Contents

[Cortex XDR 1](#_Toc152184977)

[Defender For Cloud 12](#_Toc152184978)

[Qualys 20](#_Toc152184979)

# Cortex XDR

Cortex XDR is extended detection and response system which provides visibility into endpoints, users, and networks. Helps to correlate logs from them and generate alerts. Helps identity root cause of the alerts and helps in immediate response actions.

## Modules in Cortex XDR

Navigation pane consists of:

* Dashboards and Reports
  + Dashboards
  + Reports
  + Dashboards Manager
  + Report Templates
  + Widgets Library
* Incident Response
  + Incidents
  + Incident configurations
  + Correlation rules
  + BIOC
  + Host Insights
* Endpoints section.
  + Endpoints
  + Endpoint Groups
  + Agent installation
  + Policy Management
* The lower section contains settings and quick launcher(search).
  + Setting broker VM

There are two places managing Authentication and Authorization.

1. Customer Support Portal handling Authentication and Authorization related to instances. To access the xdr management console you need to first have access to xdr gateway.
2. Cortex XDR gateway handling authorization i.e. roles for xdr.

## Agent Update options:

1. Update from management console.

2. Options to view and take action on failed agent updates.

3. Via Peer to peer updates, Broker Vm or cortex server (where server will push the updates to endpoints.).

## What is Broker VM and why is it used??

The Broker VM for Cortex XDR is a virtual machine that serves as the central communication hub for all Cortex XDR agents deployed in your organization. It enables agents to communicate with the Cortex XDR cloud service and allows you to manage and monitor the agents' activities from a centralized location.

The Broker VM must be connected to a network with internet access, and all Cortex XDR agents must be able to connect to the Broker VM over the network.

Advantages: Faster content updates, lesser traffic for content updates since many devices will take the content updates from Broker VM, Auto Updates and no management needed. you can deploy the Broker VM by following these steps:

1. Download the Broker VM image from the Cortex XDR cloud service. 2. Deploy the Broker VM on your virtualization platform.

3. Configure the Broker VM with the appropriate network settings, such as IP address, DNS, and gateway. 4. Activate the Broker VM by entering the activation key provided by the Cortex XDR cloud service.

5. Once the Broker VM is activated, you can start deploying Cortex XDR agents to your endpoints.

6. The Cortex XDR agents will automatically connect to the Broker VM and start communicating with the Cortex XDR cloud service.

## Content updates or Dynamic Updates:

These contain signature update, default configuration settings update, behaviour detection rules

update, Trusted signers, protected processes list etc.

Can happen in small chunks called minor update or all at once in Major update.

Recommended is to enable minor update.

Content updates can happen from peer devices in same subnet or from broker VM or from cortex server. This is the default order if not configured.

## Cortex Agent components

* GUI, CLI interface Cytool.
* Malware protection module,
* Exploit Protection(process injection etc.)
* Extensions( Device controls, host firewall)
* Endpoint data monitoring and uploading
* Communication module
* Metadata (like its registry entries, logs etc)
* Operating system kernel drivers.

## Communication between agent and Cortex XDR instance:

1. Https: agent will contact the instance for heartbeat, alerts data etc. Agent will initiate and then server will respond. Server cannot initiate connection since HTTPS is stateless connection.

2. Websocket-Based: server can initiate the connection using websocket since it is stateful and full duplex thus two-way communication is possible. Response actions like live response session uses this mode.

## Cyber Attack Chain: Cyber Kill Chain Model

1. Reconnaissance: gather info about the target
2. Weaponization: prepare the weapon, a pdf with exploit, an exe with trojan, a phishing mail etc.
3. Delivery: deliver it to the target via usb or email etc.
4. Exploitation: Runs the exploit code which will take adv. Of a vulnerability in the target
5. Installation: Install trojan, backdoor, reverse http connections, AutoStart, persistence, admin access etc.
6. Command and Control: start communicating to the malicious servers for data exfil or for additional malware delivery to the target.
7. Act on Objective: Success !!! Target compromised, data exfiltrated, files encrypted, image tarnished etc.

## Exploit Prevention Flow in Cortex

Some file🡪 OS finds an application to run that file🡪 OS initiate process creation → Agent injects libraries App opens and open that file exploit attempts to start executing agent detects and kills it and dumps its memory.

## Malware Protection Modules

Pre-Execution: specific protection modules similar to ASR→restictions for valid paths for running the files 🡪checks the file hash in wildfire or analyze unknown file in wildfire, local analysis and then block or allow as per result.

Post-Execution: triggers after pre-execution process created monitor process for behvaiour analysis, suspicious network/file usage.,

Mostly checks(password theft, ransomware, behaviourial threat patterns, network packets inspections)

## Data uploaded:

1. Alert related data generated and uploaded immediately.
2. Log data which is sent periodically every 5 mins contains all system resources, processes etc. which will help for behavioral threat analysis by SOC person.

## Hardening Endpoint Security

Extensions that reduce attack surface of the endpoint by providing additional security functionalities on the endpoint.

1. Device Control
2. Host Firewall
3. BitLocker Encryption

## Analytics Engine:

The cloud cortex xdr instance has analytics engine which can detect abnormal activities using machine learning models. It learns normal behaviour using supervised and unsupervised ML models through the endpoint log data and enhanced endpoint data from sources like firewall, syslog etc. and when an anomaly occurs it will generate the alerts.

## Data collections:

We can ingest logs in to cortex xdr from various external sources which will help in threat analysis and response actions.

Authentication logs: from Azure AD, ping, okta.

Firewall logs: from checkpoint fw/vpn, cisco etc.

Syslogs: in CEF, LEEF, csv, or log data in relational databases.

Windows event collection: data from endpoints Cloud logs from cloud providers.

From provided data, we can do manual analysis using XQL. or analysis is automatically done by Cortex during log stitching.

## Licenses:

Prevent: basic malware/exploit protection capabilities per agent installed.

Pro per endpoint: advanced protection, data collection and upload to data lake, analytics engine to detect behavior-based anomalies and response per agent installed.

Cloud per host: same as above but counts agent installed on public cloud. And Kubernetes supported.

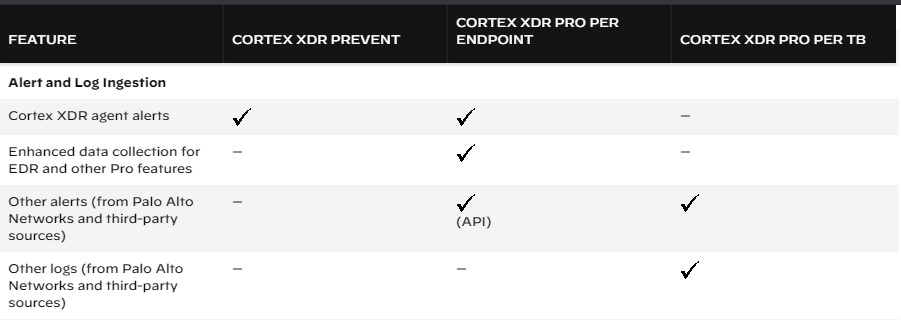
Pro per TB: provides network protection and response and based on TB of log and alert data stored. Number of agents can be unlimited. Log ingestion from external sources like firewall, azure AD, vpns etc

is only available in this feature.

Add-ons:

1. Host Insights: provides software inventory and vulnerability management.
2. Forensic addon.

Cortes XDR Features



**Exploit Protection Course**

Exploitation techniques will take advantage of a bug or vulnerability and try to execute malicious attacker's code. Multiple techniques can be used in one attack. E.g. (heap spray sql inject...)

Cortex detects and prevents exploit techniques and not individual attack patterns. Coz there will be thousands of individual attacks per year but only few new exploit techniques.

For unknown exploits if one succeeds the next one is blocked thus stopping the attack

Cortex does not need info about application functions and vulnerabilities to protect it. Not all processes are protected by Exploit protection module. If internal application wants to be protected, then it has to be tested out.

Cortex Xdr EPM has different modules that act as traps, whenever an exploit technique runs they detect it and block it.

e.g. if OS functions are used, then there are protected dlls which stop using of those functions if heap spary is used, then there is limit memory heap spray check module which will block it.

Cortex XDR Incidents Course

Groups multiple alerts, assets and artifacts which point to same root cause into one incident. One single attack with same root cause creates incidents. In cortex one incident can be assigned to one investigator and alerts cannot be assigned directly to anyone.

Artifacts are suspicious objects that cause the alert like IP, malicious file, process etc.

Alerts are grouped if they share the same causality instance ID i.e., may be same set of processes triggered both of these alerts etc.

**Alert Binding:**

How alert is linked to incident:

New alert arrives read cyber attributes of the alert like e.g. Cl instance, alert timestamps, initiating process etc. if there is an incident with same attributes then alert gets linked else new incident gets created.

If there are multiple incidents matching the alert attributes, then cortex uses degree of matching to bind the alert to the most matching incident.

**Creation of New incident:**

If a incident has too many alerts associated with it based on predefined threshold by cortex team, then if one more alerts comes up, then that will create a new incident.

Max 1000 alerts per incidents are allowed. This is because if incident has so many alerts then it will be matching with many incoming new alerts thus making it difficult to add alert to actual incident.

We can move alerts between incidents as per our analysis.

Only Medium, high and critical alerts create incidents. Some exceptions cases low alerts can also create them. Informational alerts and low alerts are attached to incident as Insights but they don't create an incident.

Options available in incidents: merge incidents, starring, change status, change severity, manage incident

Options available incidents: merge incidents, ents, starring, change status, change severity, manage incident score automatically applied by defined rules or manually apply). in

Incident severity: low, medium, high, critical

Alert severities: informational, low, medium and high.

Incident scoring: helps prioritize incidents. Manual and automatic via user defined rules and smart scoring which works when cortex xdr analytics is enabled and scoring is done by the system.

Score is assigned to the alerts not for incidents which applies it to the incident indirectly.

**Malware Protection Course**

We can configure malware protection modules MPMs in Malware profiles security settings.

There are options to audit (report) /block or disable different type of protections like behavior protection, child process creation, ransomware protection, password theft, credential gathering protection, office macros protection etc..

Each of them have a separate allow/block list where a file would be whiteslisted only from that particular behaviour.

Some modules are triggered pre-execution and some are for post-executions.

Each of them have a separate allow/block list where a file would be whiteslisted only from that particular behaviour.

Some modules are triggered pre execution and some are for post-executions.

Pre-excutions implies the module will block the file from running, Post executions MPMs will kill the process.

Pre-execution flow:

Some file MPM e.g child process creation specific allow locations wildfire lookup execution modules gets triggered. access restrictions local analysis→ ie blocking running of files from os creates process to run the file post

The access restrictions are defined in Restriction Profiles and not in malware profiles.

Allow list is an ICC which will allow certain files to run, we can find this in malware profile assigned to the endpoint and navigating to PE/DLL examination section.

Or we can view it in Action center allow/block list..

Pre-exection allow or block is decided in precedence as Admin verdict wildfire local analysis WildFire analysis has two services: 1. File Analysis service which does static analysis, dynamic analysis, heuristics analysis, baremetal VMaware analysis and then 2. verdict via verdict service.

If due to network issue, wildfire lookup is not reachable and we get unknown verdict then LOCAL analysis is triggered which uses ML to determine if file is malicious or benign,

Cached Verdicts:

The xdr agent on the endpoint maintains a cache of verdicts of previously examined files in memory and saves it to disk for persistence. The cache is updated if admin creates a verdict override using allow/block file from console. OR when endpoint scanning is triggered.

If a file verdict is not found in the local cache database, only then the xdr agent will do wildfire lookup and if that fails then the verdict is obtained from local analysis as discussed above.

Verdicts;

Malware, Benign, Grayware: allowed by cortex by default but admin can edit malware policies to block the grayware verdicts as well(treat grayware as malware). These are file which have behaviour similar to malwares but are not malicious.

Malicious files are quarantined and can be restored using console or cytool. Xdr agent cannot quarantine files from read only drives or Encrypted file system or network drives.

Allow List contains list of files and folders that are allowed to

Signed Executables

Allow List: trusted signers: maintained by cortex and by User in malware profile. Before wildfire.

Block List: Untrusted Signers: maintained only by cortex updated by content updates. Before wildfire

Allow List: Known Signers: maintained only by cortex updated by content updates. Checked after wildfire.

**Behaviourial Threat Protection:**

Triggered post execution. BTP rules are downloaded via content updates. They continuously monitor endpoint for suspicious activity and generate alert when suspicious behavior matches the RULES set. They monitor all resources on the endpoint and changes made to the endpoint to detect the attack.

A rule would be sequence of steps that are performed by a process which are mostly followed by malware. E.g. Disable UAC, create a hidden file in system32 folder, update autoruns, create PE or script

They monitor endpoint for suspicious activity and generate alert when suspicious behavior matches the RULES set. They monitor all resources on the endpoint and changes made to the endpoint to detect the attack.

A rule would be sequence of steps that are performed by a process which are mostly followed by malware. Eg. Disable UAC, create a hidden file in system32 folder, update autoruns, create PE or script file., connection to internet to a malicious site.

It can also block malicious drivers from endpoint.

**Office Macro examination:**

Checks office macros, examination is same as for PE and DLL files. i.e. cached verdicts, wildfire analysis, local analysis as per settings.

\*\*xdr calculates hash of the macro and not of the file in the cache. So if documents data change, the hash of the macro will not change. Does defender have this??

If local cache does not have it and hash is unknown to wildfire, then whole document is used for wildfire analysis. Since sometimes, document data can be malicious IP, domains which could be needed for wildfire analysis.

**Malicious Child Process creation**

Blocks malicious child process creation from known targeted processes. E.g. office apps from launching powershells etc.

This does not scan macros for malicious activity. Only checks about child process activity.

\*\*Allow list contains parent process, child process and the allowed command line path to be input to allow the operations.

**Ransomware Protection:**

Creates decoy files fake files to attract ransomware, when it acts upon it, the ransomware is blocked. behavioral analysis helps protect actual files. Also these decoy files are kept in different places in file system and It is in places where ransomware looks first.

Password theft protection: helps prevent from mimikatz, and other credential theft tools.

Block malicious causality chains: block network connections of suspicious Causaulity group owner.

**Endpoint Scanning:**

Periodic and on demand.

The endpoint scanning does not use path restrictions and child process creations etc. and local analysis which normally runs after wildfire.

It only check allow paths, admin verdict, trusted signer, untrusted signer, wildfire, know signer. Checks.

To quarantine or not it decided by Malware protection settings.

**Automation Rules Course**

Similar option is available in defender but only for Custom Detection Rules which create alerts in defender, there we have some options like collect investigate package, isolate device, restrict app execution, allow/block file etc.

Automation rules are rules that can be created by us. If the rule conditions match, they will get triggered when a new alert is created. They can do some action like e.g.: send an email, assign the incident to someone, isolate an endpoint etc.

Applies only to new alerts not to existing alerts.

Categories of action available are Communication (send email, slack msg, syslog fwding)

Or Alert/Inc mgmt. (assign incident, change alert status, change alert severity)

Or Endpoint Response Actions like (isolate endpoint, collect file, start a scan, run a script)

They are scope-based access controlled i.e. we assign tag to endpoints and group endpoints using the tag.

We control access to the rules somehow..\*\* need to explore. Permissive mode, restrictive mode etc.

Stop processing after this rule it will not process any other rule that matches same condition. This is based on Rule order. Rules on top are processed first. if stop processing rule is disabled, then all

This is based on Rule order. Rules on top are processed first, if stop processing rule is disabled, then all rules that match a criteria will be processed.

Automation Audit log we can view all the processed rules, failed rules etc.

**Response Actions Course**

What endpoint response action we can take using mgmt. console are mentioned in this course.

1. Collect file

2. Collect logs

3. Isolate endpoint

4. Terminating a process

Alert Causality Course:

Causality node types:

User, Process, Alert.

Labelling of nodes

Red Node Malware, Blue Benign,

Yellow grayware

greyed out unknown, inconclusive.

Timeline view shows data only if alerts are stictched. It has timeline, process selection pane, alerttype

Alerts contain minimal information of the suspicious activity.

Logs can be any data not related to an attack. E.g. of logs include: enhanced endpoint data collected by

Xdr agent, firewall log data or authentication logs on the endpoint.

inced endpoint data collected by

Logs can be correlated with Alerts. This enhances the data available in the alerts and helps in the analysis. This is know as Log stitching

For enhanced endpoint data(EED) Xdr agent monitor OS operations, collects logs, data sampling, compressing and uploading logs. This is there only for PRO agents.

The EED can be enabled in agent profile settings.

Data collected in EED includes process operations, file read write, Registry changes, network, windows event logs etc. Raw logs can be accesses via xgl.

Alert is sticthced if it has CGO name or some causality related information.

Attack region in causality graph shows processes that were in the attack.

Cortex xdr analyzes the collected data using ML and shows only processes that were in attack.

A list of spawners are identified and updated by content updates. They generally create child processes. It is used in causality instance analysis. E.g, spawners in windows: explorer.exe, services.exe etc.

Cortex XDR Analytics Engine detects hidden and post intrusion threats that evade network defenses. It

Alert is sticthced if it has CGO name or some causality related information.

Attack region in causality graph shows processes that were in the attack.

Cortex xdr analyzes the collected data using ML and shows only processes that were in attack.

A list of spawners are identified and updated by content updates. They generally create child processes. It is used in causality instance analysis. E.g, spawners in windows: explorer.exe, services.exe etc.

Cortex XDR Analytics Engine detects hidden and post intrusion threats that evade network defenses. It first learns normal behavior and then detects anomaly using Behavior Analytics compared to normal behavior of user, endpoints, networks.

Settings configurations analytics

Cortex XDR analytics Engine Behavior Analytics

Detectors (type of behaviors based on which alerts gets created).

Detectors Updated by content update.

Anomaly detection by learning normal behavior using log data.

Needs 30 devices data over two weeks and then only it can be enabled.

Behavioral Threat Protection in Malware Protection Madules

BTP rules.

BTP rules Updated by content updates

Common malware behaviors like registry change autoruns, disable UAC etc.

Can work directly, does not dependent on log data.

**Agent Installation:**

Agent can be installed using package downloaded from the cortex Xdr portal.

Before the download, you need to create the package in the portal.

**Policy Management**

We have 5 types of Prevention profiles. They are

1. Malware: action to be taken on detected malware and known unknown malwares, endpoint scan schedule. E.g.: exe/dll malware, ransomware protection, block office macros, endpoint scanning, Behaviour Threat Protection settings etc.
2. Exploit: settings to prevent browser and OS exploits.
3. Restriction profile: restrict executables from some folders and restrict devices etc.
4. Agent Settings:, content update settings, UI restrictions to users, source for content update, uninstall password, agent security(tamper protection), agent upgrades, agent proxy settings etc.
5. Exception: exclusions .

In all these individual settings we have an option to add folder/file exclusions as well. Like individually in malware profile we can add exclusions in exe and dll tab and then in next tab office child process we can add different exclusion..they apply only to that particular module and not for all modules.

In defender it is complete single exclusion.\*\*

Deploy profiles settings using policy rules: we can select which to deploy and rest will be default.

Thn we select endpoints.

Cortex xdr Endpoints Policy management policy rules

Profiles define the settings and then Policy Rule section can be used to apply it and deploy it to the endpoints.

**Broker VM**

Acts as a proxy

Acts as content cache.

It can also act as a syslog collector or windows event collector. For this we need to have Cortex XDR pro per GB license which is needed for log ingestion into cortex xdr.

Steps:

• Download broker VM image and install in your environment.

• Enable Agent activation where we configure what broker vm will do..i.e. Content cache for updates and proxy. Or any one of them

• Whichever policy rule applies to the endpoint you are installing agent on, you update the download source to broker vm and select broker vm. Aplly this policy to the endpoints.

• Then install the xdr using the package by mentioning proxy list in the installation command.

• Agent should be showing up on console and also the broker vm managed agents should also be populated(in settings broker vm).

**Endpoint Groups**

Why we need them?

• For scope based access control ..same as in Defender. Allow users of specific groups to access only specific Endpoint groups and not all endpoints.

• To filter and apply policies using endpoint groups instead of selecting manually or filtering criteria in the policy rule.

Endpoint groups are of 2 types. Static and dynamic.

Static means you select individual endpoints you want to add to the group.

Dynamic means you define a filtering condition like OS, Name contain etc.

**Correlation Rules:**

Correlation  correlating the logs and then generating the alerts if they match. Written XQL

Some action will be taken if they match. Timing how often the rule should run.

Option for alert suppression to suppress the alert for some cases . e.g. may be for some user if you want.

Agent Token

This is the agent uninstallation password or password which can be used for temporary troubleshooting at the endpoint.

e.g. disable some agent functionality using cortex xdr cli tool : cytool . then install some app. Or disable some functionality and then see if cortex xdr was the cause for performance issue or blocking etc.

The token is rotated every 2 weeks for each and every endpoint. We can also create a temporary token other than the actual token which can be valid only for some hours. E.g.: you share it with some support executive for some actions/troubleshooting.

You can retrieve it from portal only. You can query the token on endpoint using “cytool query token” but it will show only hash. And plain text can be retrieved from portal only.

Host Insights

This is an add-on on top of cortex xdr pro license.

This setting can be enabled for endpoints by using Agent settings Profile.

Path: cortex xdr endpointsPolicy Management profiles Agent settings profile \_-> tab cortex xdr pro capabilities.

Once you enable host insights in the profile and apply that policy to the endpoints via policy rule. Those endpoints will report host insights related data to the cortex xdr. The update on data happens every 24 hours.

What details does this give:

All the below in screenshot. E.g.: application, vulnerability, autoruns, drivers, sysinfo, local users whose credentials are saved on endpoint and not the domain users, users to groups (domain users) etc.

**Device Control**

Helps control which devices can be allowed on an endpoint and which are to be blocked.

Needs to be created using Policy Management Extensions ProfilesDevice Configuration.

Here we can allow or block device types like Disk Drive, CDROM, Floppy etc. We can also add a custom device type by adding a GUID of the device class. Each device will have a unique GUID assigned which can be used to identify the device class e.g. USB will have unique GUID, HardDisk will have unique GUID, CD will have unique GUID etc.

If you want to add some exception to some vendor device. E.g. you want to allow sandisk usb and block the rest, then you can do that using Device Exceptions profile.

Then we need to apply it to devices using the policy rules and adding device configuration/exceptions profile to the policy rule.

**Host Firewall**

Host Firewall Rule Groups: here we create the firewall rules.

Endpoints Policy managementExtensions Profiles Host Firewall. Here in profile we define if the rule groups we select applies to internal or external networks. Whether they can block it as mentioned in the rules or we can say override. Then in policy rule we apply these settings and rules to selected/queried endpoints.

# Defender For Cloud

It is a CNAPP: could native Application protection platform.

Its capabilities include:

1. DevSecOps: Defender for Devops which helps manage security of code mgmt. environments and code pipelines across multi-cloud and multi-pipeline.
2. CSPM: shows actions that can be taken to improve security posture of the cloud.
3. CWPP: cloud workload protection provides protection from threat and vulnerabilities mgmt. for servers, storages, container etc.

• Azure Defender i.e., the CWPP part and Azure Security Center i.e., CSPM part. Both combined make Defender for cloud.

When enabled for first time, we need to assign default security policy so that defender for cloud can assess the devices as per policy and show secure score and recommendations. Else secure score will not show.

The default policy is Azure security benchmark which has 200+ policy definitions, security. configuration which are checked against. Individual policy will have some non-compliant resources so for those resources we will have recommendations.

Recommendations are grouped into categories called controls.

**Data Flow in DFC:**

1. Log Analytics Agents Installed in windows, Linux resources collect events data and security configurations.
2. The data is sent to Log analytics workspace using port 443.
3. DFC takes the data from LAW and performs advanced threat analysis(threat intel, anomaly detection, behavior analytics).
4. DFC provides recommendations for enabled policies and alerts based on the analysis performed.

**Defender for Cloud JIT VM access:**

Main goal for defense is Reduce Attack Surface. It can be any security control or vuln. Remediation. It will eventually reduce the attack surface and secure your resources.

JIT protects VM from unauthorized network access. Protects the most common ports that are used for. Example ports: 3389-RDP, 22-ssh, etc. It will close those ports blocking inbound traffic and only open them for legit users for specified period.

• It will ensure that block all inbound traffic rule exists in NSG and azure firewall of the VM so that the ports are blocked. This is checked last and has least priority

If there is specific rule that allows these ports then ports are allowed else port would be blocked.

Then JIT would add a rule with greater priority in NSG which would block these ports. Even if an allow rule exists it would be blocked.

When user request access to VM, JIT will add an allow rule temporarily with even higher priority in NSG to provide access for specific period of time from that IP address. After time expiration, it will restore NSGs and Firewall to previous state thus blocking the ports.

**Agents of defender for cloud:**

1. Direct Agent an exe or msi file for log analytics agent or Microsoft Monitoring Agent (MMA) which can be deployed using common deployment tools like sccm, intune etc or installed manually.

2. Log Analytics Agent Extension the extension will install the agents on the deployed Vm. Option to deploy Log analytics agent extension are:

Automatic Provisioning option which will deploy agent to the vms automatically as it runs every 15 mins and can deploy to New discovered resources. But no option for exclusion of any VM in this method.

o Manually select a VM and then connect it to LA workspace which will install the extension. But its manual process and need to do this for all resources. New resources are not discovered and need to be done. Provides an option for exclusion of few resources.

Via SCCM or SCOM which are deployment tools.

o By creation of Azure Policy to install the log analytics agent extension. And applying that policy to management group or subscription or resource groups. Also works on VM scale sets whereas the above ones won't work on them.

• ARM template so that the agent is deployed when the VMs are created.

Recommended by Microsoft to use the Log analytics Agent extension since it keeps the agent up to date and has option to manage/update/remove via azure arm templates, cli, PowerShell etc.

**Azure Monitor Agent:**

Previously Log Analytics Agent is used to send log data to Log Analytics Workspace. There are solutions that work on those logs. There are other agents like Diagnostics Agent which sends diagnostics data to Azure Monitor. For Log analytics agent, configuration on what type of data logs need to be collected was configured from Log Analytics Workspace Agent configuration.

The Azure Monitor Agent configuration is done using Data collection Rules present in Azure Monitor. We

**Azure Monitor Agent:**

Previously Log Analytics Agent is used to send log data to Log Analytics Workspace. There are solutions that work on those logs. There are other agents like Diagnostics Agent which sends diagnostics data to Azure Monitor. For Log analytics agent, configuration on what type of data logs need to be collected was configured from Log Analytics Workspace Agent configuration.

The Azure Monitor Agent configuration is done using Data collection Rules present in Azure Monitor. We can create multiple rules and they can be used to forward logs or diagnostics to the LAW. Or only diagnostics data can be sent to azure Monitor.

**Azure Policy**

Defender for cloud is built on Azure Policy. We have Policy Initiatives which can be assigned to resources/subscriptions/management groups using policy assignments. These Initiatives can be assigned to defender for cloud and show up as recommendations.

Default Azure/Microsoft Cloud security Benchmark has around all policies in audit mode.

Defender for cloud is built on Azure Policy. We have Policy Initiatives which can be assigned to resources/subscriptions/management groups using policy assignments. These Initiatives can be assigned to defender for cloud and show up as recommendations.

Default Azure/Microsoft Cloud security Benchmark has around all policies in audit mode.

An Azure Policy is a set of rules/conditions against which resources are checked. If any resources match

the condition, then some action i.e., Effect will be taken on those resources. Helps to evaluate resource compliance against specified settings or enforce organizational policies to block deployment of non- compliant resources.

Azure Policy vs RBAC: Le. RBAC controls if user has access to do some action or not on a resource. Whereas Azure Policy will block creation of non-compliant resrource if it is defined in policy and event if user has permissions to do so in RBAC.

**Effects in Azure Policy:**

1. Modify: modify a resourc
2. Append
3. Deny
4. Audit
5. AuditifnotExists
6. DeployIfNot Exists
7. DenyAction
8. Addto Networkgroup

**Deny and Enforce a Recommendation**

On a recommendation, we have option to DENY or ENFORCE it on unhealth resources.

DENY: it will block creation of new unhealthy resources.

On a recommendation, we have option to DENY OF ENFORCE it on unhealth resources,

DENY: it will block creation of new unhealthy resources.

ENFORCE: it will create a DeployIfNotExists policy and remediate the recommendation if there is non- compliant resource.

Quick Fix: This is not available for all recommendations. But for few recommendations Azure has ARM template already. So, if you want to fix a unhealthy resource, then once you click quick fix then it will assign that remediation policy to that resource and that resource will get remediated.

**Log Analytics Workspace:**

Type of logs: Analytics Logs and Basics Logs

Analytics Logs: A table in LAW can be set as basics of Analytics. The price of Analytics Log is higher per ingestion of GB of data and lower for Basics Logs. But Analytics Logs are retained for 30 Days and can be extended to 90 days with sentinel enabled or 2 years with additional exports. Whereas for Basics Logs they are retention period is only 8 days with 22 days of archive period after which they are removed. The charge of data ingestion is less and we also pay for Kusto query run on basic logs.

Analytics Logs: A table in LAW can be set as basics of Analytics. The price of Analytics Log is higher per ingestion of GB of data and lower for Basics Logs. But Analytics Logs are retained for 30 Days and can be extended to 90 days with sentinel enabled or 2 years with additional exports. Whereas for Basics Logs they are retention period is only 8 days with 22 days of archive period after which they are removed. The charge of data ingestion is less and we also pay for Kusto query run on basic logs.

You can set any table in LAW you want to Basic or Analytics Log type. If some Log is not needed for more time then we can save the money using Basic Log Type.

**Security Policies and Recommendations**

Azure policy definitions are rules that the resources should comply with for maintaining security of env.

Group of Azure policies are policy Initiatives. They group together policies logically.

Default initiative assigned with DFC is Microsoft cloud security Benchmark. We can view edit and disable some of the policies in this initiative as per need.

We can create custom initiatives and assign them to subscription having DFC. Then we will get recommendations if resources don't comply with the policies.

We can add regulatory compliance standards to the subscription to monitor the compliance with standards or regulations.

Recommendations are generated by periodically evaluating the resources against available/enabled initiatives. Each initiatives will have multiple policies. After analyzing the policy DFC, will find misconfigurations and security issues and provide the recommendation if some resource doest not comply.

If you want to disable a security recommendation, we can go to environment settings->security policy page and then select initiative. And then for that recommendation select Disable Effect (these are called policy effects) to disable. If you want to enable some recommendation, then select Audit Effect.

Deny effect will deny the action. Example: deny creation of Vm with 4 cores. Then deny effect will block that creation ie, it will enforce that policy. Audit will only make note of violation and then it will show in recommendation that there is a Vm with 4 cores etc. but Deny will stop that violation right away.

In Defender for cloud recommendation, there is option in recommendations as below

Exempt: exempt this setting becoz it was remediated or may be it was accepted risk. This can be done from policy or by selecting a unhealthy resource in recommendation.

Open Policy Definition; to view the policy definition.

Deny: Audit policies-based recommendations will have an option to enable Deny affect so that new resources created through this would enable this setting by default.

Eg: storage should use secure transfer only i.e. https: this can be set to Deny so that if someone creates a new storage account then they need to enable https and only then they will be allowed to create the resource else it would be DENIED,

Enforce: for

Auditifnotexists policies we will have option to use be compliant. deploy if not exists. So new resources can

E.g: Vms should have antimalware installed. Now if we have this policy in auditifnotexists, then we will have enforce option.

The quick fix remediation of recommendations can be view in Azure Policy Remediation Task tab section.

**Governance RULES:**

This can be created so that specific type of recommendations can be assigned to owners and reminders about their mitigation and SLA are sent to them.

**Defender for Storage**

Protects Storages from potential threats.

Can be enabled on subscriptions or per resource.

Individual resources can be excluded from the storage plan.

About Azure Storage

Used to store different kinds of structured, unstructured, semi structured data.

SLA would be of 2 types:

Resiliency, availability i.e. ability to access the data. This is lower 4 9's.

Durability, Redundancy ie, actual data loss. This is dependent on type of storage i.e. LRS, GRS, ZRS etc. with 9 9's, 12 9's 16 9's etc.

Types of Redundancy:

* Locally Redundant Storage: 3 copies of Data are stored synchronously in the same data center in the same region.
* Zone Redundant Storage: 3 copies of data synchronously copied to 3 availability zones in the same region.
* Geo Redundant Storage: 3 copies of data in primary region using LRS and then 3 copies of data asynchronously copied to the secondary region as LRS.
* Geo Zone Redundant Storage: 3 copies of data in primary region using ZRS and then 3 copies of
* Zone Redundant Storage: 3 copies of data synchronously copied to 3 availability zones in the same region.
* Geo Redundant Storage: 3 copies of data in primary region using LRS and then 3 copies of data asynchronously copied to the secondary region as LRS.
* Geo Zone Redundant Storage: 3 copies of data in primary region using ZRS and then 3 copies of data in secondary region using LRS.
* Read Access for GRS and GZRS: same as above but read access is provided to the data in secondary region as a failover if the primary region fails.

Block Blobs object level replication using replication rules

Here we can define replication a container and its connec

**Why we need Defender on Storages?**

Someone can upload a malicious file to storage and then that could get downloaded and distributed to your organization endpoints. Thus, causing attack, compromise of endpoint etc. etc.

Data Exfiltration: Storage account could be accessed by unknown users and cause data exfiltration

sensitive data leak.

Data Corruption: Storage can be encrypted, or data can be deleted.

Issue with Traditional Security Solutions:

Storage account is not a VM on which some security solution can be configured or installed.

3rd Party solutions would upload the same data to their resource and then provide results. They may sometimes act as proxy through which you upload data and then data comes to

storage account.

They may not be able to perform comprehensive activity monitoring ie log monitoring and those may cost high.

Latency and performance issues due to 3 party solutions.

How Defender for storage works or prevents the above

1. Agentless malware scan on upload (add on)
2. Sensitive Data Discovery and Threat Detection
3. Activity Monitoring (Log Analysis and Alerts Generation)

**Malware Scanning:**

It uses Defender Antivirus capabilities for scanning the files. Create a blob index tag on each file with the malware scanning result.

Generates alert in Defender for cloud alerts.

Use cases: we can create a logic app to delete a file identified as malware on the storage. Or move it to a different container with restricted access to users, so it can be verified if true positive and then remove it.

**Agentless Malware Scan**

Copies the data to an isolated environment and scans for malware. The data is not stored to disk and is only in memory and the environment is deleted right away after scanning.

**Sensitive Data Discovery:**

Defender for storage will be able to learn about sensitive data stored.

**Defender for Cloud Apps**

A security solution that is on-premises or cloud-based solution which sits in between cloud application user and the cloud application service provider and monitors and enforces organization security policies.

3 main components or functions of a CASB solution:

1. Shadow IT Apps discovery: discovering applications that are not approved by the IT team but used by the users.
2. Threat Protection: protecting the devices/networks from malicious entities that could be from download of files or unusual behavior etc.
3. Data Loss Prevention/Information Prevention: classify sensitive information and Prevents leakage of confidential data using DLP policies.
4. Compliance: tracking compliance with standards.

**Defender for Key Vault**

Key vault is an azure resource used to store and secure secrets, keys and certificates.

Key Vaults concepts

Key vault stores 3 types of data:

1. Secrets: these do not have any format . we write them we read them from the vault.

2. Keys: these are public private keys. They have a format defined. Azure has RSA and Elliptic Curve EC keys. We can export the public key. But we cannot view or download the private key. The operations are done within key vault using private key whenever required.

E.g: user sends some encrypted data, the decryption happens using private key

3. Certificates: these are the certs used by web applications. We register them from CA(digicert and globalsign are supported by azure), they expire and renew aka Certificate Lifecycle. They are sent to resources. Private key needs to be safe. Public key is shared via the certificate.

**Key vault licenses**

Licensed based on number of keys and operations performed in the key vault.

1. Standard: means software-based keys.

2. Premium: HSM supported keys. The hardware stores and performs cryptographic ops on the key. Keys only are HSM supported. Secrets and Certificates are still software based.

There is other option called managed HSM: where the HSM partition is dedicated for the customer. This one also supports AES(symmetric crypto) other than RSA and EC(which are asymmetric).

**Access Control**

The permissions to view keys and create them can be handled by using 2 models.

1. Access Policies which are old method. Where we can define a user, Managed Identity permission to the key vault to perform read or write operations etc. But these are not granular. If you give permission to a secrets in key vault then you are giving permisisons to all the secrets. You cannot say : keyvault1, clark userssecret1: read/write, secret2: no access.

You will be given access to all secrets or no secrets. Same applies to keys and certs as well.RBAC provides granularity.

2. Role Based Access control: we can provide roles to users or Managed Identities to access the key vault. On individual secrets or keys we can block or allow a user access. Its more granular. Recommended.

With RBAC we can also use features like MFA, conditional access or PIM etc for extra security.¬¬¬

When an user/azure resource accesses the key vault it first needs to proves its identity. This is done by Managed Identity of the azure resource e.g. azure VM will have a system managed Identity which allows it to authenticate to the key vault directly. For a user it would be his ID/password.

For Onpremise resources if they are using key vault, then they can be azure ARC enabled which helps them to have a managed Identity and then provide access to key vault. If they are not then they should be service principal which needs to authenticate using password or certificate to azure key vault. That pwd and certificate management needs to be done onprem only using some vault tools coz if some on prem application is using this then we cannot put cert/pwd in config file. So we need on prem management of that and then once we authenticate we can do operations that are allowed in key vault.

**Firewall and Networking in Key vault**

We can allow/block specific virtual networks or subnets access to key vault. We can allow certain public Ips access to the key vault. We can add an IP which will be given access to key vault.

This is called service endpoint or private endpoints. We need to enable the service endpoint at the resource level e.g at VM. And then add that VM in key vault networking. This allows VM to access the key vault. If that VM has RBAC defined in access control only then it will be allowed operation. The networking part is only for network access. The RBAC defines the authorization the VM has on the key vault.

**Backup**

Key vault data can be backed up in same security world as the key vault. Security world i.e., same country as the key vault. E.g.: key vault in east US, then we can backup to any region in US. But not to Canada or another region.

In general, replication done by azure is in region pair. E.g., East US has region pair Central US, so key vault is replicated for redundancy to region pair. The backup part is done by the customer according to his needs.

**Soft Delete and Purge Protection**

Soft Delete: If key/secret or cert is deleted, it can be recovered as it is stored for 90 days as part of soft delete.

Purge protection: A malicious user can delete a key and then delete the backed-up key as well. That is why we have purge protection it does not allow to remove keys completely(purge) and they will be there for mentioned 90 days max or less as mentioned by the user during key vault creation.

Enable Audit logs i.e. diagnostic logs which can provide in depth details of access to the key vault and action performed in key vault.

**Microsoft Managed Keys vs Customer Managed Keys**

For encryption of data at rest feature, the Microsoft managed keys are used where Microsoft will handle the key update and management for storage account or VM etc.

We also have option of customer managed keys where we can use key vault to store the keys. These are to be updated, rotated and managed by us. If a new version is available some resources like storage, Vm they can take latest version automatically. For some resources like SQL, we need to configure the resource to use the latest version of the key manually else it will use the older version.

**Defender for Key vault Alerts**

It provides recommendations and alerts on any action performed on key vault.

These can be seen in Defender for cloud for entire key vaults or

For key vault account specific we can see in the key vault account pagesecurity or alerts.

The fields available on the alerts depend on the type of alert. Like if application is involved then userprincipal i.e useriD won’t be there, if an application is involved then it will have Managed identity. If alert is due to external network not from within azure then there will be no objectid

e.g. of Recommendations:

• key vaults should use soft delete

• Key vaults should use purge protection

• Key vaults should allow rotation of keys in certain days etc.

Alerts:

• Suspicous Access to key vault from suspicious IP

• Access to key vault from TOR exit node

• Access denied to key vault

• High volume of operations on key vaults etc.

How to handle these alerts

• Verify the source of the access i.e IP/user/application. Is it internal or external. Verify with that user or application owner if it is known application or user.

• If it is unknown user/IP then verify the firewall/networking configurations on the key vault. Make sure only valid users/application or Vnets/subnets are allowed to access it.

• See what was access or what action was performed: Look at the alert and diagnostics logs and see what was accessed and what actions were performed. Update RBAC permissions to the key vault if illegit users/applications were able to access the key vault and perform actions.

• Take Action: The used secrets or keys in the alert should be deleted and changed or rotated.

• If the compromised keys were used by some application, ask the application team to further check for any Indicators to mitigate them.

# Qualys

**Qualys VMDR**

Qualys Asset Inventory Management

Vulnerability Management

Qualys Patch Management

Qualys VMDR Course

VMDR Lifecycle:

Asset mgmt.: (Discover and Manage Assets in org)

→Vuln. Mgmt: (scan the assets for vulns)

=

→ Threat Detection and Prioritization: (prioritize the vuln findings by risk associated with their known threats)

→Response: Remediation: (patching) and repeat

→Response: Remediation: (patching)

and repeat.

\*\*Risk associated with Iknown eat means: some vulnerability will say remote code execution. So threat event is an activity that can have harmful/adverse impact on organization. So that is the threat and based on known severity we can prioritize them. that

Types of scanners:

Remote scanners: scans public facing devices

inside network, can be physical or virtual and scans local IPS Local Scanners: sit inside network, can be

Cloud Agent: installed on a device and scan it

Passive Scan Scanner: sniffs network traffic help discover unmanaged assets/new assets in the network

Cloud connector: helps to connect to avis or azure cloud and help show misconfigurations

SAAS CO

connector: helps connect the saas application and shows misconfigurations.

Container Sca Scanner: gets downloaded as docker image and installed as container application and helps show vulnerability and misconfigu rations in new docker images and containers.

Out of band scanner; inner; helps helps to to scan air-gapped networks.

• Apis collect data from 3 party

Cloud Agents

Devices contact Qualys cloud platform using outbound port 443.

There are Qualys scanners which can scan public facing devices and provide the vuln data to us.

the devices These do not have any installation on t we are scanning

Qualys cloud Agents are installed software on devices which will scan it for vulnerabilities based on configured timings and report data to Qualys cloud platform. The agents can be used to scan devices which cannot be reached by the qualys scanner.

The cloud agents provide vuln. Mgmt., patch mgmt., edt, file integ monitoring, policy compliance

VIB

Cloud Agents

Devices contact Qualys cloud platform using outbound port 443.

There are Qualys scanners which can scan public facing devices and provide the vuln data to us.

These do not have any installation on the devices we are scanning.

Qualys cloud Agents are installed software on on devices which will scan it for vulnerabilities based on configured timings and report data to Qualys cloud platform. The agents can be used to scan devices which cannot be reached by the qualys scanner.

The cloud agents provide vuln. Mgmt., patch mgmt., edr, file integ monitoring, policy compliance on the device installed.

AgentID is the DeviceID which is unique GUID generated for a device.

You can have agentless scanning by adding Ip addresses or range in the VMDR Asset-> address mgmt. tab.

If both agent is installed and Ip address is added for scanning in VMDR then that device will have duplicate data. To have them merged we need to enabled correlation of data.

Activation Keys

used during installation of the cloud agent on the device.

We can add tags to the key, so that agents that are deployed using this key will get specific tag This is can effective for grouping the devices logically.

We need to select the activation key and from there download the agent, since the install command will be different for each act. Key. And tagging group purpose.

Install command is something like qualysagent.exe activationkey abc customerid=xyz webserviceuri-qualyscloudurl. This would install the agent and configure it appropriately.

UnAuthenticated Scan authenticated scan Agent based scan:

Many orgs use Unauthenticated scan together with agent based scan. But issue was duplicate data. Thus qualys has unified vulnerability view which will merge the data for same asset from an unauthenticated scan and agent based scan.

To enable this we need to accept agent correlation identifier which allows qualys to merge the data.

We need to create a configuration profile in the cloud agents page configuration profile>enable scan agent scan merge, so that we allow an unauthenticated scan to read the installed agent GUID from the device during the scan.

After that we see unified view of the both the scans.

Qualys Asset Management

Global Asset View FREE) and Cyber security asset management(PAID)

GAV: Discovers assets, provides normalized\categorized data, defines criticality and tagging.

Normalization/categorization means from raw data Qualys provides readable data. But advanced asset. information is given only by CSAM. Like EOS date, license type etc.

CSAM: does all that GAV does and unsupported eos software hardware, unauthorized software, assets

that need attention, custom reports, integration with CMDB(config. Mgnt. database SNOW) Path to view assets inventory: CSAM→Inventory. Here we can view all the assets in our enw and also the softwares in software tab.

Tagging

CSAM-tags

Helps in tagging assets based on criteria. There are system defined tags and user defined tags.

E.g.: Cloud agent tag is attached to devices where cloud agent is installed. It's a system tag.

Similarly we can create a tag to group devices from a location say UK. Using the IP addresses. And then while initiating a scan we can just select this tag so that scan happens on these devices only.

we can then use it during initiating a scan or creating a report etc.

static tags need to be assigned manually and don't apply automatically to existing /new resources.

Dynamic tags can be applied automatically using the query criteria to all existing and new resources.

Asset Groups

VMDR assets asset groups

These are scannable hosts not having agents. A tag with same name will be created in CSAM->tags. Business impact high means tag will have 4 out 5 criticality score. We can edit accordingly as per business

Purging

Removal of stale assets that are not online anymore. They need to be removed as they negatively affect the security posture, accuracy of the datale.g. Ip reused and asset data might be incorrect), policy compliance, license cost etc.

Frequency: monthly to quarterly is recommended.

Purging removes:

Asset details

Vulnerability findings

Remediation tickets closed

Scanning data

Purge rules: CSAM→ rules

Purge rule can be created to remove using criteria of cloud agent based or cloud provided based metadata.

e.g. Cloud agent i.e. last time it checked in greater than 90 days.

aws ec2/azure vm status terminated or deleted for more than 5 days etc.

Assets scanned using Qualys scanner by IP/dns tracked or netbios tracked hosts cannot be purged using the purge rules.

For those assets, we need to go to VMDR-> asset search -> last scan not within 180. And then from the report actions select purge or purge all option.

Integration:

Qualys is two-way integrated with Service Now cmdb to update and get asset inventory data.

It is also integrated with JIRA for vulnerability remediation workflows.

Vulnerability Management

Knowledge Base

Path: VMDR Knowledge Base

The Knowledge base has details about all vulnerabilities.

The Vulnerabilities section in VMDR→ Vulnerabilties shows the vulnerabilities that exists in the environment in any of the hosts.

Confirmed Vulnerability: existence verified/confirmed through active tests,

Potential Vulnerability: one of vuln parameters was detected but we might need to be checked to be sure that they exist.

Half yellow/half red: If authenticated scan is enabled and it verifies the vulnerability(since authenticated provides more data compared to unauthenticated scan) then it will move the potential vulnerability to confirmed vulnerability.

I Information gathering category in KB are nothing but data that the platform needs eg version of linux or internet explorer detected etc.

Search lists are saved searches. Static list, dynamic list.

Static will have list of gid's we search.

Dynamic list will have a query eg cvss >9.0, product name contains abc, xyz etc.

Severity Level: 0 to 5.5 is highest risk and needs immediate attention.

Qualys Trurisk for vulnerability prioritization

Path: vmdr vulnerablities

QDS: Qualys Detection Scare which shows the impact of the vuln is based on CVSS and exploits of vuin. It is out of 100. QDR will reduce if mitigations are performed for vulnerabilities.

TruRisk Score: For each asset we have truRisk score based on the QDS and asset criticalility. It is out of 1000.

Formula takes weightage of the vuln by cvssle.g. 9.5 mean weightage 1,5 means weightage 0.6 etc), QDs etc.

VMDR Prioritization report we can search using asset tags and then create a report for prioritization.

Vulnerability Assessment

VMDR Scans Option Profiles

Option Profiles are the scan settings., ports to scan, authentication keys to use, performance settings etc.

VMDR Scans Authentication

Authentication tab will have authentication keys which can be used during a authenticated scan.

It will have the userid pwd to be used, which authentication protocol to use, which all IP addresses are eligible to use this authentication. Public key private key if applicable.

VMDR Scans scans: These contain the scan results as they are. And we can also create and launch a

VMDR Scans scans: These contain the scan results as they are.. And we can also create and launch a scan right away or schedule or run different type of scans from here. In this we can select the option

profile which we created which would provide the scan settings and then provide hosts which we are scanning. You can filter hosts by Ip

There is tab called schedules which shows the existing scheduled scan jobs.

Reporting

There are templates which can be created.

Host based finding: we get data from all scans and data from cloud agents and filter data by number of days. Filter by tags, Asset groups. Include them exclude them etc.

Scan based findings: get results from a specific scan that run, we may get all data.

Display options helps to include which all data we need on the report like vuln by severity, top 5 vuln, host details we need etc.

Filter: filter using search lists like search for adobe vuln. Or filter by operating system so report only contain windows data or linux data, vuln severity

Required unauthorized services, available servi it shows and if any unauthoriz running ont the host. If required service is not running any unauthorized services are running then it will show report. Similarly for ports.

User access: permission to run the template.

Actual report is run from Report tab. Report template based report.

Dashboards

We can create dashboards from existing templates from qualys. We can associate a dashboard with a tag and assign a user that tag so only those users with tag will have permissions to the dashboard.

Numberic Widget data shows upto 90 days and can show trend

Qualys Cloud Administration

Administration Users User Management

Need to limit users access and permissions so that limiting extra privileges.

Standard User roles are as follows: In addition to them, there is an option for extended permissions which can be provided.

base and remediation tickets. 1. Remediation User(lowest)access to knowledge base

2. Reader limited rights on assets but can run reports.

3. Scanner limited rights on assigned assets but can run scans, maps and reports

4. Unit Manager management of Business unit assigned

5. Manager Highest Level of permissions)→ subscription management

Other user roles are: knowledge base user access only to Knowledge base

Contact user: user who can only get communications for scans.

User Administration: user section for creation of users. For offloading the creation of new users from manager.

Extended Permissions

Can be granted by managers and unit managers.

Unit manager can grant only to users who are in his unit and only if he himself has that permissions.

Eg Turn off option profile creation for scanner users so that we have uniform scan setting which are created by unit managers.

Business Units:

Grouping of Asset groups and users.

Scanner and Reader users added to a business unit can be granted permissions to the asset groups in that business unit.

We can restrict users from looking at other users in other Bus.

Managers and Backup manager exists outside of Business Units.

We can have users who are not part of any BU. And they will have access to all assets in the subscription.

We can go to Edit basic details to view Action log shows actions taken by that user or edit extended permissions.

Account activity shows login from browser, ip address, api use etc.

In Edit basics details, we have security tab where we can enable two factor authentication.

Role Management

Administration Users Role Management

Here we can see and edit the standard roles and can create custom roles. One user with full permissions e.g. manager.

Or a user with role management role enabled can be able to access it.

Each role will have a section of permissions for each app(CSAM, VMDR, Cloud Agent etc)

From each app as well we will have permission object like add assets, edit option profile etc. Depending on the app.

There are Global Permissions which given direct permissions to each app instead of us selecting. E.B. Dashboard permission gives permission for dashboards on all app sections to the user., Reporting perm,

Tagging perm etc. A user can have multiple roles assigned.

Default user roles don't have access to administration module except for Manager and unit manager. We can create custom role and add administrative module and give permisisons like edit user, create user, delete user, access role management etc

When role is deleted it will be deleted from the users its assigned

HostID key on the device (known as AgentID on portal) uniquely identifies a host. Key location:

HKLM:Software Qualys

Clone Detection: sometimes devices may have same Host ID in that case Qualys will generate a re provision command so that the device generates a unique Host ID again. Mostly used in a Golden image scenario where child images are created from master image.

Data for EDR and FIM are event driven and for other modules like VM, PC they are user defined intervals.

Uninstallation Types:

Agents can be uninstalled using Qualys Ul or API. VM and PC data will be purged automatically. Agents can be uninstalled from cmd on device, but VM and PC data will have to be purged manually.

Agents can also be uninstalled, and data can be purged automatically using purge rules.

Configuration Profile for Cloud Agenta

We can configure agent related configuration settings in configuration profiles.

One device can be assigned to only one configuration profile. If multiple profiles are matching and applying to a device. Then we have order field. The lowest order ie, 1 (which will the

Configuration Profile for Cloud Agents

We can configure agent related configuration settings in configuration profiles.

One device ca can be assigned Ito only one configuration profile. If multiple profiles are matching and applying to a device. Then we have order field. The lowest order i.e., 1 (which will the configuration profile at the top of of the list) will take precedence to higher numbered orders.

Only one default configuration profile. We have option stop data collection for VM, pc etc for device agents having a profile. Even if that is stopped the agent will still have manifest updates, configuration update, agent version updates. We have option for preventing auto update.

Blackout windows is the time to stop the communication between cloud agent and qualys cloud to control the networ network bandwidth during peek network traffic.

CPU limiting,performance settings of the agent. the agent.

CPU limit does not apply to Flm and edr as they need processing in real time.

We can assign hosts using asset tags. Or we can add by name as well.

We have options for agent scan merge to merge duplicated data from qualys scan data and agent data.

Agent heart beat to qualys cloud is called Agent status interval

We can configu configure VM scan intervals. Scan randomization can be used to randomize scanning on host so that the communication with the platform is different for all devices for network bandwidth and disk i/o for vdi sharing same resources. Scan delay randomization will be the actual delay applied to the scan. Randomization will differentiate to the scan timing to be different.

The time when agent will scan and send data Time interval set for each scan(data collection interval) Scan Delay + randomization.

There are other settings for secure config assessment, FIm, EDR, PM

Amount of data consumed by qualys agents number of agent delta upload size.

For Linux machines, Agent scan Mode means qualys can use default user assigned for it or it can use elevate previliges where it will first use its permissions to scan and then which ever files failed due to permissions issues, it will elevate the permissions and then run them mode by using non-root no sudo. or use safe

FIM and EDR needs to be enabled from activation key as well as from configuration profile

On-Demand Scans

If we want to launch a scan right away without waiting for the scan interval timing, we can run scan on demand from portal or locally from the device

On windows: registry HKLM software qualys\qualysagent\ScanonDemand and scanonstartup can be used. First one will start a scan right away and second one will start a scan every time the device reboots. On linux and mac we have a script from qualys clouagentctl.sh which we can run with parameters for running on demand scan along with the scan type.

CSAM Course-CyberSec Asset manageront

Passive sensor: part of CSAM.

Helps eliminate blind spots. Does not actively probe the devices. Helps find un-managed assets in the environment. Longer it runs it can detect more details on unmanaged assets.

It can be virtual or physical.

Virtual can be run in vm image as we have downloaded the local virtual sensor sensor appliances, Sensor has two port. One is in promiscuous mode which sniffs traffic and other port is wan port which.