# ELC (Estée Lauder Companies) Azure Security Policy Standards & Control Document of

# Azure Security Benchmark v2.1.0

| | | | |
|---|---|---|---|
| **Standard Title** | Azure Security Policies - ELC Azure Security Benchmark v2.1.0 | **Date** | 25th April'23 |
| **Standard Owner** | Abedi Jamshid | **Effective Date** | 11th May'23 |
| **Process** | Security Engineering & Operations | **Next Revision Date** | |
| **Approved by** | Abedi Jamshid | **Role** | ED, Global Head of Security Engineering & Security Operations |

| Version | Date | Name | Reviewed By | Approved By | Comments |
|---|---|---|---|---|---|
| V1.0 | 28th June'23 | Siva Ande | Kannan / Felix | Abedi Jamshid | Initial Release |
| | | | | | |
| | | | | | |

## Azure Security Policy Hardening Standards

# Table Content


1.0 Standard Statement ..... 3

2.0 Purpose and Scope ..... 3

3.0 Standards ..... 3

3.1 Identity and Access Management ..... 3

3.2 Networking ..... 5

3.3 Crypto Key ..... 8

3.4 Storage Accounts ..... 14

3.5 Logging and Monitoring ..... 16

3.6 Virtual Machines ..... 17

3.7 App Service ..... 25

3.8 Azure Kubernetes Service ..... 27

4.0 Compliance and Exceptions ..... 27

5.0 Implementation Plan ..... 28

6.0 Change Request ..... 28

7.0 Test Plan ..... 28

8.0 Appendix ..... 29

## 1.0 Standard Statement

In accordance with the Global Information Security Policy, Cloud Security Azure policy highlights the native cloud policies and hardening with native security benchmarks that Estee Lauder Companies, Inc. (ELC) should maintain and uphold within its Azure environment.

## 2.0 Purpose and Scope

The purpose of this standard is to document the native Azure security policy standards in accordance with the Azure security Benchmarks to ensure ELC Azure resources are protected from misconfigurations, data breaches, lack of visibility, and exposure to public. This standard serves as a general security guideline for expectations and industry best practices.

This standard applies to Estee Lauder Companies Inc. (the "Company"), and its subsidiaries throughout the world (collectively, with the Company, "ELC"). The requirements presented herein must be applied to all systems which support financial reporting or financial data.

## 3.0 Standards

The following standards align with the Azure Security Benchmarks v.2.1.0 and are expected to be maintained and upheld by ELC native cloud environment.

## 3.1 Identity and Access Management

### 3.1.1 Audit Windows machines that do not have the password complexity setting enabled.

**Description:**

Requires that prerequisites are deployed to the policy assignment scope. Machines are non-compliant if Windows machines that do not have the password complexity setting enabled.

**Rationale:**

Azure password complexity is a list of rules in which passwords need to abide by. This is to ensure password protection.

### 3.1.2 Audit Windows machines that do not have the maximum password age set to specified number of days.

**Description:**

Requires that prerequisites be deployed to the policy assignment scope. Machines are non-compliant if Windows machines do not have the maximum password age set to a specified number of days. The default value for maximum password age is 70 days (about 2 and a half months).

**Rationale:**

If a user's password is always changing, it will become significantly harder for an attacker to know what it is. An example is if a user uses the same password for all accounts and one of their personal account passwords were to get compromised. Because this policy requires password change it is more than likely that their company account will be protected.

### 3.1.3 A maximum of 3 owners should be designated for your subscription.

**Description:**

It is recommended to designate up to 3 subscription owners to reduce the potential breach by a compromised owner.

**Rationale:**

The idea of this policy is the less subscription owners the less the risk it is becoming compromised. For example, if there is only one owner there is less room for an attacker to come in through.

### 3.1.4 Subscriptions should have a contact email address for security issues.

**Description:**

To ensure the relevant people in your organization are notified when there is a potential security breach in one of your subscriptions, set a security contact to receive email notifications from the Security Center.

**Rationale:** If there is a security issue, the best way to contact the customer is via email.

**3.1.5 An Azure Active Directory administrator should be provisioned for SQL servers.**

**Description:**

Audit provisioning of an Azure Active Directory administrator for your SQL server to enable Azure AD (Active Directory) authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services.

**Rationale:**

**3.1.6 There should be more than one owner assigned to your subscription.**

**Description:**

It is recommended to designate more than one subscription owner to have administrator access redundancy.

**Rationale:**

Assigning more than one subscription owner can be beneficial to companies because it allows more people to have that role as an owner.

## 3.2 Networking

All traffic should be DENY-ALL by default unless explicitly approved by ECR (Enterprise Cybersecurity and Risk) following the Security Exception process. “Please NSG (Network Security Group) Documentation to understand the Scenarios of the Azure Policies.”

**3.2.1 Non-internet-facing virtual machines should be protected with network security groups**

**Description**:

Protect your non-internet-facing virtual machines from potential threats by restricting access with network security groups (NSG).

**Rationale**:

NSGs (Network Security Group) contain a list of Access Control List (ACL) rules that allow or deny network traffic to your VM (Virtual Machines) from other instances, whether they are on the same subnet. It adds an additional later to the security for the non-internet facing VMs.

### 3.2.2 Subnets should be associated with a Network Security Group

**Description**:

Protect your subnet from potential threats by restricting access to it with a Network Security Group (NSG). NSGs contain a list of Access Control List (ACL) rules that allow or deny network traffic to your subnet.

**Rationale**:

This is used to specify which traffic can come into the subnet. It is good for having full control of the subnet eliminating unwanted traffic and therefore reducing risk for attacks.

### 3.2.3 All network ports should be restricted on network security groups associated to your virtual machine.

**Description**:

Azure Security Center has identified some of your network security groups' inbound rules to be too permissive. Inbound rules should not allow access from 'Any' or 'Internet' ranges. This can potentially enable attackers to target your resources.

**Rationale**:

By not allowing access to these ranges, it eliminates the possibility of attackers targeting your resources. It helps staying ahead of the attackers.

### 3.2.4 Internet-facing virtual machines should be protected with network security groups.

**Description:**

Protect your virtual machines from potential threats by restricting access to them with network security groups (NSG).

**Rationale:**

Anything the internet faces will always pose a threat. By adding strict NSGs it will add to that extra security that is needed. Especially when we have internet facing machines that need that extra care.

### 3.2.5 Public network access on Azure SQL Database should be disabled.

**Description:**

Disabling the public network access property improves security by ensuring your Azure SQL Database can only be accessed from a private endpoint. This configuration denies all logins that match IP (Indirect Procurement) or virtual network-based security system rules.

**Rationale:**

A private endpoint is one that uses an IP that is being used from your virtual network. If the private endpoint IP does not match the one that is being used by your virtual network that means that the user is coming from somewhere. By not allowing this we reduce the risk of security threats.

### 3.2.6 Web Application Firewall (WAF) should be enabled for Application Gateway.

**Description:**

Deploy Azure Web Application Firewall (WAF) in front of public facing web applications for additional inspection of incoming traffic. Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities such as SQL injections, Cross-Site Scripting, local and remote file executions. You can also restrict access to your web applications by countries, IP address ranges, and other http(s) parameters via custom rules.

**Rationale:**

Adding the WAF includes benefits such as updated threat intelligence, and services to help respond to real-time attack. When dealing with public facing web applications this added layer of security is needed.

### 3.2.7 Network Watcher should be enabled.

**Description:**

Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level in, to, and from Azure. Scenario level monitoring enables you to diagnose problems at an end-to-end network level view. It is required to have a network watcher resource group created in every region where a virtual network is present. An alert is enabled if a network watcher resource group is not available in a particular region.

**Rationale:**

Azure Network Watcher allows you to diagnose connectivity problems and capture packet flows to and from virtual machines and network security groups. You should enable Network Watcher because it is required for packet capture and logging. This feature is not enabled by default, you must enable it.

### 3.2.8 Azure Web Application Firewall should be enabled for Azure Front Door entry-points.

**Description**:

Deploy Azure Web Application Firewall (WAF) in front of public facing web applications for additional inspection of incoming traffic. Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities such as SQL injections, Cross-Site Scripting, local and remote file executions. You can also restrict access to your web applications by countries, IP address ranges, and other http(s) parameters via custom rules.

**Rationale:**

Public facing web application come with vulnerability issues and risks. WAF job is to look at traffic and block anything that is suspicious or that could have malware in it.

## 3.3 Crypto Key

### 3.3.1 PostgreSQL servers should use customer-managed keys to encrypt data at rest.

**Description:**

Use customer-managed keys to manage the encryption at rest of your PostgreSQL servers. By default, the data is encrypted at rest with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards. Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management.

**Rationale:**

With customer managed keys, you are responsible for your own data. Because you own the key you are also responsible for the key lifecycle management. There is more flexibility when using a customer-managed key.

### 3.3.2 Enforce SSL connection should be enabled for PostgreSQL database servers.

**Description:**

Azure Database for PostgreSQL supports connecting your Azure Database for PostgreSQL server to client applications using Secure Sockets Layer (SSL). Enforcing SSL connections between your database server and your client applications helps protect against 'man in the middle' attacks by encrypting the data stream between the server and your application. This configuration means that SSL is always enabled for accessing your database server.

**Rationale:**

Having secure connections and reducing the risk of a man-in-the-middle attack will help us further protect the confidentiality of the data.

### 3.3.3 Key Vault secrets should have an expiration date.

**Description:**

Secrets should have a defined expiration date and not be permanent. Secrets that are valid forever provide a potential attacker with more time to compromise them. It is a recommended security practice to set expiration dates on secrets.

**Rationale:**

Making sure key vault secrets have an expiration date had the same concept of resetting a password every couple of months. It is good practice and helps stay ahead of the attacker.

### 3.3.4 SQL servers should use customer-managed keys to encrypt data at rest.

**Description:**

Implementing Transparent Data Encryption (TDE) with your own key provides increased transparency and control over the TDE Protector, increased security with an HSM-backed external service, and promotion of separation of duties. This recommendation applies to organizations with a related compliance requirement.

**Rationale:**

Having secure connections and reducing the risk of a man-in-the-middle attack will help us further protect the confidentiality of the data.

### 3.3.5 Both operating systems and data disks in Azure Kubernetes Service clusters should be encrypted by customer-managed keys.

**Description:**

Encrypting OS and data disks using customer-managed keys provides more control and greater flexibility in key management. This is a common requirement in many regulatory and industry compliance standards.

**Rationale:**

Customer-managed key is how we achieve that flexibility in key management and more control overall.

### 3.3.6 MySQL servers should use customer-managed keys to encrypt data at rest.

**Description:**

Use customer-managed keys to manage the encryption at rest of your MySQL servers. By default, the data is encrypted at rest with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards. Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management.

**Rationale:**

Customer-managed key is how we achieve that flexibility in key management and more control overall.

### 3.3.7 App Service apps should have 'Client Certificates (Incoming client certificates)' enabled.

**Description:**

Client certificates allow for the app to request a certificate for incoming requests. Only clients that have a valid certificate will be able to reach the app.

**Rationale:**

The main idea is that users with a valid certificate will be able to reach the app. There is complete control over who can access it and who isn’t. This adds an extra layer of secure by only allowing whoever is preapproved to access the app.

### 3.3.8 Transparent Data Encryption on SQL databases should be enabled.

**Description:**

Transparent data encryption should be enabled to protect data-at-rest and meet compliance requirements.

**Rationale:**

Transparent data encryption performs real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requesting changes to application.

### 3.3.9 Enforce SSL connection should be enabled for MySQL database servers.

**Description:**

Azure Database for MySQL supports connecting your Azure Database for MySQL server to client applications using Secure Sockets Layer (SSL). Enforcing SSL connections between your database server and your client applications helps protect against 'man in the middle' attacks by encrypting the data stream between the server and your application. This configuration means that SSL is always enabled for accessing your database server.

**Rationale:**

Having secure connections and reducing the risk of a man-in-the-middle attack will help us further protect the confidentiality of the data.

### 3.3.10 Key Vault keys should have an expiration date.

**Description:**

Cryptographic keys should have a defined expiration date and not be permanent. Keys that are valid forever provide a potential attacker with more time to compromise the key. It is a recommended security practice to set expiration dates on cryptographic keys.

**Rationale:**

Making sure key vault secrets have an expiration date had the same concept of resetting a password every couple of months. It is good practice and helps stay ahead of the attacker.

### 3.3.11 Key vaults should have soft delete enabled.

**Description:**

Deleting a key vault without soft delete enabled permanently deletes all secrets, keys, and certificates stored in the key vault. Accidental deletion of a key vault can lead to permanent data loss. Soft delete allows you to recover an accidentally deleted key vault for a configurable retention period.

**Rationale:**

Soft delete is there in case a mistake is made, and something was deleted that wasn't supposed to be. If that information needs back, there is a way to get it. It is failsafe.

### 3.3.12 Role-Based Access Control (RBAC) should be used on Kubernetes Services.

**Description:**

To provide granular filtering on the actions that users can perform, use Role-Based Access Control (RBAC) to manage permissions in Kubernetes Service Clusters and configure relevant authorization policies.

**Rationale:**

Role-Based access allows admin to give appropriate access to different users. Here we see the implementation of least privilege.

### 3.3.13 Managed disks should be double encrypted with both platform-managed and customer-managed keys.

**Description:**

High security sensitive customers who are concerned of the risk associated with any encryption algorithm, implementation, or key being compromised can opt for additional layer of encryption using a different encryption algorithm/mode at the infrastructure layer using platform managed encryption keys. The disk encryption sets are required to use double encryption.

**Rationale:**

Double encryptions adds that extra layer of security when dealing with sensitive information. Also having the customer-managed keys allows that control and safety that is desired.

### 3.3.14 Authentication to Linux machines should require SSH keys.

**Description:**

Although SSH itself provides an encrypted connection, using passwords with SSH still leaves the VM vulnerable to brute-force attacks. The most secure option for authenticating to an Azure Linux virtual machine over SSH is with a public-private key pair, also known as SSH keys.

**Rationale:**

SSH uses a combination of public and private key pairs to secure the authentication process. Because of the need for both, it decreases the chances of an attack, it would be difficult for the attacker to gain both keys.

### 3.3.15 Vulnerability assessment should be enabled on SQL Managed Instance

**Description:**

Audit each SQL Managed Instance which does not have recurring vulnerability assessment scans enabled. Vulnerability assessment can discover, track, and help you remediate potential database vulnerabilities.

**Rationale:**

Vulnerability assessment is a great way to prevent an attack from happening. If there is a vulnerability that can be detected it can be stopped.

### 3.3.16 OS and data disks should be encrypted with a customer-managed key.

**Description:**

Use customer-managed keys to manage the encryption at rest of the contents of your managed disks. By default, the data is encrypted at rest with platform-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards. Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management.

**Rationale:**

Customer-managed keys offer more flexibility to manage access controls. Disk encryption protects the data on your device if it is lost or stolen.

## 3.4 Storage Accounts

### 3.4.1 Storage accounts should use customer-managed key for encryption.

**Description:**

Secure your blob and file storage account with greater flexibility using customer-managed keys. When you specify a customer-managed key, that key is used to protect and control access to the key that encrypts your data. Using customer-managed keys provides additional capabilities to control rotation of the key encryption key or cryptographically erase data.

**Rationale:**

Storage accounts are automatically encrypted with Microsoft-managed keys. Using a customer-managed key will add more flexibility.

### 3.4.2 Storage accounts should have infrastructure encryption.

**Description:**

Enable infrastructure encryption for higher level of assurance that the data is secure. When infrastructure encryption is enabled, data in a storage account is encrypted twice.

**Rationale:**

Double encryption of Azure Storage data protects against a scenario where one of the encryption algorithms or keys may be compromised. In this scenario, the additional layer of encryption continues to protect your data.

### 3.4.3 Storage accounts should restrict network access using virtual network rules.

**Description:**

Protect your storage accounts from potential threats using virtual network rules as a preferred method instead of IP-based filtering. Disabling IP-based filtering prevents public IPs from accessing your storage accounts.

**Rationale:**

It adds a new layer of security since storage accounts accept connections from clients on any network. To limit access to selected networks, the default actions must be changed.

### 3.4.4 Storage account public access should be disallowed.

**Description:**

Anonymous public access to containers and blobs in Azure Storage is a convenient way to share data but might present security risks. To prevent data breaches caused by undesired anonymous access, Microsoft recommends preventing public access to a storage account unless your scenario requires it.

**Rationale:**

Public access will always present itself with security issues. When you configure a container's public access level setting to permit anonymous access, clients can read data in that container without authorizing the request. This would allow unauthorized people to obtain data that they should not be allowed to.

### 3.4.5 Storage accounts should restrict network access.

**Description:**

Network access to storage accounts should be restricted. Configure network rules so only applications from allowed networks can access the storage account. To allow connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges.

**Rationale:**

Keeping network access to storage accounts restricted adds an additional layer of security by implementing the least privilege. It reduces the risk of data getting leaked but unauthorized users.

### 3.4.6 Secure transfer to storage accounts should be enabled.

**Description:**

Audit requirement of Secure transfer in your storage account. Secure transfer is an option that forces your storage account to accept requests only from secure connections (HTTPS). Use of HTTPS ensures authentication between the server and the service and protects data in transit from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking.

**Rationale:**

Enhances the security if a storage account by making sure the connection is secure. If not, it can be susceptible to attacks such as man-in-the-middle, phishing, and ransomware.

### 3.4.7 SQL servers with auditing to storage account destination should be configured with 90 days (about 3 months) retention or higher.

**Description:**

For incident investigation purposes, we recommend setting the data retention for your SQL Server' auditing to storage account destination to at least 90 days (about 3 months). Confirm that you are meeting the necessary retention rules for the regions in which you are operating. This is sometimes required for compliance with regulatory standards.

**Rationale:**

90 days (about 3 months) or higher allows Audit Logs to be used to check for anomalies and give insight into suspected breaches or misuse of information and access.

## 3.5 Logging and Monitoring

### 3.5.1 Log Analytics agent should be installed on your virtual machine for Azure Security Center monitoring.

**Description:**

This policy audits any Windows/Linux virtual machines (VMs) if the Log Analytics agent is not installed which Security Center uses to monitor for security vulnerabilities and threats.

**Rationale:**

### 3.5.2 Resource logs in IoT (Internet of Things) Hub should be enabled.

**Description:**

Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised.

**Rationale:**

If a security accident does happen one of the first steps to follow Is an investigation. In the process they usually backtrack the event and audit enabling of reassure log allows us to do this successfully.

## 3.6 Virtual Machines

### 3.6.1 Log Analytics agent should be installed on your virtual machine scale sets for Azure Security Center monitoring.

**Description:**

Security Center collects data from your Azure virtual machines (VMs) to monitor for security vulnerabilities and threats.

**Rationale:**

The log analytics agent sends data to a Log Analytics workspace and supports monitoring solutions. This is helpful because if there are vulnerabilities or threats detected it will Virtual Machines.

### 3.6.2 Audit virtual machines without disaster recovery configured.

**Description:**

Audit virtual machines which do not have disaster recovery configured.

**Rationale:**

Disaster recovery allows organizations to automatically restore server is if anything were to happen, from malicious attacks to accidental deletion.

### 3.6.3 Windows web servers should be configured to use secure communication protocols.

**Description:**

To protect the privacy of information communicated over the Internet, your web servers should use the latest version of the industry-standard cryptographic protocol, Transport Layer Security (TLS). TLS secures communications over a network by using security certificates to encrypt a connection between machines.

**Rationale:**

Having a secure communication protocol guarantees that sensitive information is not being accessed by an unauthorized third-party. Inherently protecting confidential information.

### 3.6.4 Windows Defender Exploit Guard should be enabled on your machines.

**Description:**

Windows Defender Exploit Guard uses the Azure Policy Guest Configuration agent. Exploit Guard has four components that are designed to lock down devices against a wide variety of attack vectors and block behaviors commonly used in malware attacks while enabling enterprises to balance their security risk and productivity requirements (Windows only).

**Rationale:**

Windows Defender Exploit guard is an antimalware that provides intrusion protection. It is a part of windows defender security center and can protect machines against several types of attacks.

### 3.6.5 Windows machines should meet the requirements of the Azure compute security baseline.

**Description:**

Requires that prerequisites be deployed to the policy assignment scope. Machines are non-compliant if the machine is not configured correctly for one of the recommendations in the Azure compute security baseline.

**Rationale:**

Azure security baseline are standardized documents the describe the available security capabilities and the security configurations that will help strengthen the security of the company. Making sure that the windows machines match this will help eliminate risk and vulnerabilities.

### 3.6.6 Audit Windows machines that do not have the specified Windows PowerShell modules installed.

**Description:**

Requires that prerequisites are deployed to the policy assignment scope. Machines are non-compliant if a module isn't available in a location specified by the environment variable PSModulePath.

**Rationale:**

### 3.6.7 Audit Windows machines that allow re-use of the passwords after the specified number of unique passwords.

**Description:**

Requires that prerequisites be deployed to the policy assignment scope. Machines are non-compliant if Windows machines allow re-use of the passwords after the specified number of unique passwords. The default value for unique passwords is 24.

**Rationale:**

Determines the number of unique passwords that are associated to one user account before an old password can be reused. This discourages the re-use of a password once used before and prevents users from switching between several common passwords.

### 3.6.8 Audit Windows machines that do not restrict the minimum password length to specified number of characters.

**Description:**

Requires that prerequisites are deployed to the policy assignment scope. Machines are non-compliant if Windows machines that do not restrict the minimum password length to specified number of characters. The default value for minimum password length is 14 characters.

**Rationale:**

Having a 14-character password is highly unlikely for someone to crack. This makes sure that the users associated with the company have passwords that protect their data, and it makes it difficult for the person who want to crack it.

### 3.6.9 Audit Windows machines that do not store passwords using reversible encryption.

**Description:**

Requires that prerequisites be deployed to the policy assignment scope. Machines are non-compliant if Windows machines that do not store passwords using reversible encryption.

**Rationale:**

This provides support for applications that store user passwords for authentication. If we were to store encrypted passwords in a way that would be reversible then all the passwords would be able to be decrypted. Therefore, we do not want this to be enabled.

### 3.6.10 System updates should be installed on your machines.

**Description:**

Missing security system updates on your servers will be monitored by Azure Security Center as recommendations.

**Rationale:**

Keeping systems updated will have benefits such as new security fixes, greater compatibility, and enhanced features. If systems are not kept up-to-date and fall behind, they will not be up to the company standards.

### 3.6.11 Audit Linux machines that have accounts without passwords.

**Description:**

Requires that prerequisites be deployed to the policy assignment scope. Machines are non-compliant if Linux machines that have accounts without passwords.

**Rationale:**

Not having a password increases security risk tremendously. The account could become compromised and put the companies' data at risk.

### 3.6.12 Audit Linux machines that do not have the passwd file permissions set to 0644.

**Description:**

Requires that prerequisites be deployed to the policy assignment scope. Machines are non-compliant if Linux machines that do not have the passwd file permissions set to 0644.

**Rationale:**

When permissions are set to 0644 it means that they will be readable by all user groups, but writeable by the user only. This makes sure that no one alters the data who is not supposed to, protecting the integrity of the data.

### 3.6.13 Audit Linux machines that allow remote connections from accounts without passwords.

**Description:**

Requires that prerequisites be deployed to the policy assignment scope. Machines are non-compliant if Linux machines that allow remote connections from accounts without passwords.

**Rationale:**

Accounts need to have passwords. When they do not that is when the confidentiality, integrity and authentication of the data is put at risk.

### 3.6.14 Linux machines should meet requirements for the Azure compute security baseline.

**Description:**

Requires that prerequisites be deployed to the policy assignment scope. Machines are non-compliant if the machine is not configured correctly for one of the recommendations in the Azure compute security baseline.

**Rationale:**

The security baseline are standardized documents for Azure products that describe the availability of security capabilities and security configurations with an end goal of strengthening security. Linux machines need to meet these requirements because it will ensure they are kept to the Azure standard.

**3.6.15 Adaptive application controls for defining safe applications should be enabled on your machines.**

**Description:**

Enable application controls to define the list of known-safe applications running on your machines, and alert you when other applications run. This helps protect your machines against malware. To simplify the process of configuring and maintaining your rules, Security Center uses machine learning to analyze the applications running on each machine and suggest the list of known-safe applications.

**Rationale**

Application control is implemented on all servers to restrict the execution of executables, software libraries, scripts, and installers to an approved set.

**3.6.16 System updates should be installed on your machines (powered by Update Center)**

**Description:**

Your machines are missing system, security, and critical updates. Software updates often include critical patches to security holes. Such holes are frequently exploited in malware attacks, so it is vital to keep your software updated. To install all outstanding patches and secure your machines, follow the remediation steps.

**Rationale:**

System updates are important because they contain the necessary information that is needed to keep the machines safe from newer malware.

**3.6.17 Vulnerability assessment should be enabled on your SQL servers.**

**Description:**

Audit Azure SQL servers which do not have vulnerability assessment properly configured. Vulnerability assessment can discover, track, and help you remediate potential database vulnerabilities.

**Rationale:**

SQL vulnerability assessment (VA) is a service that provides visibility into your security state and includes actionable steps to resolve security issues and enhance your database security. By staying ahead and detecting vulnerabilities early, it can reduce the risk of malware getting through.

**3.6.18 Endpoint protection solution should be installed on virtual machine scale sets.**

**Description:**

Audit the existence and health of an endpoint protection solution on your virtual machines scale sets, to protect them from threats and vulnerabilities.

**Rationale:**

System updates are important because they contain the necessary information that is needed to keep the machines safe from newer malware.

**3.6.19 System updates on virtual machine scale sets should be installed.**

**Description:**

Audit whether there are any missing system security updates and critical updates that should be installed to ensure that your Windows and Linux virtual machine scale sets are secure.

**Rationale:**

System updates are important because they contain the necessary information that is needed to keep the machines safe from newer malware.

**3.6.20 Virtual machines should be migrated to new Azure Resource Manager resources.**

**Description:**

Use new Azure info Resource Manager for your virtual machines to provide security enhancements such as: stronger access control (RBAC), better auditing, Azure Resource Manager based deployment and governance, access to managed identities, access to key vault for secrets, Azure AD-based authentication and support for tags and resource groups for easier security management.

**Rationale:**

Azure resource manager provides a management layer that enables you to create, update, and delete resources in your account. Making sure that VMs are migrated to new azure manage resources will also make it a little easier to organize security management.

### 3.6.21 VM Image Builder templates should use private link.

**Description:**

Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your VM Image Builder building resources, data leakage risks are reduced.

**Rationale:**

Having a secure connection between customers and services over the Azure backbone network is important because there can be security threats that can take data when it is transferred. Having a secure connection reduces this risk.

### 3.6.22 A vulnerability assessment solution should be enabled on your virtual machines.

**Description:**

Audits virtual machines to detect whether they are running a supported vulnerability assessment solution. A core component of every cyber risk and security program is the identification and analysis of vulnerabilities. Azure Security Center's standard pricing tier includes vulnerability scanning for your virtual machines at no extra cost. Additionally, the Security Center can automatically deploy this tool for you.

**Rationale:**

Vulnerability assessment solution on Azure will inform us of any security misconfigurations, report on vulnerabilities found in the OS and the application layer. It does this by continuously monitoring the VM servers. It will also offer solutions to these issues. It is important for us to implement this rule to stay ahead of these issues and not let them grow.

## 3.7 App Service

### 3.7.1 App Service apps should only be accessible over HTTPS.

**Description:**

Use of HTTPS ensures server/service authentication and protects data in transit from network layer eavesdropping attacks.

**Rationale:**

When using HTTPS, it protects sensitive data from attacks such as eavesdropping. In such an attack, it is hard to know the attacker is listing before it is too late. So, it is important to implement such rules that protect our data.

### 3.7.2 App Service apps should use managed identity.

**Description:**

Use a managed identity for enhanced authentication security.

**Rationale:**

A managed identity from Azure Active Directory (Azure AD) allows your app to easily access other Azure AD-protected resources such as Azure Key Vault. This ensures that only the user allowed to access that information's is supposed to.

### 3.7.3 Infrastructure encryption should be enabled for Azure Database for PostgreSQL servers.

**Description:**

Enable infrastructure encryption for Azure Database for PostgreSQL servers to have higher level of assurance that the data is secure. When infrastructure encryption is enabled, the data at rest is encrypted twice using FIPS 140-2 compliant Microsoft managed keys.

**Rationale:**

Azure Database for PostgreSQL uses storage encryption of data at-rest for data using Microsoft's managed keys. Data, including backups, are encrypted on disk and this encryption is always on and cannot be disabled. The encryption uses FIPS 140-2 validated cryptographic module and an AES 256-bit cipher for the Azure storage encryption. Infrastructure double encryption adds a second layer of encryption using service-managed keys. It uses FIPS 140-2 validated cryptographic module, but with a different encryption algorithm. This provides an additional layer of protection for your data at rest.

### 3.7.4 App Service apps should have remote debugging turned off.

**Description:**

Remote debugging requires inbound ports to be opened on an App Service app. Remote debugging should be turned off.

**Rationale:**

Because it needs inbound ports to be opened, it can lead to extra traffic flow which outs more risk for malware to enter. Therefore, remote bugging should be turned off.

### 3.7.5 Function apps should have remote debugging turned off.

**Description:**

Remote debugging requires inbound ports to be opened on Function apps. Remote debugging should be turned off.

**Rationale:**

Because it needs inbound ports to be opened, it can lead to extra traffic flow which outs more risk for malware to enter. Therefore, remote bugging should be turned off.

### 3.7.6 SQL managed instances should use customer-managed keys to encrypt data at rest.

**Description:**

Implementing Transparent Data Encryption (TDE) with your own key provides you with increased transparency and control over the TDE Protector, increased security with an HSM-backed external service, and promotion of separation of duties. This recommendation applies to organizations with a related compliance requirement.

**Rationale:**

With customer managed keys, you are responsible for your own data. Because you own the key you are also responsible for the key lifecycle management. There is more flexibility when using a customer-managed key.

## 3.8 Azure Kubernetes Service

**Azure Container Instance container group should use customer-managed key for encryption.**

**Description:**

Secure your containers with greater flexibility using customer-managed keys. When you specify a customer-managed key, that key is used to protect and control access to the key that encrypts your data. Using customer-managed keys provides additional capabilities to control rotation of the key encryption key or cryptographically erase data.

**Rationale:**

In this case it makes sense to use customer-managed keys for encryption. The responsibility is with the customer who is wanted.

**Kubernetes clusters should not allow container privilege escalation.**

**Description:**

Do not allow containers to run with privilege escalation to root in a Kubernetes cluster. This recommendation is part of CIS 5.2.5 which is intended to improve the security of your Kubernetes environments. This policy is available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes.

**Rationale:**

This is for the overall improvement for security of the Kubernetes. It keeps the data in the containers, in their respective containers.

## 4.0 Compliance and Exceptions

Compliance with this standard is mandatory and will be enforced and executed by the Security Engineering & Operation – Cloud Security Team. Non-compliance with this Procedure may result in disciplinary action including dismissal.

Any exceptions to the standards need to be reviewed, assessed, and approved by Global Head, Security Engineering & Operations. All exception requests must be submitted for approval to ECR via a ServiceNow ticket. Exception requests will be reviewed on a case-by-case basis and are subject to the approval of the standard owner.

## 5.0 Implementation Plan

Cloud Security Team will plan this Azure Security policies implementation across all the Azure Management groups in co-ordinations with other team.

## 6.0 Change Request

The Cloud Security Team will follow the ELC IT (Information Technology) Security process and raise the Change Request which is required for the implementation.

## 7.0 Test Plan

Cloud Security Team will plan the test case as per the IT security guidelines and implement the Azure policies on the POC environments before implement on the prod environments, it will deploy in Audit mode during the initial phase and slowly enforce to the deploy mode.

## 8.0 Appendix

| Abbreviation | Description |
|---|---|
| Poc | Testing Environment |
| AKS | Azure Kubernetes Service |
| SSH | Secure Shell Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
| SNOW (Service Now) | ServiceNow |
| SQL | Sequel Query Language |
| VNET | Virtual Networks |
| Azure ARC | Azure Architecture |
| Azure AD | Azure Active Directory |
| DR | Disaster Recovery |
| DC | Data Centre |

## 8.1 External Documents for Reference

- Azure Security Benchmark V3
- CIS Controls (v7)
- NIST Cyber Security Framework (v1.1)
- NIST SP 800-57 Pt. 1 Suggested crypto periods for key types
- Azure_Security_Benchmark_V3
- https://elcompanies.sharepoint.com/:f:/s/CloudSecurity/EijeYgvn7QJMroSKfXcXaSUBX8h5fditQG2ZMtJHPpNSzQ?e=wwhdsH