Microsoft

WorkshopPLUS - Microsoft Azure: Security Best Practices

WorkshopPLUS

Maximise Your Investment in Microsoft Azure and Increase Your Security Posture for Application and Data Access

Target Audience:

This workshop is intended for organisations who use Microsoft Azure and would like to understand and explore the security features available.

Overview

In today's complex and regulated environment, businesses need to focus on building secure solutions in the cloud that deliver value to their customers, partners, and shareholders. Cloud computing offers an opportunity to transfer some of the cost, risks, and effort of managing an IT infrastructure to an independent and experienced provider.

Microsoft has decades-long experience building enterprise software and running some of the largest online services in the world. Microsoft has leveraged this experience to implement and continuously improve security-aware software development, operational management, and threat mitigation practices that are essential increase protection of services and data in the cloud.

The Azure Security workshop provides attendees with broad knowledge and understanding of the key Security features available in Azure.

Key Features and Benefits

Each module presents technical level explanation of Azure security features and recommended best practices.
The lab materials allow participants the opportunity to build their Azure environment from the beginning, while allowing them to focus on the security features described in each module. Both Azure Resource Manager and Azure Service Manager are used during the labs to illustrate their differences.

Takeaways:

After completing this workshop you will gain broad knowledge about key Security features available in Azure that will help you decide what is best for you to secure your environment, based on the following Microsoft's foundational principals:

- Security: Our priority is to safeguard your data with state-of-the-art technology, processes, and encryption.
- Privacy and control: You control the privacy of your data, who has access to it, and where it resides.
- Compliance: We will always offer the largest portfolio of compliance standards and certifications in the industry.
- Transparency: You will always have complete visibility into where your data is located and how it's managed.

Delivered by experienced Microsoft engineers, the AZURE Security workshop helps you understand and implement security features on Azure.

Pre-requisites:

- Familiarity with Microsoft infrastructure components (i.e. Active Directory, Windows Server/Client)
- Understanding the differences between ASM and ARM
- Exposure to deployment of resources in both models using the Portal and PowerShell
- Exposure to ARM Templates

Key Focus Areas:

- Data Security and Compliance
- Identity Protection
- Securing Azure access
- Web Security
- Auditing and Monitoring

Syllabus

This workshop runs for 3 full days. Students should anticipate consistent start and end times for each day. Early departure on any day is not recommended.

Module 1: Introduction to Microsoft Azure Security: This module introduces the Security technologies available on Microsoft Azure, an overview of Microsoft's Cybersecurity Architecture and how you can leverage the Cloud to improve protection, detection, and response against threats.

Module 2: Network Security : This module introduces the components available to secure network communications in Azure. You will learn how to use Network Security Groups to create rules (ACLs) to control access by permitting or denying communication between the workloads, as well as configure secure communications between on premises to Azure.

Module 3: Cloud Identity and Access : This module introduces the "Identity is the new perimeter" concept and will describe the risk events and potential vulnerabilities affecting your organization's identities, and how Azure security features can help mitigate those risks, such as security controls available in Microsoft Azure Active Directory (Azure AD), Azure AD Application Proxy, Privileged Identity Management, and Cloud App Security.

Module 4: Encryption and Data Protection : This module introduces the Azure key vault and various scenarios it can be used to encrypt and protect your data in Azure. This includes encrypting data at rest, in transit, and in use, by authenticating only authorized users against the database or application, and limiting user access to the appropriate subset of data.

Module 5: Threat management: In this module you will learn the importance of deploying any kind of antimalware solution to Azure Virtual Machines. You will be introduced to the Microsoft Antimalware architecture, deployment scenarios using PowerShell and the Azure Portal.

Module 6: Azure Web Security: This module covers the common threats of web apps and the capabilities that Azure has to securely manage and access web apps.

Module 7: Azure Monitoring, logging, and reporting : This module covers mechanisms for continuous monitoring and auditing of activities to help in the detection of potential threats and provide a record of critical events in case of a breach. These rich security capabilities are each balanced by the ability to quickly implement features and mitigate security risk without compromising developer productivity or customers' experience.

Microsoft

This data sheet is for informational purposes only.
MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY