS protection standard is relatively easy to enable and requires no changes to your applications. Protection policies are tuned through dedicated traffic monitoring and machine learning algorithms. Policies are applied to public IP addresses, which are associated with resources deployed in virtual networks such as Azure load balancer, an application gateway.

Both the basic and standard tears provide always on traffic monitoring and real time mitigation of common network level attacks. They provide the same defense is that Microsoft's online services use. The Azure global network is used to distribute and mitigate attack traffic across Azure regions.

The standard service tiers can help prevent :

* Volumetric attacks, where the goal of this attack is to flood the network claire with a substantial amount of seemingly legitimate traffic.
* Protocol attacks, which render a target inaccessible by exploiting a weakness in the Layer three and Layer four protocol stack and
* Resource layer or application layer attacks, which is provided only with web application firewall.

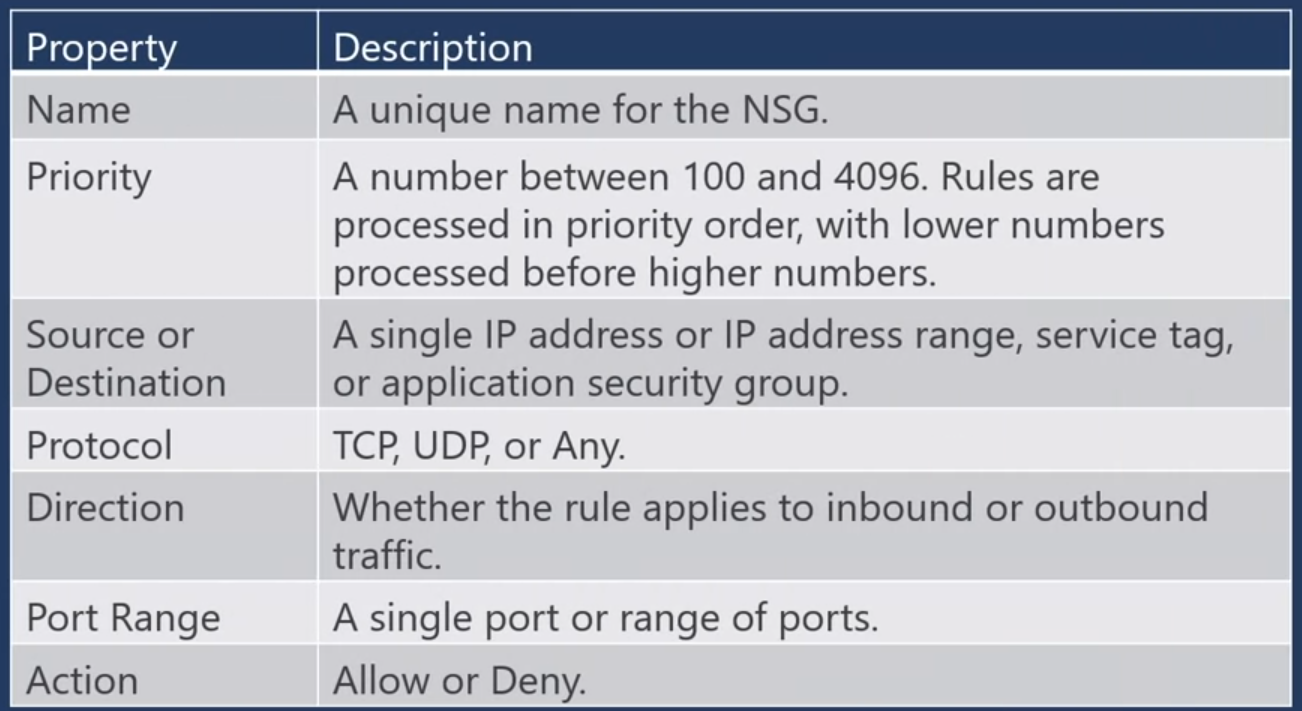
These attacks target web application packets to disrupt the transmission of data between the hosts. You need a Web Application Firewall (WAF) to protect against layer seven attacks. DDoS protection standard protects the WAF from volumetric and protocol attacks.

----------------------------------------------------------------------------------------------------------------------------------------------------------

**Filter network traffic by using network security groups**

Although Azure firewall and Azure DDoS protection can help control what traffic can come from outside sources. Tailwind traders also want to understand how to protect its internal networks on Azure. Doing so, will give the company and extra layer of defense against attacks. Now, you will examine network security groups are NSGs.

**A Network security group (NSG) enables you to filter network traffic to and from Azure resources within an Azure virtual network**. You can think of NSGs 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. A network security group can contain as many rules as you need within Azure subscription limits. When you create a network security group, Azure creates a series of default rules to provide a baseline level of security. You can't remove the default rules, but you can overwrite them by creating new rules with higher priorities. Each rule specifies the properties you can see in the table on screen.



----------------------------------------------------------------------------------------------------------------------------------------------------------

**Exercise - Configure network access to a VM by using a network security group**

In this exercise, you configure network access to a virtual machine (VM) running on Azure.

You start by creating a Linux VM and installing Nginx, a popular web server, on that VM. To make your web server accessible, you then create a network security group (NSG) rule that allows inbound access on port 80 (HTTP).

There are many ways to create and manage VMs, including their network settings. For example, you can use the Azure portal, the Azure CLI, Azure PowerShell, or an Azure Resource Manager (ARM) template.

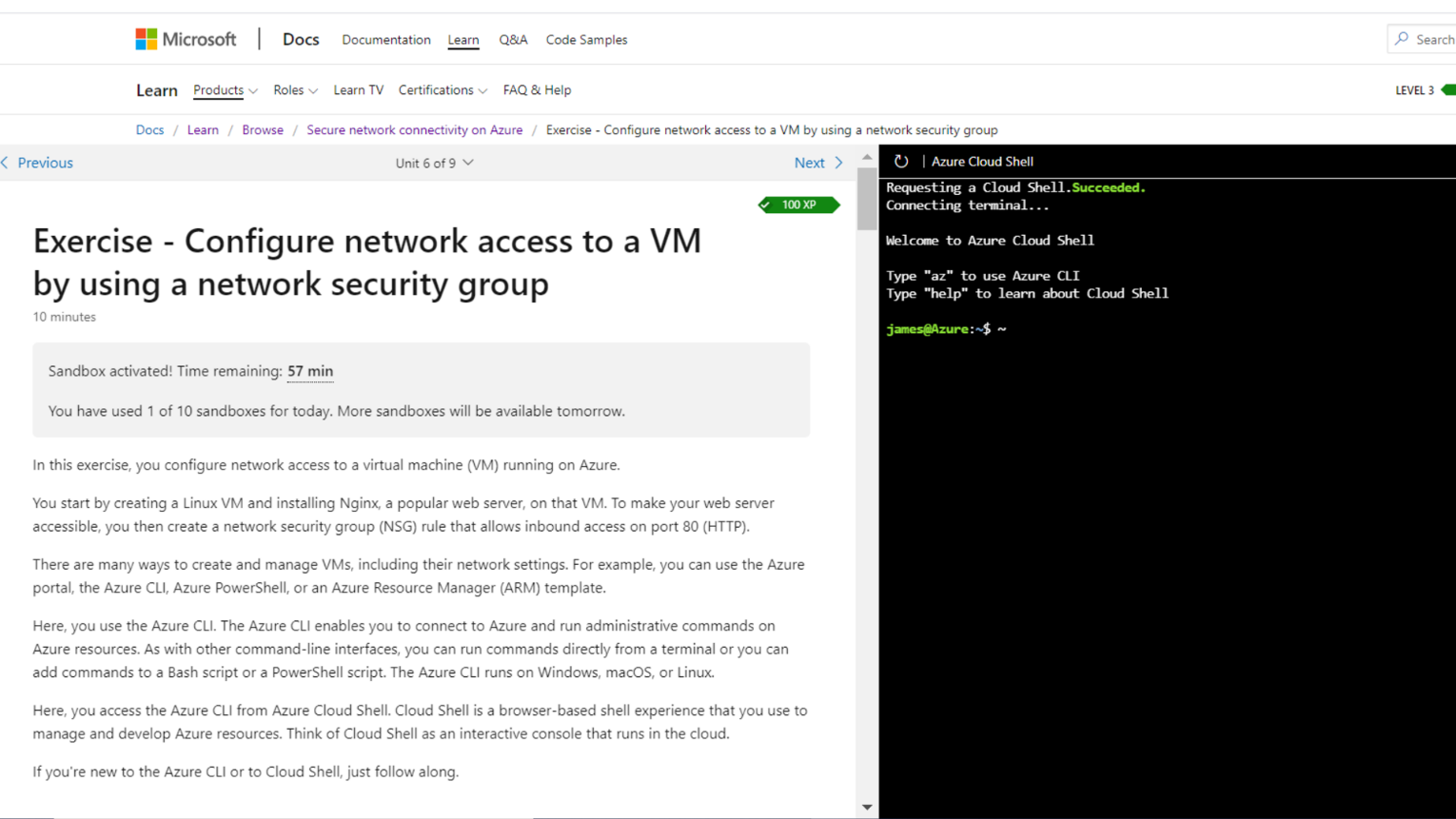
Here, you use the Azure CLI. The Azure CLI enables you to connect to Azure and run administrative commands on Azure resources. As with other command-line interfaces, you can run commands directly from a terminal or you can add commands to a Bash script or a PowerShell script. The Azure CLI runs on Windows, macOS, or Linux.

Here, you access the Azure CLI from Azure Cloud Shell. Cloud Shell is a browser-based shell experience that you use to manage and develop Azure resources. Think of Cloud Shell as an interactive console that runs in the cloud.

If you're new to the Azure CLI or to Cloud Shell, just follow along.

Click the link below to start the exercise.   <https://docs.microsoft.com/en-us/learn/modules/secure-network-connectivity-azure/6-configure-access-network-security-group>

<https://learn.microsoft.com/en-us/training/paths/azure-fundamentals-describe-azure-architecture-services/>



---------------------------------------------------------------------------------------------------------------------------------------------------------

**Combine Azure services to create a complete network security solution**

When you're considering an Azure security solution, consider all the elements of defense-in-depth. Next, we will present some recommendations on how to combine Azure services to create a complete network security solution.

* The perimeter layer is about protecting your organization's resources from network-based attacks. Identifying these attacks, alerting the appropriate security teams, and eliminating their impact are important to keeping your network secure. To do this, you can use :
  + Azure DDoS protection to filter large-scale attacks before they can cause a denial of service for users.
  + Use perimeter firewalls with Azure Firewall to identify and alert on malicious attacks against your network.

At this layer, the focus is:

* **Limit network connectivity,** on limiting network connectivity across all of your resources to allow only what's required.
* **Segment your resources and use network-level controls** to restrict communications to only what's needed. By restricting connectivity, you reduce the risk of lateral movement throughout your network from an attack.
* **Use network security** groups to create rules that define allowed inbound and outbound communication at this layer.

The recommended practices for securing the network layer are :

* to limit communication between resources by segmenting your network and configuring access controls.
* Deny by default,
* Restrict inbound Internet access
* Limit outbound where appropriate
* Implement secure connectivity to on-premises networks.

You can combine Azure networking and security services to manage your network security and provide increased layered protection. Here are two ways you can combine services.

* **Azure Firewall complements the functionality of network security groups (NSG).**
  + Together, they provide better defense-in-depth network security.
  + Network security groups provide distributed network layer traffic filtering to limit traffic to resources within virtual networks in each subscription.
  + Azure Firewall is a fully stateful centralized network firewall-as-a-service. It provides network level and application-level protection across different subscriptions and virtual networks.
* You can also combine **Azure Application Gateway Web Application Firewall (WAF) and Azure Firewall**.
  + WAF is a feature of Azure Application Gateway that provides your web applications with centralized inbound protection against common exploits and vulnerabilities.
  + Azure Firewall provides inbound protection for non-HTTPS protocols. For example, RDP, SSH, and FTP. Outbound network-level protection for all ports and protocols, and application-level protection for outbound HTTPS. Combining them provides more layers of protection.

----------------------------------------------------------------------------------------------------------------------------------------------------------

Identifying beneficial Azure services depends on your organization's specific needs, but here are some commonly valuable ones:

1. \*\*Azure Virtual Machines\*\*: For flexible compute power. If your department requires scalable resources for applications or testing environments, this is essential.

2. \*\*Azure Functions\*\*: For serverless computing, enabling you to run code without managing servers. This can streamline workflows and reduce overhead for small, event-driven tasks.

3. \*\*Azure DevOps\*\*: To improve collaboration in software development. It offers tools for CI/CD, project management, and version control, which can enhance productivity.

4. \*\*Azure SQL Database\*\*: If your organization needs reliable and scalable database solutions. It simplifies database management and can handle varying loads efficiently.

5. \*\*Azure Blob Storage\*\*: For cost-effective storage of large amounts of unstructured data. This is ideal for backup, archiving, or big data applications.

6. \*\*Azure Machine Learning\*\*: To leverage AI and data analytics. If your work involves data analysis, this can help automate processes and gain insights.

7. \*\*Azure Logic Apps\*\*: To automate workflows and integrate apps and services. This can save time on repetitive tasks and improve efficiency.

\*\*Service That Could Help Most\*\*: If your daily work involves frequent tasks that could be automated, \*\*Azure Logic Apps\*\* might provide the most immediate benefit by streamlining processes and improving efficiency. If your focus is on development, then \*\*Azure DevOps\*\* would likely be the most impactful for enhancing collaboration and deployment practices.

Choosing the right service ultimately hinges on your specific challenges and objectives!

Based on the management tools and security solutions studied, Azure Security Center, Azure Monitor, and Azure Sentinel would be particularly beneficial for an organization.

Azure Security Center provides a unified view of security across Azure resources, helping to identify vulnerabilities and offering best practice guidelines. This is crucial for enhancing the organization’s security posture and ensuring compliance with data protection regulations.

Azure Monitor offers comprehensive monitoring capabilities, allowing teams to collect and analyze telemetry data from Azure resources. It helps identify performance issues and resource utilization, leading to improved operational efficiency and quicker troubleshooting.

Among these, Azure Monitor would likely be the most beneficial for daily work. Its ability to set up alerts and create customized dashboards enables proactive monitoring of applications and services. This enhances responsiveness to performance issues, ultimately improving productivity and service reliability.

---------------------------------------------------------------------------------------------------------------------------------------------------------

1. DDoS Protection can help protect your Azure resources from DDoS attacks. A DDoS attack attempts to overwhelm and exhaust an application's resources, making the application slow or unresponsive to legitimate users.
2. Azure Firewall provides Network Address Translation (NAT) rules that can define destination IP addresses and ports to translate inbound requests.
3. The Basic service tier is automatically enabled for free as part of your Azure subscription. Always-on traffic monitoring and real-time mitigation of common network-level attacks provide the same defenses that Microsoft's online services use. The Basic service tier ensures that Azure infrastructure itself is not impacted during a large-scale DDoS attack. Azure's global network is used to distribute and mitigate attack traffic across Azure regions.
4. The Standard service tier provides additional mitigation capabilities that are tuned specifically to Azure Virtual Network resources. The Standard tier also provides always-on traffic monitoring and real-time mitigation of common network-level attacks.
5. A Network Security Group (NSG) enables you to filter network traffic to and from Azure resources within an Azure Virtual Network. You can think of network security groups like an internal firewall.
6. A network security group rule enables you to filter traffic to and from resources by source and destination IP address, port, and protocol.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

----------------------------------------------------------------------------------------------------------------------------------------------------------

1. Azure Sentinel is Microsoft's cloud-based SIEM solution and can combine and report on security data from different sources.
2. Secure score is based on security controls, or groups of related security recommendations. Your score is based on the percentage of security controls that you satisfy. The more security controls you satisfy, the higher the score you receive.
3. Azure Key Vault is a centralized cloud service for storing your applications' secrets in a single, central location. It provides secure access to sensitive information by providing access control and logging capabilities.
4. Azure firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
5. Azure Firewall allows the configuration of application rules that define fully qualified domain names (FQDNs) that can be accessed from a subnet.

A white text on a blue background

Description automatically generatedA screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

---------------------------------------------------------------------------------------------------------------------------------------------------------

**Weekly Summary**   
Tailwind Traders face several security challenges. In today's digital world, its needs aren't unique. Azure provides tools and services that can help you detect an act on important security events. It also provides ways to help keep your data safe, which can prevent security incidents from happening to begin with.

1. In the first lesson, you learned about Azure services that relate to security.

* Azure Security Center provides visibility of your security posture across all of your services, both on Azure and on-premises.
* Azure Sentinel aggregates security data from many different sources and provides additional capabilities for threat detection and response.
* Azure Key Vault stores your application secrets such as passwords, encryption keys, and certificates in a single central location.
* Azure Dedicated Host provides dedicated physical servers to host your Azure VMs for Windows and Linux.

2. In the second lesson, you learned about some of the ways you can secure network traffic, both on Azure and in your on-premises data center. We covered an important topic, defense in depth. Defense in depth helps us think about security as a multiple layer, multiple vector concern. Threats come from places we don't expect, and they can come with surprising strength. Tailwind traders now has a few tools and services that it can use to secure its networks.

* Azure firewall is a managed cloud-based network security service that helps protect resources in Azure virtual networks.
* An Azure virtual network is similar to a traditional network that you'd operate in your own data center. It enables virtual machines and other computer resources to securely communicate with each other. The internet and on-premises networks.
* A network security group enables you to filter network traffic to and from Azure resources within a Virtual Network.
* Azure DDoS protection helps protect Azure resources from DDoS attacks.

----------------------------------------------------------------------------------------------------------------------------------------------------------  
**Additional reading**

**Azure Security Center**

1. Take the [Resolve security threats with Azure Security Center](https://docs.microsoft.com/en-us/learn/modules/resolve-threats-with-azure-security-center/) <https://learn.microsoft.com/en-us/training/paths/sc-200-mitigate-threats-using-azure-defender/> module to use the alert capabilities of Azure Security Center to watch for and respond to threats.
2. Then review the [planning and operations guide](https://docs.microsoft.com/en-us/azure/security-center/security-center-planning-and-operations-guide) <https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-planning-and-operations-guide>  to optimize your use of Security Center based on your organization's security requirements and cloud management model.

**Azure Sentinel**

1. [Design a holistic monitoring strategy on Azure](https://docs.microsoft.com/en-us/learn/modules/design-monitoring-strategy-on-azure/) <https://learn.microsoft.com/en-us/training/modules/design-monitoring-strategy-on-azure/> goes into greater depth on how Azure Sentinel can help monitor and respond to security threats across your organization.
2. Also learn how to [connect data sources](https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources) <https://learn.microsoft.com/en-us/azure/sentinel/connect-data-sources?tabs=azure-portal> to Azure Sentinel.

**Azure Key Vault**

Gain additional hands-on experience with Azure Key Vault in [Manage secrets in your server apps with Azure Key Vault](https://docs.microsoft.com/en-us/learn/modules/manage-secrets-with-azure-key-vault/) <https://learn.microsoft.com/en-us/training/modules/manage-secrets-with-azure-key-vault/>  and [Configure and manage secrets in Azure Key Vault](https://docs.microsoft.com/en-us/learn/modules/configure-and-manage-azure-key-vault) <https://learn.microsoft.com/en-us/training/modules/configure-and-manage-azure-key-vault/>

---------------------------------------------------------------------------------------------------------------------------------------------------------

**Congratulations and next steps**

Congratulations, you have completed the Azure Management Tools and Security Solutions Course.

Management tools encompass a wide array of tools and services from Microsoft Azure. In this course, you have looked at many of these tools and services and chose the best one for a given business scenario. You have also examined the various services you can use to help ensure that your cloud resources are safe, secure and trusted. At this point, you should be able to choose :

* the correct Azure Artificial Intelligence Service to address different kinds of business challenges.
* The best software development process, tools and services for a given business scenario.
* The correct cloud monitoring, service and management tool to address different kinds of technical needs and challenges.
* The right serverless computing technology for your business scenario.
* And the best Azure IoT service for a given business scenario.

You should also be able to :

* Strengthen your security posture and protect against threats by using Azure Security Center.
* Collect and act on security data from many different sources by using Azure Sentinel.
* Store and access sensitive information such as passwords and encryption keys securely in Azure Key Vault.
* Manage dedicated physical servers to host your Azure VMs for Windows and Linux by using Azure dedicated host.
* Secure network connectivity on Azure.

Demonstrating knowledge of these topics is a **requirement in the AZ-900 Microsoft Azure Fundamentals exam**. You are one step further down the road to certification.

The next course will cover identity, governance, privacy and compliance features on Azure. It would be the next step in further preparing for the AZ-900, so you can pursue a career using Microsoft Azure.Make sure to check the reading material that follows, for information on what's to come in the next course.

----------------------------------------------------------------------------------------------------------------------------------------------------------

**What to expect next**

**The next course will cover Azure Identity Services, how to build a Cloud Governance Strategy on Azure, Privacy, Compliance & Data Protection Standards on Azure, and how to Manage Costs & SLA Service Cycles.**

**Module 1**

**In module 1, you will learn about Azure Identity Services.**

**You will study the difference between authentication and authorization, Azure Active Directory provides identity and access management, and the role single sign-on (SSO), multifactor authentication, and Conditional Access play in managing user identity.**

**Module 2**

**Module 2 will deal with building a Cloud Governance Strategy on Azure.**

**You will learn how to make organizational decisions about your cloud environment by using the Cloud Adoption Framework for Azure and how to define who can access cloud resources by using Azure role-based access control.**

**You will also learn how to apply a resource lock to prevent accidental deletion of your Azure resources and how to apply tags to your Azure resources to help describe their purpose.**

**You will cover how to control and audit how your resources are created by using Azure Policy and how to enable governance at scale across multiple Azure subscriptions by using Azure Blueprints.**

**Module 3**

**In module 3, you will address Privacy, Compliance & Data Protection Standards on Azure.**

**You will be able to explain the types of compliance offerings that are available on Azure. Also, you will access the Microsoft Privacy Statement, the Online Services Terms, and the Data Protection Addendum to learn what personal data Microsoft collects, how Microsoft uses it, and for what purposes.**

**You will gain insight into regulatory standards and compliance on Azure from the Trust Center and from the Azure compliance documentation. You will also be able to explain Azure capabilities that are specific to government agencies.**

**Module 4**

**Finally, module 4, will cover Managing Costs & SLA Service Cycles.**

**In module 4, you will learn how to:**

* **Use the Total Cost of Ownership Calculator to compare your current datacenter costs to running the same workloads on Azure.**
* **Describe the different ways you can purchase Azure products and services.**
* **Use the Pricing calculator to estimate the monthly cost of running your cloud workloads.**
* **Define some of the major factors that affect total cost and apply recommended practices to minimize cost.**
* **Describe what a service-level agreement (SLA) is and why SLAs are important.**
* **Identify factors, such as the service tier you choose, that can affect an SLA.**
* **Combine SLAs to compute a composite SLA.**
* **Describe the service lifecycle in Azure, including how to access new capabilities that are coming to Azure.**

---------------------------------------------------------------------------------------------------------------------------------------------------------

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

----------------------------------------------------------------------------------------------------------------------------------------------------------