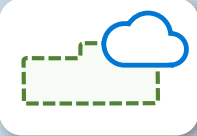
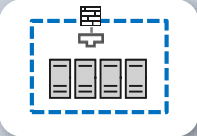
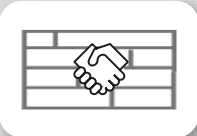


Shared Responsibility and Key Strategies for Azure environments

| Responsibility | SaaS | PaaS | IaaS | On-prem | |
|---------------------------------------|-----------|-----------|-----------|----------|--|
| Information and Data | Customer | Customer | Customer | Customer |  <p>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.</p> |
| Devices (Mobile and PCs) | Customer | Customer | Customer | Customer | |
| Accounts and Identities | Customer | Customer | Customer | Customer | |
| Identity and directory infrastructure | Customer | Customer | Customer | Customer |  <p>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</p> |
| Applications | Microsoft | Customer | Customer | Customer | |
| Network Controls | Microsoft | Customer | Customer | Customer | |
| Operating system | Microsoft | Microsoft | Customer | Customer | |
| Physical hosts | Microsoft | Microsoft | Microsoft | Customer |  <p>“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</p> |
| Physical network | Microsoft | Microsoft | Microsoft | Customer | |
| Physical datacenter | Microsoft | Microsoft | Microsoft | Customer | |

Microsoft
 Customer