Shared Responsibility and Key Strategies for Azure environments

Responsibility	SaaS	PaaS	IaaS	On-prem
Information and Data	🟦	🟦	🟦	🟦
Devices (Mobile and PCs)	🟦	🟦	🟦	🟦
Accounts and Identities	🟦	🟦	🟦	🟦
Identity and directory infrastructure	◩	◩	🟦	🟦
Applications	⬜	◩	🟦	🟦
Network Controls	⬜	◩	🟦	🟦
Operating system	⬜	⬜	🟦	🟦
Physical hosts	⬜	⬜	⬜	🟦
Physical network	⬜	⬜	⬜	🟦
Physical datacenter	⬜	⬜	⬜	🟦

⬜ Microsoft 🟦 Customer

ESTABLISH A MODERN PERIMETER

For data across all workloads, organizations should establish a modern perimeter of consistent, centrally managed identity controls to protect their data, devices, and accounts.

MODERNIZE INFRASTRUCTURE SECURITY

For workloads that require managing OS and infrastructure components (PaaS, IaaS, and On-Premises), organizations should take advantage of cloud to modernize their infrastructure and network security strategy as well as integrating security into DevOps process

“TRUST BUT VERIFY” EACH CLOUD PROVIDER

For responsibilities performed by the cloud provider, organizations should take a “Trust but Verify” approach and evaluate cloud providers to ensure they are performing their security responsibilities well