Quick *Review*

Azure
Active Directory

1 Identity

Microsoft’s cloud-based identity and access management service.

2 Applications

You can also give access to your applications.

3 Products

This is used by both Azure and Microsoft 365.

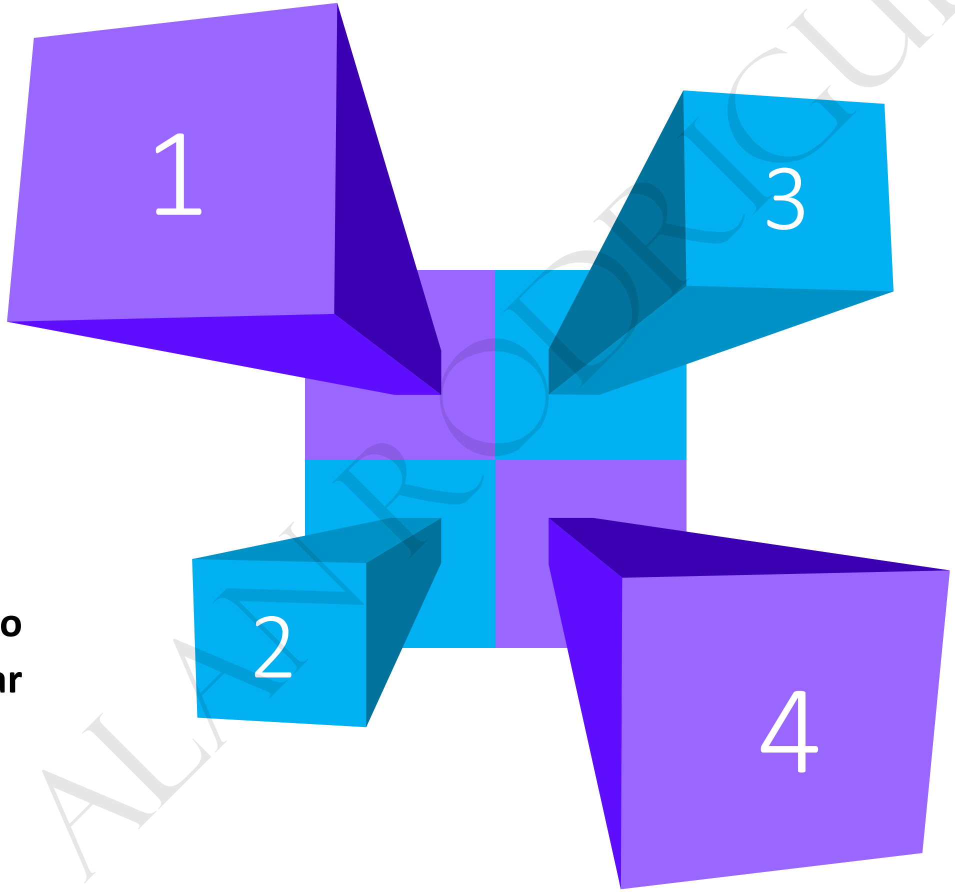
Azure AD Custom Domains

Header

Add the custom domain name in Azure AD

Header

Add the DNS information to your domain registrar



Header

Verify the custom domain name in Azure AD

Header

Make the domain as the primary domain for new users

Review

C

Azure AD

Licensing

Azure AD Free – User and groups management. Basic reports. Self-service password change for cloud users.

Azure AD Premium P1 – Dynamic groups, hybrid identities benefits

Azure AD Premium P2 – Conditional Access , Azure AD identity Management, Azure AD Privileged Identity Management.

Dynamic Groups

Users and devices can be added to groups automatically based on the rules defined and the attributes of the user or device.

You need to have Azure AD Premium P1 licenses.

You can’t create one rule for both users and devices.

Group Owners

Can manage the group which includes membership of users to groups.

The group owner does not need to be a member of the group.

Once a group is assigned an owner, you can't delete the owner, you need to change the owner.

Deleted users

When you delete a user in Azure AD, the account is still in place for 30 days. The account will be in a suspended state.

You can still restore the user during this time.

After the 30-day window, then the user is permanently deleted.

Applications

Azure AD Roles

Application Administrator

This role allows one to manage all aspects of enterprise applications, application registrations and application proxy settings.

The user also has the ability to grant consent for delegated permissions and application permissions.

Here the user will also NOT be added as an owner when creating the new application.

Azure

AD Roles

Cloud Application Administrator

This role allows one to manage all aspects of enterprise applications, application registrations BUT NOT application proxy settings.

The user also has the ability to grant consent for delegated permissions and application permissions.

Here the user will also NOT be added as an owner when creating the new application.

Azure

AD Roles

Application Developer

Here users can create application registrations if the setting of “Users can register applications” is set to No.

This role can also grant permission to consent on one's own behalf when the "Users can consent to apps accessing company data on their behalf" setting is set to No.

But the user will be assigned as the owner of the application.

Identity *Protection*

Identity Protection

Has the ability to automatically detect and remediate identity-based risks

Uses its own threat intelligence to understand identity-based risks

The different risks

Leaked credentials

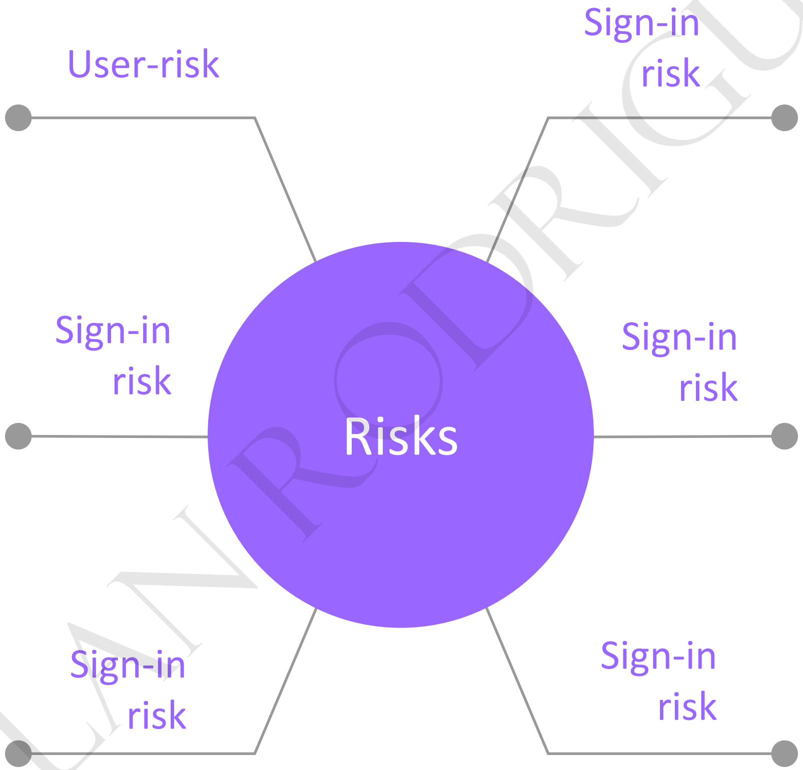
This detects if the users' credentials have been leaked

Anonymous IP Address

Anonymous IP address – The user is not signing in from a typical IP address

Atypical travel

Here sign-ins are happening from different geographic locations



Malware

Here the user’s device could be infected with a malware

Password spray

Someone is trying out different passwords

Unfamiliar sign-in properties

Not the typical behavior the user sign ins

Permissions required

Global Administrator

Here the user will have full access to Identity Protection

Security Administrator

Here the user will have full access to Identity Protection

Except be able to reset the user's password

Security Operator

Can view the Identity protection reports and dismiss user risks etc.

But the user can't configure the policy, reset a user password or configure alerts

Security Reader

Can only view the Identity protection reports.

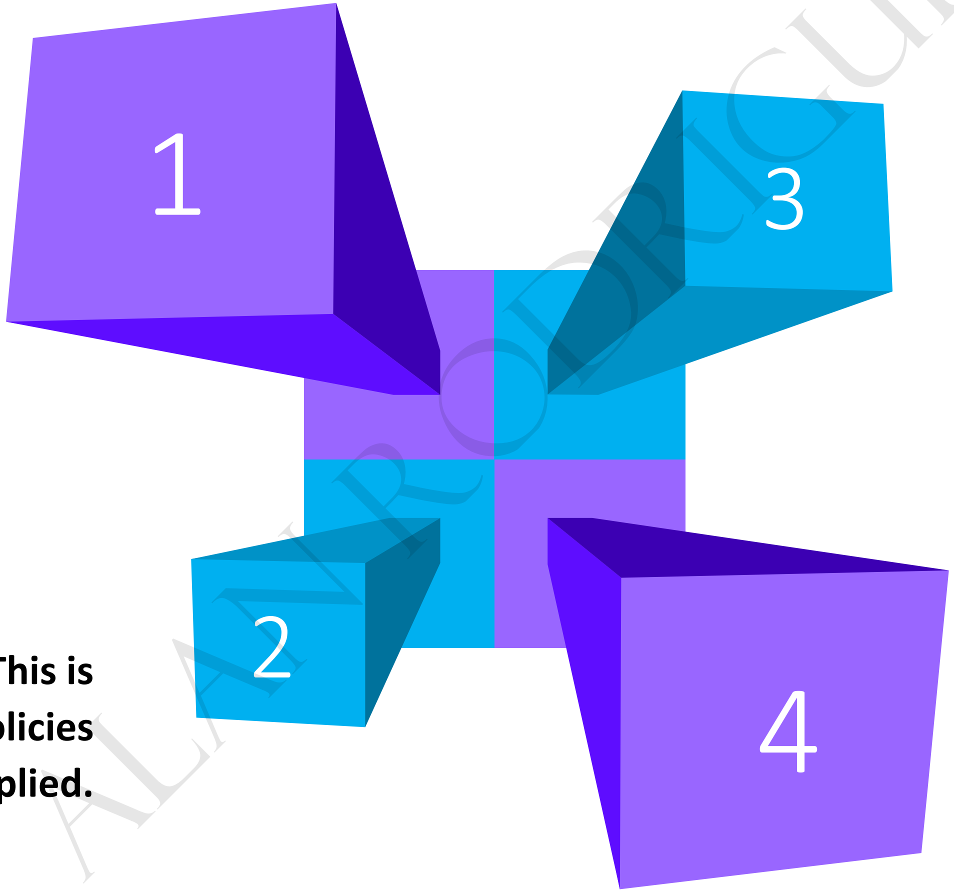
Identity Protection

Hybrid Identities

If you had implemented hybrid identities with Azure AD Connect, then to get a report on leaked credentials , ensure to use Password hash synchronization.

Azure Blueprints

Azure Blueprints



Role assignments – If you need specific roles to be assigned.

Resource groups – If you need certain resource groups to be in place.

Policy assignments – This is if you need specific policies to be applied.

Azure Resource Manager templates – If there are resources that need to be deployed.

Azure Blueprints - Stages

Definition – Here you define the Blueprint itself. The Blueprint needs to be saved to either a management group or a subscription.

When you save the Blueprint to a management group, the Blueprint can be assigned to any subscription which is part of the management group.

To save the Blueprint definition, you need to have Contributor access to either the management group or the subscription.

Azure Blueprints - Stages

Publishing – Once the Blueprint is defined, you can publish it. Here you can assign a version number for the Blueprint.

Assignment – Here the Blueprint is then assigned to a subscription.

You can protect resources deployed via the Blueprint resource locks.

Here even if there is a user with the Owner role, still the user will not be able to remove the lock.

You can only remove the lock by unassigning the blueprint.

Azure Virtual Machine Security

Using Role-based access control

Control who has access to your virtual machine.

Control who can stop or start the virtual machine.

Control who can change the properties of the virtual machine.

Azure Virtual Machine Security

Protect against malware

Install an antimalware solution that can help identity and remove viruses.

You can use Microsoft Antimalware solution.

Or use partner endpoint solutions (Trend Micro, McAfee).

Azure Virtual Machine Security

Update Management for your virtual machines

You manage the updates for your virtual machine.

Always deploy the latest security updates.

If you are deploying a new virtual machine, always use the latest image which has all the latest security updates.

Azure Virtual Machine Security

Use Microsoft Defender for Cloud

This tool can give you several recommendations on how to improve the security posture of your virtual machines.

It can also actively monitor for any threats to your virtual machines.

You can use features such as Just-in-time VM access to give access to your virtual machines.

Azure Virtual Machine Security

Azure Disk Encryption

Encrypt the disks on your virtual machine using Azure Disk Encryption.

This can be used to encrypt both Windows and Linux based virtual machines.

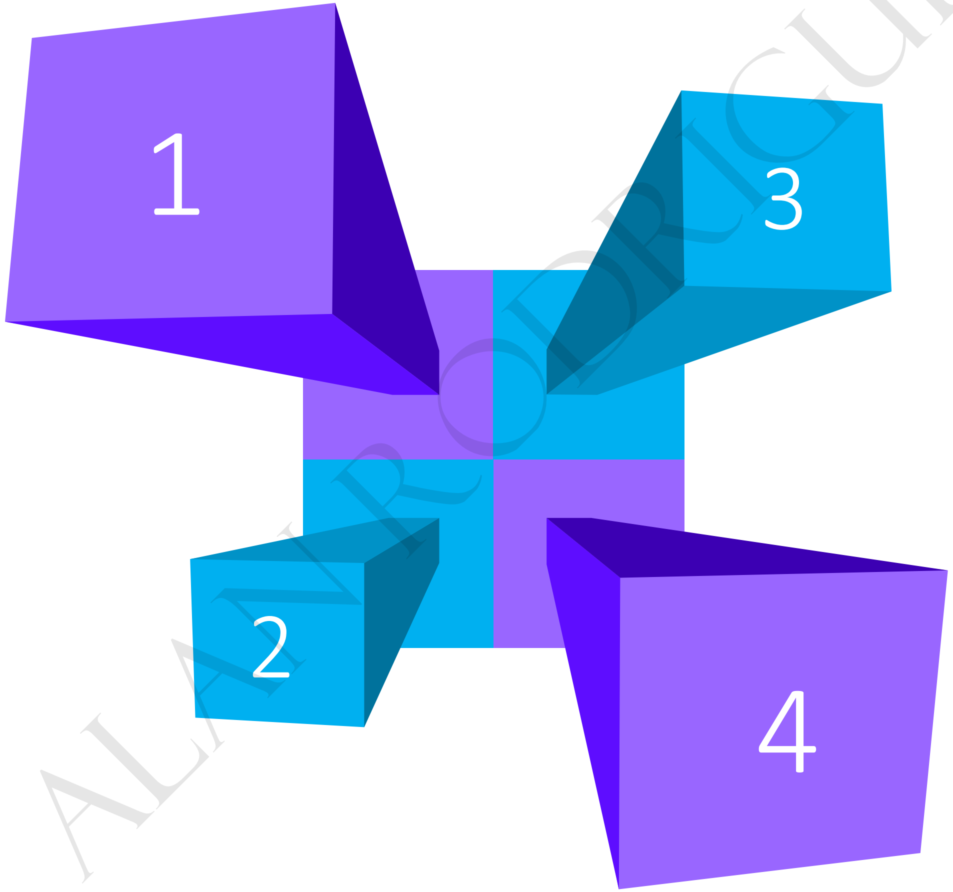
Use Network Security Groups

Ensure to restrict inbound and outbound traffic via Network Security Rules.

Continuously review the rules you have in place.

Microsoft *Antimalware*

Microsoft Antimalware for Azure VM



Purpose

This is a free real-time protection software that helps to remove viruses, spyware and other malicious software.

Agent

Here you install the agent via an extension on an Azure virtual machine.

Scanning

There is a scheduled scan which can occur on the virtual machine.

Remediation

It can also take appropriate actions on detected malware by deleting or quarantining the malicious files.

Vulnerability *Assessment*

Vulnerability assessment

With Microsoft Defender for Cloud plans, you can deploy a vulnerability assessment solution to your virtual machines.

You can deploy Microsoft Defender for Endpoint which is supported for Azure virtual machines and Azure Arc-enabled machines.

This helps to discover vulnerabilities and misconfigurations in real time. Here there is no need of agents or periodic scans.

Vulnerability assessment

With Microsoft Defender for Cloud plans, you can also opt to deploy the Qualys scanner.

Here you don't need a separate Qualys license or account.

This is also supported on Azure virtual machines and Azure Arc-enable servers.

Vulnerability assessment

An extension to the Azure virtual machine will be deployed when you opt to deploy the vulnerability assessment solution.

The scanning begins automatically as soon as the extension is installed successfully when it comes to the Qualys scanner.

For the Qualys scanner, the scan is then run every 12 hours.

Update *Management*

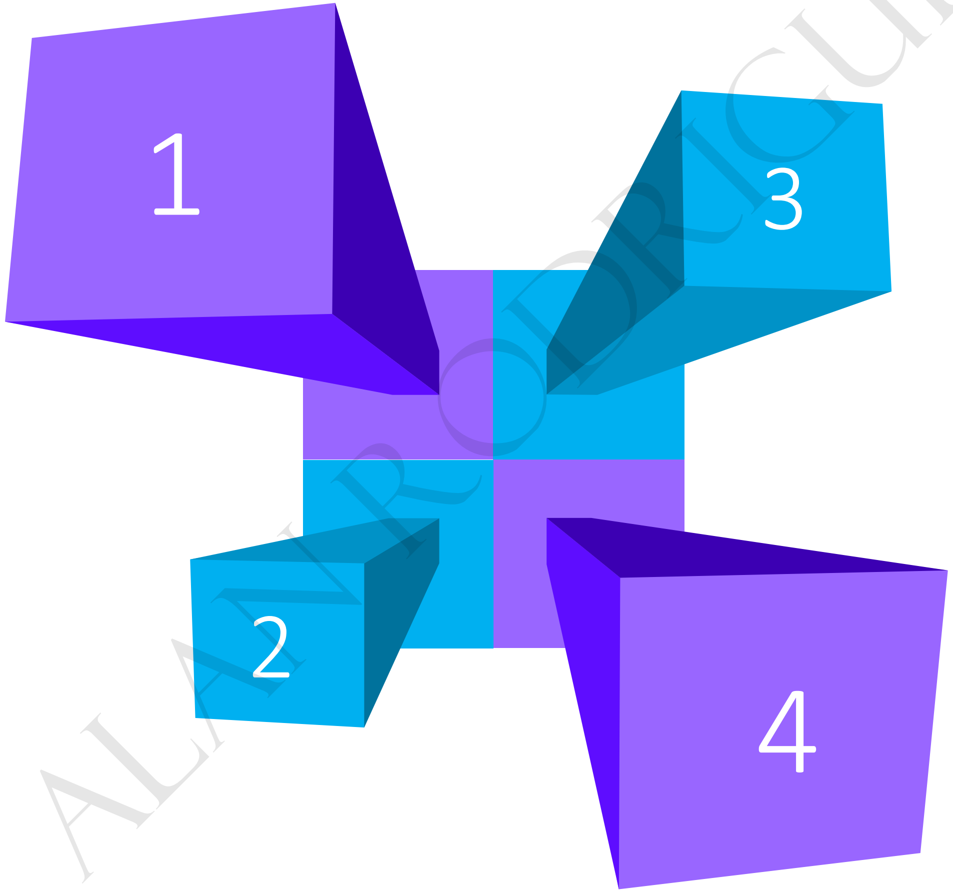
Update Management

Manage the updates

Here you can manage the updates for your Windows and Linux virtual machines. This can be VM's on Azure. Or physical or VM's in your on-premises environment.

Updates

Here you can assess the updates and manage the process of installation.



Scans

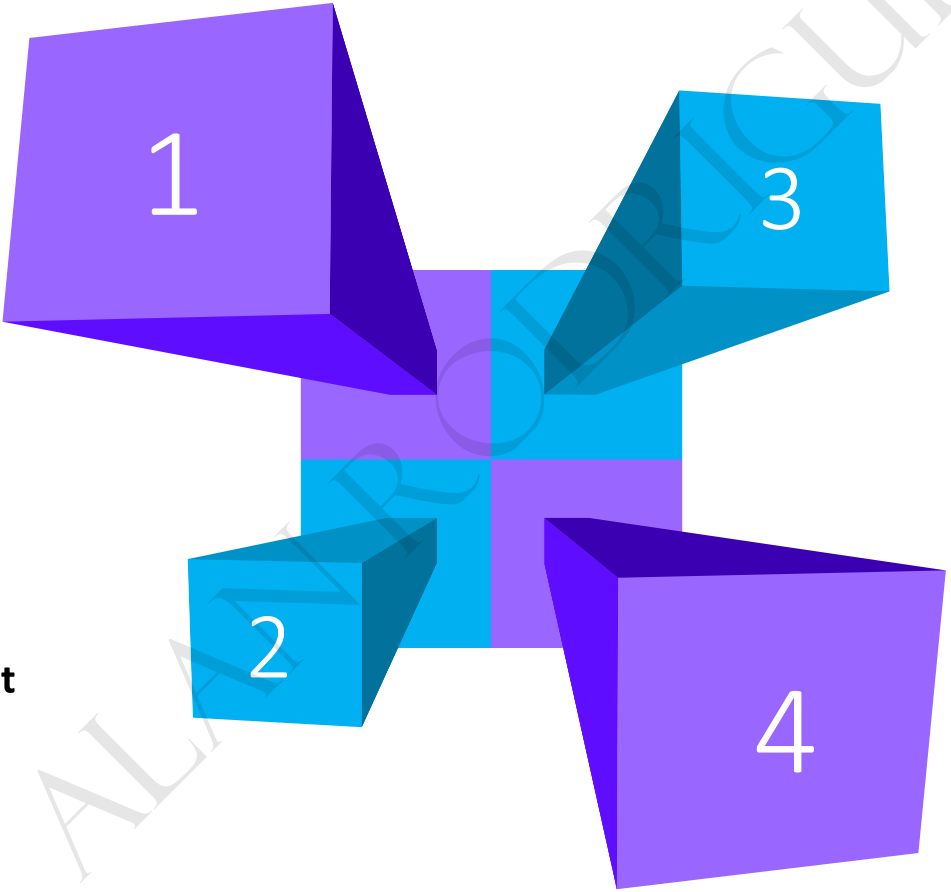
For Windows machines, the scan is done twice per day. For Linux VM's the scan is done every hour.

Classification

You have a classification for the updates – Critical updates , security updates etc.

Just-in-time *VM access*

Just-in-time VM Access



Lock the Inbound Traffic

This feature can be used to select the ports on the virtual machine that will be blocked for inbound traffic.

Control

Here you can select which ports from relevant IP addresses and even for a specific amount of time.

Request access

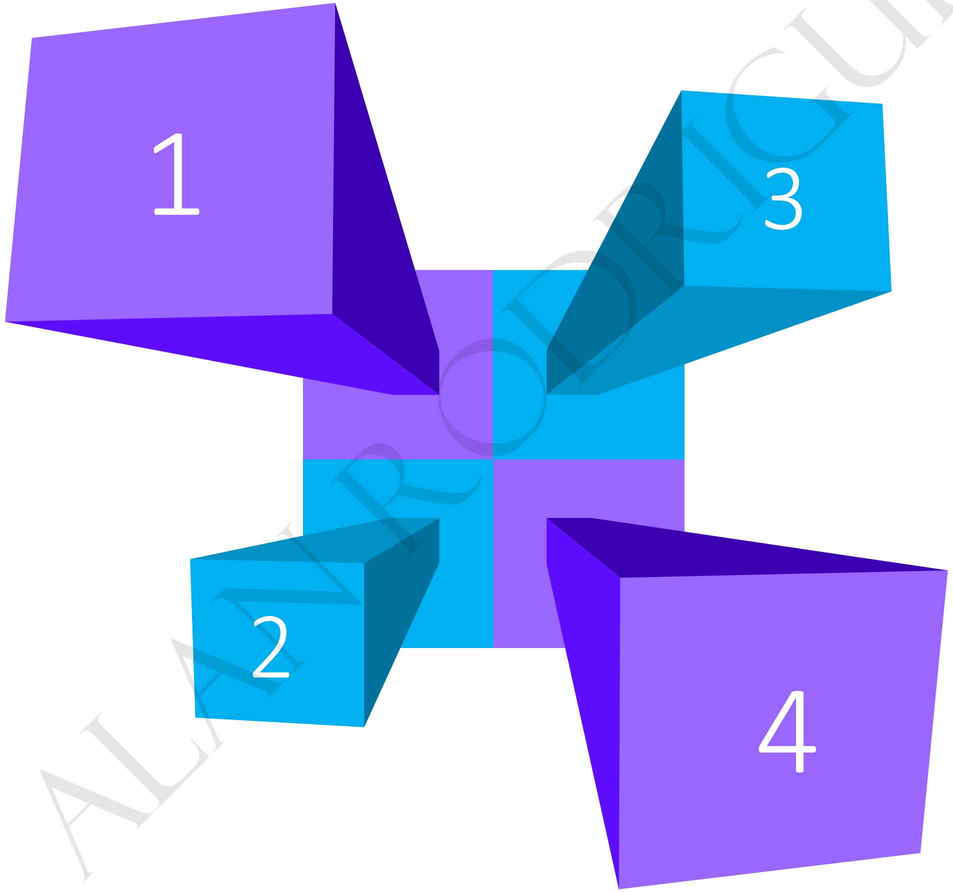
A user needs to have the right role in place to request access to the virtual machine.

Network Security Groups

Just-in-time manages the rules in the Network Security group.

Workload *Protection*

File Integrity Monitoring



Detect changes

Examines operating system files, Windows registries, application software, Linux system files.

Change Tracking

The Log Analytics agent sends data reporting the state of items on the machine.

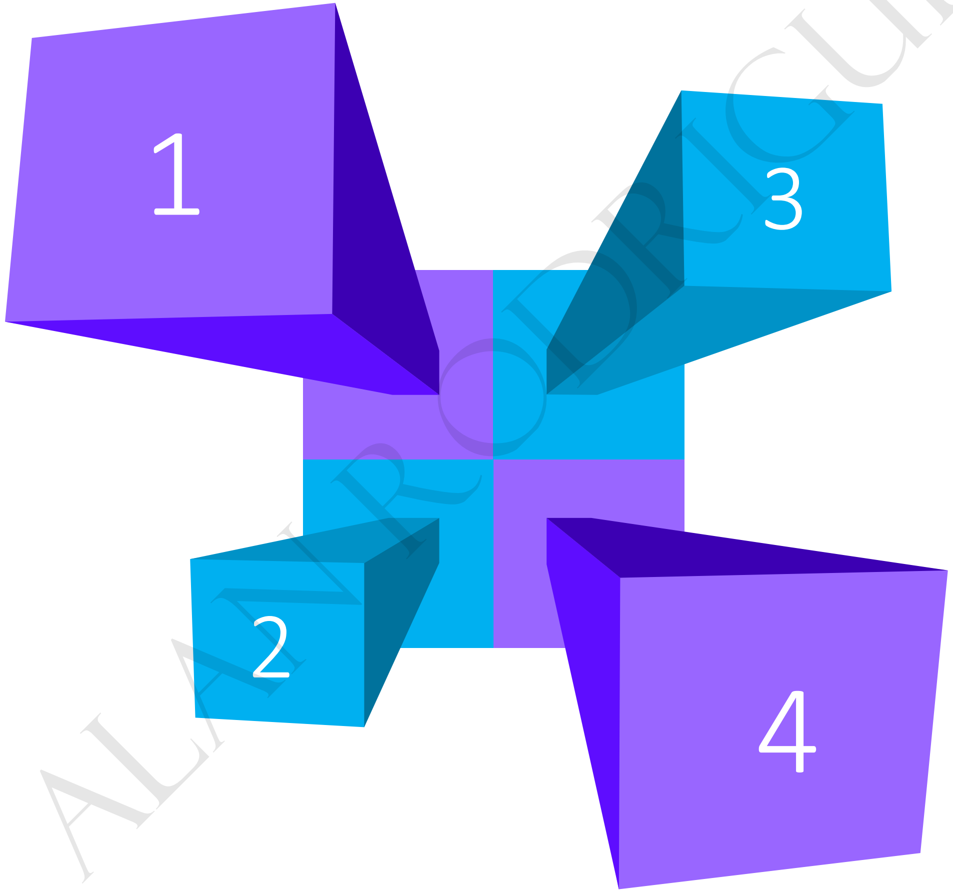
Files

You can also mention which files and folders to monitor.

Cloud

You can also connect your machines in your AWS cloud environments.

Adaptive Application Controls



Applications

This is an intelligent and automated solution that can be used to define an allow list of known-safe applications.

Identify

This then helps to identify any sort of potential malware, outdated or unauthorized applications.

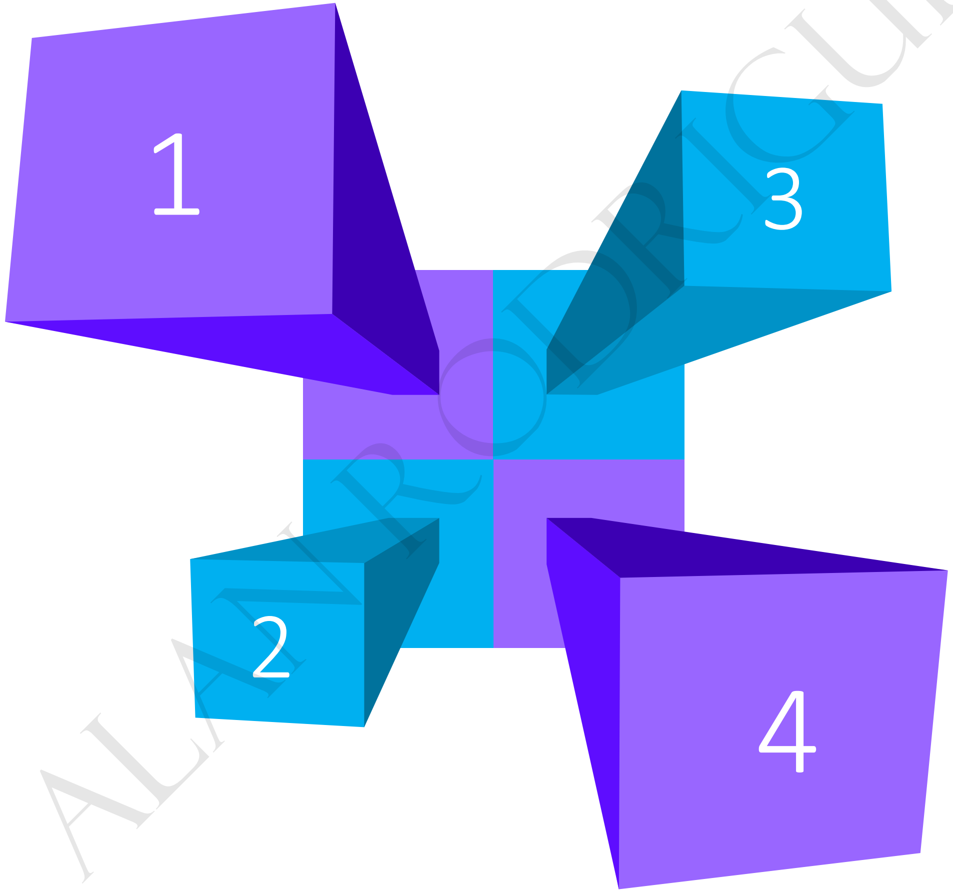
Groups

Applications can be segregated into groups if they run the similar types of applications.

Rules

You can define rules to configure how applications are managed when it comes to Adaptive application controls.

Network hardening



Network Security Groups

It helps to harden the Network Security Group rules.

Identification

It uses internal machine learning algorithms to provide indicators on how to harden the Network Security Groups.

Requirement

Some of the requirements to enable this feature on VM's – Microsoft Defender for servers, 30 days of traffic data.

Alerts

You get alerts if traffic flowing via the resource is not within the defined IP range.

Microsoft Sentinel

Threat protection

What is Microsoft Sentinel

This is a cloud service that provides a solution for SEIM (Security Information Event Management) and SOAR (Security Orchestration Automated Response)

This provides a solution that helps in the following

Collection of data – Here you can collect data across all users, devices, applications and your infrastructure. The infrastructure could be located on-premise and on the cloud.

It helps to detect undetected threats.

What is Microsoft Sentinel

It helps to hunt for suspicious activities at scale.

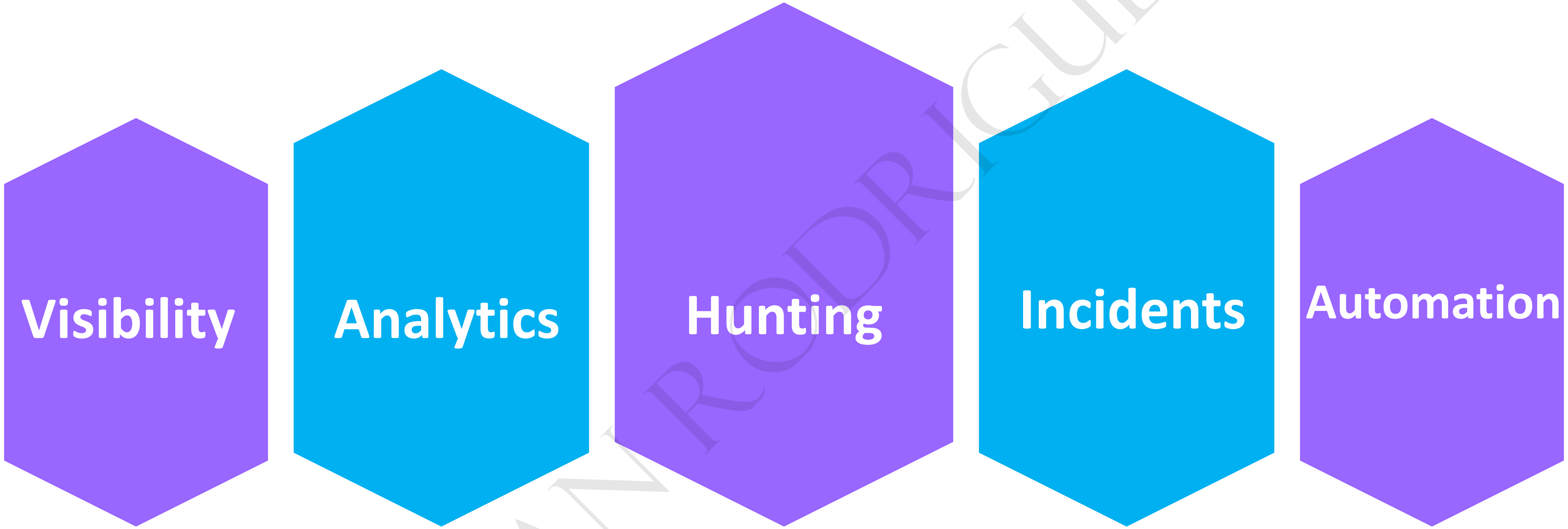
It helps to respond to incident rapidly.

Once you start using Microsoft Sentinel, you can start collecting data using a variety of connectors.

You have connectors for a variety of Microsoft products and other third-party products as well.

You can then use in-built workbooks to get more insights on the collected data.

Microsoft Sentinel



Microsoft Sentinel

Microsoft *Sentinel*

Data Connectors

Ingestion

You can connect to a variety of data sources. Data then gets ingested in Microsoft Sentinel.

Azure Firewall

Here the events get stored in the AzureDiagnostics table.

Security

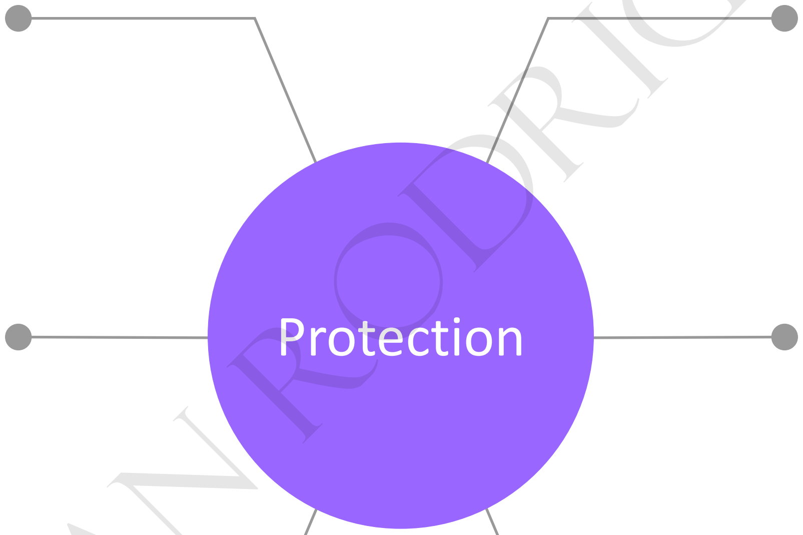
The security events from Windows machines get stored in the SecurityEvent table.

Azure AD Identity Protection

Here the data gets ingested in the SecurityAlert table.

Sentinel

Analytics - Rules



Protection

Microsoft Security

These are rules that create incidents from alerts that are generated in other Microsoft security solutions.

Fusion

These are based on the Fusion engine that is able to detect advanced multistage attacks.

Anomaly

These are based on machine learning algorithms to detect specific types of anomalous behavior.

Scheduled

These are rules written by Microsoft security experts.

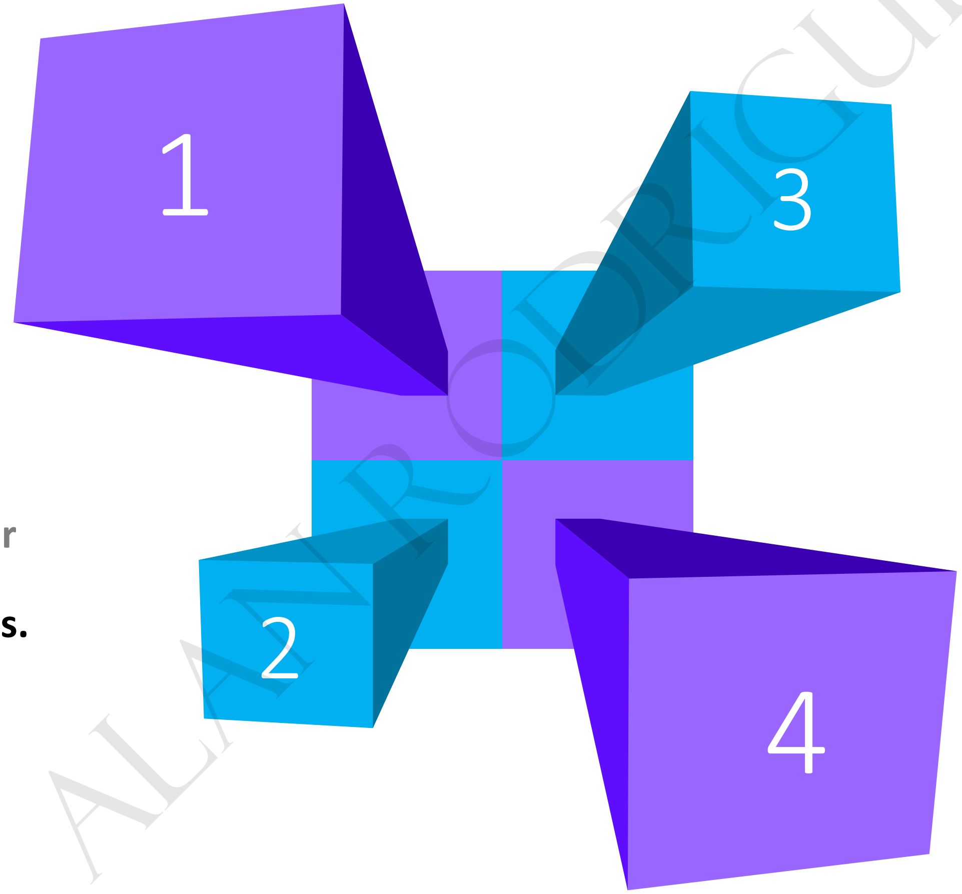
Near-real-time

These are a limited set of scheduled rules that are designed to run every minute.

Machine Learning

These are behavioral analytic rules that are based proprietary Microsoft machine learning algorithms.

Microsoft Sentinel Roles



Microsoft Sentinel Reader

View data, incidents, workbooks and other Sentinel resources.

Microsoft Sentinel Responder

Can also manage incidents.

Microsoft Sentinel Contributor

Can also create, edit workbooks, analytics rules.

Microsoft Sentinel Automation Contributor

Can also add playbooks to automation rules.

User and Entity
Behavior Analytics

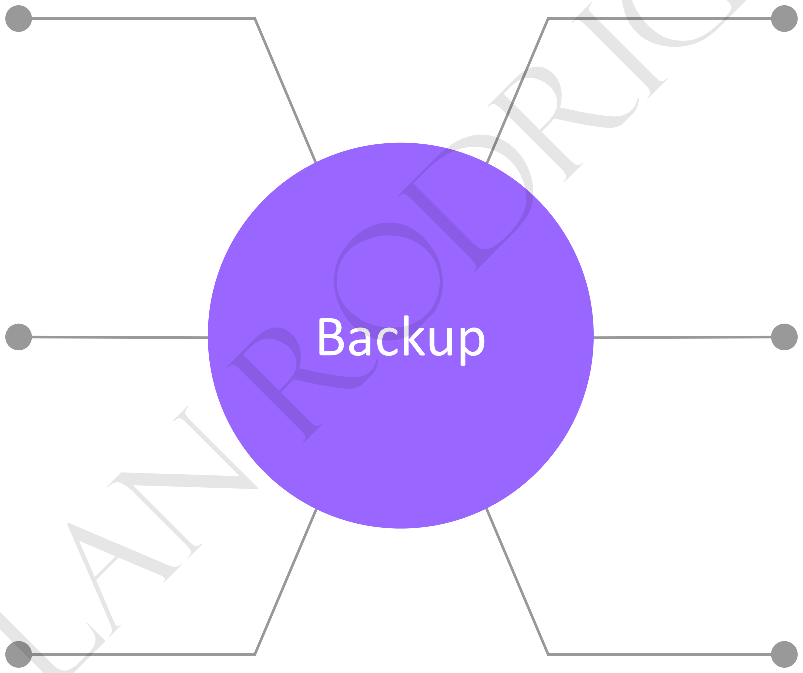
This feature analyzes the collected data and then builds a baseline profile of the entities such as users, hosts, IP addresses and applications.

It then uses machine learning capabilities to detect any sort of anomalous activities .

There are insights based on different sources.

Azure key vault *backup*

Azure Key Vault Backup



Perform backup

With the Azure Key Vault service, you can individually backup your secrets , keys and certificates.

Offline copy

Here you can create an offline copy of all of the secrets that you store in the key vault.

Soft Delete

If you want to protect against accidental or malicious deletion of secrets, then use the soft-delete and purge protection features.

Individual secrets

With this feature, you can't backup the entire key vault in one operation. You can only backup individual secrets at a time.

Download backup

When you download a backup of a secret, key or certificate, the downloaded blob will be an encrypted blob.

Restore

To perform a restore, you can choose a key vault which is in the same Azure subscription and same Azure geography

Data Masking

Azure SQL Database Data Masking

Here the data in the database table can be limited in its exposure to non-privileged users.

You can create a rule that can mask the data.

Based on the rule you can decide on the amount of data to expose to the user.

Azure SQL Database Data Masking

There are different masking rules

Credit Card masking rule – This is used to mask the column that contain credit card details. Here only the last four digits of the field are exposed.

Email – Here first letter of the email address is exposed. And the domain name of the email address is replaced with XXX.com.

Custom text- Here you decide which characters to expose for a field.

Random number- Here you can generate a random number for the field.

Auditing

Azure SQL Database server auditing

You can enable auditing for an Azure SQL database and also for Azure Synapse Analytics.

This feature can be used to track database events and write them to an audit log.

The logs can be stored in an Azure storage account, Log Analytics workspace or Azure Event Hubs.

This helps in regulatory compliance. It helps to gain insights on any anomalies when it comes to database activities.

Auditing can be enabled at the database or server level.

If it is applied at the server level, then it will be applied to all of the databases that reside on the server.

Always Encrypted

Always Encrypted feature

The Always Encrypted Feature can be used to encrypt data at rest and in motion.

You can encrypt multiple columns located in different tables.

You can encrypt multiple columns located in the same table.

You can just encrypt one specific column.

Always Encrypted feature

You have 2 types of encryption

Deterministic encryption – Here the same encrypted value is generated for any given plain text value. This is less secure. But it allows for point lookups , equality joins, grouping and indexing on encrypted columns.

Randomized encryption – This is the most secure encryption method. But it prevents the searching, grouping , indexing and joining on encrypted columns.

Always Encrypted feature

We can enable the Always Encrypted feature using SQL Server Management Studio.

There are 2 keys that get created when the Always Encrypted feature is enabled for a database.

Column master key – This is an encryption key that needs to be stored in an external data store. Here you can store the key in a Windows certificate store or in the Azure key vault service.

Column Encryption key – This is generated from the column master key and is used to encrypt the actual column.

The user who is implementing the Always Encrypted feature needs to have the following permissions for keys – *create, get, list, sign, verify, wrapKey, unwrapKey*