Azure Hybrid Cloud Whitepaper

Table of Contents

1. Security challenges in the present infrastructure and their solutions with Hybrid Cloud 3

1.1. What is Hybrid Cloud? 3

1.2. Basic types of cloud services 4

1.2.1. Private cloud 4

1.2.2. Public cloud 4

1.3. Benefits and downsides of the Hybrid Cloud solution 6

1.3.1. Advantages 6

1.3.2. Disadvantages 7

1.4. Applications within the Hybrid Cloud 7

1.5. Security within the Hybrid Cloud 8

1.6. Azure Hybrid Cloud solution 10

2. The possibilities of increased transparency and manageability of Hybrid Cloud in Cyber Security 11

2.1. MDE 11

2.1.1. Threat & Vulnerability Management 12

2.1.2. Attack surface reduction 12

2.1.3. Next generation protection 13

2.1.4. Endpoint detection and response 13

2.1.5. Automated investigation and remediation 14

2.1.6. Secure Score 14

2.1.7. Microsoft Threat Experts 15

2.2. MCAS 16

2.2.1. Cloud Application sanctioning and control 16

2.2.3. Cloud Discovery 16

2.2.4 .Application-links 17

2.2.5. Conditional Access App Control 17

2.3. Intune 17

2.3.1. MDM 19

2.3.2. MAM 20

2.4. Azure Sentinel 21

2.4.1. Workbooks 21

2.4.2. Analytics 21

2.4.3. Security automation and orchestration 21

2.5. Threat Hunting 22

3. Using the modularity and elasticity provided by Cloud models and the distributed Security responsibility models 23

3.1. On Premises model 23

3.2. Infrastructure as a Service (Iaas) 24

3.3. Platform as a Service (PaaS) 24

3.4. Software as a Service (SaaS) 24

3.5. Applications within a Hybrid Cloud environment 25

3.6. It Security and Data Protection services within the Azure Cloud 26

3.7. Audit and Compliance within the Azure Cloud 28

1. Security challenges in the present infrastructure and their solutions with hybrid cloud

1.1 What is hybrid cloud?

A hybrid cloud is a computing environment that combines a public cloud and a private cloud by allowing data and application to be shared between them. When computing and processing demand fluctuates, hybrid cloud computing gives businesses the ability to seamlessly scale their
on-premises infrastructure up to the public cloud to handle any overflow—without giving third-party datacenters access to the entirety of their data. Organizations gain the flexibility and computing power of the public cloud for basic and non-sensitive computing tasks, while keeping business-critical applications and data on-premises, safely behind a company firewall.[1]

One of the crucial point that with hybrid cloud services companies gain more control over their private data. An organization can store sensitive data on a private cloud or local data center and simultaneously leverage the robust computational resources of a managed public cloud. A hybrid cloud relies on a single plane of management, unlike a multi-cloud strategy wherein admins must manage each cloud environment separately.[2]

[1] https://azure.microsoft.com/hu-hu/overview/what-is-hybrid-cloud-computing/
[2] https://www.citrix.com/glossary/what-is-hybrid-cloud.html

1.2 Basic types of cloud services

1.2.1 Private cloud

In this case the cloud infrastructure and resources are deployed on-premises. Managed and owned by the organization. Private cloud apps and services requires a large upfront capital expense for equipment and software, a lengthy deployment, and in-house IT expertise to manage and maintain the infrastructure. It's also expensive and time-consuming to scale capacity (because you have to purchase, provision, and deploy new hardware) and add capabilities (because you have to purchase and install new software).[3] On the other hand, gives maximum control over the computing environment and data. What can be crucial when company is dealing with highly sensitive data or requested by governmental regulations.

Two models for cloud services can be delivered in a private cloud. The first is infrastructure as a service (IaaS) that allows a company to use infrastructure resources such as compute, network, and storage as a service. The second is platform as a service (PaaS) that lets a company deliver everything from simple cloud-based applications to sophisticated-enabled enterprise applications.[4]

Advantages:

- **Security**: Data and applications remain behind your firewall and are accessible only to your enterprise. More suited for storing sensitive data
- **Flexibility**: Ability to move non-sensitive data to a public cloud to accommodate sudden bursts of demand on your private cloud[5]

Disadvantages:

- **Higher costs:** Increased initial charges and the need to repay costs of the equipment you purchase.[6]
- **Responsibility:** Operating and maintaining own data center, ensuring hardware and enterprise software security

1.2.2 Public cloud

A public cloud is a pool of virtual resources—developed from hardware owned and managed by a third-party company—that is automatically provisioned and allocated among multiple clients through a self-service interface. It's a straightforward way to scale out workloads that experience unexpected demand fluctuations.[7]

[3] https://www.ibm.com/cloud/learn/hybrid-cloud
[4] https://azure.microsoft.com/en-us/overview/what-is-a-private-cloud/
[5] https://www.netapp.com/us/info/what-is-hybrid-cloud.aspx
[6] https://www.netapp.com/us/info/what-is-hybrid-cloud.aspx
[7] https://www.redhat.com/en/topics/cloud-computing/what-is-public-cloud

It is public because:

- **Resource allocation:** Tenants outside the provider's firewall share cloud services and virtual resources that come from the provider's set of infrastructure, platforms, and software.[8]
- Use agreements: Resources are distributed on an as-needed basis, but pay-as-you-go models aren't necessary components.[9]
- **Management:** At a minimum, the provider maintains the hardware underneath the cloud, supports the network, and manages the virtualization software.[10]

Public cloud solutions allow organizations to scale at a near infinite rate, something that would not be possible in an on-premises data center. As a business grows, it doesn't need to acquire additional hardware or maintain a sprawling network. Likewise, cloud-based services and applications require far less hardware than applications delivered in a traditional manner.[11]

Advantages:

- **Scalability:** Due to on-demand cloud resource is mostly unlimited. As for example Azure and AWS as service providers
- **Lower capital expenditure***:* Because the resources are coming from the service provider there is no need to purchase own data center equipment
- **Reliability:** Mostly because services are distributed across multiple data centers

Disadvantages*:*

- **Control over data security***:* no exact location for the data, as it's in the cloud (*try to think about an infinite raid array*)
- **Higher operational expenditure:** As performance scales, up the cost-per-hour fees rise

[8] https://www.redhat.com/en/topics/cloud-computing/what-is-public-cloud
[9] https://www.redhat.com/en/topics/cloud-computing/what-is-public-cloud
[10] https://www.redhat.com/en/topics/cloud-computing/what-is-public-cloud
[11] https://www.citrix.com/glossary/what-is-public-cloud.html

1.3 Benefits and downsides of the Hybrid Cloud solution

In most cases, companies continue to maintain their data centers for ensuring security, compliance, and operational control. Nonetheless, enterprises are always in need of more resources. For instance, your organization may need additional computing and storage resources to meet the occasional demand spike. Then the business can scale back to the original in-house servers when demand subsides.

Restricting your cloud computing infrastructure to the boundaries of your private data centers doesn't seem a sensible choice. Demand on business resources and the lag time this creates, will require a public cloud service to access as many resources as needed. Integrating a public cloud service into your existing IT strategy not only ensures an affordable solution for processing high-volume data spikes but also helps in avoiding costly downtime.[12]

1.3.1 Advantages

- With hybrid cloud, the organization's workload is contained within a private cloud while retaining the ability to spontaneously increase their workload and perform the spikes of usage on the public cloud[13]
- It's cost effective because organizations pay for the public cloud portion of their infrastructure only when it is needed

[12] https://readwrite.com/2019/08/29/hybrid-cloud-solutions-the-future-of-enterprise-it/
[13] https://vexxhost.com/blog/adv-disadv-of-hybrid-cloud/

- One of the best benefits of hybrid cloud is that you get a centralized private infrastructure on premises
- From security perspective crucial and sensitive information can be stored securely on-premise (100% control over the data)
- Faster speed to market. Sometimes to build up a new infrastructure can take too much time.

1.3.2 Disadvantages

- Although the long-term cost savings are one of the many benefits, the initial deploying cost of a hybrid cloud exceeds as compared to the setup cost incurred in case of a public cloud. While creating a hybrid cloud environment, specific hardware is required to deploy on premises, and that's what shaves off a large chunk of the budget[14]
- Commonly hybrid cloud is secure but it is necessary to take further steps by IT experts to maximize the data security
- If not picked correctly, cloud compatibility can become a real nuisance for Hybrid Cloud environments. A fast-performing on-premise infrastructure may not be able to successfully perform in coherence with a slow performing public infrastructure resulting in a sluggish performance of the Hybrid Cloud[15]

1.4 Applications within the Hybrid Cloud

The tide of businesses re-architecting their applications to be cloud-native, however, hasn't materialized in the way many predicted. It's a sad fact that re-developing apps can be time-consuming, expensive and unsuitable for legacy systems.

Many businesses are either phasing them out or switching to new applications altogether. New functions, however, are developed in cloud-native forms. Legacy apps, particularly, are being targeted with cloud-first features, resulting in the applications themselves becoming hybrid. The benefits of hybrid are given; scalability, affordability, flexibility.

[14] https://vexxhost.com/blog/adv-disadv-of-hybrid-cloud/
[15] https://vexxhost.com/blog/adv-disadv-of-hybrid-cloud/

A business' IT success in 2020 will depend on their ability to grapple with skills shortages, overcome the challenge of legacy, and embrace new opportunities that cloud technologies will bring.[16]

1.5 Security within the Hybrid Cloud

Security within the Hybrid Cloud can mean new challenges regarding IT security, but following the below can help to lower the risks associated with this operation model.

Approach it as shared responsibility: Companies should approach hybrid cloud security as a joint endeavor with their cloud service provider. Assuming the cloud partner will take care of everything once the data leaves the on-premises systems is a recipe for oversights and errors. Even with the best-equipped hybrid cloud provider out there, maintaining security still requires a proactive mindset[17]

Process standardizations: Companies that use different processes for public and private cloud environments, or that fail to implement processes, risk introducing disparities that could lead to manual errors and potential security loopholes. These processes will likely be unique to an organization's needs, but some general best practices apply.[18]

Importance of verifications: Hybrid cloud computing environments tend to blast through traditional network perimeters, as companies distribute workloads across different infrastructures and locations. This means conventional, perimeter-based protections no longer

[16] https://www.itproportal.com/features/2020-forecast-cloud-y-with-a-chance-of-hybrid/
[17] https://www.ibm.com/blogs/cloud-computing/2019/05/02/strong-hybrid-cloud-security-strategy/
[18] https://www.ibm.com/blogs/cloud-computing/2019/05/02/strong-hybrid-cloud-security-strategy/

work. Adopt a never trust, always verify approach to all computing resources across both infrastructures. [19]

Visibility and ownership: One danger in dealing with two different environments is that it can be difficult to get a comprehensive view of what's happening across the entire infrastructure. Explore using a management system that can aggregate monitoring and asset management across both private and public clouds. Ideally, administrators should be able to see both from a single dashboard. Security teams should also ensure that all assets and data across both environments have defined ownership. An individual or team should be responsible for them so that nothing falls through the cracks.[20]

Technical controls: Technical controls are the heart of hybrid cloud security. The centralized management of a hybrid cloud makes technical controls easier to implement. Some of the most powerful technical controls in your hybrid cloud toolbox are encryption, automation, orchestration, access control, and endpoint security.[21]

Automation: Manual monitoring for security and compliance often has more risks than rewards. Manual patches and configuration management risk being implemented asynchronously. It also makes implementing self-service systems more difficult. If there is a security breach, records of manual patches and configurations risk being lost and can lead to team in-fighting and finger-pointing. Additionally, manual processes tend to be more error prone and take more time.[22]

Endpoint security: Endpoint security often means using software to remotely revoke access or wipe sensitive data if a user's smartphone, tablet, or computer gets lost, stolen, or hacked. Users can connect to a hybrid cloud with personal devices from anywhere, making endpoint security an essential control. Adversaries may target your systems with phishing attacks on individual users and malware that compromises individual devices.[23]

[19] https://www.ibm.com/blogs/cloud-computing/2019/05/02/strong-hybrid-cloud-security-strategy/
[20] https://www.ibm.com/blogs/cloud-computing/2019/05/02/strong-hybrid-cloud-security-strategy/
[21] https://www.redhat.com/en/topics/security/what-is-hybrid-cloud-security
[22] https://www.redhat.com/en/topics/security/what-is-hybrid-cloud-security
[23] https://www.redhat.com/en/topics/security/what-is-hybrid-cloud-security

1.6 Azure Hybrid Cloud solution

Customer environments are evolving, becoming increasingly complex with many applications often running on different hardware across on-premises datacenters, multiple clouds, and the edge. Managing these disparate environments at scale, ensuring uncompromised security across an entire organization, and enabling developer agility and innovation are critical to success. [24]

Unified identity platform: Enhance security, simplify access, and set smart policies across your different environments with a single identity platform

Windows Server and SQL Server for less: Take advantage of the Azure Hybrid Benefit and save 40% on virtual machines by using your existing SQL Server or Windows Server license investments

AI at the edge: Analyze information close to the physical world where the data resides by deploying Azure Cognitive Services in containers. Deliver real-time insights and immersive experiences that are highly responsive and contextually aware

Cohesive security management: Bring cloud scale and AI-powered security protections to your on-premises virtual machines and IoT devices, all managed centrally along with security for your cloud resources through Azure Security Center

[24] https://azure.microsoft.com/en-us/overview/azure-hybrid/

Database consistency with common code base: Achieve greater flexibility, scale, and availability. You decide where you want your SQL or PostgreSQL data to reside and get frictionless database migration with no code changes at an industry leading total cost of ownership (TCO).[25]

2. The possibilities of increased transparency and manageability of Hybrid Cloud in Cyber Security

This section of this document is mostly about the Cyber Security aspects of Microsoft Azure, as currently this is the only cloud environment with native integration with existing Microsoft Windows/Office environments. As these environments are the most common nowadays, securing them is of utmost importance.

The below sections are containing the applications and services Azure provides to enhance and augment the Cyber Security of the hybrid and public cloud environments.

2.1 Microsoft Defender for Endpoint

The Microsoft Defender for Endpoint is a tool to detect and prevent threat and if an attack was successful, investigate, react and mitigate (*Incident Response)*..

The platform is capable of protecting MacOS and Linux systems besides Microsoft and the Windows 10 OS-es are containing its agent built-in (*for Windows 7 SP1 and Windows 8.1 an agent is needed*). These agents are responsible for the communication between Azure and the On-Premise infrastructure.[26]

[25]https://azure.microsoft.com/en-us/overview/hybrid-cloud/#overview

[26]https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/onboard-downlevel

According the the system management platform, these agents can be set up via Group Policy, System Center Configuration Manager (*SCCM*), Mobile Device Management (*Intune*), or with by executing a script on the endpoints[27]. Endpoints can be monitored on a cloud-based portal (*security.microsoft.com*) after successful integration.

MDE can provide the following features:

- Threat & Vulnerability Management
- Attack surface reduction
- Next generation protection
- Endpoint detection and response
- Automated investigation and remediation
- Secure score
- Microsoft Threat Experts

2.1.1 Threat & Vulnerability Management

MDE continuously scans the software and pathcees on the endpoints and when it detects a vulnerability ot a missing patch, MDE Threat and Vulnerability Management will alert and also capable of mitigating these issues with a "*remediation task*".

The advantage of the system is the real-time monitoring capability of such tasks and the single-pane-of-glass approach for different working groups (*IT Security and Operations*), to support the joint operation. [28]

2.1.2 Attack surface reduction

The Attack surface reduction (*ASR*) system is a capable learning, auditing and restriction platform for hardening. It's rule and behaviour analytics based and can ensure the hardening restrictions are in place (*like macro execution policies, for example*).

Suspicious behaviour examples:

- Executable scripts and files in Office documents
- Obfuscated or suspicious script

ASR supports the following operating systems: Windows 10 1709, 1803 or newer, Windows Server 2016 1803 or newer, Windows Server 2019.

[27] https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/configure-endpoints

[28] https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/next-gen-threat-and-vuln-mgt

To use the complete ASR ruleset, you need at least Windows 10 enterprise license, with Windows E5 license, you can use the further capabilities of MDE.[29]

2.1.3 Next generation protection

The Next generation protection (*NGP*) modul is the Windows Defender Antivirus adapted for cloud. Defender is capable of behaviour analytics, heuristics and machine learning based scanning and protection.[3031]

2.1.4 Endpoint detection and response

MDE's Endpoint detection and response (*EDR*) is helping in the analysis of incident alerts. On the course of a cyber-attack, there are loads of alerts, which can be a heavy burden to to see through. MDE is capable of grouping them to help the analyst evaluate them and react faster.

MDE is capable of both automatic and manual incident response, by doing a "live response session"[32]

[29] https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction

[30] https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/configure-windows-defender-antivirus-features

31 https://techcommunity.microsoft.com/t5/microsoft-defender-atp/protecting-windows-server-with-windows-defender-atp/ba-p/267114#

[32] https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/overview-endpoint-detection-response

2.1.5 Automated investigation and remediation

DATP is capable of scripted automated alert evaluation and response, via playbooks. This feature can sufficiently decrease the analysts low level tasks, therefore they can focus on the more important and complex assignments.

MDE capable of automated investigation and remediation on the following systems:

- Windows Server 2019
- Windows 10, version 1709, 1803 or never[33]

2.1.6 Secure Score

Secure Score is a high-level overview about the security posture of an organization. The score and the number of tasks to do is linked (*higher score=more tasks*). The basis of scoring are the recommended security setup and security related tasks (*like setting up MFA, Alerting and Reporting*).

You can only access Secure Score with the proper priveleges, which are the following:

Read and write privilege roles:[34]

- Global administrator
- Security administrator
- Exchange administrator
- SharePoint administrator

Read-only privilege roles:

- Helpdesk administrator
- User administrator
- Service administrator
- Security reader
- Security operator
- Global reader

[33] https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/automated-investigations

[34] https://docs.microsoft.com/en-us/microsoft-365/security/mtp/microsoft-secure-score

2.1.7 Microsoft Threat Experts

The Microsoft Threat Experts service is available on-demand. Its purpose is to help secure the organization, with the help of Microsoft's experts.

This service consists of two parts:

- Targeted attack notification
- Experts on demand

Targeted attack notification is a proactive threat hunting service, where the experts are searching targeted attacks regarding the organization and alerting when they find one. This service also contains the continuous monitoring and analysis of threats, AI based attack detection and risk identification.

Experts on demand enables the organization to contact Microsoft's security expert team regarding alerts and solutions against new threats.[35]

[35] https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-threat-experts

2.2 Cloud App Security

Microsoft' Cloud App Security is a Cloud Access Security Broker (*proxy*), what supports log collection, API connectors and reverse proxy. It integrates natively with other Microsoft products and can discover and regulate Shadow IT. Also capable of protecting sensitive data and against threats and anomalies.

Cloud App Security enables the following:[11]

2.2.1 Cloud Application sanctioning and control

Easy-to-install APIs enables control and transparency of cloud applications.

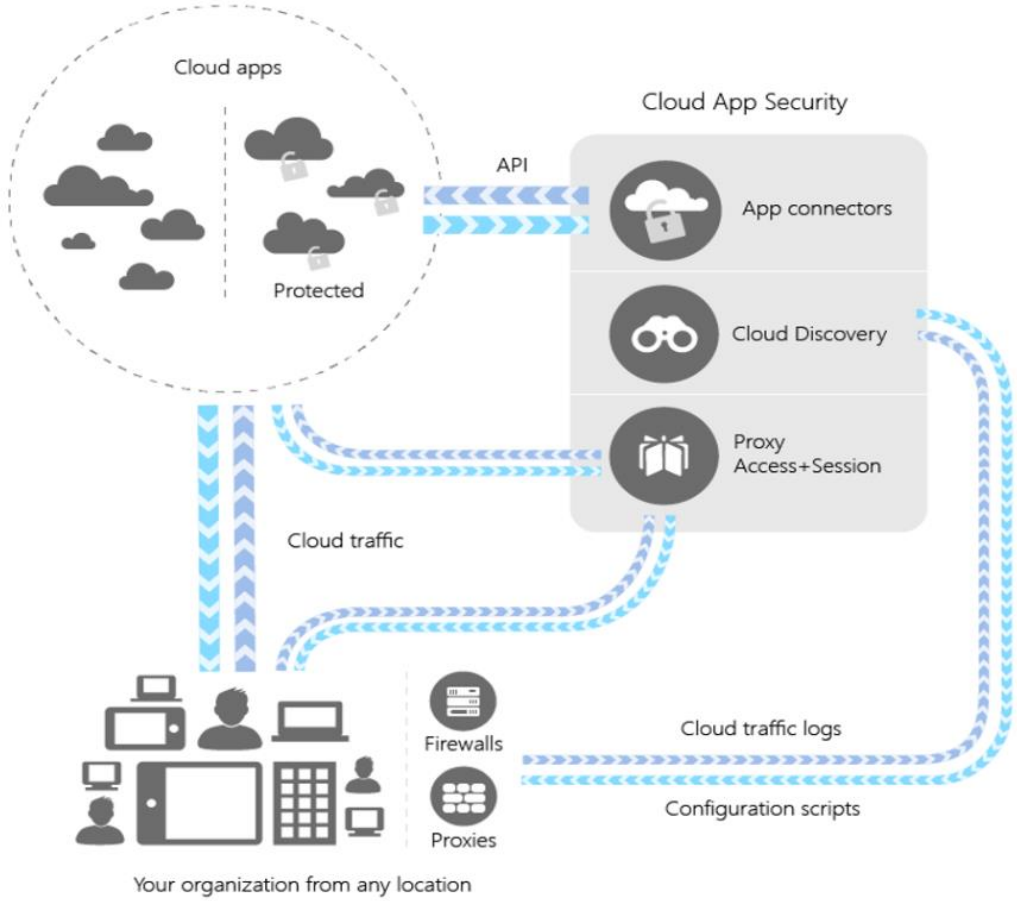


Figure 1: The structure of Cloud App Security [11]

2.2.3 Cloud Discovery

Cloud Discovery analysis traffic and compares it with MCAS's database of more than 16000 cloud apps. By doing this, it enables to create snapshot or running reports, for increased transparency.

Snapshot reports are evaluating manually uploaded firewall and proxy logs, rolling reports analysing Cloud App Security's complete forwarded network traffic to discover anomalies via Machine Learning or policies. [12]

Sanctioning and refusing cloud application traffic

With Cloud App Catalogue, MCAS is capable of sanctioning applications. These sanctions can be based on certificates, best practices and frameworks, which can be granularly customized according to the needs of the organization. According to these, Cloud App Security can assign a risk score to the application.[36]

2.2.4 Application-links

The application-links can perform integration between the application and MCAS through the API of the given cloud application. To perform this process, the application administrator must grant access to MCAS. After that, it queries the application's logs, scans the data, and with the help of MCAS, threats can be discovered and policies can be implemented.[37]

2.2.5 Conditional Access App Control

Conditional Access App Control uses reverse proxy to enable real-time monitoring and infrastructural transparency. This enable the rule-based control of an organization's network traffic and can help to avoid data losses by restricting uploads and downloads to cloud providers. It can also help by enforcing traffic encryption and to restrict access from non-organizational or risky IP addresses.

2.3 Intune

Intune is a Cloud-based MDM and MAM application, what can be licensed with the Microsoft Enterprise Mobility + Security (*EMS*) package and integrated with other Microsoft services, like Active Directory or Microsoft 365.

[36] https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security

[37] https://docs.microsoft.com/en-us/cloud-app-security/set-up-cloud-discovery

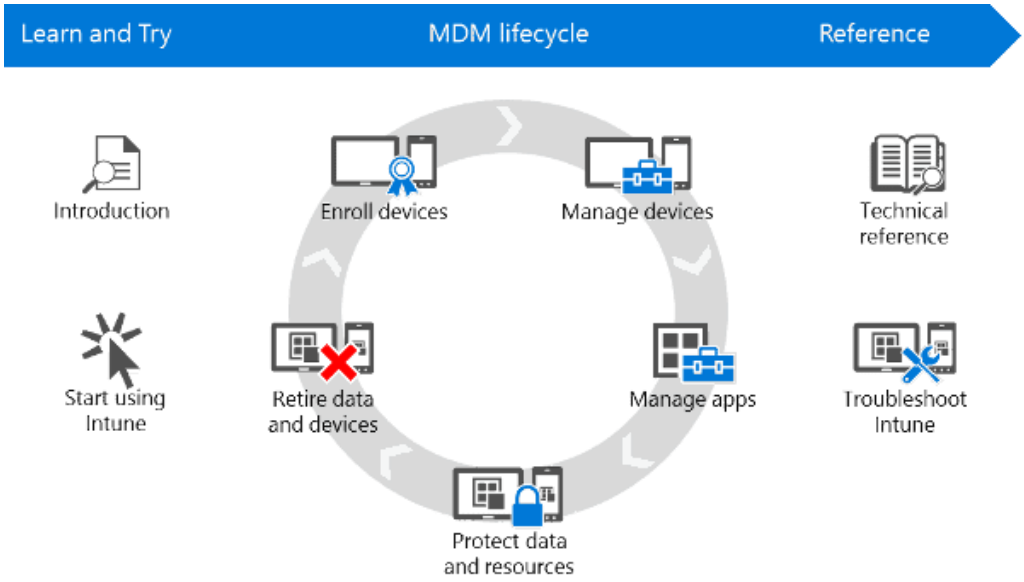


Figure 2: Intune lifecycle[38]

Intune features:

- Usage rules and regulations for both organization and employee owned devices
- Application and certificate deployment on on-premise and mobile devices
- Data protection by controlling of accesses and sharing
- Device and application compliance

[38] https://www.prajwaldesai.com/microsoft-intune-overview-and-features/

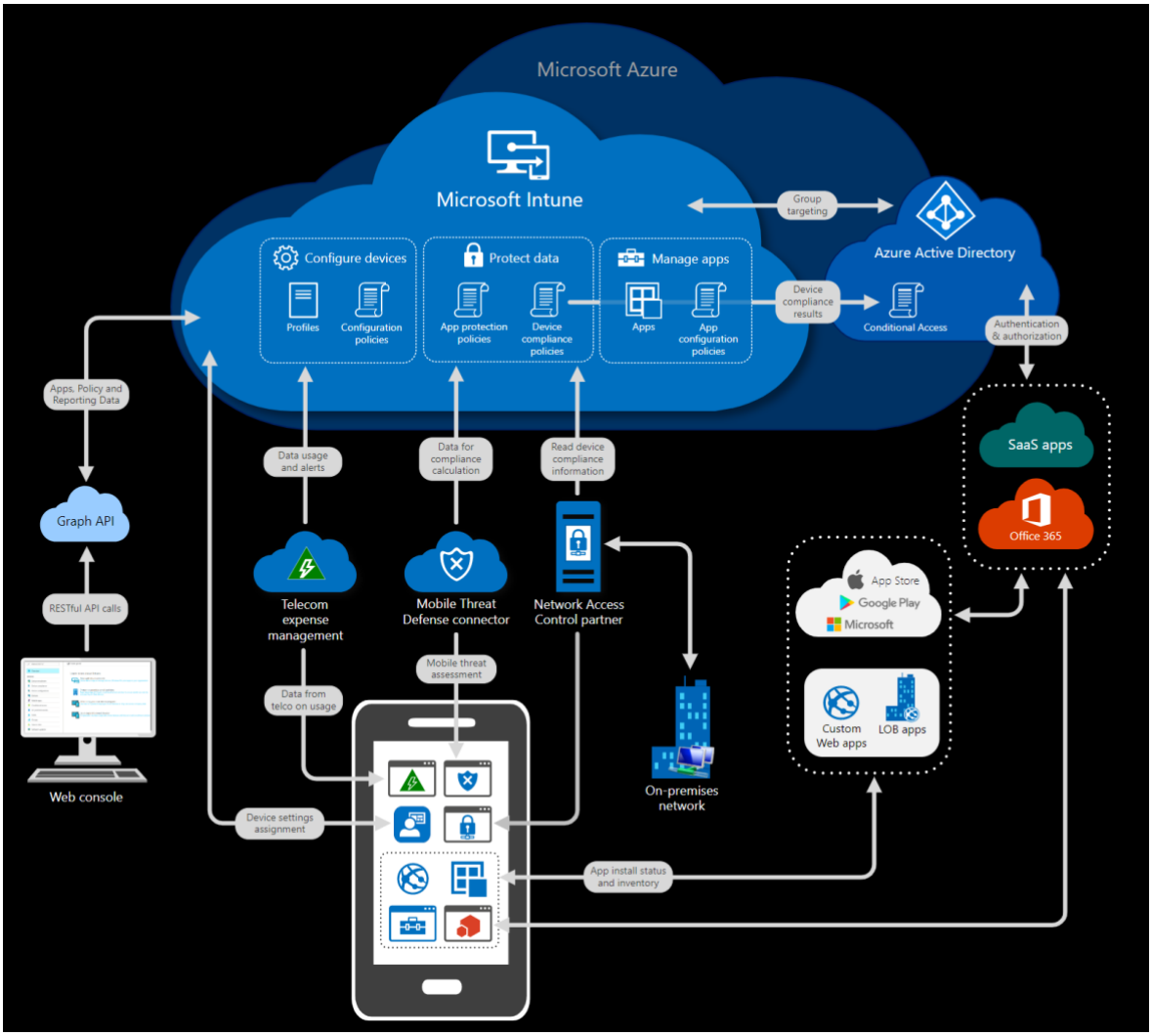


Figure 3: The structure of Intune[39]

2.3.1 MDM

There are various ways within Intune to manage Mobile Devices. Organization-owned devices can be managed fully (*settings and security*) by Intune. To this this, you have to register the device to deploy the configured rules and settings (like PIN and VPN settings, certificates.

With BYOD devices, the user can decide between full/partial management. By registering the device, the user can access everything set up to access, but by not registering, Email or Microsoft Teams is still available by using MFA.

With registered and managed devices, the organization is capable of:[40]

- Maintaining an inventory of devices capable of accessing the infrastructure
- Configuring devices to comply with organizational regulations

[39] https://docs.microsoft.com/en-us/intune/fundamentals/what-is-intune
[40] https://docs.microsoft.com/en-us/intune/configuration/device-profiles

- Deploying VPN and WIFI certificates
- Listing the compliant and non-compliant devices
- Wiping the stolen or decommissioned devices

2.3.2 MAM

Mobile Application Management protects the data of the organization in regards of mobile applications. This service is available for organization-managed devices.

With Intune managed devices, the organization is capable of:

- Adding mobile application to users and groups and devices within them
- Preconfiguring the applications
- Reporting on the applications and their usage

One of the applications-based security features within Intune is app protection policies. With Azure AD Identity, there's an option to distinct personal and organizational data and possible to regulate user actions like copy and paste. App protection policy can be created regarding Intune-enrolled, not enrolled and other MDM enrolled devices.[41]

[41] https://docs.microsoft.com/en-us/intune/apps/app-protection-policy

2.4 Azure Sentinel

Azure Sentinel is a cloud-native security information and event management (*SIEM*) and security orchestration automation and response (*SOAR*) solution. With Azure Sentinel organizations can lower the risks of sophisticated and non-sophisticated attacks.

To integrate Azure Sentinel, the organizations first need to connect log sources. Sentinel provides native connectors to Microsoft Azure applications, like Office 365, Azure AD, Azure ATP, Microsoft Cloud App Security. Besides these native connectors, log collection is available though Syslog and REST API.

2.4.1 Workbooks

After connecting the log sources, Azure Sentinel is capable of automatic Incident response, based on Workbooks. Workbooks are available out-of-the-box box, but can also be created from scratch, with the proper privileges.[18]

2.4.2 Analytics

The Azure Sentinel Analytics correlates alarms into incidents. These incidents are alarms bound together which are increases risks to the organization. Besides the out-of-the-box correlation, organizations can write their own too and there is also an option to use machine learning to create anomaly-based rules. [17]

2.4.3 Security automation and orchestration

Playbooks are available to automate responses to threats detected by Sentinel. Playbook are batch processes, which can be manually or automatically run on alerts generated by Azure Sentinel.

This system is based on Azure Logic Apps, therefore it can use its integrated templates. Their usability is tenant-locked, therefore only the designated Azure subscribers can use them in a multi-tenant environment.[42]

[42] https://docs.microsoft.com/en-us/azure/azure-monitor/app/usage-workbooks

2.5 Threat Hunting

Azure Sentinel contains integrated search-and-query tools, based on the MITRE framework, which can help proactively discover threats regarding the organization. By using these queries as templates, new rules can be created for detection.

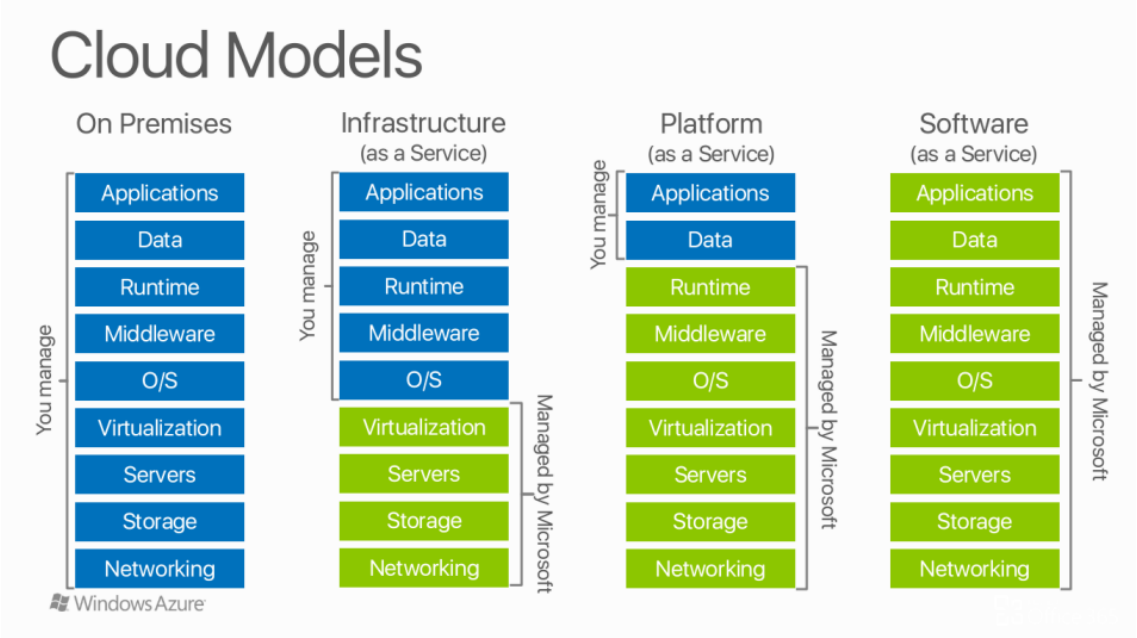
There is also an option to create bookmarks, which are usable to mark the suspicious or unusual findings in a dashboard for easier usage and sorting. Sentinel is also capable of creating Notebooks, which are step-by-step playbooks for the steps used in the Threat Hunting process. These notebooks can be shared within an organization.[43]

[43] https://docs.microsoft.com/en-us/azure/sentinel/hunting

3. Using the modularity and elasticity provided by Cloud models and the distributed Security responsibility models

Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. The responsibility of managing various aspects of hosting is split between the consumer and the service provider, usually in a manner that adheres to one the following models:

- On-premise (*self-hosted*)
- IaaS (Infrastructure as a Service)
- PaaS (Platform as a Service)
- SaaS (Software as a Service)



3.1 On Premises model

This model is not a cloud service, but is included rather to illustrate what responsibilities exist when operating your own hosting infrastructure. With the on-premise model, all aspects of hosting are the responsibility of the user. This includes the set-up costs, development, deployment, maintenance, upgrading and securing of the infrastructure and the software running on it. More colloquially, this model is equivalent to buying your own servers and software as well as hiring a team of professionals to configure, maintain and secure it.

3.2 Infrastructure as a Service (Iaas)

With this model, the hardware portion of hosting is handled by the cloud service provider. Low level physical details are abstracted, meaning the consumer only has to deal the software that is to be implemented. Typical details that will be handled by the service provider include: physical computing resources, location, data partitioning, scaling, security and backup.

The consumer will typically be given access to a hypervisor on which they can run virtual machines for which they are responsible. Often times, the economies of scale provided to cloud service providers, make the cost hosting a lot more favorable for smaller entities as well as eliminating startup costs. On the other hand, misconfigurations could lead to unexpected costs.

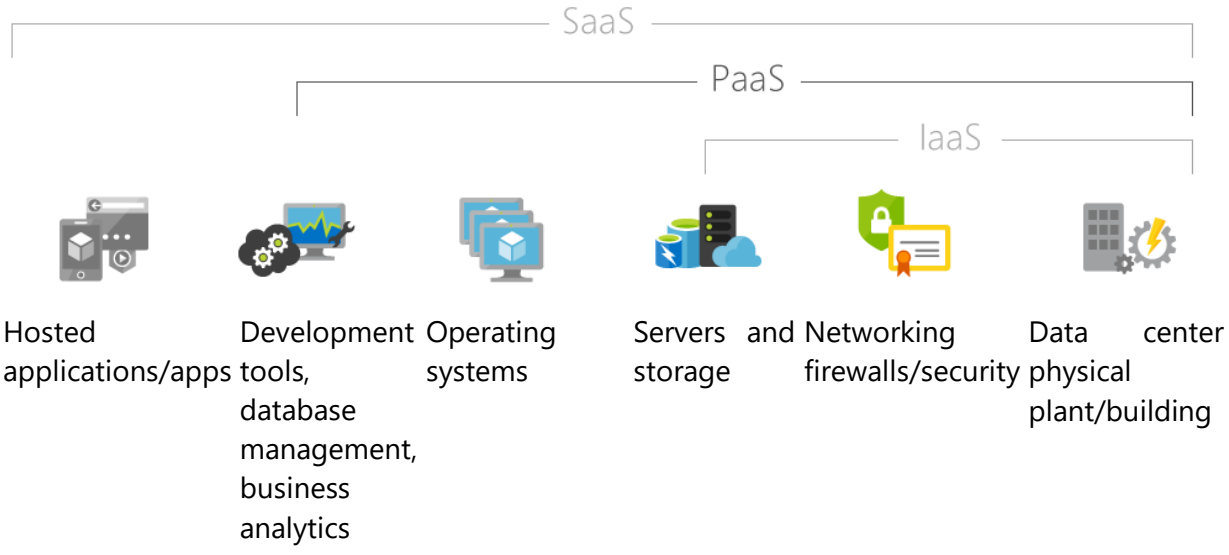
3.3 Platform as a Service (PaaS)

With this model, even fewer low-level aspects are handled by the consumer. Now, software such as the operating system is also the responsibility of the service provider. The consumer only has to deploy their application to the platform. The application and thus the consumer is given access to system resources through libraries, services and tools supplied by the provider.

Additionally, the cloud provider will typically provide a programming-language execution environment, database and webserver. Thus, developers will usually develop and execute their programs directly in the cloud.

3.4 Software as a Service (SaaS)

This model offloads all responsibilities associated with hosting to the cloud service provider and the consumer is only given access to the application through a thick or thin client. SaaS is more so a subscription to software that is hosted off site, rather than making resources available for the consumer to host their own applications as it is with the previous models. The consumer is only responsible for limited user specific configuration settings to tailor the software experience to the needs.



3.5 Applications within a Hybrid Cloud environment

Cloud hosting is a type of managed service that exist due to the complex, yet indispensable nature of IT infrastructure and business software. The purposes of the cloud hosting models above, is to offload cost (both monetary and temporal) to the service provider and to share the responsibility of maintenance, securing and anticipating growth. Azure cloud hosting puts an emphasis on modularity and elasticity with regards to its infrastructure and services.

- **Modularity** means than services and infrastructure building blocks can be provisioned and flexibly interconnected in any way the customer sees fit.
- **Elasticity** means that the resources that underpin a service can be scaled up or down on the fly seamlessly depending on demand.

Data centers are built with standardized hardware and are also made up of multiple identical building blocks of infrastructure. The architecture of these datacenters is also designed so that these building blocks can easily be added, remove or swapped out in order to achieve scalability and quick hardware replacements.

Customers are not given direct access to this datacenter infrastructure, and provisioning of resources doesn't mean that more of these physical building blocks are added. A hypervisor runs on the datacenter infrastructure and virtualized subsets of this infrastructure is what actually gets allocated to the customer. This virtualization also adds a level of abstraction, meaning the customer doesn't have to deal with many of the fine details of managing the hardware.

The client-side provisioning and configuration of cloud infrastructure is straight forward and easily tailored to customers specifications, done through either a web interface or command line.

The cost savings of migrating to cloud hosting can be substantial. One third of surveyed companies in the United States reported an increase in profit between 10 to 25 percent and a further 19% percent of companies reported increased profits between 25 and 50 percent as a direct consequence of their cloud computing investments.[44]

The substantial increase in profits can be attributed to a reduction in operating costs, among other reasons. Since the management of hosting infrastructure and software (*depending on the service model*) is split between the customer and the service provider, the customer can save on infrastructure related investment and does not have to maintain as large of an IT team. Many large organizations have saved between £500,000 and £4,000,000.[2] Even a direct comparison between the operating costs of a single small server hosted locally and the cost of an equivalent cloud service, can result in savings above 50%.[45]

[44] Cloud Computing Research, Manchester Business School, Nicholson et. al. (2013)
[45] Cloud Computing: Case Studies and Total Cost of Ownership, Han, Yan. (2012)

3.6 It Security and Data Protection services within the Azure Cloud

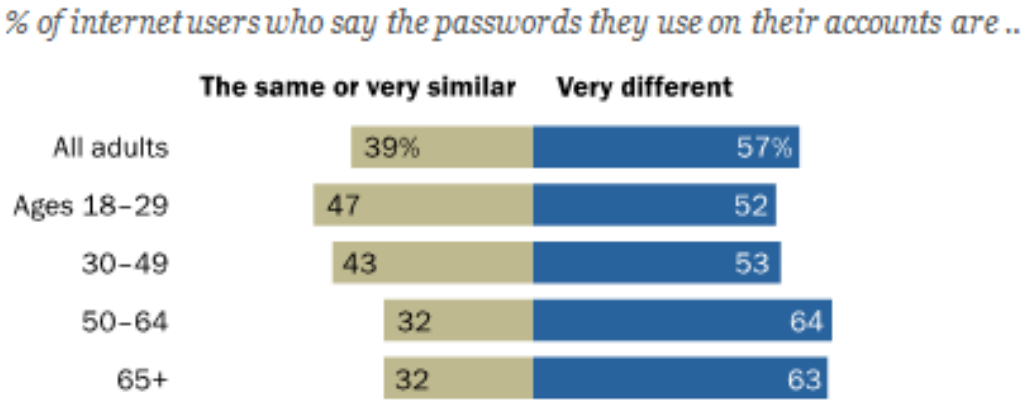
It is also worth mentioning the additional services and tools that cloud hosting provides and the optimization that can be achieved by them, all without any development costs to the consumer. Azure for instance list over 600 services and tools, that are made available to help optimize and streamline operation, maintenance and development of cloud infrastructure and applications, many of which indirectly result in cost savings.[46]

Creating global infrastructure is another notably complex and resource intensive task, that is simplified with cloud computing. It is no longer necessary to maintain datacenters across the world in order to improve quality of service and to comply with data regulations. Azure provides datacenters in 56 regions, allowing for global needs to be met whilst only being managed from one central location by one team.

Cloud service providers are often highly security focused, allowing for improved security through the tools and services supplied by them. Azure allows for the easy migration of existing Active Directory implementations to cloud instances as well as straight forward configuration of role-based access control. Privileged identity management removes the necessity for having service accounts for applications attempting to access resources.

Azure provides native multi factor authentication, making compromised passwords useless without a second authentication method. 81% of hacking-related breaches leveraged either stolen and/or weak passwords, thus having MFA significantly reduces the attack surface of one's applications and infrastructure.[47] Native authentication methods in Azure include a **password, mobile app, SMS and phone call**. Administrators can also set trusted IP addresses, receive fraud alerts and view multifactor authentication related reports.

[46] https://azure.microsoft.com/en-us/services/
[47] Verizon Data Breach Investigations Report



[48]

For hybrid cloud deployments, Azure provides a native Site-to-Site VPN to easily connect cloud virtual networks to on premises networks. Single clients can also connect to cloud virtual networks through the Point-to-Site VPN. All VPNs communicate through a secure IPsec/IKE tunnel.

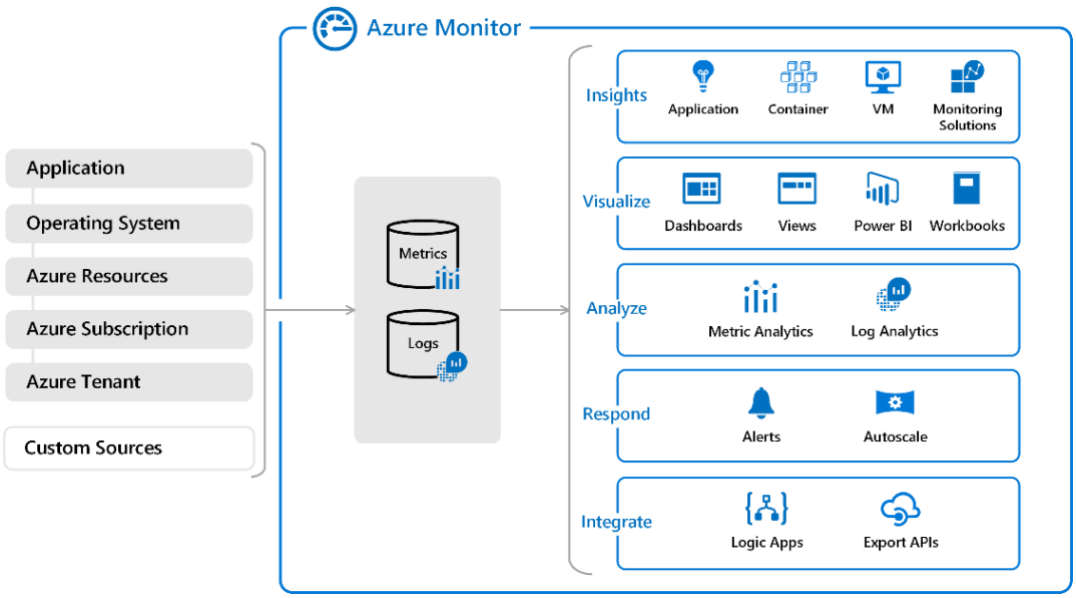
Many other tools exist to improve the security posture of an azure environment. These tools include the following:

- **Network Security Group rules**: Allows for the configuration of complex rules for allowing and denying connections. Rules can include dynamically updating tags that can be assigned to IP ranges.
- **Just in time VM access:** Users with sufficient RBAC privileges can request direct access to virtual machines that can be granted for specific ports for a specific time range. NSGs are automatically updated to allow the connection.
- **Route control and forced tunneling:** Custom routes can be defined when configuring networking and services can be denied direct access to the internet.
- **Virtual network security appliances:** Such as IDS/IPS's, additional firewalls, additional DDOS protection, Network level antivirus and Antimalware, Anti-bot protection and Application access control.
- **Azure Firewall:** High availability, scalable firewall that allows application FQDN filtering rules and network traffic filtering rules.
- **Azure Security Center:** Provides advanced threat protection against a variety of hazards and gives a numerical score for security posture as well as recommendations, security alerts and remediation steps.
- **Azure Network Watcher:** Provides capability to monitor, diagnose and view metrics of resources in a virtual network.

[48] Americans and Cybersecurity, PEW Research Center March 30 – May 3 2017

3.7 Audit and Compliance within the Azure Cloud

Many tools exist for the auditing of an azure environment. Log collection is available for all Azure service and logs can be processed in azure monitor as well as Azure Security Center (for security related logs). Azure Monitor enables diagnosis of infrastructure related issues, identify application related issues, provide log analytics, create automated actions, and create visualizations.



Azure monitor collects data from the following sources:

- **Application monitoring data**: Metrics of applications hosted in your cloud.
- **Guest OS monitoring data:** Data about the operating systems running on your virtual machines.
- Azure resource monitoring data: Data about Azure resources.
- **Azure subscription monitoring data:** Data about the activity of an Azure subscription.
- **Azure tenant monitoring data:** Data about tenant-level Azure services, such as Azure Active Directory.

Azure Security Center can also be used to audit the security posture of your azure environment, through the log analytics, recommendations and the configuration of security policies that can be enforced for the whole tenant.

Many tools are also provided for compliance purposes such as the Regulatory compliance dashboard in Azure Security Center. This dashboard provides information on your compliance posture for preset standards and regulations, based on continuous assessment of your Azure environment.

Intune allows for compliance and conditional access through a broad set of access controls. Intune can be configured to deny access to network resources until a device meets organizational requirements and specifications. For example, administrators can set up a policy where a device needs to meet certain conditions such as not being jail-broken or rooted or to have an up to date operating system in order to access company resources.