

SC-100 Microsoft Cybersecurity Architect

Interactive case study scenario: Enhancing user access control and threat resilience



About the organization

- Contoso Healthcare Solutions provides clinical trial management and health research services across the U.S.
- Headquartered in **Boston**, partnering with hospitals, research institutions, and pharmaceutical companies.
- Operates a **hybrid IT environment**:
 - On-premises datacenters for data storage and archival
 - Microsoft Azure for AI diagnostics and collaborative analytics



Identity & access landscape

- Internal applications use **Active Directory (AD)** for authentication.
- Cloud-based SaaS tools integrated with **Microsoft Entra ID**.
- Access to on-prem clinical systems via **VPN** and **local credentials**.
- External physicians and researchers use **Microsoft Entra External ID** with **multi-factor authentication (MFA)** for secure cloud access.



Challenges:

- Frequent user role changes
- Ad hoc access requests
- Delayed deprovisioning and increased admin burden



Data management & privacy

- Uses **on-prem file servers** and **tape libraries** for research data.
- Tapes are regularly shipped to **offsite locations** for archival.



Challenges:

- Increasing data volumes are straining established storage workflows.
- Heightened focus on patient data privacy and the need to prevent accidental or malicious disclosure of protected health information is adding operational complexity.



Security incident: Ransomware attack

- A targeted **ransomware attack** encrypted parts of the **tape-stored data**.
- Data was recovered using **offsite backups**, but:
 - Clinical trials were delayed
 - Incident response was slow and uncoordinated
 - Regulatory reporting was time-consuming



Post-incident findings:

- Gaps in response tools and coordination
- Systems not aligned with compliance baselines
- Unpatched vulnerabilities in some environments



Your role as security architect

Design a **Zero Trust–aligned security solution** that:

- Addresses **access and identity risks**
- Strengthens **defenses across cloud and on-prem systems**
- Enhances **response, compliance, and business continuity**