

CUBESYS DISCUSSION SERIES

TOP 10 WAYS TO SECURE YOUR AVD PLATFORM



TODAY'S DISCUSSION FORMAT



The discussion is being recorded.



Please use the chat window to ask your questions.



We have our experts on hand to answer your questions.



The video and content will be sent via email post event.

Top 10 ways to secure your AVD platform

PANEL OF SPEAKERS



Shabaz Darr

Microsoft MVP



Paul Heaton

Co-Founder & CEO
cubesys

Date: Wednesday 18 October 2023 | 10:00 am - 10:45 am AEDT



CUBESYS

TOP 10 WAYS TO SECURE YOUR AVD PLATFORM



Number 1:

Plan your IAM strategy carefully





Number 1:

- Cloud Native?
 - Hybrid?
- Authentication?



Number 2:



Implement robust but flexible
Conditional Access Policies



Number 2:

- Implement MFA
 - Risk/Location
- Corporate or Personal Devices?





Number 3:

Secure your virtual network





Number 3:

- RDP Short-path
- Azure Private DNS
- Azure Private Link



Number 4:



Enable Microsoft Defender for Cloud



Number 4:



- Manage Vulnerabilities
 - Assess Compliance
- Improve Security Posture in AVD





Number 5:

Enable Endpoint Protection





Number 5:

- Install EDR product
- Enable Threat & Vulnerability management



Number 6:



Enable OS Disk Encryption



Number 7:



Implement a regular patch schedule





Number 8:

Configure Session Host Security





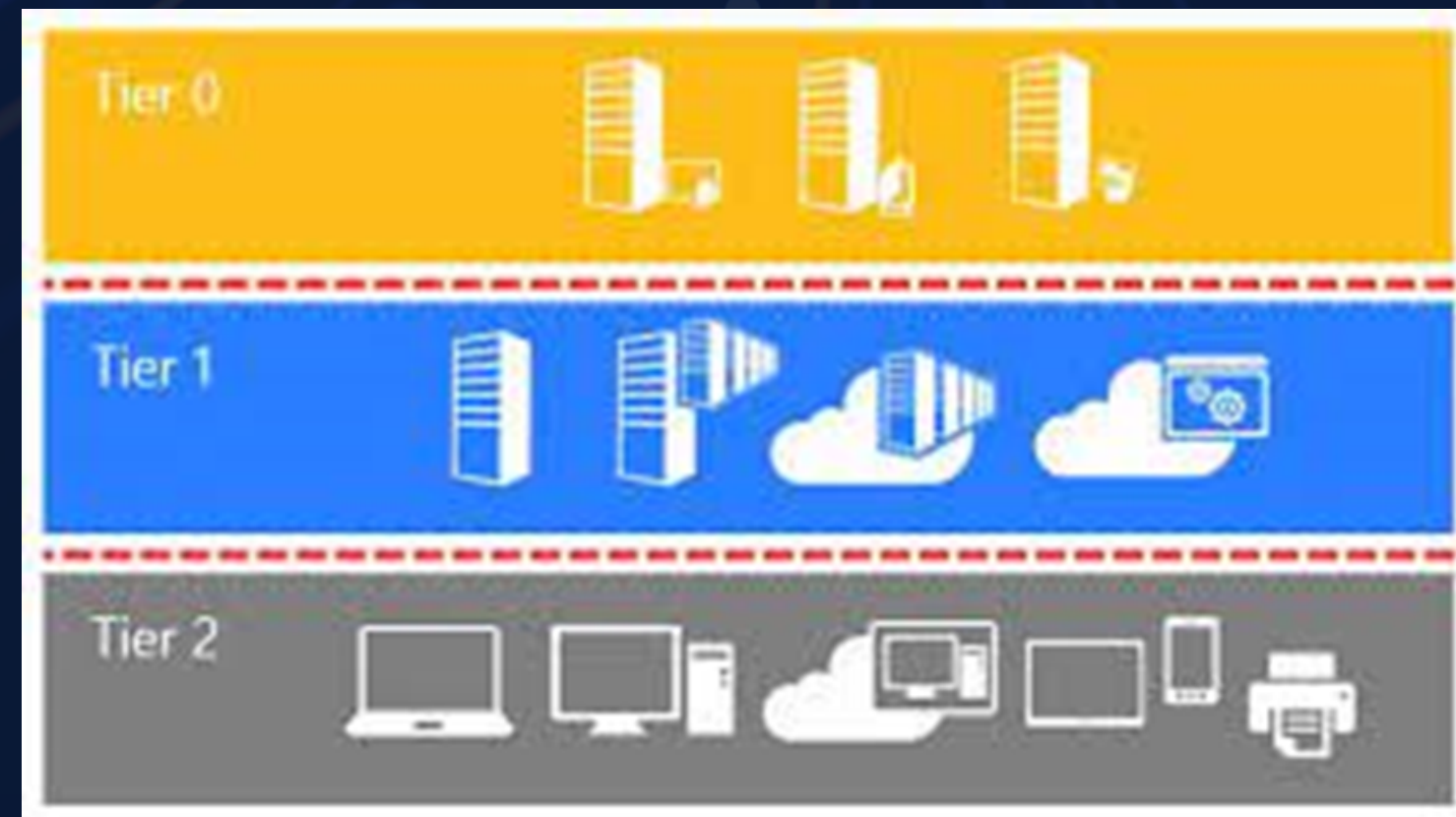
Number 8:

- Max inactive time policy
- Screen lock for idle sessions



Number 9:

Tiered Admin Access



Number 10:



Implement Compliance Policies



Microsoft Intune

CUBESYS DISCUSSION SERIES

TOP 10 WAYS TO SECURE YOUR AVD PLATFORM

Thank you