



**18 APRIL
2026**

**MICROSOFT
MUMBAI**

#GlobalAzure #Apr26MTP #mumtechup








From Root to Rootless: Securing Containers One Layer at a Time



Maninderjit Bindra
Principal Software Engineer
Microsoft

Agenda

Securing Containers on Your Machine

-  The Root User Problem
-  Non-Root Users & Distroless Images
-  The Rootful Daemon Gap — Docker socket escalation & privileged breakout
-  Rootless Containers
-  Sandboxes & MicroVMs
-  The Dev Container Trap
-  Other Traps (like secrets with build args)

Extending these concepts when Moving to the Cloud

 AKS in Production

References

- <https://github.com/manisbindra/sbi> in process of migration to <https://github.com/microsoft/sbi>
- <https://docs.docker.com/ai/sandboxes/>