

# Top 20 Microsoft Azure Vulnerabilities and Misconfigurations

---

 [infosecmatter.com/top-20-microsoft-azure-vulnerabilities-and-misconfigurations](https://infosecmatter.com/top-20-microsoft-azure-vulnerabilities-and-misconfigurations)

August 30, 2020

In this article, we will look on the top 20 vulnerabilities and misconfigurations of the Microsoft Azure cloud that are commonly found during credentialed security audits and architecture reviews.

Information in this post can hopefully aid security architects, auditors and other professionals in assessment of the security posture of a given Azure cloud environment.

## Introduction

---

Many organizations today have adopted cloud technologies such as Microsoft Azure or Amazon Web Services (AWS) to simplify and outsource the management of their IT infrastructure.

But as any other cloud technology, Microsoft Azure is a complex topic. To set it up securely requires a significant effort, knowledge of multiple technological areas, and also understanding of the Azure ecosystem.

Azure cloud environment initially comes pre-configured with basic features, minimum hardening and benevolent security settings, to simply work out-of-the-box.

Without putting extra effort into securing it, organizations can easily become vulnerable and prone to cyber attacks aimed against their cloud infrastructures.

## Top 20 Microsoft Azure vulnerabilities

---

The following section contains list of top 20 vulnerabilities and misconfigurations that are commonly found during credentialed security audits and configuration reviews of Microsoft Azure cloud environments.

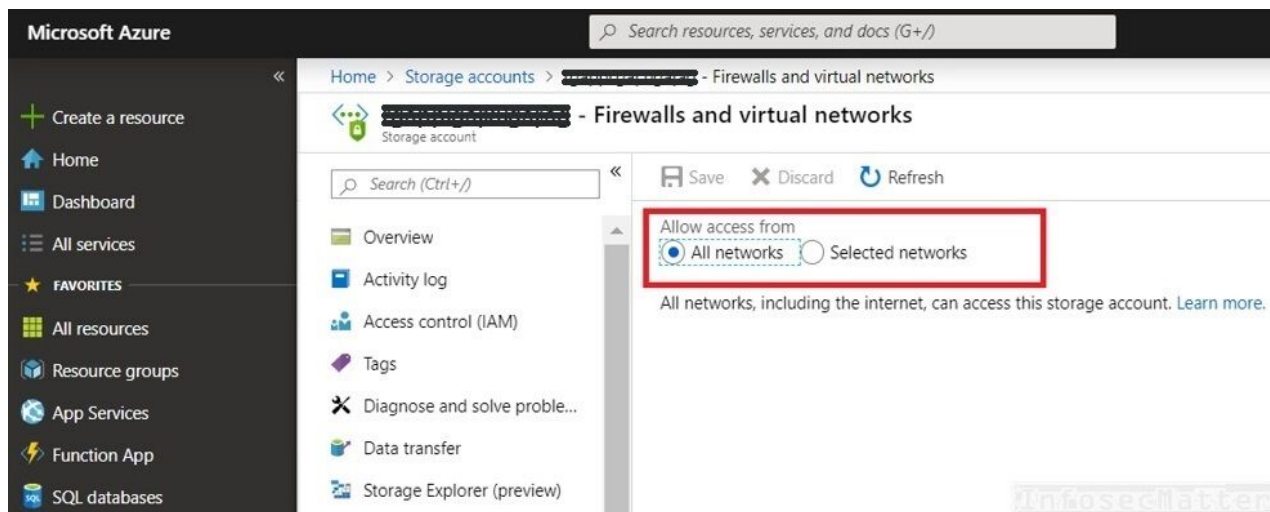
Credentialed means that the auditors had access to the Microsoft Azure administration console ([Azure Portal](#)), which was granted by the customers.

Note that the list is organized in a random manner – it is therefore more like a checklist rather than an ordered ranking list.

Let's get to it!

### 1. Storage accounts accessible from Internet

---

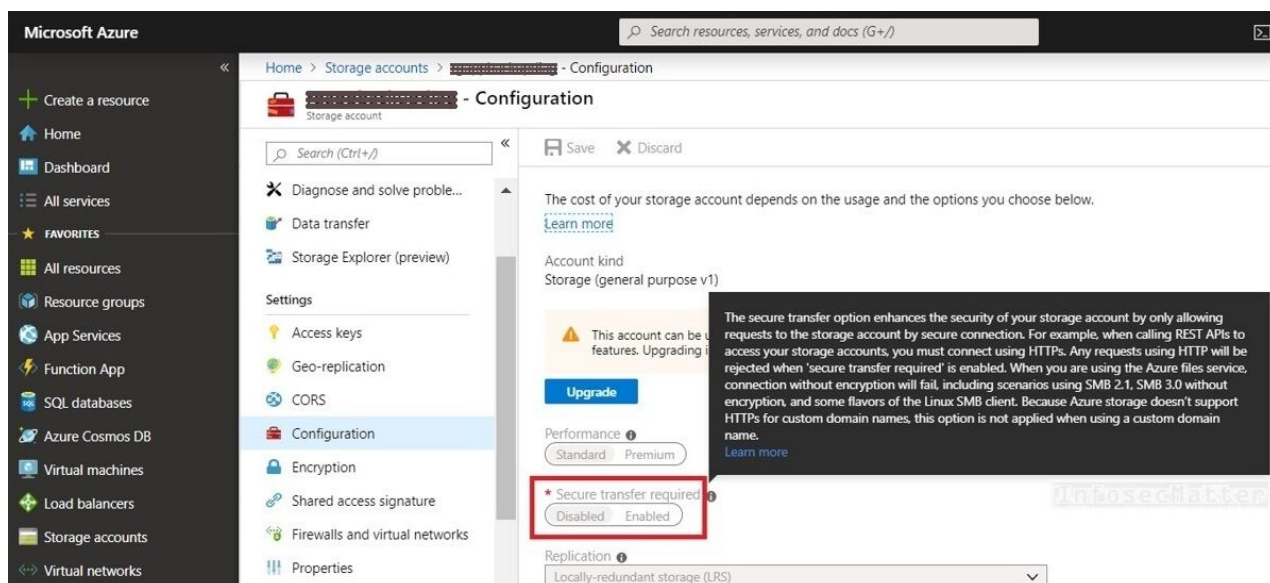


The default setting of Azure storage accounts is to allow access from anywhere, including the Internet. Such settings naturally presents a risk of potential unauthorized access to data, data leakage, exfiltration etc.

It is always prudent to adopt the principle of least privilege and limit access to each storage account only from selected IP addresses, network ranges or VNet (Azure Virtual Network) subnets.

More information on this topic can be found [here](#).

## 2. Storage accounts with insecure transfer allowed



This settings enables enforcement of secure (encrypted) data transfers towards the storages. This means that any requests via insecure protocols such as HTTP or SMB without encryption will be rejected.

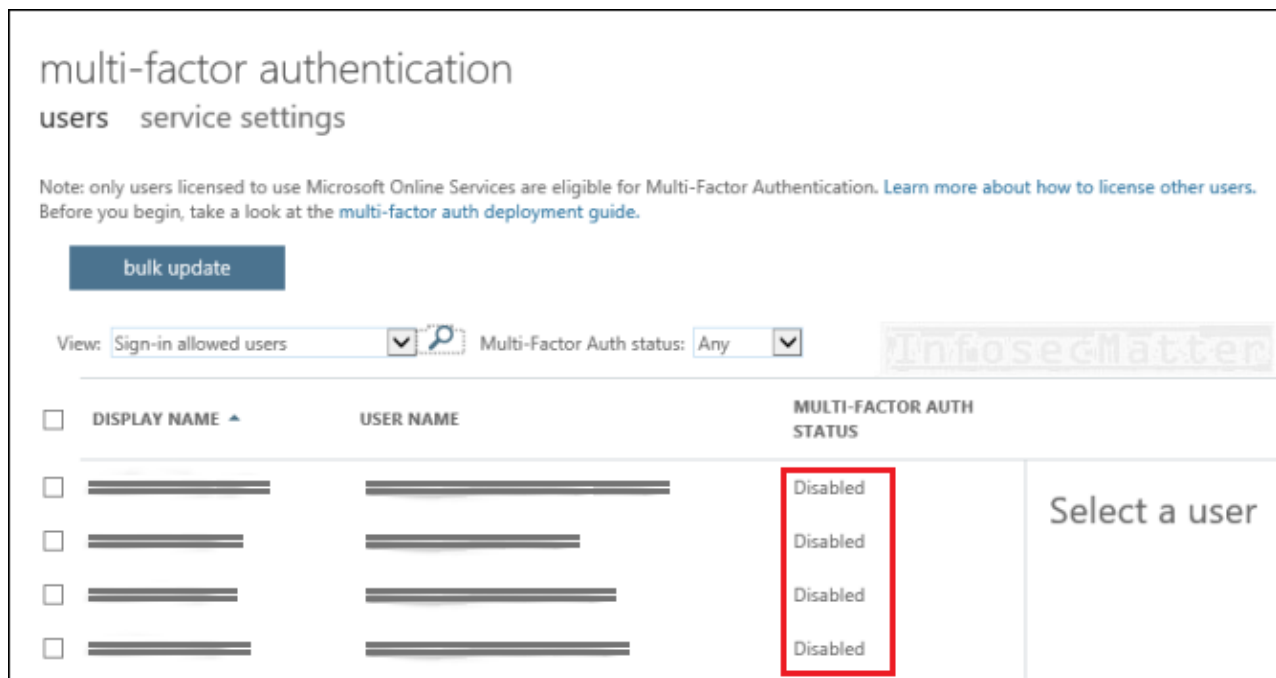
The default settings is to accept any protocol, which unavoidably opens up the cloud storages to the eavesdropping attacks. A well positioned attacker could potentially eavesdrop on the communication and gain access to sensitive or private information passing by.

Needless to say, secure data transfers should be enabled for all storage accounts.

More information about secure data transfers in Azure can be found [here](#).

### 3. Lack of multi-factor authentication for privileged users

---



Multi-factor authentication (MFA) should be required for any user who has administrative or write privileges to any Azure resources. This includes roles such as:

- Administrators
- Service co-administrators
- Subscription owners
- Contributors

Protecting these high-privileged accounts with MFA is extremely important, since they are of a high risk of being targeted by adversaries.

With MFA enabled, an attacker would have to compromise at least 2 different authentication mechanisms belonging to the user, which reduces the risk significantly.

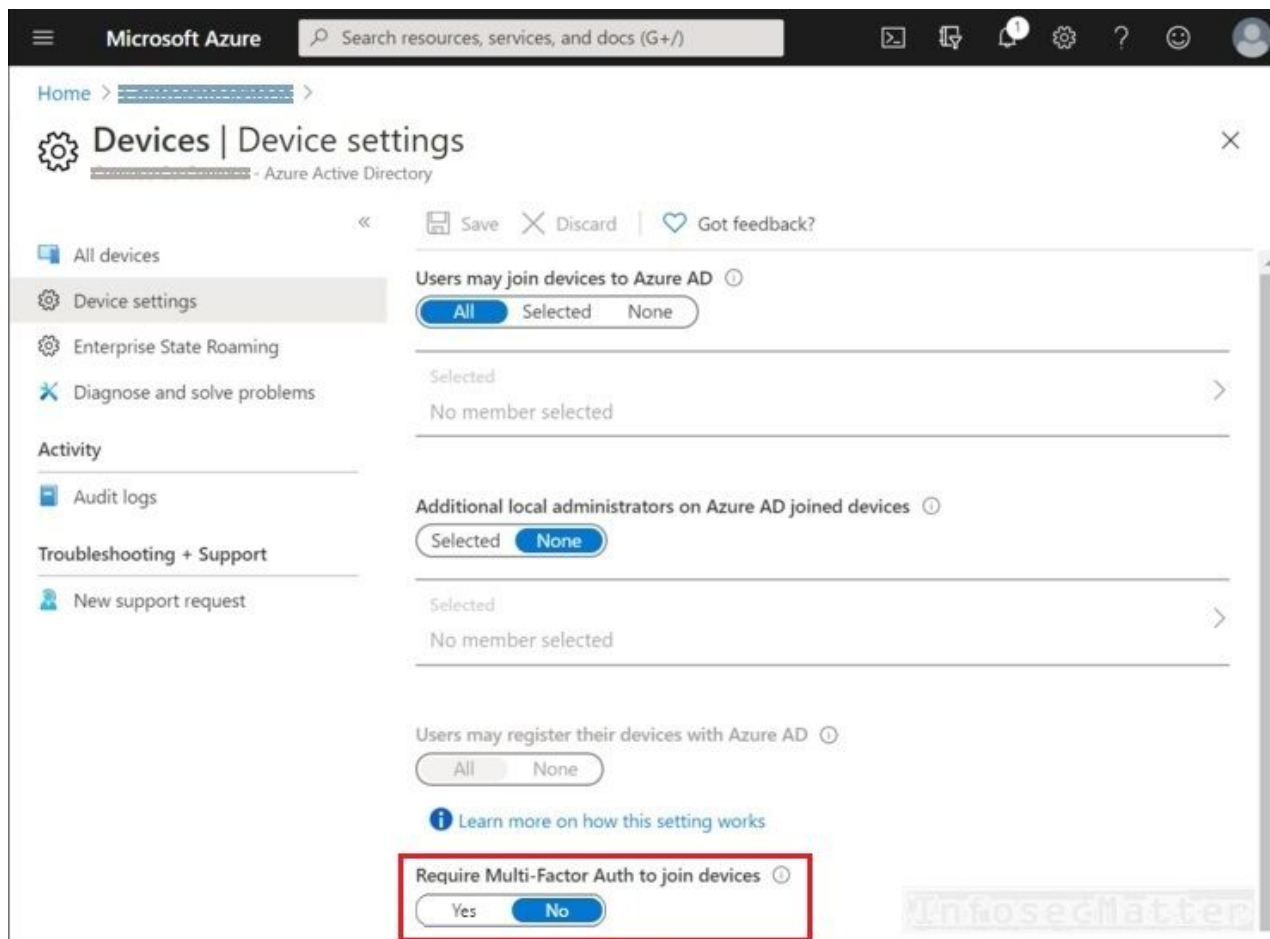
Note that Microsoft Azure supports whole variety of MFA solutions and options, some of them free, some of them on subscription basis as per premium plans, e.g.:

- Azure Multi-Factor Authentication
- Conditional Access Policies

In any case, some sort of MFA should be enforced for all administrative users, at minimum.

### 4. Lack of multi-factor authentication to join devices

---



All users should be required to provide second method of authentication before they can join a device to the Active Directory.

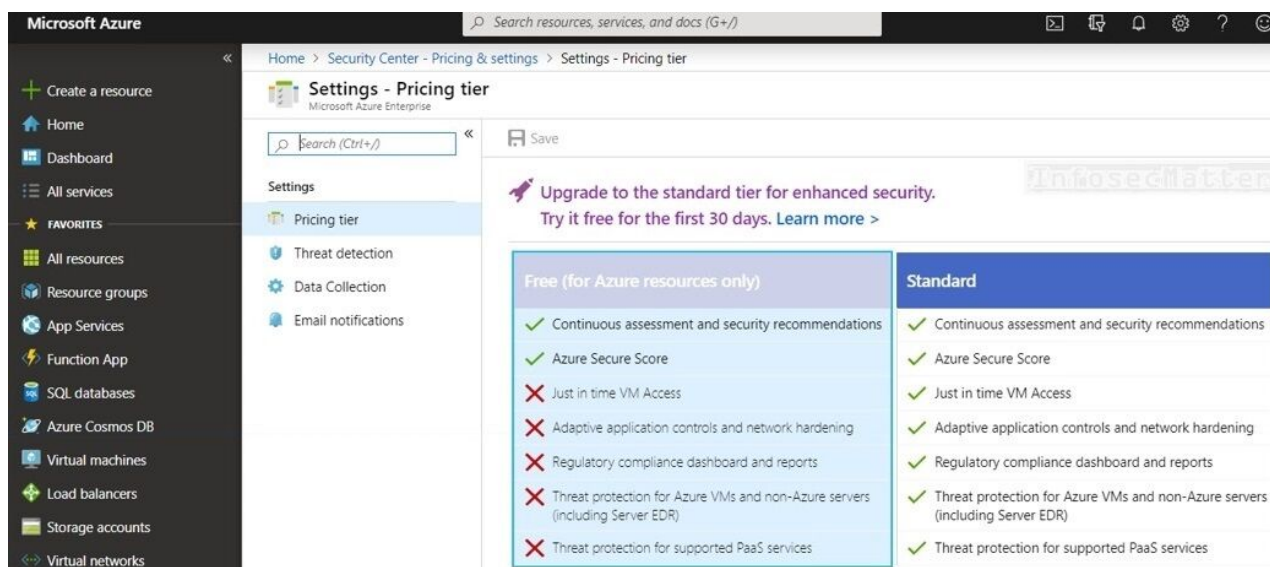
This is to ensure that there are no rogue devices added to the directory by using credentials of a compromised user account.

The risk is that an attacker could join an unmanaged, non-compliant and potentially malicious device into the organization which could then access apps and other resources of the organization.

More information about device management can be found [here](#).

## 5. Azure Security Center with Basic pricing tier

---



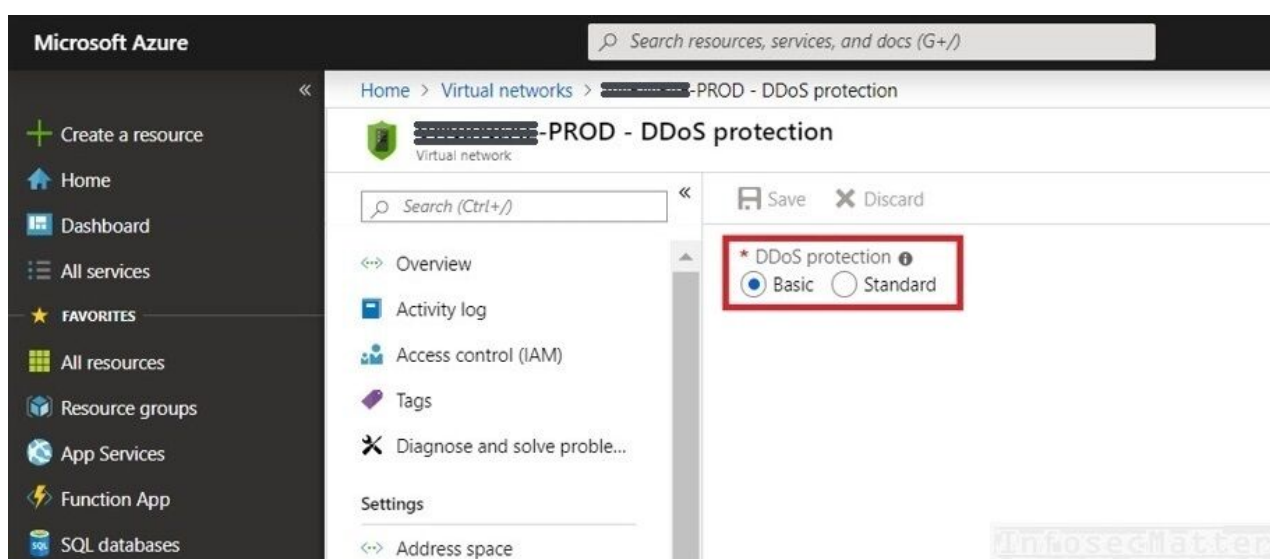
The enhanced Standard pricing tier in Azure Security Center has the following supplementary security features in comparison with the Free (Basic) tier:

- Threat detection and threat intelligence feeds
- Anomaly detection, behavior analysis and security alerts
- Machine learning with potential to identify novel attacks and zero-day exploits
- Vulnerability scanning and vulnerability management of the entire infrastructure
- Advanced access and application controls to block malware and other network attacks

This can certainly help in defense from some cyber attacks and despite the increased costs, it is something that should be enabled in every production environment.

More details about the Security Center pricing and all the security features can be found [here](#).

## 6. Azure Virtual networks with Basic DDoS protection



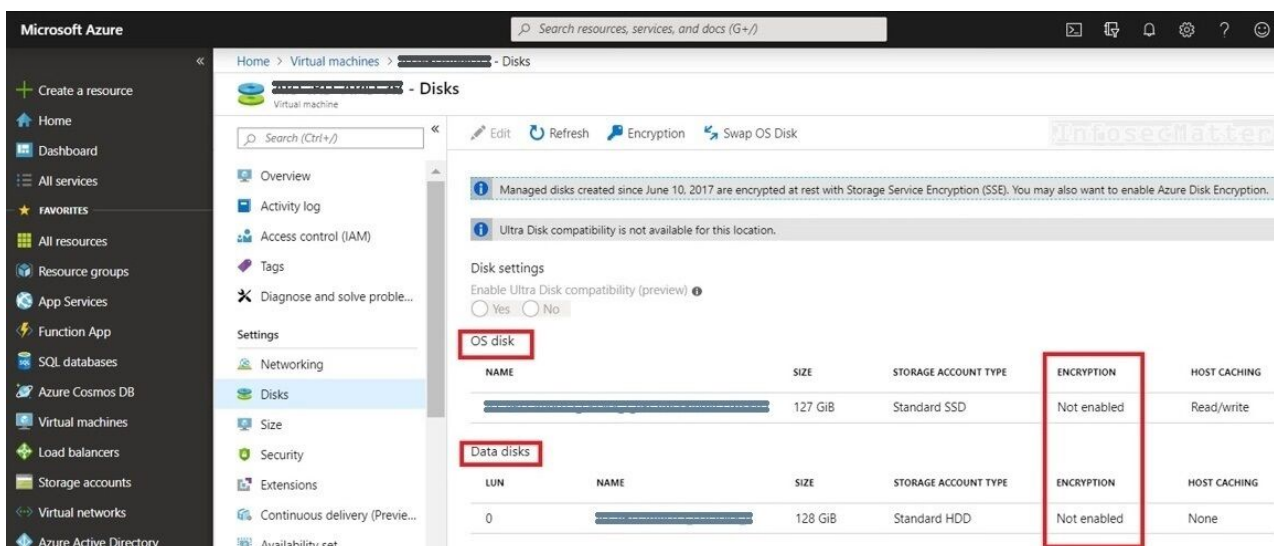
The enhanced Standard DDoS (Distributed Denial of Service) protection provides the following additional defenses when compared with the Basic DDoS protection:

- Near real-time telemetry and traffic monitoring
- Ongoing attack alerts and notifications
- Adaptive tuning and traffic profiling
- Detailed attack analysis

Again, this is something that can certainly help in defending from network based DDoS attacks. The Standard DDoS should be enabled on all important VNets in every production environment.

The only downside is that this is a premium feature and thus with additional costs. Pricing details on the Azure DDoS protection can be found [here](#).

## 7. Unencrypted OS and Data disks



The screenshot shows the Azure portal interface for a virtual machine's disks. The left sidebar contains navigation options like 'Create a resource', 'Home', 'Dashboard', and 'All services'. The main area is titled 'Disks' and includes a search bar and buttons for 'Edit', 'Refresh', 'Encryption', and 'Swap OS Disk'. A message states: 'Managed disks created since June 10, 2017 are encrypted at rest with Storage Service Encryption (SSE). You may also want to enable Azure Disk Encryption.' Another message says: 'Ultra Disk compatibility is not available for this location.' Below these, there are 'Disk settings' with a toggle for 'Enable Ultra Disk compatibility (preview)' set to 'No'. The 'OS disk' section is highlighted with a red box. Below it, a table lists disks with columns: NAME, SIZE, STORAGE ACCOUNT TYPE, ENCRYPTION, and HOST CACHING. The 'Data disks' section is also highlighted with a red box. The 'Encryption' column in the table is highlighted with a red box, showing 'Not enabled' for both the OS and data disks.

NAME	SIZE	STORAGE ACCOUNT TYPE	ENCRYPTION	HOST CACHING	
OS disk	127 GiB	Standard SSD	Not enabled	Read/write	
LUN	NAME	SIZE	STORAGE ACCOUNT TYPE	ENCRYPTION	HOST CACHING
0	Data disk	128 GiB	Standard HDD	Not enabled	None

Needless to say, disk encryption should be a standard in every production environment, on workstations, servers and in the cloud as well.

In the cloud world, this is sometimes referred to as “encryption at rest” and Azure supports disk encryption for both Windows and Linux VMs:

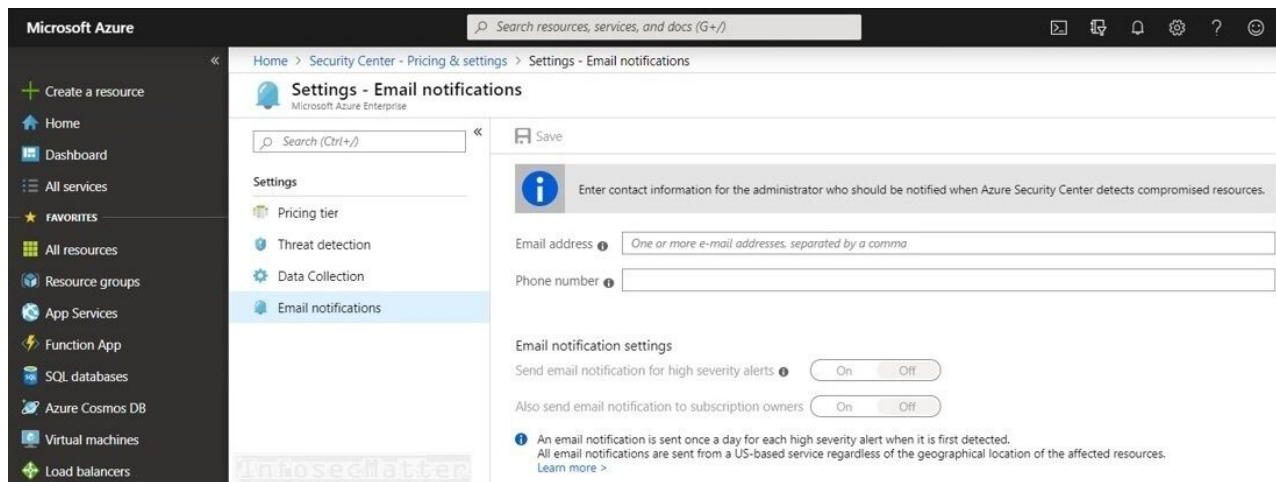
- On Windows it uses BitLocker
- On Linux it uses DM-Crypt

As stated in the [documentation](#), the disk encryption should not impact the performance and there are no additional costs to it, so there is really no excuse to not have encryption enabled for all the disks, that includes:

- OS disks
- Data disks
- Unattached disks



## 8. Email notifications missing in Security Center

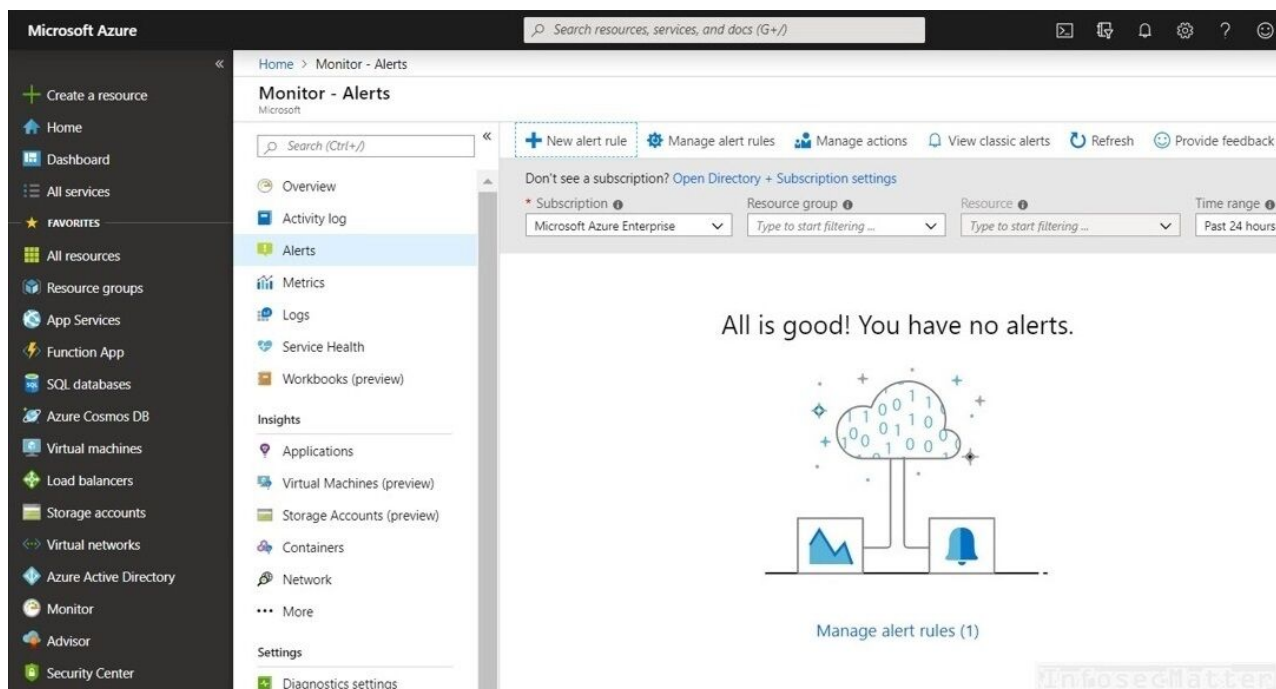


Running a production environment on Azure cloud without configuring email notifications in the Azure Security Center is a major mishap.

The Azure Security Center should be always configured with an email address and/or a phone number, in order to receive notifications about incidents, e.g. when a particular resource gets compromised.

This is something that should be configured in every environment and always monitored with a very high priority.

## 9. Log alerts missing in Azure Monitor



Azure monitoring and alerting allows to create custom alerts tailored to the specific needs of the services deployed in the Azure cloud.

If this is properly configured with relevant alerting conditions, it can provide early indications of issues in the environment, rather than relying on the built-in Azure security features.

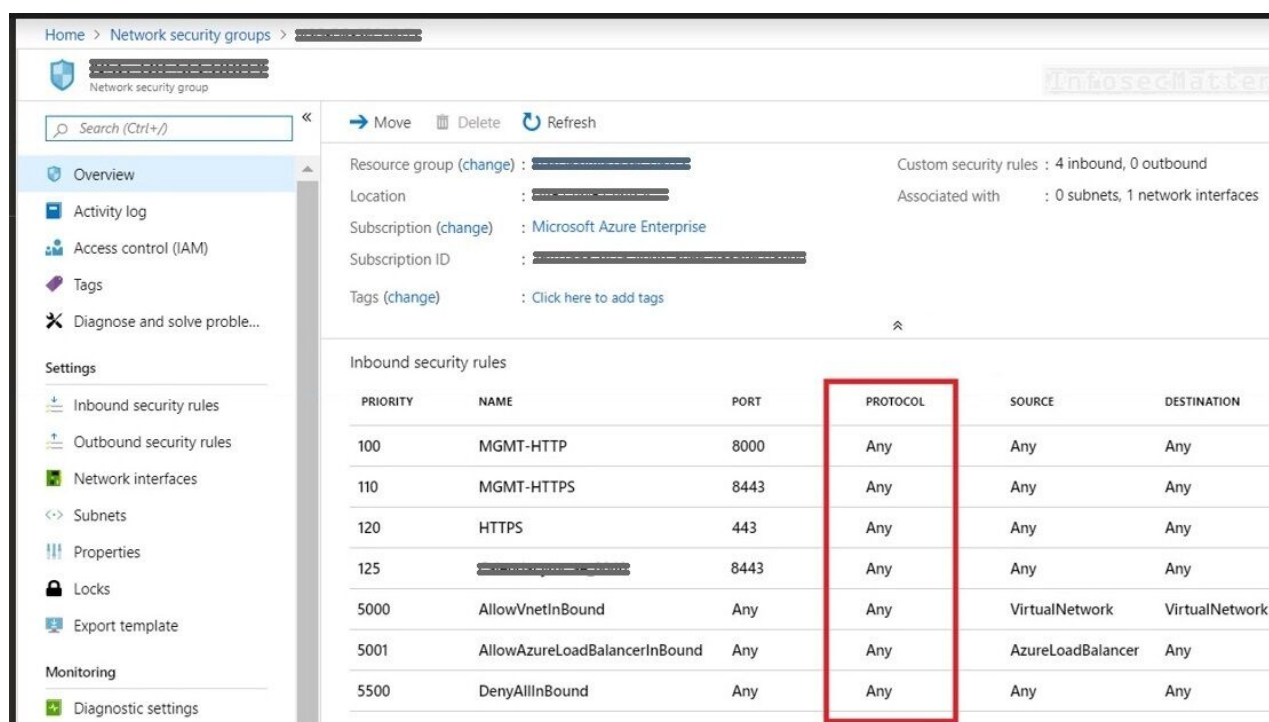
In Azure architecture reviews, It is therefore always expected to see a well-defined list of custom alerts relevant to the environment.

Here's a sample list of what we can alert on using the Azure monitoring alerts:

- Metric values
- Log search queries
- Activity log events
- Health of the underlying Azure platform
- Tests for website availability

More information on the Azure monitoring and alerting can be found [here](#).

## 10. Azure NSG inbound rules configured with ANY



The screenshot displays the Azure portal interface for a Network Security Group (NSG). The left sidebar shows the navigation menu with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problem..., Settings, and Monitoring. The main content area shows the NSG configuration, including Resource group, Location, Subscription, and Subscription ID. Below this, the 'Inbound security rules' table is visible. The table has columns for PRIORITY, NAME, PORT, PROTOCOL, SOURCE, and DESTINATION. The 'PROTOCOL' column is highlighted with a red box, showing that several rules are configured with 'Any' as the protocol, which is a common misconfiguration.

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION
100	MGMT-HTTP	8000	Any	Any	Any
110	MGMT-HTTPS	8443	Any	Any	Any
120	HTTPS	443	Any	Any	Any
125		8443	Any	Any	Any
5000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork
5001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any
5500	DenyAllInBound	Any	Any	Any	Any

Common misconfiguration when defining firewall rules in the NSG (Network Security Groups) is to use the protocol “ANY”, source “ANY” or the destination “ANY”.

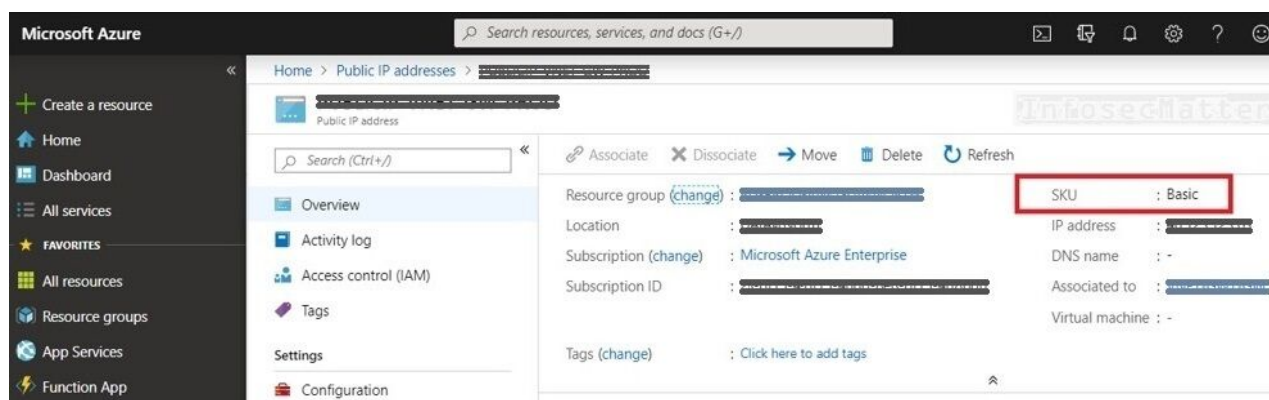
Such practice can lead to a risk of allowing more traffic in than what is intended. For attackers, these little seemingly benign details often times play an important role for allowing them to breach the premises. Do not give them these opportunities.

The best practice is to always stick to the principle of the least privilege. Define the firewall rules in a way to allow only a specific protocol with well-defined source and destination addresses.



Note that it is highly recommended to enable the Layer 7 firewall in Azure, which is application aware. Layer 7 firewall provides enhanced security features across the whole Azure network, including applications.

## 11. Public IP addresses configured as Basic SKU



Configuring public IP address in Azure as Standard SKU (Stock Keeping Unit) has the following advantages over the Basic SKU:

- Truly static IP address
- Secure by default, closed to inbound traffic
- Allows for zone-redundancy and zoning (regional, geographic etc.)
- Allows for future scalability

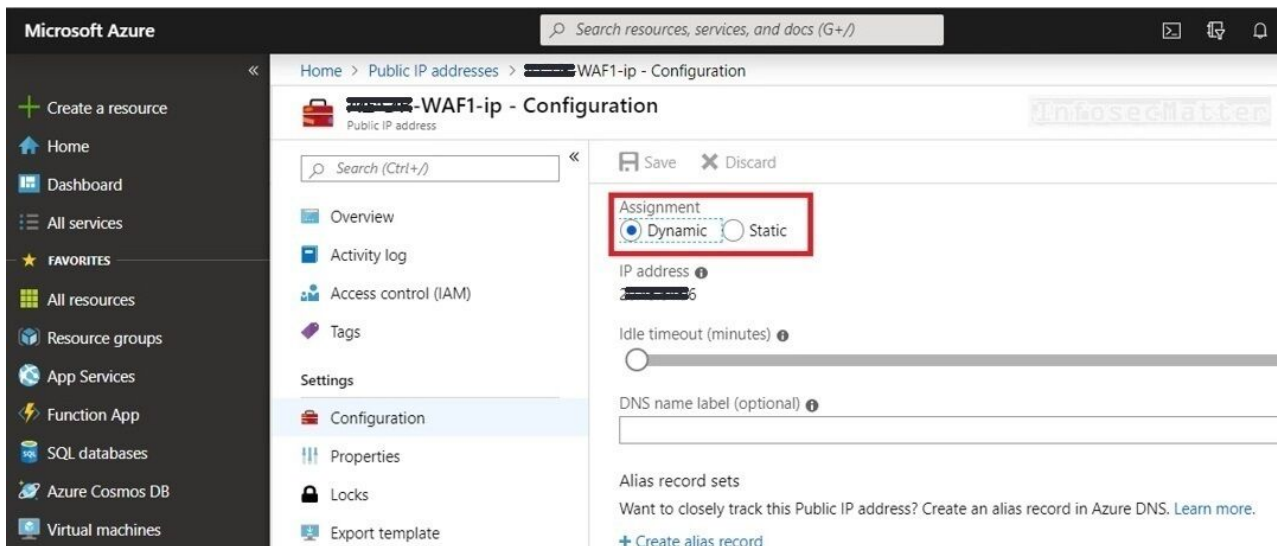
In case of Basic SKU, the main security concern is the overall openness. Unless specifically protected by a firewall, the system assigned the public IP address with Basic SKU would be completely exposed to the outside world by default.

Needless to say, this is highly undesirable in any production environment. In a production environment, all public IP addresses should be configured as Standard SKU with their network flow well understood.

Note that this settings cannot be changed once the IP address has been configured either way. Therefore fixing this may require planning for a downtime and migration.

For more details about the Basic and Standard SKU, see [this](#) page.

## 12. Dynamic IP addresses for publicly facing services



This is not really a security vulnerability per se, but it is a major misconfiguration for any publicly facing system.

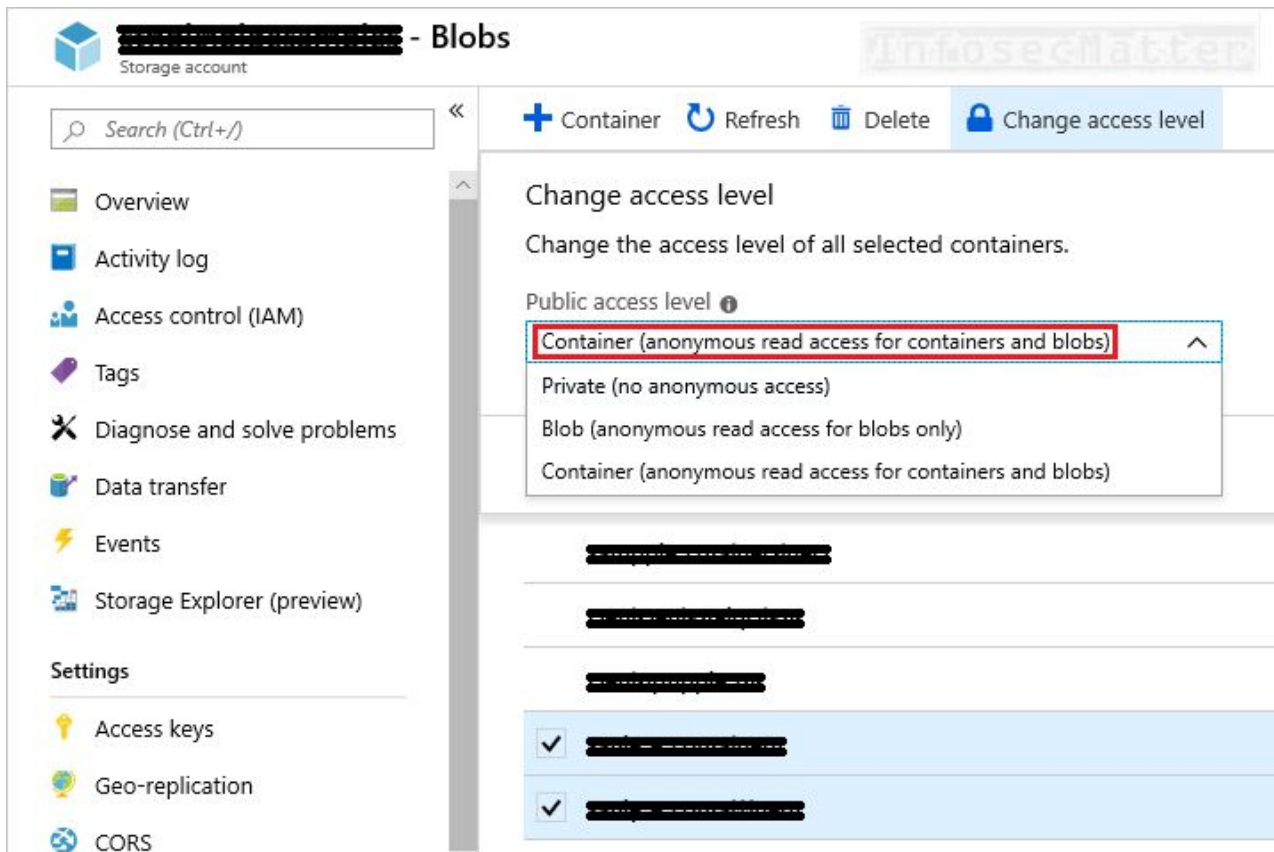
If the IP address is dynamic, it means that it can change at any given time – e.g. after a reboot or a DHCP lease renewal. And when it happens for a publicly available system, then it can break all sorts of things down the road. For instance:

- DNS records
- Monitoring and log alerts
- System integration and interoperability

This can cause unnecessary availability issues (e.g. a DoS). It is therefore always strongly recommended to use a static IP address for any publicly facing service.

### 13. Blob storage with anonymous read access level

---



Azure Blob storage is a powerful and convenient way of sharing data on the cloud. It supports the following 3 access control (level) options:

1. Private (no anonymous access)
2. Blob (anonymous read access for blobs only)
3. Container (anonymous read access for containers and blobs)

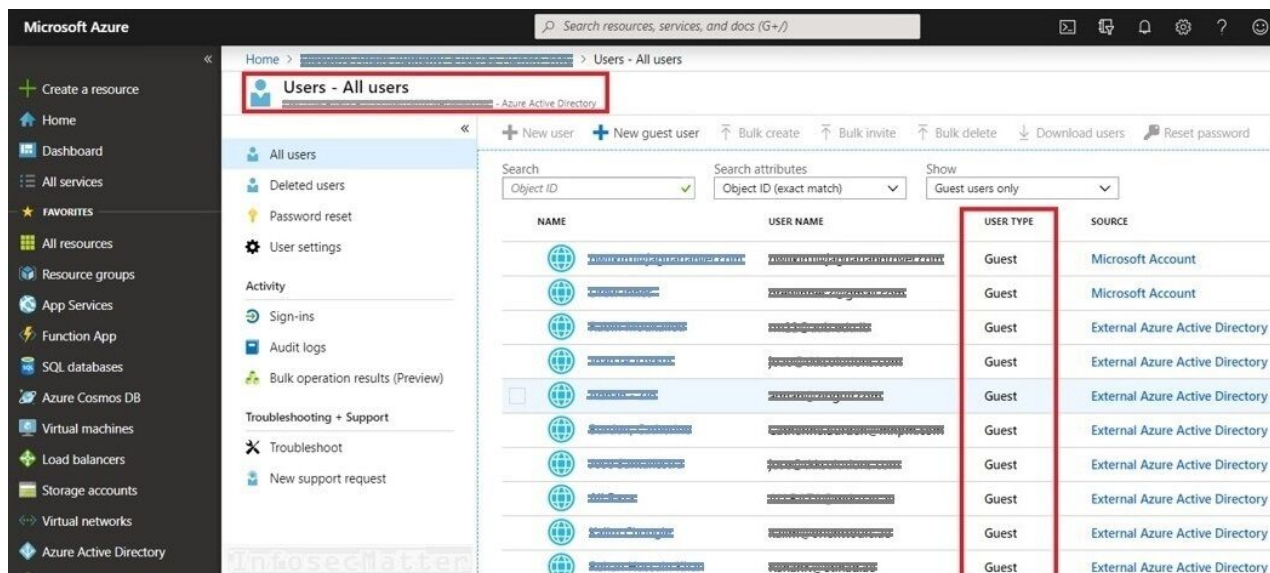
Configuring access level as either 2 latter options (anonymous read access) naturally presents a security risk of unauthorized access to data, data leakage, exfiltration etc.

In a production environment, all blob storages should be set to private, disallowing any anonymous access.

More information about access controls for containers and blobs can be found [here](#).

## 14. High number of guest users in Azure AD

---



Guest users in Azure Active Directory (AD) are accounts typically created for external users such as vendors, contractors, partners, customers and other temporary roles.

They are simply outsiders and it is therefore prudent to keep the number of them as low as possible.

The problem is that some organizations tend to pile up guest users as time goes by and forget to revoke their access after they are no longer needed, which is very risky.

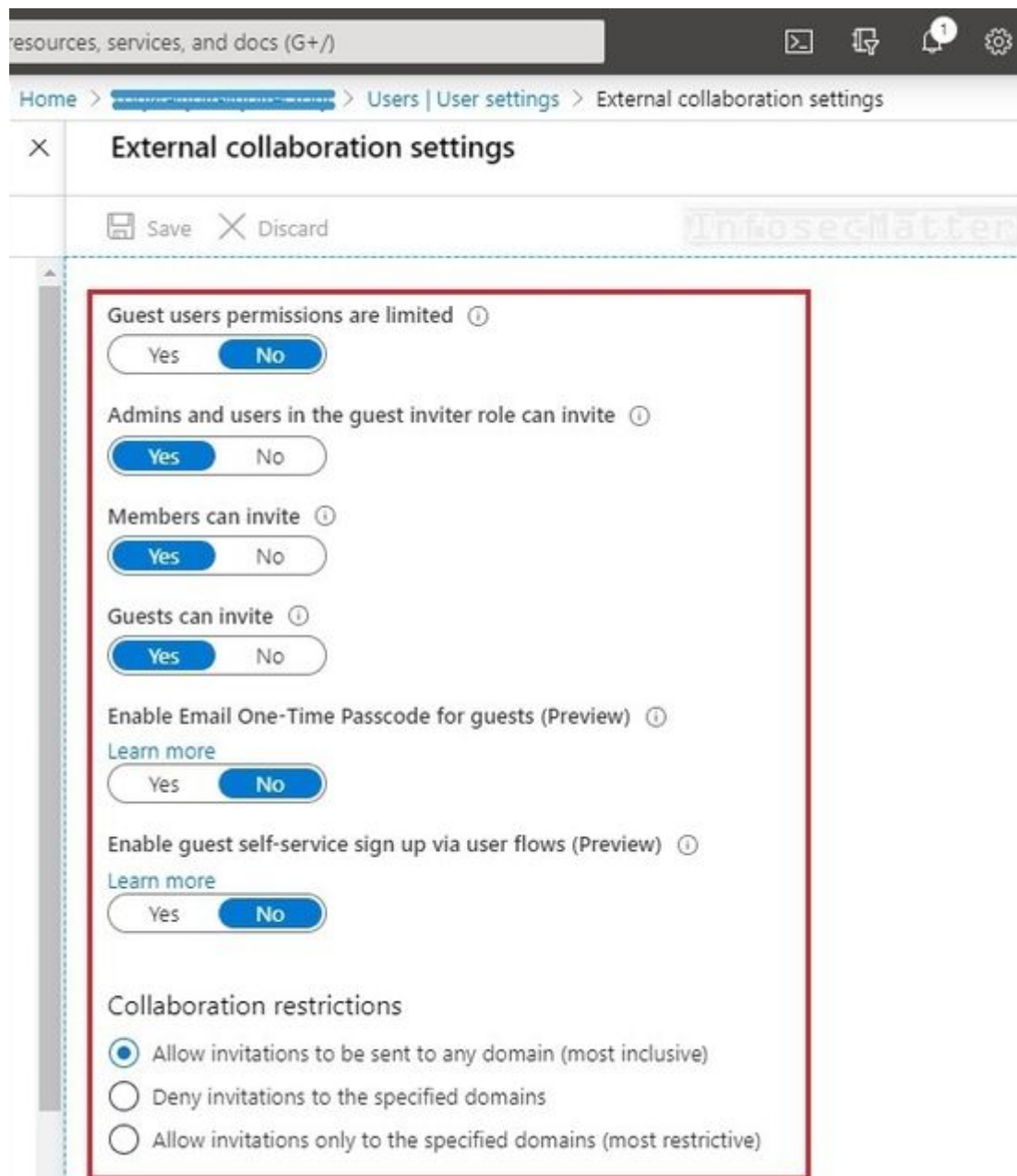
Guest users often times provide means of getting foothold into the environment and this can consequently lead to privilege escalation and other issues within the Azure cloud environment.

Therefore, number of guest accounts should be always kept in check. In fact, CIS Benchmark even recommends having no guest users at all.

Here's how we can find all guest users using Azure CLI:

```
az ad user list --query "[?additionalProperties.userType=='Guest']"
```

## 15. Insecure guest user settings in Azure AD



Having guest users in the Azure Active Directory is one thing, giving them exorbitant privileges is another.

By default, guests have very limited privileges in comparison with fully fledged member users (see the differences [here](#)), but in Azure AD guests can also be configured to have the very same privileges as member users!

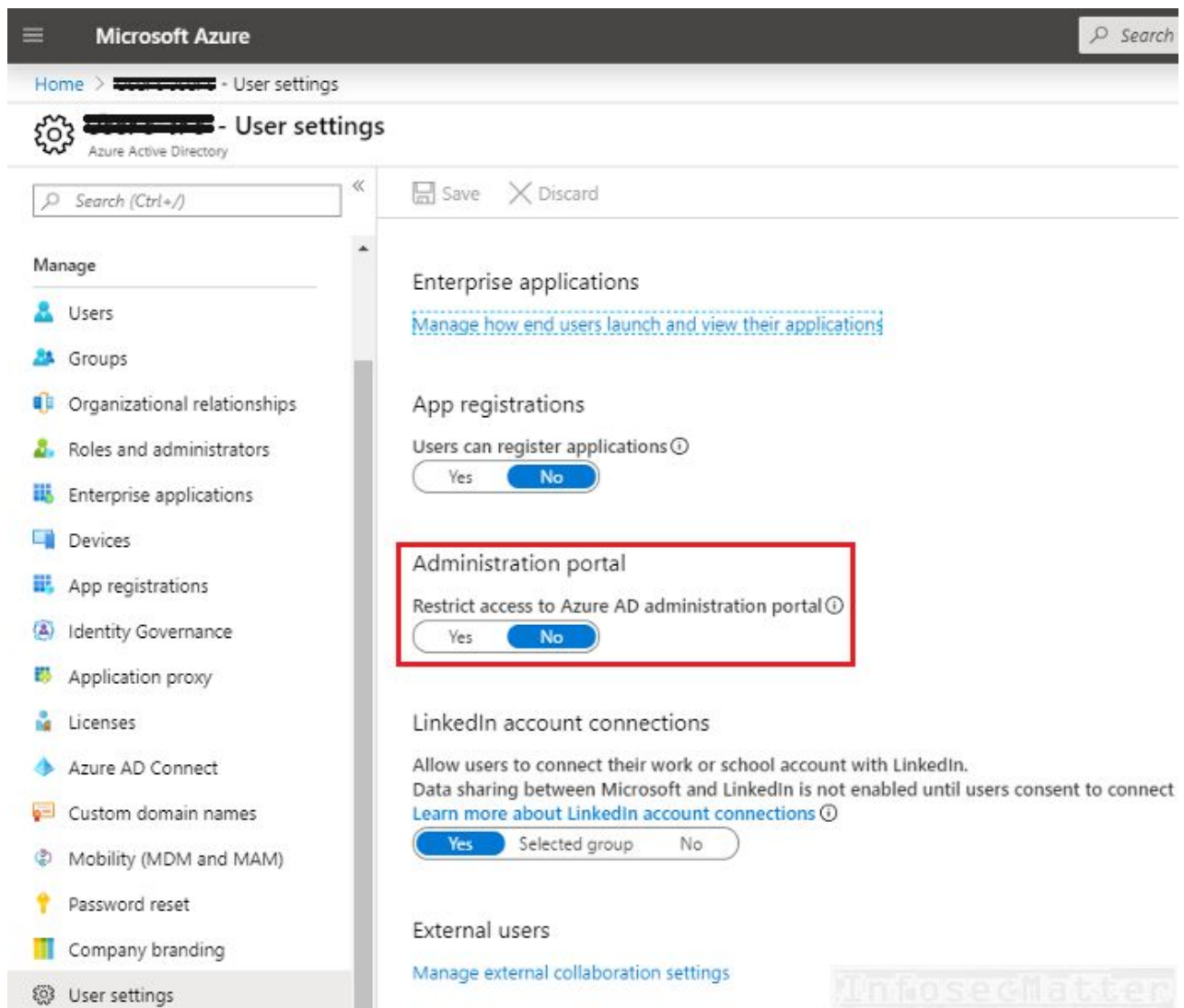
This is configured through the external collaboration settings such as the one shown above. The configuration depicted above will grant guest users permissions to:

- Enumerate all other users and groups (including members)
- Read properties of all registered and enterprise applications
- Invite other users from outside into the organization

From the security standpoint this is of course extremely insecure and it should be changed ASAP, unless there is a very very strong justification for it.

But again, it is recommended to have no guest users at all.

## 16. Unrestricted access to Azure AD administration portal



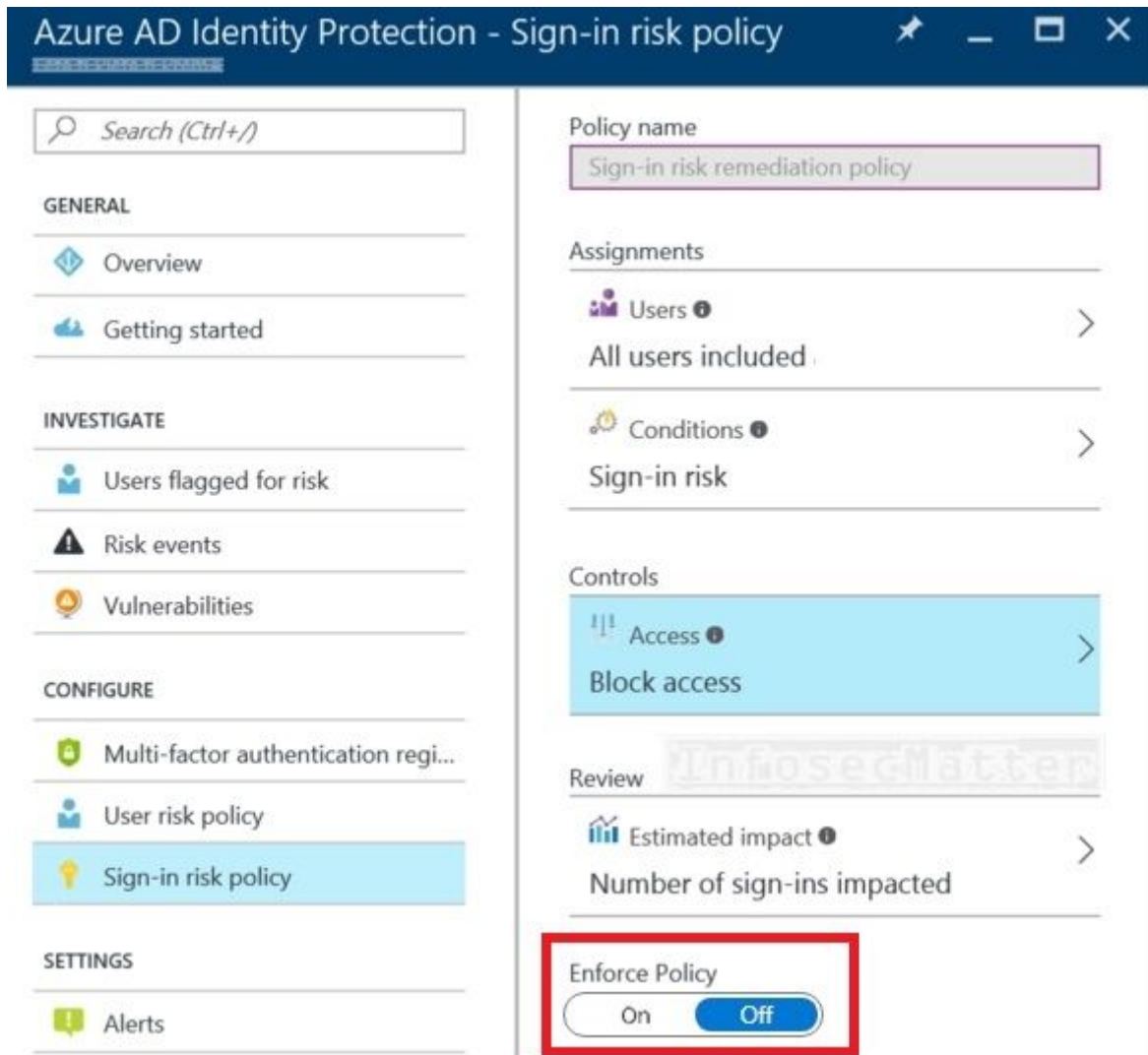
The Azure AD administrative portal contains large amount of sensitive information and by default, any user under Azure AD can access it.

This means that it is possible to login to the <https://portal.azure.com/> as a standard (member) user and browse around, view pretty much all the settings, other users' details, group membership, applications etc.

This is of course major security risk and therefore should be restricted.

## 17. Azure Identity Protection feature is disabled





Azure Identity Protection adds an extra layer of protection for user accounts in Active Directory to mitigate the login (sign-in) risks such as:

- Atypical travel of a user
- Malware linked source IP address
- Leaked credentials of a user
- Password spraying attempts
- Anonymous source IP address (e.g. Tor)

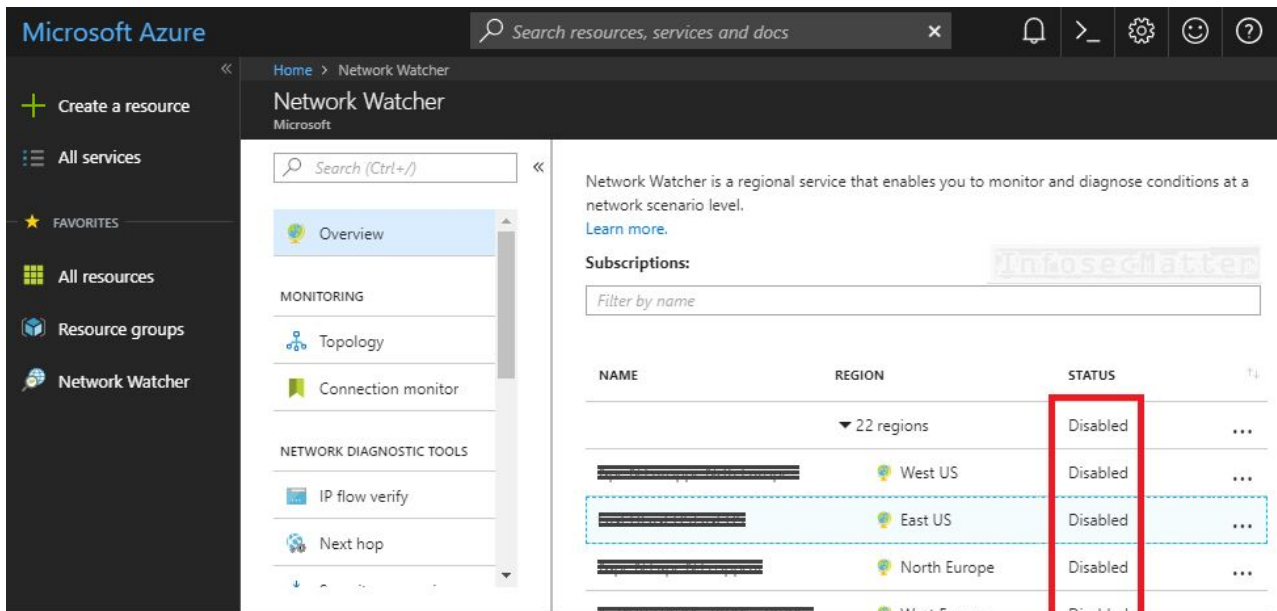
This is definitely something that helps to keep the Azure AD environment more secure and therefore is highly recommend to have this enabled.

The only downside is that this is a premium feature which adds additional costs (see the pricing details [here](#)).

More information about Azure Identity Protection can be found [here](#).

## 18. Azure Network Watcher is disabled

---



Azure Network Watcher provides vital diagnostic and visualization tools for understanding and troubleshooting of network issues within the Azure network.

It also provides network flow analysis for the NSG (Network Security Groups) Azure firewall, including packet capture to and from a particular VM and many other diagnostic features.

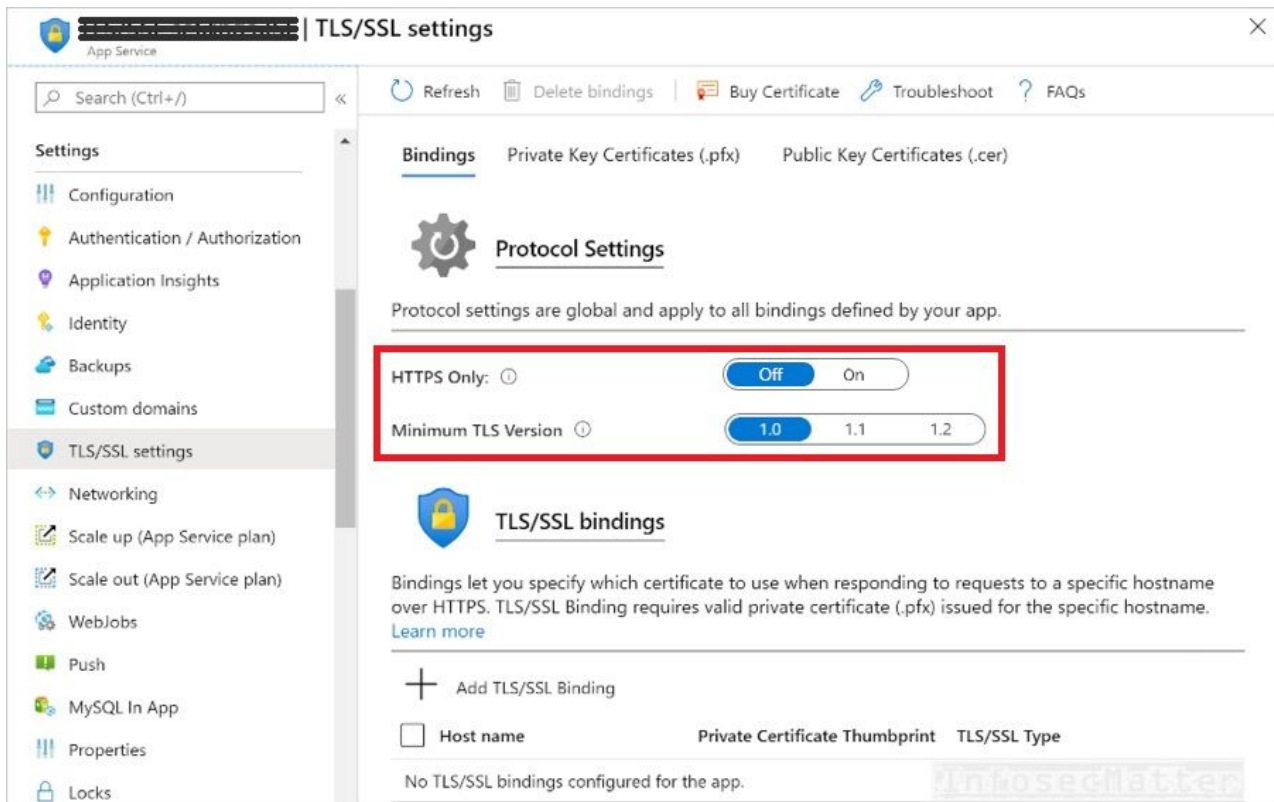
By default this is disabled, but it is recommended to have this enabled for all regions.

Here's how we can also check status of the Network Watcher using Azure CLI:

```
az network watcher list
```

For more information about Azure Network Watcher, check the official documentation [here](#).

## 19. HTTPS only traffic is not enforced for all web apps



From a security standpoint, accepting only secure (encrypted) HTTPS connections should be a standard today for all web applications – both internal and external (publicly exposed).

This adds much needed layer of security, confidentiality and privacy.

When the settings above is enabled, every incoming insecure (plaintext) HTTP request to the given Azure web service will be redirected to its HTTPS port.

This should be configured for all Azure web services.

The same strategy should be enforced when it comes to databases in Azure, e.g.:

- MySQL server
- PostgreSQL server

All servers should have enabled the 'Enforce SSL connection' option.

Now you may wonder which TLS should be selected?

Both NIST (National Institute of Standards and Technology) and PCI (Payment Card Industry) do not consider TLS version 1.0 nor 1.1 to be a strong cryptography.

Therefore, TLS version 1.2 should always be selected, at minimum.

## 20. Monitoring policies in Azure Security Center

## ASC Default (subscription: [REDACTED])

Edit Initiative Assignment

Assigned by

Security Center

### PARAMETERS

Infosec matter

\* Monitor virtual machine scale sets system updates ⓘ

Disabled



AuditIfNotExists

Disabled

\* Monitor virtual machine scale sets OS vulnerabilities ⓘ

AuditIfNotExists



\* Monitor system updates ⓘ

AuditIfNotExists



\* Monitor OS vulnerabilities ⓘ

AuditIfNotExists



\* Monitor endpoint protection ⓘ

AuditIfNotExists



\* Monitor disk encryption ⓘ

AuditIfNotExists



\* Monitor network security groups ⓘ

AuditIfNotExists



\* Monitor web application firewall ⓘ

AuditIfNotExists



\* Enable Next Generation Firewall (NGFW) monitoring ⓘ

AuditIfNotExists



\* Monitor vulnerability assesment ⓘ

AuditIfNotExists



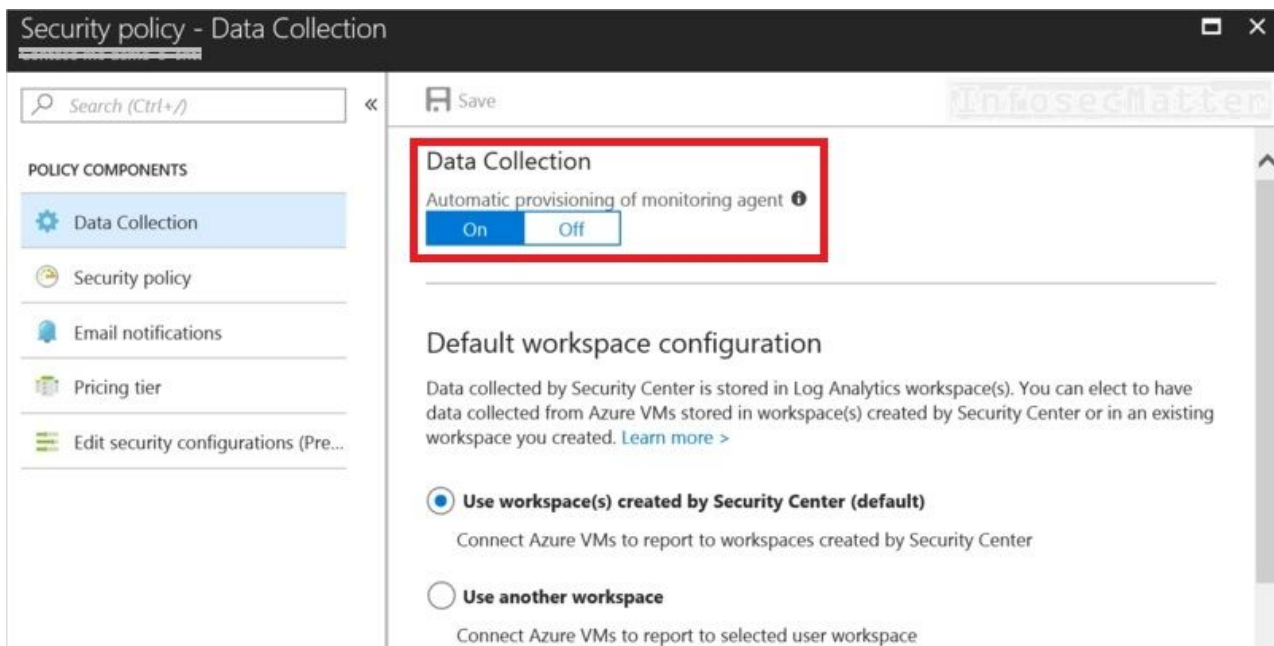
The [CIS Benchmark](#) recommends having enabled the following monitoring policies in the Azure Security Center:

- Compute And Apps:
  - System Updates
  - OS Vulnerabilities
  - Endpoint Protection
  - Disk encryption
  - Vulnerability Assessment
  - Adaptive application controls
- Network:
  - Network Security Groups (NSG)
  - Web Application Firewall (WAF)
  - Next Generation Firewall (NGFW)

- Data:
  - Storage Encryption
  - SQL Auditing
  - SQL Encryption

All these policies should be enabled (set to 'AuditIfNotExists') in every production environment. These policies provide essential security monitoring of the Azure cloud components.

Having these policies enabled should be also accompanied by having the 'Automatic provisioning of monitoring agent' enabled as well:



This will ensure that the Azure Monitoring Agent is provisioned on all existing virtual machines deployed in the environment and also on any new ones created in the future.

More information about Azure security policies can be found [here](#).

## Conclusion

Assessing security posture of Microsoft Azure cloud environments is no easy task. It is a very complex topic requiring deep knowledge of many areas reaching far more than just the Azure cloud itself.

The whole ecosystem keeps changing – always evolving, introducing new features, adapting to new requirements and so on.

I hope that this article provided at least some helpful insights into the world of Azure cloud auditing and equipped you with some practical information so that you can help your clients make their cloud infrastructure more secure.

If you have enjoyed this article and you would like more like it, please [subscribe](#) to our mailing list and follow us on [Twitter](#) and [Facebook](#) to get notifications about new content.