Deploying a cloud application on Azure is fast, easy, and cost-effective. Before deploying an application, it's useful to have a checklist. A checklist can assist you in evaluating your application against a list of essential and recommended security actions.

Introduction

Azure provides a suite of infrastructure services that you can use to deploy your applications. Azure Operational Security refers to the services, controls, and features available to users for protecting their data, applications, and other assets in Microsoft Azure.

To get the maximum benefit out of the cloud platform, we recommend that you use Azure services and follow the checklist. Organizations that invest time and resources assessing the operational readiness of their applications before launch have a higher rate of satisfaction than those that don't. When performing this work, checklists can be an invaluable mechanism to ensure that applications are evaluated consistently and holistically.

Checklist

This checklist is intended to help enterprises think through various operational security considerations as they deploy sophisticated enterprise applications on Azure. It can also be used to help you build a secure cloud migration and operation strategy for your organization.

Checklist Category	Description
Security Roles & Access Controls	• Use Azure role-based access control (Azure RBAC) to provide user-specific that used to assign permissions to users, groups, and applications at a certain scope.
Data Protection & Storage	• Use Management Plane Security to secure your Storage Account using Azure role-based access control (Azure RBAC). • Data Plane Security to Securing Access to your Data using Shared Access Signatures (SAS) and Stored Access Policies. • Use Transport-Level Encryption – Using HTTPS and the encryption used by SMB (Server message block protocols) 3.0 for Azure File Shares.
Checklist Category	**Description**
	• Use Client-side encryption to secure data that you send to storage accounts when you require sole control of encryption keys.

	• Use Storage Service Encryption (SSE) to automatically encrypt data in Azure Storage, and Azure Disk Encryption for Linux VMs and Azure Disk Encryption for Windows VMs to encrypt virtual machine disk files for the OS and data disks. • Use Azure Storage Analytics to monitor authorization type; like with Blob Storage, you can see if users have used a Shared Access Signature or the storage account keys. • Use Cross-Origin Resource Sharing (CORS) to access storage resources from different domains.
Security Policies & Recommendations	• Use Microsoft Defender for Cloud to deploy endpoint solutions. • Add a web application firewall (WAF) to secure web applications. • Use Azure Firewall to increase your security protections. • Apply security contact details for your Azure subscription. The Microsoft Security Response Center (MSRC) contacts you if it discovers that your customer data has been accessed by an unlawful or unauthorized party.
Identity & Access Management	• Synchronize your on-premises directory with your cloud directory using Azure AD. • Use single sign-on to enable users to access their SaaS applications based on their organizational account in Azure AD. • Use the Password Reset Registration Activity report to monitor the users that are registering. • Enable multi-factor authentication (MFA) for users. • Developers to use secure identity capabilities for apps like Microsoft Security Development Lifecycle (SDL) . • Actively monitor for suspicious activities by using Azure AD Premium anomaly reports and Azure AD identity protection capability.
Ongoing Security Monitoring	• Use Malware Assessment Solution Azure Monitor logs to report on the status of antimalware protection in your infrastructure. • Use Update Management to determine the overall exposure to potential security problems, and whether or how critical these updates are for your environment. • The Azure Active Directory portal to gain visibility into the integrity and security of your organization's directory.

Checklist Category	Description
Microsoft Defender for	• Use Cloud Security Posture Management (CSPM) for hardening guidance that helps you efficiently and effectively improve your

Cloud detection capabilities	security. • Use alerts to be notified when threats are identified in your cloud, hybrid, or on-premises environment. • Use security policies, initiatives, and recommendations to improve your security posture.

Conclusion

Many organizations have successfully deployed and operated their cloud applications on Azure. The checklists provided highlight several checklists that are essential and help you to increase the likelihood of successful deployments and frustration-free operations. We highly recommend these operational and strategic considerations for your existing and new application deployments on Azure.

Next steps

To learn more about security in Azure, see the following articles:

- Shared responsibility in the cloud.
- End-to-end security in Azure.
- Ransomware protection in Azure