INTERCEPT

Azure Security Best Practices Checklist

This checklist includes a brief overview of the **best practices for securing your workloads in Azure** based on the insights from “Azure Security Best Practices”.

Identity and Access Management (IAM)

☐ **Adopt Zero Trust:** Enforce Zero Trust where every access request is strictly verified, and no entity is trusted by default from inside or outside the network.

☐ **Enable Multi-Factor Authentication (MFA):** Set up MFA for all users with security defaults, conditional access or risk-based conditional access.

☐ **Set up a Conditional Access:** Configure at minimum Conditional Access-Based (P1) policy for more granular control or upgrade with Risk-Based Conditional Access (P2).

☐ **Apply Single sign-on (SSO):** Configure SSO to allow users to log in once and access all associated applications seamlessly.

☐ **Employ role-based access control (RBAC):** Implement RBAC to grant granular permissions, enabling administrators to manage access securely.

☐ **Leverage Passwordless Authentication:** Allow users to access services without traditional passwords.

☐ **Employ Multiple Layers of Security:** Build a fortress starting with strong passwords, then layer on MFA, conditional access, and Privileged Identity Management (PIM).

☐ **Deploy Privileged Identity Management (PIM):** Use for just-in-time and approval-based high-level admin access.

Network Security

☐ **Use Azure Firewall:** Strengthen your network with Azure Firewall, DDoS protection, intrusion detection, and vulnerability management.

☐ **Monitor Network Performance:** Use Azure Monitor and Network Watcher for real-time monitoring and diagnostics.

☐ **Apply Network security groups (NSGs):** Use NSG’s on subnets for broad control or on VMs for traffic management.

☐ **Utilise Azure Virtual Network:** Connect and manage Azure services and on-premise infrastructure securely with Azure Vnets.

☐ **Use ExpressRoute:** Opt for ExpressRoute for a secure, direct connection to Azure, not the public internet.

☐ **Restrict access to your Virtual Machines:** Disable RDP and SSH ports and use Azure Bastion for safe remote access without public internet exposure.

☐ **Implement the Hub-Spoke Model:** Use the Hub-Spoke model for streamlined network management and security.

☐ **Leverage Azure Private Link:** Connect your Azure services directly and securely without public internet exposure.

Protecting Secrets

☐ **Protect your secrets with Azure Key Vault:** Store secrets, keys and certificates in Azure Key Vault to manage them without exposing sensitive data.

☐ **Rotate Secrets Regularly:** Automate key and secret rotation to reduce old credentials being exploited.

☐ **Enable Soft Delete:** Enable soft delete for deleted keys and secrets for when it's accidentally deleted, etc.

☐ **Leverage Managed Identities:** Use Azure-managed identities to access services without embedded credentials.

☐ **Implement Secret Scanning Tools:** Deploy secret scanning tools in your CI/CD pipeline to detect and prompt secret replacement.

☐ **Avoid Hardcoding Secrets:** Store secrets in environment variables or config tools not in code.

☐ **Implement Network Isolation:** Use firewalls and network security groups to limit access to key vaults.

☐ **Monitor and Log Access:** Monitor secret access and activity with Azure Monitor and Key Vault logs.

☐ **Use HSM-Protected Keys:** For highly sensitive data, consider using HSM to protect encryption keys in Azure Key Vault.

Data Protection

☐ **Endpoint Protection:** Enforce security policies on all devices accessing data.

☐ **Secure Management Workstations:** Utilise privileged access workstations to reduce the attack surface and secure sensitive tasks and data.

☐ **Disk Encryption:** Use Azure Disk Encryption on Linux and Windows VMs to protect data at rest.

☐ **Use HTTPS for Azure Storage:** Use HTTPS for Azure Storage, whether through the portal or storage REST API.

☐ **Establish Secure Network Connections:** Use site-to-site and point-to-site VPNs for connecting networks and workstations to Azure.

☐ **Encrypt Confidential Files:** Encrypt sensitive data in your cloud storage or server using AES-256.

☐ **Secure data in transit:** Employ Transport Layer Security (TLS) 1.3 to encrypt data in transit.

Operational Security

☐ **Leverage Azure Policy:** Enforce security policies across all devices accessing data to maintain consistent protection regardless of location.

☐ **Update software regularly:** Schedule updates, use Azure Update Management to keep VMs up-to-date and automate updates with Azure Automation.

Bonus Tips

☐ **Enable Microsoft Defender for Cloud:** Use Defender for Cloud to check your resources' security and be alerted when something needs your attention.

☐ **Separate Azure subscription for production:** Keep production data and other assets out of your dev/test environments and apply different policies across resources in multiple subscriptions.

Download this checklist & follow the tips if you want a secure Azure environment!

Remember, there is *no such thing as a silver bullet* when it comes to security. It is an ongoing process that requires constant attention and adaptability to withstand increasingly sophisticated cyberattacks. Continuously test and evaluate your functionalities to ensure they function as expected to secure your Azure environment.

Want a Free Azure Security Scan?

After the scan, you will receive:

- ✓ Confirmation and additional insight into the actual safety of your environment.
- ✓ A verification that your security aligns with Microsoft's best practices (a proven footprint).
- ✓ The free benefit of an expert review.

Click on the URL below:
Azure Security Scan

Does security feel like an uphill battle to you? Intercept can help you!
As Azure Expert MSP partner, and dedicated cloud specialist, we can protect your cloud infrastructure, and ensure your organisation remains safe and compliant.

Get in touch!
(+31) 38 777 98 20
info@intercept.cloud