Az COMMUNITY

Conference 2022

Asia's Largest Azure Community Conference

#AzConfDev

Ankit Rao

Senior Software Engineer, Zscaler

: @_AnkitRao

: @ankit-rao

#AzConfDev

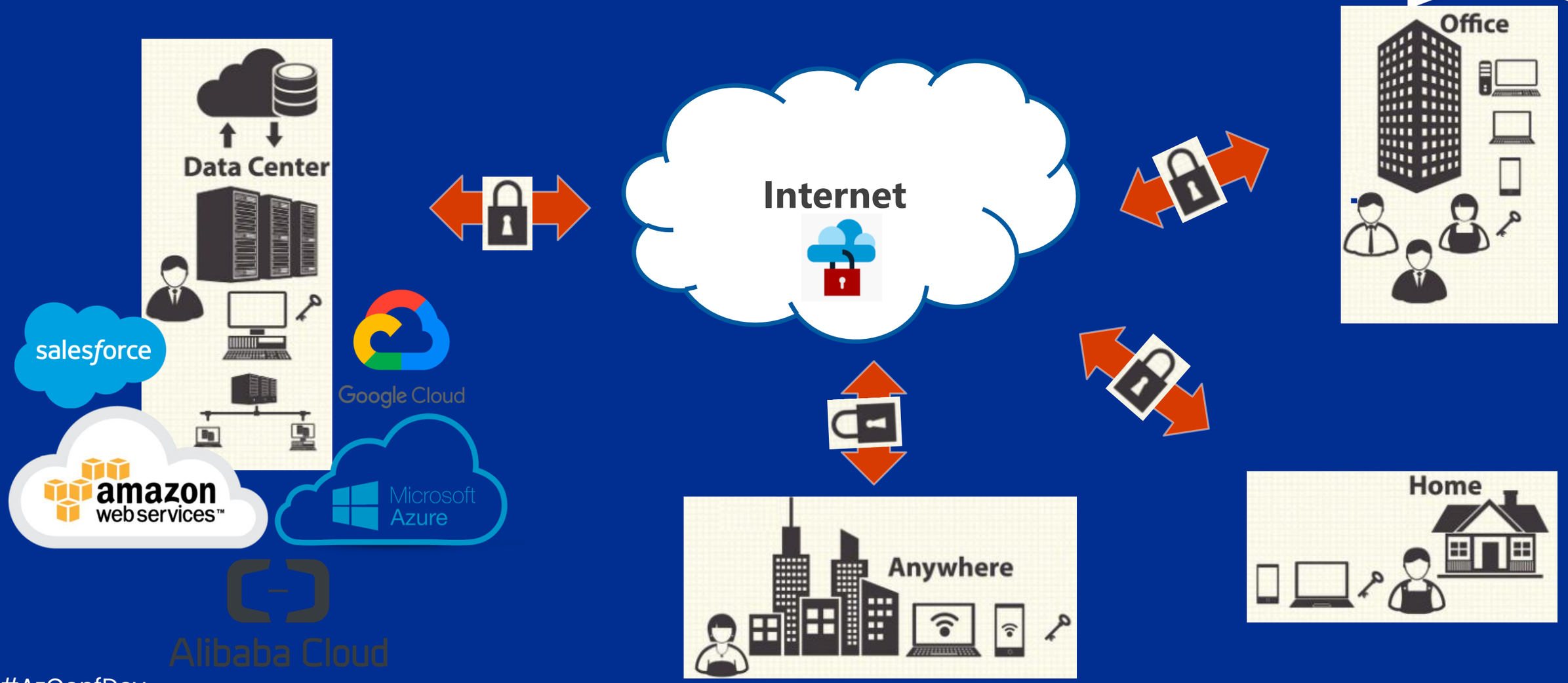
Demystifying Cloud Security for multi-cloud environments using Microsoft Defender for Cloud

#AzConfDev

Agenda

- Motivation
- Cloud Security – A shared responsibility model.
- Cloud Security Posture Management.
- Introduction to Microsoft Defender for Cloud.
- Demo (Multi-cloud Security Posture Management)
- QnA

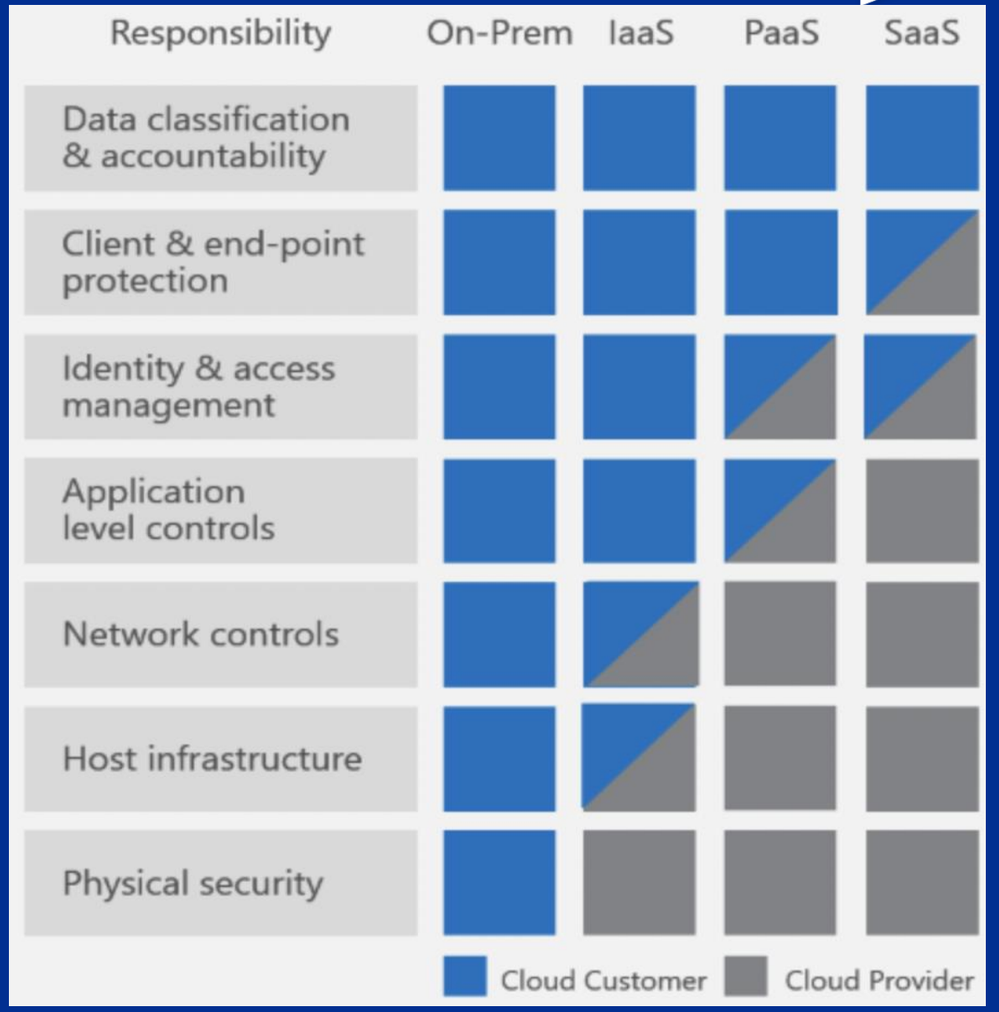
Introduction to Cloud and Public Cloud Service Providers



Cloud Security – A shared responsibility model

- Cloud security refers to the technologies, policies, controls, and services that protect cloud data, applications, and infrastructure from threats.

- Cloud Security is a shared responsibility model. The diagram besides, provides a beautiful illustration of the same.



Cloud security compliance standards

NIST 800-53
NIST 800-171

PCI DSS 3.2

SOC 2

HIPAA

ISO 27001

Challenges involved in implementing Cloud Security

- Lack of cloud security architecture and strategy.
- Distributed and ever-changing nature of cloud.
- Lack of Personnel Experienced in Cloud Security Measures.
- Compliance and Regulations.

Cloud Security Posture Management (CSPM)

- Cloud Security Posture Management (CSPM) is **defined by Gartner** as: "a continuous process of cloud security improvement and adaptation to reduce the likelihood of a successful attack."
- The unique nature of the cloud requires a new security concept that can address the distributed and constantly changing cloud infrastructure.
- CSPM aims to help the user with :

Developing and enforcing end-to-end security policies

Risk & vulnerability assessment and risk visualization

Compliance monitoring, incident response and DevOps integration

Microsoft Defender for Cloud - Features

Defender for Cloud fills three vital needs as you manage the security of your resources and workloads in the cloud and on-premises :

Continuously Assess (Know your security posture. Identify and track vulnerabilities.)	Secure (Harden resources and services with Azure Security Benchmark)	Defend (Detect and resolve threats to resources and services)
•Secure score •Vulnerability assessments •Asset inventory •Regulatory compliance •File integrity monitoring	•Security recommendations •Just-in-time VM access •Adaptive network hardening •Adaptive application control	•Microsoft Defender •Security alerts •Integration with Microsoft Sentinel (or other SIEM)

Microsoft Defender for Cloud - Demo

Overview of the findings provided by Microsoft Defender

- Lack of encryption on databases or data storage, application traffic, especially that which involves sensitive data.
- Improper encryption key management such as not rotating keys regularly.
- Overly liberal account permissions.
- No multi-factor authentication enabled on critical system accounts.
- Misconfigured network connectivity, particularly overly permissive access rules or resources directly accessible from the internet.
- Data storage exposed directly to the internet.
- Logging is not turned on to monitor critical activities such as network flows, database access, or privileged user activity.
- Vulnerability assessments , OS baseline misconfigurations and alerting.

Limitations

- Microsoft Defender for Cloud is still in the initial phase and there is a good room for improvement around the coverage of more security best practices (recommendations).
- No on-demand scan facility yet.
- The alert mechanism is expected to improve overtime.

Microsoft Defender for Cloud - Pricing

Resource Type	Price
Microsoft Defender for Servers	**$14.60**/Server/month Included data - 500 MB/day
Microsoft Defender for App Service	**$14.60**/App Service/month
Microsoft Defender for SQL on Azure	**$15**/Instance/month[2]
Microsoft Defender for Storage[1]	**$0.02**/10K transactions
Microsoft Defender for Kubernetes	**$0.00268**/vCore/hour
Microsoft Defender for ACR	**$0.29**/image
Microsoft Defender for Containers	**$7**/vCore/month [4 5]
Microsoft Defender for Key Vault	**$0.02**/10K transactions

References

- Microsoft Defender for Cloud (Link)
- Microsoft Defender for Cloud pricing (Link)
- Shared responsibility in the cloud (Link)

Platinum Partner

Gold Partner

Silver Partner

Q & A

: @_AnkitRao

: @ankit-rao

#AzConfDev

Thank You!

#AzConfDev