Robust Cloud Security and Data Protection Methodology in Wipro

Shape

Description automatically generated



Cloud Security and Data Protection

Whitepaper

April 2023

[1 Executive Summary 2](#_Toc132453526)

[**1.1** **Cloud Security and Data Protection Dynamics** 2](#_Toc132453527)

[**1.2** **Case Study – Wipro** 2](#_Toc132453528)

[1.2.1 Migration Challenges 2](#_Toc132453529)

[1.2.2 Security Challenges 2](#_Toc132453530)

[1.2.3 Organization Challenges 3](#_Toc132453531)

[2 Our Approach/ Methodology/ Solution 4](#_Toc132453532)

[**2.1** **Our Approach/Solution** 4](#_Toc132453533)

[**2.2** **Identity and Access management:** 4](#_Toc132453534)

[**2.3** **Networking Security:** 5](#_Toc132453535)

[**2.4** **Data Protection Security:** 5](#_Toc132453536)

[**2.5** **Governance and Compliance:** 5](#_Toc132453537)

[**2.6** **Application and Services Security:** 5](#_Toc132453538)

[3 Implementation 6](#_Toc132453539)

[**3.1** **Components and Service detail descriptions:** 7](#_Toc132453540)

[4 Conclusion 10](#_Toc132453541)

# Executive Summary

## **Cloud Security and Data Protection Dynamics**

Data during workload migration to cloud refers to the data that is being generated, processed, and used by an application or system while it is actively running or operational. This data can include various types of information such as user input, application configuration settings, intermediate processing results, and other relevant data that is required for the application to function properly.

Data during user migration to cloud typically refers to the data associated with individual users or accounts, such as usernames, passwords, email addresses, personal settings, permissions, and other user-related information like additional user attributes or metadata.

Data protection is a critical consideration so, Wipro define processes and strategies, implementing a zero-trust security model in the cloud that can help safeguard data from unauthorized access, prevent data breaches, and ensure compliance with data protection regulations. Zero trust is a security approach that assumes that no user or system can be trusted by default, and access to resources is granted based on continuous verification of various factors, such as user identity, device posture, location, and other contextual information. It is important to comply with relevant data protection and privacy regulations, such as GDPR to ensure that data is handled in compliance with applicable laws and regulations. Regular security assessments, audits, and updates should be conducted to ensure the effectiveness and resilience of the data protection measures. By implementing the security measures, organizations can help protect their data during migration in the cloud and ensure that data remains secure and compliant with applicable regulations.

**Industry Overview/ Introduction**

## **Cloud Security Alliance Survey Report 2023**

As per the Cloud Security Alliance Survey Report 2023, 96% of organisation have insufficient security for some of their sensitive data.

Chart

Description automatically generated

In addition to struggling with securing sensitive data, organizations are struggling with tracking data in the cloud. Over a quarter of organizations aren’t tracking regulated data, nearly a one third aren’t tracking confidential or internal data, and 45% aren’t tracking unclassified data.

Chart, bar chart

Description automatically generated

Insufficient security and tracking leads to threats. Threat to data can be from external and internal sources. External threats include hackers, cyber criminals, and malicious software, while internal threats come from employees, contractors, and other trusted individuals with access to sensitive information. Common types of cyber-attacks include phishing, malware, ransomware attacks, denial-of-service attacks, and social engineering attacks. These attacks can result in data theft, data corruption, data loss, leading to financial losses, legal liabilities, and reputational damages.

# Wipro Approaches/Methodology

To overcome the challenges, Wipro adapt Zero Trust principles and follow defence-in-depth strategy that addresses data protection in the cloud, taking into consideration the requirements and risks of the data migration to cloud environment. When implementing zero trust in the cloud, the following data protection principles can be applied:

* Identity and access management
* Network security
* Data Protection
* Governance and compliance
* Application and Services Security

## **Identity and Access management:**

* 1. **Assign permissions to users, groups, and applications at a certain scope through Azure RBAC**. Wipro guideline is to grant permissions based on predefined roles, rather than granting permissions directly to individual users. RBAC allows you to assign permissions to roles, and then assign users to those roles based on their job responsibilities. This makes it easier to manage access permissions based on need-to-know and least privilege principles, as roles can be defined and managed centrally, and access can be easily revoked or modified as needed.
     1. **Grant access based on a need-to-know basis and least privilege security principles**: Access should be based on a user's role, responsibilities, and the specific tasks they need to complete. Wipro recommends avoid granting blanket/admin access to all resources, users, or systems, and regularly review and revoke access that is no longer needed.

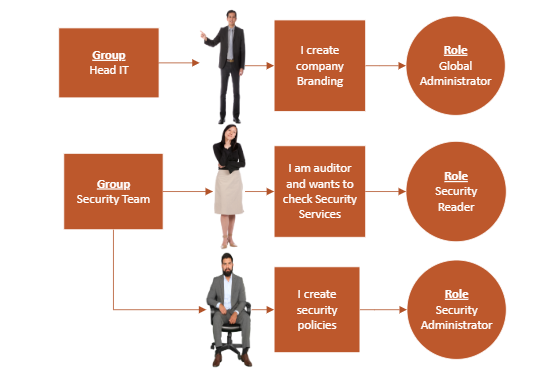


Figure 1: Role based least Privileges specific to task.

* 1. **Prevent deletion or modification of a resource, resource group, or subscription through management locks.** Management locks in Azure are a way to prevent accidental or unauthorized deletion or modification of resources, resource groups, or subscriptions. Wipro suggested to apply locks on resources, resource group and subscription.
  2. **Use Managed Identities to access resources in Azure**. Wipro recommends using managed identities that provide a secure and convenient way to authenticate and authorize applications running on Azure resources to access other Azure resources without the need for explicit credentials or secrets.

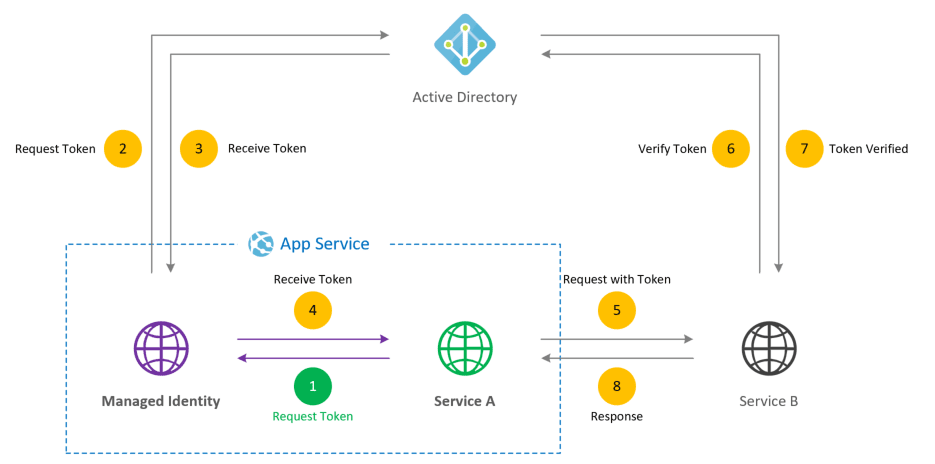


Figure 2: Managed Identity access for Azure Resources [Reference](https://marczak.io/posts/2019/07/securing-websites-with-msi/)

* 1. **Support a single enterprise directory. Keep the cloud and on-premises directories synchronized, except for critical-impact accounts.** By using Azure AD Connect and implementing the appropriate synchronization filters, monitoring, and security measures, single enterprise directory can be supported while keeping the cloud and on-premises directories synchronized, except for critical-impact accounts. Wipro suggested that helps to maintain consistency across the directories while ensuring that sensitive accounts are protected and aligned with your organization’s security policies.

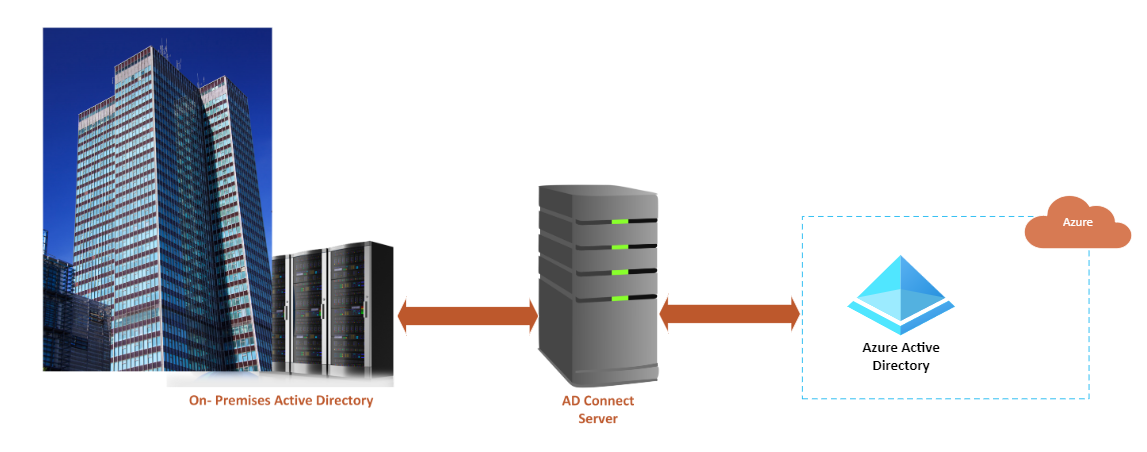


Figure 3: AD Connect user sync. Between On premises AD to AAD

* 1. **Set up Azure AD Conditional Access.** Wipro emphasis onleveraging Azure AD Conditional Access, enforce and measure key security attributes when authenticating all users, including critical-impact accounts, to ensure that only authorized users with the necessary security attributes can access cloud resources.

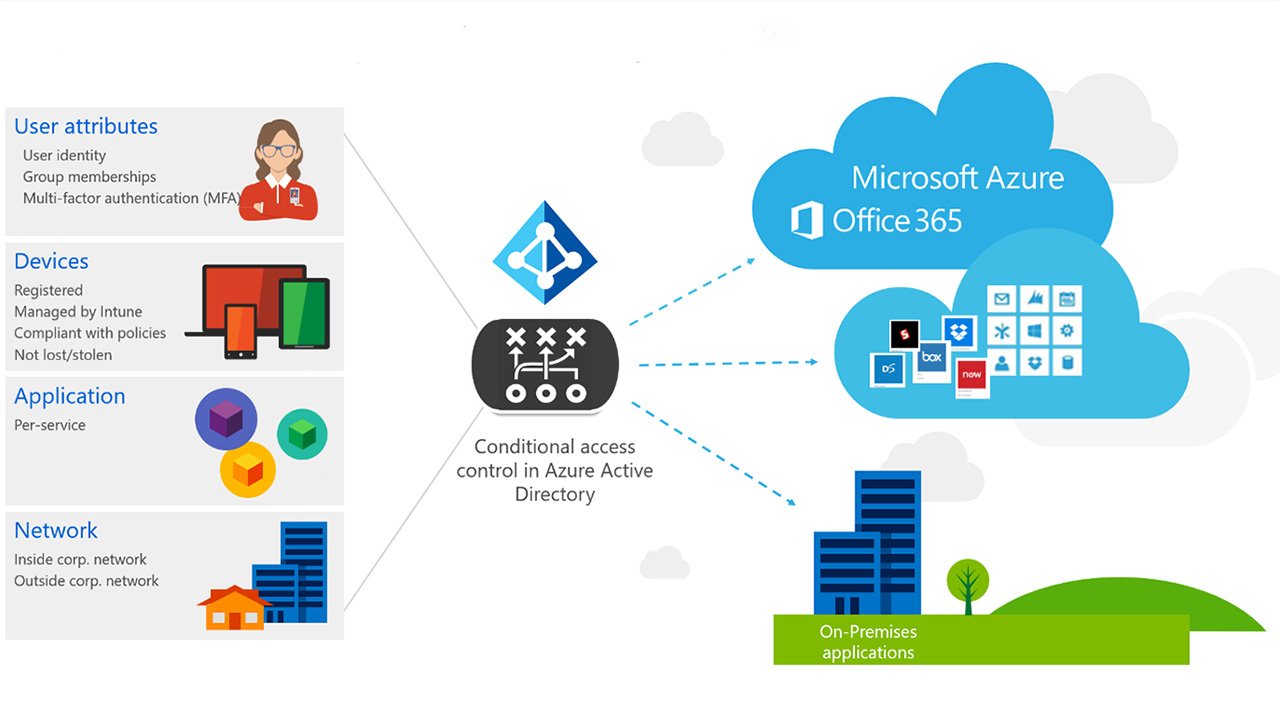


Figure 4: Conditional Access Controls [Reference](https://winbuzzer.com/2016/10/05/microsoft-generally-releases-azure-ad-conditional-access-policies-xcxwbn/)

* 1. **Have a separate identity source for non-employees**. Wipro guides to invite non-employees as guest users in Azure AD, creating user accounts in the external identity source, or provisioning accounts through a federated identity provider, depending on the chosen identity source. Revoke access for non-employees who no longer require it.
  2. **Preferably use password less methods or opt for modern password methods**: Wipro directs to use password less authentication methods supported by Azure AD, such as Microsoft Authenticator app, Windows Hello, and FIDO2 security keys.
     1. Windows Hello is a biometric authentication feature in Windows operating systems that allows users to authenticate to their devices using various biometric factors, such as facial recognition, fingerprint recognition, or iris recognition.
     2. FIDO2 security keys are physical devices that users can plug into their devices, such as a USB port, and use to authenticate without the need for a password. This eliminating the risk of password-related attacks, such as phishing, brute force, and password spraying.
     3. Password less methods for service accounts includes certificate-based authentication or managed identities for Azure resources.



Figure 5: Password less authentication [Reference](https://www.bing.com/images/search?view=detailV2&ccid=cT1ASIhr&id=05179A713312BF6EEB2350658CA09726071A423B&thid=OIP.cT1ASIhrKSczwDlei7lW8AHaCJ&mediaurl=https%3a%2f%2foceanleaf.ch%2fcontent%2fimages%2f2021%2f11%2fpassword-less-methods.png&exph=580&expw=2000&q=modern+password+less+methods+&simid=608016551813716969&FORM=IRPRST&ck=50BD5DE177917B928B513B5EDA7583D9&selectedIndex=18)

* 1. **Block legacy protocols and authentication methods. Wipro highly object using common legacy and** authentication methods like:
     1. SMBv1 (Server Message Block version 1): SMBv1 is an old network file sharing protocol used by Windows operating systems prior to Windows 10 and Windows Server 2016.
     2. It is recommended to disable NTLM (NT LAN Manager) and use more modern authentication methods, such as Kerberos or OAuth.
     3. SSL (Secure Sockets Layer) and early versions of TLS (Transport Layer Security are deprecated and known to have multiple security vulnerabilities, including POODLE, BEAST, and DROWN attacks. So, Use TLS 1.3 version.
     4. It is recommended to use more secure authentication methods, such as multi-factor authentication (MFA) or OAuth, instead of basic authentication.
     5. It is important to enforce strong password policies, such as using long, complex passwords with a combination of letters, numbers, and special characters, and regularly changing passwords to prevent unauthorized access.

## **Networking Security:**

* 1. **Segment network and create secure communication paths between segments**: Wipro guides to determine the different segments like VNets in your network based on factors such as department, location, or sensitivity of data and specify what traffic is allowed or denied between segments through firewalls and NSG rules.

Graphical user interface, application

Description automatically generated

Figure 6: Network Level segmentation [Reference](https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/network-level-segmentation)

* 1. **Protect all public endpoints with Azure Front Door, Application Gateway, Azure Firewall, Azure DDoS Protection:** 
     1. Wipro mentioned that Front Door can be configured to route traffic to backend services, such as web apps or APIs, and apply various security features like Web Application Firewall (WAF), SSL/TLS termination, and custom domain management. Front Door also offers DDoS protection and can automatically mitigate common DDoS attacks.
     2. Wipro suggest using Application Gateway to protect your web applications from common web vulnerabilities, such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF). Application Gateway can also provide SSL offloading, which allows you to terminate SSL/TLS connections at the gateway, reducing the load on your backend servers.
     3. Wipro recommend using Azure Firewall to create and enforce network and application-level policies to allow or deny traffic based on application protocols, ports, and IP addresses. It can also integrate with Azure Sentinel, a cloud-native security information and event management (SIEM) service, for advanced threat detection and response.
     4. Azure DDoS Protection Basic is automatically enabled for all Azure resources by default, and you can configure it to monitor, detect, and mitigate DDoS attacks in real-time.

A diagram of a network

Description automatically generated with low confidence

Figure 7: Protect all Public endpoints [reference](https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-protection-reference-architectures)

* 1. **Keep virtual machines private and secure when connecting to the internet with Azure Virtual Network NAT (NAT gateway):** 
     1. When creating VMs within an Azure virtual network, Wipro guides to use private IP addresses to keep the VMs isolated from the public.
     2. Wipro recommends using Network Security Groups (NSGs) to apply inbound and outbound rules to control traffic to and from the VMs. For outbound traffic, allow only necessary protocols and ports required for the VMs to communicate with the internet, and deny all other traffic. This helps in reducing the attack surface and limiting the outbound traffic from VMs.
     3. Wipro suggest deploying a NAT gateway in virtual network to enable outbound internet connectivity for VMs. NAT gateway provides a secure and controlled way for VMs to access the internet using private IP addresses. It acts as a bridge between the private IP addresses of the VMs and the public IP addresses of the internet, allowing VMs to securely access the internet without exposing their private IP addresses to the public.
     4. Wipro mandate to enable logging and monitoring for the NAT gateway to capture and analyze the traffic going through it. This helps in detecting any unusual or suspicious activity and enables you to take appropriate action to mitigate potential security threats.
     5. Wipro proposes keeping VMs up to date with the latest security patches and updates to protect against known vulnerabilities. Regularly review and apply security updates to the VMs to keep them secure and protected from potential attacks.
     6. Wipro guides using strong authentication methods, such as SSH keys or Azure AD-based authentication, to authenticate and authorize access to VMs. Restrict access to VMs only to authorized personnel, and regularly review and update access permissions to prevent unauthorized access.
     7. Wipro suggest following Azure security best practices, such as using Azure Managed Disk for VM storage, enabling Azure Security Center for threat detection and monitoring, and implementing backup and disaster recovery solutions for VMs, to enhance the overall security posture of your virtual network.

A diagram of a network

Description automatically generated with low confidence

Figure 8: Outflow of traffic using NAT gateway

## **Data Protection Security:**

* 1. Wipro guides using identity-based storage access controls that help ensure that your sensitive data is protected from unauthorized access and theft. This involves configuring access policies that define who can access specific files or folders, and what level of access they have (read-only, read-write, etc.).
  2. Wipro advises to use built-in features for data encryption for Azure services. Some of the built-in features for data encryption in Azure services:
     1. **Azure Disk Encryption**: This feature encrypts virtual machine disks using industry-standard encryption algorithms such as BitLocker or DM-Crypt. This helps protect your data in case of theft, unauthorized access, or if your data is accessed by someone who is not authorized to do so.
     2. **Azure Storage Service Encryption**: This feature encrypts data at rest in Azure Storage using 256-bit AES encryption. It also supports customer-managed keys for greater control over data access.
     3. **Azure SQL Database Transparent Data Encryption**: This feature encrypts data at rest in Azure SQL Database using a symmetric key. This helps protect against unauthorized access to your data and can help you comply with regulatory requirements.
     4. **Azure Key Vault**: This feature enables you to securely store and manage cryptographic keys and secrets used for data encryption in Azure. This helps protect your data from unauthorized access and ensures that your encryption keys are managed securely.

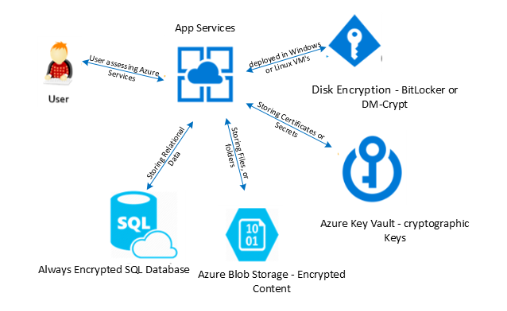


Figure 9: In-Built Encryption

* 1. Wipro suggests classifying all stored data and encrypt it. Some steps to classify and encrypt stored data:
     1. Start by identifying all the types of data to be stored, including customer information, financial data, and intellectual property.
     2. Next, classify data according to its sensitivity and risk level. This could involve creating different categories such as highly sensitive, sensitive, and non-sensitive data.
     3. Next, determine which data requires encryption. For example, highly sensitive data such as credit card numbers and social security numbers may require stronger encryption than non-sensitive data.
     4. Choose encryption methods that are appropriate for data types and encryption requirements. For example, you might use AES encryption for highly sensitive data, while using a less intensive encryption method for less sensitive data.
     5. Finally, implement encryptions for all classified data, making sure to use strong encryption keys and protect them using access controls and other security measures.
     6. Wipro guides protecting data moving over a network through encryption at all points so that it's not accessed unauthorized users. Use secure communication protocols such as HTTPS, or TLS to encrypt data in transit. These protocols provide a secure channel for data to be transmitted over the network.
  2. Wipro suggests storing keys in managed key vault service with identity-based access control and audit policies.
  3. Wipro guides rotating keys and other secrets frequently to reduce the risk of security breach.
     1. Define a key rotation policy that specifies how often keys and other secrets should be rotated.
     2. Use automation tools to rotate keys and other secrets on a regular basis.
     3. Manage and protect old keys and other secrets to ensure that they are securely disposed of or archived.
     4. Test key rotation processes to ensure that they are working as intended and that the new keys and secrets are being used properly.
     5. Monitor for issues: Monitor for any issues or errors during the key rotation process, such as failed rotations or unexpected downtime. This can help you quickly identify and resolve any issues that may arise.

## **Governance and Compliance:**

Governance defines how is the organization's security going to be monitored, audited, and reported? Compliance defines what regulations and standards to be followed like CIS benchmark, NIST etc.

* 1. Wipro recommends creating a landing zone for the workload.
     1. Use Infrastructure as Code (IaC) as Terraform or CloudFormation that can be used to create a repeatable infrastructure deployment. These tools allow you to define the infrastructure as code, which can be versioned, tested, and deployed automatically.
     2. Implement security controls such as firewalls, network security groups, and access controls to ensure that the landing zone is secure. Use best practices such as the principle of least privilege to minimize the attack surface.
     3. Automate workload deployment such as Ansible or Chef to automate the deployment of workloads into the landing zone. This ensures that the deployment is repeatable and consistent.
  2. Enforce creation and deletion of services and their configuration through Azure Policies. If any non-compliance issues are detected, take corrective action to bring the resources into compliance with the policy. This could involve deleting unauthorized resources or configurations or modifying existing resources to comply with the policy rules.
  3. Wipro suggest ensuring consistency across the enterprise by applying policies, permissions, and tags across all subscriptions through careful implementation of root management group.
     1. **Create a root management group**: The root management group is the top-level management group in your hierarchy. It represents your entire organization and is used to apply policies, permissions, and tags across all subscriptions. To create a root management group, you need to have the Owner or Contributor role at the tenant level.
     2. **Define policies**: Policies are used to enforce standards and governance across all subscriptions in your organization. By defining policies at the root management group level, you can ensure that they are applied consistently across all subscriptions. Policies can be used to enforce security controls, compliance requirements, and other standards.
     3. **Assign permissions**: Permissions are used to control access to resources in your subscriptions. By assigning permissions at the root management group level, you can ensure that they are applied consistently across all subscriptions. You can assign permissions to users, groups, and applications.
     4. **Apply tags**: Tags are used to categorize resources and enable cost allocation and reporting. By applying tags at the root management group level, you can ensure that they are applied consistently across all subscriptions. Tags can be used to identify resources by department, project, or cost center.Top of Form
  4. Wipro guides to understand regulatory requirements such as GDPR, HIPAA, PCI DSS, or SOC 2 and operational data like customer data, financial data, or employee data that may be used for audits.
  5. Wipro recommends to Continuously monitor using Azure Monitor, Azure Security Center, and Azure Sentinel and assess the compliance like industry-specific regulations or internal policies of your workload. Perform regular attestations such as self-assessments, engaging with third-party auditors, or completing compliance questionnaires to avoid fines.
  6. Wipro suggests reviewing and apply recommendations given by Defender for Cloud, Azure Advisor.
  7. Wipro ask to remediate basic vulnerabilities such as such as weak passwords, unpatched A screenshot of a computer

     Description automatically generated with medium confidencesoftware, and misconfigured network security to keep the attacker costs high. Implement basic security controls such as multi-factor authentication, network segmentation, and encryption of data at rest and in transit.

Figure 9: Defender for Cloud for Compliance and Governance

## **Application and Services Security:**

* 1. Wipro suggest to Identity and classify applications based on high potential impact and high potential exposure to risk. For example, applications that process sensitive data or support critical business processes may be categorized as high impact/high risk.
  2. Wipro recommends to choose native capabilities like Azure Active Directory ([Azure AD](https://learn.microsoft.com/en-us/azure/active-directory/)), [Azure AD B2B](https://learn.microsoft.com/en-us/azure/active-directory/b2b/), [Azure AD B2C](https://learn.microsoft.com/en-us/azure/active-directory-b2c/), or third-party solutions to authenticate and grant permission to users, partners, customers, applications, services, and other entities.
  3. Wipro states to use established capabilities from cloud providers such as native encryption in cloud services to encrypt and protect data. If direct use of cryptography is required, use well-established cryptographic algorithms, and not attempt to invent their own.
  4. Wipro guides to use managed identity services to authenticate then using any keys or username and passwords

# Case Study – Wipro

One of the Wipro Germany clients, who is into aluminium rolling and recycling manufacturing company wants to migrate from its parent company, due to some disputes. They want to migrate their Users and Servers from their parent company to Azure cloud.

## **Migration Challenges**

* Identify Users and seamlessly allow them to access existing applications, they were already using. Create their new User ID and email Id but still letting them use the applications and servers with same privileges and MFA authentication.
* Segregate parent company servers from newly formed company servers and migrate them to new Azure Subscription without compromising the security.
* Understanding the existing newly formed company On-premises infrastructure like firewall and Zscalar settings and securing existing endpoints like laptops, desktops and mobile.
* Parent company was charging newly formed company for every information and therefore not actively responding during assessment to migration process. Delay in responds from parent company causing delay in assessing and migrating servers and users.

## **Security Challenges**

* **External attack**: During migration hackers get activated and start finding loopholes like hacking management ports (RDP ports) and sent malware, e.g., trojan, send phishing emails, leverage social engineering to steal passwords, plan DDoS attacks.
* **Data Exposure**: Business suffers data loss due to incomplete, corrupt, and missing files.
* **Access management**: While migrating, instead of following least access permission and MFA enabled access to users (who are migrating and performing one or another task in Azure Subscription) if given full privileges or admin or contributor role then it opens new attack surfaces and unauthorized access to sandbox environment.
* **Lack of Employee training**: Employees might make errors that could corrupt, erase, or expose business data during the migration process. An employee can unintentionally share files with confidential information while transferring workloads.
* **Faulty Organisation onboarding process**: An insider agent or an employee working on behalf of outsider hackers to send information.
* **Lack of Governance**: Insufficient policies and controls are added during migration that leads to misconfigurations and exposing workloads to public.
* **Lack of Cyber Security skilled resources:** Resourcesonboarded are not cloud skilled to maintain secure network, endpoints, and access management.
* **Lack of planning**: Insufficient inventory details causes lack of planning like priority setting and addressing their dependencies.
* **Patching**: Outdated versions of Windows Server across their computer systems
* **Poor tracking, monitoring and alert system:** Poor tracking, monitoring and alert system is a challenge to security. Policies must be defined in compliance with industry regulations. Monitoring monitors health, performance and security of Azure resources and alerts can be used to notify relevant stakeholders about potential security incidents or performance anomalies in real-time.
* **Missing Audit:** It's important to review and configure logging and auditing settings for all relevant cloud services, third-party services, and custom applications or scripts. Regularly reviewing and analysing audit logs can help you detect and respond to potential security incidents and ensure compliance with organizational and regulatory requirements.
* **Week encryption and decryption algorithm**. To mitigate risks associated with weak encryption and decryption practices, it's important to follow best practices for encryption and decryption, such as using strong encryption algorithms, implementing robust key management practices, using secure key exchange mechanisms, enforcing strong password policies, and optimizing encryption and decryption performance.

## **Implementation/Solution**

Considering all the security parameters above, in Azure following Azure Services were implemented.

* Data exfiltration and Security is managed through Microsoft 365 defender for emails.
* NSG, ASG, Firewall, Zscalar manages traffic incoming and outgoing rules.
* Palo Alto VM Series 500 was used as Firewall to filter traffic and route to the respective servers.
* Security monitoring and Governance is maintained through Log Analytics, Defender for Cloud, Azure Policies, Conditional Access policies.
* Hardening of Azure VM’s are managed for regular updates and patches.
* Next generation Anti-Virus CyberReason was used for Servers and Endpoints protection.
* PKI was for issuance of multipurpose certificates.
* AD connect was used for Syncing of users from On Premises Active Directory to Azure Active directory.
* Forcepoint DLP Endpoint solution was used to monitor, detect, and restrict loss of sensitive data through the Endpoint risk vectors like USB, FTP, HTTP/HTTPS, Endpoint applications, Endpoint LAN’s, and Endpoint Printing.
* Built-in Windows/Linux data protection feature, bitlocker was used to encrypts drives, and prevents the theft of data.
* For performing infrastructure vulnerability assessments and reporting, a cloud-based infrastructure vulnerability management solution (Qualys) was used in SPEIRA Azure cloud.
* Setup of SIEM solution at Speira leveraging Wipro’s Security Intelligence as a Service model (SIaaS) based on IBM Qradar platform on Multitenancy.
* Just-in-time VM access to be leveraged to lock down inbound traffic to critical Azure VMs.
* Azure WAF over Application Gateway to be leveraged for critical web applications.
* Azure DDoS Protection STANDARD service to be leveraged for prevention again DDoS attacks.
* Multi Factor Authentication for Users was incorporated.
* TLS is used for data-in-transit protection and Transparent data encryption is used for data-in-rest protection.
* RDP/SSH access to all these critical workloads to be restricted using -   
     1.  Bastion Host   
     2.  IP addresses to be explicitly configured in NSG.
* Azure Active Directory have Global Administrators and two or more emergency access (break glass) accounts to be created as per Microsoft recommendation.

A picture containing text, diagram, screenshot, plan

Description automatically generated

A picture containing text, screenshot, font, number

Description automatically generated

# Referrals

[Network-level segmentation workloads - Azure Architecture Center | Microsoft Learn](https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/network-level-segmentation)

[Azure DDoS Protection reference architectures | Microsoft Learn](https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-protection-reference-architectures)

[modern password less methods - Bing](https://www.bing.com/images/search?view=detailV2&id=05179A713312BF6EEB2350658CA09726071A423B&thid=OIP.cT1ASIhrKSczwDlei7lW8AHaCJ&exph=580&expw=2000&q=modern+password+less+methods+&form=IRPRST&selectedindex=18&vt=0&sim=11)

[Microsoft Generally Releases Azure AD Conditional Access Policies - WinBuzzer](https://winbuzzer.com/2016/10/05/microsoft-generally-releases-azure-ad-conditional-access-policies-xcxwbn/)

[Securing Azure Services with Managed Identities | Marczak.IO | Adam Marczak](https://marczak.io/posts/2019/07/securing-websites-with-msi/)

# Conclusion

Data security is a critical aspect of modern-day business operations. Organisations must take proactive measures to safeguard their data against unauthorised access, theft, and data breaches. Organisations should implement a range of security measures including access control, encryption, data backup and recovery, regular software updates and employee training and education to ensure the confidentiality, integrity, and availability of their data. By taking a proactive approach to data security, organisations can minimize the risk of data breaches and protect their sensitive information.

1. About the author/s

Preity Gupta [www.linkedin.com/in/preitygupta](http://www.linkedin.com/in/preitygupta):

* Certified Cloud Security Leader with 16+ years of extensive experience in strategizing Cloud Security posture for vivid clients
* Outstanding talents in Governance, Compliance, Risk management, Cloud Security, Application Security, Integration Security, Infrastructure Security, Data Security, Technical leadership, and people management.
* Strong Analytical, Organizational, and Problem-solving skills, with highest levels of ethical, professional, and personal excellence.
* Areas of Expertise: - Cloud Architecture & Strategy | Cloud Transformation & Migration |
* Cloud Security Architecture| Cloud Security Posture Management

1. Reviewer

Dilip Subramanian, Specialist Senior Manager (Chief Cloud Architect)

dilip.subramanian@wipro.com