Microsoft Azure Security Essentials

Course Navigation

Microsoft Azure Security Essentials

Course Navigation

Back to Main

Course Introduction

What to Expect

Course Navigation

Welcome to Microsoft Azure Security Essentials

Next

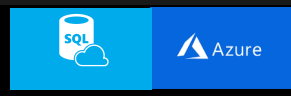
Back to Main

Next Sections

Course Introduction

What to Expect

Course Navigation



Purpose and Scope

This course is designed to bring out some of the core security technologies with an Azure Defense in-depth approach and cater to those individuals that may be new to Azure or may not carry an extensive security background. Security is everyone's job, and this course will help facilitate that mindset, all while maintaining confidentiality, integrity, and availability of customer data.

Prerequisites

- Basic understanding of cloud computing concepts
- Beginner level system and security administration
- General knowledge of Azure platform and infrastructure

Top Security Features in Azure ?

- Secure Networks-build encrypted IPSec tunnel. Segment instances within deployments in one customer subscription.
- Key Logs-Azure keys are 256-bit AES encrypted, access to Microsoft Security Vault.
- Provides Malware Protection-integrate options with the ability to enable anti-malware from the Azure management portal.
- Access Management-Multi-Factor Authentication service that can also be used during on-premise migrations. Microsoft also allows you to conduct your own penetration tests to validate their security

Back

Back to Main

Next Sections

Microsoft Azure Security

One of the biggest reasons to take full advantage of securing applications and services within Azure is its wide array of security tools and capabilities. With these secure platforms come the enhanced ability to customize security based on your organization's deployments.

Azure Security Center — Unify security management and enable advanced threat protection for workloads in the cloud and on-premises.

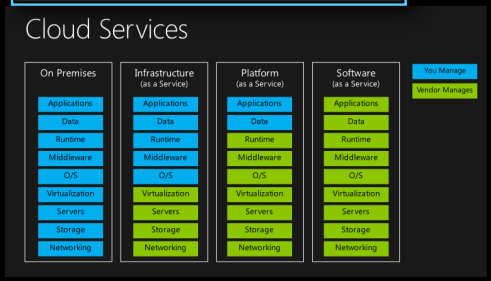
Key Vault — Safeguard encrypted keys and other secrets used by cloud apps and services.

Azure DDoS Protection — Protect your Azure resources from the denial of service threats.

Azure Information Protection — Control and help secure email, documents, and sensitive data that you share outside your company.

Application Gateway — Protect your applications from common web vulnerabilities and exploits with a built-in web application firewall.

Here is an example of the services layout offering for Azure:



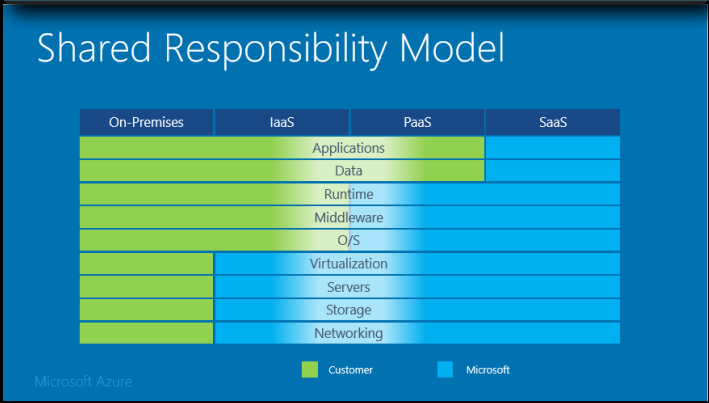
Security in the Cloud

Shared Responsibilities

The **National Institute of Standards (NIST)** recognizes the three main service models for cloud computing as IaaS, PaaS, and Saas.

- **IaaS —** Infrastructure as a service are online services that provide a high-level API used for dereferencing various low-level details of underlying network infrastructure like physical computing resources, location, scaling, and backup.
- **PaaS — C**ategory of cloud computing that provides a platform allowing customers to develop, run, and manage applications without the complexity of building and maintaining the infrastructure.
- **SaaS —** A software licensing and delivery model in which software is licensed on a subscription basis and is centrally located.

Note: *The following illustration is just one of many examples that can be found on the internet but gives a simplistic view of shared responsibilities for these standard cloud service models.*



Back

Next

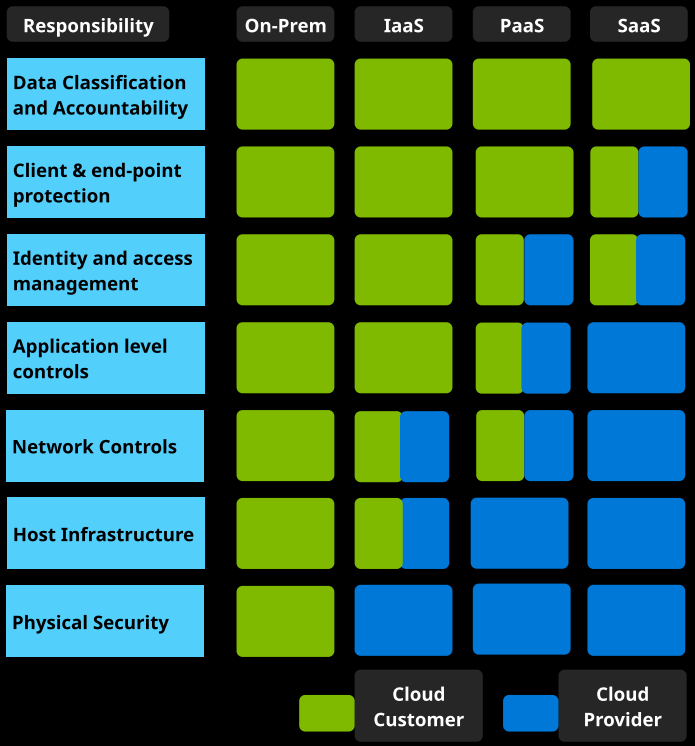
Back to Main

Next Sections

Security in the Cloud

Shared Responsibilities

Microsoft has seven shared responsibilities they feel organizations should consider that will help contribute to being compliant and having a secure computing environment.



Back
Next

Back to Main
Next Sections

Compliance obligation, data classification, and accountability

It is important to understand that on-premises and cloud models share some of the responsibilities between customer and provider. However, it is the customer that is accountable to ensure their solution and its data is securely identified, labeled, and correctly classified to meet any compliance obligation.

- **SaaS** solutions such as Office 365 and Dynamics 365 offer customer data protection using Lockbox and **Data Loss and Prevention**. However, customers must manage, classify, and configure the solutions to address their own unique requirements for security and compliance.

- **PaaS** solutions, a customer's accountability for data classification and management, should be acknowledged as an essential part of the planning process. Customers will need to configure and establish a process that protects the solution's feature set as well as the data. **Azure Rights Management services** is a Paas service that provides data protection and the capability for customers and has been integrated into many of the Microsoft SaaS solutions.

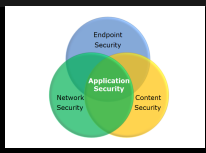
- **IaaS** service model, for capabilities such as virtual machines, storage, and networking, is the customer's responsibility to configure and protect the data that is stored and transmitted. IaaS based solution, data classification, must be considered at all layers of the solution. A misconfigured server can affect how the data that is stored in the service is protected. Compliance also requires that customers audit all deployed virtual machines within their solutions.

Client and End-Point Protection

With there now being a large variety of devices used, it is essential that boundaries are defined and responsibilities identified for these devices that are connecting to a cloud service. CSP's can facilitate capabilities to manage end-point devices. Microsoft Intune provides secure device management, mobile application management, and PC management capabilities. Using a mobile management solution still requires customer accountability for its users.

Identity and Access Management

Users or identity management is one of the core services that organizations work to provide in a seamless fashion, and in many cases, can be simple to use and easy to manage. IAM provides users the ability to access and use resources in their environment and is what distinguishes between identity (who) and access control (what). For PaaS and SaaS solutions, IAM is a shared responsibility that requires an effective implementation plan that includes configuration of an identity provider, the configuration of administrative services, establishing and configuration of user identities, and implementation of service access controls. Additional considerations should be take with two-factor authentication, role-based access control, just-in-time administrative controls, and monitoring and logging of both users and control points. Azure AD provides these controls along with the ability to provision these controls for on-premises. IAM for virtual machines must be configured at the virtual machine level. Compliance needs to be taken into consideration when running these infrastructure layered services.



Application-Level Control

Platform-managed applications and services, such as web services, batch, docDB, IoT, analytics media services, and other related capabilities, reduce the customer's responsibility by providing a more comprehensive secure solution that is managed by the CSP. Managed applications require customers to configure these services correctly, but offer more security capabilities and integration with other solutions such as identity management. Shared responsibility between CSP and the customer can be illustrated in a web service deployment. By default, Azure web service is open for public view, which may not be the desired state and will require customer configuration during the designing phase. A benefit of PaaS solutions is that they do not require the customer to implement the same security configurations as an infrastructure deployment, such as a virtual machine — the CSP already takes care of that. Examples include patch management, antimalware, and baseline configuration. CSP audit reports can be used to supplement customer deployment to meet regulatory obligations. In the IaaS model, customers are responsible for protecting and securing the operating system and application layers of virtual machines to prevent attacks and compromises. If the IaaS deployment goal is to establish a web service offering, the administrator will need to secure both the virtual machine as well as the web service, which also requires expertise in several security domains. The VM stack for Windows and Linux requires skilled administrators to manage and secure the host and its dependencies.

Network Control

Network control includes configuration, management, and securing network elements such as virtual networking, load balancing, DNS, and gateways. In SaaS solutions, network controls are managed by and secured for the customer. The service provider provides PaaS network solutions.

Network Control (Cont)

With Azure, hybrid solutions are the exception because virtual machines are placed on an Azure Virtual Network, which allows customers to configure network-level services. In a SaaS solution, the customer shares responsibility with a service provider to deploy, manage, secure, and configure networking solutions to be implemented.

Host Infrastructure

The host infrastructure responsibility includes the configuration, management, and securing of the compute (virtual hosts, containers, service fabric, auto-scaling), storage (object, CDN, file storage), and platform services. The CSP will operate and secure the host services, such as the operating systems of the service.

IaaS providers share responsibility with customers to ensure the service is optimally configured and secured. This responsibility includes the configuration of the permissions and network access controls required to ensure that networks can communicate correctly and that the devices can attach and mount the correct storage devices.

As with Network control, host controls in an IaaS deployment require customers to be familiar with managing and securing virtual machines. This requirement includes the network management, patching, operating system configuration, application feature deployment, access control, and identity management configuration. IaaS solutions require the most understanding of the host operating system and supporting service stack.

Physical Security

The elements that can be considered part of physical security include buildings or facilities, servers, and networking devices. Customers consider one of the most important values in moving to a cloud service to be the management of the physical environment. CSP's have building security processes and policies that help ensure the infrastructure is protected from unauthorized physical access, that power is maintained in a highly available method, and that if disaster strikes, the service or services should failover to a new physical location providing continued service. Other considerations are capabilities such as cooling, air management (air quality), device management, and power regulation. Microsoft follows these principles in all of its data centers.

Shared Responsibilities Recap

For **on-premises solutions**, the customer is accountable and responsible for all aspects of security and operations.

For **IaaS solutions**, elements such as buildings, servers, networking hardware, and the hypervisor should be managed by the platform vendor. The customer is responsible or has a shared responsibility for securing and managing the operating system, network configuration, applications, identity, clients, and data.

For **SaaS solutions**, a vendor provides the applications and abstracts customers from the underlying components. The customer is also still accountable and must ensure the data is classified correctly, and they share a responsibility to manage their users and end-point devices.

In the **shared responsibility model**, cloud providers offer considerable advantages for security and compliance, but these advantages do not absolve the customer from protecting their users, applications, and service offerings.

Back

Back to Main

Next Sections

Azure Customer Data Protection

Microsoft operations and support personnel are denied access to customer data by default. When granted customer data access, leadership approval is required, and then access is carefully managed and logged. The following Azure Security Policy establishes the access-control requirements:

- No Access to customer data by default.
- No User or administrator accounts on customer virtual machine (VMs).
- Grant the least privilege that's required to complete tasks, audit, and log access requests.

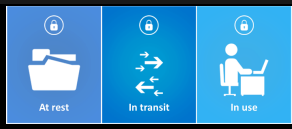
Typically Microsoft support personnel are assigned unique corporate Active Directory accounts. Azure relies on **(MSIT) Microsoft Information Technology** to access corporate Active Directory to control access to key information systems. Multi-factor authentication is required, and access to these systems is only granted from secure consoles. All access attempts are monitored and can be displayed via a basic set of reports.

Data protections Options

- Azure provides strong data protection by default but also with a variety of customer options.

- **Data Segregation:** Azure is a multi-tenant service, which means there are multiple customer deployments and VMs that are stored on the same hardware. Azure uses a logical isolation concept to segregate for each customer's data. This provides both scale and economic benefits to these multi-tenant services while preventing them access to each other's data.

Next



Data Protection Options (Cont)

- **At-Rest Data Protection:** Customers are responsible for ensuring that data stored in Azure is encrypted in accordance with their standards. Azure offers a wide range of encryption capabilities, giving those customers flexibility to choose the solution that best fits their needs. **Azure Key Vault** helps customers maintain control of keys that are used by cloud applications and services to encrypt data. Azure Disk Encryption enables customers to encrypt VMs. Azure Storage Service Encryption makes it possible to encrypt all of the data that is housed in the customer's storage account.

- **In-Transit Data Protection:** Customers can enable encryption for traffic between their own VM's and end users. Azure protects data in transit to or from outside components and data in transit internally, such as between two virtual networks. Azure uses the industry-standard Transport Layer Security (TLS) 1.2 or later protocol with 2,048 -bit RSA/SHA256 encryption keys, to encrypt communication between:

  - The customer in the cloud.
  - Internally between Azure systems and data centers.

- **Encryption:** The encryption of data in storage and in transit can be deployed by customers as a best practice for ensuring confidentiality and integrity of data. Customers are able to configure SSL with ease in their cloud environment to protect communications going out to the internet as well as an internal deployment between VM's.

Data Protection Options (Cont):

Data Redundancy: There are options that Microsoft has put forth when it comes to protecting users from things such as cyberattacks or physical damage to a datacenter. Customers have an option for these services:

- In-country/in-region storage for compliance or latency considerations.
- Out-of-country/out-of-region storage for security or disaster recovery.

Data can be replicated within a selected geographic area for redundancy but cannot be transmitted outside it. Customers have options for replicating data, including the number of copies and the number and location of replication data centers.

When you create your storage account, the following replication options can be selected:

- **Locally redundant storage (LRS)**: Locally maintains three copies of your data. This LRS data is replicated three times within a single facility in a single region. LRS protects your data from normal hardware failures, but not from the failure of a single facility.
- **Zone redundant storage (ZRS)**: Zone-redundant storage maintains three copies of your data. ZRS is replicated three times across two to three facilities to provide higher durability than LRS. Replication occurs within a single region or across two regions. ZRS helps to ensure the stability of your data in a single region.
- **Geo-redundant storage (GRS)**: Geo-redundant storage is enabled for your storage account by default when it is created. GRS maintains six copies and replicates 3 copies to the primary and secondary regions creating failover points between the two.

Customer Data Ownership

Microsoft does not assume responsibility for inspecting, approving, or monitoring applications that customers deploy to Azure. Microsoft is also not part of the decision-making process of what kind of data customers are going to store in Azure. Microsoft does not claim the ownership stake into the customer information that's entered into Azure.

Records Management

Azure has established internal records-retention requirements for back-end data. However, customers are responsible for identifying their own retention requirements. For those records stored in Azure, customers are responsible for extracting their data and retaining their content outside of Azure for a customer-specified period.

Electronic Discovery (e-discovery)

Azure customers are responsible for complying with e-discovery requirements in their Azure services. If Azure customers need to preserve their data, they may export and save the data locally. Customers can also put in for special requests from Azure support to have their data exported. With customers having the ability to export their own data, Azure takes additional steps to conduct extensive logging and monitoring internally.

Where is your customer data?

- Azure has announced there are 55 regions available in 140 countries around the world. Most of the Azure services enable customers to specify the region where their data will be stored. Microsoft may replicate this data to other regions for high availability, but Microsoft will not replicate or move the customer data outside of the Geolocation. Customers and their end-users may move, copy, or access their customer data from any location globally.
- **Data Storage for regional services:** Most Azure services are deployed regionally and enable the customer to specify the region into which the service will be deployed. Examples of such Azure services include virtual machines, storage, and SQL Databases.
- **Data Storage for non-regional services:** Certain Azure services do not enable the customer to specify the region where the service will be deployed. These services may store customer data in Microsoft Data Centers unless specified.

Back

Next

Back to Main

Next Sections

Access to your data at anytime

Microsoft business cloud services takes strong measures to protect customer data from inappropriate access or use by unauthorized persons. This includes restricting access by Microsoft personnel and subcontractors, and carefully defining their requirements when responding to government requests for customer data. Microsoft Azure, Dynamics 365, Intune, and Office 365 subscribers can access it to retrieve their data at any time without notification.

Microsoft Data Classification

Administrator Data: This data contains information about administrators and is supplied during sign up, purchase, or administration of Microsoft services. It also includes aggregated data usage information about your account and the controls that have been selected. This information is used to complete transactions and detect and prevent fraud.

Customer Data: Customer data is all data, including text, sound, video, or image files and software that you provide to Microsoft or that is provided on your behalf through the use of Microsoft enterprise online services, excluding Microsoft Professional Services. An example would be data that you upload for storage or processing as well as applications that upload distribution through a Microsoft enterprise cloud service.

Customer Content: This is considered a subset of customer data, which may include Exchange online email and attachments, Power BI reports, Sharepoint online site content, and Instant Message conversations.

Microsoft Data Classification (Cont)

Object Metadata: Customer provided information used to identify or configure online resources, such as software, systems, or containers, but does not include their content or user identities. Examples include names and technical settings of Azure Storage Accounts, Virtual machines, Azure Databases, and data collections (tables, column headings, labels, and document paths). Customers should not include personal or other sensitive information in the object metadata due to the commonly shared nature across global Microsoft systems to facilitate operations and troubleshooting.

Payment Data: Information you provide as a customer when making online purchases with Microsoft. This may include a credit card number and security code, name and billing address, or other financial data. Payment data is used to complete transactions, as well as to detect and prevent fraud.

Personal Data: Data that is associated with a specific person. Personal data provided by customers through their use of the service, such as names and contact information. However, personal data can also include user ID, or an identification number assigned by a system, but is considered pseudonymous because it alone cannot identify the individual.

Support and Consulting Data: This means all data, including text, sound, image files, or software that are provided to Microsoft to obtain Professional Services or Support. This may include information collected over the phone, chat, e-mail, or web form. It may also include problem descriptions, files transferred to Microsoft to resolve support issues, or by accessing customer systems remotely with customer permission. This doesn't include administrator or payment data.

Managing Compliance in the Cloud

The amount of data being created, shared and stored has increased exponentially which has also added the complexity on how to maintain security and compliance more than ever before.

Microsoft Compliance Score

- This Microsoft feature helps organizations assess data protection with an ongoing basis and gives recommended actions and solutions to help progress towards compliance.
- Compliance Score also supports more than 10 global, regional, and industrial assessments, including GDPR, CCPA, ISO 27701, ISO 27001, HIPAA, FFIEC, and many more.

Six Key Privacy Principles for Governing Data

- **Control**: Customer controlled privacy through easy to use tools.
- **Transparency:** Transparent about data collection in order to make informed decisions.
- **Security:** Protection through strong security and encryption.
- **Strong Legal Protection:** Respecting local privacy laws and legal protection.
- **No Content-Based Targeting:** Emails, chat, files, or any other personal content will not be used to target ads.
- **Benefits to Customer:** Data that is collected is only collected to benefit the customer.

Audit Reports

Microsoft has resources that customers can use through their trust center to verify and assist with compliance and control requirements.

Wrapping Up

3.1.1-Securing Customer Data in Azure Services

By default, operations and support personnel from Microsoft are denied access. Access must be granted by leadership. Certain personnel are assigned Active Directory accounts, and Azure relies on (MSIT) Microsoft Information Technology to control access. Least privilege with no administrator accounts on VM's is still the deployment process, and requests must be logged for access and may be subject to audits for compliance.

Azure data protection options

- Data Segregation
- At-Rest Data Protection
- In-transit data protection
- Encryption
- Data Redundancy

3.1.2-Managing Data Location in Azure Services

- Microsoft has 55 regions in 140 countries
- Data Storage for Regional Services
- Data Storage for Non-Regional Services

3.1.3-Who can access you data and on what terms?

Microsoft Data Classification

- Administrator Data
- Customer Data
- Object Metadata
- Payment Data
- Personal Data
- Support and Consulting Data

Back

Next

Wrapping Up

3.1.4 Review Certification for Azure Services, Transparency Hub

Microsoft has implemented a feature called **Compliance Score** and bases six key privacy principles for governing data:

- Control
- Transparency
- Security
- Strong Legal Protection
- No Content-Based Targeting
- Benefits to Customer

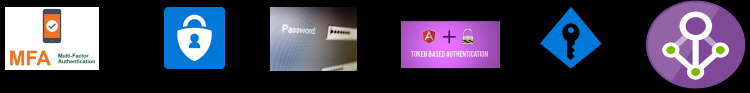
Microsoft has resources that customers can access via the **Trust Center** for Audit Reports to assist with base lining compliance standards.

Back

(IAM) The framework and processes that facilitate the management of electronic digital identities. Microsoft has built-in identity-based controls to help secure systems, applications, and data.

Secure Identity

In order to manage identity and access, Microsoft has multiple security practices and technologies that can be used across many of its products and services.

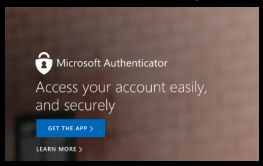


- **Multi-Factor Authentication**
- **Microsoft Authenticator**
- **Password Policy**
- **Token-Based Authentication**
- **Role-Based Access Control (RBAC)**
- **Integrated Identity Management (Hybrid Identity)**

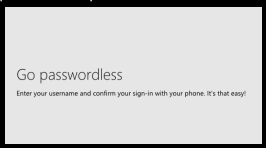
Next

Microsoft Authenticator

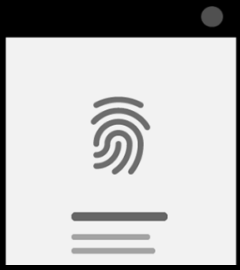
- Many of the wearable devices today can be integrated with **Azure AD** and **Microsoft Accounts** by the simple download of an App.

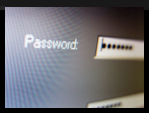


- Options for passwordless.



- Use a mobile device to provide an extra layer of security, add multiple accounts for two-step verification, and secure online accounts with time-based OTP (one-time password) codes.





Azure Active Directory

- Password Policy Enforcement
- Administrator reset policy differences
- UserPrincipalName policies that apply to all user accounts
- Password expiration policies in Azure AD

Token-Based Authentication

- **Authentication**: The process or action of verifying identity.
- **Authorization**: Grants an authenticated user permissions to specific resources or data.

Azure AD is a centralized identity provider in the cloud. Delegating authentication and authorization to it enables scenarios such as Conditional Access Policies. These policies require a user to be in a specific location, the use of multi-factor authentication, as well as enabling a user to sign in once and then automatically sign in to all of the web apps that share the same centralized directory known as Single Sign-On (SSO).

- **OAuth 2.0**
- **OpenID Connect**

Tenants

A cloud identity provider serves many organizations that are partitioned out to separate tenants via Azure AD for a single organization. Tenants keep track of their users and associated apps.

Token-Based Authentication (Cont)

Security tokens

- Security tokens contain information about users and apps. Azure AD uses JSON based tokens (JWTs) that contain claims. A claim provides assertions about one entity to another. Applications can use claims
- A claim consists of key-value pairs
- Tokens are signed by the Security Token Server (STS) with a private key.
- The application verifies the signature by using the STS public key to validate the signature was created using the private key.
- Tokens are only valid for a limited time. However, refresh tokens can be supplied that will refresh the access token when being passed in the authorization header. This is essentially how someone leaving an enterprise is handled. STS receives a refresh token and won't issue another valid token if the user is no longer authorized.

Token-Based Authentication (Cont)

Application Model

- In this description, it is important to understand that applications can sign in users that have access to a particular app. Both the user and the application will need to be registered with the identity provider. Registering with Azure AD, you are providing an identity configuration for an application that allows it to integrate with Azure AD. Registering the app will also allow you to :

- Consent is the process of a resource owner granting authorization for a client application to access protected resources, under specific permissions, and on behalf of the resource owner. This ultimately enables administrators to decide what apps are allowed to users and can also dynamically grant or deny consent for apps on their behalf with the Microsoft identity platform.

Token-Based Authentication (Cont)

Web App sign-in flow with Azure AD

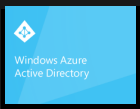
When a user navigates in the web browser, the following happens:

- The web app determines whether the user is authenticated.
- If the user isn't authenticated, the web app delegates to Azure AD to sign in the user.
- The user is asked to consent to the access that the client app needs. Once the user has successfully authenticated, the following happens:
- Azure AD sends a token to the web app.
- A cookie is saved, associated with Azure AD's domain.
- The web app displays the protected page and saves a session cookie in the browser's cookie jar.
- The web app determines when the user is authenticated.
- The web app delegates sign-in to Azure AD and obtains a token

Token-Based Authentication (Cont)

Desktop and Mobile app sign-in flow with Azure AD

- There are slight differences with the sign-in workflow between desktop and mobile applications. Both can use embedded Web control, or a system browser for authentication. Microsoft authentication library (MSAL) is used to acquire access tokens and call web APIs. MSAL uses a browser to get tokens, and as with web apps, delegates authentication to Azure AD.
- Because Azure AD saves the same identity cookie in the browser as it does for web apps, if the native or mobile app uses the system browser it will immediately get SSO with the corresponding web app.
- By default, MSAL, uses the system browser except for .NET framework desktop applications where an embedded control is used to provide an integrated user experience.



Secure Apps and Data

Azure Active Directory is an identity access management cloud solution that can secure access to data in applications both on-site and in the cloud and simplifies the management of users and groups. With a combination of core directory services, advanced identity governance, security, and application access management, the task for developers becomes much easier when building policy-based identity management into their apps.

- **Cloud App Discovery-Features**

  Snapshot Reports
  Continuous Reports

- **Identify Anomalous by connecting**

  Microsoft Defender ATP integration
  Log Collector
  Zscaler integration
  Iboss integration

- **Process for generating information on risk assessments**

  Upload
  Parse
  Analyze
  Generate

Secure Apps and Data (Cont)

Azure Active Directory Identity Protection—A security service that uses Azure Active Directory anomaly detection capabilities to provide a consolidated view into the risk detections and potential vulnerabilities that could affect your organization's identities. There are three key tasks associated with Identity Protection.

- Automate the detection and remediation of identity-based risks
- Investigate risks using data in the portal
- Export risk detection data to third-party utilities for further analysis

Other key factors weigh in with Identity Protection and the interaction that takes place with Azure AD. Some of the consumer space with Microsoft accounts, as well as important information, can be fed into tools such as Conditional Access, or into a Security Information Event Management (SIEM) solution to provide additional investigative capabilities and enforced policies.

Automation is important due to the large number of events. Trending over the last few years for the top attacks are:

- **Breach replay**
- **Password**
- **Spraying**
- **Phishing attempts**

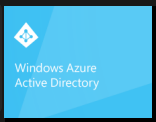
Risk detection and remediation—Identity Protection identifies the mentioned risk classifications.

Secure Apps and Data (Cont)

Azure Active Directory Identity Protection

Risk detection and remediation:

Risk detection type	Description
Atypical travel	Sign in from an atypical location based on the user's recent sign-ins.
Anonymous IP address	Sign in from an anonymous IP address (for example: Tor browser, anonymizer VPNs).
Unfamiliar sign-in properties	Sign in with properties we've not seen recently for the given user.
Malware linked IP address	Sign in from a malware linked IP address
Leaked Credentials	This risk detection indicates that the user's valid credentials have been leaked
Azure AD threat intelligence	Microsoft's internal and external threat intelligence sources have identified a known attack pattern



Secure Apps and Data (Cont)

Azure Active Directory Identity Protection

Risk Investigation

Administrators can review detection's and take manual action on them if needed. There are three key reports:

- Risky Users
- Risky sign-ins
- Risk detections

Exporting Risk Data

Data from identity protection can be exported to other tools for archive and further investigation and correlation. The Microsoft Graph based APIs allow organizations to collect data for further processing in a tool such as their SIEM. You can also connect data from the Azure AD Identity Protection service into **Azure Sentinel** and stream alerts and create and view custom dashboards in order to improve investigation.

Additional information about how to access the Identity Protection API can be found by clicking on the following link to Microsoft:

Identity Protection and Microsoft Graph

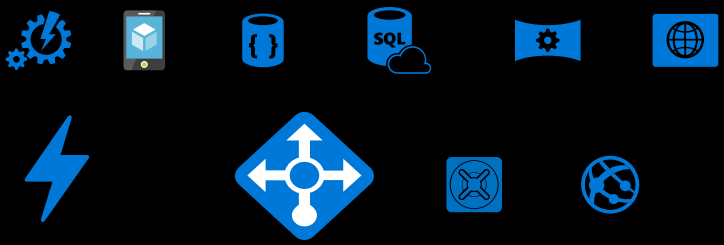
Information about integrating Identity Protection using Azure Sentinel can be found at this location:

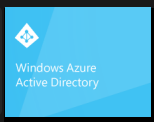
Connect Data from Azure AD Identity Protection

Secure Apps and Data (Cont)

Azure Active Directory Domain Services—Enables you to join Azure VMs to a domain without the need to deploy domain controllers, Users sign in to these VMs by using their corporate Active Directory credentials, and can access resources. Azure AD carries many of the same traditional domain services such as:

- Join VM's to the domain as mentioned without domain controllers as stated, and use Group Policy to administer these VM's that have been joined for baseline security.
- Migrate to the on-premises apps without identity worries using features like **domain join**, **LDAP**, **NT LAN Manager (NTLM)**, and **Kerberos** authentication. Migrate legacy AD aware applications on-premise to Azure.
- Speedy deployments in minutes so that you can pay as you go based on the size of your organization's directory services.



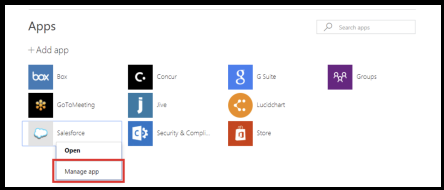


Secure Apps and Data (Cont)

Azure Active Directory B2C—A highly available global identity management service for consumer-facing apps that can scale to hundreds of millions of identities and integrate across mobile and web platforms. Your customers can sign in to all your apps through customizable experiences that use existing social media accounts, or you can create new standalone credentials.

Azure Active Directory B2B Collaboration—A highly available global identity management service for consumer-facing apps that can scale to hundreds of millions of identities and integrate across mobile and web platforms. Your customers can sign in to all your apps through customizable experiences that use existing social media accounts, or you can create new standalone credentials. Some of the advantages include:

- The partner uses their own identities and credentials; Azure AD is not required.
- You don't need to manage external accounts or passwords.
- You don't need to sync accounts or manage account lifecycles.
- Invite guest users with the invitation and redemption process.
- You can also control conditional access at the tenant level, application level, and assign specific guest permissions in order to secure corporate applications and data. This can all be done from the Azure portal. Application and Group owners can manage all of this in a self-service fashion.



Secure Apps and Data (Cont)

Azure Active Directory Join—Enables you to extend cloud capabilities to Windows 10 devices for centralized management. It makes it possible for users to connect to the corporate or organizational cloud through Azure Active Directory and simplifies across apps and resources.

BYOD (Bring Your Own Device) has created some challenges of protecting organizational assets but also allowing those end users to be as productive as possible with access.

In order to protect your device, it is important to manage device identities with tools such as Microsoft Intune to ensure security standards and compliance are met. Azure Active Directory AD enables Single Sign-On to devices, apps, and services from anywhere through these devices. Device identity management is the foundation for **device-based Conditional Access**. This ensures that only devices that are being managed have access to resources in the environment. The following link goes into more detail around Conditional Based Access.

Device-based Conditional Access

There are multiple options when it comes to adding devices into Azure AD.

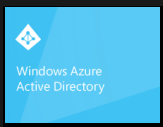
Secure Apps and Data (Cont)

Azure Active Directory Join

- **Azure AD Registered**
  - Devices that are Azure AD registered are typically personally owned or mobile devices, and are signed into with a personal Microsoft account or another local account:
    - Windows 10
    - IOS
    - Android
    - MacOS
- **Azure AD joined**
  - Devices that are Azure AD joined and owned by an organization, and are signed in to with an Azure AD account belonging to that organization. They exist only in the cloud:
    - Windows 10
- **Hybrid Azure joined**
  - Devices that are hybrid Azure AD joined are owned by an organization. They exist in the cloud and on-premises:
    - Windows 7,8.1, or 10
    - Windows Server 2008 or newer

Devices that are Azure AD joined or hybrid Azure AD joined both benefit from SSO to an organization's on-premises resources as well as cloud resources. The following link provides more information to how SSO to on-premise resources works on Azure AD joined devices.

SSO to on-premise working with Azure AD joined devices



Secure Apps and Data (Cont)

Azure Active Directory Join

Device Management
Devices in Azure AD can be managed using Mobile Device Management (MDM) tools. I

Resource Access
Registering and joining devices to Azure AD

Device Security

- **Azure AD registered devices** utilize an account managed by the end user, this account is either a Microsoft account or another locally managed
- **Azure AD joined or hybrid Azure AD joined devices** utilize an organizational account in Azure AD
- **Provisioning:**
  - Getting devices in to Azure AD can be done in a self-service manner

Secure Apps and Data (Cont)

Azure Active Directory Application Proxy provides SSO and secures remote access for web applications hosted on-premises.

Azure AD Application Proxy provides:

- **Ease of use**
- **Secure**
- **Cost-Effective**

- Application Proxy primarily serves as a feature of Azure AD that enables users to access on-premise web applications from a remote client. Application proxy has a service that runs in the cloud, and a connector that runs on an on-premise server. The two work together to pass a user sign-on token from Azure AD to the web application.

Application Proxy works with:

- Web applications that use **Integrated Windows Authentication**
- Web applications that use form-based or header-based access
- Web APIs that you want to expose to rich applications on different devices
- Applications hosted behind a **Remote Desktop Gateway**
- Rich client apps that are integrated with **Active Directory Authentication Library (ADAL)**

RBAC

RBAC is an authorization system built on **Azure Resource Manager**. I
What can you do with RBAC?

- Allow one user to manage virtual machines in a subscription and another to manage virtual networks.
- Allow a DBA group to manage the SQL database in a subscription.
- Allow a user to manage all resources in a resource group, such as virtual machines, websites, and subnets.
- Allow an application to access all resources in a resource group.

Best practice for using RBAC

Using RBAC, you can split out duties within your team and grant only the amount of access to users that they need to perform their jobs.

How RBAC works

The way you control access to resources using RBAC is to create role assignments. This is a key concept to understand, as it is how permissions are enforced. Role assignments consist of three elements: **Security Principal**, **Role Definition**, and **Scope.**

RBAC (cont)

Security Principal

A **Security Principal** is an object that represents a user, group, service principal, or managed identity that is requesting access to Azure resources.

- **User:** An individual who has a profile in Azure Active Directory.
- **Group:** A set of users created in Azure Active Directory.
- **Service Principal:** A security identity used by applications or services to access specific Azure resources.
- **Managed identity:** An identity in Azure AD is automatically managed by Azure.

Role definition

A **role definition** is a collection of permissions. Typically referred to as a **role**, it lists out the operations that can be performed, such as read, write, and delete. Roles can be high level, like owner or specific, like virtual machine reader.

RBAC (cont)

Role definition
Azure includes several **built-in roles** that you can use. The following lists four fundamental built-in roles. The first three listed apply to all resource types.

- **Owner** - Has full access to all resources, including the right to delegate access to others.
- **Contributor** - Can create and manage all types of Azure resources but can't grant access to others.
- **Reader** - Can view existing Azure resources.
- **User Access Administrator** - Lets you manage user access to Azure resources.

The rest of the built-in roles allow the management of specific Azure resources. For example, the **Virtual Machine Contributor** role

Scope

- **Scope** - is the set of resources that access applies to.

In Azure, scopes can be defined at multiple levels: subscription, resource group, resource, or management group. For more information on management groups, click on the following link.

Management Group

RBAC (cont)

Scope
Scopes are structured in a parent-child relationship .

When you grant access at a parent scope, those permissions are inherited to the child scopes.

Examples:

- If you assign the **Owner** role to a user at the management group scope, that user can manage everything in all subscriptions in the management group.
- If you assign the **Reader** role to a group at the subscription scope, the members of that group can view every resource group and resource in the subscription.
- If you assign the **Contributor** role to an application at the resource group scope, it can manage resources of all types in that resource group, but not other resource groups in the subscription.

RBAC (Cont)

Role Assignments

A **role assignment** is the process of attaching a role definition to a user, group, service principal.

For example, a role assignment in which the **Marketing** department has been assigned the **Contributor** role for the **Sales** resource group.

- This means that users in the Marketing group can create or manage any Azure resource in the **Sales** resource group.
- Marketing users do not have access to resources outside the **Sales** group unless they are part of another role assignment.

RBAC (Cont)

Multiple Role Assignments

RBAC is an additive model so that you can have overlapping role assignments to your effective permissions. Here is an example where a user is granted the **Contributor** role at the subscription scope and the **Reader** role on a resource group. The addition of the Contributor permissions and the Reader permissions is effectively the Contributor role for the resource group. Therefore, in this case, the Reader role assignment has no impact.

Deny assignments

Previously, RBAC was an allow-only model with no deny, but now RBAC supports **deny** assignments in a limited way. A deny assignment attaches a set of deny actions to a user, group, service principal, or managed identity at a particular scope for the purpose of denying access. Deny assignments take precedence over role assignments. You can learn more about deny assignments from the following Microsoft web page.

Deny Assignments for Azure Resources

RBAC (Cont)

How RBAC Determines if a User has Access to a Resource

The following high-level steps explain how RBAC determines if a user has access to a resource on the management plane. This can be beneficial if you are trying to troubleshoot an access issue.

- Acquires a token for Azure Resource Manager
- Then makes a REST API call to Azure Resource Manager with the token attached.
- Azure Resource Manager retrieves all the role assignments and deny assignments that apply to the resource upon which the action is being taken.
- Azure Resource Manager narrows the role assignments
- Azure Resource Manager determines if the action in the API call is included in the roles the user has for this resource.
- If the user doesn't have a role with the action at the requested scope, access is not granted.
- If a deny assignment applies, access is blocked. Otherwise, access is granted.

Note: Using this feature is free and included in your Azure subscription.

Wrapping Up

Secure Identity
(Click Here)

Secure Apps and Data
(Click Here)

Role-Based Access Control
(Click Here)

Secure Identity

In the review, we talk about how Microsoft uses multiple security practices and technologies across its products and services to manage their identity and access:

- **Multi-factor authentication** requires users to use multiple methods for access, on-premises, and in the cloud. It provides strong authentication with a range of easy verification options while accommodating users with a simple sign-in process.
- **Microsoft Authenticator** provides a user-friendly multi-factor authentication experience that works with both Microsoft Azure Active Directory and Microsoft accounts and includes support for wearables and fingerprint-based approvals.
- **Password policy enforcement** increases the security of traditional passwords by imposing length and complexity requirements, forced periodic rotation, and account lockout after failed authentication attempts.
- **Token-based authentication** enables authentication via Azure Active Directory.
- **Role-based access control (RBAC)** enables you to grant access based on the user's assigned role, making it easy to give users only the amount of access they need to perform their job duties. You can customize RBAC per your organization's business model and risk tolerance.
- **Integrated identity management (hybrid identity)** enables you to maintain control of users' access across internal data centers and cloud platforms, creating a single user identity for authentication and authorization to all resources.

Secure Apps and Data

In the next section, we take a more comprehensive look into Azure Active Directory and some of its key functionalities:

- **Cloud App Discovery** is a premium feature of Azure Active Directory that enables you to identify cloud applications that are used by the employees in your organization.
- **Azure Active Directory Identity Protection** is a security service that uses Azure Active Directory anomaly detection capabilities to provide a consolidated view into risk detection and potential vulnerabilities that could affect your organization's identities.
- **Azure Active Directory Domain Services** enables you to join Azure VMs to a domain without the need to deploy domain controllers. Users sign in to these VMs by using their corporate Active Directory credentials and can seamlessly access resources.
- **Azure Active Directory B2C** is a highly available, global identity management service for consumer-facing apps that can scale to hundreds of millions of identities and integrate across mobile and web platforms. Your customers can sign in to all your apps through customizable experiences that use existing social media accounts, or you can create new standalone credentials.
- **Azure Active Directory B2B Collaboration** is a secure partner integration solution that supports your cross-company relationships by enabling partners to access your corporate applications and data selectively by using their self-managed identities.
- **Azure Active Directory Join** enables you to extend cloud capabilities to Windows 10 devices for centralized management. It makes it possible for users to connect to the corporate or organizational cloud through Azure Active Directory and simplifies access to apps and resources.
- **Azure Active Directory Application Proxy** provides SSO and secures remote access for web applications hosted on-premises.

Role-Based Access Control

Finally, we discuss the significance of **RBAC.** We learn that RBAC's primary function is to provide access management control and is built on the Azure Resource Manager.

We highlighted what we can do with RBAC:

- Allow one user to manage virtual machines in a subscription and another to manage virtual networks.
- Allow a DBA group to manage the SQL database in a subscription.
- Allow a user to manage all resources in a resource group, such as virtual machines, websites, and subnets.
- Allow an application to access all resources in a resource group.

Some of the Best Practices for RBAC

Using RBAC, you can split out duties within your team and grant only the amount of access to users that need to perform their jobs. Instead of giving everybody unrestricted permissions in your Azure subscription or resources, you can allow only certain actions for a particular scope. W planning the access control strategy, we should practice granting users the least privilege to get their work done.

How RBAC Works

The way you control access to resources using RBAC is to create role assignments. This is a key concept to understand and is how permissions are enforced. Role assignments consist of three elements: **Security Principal**, **Role Definition**, and **Scope**. Then, finally, they are followed by deny assignments.

Back

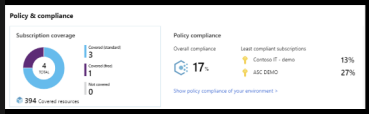
Security and the Audit Dashboard

Azure Security Center has key functionality around viewing organizational security posture. This section provides an overview of some of these key elements.

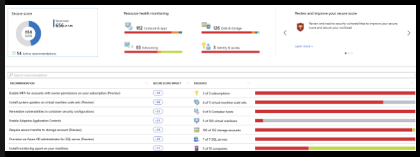
Security and Audit Solution: Security Center is a native PaaS solution built into Azure that monitors and protects without necessitating any deployment. This can integrate with on-premise and non-Azure environments. Here are some examples of key features for security and auditing controls.

Policy Management: You can set policies to run on management groups, across subscriptions, and for a whole Tenant.

Policy and Compliance: Identify Shadow IT subscriptions labeled with **not covered** in the dashboard. This helps to regulate policy coverage across the environment.



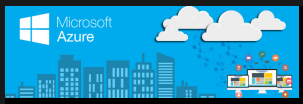
Networking: Shows your topology as well as a Secure Score. The secure scores assist with recommendations based on priority.



Next

Back to Main

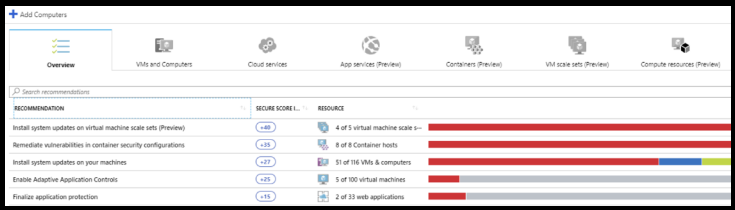
Next Sections



Security and the Audit Dashboard (cont)

Protecting against threats: Security Center threat protection enables you to detect and prevent threats at the IaaS layer and for non-Azure servers at the PaaS in Azure.

- **Kill-chain Analysis:** Correlates alerts in your environment to help you understand the full story of an attack campaign, where it started, and the impact on your resources.



Advanced Threat Protection: This has adaptive controls for application policies, and can also help protect the PaaS environment with behavioral Analytics for anomaly detection.

Block Brute Force attacks: Harden the Network with unnecessary access and build alerting.

Course Navigation

Security in the Cloud
Section 2

Transparency
Section 3

Identity and Access Management
Section 4

Operations
Section 5

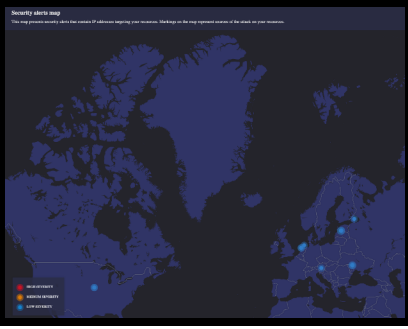
Security and the Audit Dashboard
Application Insights
Azure Monitor
Azure Monitor Logs
Azure Advisor
Azure Security Center
Conclusion

Storage
Section 6

SECURITY ALERT

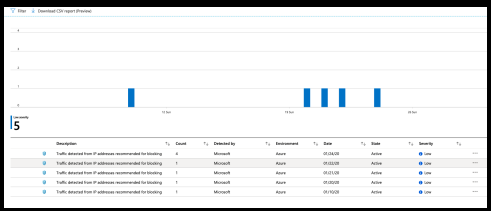
Security alerts map view

- This interactive map can help identify source IP attempts on inbound traffic with a description of what actions should be taken.



Security alerts graph view

- This graph view contains the same information with an option to export to CSV.



Back
Next

Back to Main
Next Sections

Course Navigation

Security in the Cloud
Section 2

Transparency
Section 3

Identity and Access Management
Section 4

Operations
Section 5

Security and the Audit Dashboard
Application Insights
Azure Monitor
Azure Monitor Logs
Azure Advisor
Azure Security Center
Conclusion

Storage
Section 6

Application Insights

- Application Insights is an extensible Application Performance Management (APM) service for web developers. You can monitor live web applications and automatically detect performance anomalies. It also includes analytics tools to diagnose issues and to understand what users are doing when interacting with web applications. There is a full time monitoring pre- and post-deployment phase.
- It also creates charts and tables that show trends like high peak usage times, how responsive the app is during these times, and how well it is served by external services and dependencies.
- Crashes, failures, and performance data are searchable, which can help diagnose issues. This also serves as a great security tool because it helps with the availability, confidentiality, and integrity of the application that could be deemed critical to business operations.

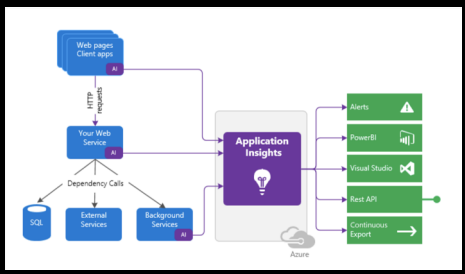


Diagram by Microsoft
https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview

Back
Next

Back to Main
Next Sections

What Does Application Insights Monitor?

Application Insights are aimed at the development team to help you understand how your app is performing and how it's being used. From a high level, it monitors:

- **Request rates, response times, and failure rates**
- **Dependency rates, response times, and failure rates**
- **Exceptions**
- **Page views and load performance**
- **AJAX calls from web pages** - rates, response times, and failure rates
- **User and session counts**
- **Performance counters**
- **Host diagnostics**
- **Diagnostic trace logs**
- **Custom events and metrics**

There is also multiple types of alerts:

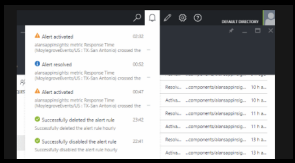
- **Metric Alerts** tell you when response times, exception counts, page views, and CPU usage crosses a certain threshold.
- **Log Alerts** describe alerts where the alert signal is based on a custom Kusto query.
- **Web tests** tell you when your site is unavailable on the internet or is responding slowly.
- **Proactive diagnostics** are configured automatically to notify you about unusual performance patterns.

Set a Metric Alert

- Opening alert, you can specify specific conditions and have it viewable in **Alert Monitor**.

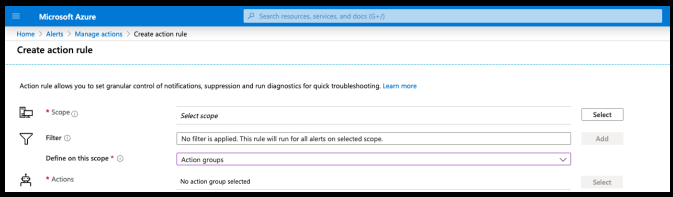
See your Alerts

- You get an email when an alert changes state between inactive and active.
- The current state of each alert is shown in the *Alert* rules tab.
- There's a summary of recent activity in the *Alerts* drop-down:



Manage Actions

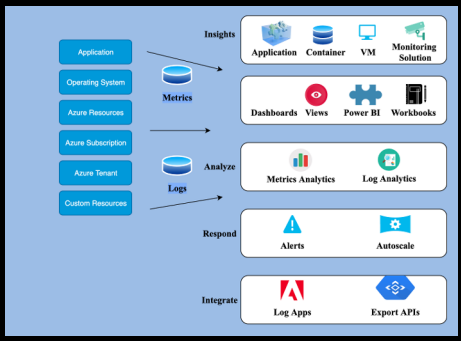
You can create action rules for the alerts you create, including features like **Action Group** creation that can send notifications out to bulk emails and various mobile devices when alerts are triggered.



Azure Monitor

- Azure Monitor delivers a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments. It helps you understand how your applications are performing and proactively identifies issues affecting them and the resources they depend on.

- The following diagram gives a high-level view of Azure Monitor. This also shows the data stores where the metrics and logs are stored. On the left are the monitoring data sources that populate these stores, then on the right are the different functions that **Azure Monitor** performs with this collected data for analysis, alerting, and potentially sending to external systems.



What Azure Monitor collects

- Application monitoring data
- Guest OS monitoring data
- Azure resource monitoring data
- Azure subscription monitoring data
- Azure tenant monitoring data

Azure Monitor (cont)

- **Azure Monitor for VM's**-This is a feature that you can turn on in Azure Monitor that will allow you to see scale sets and analyze things such as performance and health on Windows and Linux VM's.
- **Access Mode**-This is the log analytics workspace and defines the scope of data that can be accessed. Users have two options to access the data:

  Workspace-context: You can view all logs in a workspace that you have permission to. Queries are scoped to all data and tables. This mode is typically used when selecting the workspace and using Azure monitor.

  Resource-Context: This is used when selecting logs from a particular resource or resource group. The data is only scoped for that particular resource group or subscription, and subsequently allows granular data pertaining to RBAC

- **View Designer**-allows you to create custom views for Azure Monitor via a dedicated log analytics workspace. The following tiles are available when creating these custom views.

  Number: The count of records from a query
  Two Numbers: The counts of records from two different queries
  Donut: A chart that's based on a query, with a summary value un the center.
  Line chart and callout: A line chart that's based on a query, and a callout summary value.
  Line Chart: A line chart that's based on a query.
  Two Timelines: A column chart with two series, each based on a separate query,

Azure Monitor Logs

Log Analytics service is what manages your cloud-based data securely with the following methods:

- **Data segregation**
- **Data retention**
- **Physical security**
- **Incident Management**
- **Compliance**
- **Security standards certification**

Certifications and Attestation
Azure Log Analytics meets the following requirements:

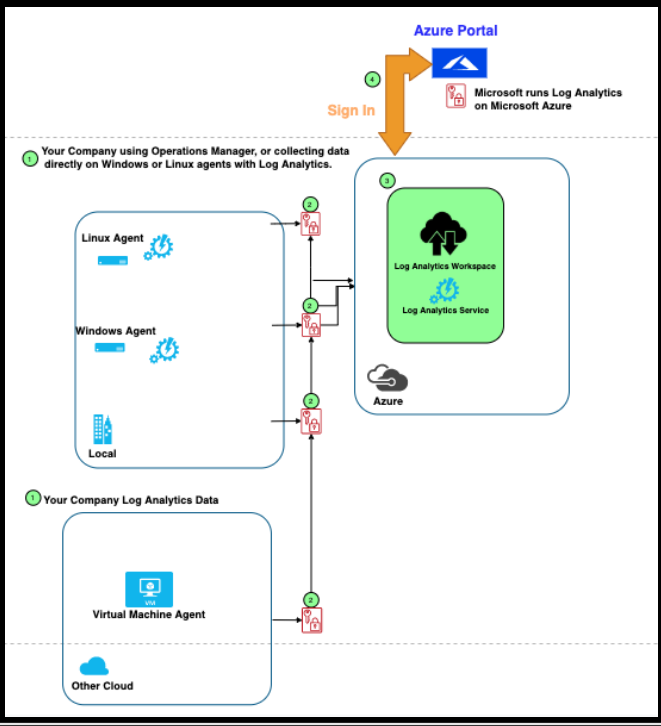
- ISO/IEC 27001
- ISO.IEC 27018:2014
- ISO 22391
- PCI Compliant, Data Security Standard PCI DSS, PCI Security Standards Council
- Service Organization Controls (SOC) 1 Type 1 n SOC 2 Type 1 compliant
- HIPAA and HITECH for companies that have HIPAA Business Associate Agreement
- Windows Common Engineering Criteria
- Microsoft Trustworthy Computing
- Log Analytics Components adhere to Azure compliance

Data security using TLS 1.2: While data is being ingested into Log Analytics, the recommendation is to implement at least Transport Layer Security (TLS) 1.2. Older versions of TLS/Secure Sockets Layer (SSL) have been found to have vulnerabilities. It is recommended not to use these. The PCI Security Standards Council set a deadline in June of 2018 to disable the older versions of TLS/SSL. If you are not on the required TLS version, there will be problems sending your data to Log Analytics.

Azure Monitor Logs (Cont)

Cloud Computing Security Data Flow

The following diagram shows a cloud security architecture as a flow of information from a company and how it is secured as it moves to the Log Analytics service.



Back

Next

Back to Main

Next Sections

Azure Monitor Logs (Cont)

Log Analytics and Collection of Data

For an organization to send data to log analytics, you will need to configure a Windows or Linux agent to run on the Azure virtual machine as well as on-premises or physical computers in your environment. There is an option to use Operations Manager, from the management group that has been configured to run the Operations Manager agent. Typically for a given environment, there are multiple workspaces created that can accept logs from Log Analytics using an Organizational ID or a Microsoft Account into Azure with this functionality. Solutions do not necessarily go through the Operations Manager. You can also hook a resource or solution directly to the Log Analytics service. These communications are all encrypted through TLS (HTTPS). Microsoft SDL uses a process to ensure all of the encryption methods are kept up to date. Detailed information on the type of data can be found at the following link:

https://docs.microsoft.com/en-us/azure/azure-monitor/insights/solutions

Send data from agents

Enrollment keys are used to establish a secure connection from the agent and the log analytics solution using certificate-based authentication and SSL port 443. Log Analytics uses a secret store to maintain keys, and these keys are rotated every 90 days. This is all within the regulatory and compliance scope in Azure. The agents use a read-only storage key to read the diagnostic events in the Azure tables. One of the benefits to an Operations Manager integration if this resource or agent goes down, there is historical data that the Operations Manager cache preserves with these events still available. As events are triggered, and the agents continue to queue data to the Operations Manager, you can also change an agent queue limit through a registry key modification on the agent if a host resource becomes unavailable. This allows the data to be compressed and sent directly to the agent service bypassing Operations Manager so that it doesn't impact its load and services it is providing to the rest of the environment. ExpressRoute is another way to add security to the data being transmitted. ExpressRoute is a way to directly connect Azure from your existing WAN network using multi-protocol label switching (MPLS) VPN.

Course Navigation

Security in the Cloud
Section 2

Transparency
Section 3

Identity and Access Management
Section 4

Operations
Section 5

Security and the Audit Dashboard
Application Insights
Azure Monitor
Azure Monitor Logs
Azure Advisor
Azure Security Center
Conclusion

Storage
Section 6

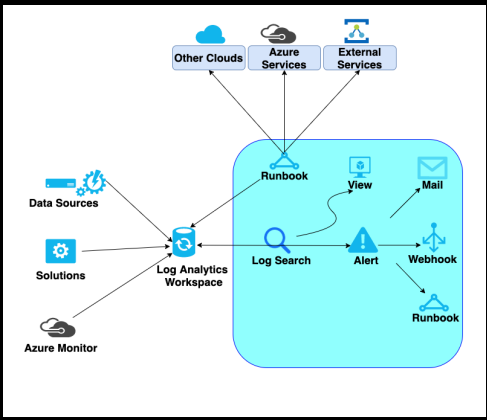
Azure Monitor Logs (Cont)

Using Log Analytics to access the data

To access the Log Analytics workspace, you will sign in to the Azure portal with your organizational or Microsoft account. Secure HTTPS is used to communicate between the Azure portal and Log Analytics service, a session ID in this process is also created when it is generated over a user client (Web Browser) and data stored in the local cache until the session is terminated. Once terminated, the cache is deleted. Client-side cookies, which do not contain personally identifiable information, are not automatically removed. Those applicable session cookies get labeled as HTTPOnly and are secured. After a pre-determined idle period, the Azure portal is then terminated.

Management Solution

Management solutions contain Azure resources that work together to achieve a particular management scenario. This can be a customized design, and the following diagram shows a common pattern for a management solution.



Back
Next

Back to Main
Next Sections

Azure Advisor

- Advisor is a personalized cloud consultant that can assist with following best practices to optimize deployments. It Analyzes resource configuration and usage telemetry and is then able to pass along recommendations to improve cost, performance, high availability and security of Azure resources. Advisor can be accessed via the Azure portal . The Dashboard will display recommendations for all of your subscriptions and resource types. These recommendations are divided into the followiing categories:

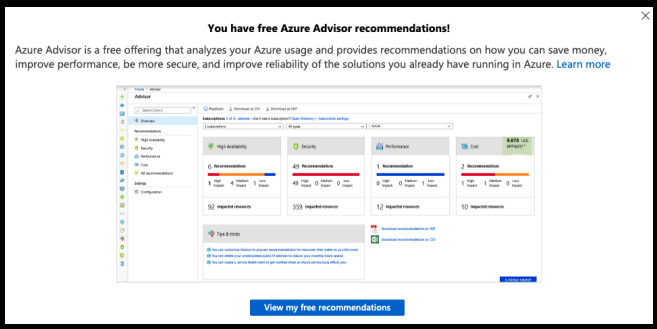
High Availability-To ensure and improve the continuity of your business-critical applications.

Security-To detect threats and vulnerabilities that might lead to security breaches

Performance-To improve the speed of your applications

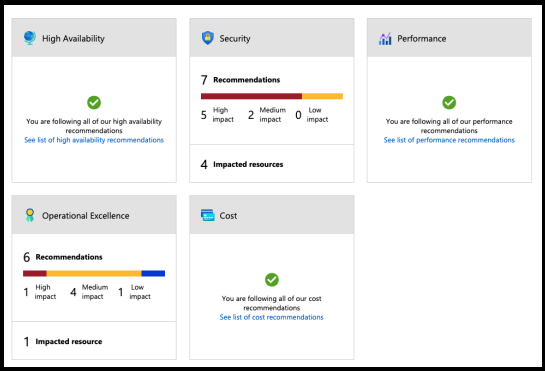
Cost-To optimize and reduce your overall spending

- Here is an example of Azure Advisor's automated message some may receive while logged into a portal instance.



Azure Advisor (cont)

- Here are the results returned upon selecting **View my free advisor recommendations**:



- This is a personalized cloud consultant that will help you follow best practices. It also integrates with SQL Database and Security Center to a centralized dashboard. This can help simplify an IT professional's job and maximize productivity, as well as help improve cost management by detecting underutilized resources.

Azure Security Center

Security Center helps to prevent, detect, and respond to threats by creating better visibility into and control of the Azure resources in your environment. It provides integrated monitoring and policy management across subscriptions and helps detect threats that might normally go unnoticed. It creates an operational opportunity by collaborating into a centralized dashboard, providing various alerting and recommendation capabilities.

Architecture

Security Center is a native part of Azure PaaS that monitors service fabric, SQL databases, and storage accounts without necessitating any additional deployments. For non-Azure servers and virtual machines, an agent can be installed in order to bring these into a Security Center environment. Any virtual machines created in Azure will be auto-provisioned into Security Center. Agents collect information brought in from the security analytics engine to provide recommendations or hardening tasks to secure workloads, as well as give visibility to threat detection alerts that should be investigated in a timely manner to ensure there aren't malicious attacks taking place on these workloads.

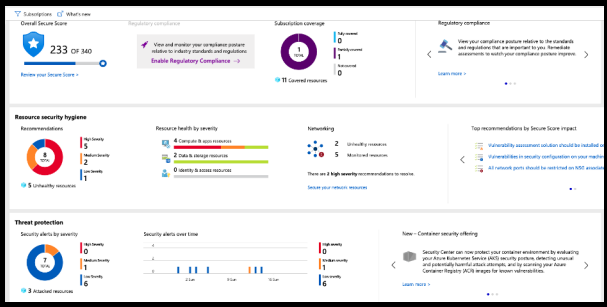
Security Policies

Once Security Center has been enabled, a default policy is applied for free and standard tiers in subscriptions that only contain audit policies.

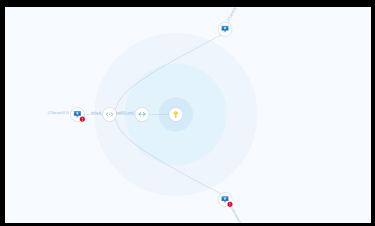
Azure Policy can be used to manage security policies in Security Center with an ability to edit the **built-in default policy** (called ASC) under free and standard tiers as well as **add your own custom policy** with recommendations if the resources don't follow these policies you create. You can also add **regulatory and compliance policies** and bring this into a Security Center Dashboard to facilitate and maintain better control of meeting compliance for your resources.

Azure Security Center (cont)

- **Organizational Security Policy and Compliance:** Security Center policies are built on top of Azure policy controls, which means you can set your policies to run on management groups across various subscriptions or an entire tenant.



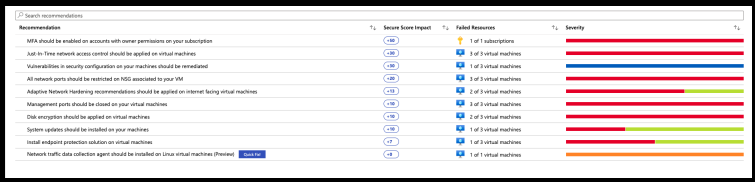
- **Continuous Assessments:** Security Center discovers new resources that are being deployed across workloads. In order to see some of these workloads there is a **Network Map** feature in Security Center to display if nodes are properly configured and how they are connected, which can assist in blocking unwanted connections or attackers. Here is an example of a network topology map that was pulled up in Security Center/Networking menu:



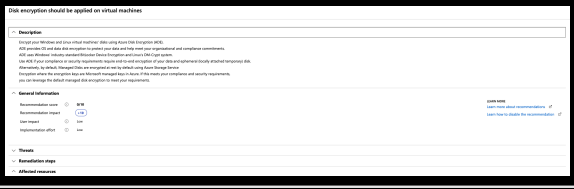
Azure Security Center (cont)

- **Secure Score:** Security Center provides an overall score that will get associated to all the recommendations you receive and is based on priority with the intent to improve overall security posture.

- **Recommendations:** These recommendations bring out some of the security concerns found on workloads, essentially conducting some of the administrative tasks for you by finding vulnerabilities and leaving specific instructions on how to remediate them.



This is an example of remediation steps for enabling disk encryption for specific virtual machines in an environment:

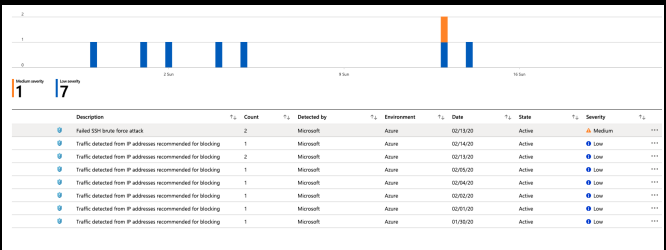


Azure Security Center (cont)

- **Advanced Threat Protection:** Security Center provides native integration with Microsoft Defender Advanced Threat Protection without having to do any configuration on Windows virtual machines and servers. This is also offered out of the box for Linux virtual machines and servers. You can automate application control policies on server environments as well as have adaptive application controls enabled, allowing app whitelisting across Windows servers.

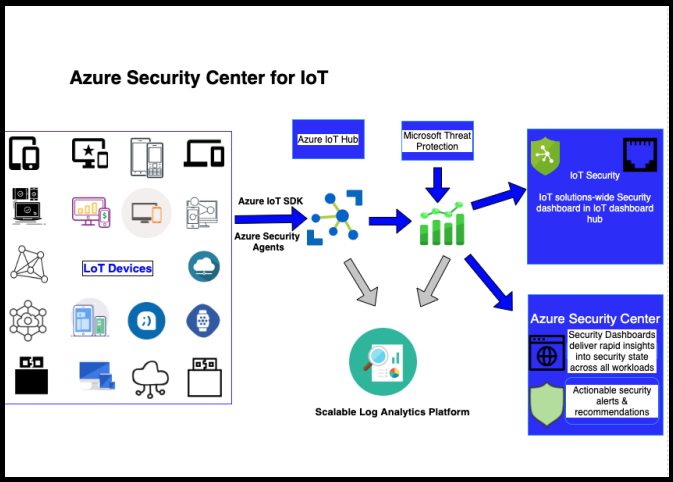
- **PaaS Protection:** Security Center has the ability to help detect threats across PaaS services running in Azure, which includes Azure App Service, Azure SQL, and Azure Storage Accounts, as well as more data services. Microsoft Cloud App Security's user entity behavioral analytics (UEBA) can perform anomaly detection in activity logs and is a native PaaS-integrated solution.

- **Brute Force Attacks:** Security Center can help limit exposure to these types of attacks by limiting access to virtual machine ports and using just-in-time VM access. This is a form of hardening the network by preventing unnecessary access, and you can set security policies on specific ports for authorized users, specific allowed IP ranges or addresses, and even set it up to only be allowed or opened for a limited amount of time. The picture below shows a few examples, such as a failed SSH brute force attack.



Azure Security Center (cont)

- **Security Center for IoT:** This can simplify hybrid workloads by implementing protection and delivering unified visibility control, adaptive threat prevention, and intelligent threat detection and response across various workloads running on edge, on-premises, and in Azure, as well as other cloud solutions.



- **Adaptive threat prevention:** Azure Security Center and the use of a centralized IoT dashboard can help reduce the attack surface and remediate issues before they become exploited.
- **Intelligent threat detection and response:** There is advanced analytics data that can be consumed — anywhere from behavioral machine learning to monitoring controls — to identify incoming attacks and post-breach activity.

■ Wrapping up

5.1.1 Security and the Audit Dashboard

Security Center is a native PaaS solution built into Azure that monitors and protects without necessitating any deployment. This can integrate with on-premises and non-Azure environments. Some of the key features we discussed included some of the audit controls, such as policy and compliance, with many features having the ability to be fully integrated into Security Center as a centralized dashboard. This was discussed in more detail within the Security Center section 5.1.6.

5.1.2 Application Insights

In this section, we discussed some of the key features of Application Insights. This is an extensible Application Performance Management (APM) service for web developers. This helps to see qualifying trends and application performance anomalies, as well as rules that can be built and customized with actions.

5.1.3 Azure Monitor

Azure Monitor delivers a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments. Here are some examples we discussed on the data Azure Monitor is collecting:

- Application monitoring data
- Guest OS monitoring data
- Azure resource monitoring data
- Azure subscription monitoring data
- Azure tenant monitoring data

Wrapping Up

5.1.4 Azure Monitor Logs

Log Analytics service is what manages your cloud-based data securely. We also discussed how log analytics meets some of the most common certification and attestation requirements, such as ISO/IEC 27001,

Data that is being ingested into log analytics is using TLS 1.2 encryption or higher. For an organization to send data to log analytics, you will need to configure a Windows or Linux agent to run on the Azure virtual machine as well as on-premises or physical computers in your environment.

5.1.5 Azure Advisor

Advisor is a personalized cloud consultant that can assist with following best practices to optimize deployments. It analyzes resource configuration and usage telemetry and is then able to pass along recommendations to improve cost, performance, high availability, and security of Azure resources. Advisor can be accessed via the Azure portal. The dashboard will display recommendations for all of your subscriptions and resource types. These recommendations are divided into the following categories:

- High Availability
- Security
- Performance
- Cost

Course Navigation

Security in the Cloud
Section 2

Transparency
Section 3

Identity and Access Management
Section 4

Operations
Section 5

- Security and the Audit Dashboard
- Application Insights
- Azure Monitor
- Azure Monitor Logs
- Azure Advisor
- Azure Security Center
- Conclusion

Storage
Section 6

Wrapping Up

5.1.6 Azure Security Center

Security Center helps prevent, detect, and respond to threats by creating a better visibility and control to the Azure resources in your environment. It provides integrated monitoring and policy management across subscriptions and helps detect threats that might normally go unnoticed. It creates an operational opportunity by collaborating into a centralized dashboard, providing various alerting and recommendation capabilities. We discussed at a high level the following topics in relation to Azure Security Center:

- Architecture
- Security Policies
- Policy and Compliance
- Continuous Assessments
- Security Score
- Recommendations

Then we covered defending against threats by using Advanced Threat Protection, as well as PaaS protection, brute force attacks, and the ability to have a centralized monitoring environment to increase security posture for IoT devices via adaptive threat prevention and intelligent threat detection and response.

Back

Back to Main

Next Sections

Shared Access Signature (SAS)

Shared access signatures provide delegated access to resources in storage accounts, meaning you can grant a client limited permissions to objects in your storage account for a specified period and with a specified set of permissions. You can also grant these limited permissions without having to share your account access keys.

Azure supports **three types** of shared access signatures:

- **User Delegation SAS:** This type of delegation is secured with Azure Active Directory credentials and also by the permissions that get specified for the SAS. A user delegation SAS applies to Blob storage only.
- **Service SAS:** This is secured with a storage account key. A service SAS delegates access to a resource in only one of the Azure Storage services: Blob storage, Queue Storage, Table storage, or Azure Files.
- **Account SAS:** This SAS is secured with the storage account key. An account SAS delegates access to resources in one or more of the storage services. All of the operations available via a service or user delegation SAS are also available via an account SAS. You can also delegate access to operations that apply at the level of service, such as **GET/Set Service Properties** and **Get Service Stats** operations. You can also delegate this access to read, write, and delete operations on blob containers, tables, queues, and file shares that are not permitted with a service SAS.

There are **two forms** a shared access signature can take:

- **Ad hoc SAS:** This means the start time, expiry time, and permissions are specified in the SAS URI. Any type of SAS can be considered an ad hoc SAS.
- **Service SAS with stored access policy:** This is defined on a resource container and can be used to manage constraints for one or more service SAS. The SAS then inherits the constraints — including start time, expiry time, and permissions — in the stored access policy.

Next

Back to Main
Next Sections

Shared Access Signature (cont)

How a Shared Access Signature Works

A shared access signature is a signed URI that points to one or more storage resources and includes a token that contains a special set of parameters. The token indicates how the resource will be accessed by the client. One of these query parameters, the signature, is constructed from the SAS parameters and signed with the key that was used to create the SAS. Azure Storage uses this signature to authorize access to the storage resource.

SAS Signature

You can sign a SAS with:

- **A user delegation key:** Created using Azure Active Directory credentials. A security principal must be assigned a RBAC role that includes the **Microsoft.Storage/storageAccounts/blobServices/generateUserDelegationKey** action.
- **The storage account key:** Both a service SAS and an account SAS are signed with the storage account key. In order to create a SAS that is signed with the account key, an application needs to have access to the key.

SAS Token

- Client applications provide a SAS URI to Azure Storage as part of the request. If the service that validates the signature is valid, then the request is authorized. Otherwise, the request is declined with error 403 (Forbidden). Here is an example of a SAS URI showing the resource URI and the SAS token:

Back Next

Back to Main Next Sections

Shared Access Signature (cont)

Best Practices When Using SAS

There are two potential risks that fall in line with shared access signatures to be aware of:

- If a SAS is leaked, it can be used by anyone that obtains it, which can potentially compromise the storage account.
- If a SAS provided to a client application happens to expire and the application is unable to retrieve a new SAS from the service, the application functionality and availability may be at risk.

Mitigate Risks with These Recommendations

- **Always use HTTPS** to create or distribute a SAS. If a SAS is passed over HTTP and intercepted, an attacker performing a man-in-the-middle attack is able to read the SAS and then use it just as the intended user could have, potentially compromising sensitive data or allowing for data corruption by the malicious user.
- **Use a user delegation SAS when possible.** A user delegation SAS provides superior security to a service SAS or an account SAS. A user delegation SAS is secured with Azure AD credentials, so that you do not need to store your account key with your code.
- **Have a revocation plan in place for a SAS.** Make sure you are prepared to respond if a SAS is compromised.
- **Define a stored access policy for a service SAS.** Stored access policies give you the option to revoke permissions for a service SAS without having to regenerate the storage account keys. Set the expiration on these very far in the future (or infinite) and make sure it's regularly updated to move it farther into the future.
- **Use near-term expiration times on an ad hoc SAS service SAS or account SAS.** In this way, even if a SAS is compromised, it's valid only for a short time. This practice is especially important if you cannot reference a stored access policy. Near-term expiration times also limit the amount of data that can be written to a blob by limiting the time available to upload to it.

Shared Access Signature (cont)

Mitigate Risks with These Recommendations (cont):

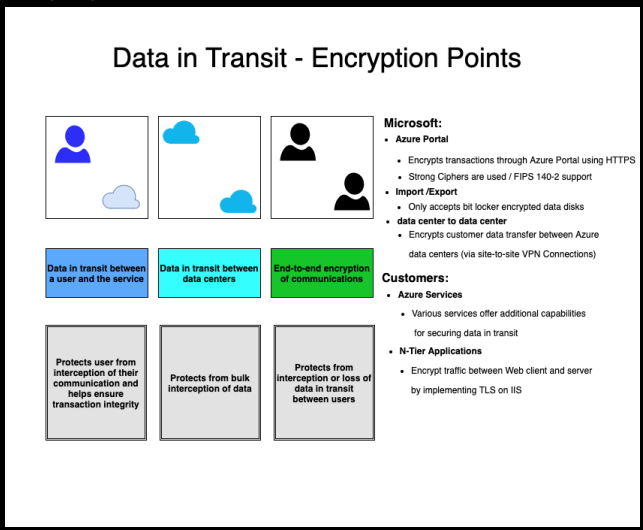
- **Have clients automatically renew the SAS if necessary.** Clients should renew the SAS well before the expiration in order to allow time for retries if the service providing the SAS is unavailable. If your SAS is meant to be used for a small number of immediate, short-lived operations that are expected to be completed within the expiration period, then this may be unnecessary as the SAS is not expected to be renewed. However, if you have a client that is routinely making requests via SAS, then the possibility of expiration comes into play. The key consideration is to balance the need for the SAS to be short-lived (as previously stated) with the need to ensure the client is requesting renewal early enough (to avoid disruption due to the SAS expiring prior to successful renewal).
- **Be careful with SAS start time.** If you set the start time for a SAS to **now**, then due to clock skew (differences in current time according to different machines), failures may be observed intermittently for the first few minutes. In general, set the start time to be at least 15 minutes in the past. Or, don't set it at all, which will make it valid immediately in all cases. The same generally applies to expiry time as well — remember that you may observe up to 15 minutes of clock skew in either direction on any request. For clients using a REST version prior to 2012-02-12, the maximum duration for a SAS that does not reference a stored access policy is one hour, and any policies specifying longer term than that will fail.
- **Be careful with SAS datetime format.** If you set the start time and/or expiry for a SAS, for some utilities (e.g., for the command line utility AzCopy) you need the datetime format to be '+%Y-%m-%dT%H:%M:%SZ', specifically including the seconds, in order for it to work using the SAS token.
- **Be specific with the resource to be accessed.** A security best practice is to provide a user with the minimum required privileges. If a user only needs read access to a single entity, then grant them read access to that single entity, and not read/write/delete access to all entities. This also helps lessen the damage if a SAS is compromised because the SAS has less power in the hands of an attacker.

Encryption in Transit

This is a mechanism of protecting data when it is in motion or being transmitted across networks. With Azure Storage, you can secure data using:

- **Transport-level encryption**, such as HTTPS when you transfer data into or out of Azure Storage.
- **Wire encryption**, such as SMB 3.0 encryption for Azure File shares.
- **Client-side encryption** to encrypt the data before it is transferred into storage and to decrypt the data after it is transferred out of storage.

The following diagram illustrates data in transit:



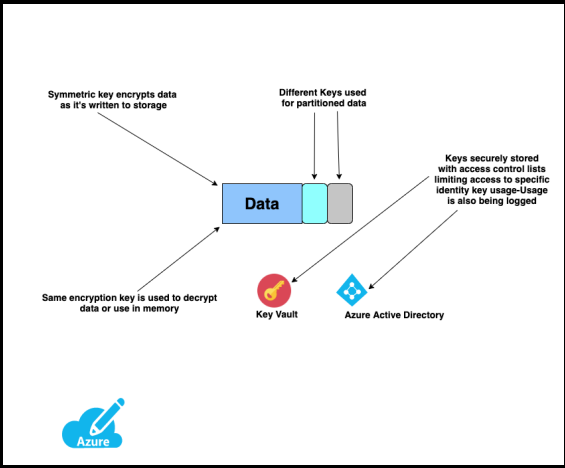
Back to Main

Encryption at Rest

In many cases, data encryption at rest is mandatory not only for privacy but also for compliance requirements. For data encryption at rest, this is broken down into three Azure storage security features:

- **Storage Service Encryption:** Allows you to request encryption automation whenever data is getting written to Azure storage
- **Client-Side Encryption:** Also provides encryption for data at rest
- **Azure Disk Encryption:** Allows you to encrypt the OS disks and data disks used by an IaaS virtual machine

The following diagram illustrates an example of data at rest:



Back
Next

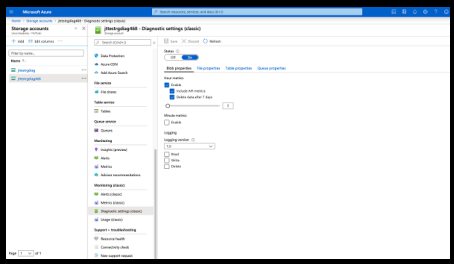
Storage Analytics

This performs logging and provides metric data for storage accounts. You can use it to trace requests, analyze usage, and determine issues that may be happening for a storage account. The logs from Storage Analytics detail information about successful and failed requests to a storage service. This in turn can be used to monitor individual requests and diagnose storage service issues. Request data gets logged on a best-effort basis. Examples of the types of authenticated requests include:

- Successful requests
- Filed requests, including timeout, throttling, network, authorization, and other pertinent errors
- Requests using a Shared Access Signature (SAS), including failed and successful requests
- Requests to analytics data

Storage Analytics has to be enabled for each individual service you want to monitor and will need to be turned on from the Azure Portal. This can also be enabled with the REST API or the client library. This aggregated data is stored in a well-known blob (for logging) and in well-known tables (for metrics), which may be accessed using Blob service and Table service APIs. With Storage Analytics, there is a 20 TB limit on the amount of stored data that is independent of the total limit for your storage account.

Here is an example of the Storage Accounts page in the Azure Portal where you would set up monitoring on a particular storage account:



Shared Access Signature (cont)

Mitigate Risks with These Recommendations (cont):

- **Understand that your account will be billed for any usage, including via a SAS.** If you provide write access to a blob, a user may choose to upload a 200 GB blob. If you've given them read access as well, they may choose to download it 10 times, incurring 2 TB in egress costs for you. Again, provide limited permissions to help mitigate the potential actions of malicious users. Use short-lived SAS to reduce this threat (but be mindful of clock skew on the end time).

- **Validate data written using a SAS.** When a client application writes data to your storage account, keep in mind that there can be problems with that data. If your application requires that data be validated or authorized before it is ready to use, you should perform this validation after the data is written and before it is used by your application. This practice also protects against corrupt or malicious data being written to your account, either by a user who properly acquired the SAS or by a user exploiting a leaked SAS.

- **Know when not to use a SAS.** Sometimes the risks associated with a particular operation against your storage account outweigh the benefits of using a SAS. For such operations, create a middle-tier service that writes to your storage account after performing business rule validation, authentication, and auditing. Also, sometimes it's simpler to manage access in other ways. For example, if you want to make all blobs in a container publicly readable, you can make the container public rather than providing a SAS to every client for access.

- **Use Azure Monitor and Azure Storage logs to monitor your application.** You can use Azure Monitor and storage analytics logging to observe any spike in authorization failures due to an outage in your SAS provider service or to the inadvertent removal of a stored access policy.

The following links can be used for in depth documentation from Microsoft:

- **Azure Storage metrics in Azure**
- **Azure Storage analytics logging**

Cross-Origin Resource Sharing (CORS)

This is a mechanism that allows domains to give each other permission for accessing each other's resources. The User Agent sends extra headers to ensure that the JavaScript code loaded from a certain domain is allowed to access these resources located in another domain. The latter domain then replies with an acknowledgment via extra headers, either allowing or denying the original domain access to its resources.

Azure storage services now support CORS. Once the proper rules are set, and a properly authenticated request takes place, the domain receiving the request will evaluate and determine if this request is allowed according to the specified rules.

A CORS request from an originating domain may consist of two separate requests:

- **A Preflight Request:** This queries the CORS restrictions imposed by the service. The preflight request is required unless the request is what is referred to as a **Simple Method**, meaning GET, HEAD, or POST. In Preflight requests, the restrictions are set up by the account owners. A Web Browser, or another agent, sends an **OPTIONS** request that includes headers, a method, and an origin domain. If the options request doesn't contain the correct CORS information, it will return a status code 400 (bad request).

- **Actual Request:** Once the preflight request is accepted and the response returned, the browser will dispatch the actual request against the storage resource. The browser then denies the actual request immediately if the preflight request was rejected. If a match is found, the Access-Control headers are added to the response back to the client. If a match is not found, the CORS Access-Control headers are not returned.

CORS Rules

Each element included in a CORS element is described below:

- **AllowedOrigins**: The origin domains that are permitted to make a request against the storage service via CORS. The origin domain is the domain from which the request originates. Note that the origin must be an exact case-sensitive match with the origin that the user sends to the service. You can also use the wildcard character **`*`** to allow all origin domains to make requests via CORS.
- **AllowedMethods**: The methods (HTTP request verbs) that the origin domain may use for a CORS request. In the example above, only PUT and GET requests are permitted.
- **AllowedHeaders**: The request headers that the origin domain may specify on the CORS request. In the example above, all metadata headers starting with **`x-ms-meta-data`**, **`x-ms-meta-target`**, and **`x-ms-meta-abcare`** are permitted. Note that the wildcard character **`*`** indicates that any header beginning with the specified prefix is allowed.
- **ExposedHeaders**: The response headers that may be sent in response to the CORS request and exposed by the browser to the request issuer. In the example above, the browser is instructed to expose any header beginning with **`x-ms-meta`**.
- **MaxAgeInSeconds**: The maximum amount of time that a browser should cache the preflight OPTIONS request.

The Azure storage services support specifying prefixed headers for both the **AllowedHeaders** and **ExposedHeaders** elements. To allow a category of headers, you can specify a common prefix to that category. For example, specifying **`x-ms-meta*`** as a prefixed header establishes a rule that will match all headers that begin with **`x-ms-meta`**.

CORS Rules (Cont)

The following limitations apply to CORS rules:

- You can specify up to five CORS rules per storage service (Blob, File, Table, and Queue).
- The maximum size of all CORS rules settings on the request, excluding XML tags, should not exceed 2 KB.
- The length of an allowed header, exposed header, or allowed origin should not exceed 256 characters.
- Allowed headers and exposed headers are:
  - Literal headers, where the exact header name is provided, such as **`x-ms-meta-processed`**. A maximum of 64 literal headers may be specified on the request.
  - Prefixed headers, where a prefix of the header is provided, such as **`x-ms-meta-data*`**. Specifying a prefix in this manner allows or exposes any header that begins with the given prefix. A maximum of two prefixed headers may be specified on the request.
  - The methods (or HTTP verbs) specified in the **AllowedMethods** element must conform to the methods supported by Azure storage service APIs. Supported methods are DELETE, GET, HEAD, MERGE, POST, OPTIONS, and PUT.

Understanding CORS Rule Evaluation Logic

When a storage service receives a preflight or actual request, it evaluates the request based on the CORS rules you established for the service via the appropriate Set Service Properties operation. CORS rules are evaluated in the order in which they were set in the request body of the Set Service Properties operation.

CORS Rules (Cont)

Understanding CORS rule evaluation Logic (cont)

CORS rules are evaluated as follows:

a. First, the origin domain of the request is checked against the domains listed for the **AllowedOrigins** element. If the origin domain is included in the list, or all domains are allowed with the wildcard character *****, then rules evaluation proceeds. If the origin domain is not included, then the request fails.

b. Next, the method (or HTTP verb) of the request is checked against the methods listed in the **AllowedMethods** element. If the method is included in the list, then rules evaluation proceeds; if not, then the request fails.

c. If the request matches a rule in its origin domain and its method, that rule is selected to process the request, and no further rules are evaluated. Before the request can succeed, however, any headers specified on the request are checked against the headers listed in the **AllowedHeaders** element. If the headers sent do not match the allowed headers, the request fails.

Since the rules are processed in the order that they are present in the request body, best practices recommend that you specify the most restrictive rules with respect to the first origins on the list, so that these are evaluated first. Specify rules that are less restrictive – for example, a rule to allow all origins – at the end of the list.

Example - CORS rules evaluation

CORS Rules (Cont)

Understanding how the Vary Header is set:

The Vary header is a standard HTTP/1.1 header consisting of a set of request header fields that advise the browser or user agent about the criteria that was selected by the server to process the request. The Vary header is mainly used for caching by proxies, browsers, and CDNs, which use it to determine how the response should be cached.

Azure Storage sets the Vary header to Origin for actual GET/HEAD requests in the following cases:

- When the request origin exactly matches the allowed origin defined by a CORS rule. For it to be an exact match, the CORS rule may not include a wildcard * character.
- There is no rule matching the request origin, but CORS is enabled for the storage service.

In the case where a GET/HEAD request matches a CORS rule that allows all origins, the response indicates that all origins are allowed, and the user agent cache will allow subsequent requests from any origin domain while the cache is active. Note that for requests using methods other than GET/HEAD, the storage services will not set the Vary header, since user agents do not cache responses to these methods.

Azure Response to Get/Head requests example

Request	Account setting and result of rule evaluation	Account setting and result of rule evaluation	Account setting and result of rule evaluation	Response	Response	Response
Origin header present on request	CORS rule(s) specified for this service	Matching rule exists that allows all origins (*)	Matching rule exists for exact origin match	Response includes Vary header set to Origin	Response includes Access-Control-Allowed-Origin: "*"	Response includes Access-Control-Exposed-Headers
No	No	No	No	No	No	No
No	Yes	No	No	Yes	No	No
No	Yes	Yes	No	No	Yes	Yes
Yes	No	No	No	No	No	No
Yes	Yes	No	Yes	Yes	No	Yes
Yes	Yes	No	No	Yes	No	No
Yes	Yes	Yes	No	No	Yes	Yes

Wrapping Up

In this section, we highlighted the following topics:

6.1.1 Shared Access Signature

- We discussed how SAS is constructed and how the elements work with a secure token. This is a signed URI that points to a designated storage resource.

6.1.2 Encryption in Transit

- This is a method for encrypting data at the transport layer while it is in motion.

6.1.3 Encryption at Rest

- Encrypting data not in motion using symmetric encryption methods to encrypt and decrypt large amounts of data quickly.

6.1.4 Storage Analytics

- Performs logging and provides metrics data for a storage account. You can use this data to trace requests, analyze usage trends, and diagnose issues with storage accounts.

Wrapping Up (Cont)

6.1.5 Enabling Browser-Based Clients Using CORS

- **Cross-Origin Resource Sharing:** This is a mechanism that allows restricted resources on a web page to be requested from another domain outside of the originating domain. A web page may freely embed things like cross-origin images, stylesheets, scripts, iframes, and videos.

- We discussed the architecture behind CORS, the different types of requests, the limitations when it comes to rules and, an overview of evaluating CORS logic.

Back

Course Navigation

Identity and Access Management
Section 4

Operations
Section 5

Storage
Section 6

Networking
Section 7

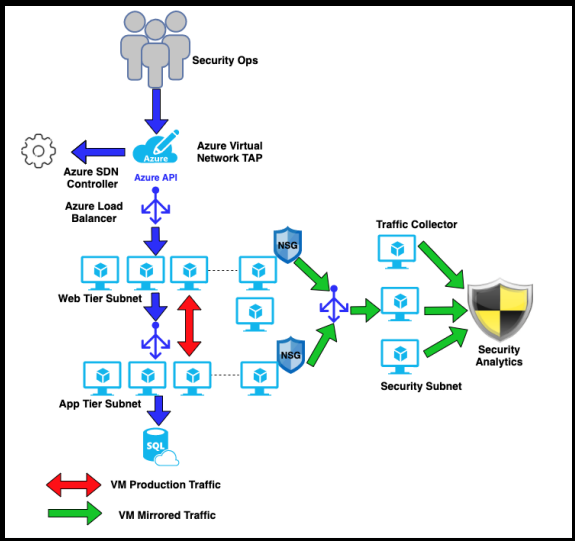
Network Layer Controls
Network Security Groups (NSG)
Route Control and Forced Tunneling
Application Gateway
Web Application Firewall
Security Center
Conclusion

Compute
Section 8

Network Access Control

This is the act of limiting connectivity to and from specific devices or subnets and represents the foundation of network security. The goal of network access control is to make sure that your resources are accessible to only users that are allowed this access.

The following diagram is one of many examples for Network Access Control topology with Azure:



Next

Back to Main
Next Sections

Network Security Groups

This is a basic stateful packet filtering firewall and enables access control based on a 5-Tuple concept. 5-Tuple refers to a set of five different values that are comprised of a TCP/IP connection. This includes a source IP address/port number, destination IP address/port number, and the protocol that is in use. NSGs do not provide application layer inspection or authenticated access controls. They can be used to control traffic between an Azure Virtual Network and the internet.

Virtual Networks:
This is the building block for a private network in Azure. This enables many types of Azure resources, such as virtual machines that securely communicate with each other, the internet, and on-premises networks. The concepts are similar to a traditional network that you would operate in your own data center but carries the benefits that come from Azure, such as infrastructure, availability, and isolation.

Concepts:

- **Address Space:** When creating virtual networks, you have to specify a private IP address using public and private addresses. Azure assigns resources in a virtual network private IP from the address space that you specify. An example would be an address space getting assigned to 100.10.10.0/20; the VM would be assigned a private IP in that address space range.
- **Subnets:** This allows you to segment your network into a sub-network and allocate a portion of the IP spaces to each subnet. You can then deploy resources in a specific subnet, just like a traditional network. You can then segment the subnets that are appropriate for your internal network, and this will improve address allocation efficiency. Resources can then be secured using Network Security Groups.
- **Regions:** A VNet is scoped to a single region/location; however, multiple virtual networks from different regions can be connected through Virtual Network Peering.
- **Subscription:** VNet is scoped to a subscription; you can implement multiple virtual networks in a subscription and region.

Network Security Groups (Cont.)

Best Practices

It is important in the design phase to try and implement with a universal design principle:

- Ensure non-overlapping address spaces. Make sure VNet address space (CIDR block) does not overlap with your organization's other ranges.
- Be sure not to cover the entire address space of the VNet. Planning ahead will save time and ensure the proper reservation of address space for the future.
- It is recommended to have fewer large VNets than multiple small VNets. This can prevent management overhead.
- Be sure to secure the VNets using Network Security Groups (NSG).

Communicate with the Internet

All resources in a VNet can communicate outbound to the internet by default. You can communicate to an inbound resource by assigning a public IP address or public load balancer. You can also use the public IP or public load balancer to manage your outbound connections.

Communicate Between Azure Resources

Azure resources communicate with each other in the following ways:

- **Through a virtual network**: You can deploy VMs, and several other types of Azure resources to a virtual network, such as Azure App Service Environments, the Azure Kubernetes Service (AKS), and Azure Virtual Machine Scale Sets.
- **Through a virtual network service endpoint**: Extend your virtual network private address space and the identity of your virtual network to Azure service resources, such as Azure Storage accounts and Azure SQL databases, over a direct connection. Service endpoints allow you to secure your critical Azure service resources to only a virtual network.
- **Through VNet Peering**: You can connect virtual networks to each other, enabling resources in either virtual network to communicate with each other, using virtual network peering. The virtual networks you connect can be in the same, or different, Azure regions.

Network Security Groups (Cont.)

Communicate with On-Premise Resources: 

You can connect on-premise computers and networks to virtual networks using any combination of the following options:

- **Point-to-site virtual private network (VPN):** Established between a virtual network and a single computer in your network. Each computer that wants to establish connectivity with a virtual network must configure its connection. This connection type is great if you're just getting started with Azure, or for developers, because it requires little or no changes to your existing network. The communication between your computer and a virtual network is sent through an encrypted tunnel over the internet.
- **Site-to-site VPN:** Established between your on-premises VPN device and an Azure VPN Gateway that is deployed in a virtual network. This connection type enables any on-premises resource that you authorize to access a virtual network. The communication between your on-premises VPN device and an Azure VPN gateway is sent through an encrypted tunnel over the internet.
- **Azure ExpressRoute:** Established between your network and Azure, through an ExpressRoute partner. This connection is private. Traffic does not go over the internet.

Route Network Traffic: 

Azure routes traffic between subnets, connected virtual networks, on-premises networks, and the Internet, by default. You can implement either or both of the following options to override the default routes Azure creates:

- **Route tables:** You can create custom route tables with routes that control where traffic is routed to for each subnet.

- **Border gateway protocol (BGP) routes:** If you connect your virtual network to your on-premises network using an Azure VPN Gateway or ExpressRoute connection, you can propagate your on-premises BGP routes to your virtual networks.

Route Control and Forced Tunneling:
The ability to control routing on Azure networks is critical for security and access control. If you need to ensure that all inbound/outbound traffic is going through a virtual security appliance, you need to be able to customize routing.

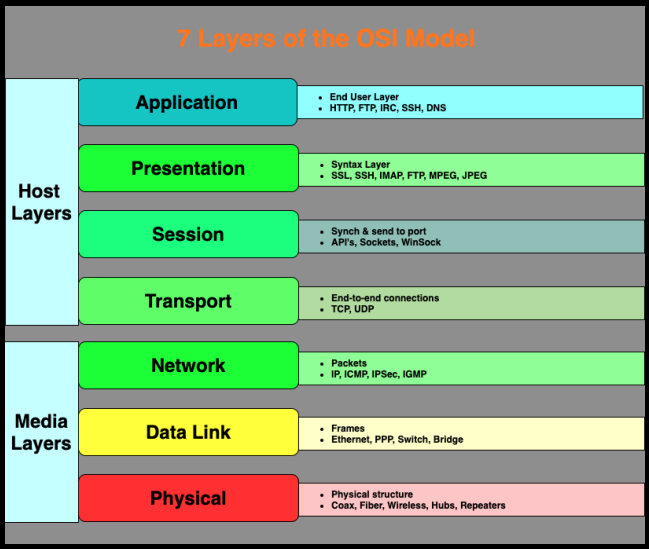
User-Defined Routes:
Allow you to customize inbound and outbound traffic for virtual machines or subnets to ensure the most secure route possible. Forced tunneling can be put in place to secure services that are not allowed to initiate connections to the internet. Due to the nature of inbound requests and the dependencies placed on internet facing web servers, traffic is allowed inbound to these servers. However, forced tunneling usually comes into play for outbound traffic to the internet and is commonly forced to go through on-premise security proxies and firewalls.

Virtual Network Security Appliances:
So far, we have discussed options for Network security referencing Network Security Groups, Forced Tunneling, and User-Defined Routes. These provide a level of security at the transport layers of the OSI model. However, there may be times when you need to enable security at a higher level of the stack. You can do a search in the Marketplace in the Azure Portal for "**security**" and "**security appliance**" for some of these solutions that Microsoft has partnered with.

OSI Model:
Circling back on this conceptual model, this is what characterizes and standardizes the communication functions without the internal structure of technology. The goal is to standardize these communications in an interoperable fashion due to the diverse communication systems that are out there. The design is to provide error-free communications and is a product that was designed by the Open Systems Interconnection project by the International Organization for Standardization (ISO).

OSI Model (Cont.)

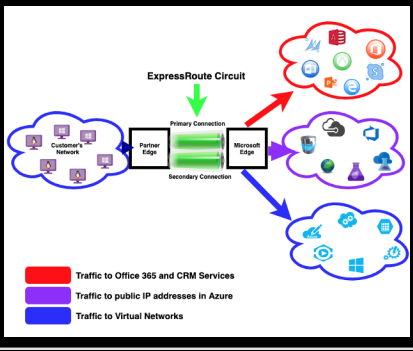
The following example diagram shows the stacked OSI Model:



VPN Gateway:
To send network traffic between your Azure Virtual Network and your on-premises site, you must create a VPN Gateway for your Azure Virtual Network. VPN Gateway is a type of virtual gateway that sends encrypted traffic across a public connection. You can also use the VPN Gateway to send traffic between your VNet and over the Azure Network Fabric.

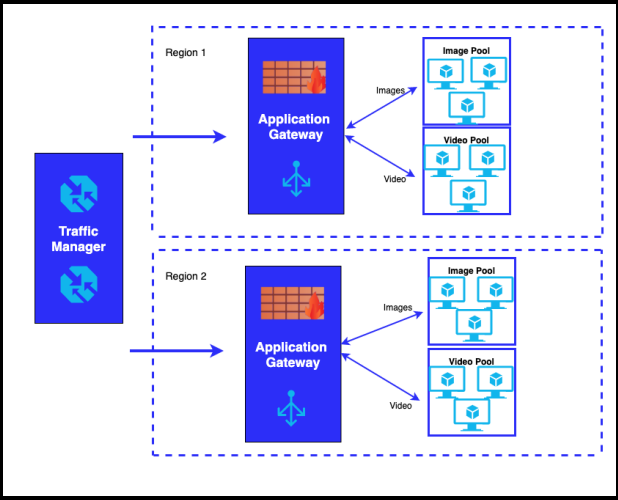
Express Route:
Microsoft Azure Express Route is a dedicated Wan link that lets you extend your on-premises networks into the Microsoft Cloud over a dedicated private connection facilitated by a connectivity provider. You can establish connections to Microsoft cloud services, such as Azure, Office 365, and CRM online. Connectivity can come from any-to-any (IP VPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a co-location. ExpressRoute connections do not go over the public internet, so it can be considered more secure than VPN-based solutions. This also improves the reliability, speeds, and lower latencies than a typical connection over the internet.

The following diagram illustrates an **ExpressRoute Circuit**:



Application Gateway
This is a Microsoft Azure feature that works from a layer 7 load balancing capability for applications. It allows you to optimize web servers in production by offloading CPU intensive SSL termination to the Application Gateway. It also provides other layer 7 routing capabilities, including round-robin of distributing incoming traffic, cookie-based session affinity, URL path-based routing, and the ability to host multiple websites behind a single Application Gateway. It also serves up redundancy in that it can fail over performance-routing HTTP requests between servers that are in the cloud or on-premise.

The following diagram illustrates how the Application Gateway fits within the Azure scope:



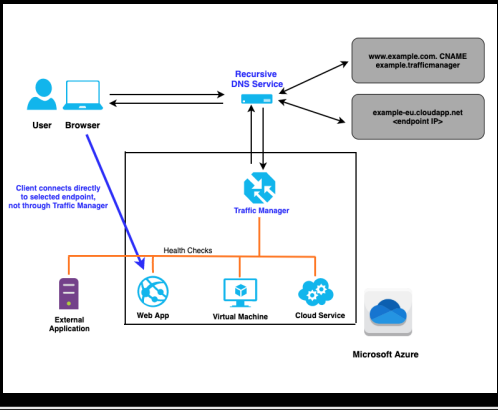
Web Application Firewall

This is a feature of Azure Application Gateway that provides protection to web applications that are using the application gateway for standard Application Delivery Control (ADC) functions. The Web Application Firewall does this by protecting against most of the OWASP (Open Web Application Security Project) top 10 web vulnerabilities:

- SQL injection protection
- Common Web Attack Protection such as command injection, HTTP request smuggling, HTTP response splitting, and remote file inclusion attack
- Protection against HTTP protocol violations
- Protection against HTTP protocol anomalies such as missing host user-agent and accept headers
- Prevention against bots, crawlers, and scanners
- Detection of common application misconfigurations such as Apache and IIS

Traffic Manager

Microsoft Azure Traffic Manager allows you to control the distribution of user traffic for service endpoints in different data centers. Service endpoints that are supported by traffic manager inside Azure VM's, Web Apps, and Cloud services. You can also use Traffic Manager with external non-Azure endpoints. Traffic Manager uses DNS to direct client requests to the most logical endpoint, based oh the routing methods that have been defined as well as the health of the endpoints at the time of the request.



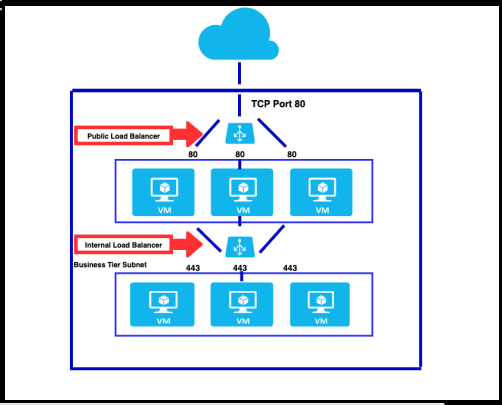
Web Application Firewall (Cont.)

Azure Load Balancer
Load balancer operates at layer 4 of the OSI model. It's a single point of contact for clients and evenly distributes the load for incoming traffic across groups of backend resources and servers.

Public Load Balancer
This can provide outbound connections for VM's inside the Virtual Network. This is accomplished by a private IP translation to the public address. Public load balancers are essentially used to balance internet traffic from VM's.

Internal or Private Load Balancer
This is used where private IP's are needed at the front end only. Internal load balancers are used to balance traffic inside your virtual network. A load balancer can be accessed by means of a frontend service for on-premise or hybrid environments.

This diagram is an example of multi-tier applications that are using both public and internal Load Balancers:



Security Center

Continuously analyzes the security state of your Azure resources for network security best practices. When Security Center identifies potential vulnerabilities, it creates recommendations that will guide you through the remediation steps or process of configuring the needed controls to harden and protect resources.

As discussed in previous lessons, the three most important security challenges Security Center addresses are:

- **Rapidly changing workloads**
- **Increasingly sophisticated attacks**
- **Security skills are in short supply**

Security addresses these by:

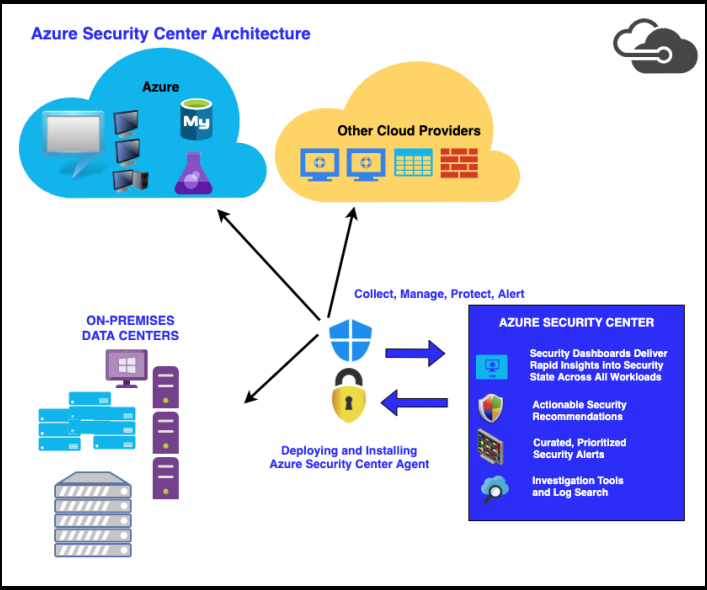
- **Strengthen security posture**: Assessments of the environment, giving status updates
- **Protect against threats:** Raises threat prevention and threat detection concerns
- **Get secure faster:** Done at cloud speed, natively integrated with auto-provisioning and protection

Once again in referencing the capabilities:

- **Security Policy and Compliance:** Manage security policies across subscriptions and entire tenants. This includes tracking governance and compliance.
- **Continuous Assessments:** This includes features such as Network Map, Secure Score, and Recommendations.
- **Threat Protection:** From non-Azure servers to different Infrastructure layers in Azure.
- **Advanced Threat Protection:** Integrates with Security Center offering robust protection.

Security Center (Cont.)

- The following diagram illustrates a high level architecture behind Security Center:



Course Navigation

Identity and Access Management
Section 4

Operations
Section 5

Storage
Section 6

Networking
Section 7

- Network Layer Controls
- Network Security Groups (NSG)
- Route Control and Forced Tunneling
- Application Gateway
- Web Application Firewall
- Security Center
- Conclusion

Compute
Section 8

Wrapping Up

7.1.1 Network Layer Controls
In this section, we discussed Network Access Controls and how this limits the connectivity to certain subnets and resources and is really the foundation around Network Security.

7.1.2 Network Security Groups
This emphasized how Azure resources can communicate with one another through means of Virtual networks (VNet). We touched on Site-to-Site, Point-to-Site, and ExpressRoute communications that can also integrate with on-premises resources.

7.1.3 Route Control and Forced Tunneling
In this section, we talked about the ability to customize routes for inbound and outbound traffic in order to secure and improve performance, how Azure also offers secure virtual network appliances in the marketplace, and we touched on the 7 layer OSI model.

7.1.4 Application Gateway
This section provided insight into Azures Application Gateway that helps to load balance applications based on the 7 layer OSI model.

7.1.5 Web Application Firewall
This section focused on the application firewall's ability to protect against the top 10 web vulnerabilities based on the OWASP . Then we discussed Traffic Manager, Azure, and Public and Private Load Balancing capabilities

7.1.6 Security Center
As this really shows some of the major security features within Azure, we demonstrated the capabilities along with an architecture example.

Back

Back to Main

Next Sections

Capabilities for additional Security

With Azure IaaS, you can use many of the vendor products for antimalware software. This includes Symantec, Trend Micro, McAfee, and Kaspersky to protect virtual machines from malicious files, adware, and other threats. Microsoft Antimalware for Azure Cloud Services and virtual machines is an extra defense in depth that can help protect, identify and remove viruses, spyware, and other malicious software. Microsoft Antimalware provides configurable alerts when known malicious triggers attempt to install in your Azure systems. These types of software programs for added protection can be deployed through Security Center.

Antimalware: The built-in Azure antimalware protection components are built on the same technology as Microsoft Security Essentials (MSE), Microsoft Forefront Endpoint Protection, System Center Endpoint Protection, Intune, and Windows Defender. There is a baseline monitoring that is installed by default, but you may need to have protection deployed based on workloads and turn on monitoring for some of these solutions. The following core features are available by default:

- **Real-time protection:** Monitors activity in Cloud Services and on Virtual Machines to detect and block malware execution.
- **Scheduled scanning:** Scans periodically to detect malware, including actively running programs.
- **Malware remediation:** Automatically takes action on detected malware, such as deleting or quarantining malicious files and cleaning up malicious registry entries.
- **Signature updates:** Automatically installs the latest protection signatures (virus definitions) to ensure protection is up-to-date on a pre-determined frequency.
- **Antimalware Engine updates:** Automatically updates the Microsoft Antimalware engine.

Capabilities for Additional Security

Antimalware (Cont)

Antimalware Platform updates: Automatically updates the Microsoft Antimalware platform.

Active protection: Reports telemetry metadata about detected threats and suspicious resources to Microsoft Azure to ensure rapid response to the evolving threat landscape, as well as enabling real-time synchronous signature delivery through the Microsoft Active Protection System (MAPS).

Samples reporting: Provides and reports samples to the Microsoft Antimalware service to help refine the service and enable troubleshooting.

Exclusions: Allows application and service administrators to configure exclusions for files, processes, and drives.

Antimalware event collection: Records the antimalware service health, suspicious activities, and remediation actions taken in the operating system event log and collects them into the customer's Azure Storage account.

Architecture

The Microsoft Antimalware for Azure includes the client and service, classic deployment model, and PowerShell cmdlets, along with a Diagnostics Extension. According to Microsoft, this antimalware is supported on Windows Server 2008 R2, 2012, and 2012 R2. It is not supported on any of the Linux family of operating systems. The software comes disabled by default on all guest operating systems in the cloud. The antimalware will, however, run on Azure app services by default, just not by default on VM's hosting customer content.

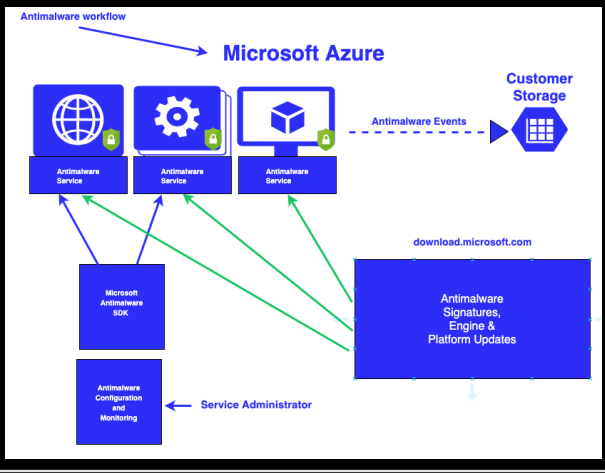
Capabilities for additional security

Antimalware Architecture (Cont)

Microsoft Antimalware Workflow

Azure Administrators can enable the antimalware services with these options:

- Virtual Machines — from the Azure portal using **Security extensions**
- Virtual Machines — using the Visual Studio virtual machines configuration in **Server Explorer**
- Virtual Machines and Cloud Services — using the **Classic Deployment Model**
- Virtual Machines and Cloud Services — using **AntiMalware Powershell cmdlets**



Hardware Security Module

Protecting the keys that provide encryption and authentication is critical and can be done using the **Azure Key Vault**. The key vault provides options for storing your keys in HSMs (Hardware Security Modules) that have been certified to FIPS (Federal Information Processing Standards)

Azure Key Vault-primary usage

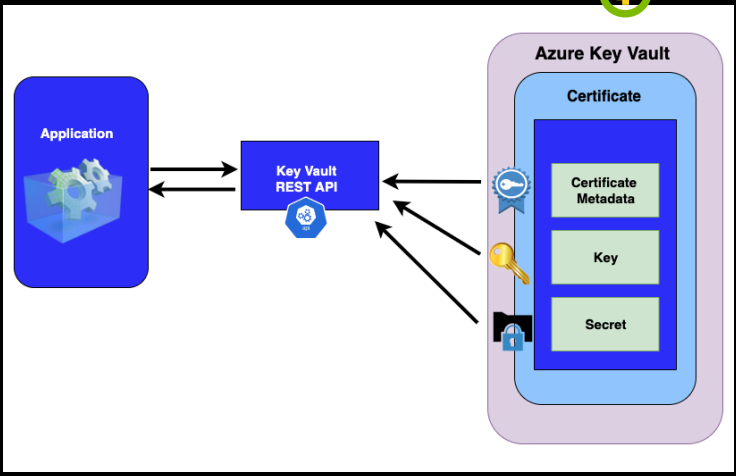
- **Secrets Management:** Azure Key Vault can be used to securely store and tightly control access to tokens, passwords, certificates, API keys, and other secrets
- **Key Management:** Azure Key Vault can also be used as a Key Management solution. Azure Key Vault makes it easy to create and control the encryption keys used to encrypt your data.
- **Certificate Management:** Azure Key Vault is also a service that lets you easily provision, manage, and deploy public and private Transport Layer Security/Secure Sockets Layer (TLS/SSL) certificates for use with Azure and your internal connected resources.
- **Store secrets backed by Hardware Security Modules:** The secrets and keys can be protected either by software or FIPS 140-2 Level 2 validated HSMs.

Monitoring Access and use in Key Vault

Another big advantage on making a switch to Azure Key Vault is the fact that you can monitor how and when the keys are being accessed. Every vault that you create you can turn on logging.

Hardware Security Module (Cont.)

Here is an example workflow diagram for Azure Key Vault:



Azure Backup

- This solution protects application data and has a minimal operating cost. It also protects virtual machines running Windows and Linux. It especially pertains to the section backing up Key Vault data.

Auto Site Recovery

- This feature is able to provide replication, failover, and recovery for unplanned outages or major service impacting events. The intention is to have a secondary location take over the environment in case the primary goes down. This is important when it comes to restoring Key Vault in an unplanned event.

Transparent Data Encryption
TDE and column level encryption (CLE) are SQL server encryption features that require customers to manage and store cryptographic keys for encryption. Azure Key Vault is designed to improve the security and management of these keys as well and store it in a highly available location for consumers. This can also be fully integrated with on-premises SQL servers.

TDE
This performs the real-time I/O encryption and decryption of the data and log files. The encryption uses a Database Encryption Key (DEK), which is stored in the database boot record for availability during recovery. DEK is a symmetric key secured by using a certificate stored in the master database of the server or the main asymmetric key protected by an EKM module. TDE protects data "at rest", meaning data and the log files. This complies with many of the laws and regulatory demands when it comes to safeguarding this data. Developers can also encrypt using AES and 3DES algorithms without changing applications.

About TDE
Encryption of the database is done from a page level, meaning the data is encrypted prior to being written to a disk, then decrypted when read into memory. TDE does not increase the size of an encrypted database.

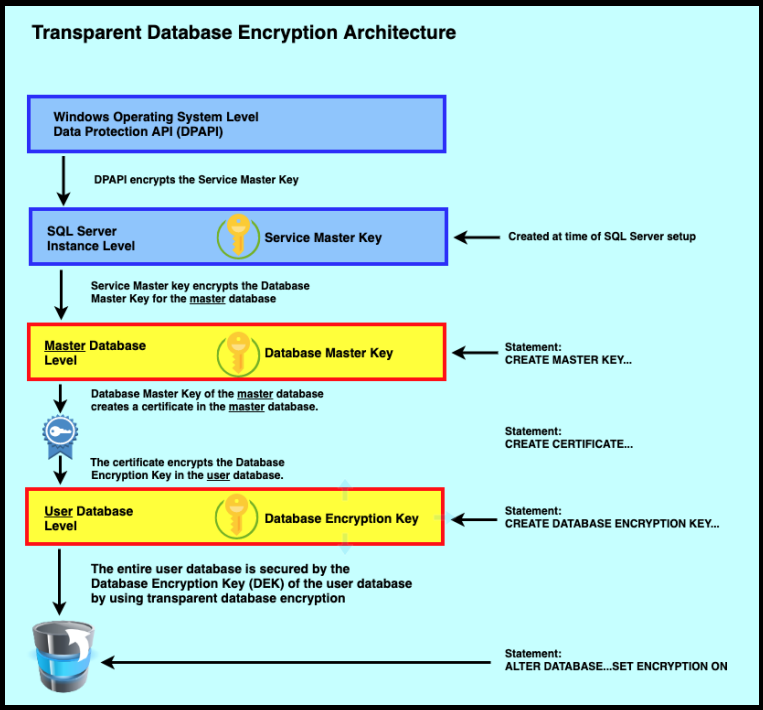
Information on SQL database
Using TDE with SQL V12, the server-level certificate is stored in the master database and is auto-created when SQL is getting deployed. To move a TDE database on to a SQL database, you do not have to decrypt the data for the move operation.

Information on SQL Server
Once secured, the database can be restored using the appropriate certificate. When enabling TDE, the certificate and private key should be backed up. If you ever need to restore or attach the database to another instance, both are needed.

Transparent Data Encryption (Cont.)

Encryption Hierarchy

The following illustration shows the architecture of TDE encryption:



VM Disk Encryption

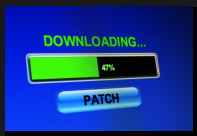
This feature helps to encrypt Windows and Linux IaaS virtual machine disks. It applies the industry standard BitLocker feature of Windows and DM-Crypt features of Linux to provide volume encryption for the OS and the data disks. This solution is also integrated with Azure Key Vault to help control and manage the disk-encryption keys and secrets in your Key Vault subscription. It also ensures the disks of the VM's that contain data at rest in Azure Storage are encrypted as well.

Azure Disk Encryption Considerations for Linux

- Uses DM-Crypt
- Integrates with Azure Key Vault
- Security Center can alert when disks for Linux aren't encrypted
- Specific supported Linux Operating systems can be found within the Microsoft Support Pages
- Know the size requirements
- Know the Network endpoint requirements and connecting to Azure Storage and Active Directory
- Encryption Key storage requirements

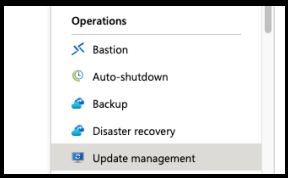
Azure Disk Encryption Considerations for Windows

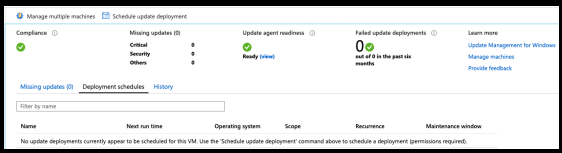
- Uses BitLocker feature for windows to encrypt
- Security Center can alert when disks for Windows aren't encrypted
- Azure Disk Encryption is not available for Basic A-Series VM's
- Not supported on VM's less that 2 GBs of memory
- Supported operating system families for client is Windows 8 and later, for a server it is Windows 2008 R2 or later
- To obtain a token it must be connected to a Azure Active Directory endpoint
- Must be able to connect to the KeyVault to obtain encryption keys
- Outbound rules may need to be applied if the VM is not able to connect to the internet and Azure Key Vault is behind a firewall



Patching and Compliance
Patch updates are essential for not only fixing potential issues within the operating system and specific software deployments, but it's also a critical element for having a strong security posture and often means the responsibility of maintaining compliance. Azure simplifies the process, and this becomes important, especially if you have been consumed by growth and need to stay ahead in order to maintain control of your environment.

Automation is key!!
Security Center, and many other areas in Azure, have the ability to collect the transparent data in your systems with many of these features having alerting capabilities. One immediate way to turn on patching automation is through the **Update Management** feature in a single VM.





You can also schedule custom deployments for patch management in the event you have to maintain high availability for solutions, and this needs to go through your organization's **Change Management Process.**

Working with Security Policies

As we have discussed previously, the Security Center's role for working with security policies, including built-in or custom ones you may build for your environment, is important to ensure you have the right policies in place. There are the key fundamentals for these policies that you will have to know.

- **Know how to properly manage:** There is a specific breakdown when it comes to identifying policies. You can view these through the security policy page and select the subscription, management group, or workspace that contains the policy you need to see. You can also add in policy packages. For instance, you can add in the Compliance package Azure CIS 1.1.0 to an existing security policy, and it will begin to pull in the scope of the data design from this regulatory package. This is known as **Dynamic Compliance Packages.**

- **Who can edit security policies?** Security Center uses RBAC, which also provides the built-in roles that can be assigned to users, groups, and services in Azure. There are two specific Security Center roles **Security Reader** and **Security Admin**.

- **Disabling Security Policies:** It is also important to know how to disable a security policy from the Policy and Compliance section. If it is generating recommendations that are not relevant to your environment, you may need to disable a particular policy.

Reporting: 

You can essentially query against data from **Application Insights** to generate custom reports on a schedule.

Connector using Microsoft Flow: 
You can connect Microsoft flow data to Application Insights. One example would be to use MS Flow to connect to a specific application ID and visualize the telemetry data for how many failed requests took place for that application.

Reporting (Cont.)

Automated Custom Reports:
Periodic reports can help a team on the information front on how business-critical services are running. Developers can use automated reports to give trending information, such as latency in applications.

Each enterprise has its own unique reporting needs, such as:

- Specific percentile aggregations of metrics or custom metrics in a report.
- Have different reports for daily, weekly, and monthly roll-ups of data for different audiences.
- Segmentation by custom attributes like region or environment.
- Group some AI resources together in a single report, even if they may be in different subscriptions, resource groups, etc.
- Separate reports that contain sensitive metrics are sent to a selective audience.
- Reports to stakeholders who may not have access to the portal resources.

Some of the key things we reviewed in section 8:

8.1.1 Antimalware and Antivirus
In this section, we talked about the ability to add in Antimalware/Antivirus from Azure as an extra layer of security. There is a default installation that comes with the VM's in your subscription with an ability to turn on features to give it more robust **Real-time-Protection, Schedule Scans, Malware Remediation, Signature Updates,** and **Engine Updates.**

8.1.2 Hardware Security Module (HSM)
Protecting Encryption and Authentication is the key take away from HSM. **Key Management, Certificate Management,** and **Stored Secrets in HSM** are the key features. We gave a workflow diagram and discussed the importance of Azure backups and site recovery as it pertains to Key Vault.

8.1.3 SQL VM TDE
TDE performs real-time I/O encryption and decryption of the data and log files. This can also be managed by Key Vault. Validating another reason to ensure periodic backups are taking place, if you have to restore and reattach a SQL database, and if you will need the certificate and private key that is stored securely in Key Vault.

8.1.4 VM Disk Encryption
Used to encrypt Windows with BitLocker, and Linux with DM-Crypt, there are specific requirements for each Operating System Family that can be found on the Microsoft Support Documents. Azure Key Vault can integrate with VM Disk encryption and assist in managing. Security Center can send you alerts for VM's that get deployed into the environment that does not have disk encryption set up.

Conclusion (Cont.)

8.1.5 Patch Updates
Both patching and updating help to improve security and provide service availability as well as help with regulatory and compliance demands. This can be fully integrated with the Security Center for automation to a centralized dashboard, or you can turn on the Update Management service for a single VM.

8.1.6 Security Policy and Management and Reporting
When working with security policies, it is important to know how to properly manage who can edit and how, and disabling permissions when needed. Azure also offers many reporting features within the security policies scope as well as your entire environment. Applications such as Microsoft Flow can be integrated with Azure with the ability to pull telemetry data from Application Insights.

Back

SDL Overview

- Microsoft Development (SDL) offers information on security considerations throughout all phases of the development process. This can help developers build secure software, address security compliance, and reduce cost. This brings security to the forefront of this development, and since it's 2008 inception, the Cloud, Internet of Things (IoT), and Artificial Intelligence (AI) have all been introduced.

Best Practices

- **Provide Training:** It is now the job of everyone to understand security basics, especially for many of the developers building software applications and those that support them. In general, they don't have to be security experts, but this will re-enforce and compliment the development life cycle.

- **Define Security Requirements:** Security and privacy need to be reflected in the development methodology and have continuous updates and changes that enhance the required functionality and security. This has an advantage when security is part of the initial design phase. This allows developers to integrate security and minimize disruption. Factors that are up for consideration are legal and compliance and industry-standard best practices with monitoring for known threats in all of the planning.

- **Define Metrics and Compliance Reporting:** It is imperative that the acceptable levels of security quality and the responsible teams for meeting these requirements are defined during the initial design. This helps to set expectations and for organizations to understand the risks associated with security vulnerabilities and issues up front, but also gets the communication cycle and the constant mitigation for these standards and what it takes to maintain out in the open. This also helps define what issues are critical or important in the security rating. These mechanisms help to track key performance indicators (KPIs).

SDL Overview (Cont.)

Best Practices

- **Perform Threat Modeling:** This should be used in environments where there is an underlying security risk. This can be applied at the component, application, or system level. It also allows for teams to consider, document, and discuss the security implications and correlate this information to the operational level of their current environment. This is a more effective and less expensive way to identify security vulnerabilities, determine risks from those threats, and be able to make security decisions to address and mitigate.

- **Establish Design Requirements**: This usually involves the implementation side for engineers from the SDL standpoint. This helps identify security decision points such as cryptography, type of authentication, logging, and many others. It is important that the resources that are part of these implementations truly know what the products do and if these will be a good fit for your environment.

- **Define and Use Cryptography Standards**: Clear encryption standards need to be made to ensure all data and sensitive information is properly secured with the potential of being transmitted from a wide variety of mobile and computing devices that are being allowed to access your organization's resources.

- **Manage the Security Risk of Using Third-Party Components:** Knowing the risk associated with third-party components, such as potential security vulnerabilities within the systems they are integrated with, is an important discussion that needs to take place on a regular basis. Keep the accountability of all of these systems to ensure that they are receiving the proper security patching and be sure to give the proper validation periods to these third-party systems.

- **Perform Static Analysis Security Testing (SAST)**: This has to do with analyzing source code compilations and providing highly scalable methods of implementing secure code. This allows developers to pinpoint flaws and replace them with safer alternatives while actively coding. This can also help track development changes taking place through the life cycle.

SDL Overview (Cont.)

Best Practices

- **Perform Dynamic Analysis Security Testing (DAST):** This is an initiative for run-time verification on packaged software that checks functionality once all of the components are integrated and running. This is typically achieved via a tool or suite of prebuilt attacks that can monitor the application behavior for things such as memory corruption, user privilege issues, or other defined security problems.

- **Perform Penetration Testing:** This is a security analysis testing that takes place by professionals that simulate the actions taken by a hacker. The objective is to uncover potential vulnerabilities resulting from things such as coding errors or misconfigurations.

- **Establish a Standard Incident Response Process:** Preparing an Incident Response Plan (IRP) is one of the first steps that should be taken to address new threats that can emerge over time. Most organizations have a Product Security Incident Response Team (PSIRT). It is important that the IRP works in coordination with this team and identifies critical areas such as who to contact during a security emergency, and what protocol to establish during this time. There are usually several teams that need to be involved, and you should test your Incident Response Plan regularly.

Secure Platform

Mandatory Security Training and Background Checks

Mandatory Security Training: Microsoft is making this information available for the processes they have in place when it comes to mandatory security training with their employees. This is an important audit verification in the event that auditors come in. Your organization needs this documented for audit purposes to ensure that the CSP that is hosting your resources and data are falling within the scope of regulatory and compliance.

The following screenshot represents the control responses that were given by Microsoft and orchestrated by the Cloud Security Alliance (CSA). This pertains to mandatory security training, and Microsoft wants you to see this in case you need to use something of this nature as an example for your own organization and audit requirements.

Created by Microsoft

IS-11 **Information Security - Training / Awareness**	A security awareness training program shall be established for all contractors, third party users and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, process and policies, relating to their function relative to the organization.	All appropriate Microsoft staff take part in a Windows Azure and/or GFS sponsored security-training program and are recipients of periodic security awareness updates when applicable. Security education is an on-going process and is conducted regularly in order to minimize risks. An example of an internal training is Microsoft Security 101. Microsoft also has non-disclosure provisions in our employee contracts. All Windows Azure and/or GFS staff are required to take training determined to be appropriate to the services being provided and the role they perform. "Information security awareness, education and training" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 8.2. For more information review of the publicly available ISO standards we are certified against is suggested.

Mandatory Security Training, Background Checks ← **Standard Response to Request for information >Security and Privacy Document**

Course Navigation

Networking
Section 7

Compute
Section 8

Secure Platform
Section 9

Security Development Cycle and Internal Audits

Mandatory Security Training and Background Checks

Penetration Testing, Intrusion Detection, DDoS, Audits, and Logging

State of the Art Data Centers, Physical Security, and Secure Networks

Security Incident Response and Shared Responsibility

Conclusion

Wrapping Up
Section 10

Back to Main

Background Checks: Similar to the first example, background checks for Microsoft's internal staff fall under the HR section of their control matrix. The screenshot below illustrates that example:

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
HR-01 Human Resources Security - Background Screening	Pursuant to local laws, regulations, ethics and contractual constraints all employment candidates, contractors and third parties will be subject to background verification proportional to the data classification to be accessed, the business requirements and acceptable risk.	All Microsoft US-based full-time employees (FTE) are required to successfully complete a standard background check as part of the hiring process. Background checks may include but are not limited to review of information relating to a candidate's education, employment, and criminal history.
HR-02 Human Resources Security - Employment Agreements	Prior to granting individuals physical or logical access to facilities, systems or data employees, contractors, third party users and customers shall contractually agree and sign the terms and conditions of their employment or service contract, which must explicitly include the parties responsibility for information security.	All appropriate Microsoft employees take part in a Windows Azure sponsored security-training program, and are recipients of periodic security awareness updates when applicable. Security education is an on-going process and is conducted regularly in order to minimize risks. Microsoft also has non-disclosure provisions in our employee contracts. All Windows Azure contractor staff and GFS staff are required to take any training determined to be appropriate to the services being provided and the role they perform. "Roles and responsibilities as well as information security awareness, education and training" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 8. For more information review of the publicly available ISO standards we are certified against is suggested.
HR-03 HR- Employee Termination	Roles and responsibilities for following performing employment termination or change in employment procedures shall be assigned, documented and communicated.	Microsoft Corporate Human Resources Policy drives employee termination processes. "Termination or change of employment" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 8.3. For more information review of the publicly available ISO standards we are certified against is suggested.

Mandatory Security Training, Background Checks

Standard Response to Request for the Information > Security and Privacy Document

Control ID in CCM[1]	Description (CCM Version R1.1. Final)	Microsoft Response
CO-01 Compliance - Audit Planning	Audit plans, activities and operational action items focusing on data duplication, access, and data boundary limitations shall be designed to minimize the risk of business process disruption. Audit activities must be planned and agreed upon in advance by stakeholders.	Our goals are to operate our services with security as a key principle, and to give you accurate assurances about our security. We have implemented and will maintain reasonable and appropriate technical and organizational measures, internal controls, and information security routines intended to help protect customer data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction. Each year, we undergo third-party audits by internationally recognized auditors to validate that we have independent attestation of compliance with our policies and procedures for security, privacy, continuity and compliance. ISO 27001 certifications for Windows Azure and Global Foundation Services (which runs the physical infrastructure) can be found on the website of our external ISO auditor, the BSI Group. Additional audit information is available under NDA upon request by prospective customers. Windows Azure independent audit reports and certifications are shared with customers in lieu of allowing individual customer audits. These certifications and attestations accurately represent how we obtain and meet our security and compliance objectives and serve as a practical mechanism to validate our promises for all customers. For security and operational reasons, Windows Azure does not allow our customers to perform their own audits on Microsoft's Windows Azure platform service, although customers are allowed to perform non- invasive penetration testing of their own application with prior approval. "Monitor and review the Information Security Management System (ISMS)" is covered under the ISO 27001 standards, specifically addressed in Clause 4.2.3. For more information review of the publicly available ISO standards we are certified against is suggested.
CO-02 Compliance - Independent Audits	Independent reviews and assessments shall be performed at least annually, or at planned intervals, to ensure the organization is compliant with policies, procedures, standards and applicable regulatory requirements (i.e., internal/external audits, certifications, vulnerability and penetration testing)	For more information see CO-01

Standard Response to Request for information >Security and Privacy Document

Secure Platform

Penetration Testing, Intrusion Detection, DDoS, Audits, and Logging

Intrusion Detection Example

SA-14 Security Architecture - Audit Logging / Intrusion Detection	Audit logs recording privileged user access activities, authorized and unauthorized access attempts, system exceptions, and information security events shall be retained, complying with applicable policies and regulations. Audit logs shall be reviewed at least daily and file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents. Physical and logical user access to audit logs shall be restricted to authorized personnel.	Access to logs is restricted and defined by policy and logs are reviewed on a regular basis. "Audit logging" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 10.10.1. For more information review of the publicly available ISO standards we are certified against is suggested.

Created by Microsoft

DDoS Example
Learning about Microsoft Threat Protection
https://www.microsoft.com/en-us/security/business/threat-protection

DDOS Protection Plans

Audits and Logging Example

SA-14 Security Architecture - Audit Logging / Intrusion Detection	Audit logs recording privileged user access activities, authorized and unauthorized access attempts, system exceptions, and information security events shall be retained, complying with applicable policies and regulations. Audit logs shall be reviewed at least daily and file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents. Physical and logical user access to audit logs shall be restricted to authorized personnel.	Access to logs is restricted and defined by policy and logs are reviewed on a regular basis. "Audit logging" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 10.10.1. For more information review of the publicly available ISO standards we are certified against is suggested.

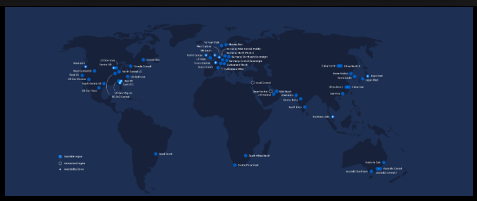
Created by Microsoft

Security Operations
https://www.microsoft.com/en-us/security/business/operations

Standard Response to Request for Information > Security and Privacy Document

Secure Platform

State of the Art Data Centers, Physical Security, and Secure Networks



Azure Data Centers

As discussed many times throughout the course, Azure data centers can provide you with highly available servers and storage. This comes without the high capital expenditures, installation and configuration costs, and service and maintenance decisions.

Physical Security

Microsoft takes a layered approach to physical security for their data centers. This includes access approval at the facility perimeter, building perimeter, inside the building, and on the data center floor. This reduces the risk of unauthorized access to the data center resources. The starting point is a business justification to access the facilities. All of this is approved on a need-to-access basis by Microsoft employees.

The next layer is the perimeter access with additional security in place for security personnel. The final layer is the data center floor, in which you will need to pass full body metal detection screening. Everything accessed during the data center visits is tracked.

Secure Networks

Virtual machines are required to be connected to the Azure Virtual Network. This is a logical construct built on top of the physical Azure network fabric.

- **Network Access Control:** This is the act of limiting connectivity to and from specific devices or subnets within a virtual network space. As discussed in previous lessons, Azure supports several types of Network Access control. Network Layered Control, Route Control, Forced Tunneling, and Virtual Network Security Appliances.

Secure Networks (Cont.)

Network Layered Control: The goal of network access control is to restrict virtual machine communication to the necessary systems, while other communication attempts are blocked.

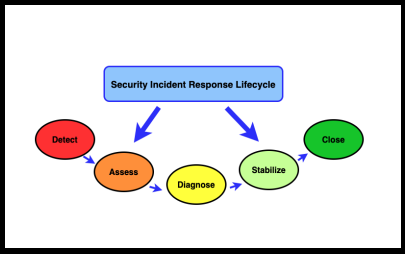
Network Security Rules (NSG): NSG is a basic, stateful, packet filtering firewall and enables controlled access based on the 5-tuple concepts as previously discussed. At a minimum, NSG's functionality is to simplify management and reduce the chances of configuration mistakes.

Additional Network Security: We have just barely tapped into the surface of Network Security and Azure. Some of the other featured highlights that have been discussed previously throughout this course are:

- ASC just in time VM access
- Service Endpoints
- Route Control and Forced Tunneling
- Virtual network security appliances
- Securing remote access and cross-premises connectivity
- Availability through HTTP-based load balancing
- Network and Global level load balancing
- DDoS Protection
- Azure Traffic Manager
- Monitoring Threat Detection
- Logging

Security and IT Risk: As the world of technology has changed, it has become important to think about security, as it is one of the most critical components of your environment. There has to be a balance of autonomy empowering other parts of your organization to adapt and transform to security demands. Updating and scaling must be in the plans, and education and information can help to achieve success in raising awareness for your entire organization.

- **Security Incident:** An occurrence that potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
- **Security Incident Roles and Responsibilities:** Responsibilities will need to be defined on who takes part during a security incident. Defining those roles should be developed into your Incident Response Plan (IRP). Examples may include a Security Team on-call, Security Incident Manager, Forensics Engineer, and Executive on-call.
- **Security Incident Response Lifecycle:** Microsoft follows a 5-step incident response process when managing a security incident. You will see other variations of this concept with NIST, CIS, and ITIL, and many more that are available to the public.



- Here is a similar view that was demonstrated back in Section 2. It is important to know that this is a layered approach when it comes to cloud security. It is essential for customers that are moving to the cloud to have an understanding of this type of model. There are considerable advantages moving to a cloud model, but the customer still needs to be responsible for protecting their users, applications, and service offerings.

	Infrastructure-as-a-service (IaaS)	Platform-as-a-service (PaaS)	Software-as-a-service (SaaS)
People	You	You	You
Data	You	You	You
Applications	You	You	CSP
Operating system	You	CSP	CSP
Virtual networks	You	CSP	CSP
Hypervisors	CSP	CSP	CSP
Servers and storage	CSP	CSP	CSP
Physical networks	CSP	CSP	CSP

9.1.1 Security Development Cycle and Internal Audits
In this section, we featured the Security Development Lifecycle (SDL) best practices. This assists developers in determining security requirements for applications, training, reducing cost, and helps with compliance and reporting needs.

9.1.2 Mandatory Security Training and Background Checks
This falls within the processes for internal Microsoft staff that have been made public to provide information that you may need to provide to your audit teams. It also shows examples of the controls that may need to be put into place at your organization.

9.1.3 Penetration Testing, Intrusions Detection, DDoS, Audits, and Logging
Microsoft has also given examples of audit controls that have been made public for these topics and has provided information on their Threat Protection and Operations websites.

9.1.4 State of the Art Data Centers, Physical Security, and Secure Networks
Azure Data Centers offer high availability infrastructure to protect your data. Along with this comes the tightened physical security controls that have been put in place. There are access points to get on the Microsoft properties, all the way down to the need-to-access data center floor approach. This offers a layered physical security design. Then we talked about some of the high-level offerings when it comes to Network Security, starting with Network Access Control, which limits the connectivity to resources.

9.1.5 Security Incident Response and Shared Responsibility
It is important to develop an Incident Response Plan (IRP) that is consistently tested and updated and controlled. Even if you are not part of an incident response team, it is a good idea to know emergency contacts and how to access the IRP. When it comes to Shared Responsibility, it is important to know your roles as well as the role of the CSP. This is especially true for those that are just adopting a cloud platform.

Back

Back to Main

Helpful Links

- National Institute of Standards and Technology has a vast amount of Cloud an Security resource documentation. Access by clicking on the Nist logo.

NIST

Cloud Computing Security Essentials and Architecture

Managing Risk in the Cloud

What's Special About Cloud Cloud Computing?

- Center for Internet Security offers a wide range of cloud security documentation. You can sign up for a free account that will allow you to gain access to their workbench documentation by clicking on the logo below:

CIS Center for Internet Security®

Next

Back to Main

Azure Career?

If you are just getting started or are in the middle of pursuing a career in Azure, there is an opportunity to learn a vast amount of technology, depending on your interests. Here are a couple of great reference links that outline some of the Azure Career paths that have been provided by Microsoft.

Microsoft Role-Based Certification Roadmap

Microsoft Learn Certifications

Back

Back to Main