Microsoft

Case study scenario summary: Securing endpoints and infrastructure

About the organization

- Litware Inc. is a supplier of robotics and precision automation solutions for the automotive sector.
- Headquartered in Birmingham, UK, with over 40 global sites including production facilities, R&D centers, and logistics hubs.
- Maintains supply chain and manufacturing processes through:
    - Cloud-based systems
    - IoT technologies
    - Data-driven initiatives

Scenario & challenges

IT and cloud environment

Scenario

- Operates a hybrid IT environment with a growing Microsoft cloud presence.
- Azure supports engineering collaboration, telemetry processing, and supplier integration systems.
- Regional teams manage their own Microsoft Azure subscriptions and provision resources ad hoc to support urgent production and logistics needs.

Challenges

- Variability in cloud security configurations across business units due to decentralized provisioning.

On-premises production systems

Scenario

- Production systems in factory environments include:
    - Microsoft Entra-joined Windows 11 engineering workstations
    - Microsoft Entra-registered Red Hat Enterprise Linux (RHEL) gateway appliances
    - IoT sensors and embedded industrial controllers
- Edge computing nodes run Ubuntu Server with containerized workloads.
- These nodes process time-sensitive machine and sensor data locally and forward insights to Azure Log Analytics.

Challenges

- Containerized workloads introduce supply chain vulnerabilities that could compromise manufacturing quality.
- Real-time processing requirements may bypass security controls, risking operational reliability.

Network architecture and OT environment

Scenario

- Operational systems, including IoT devices and OT controllers, are on the same network as plant-floor engineering stations.
- This setup supports communication, firmware updates, and operational efficiency.
- The OT environment includes legacy PLCs and purpose-built sensors.
- Many devices are kept operational beyond their original service timelines due to high replacement cost and complexity.
- Devices rely on proprietary communication methods and default configuration settings that have remained largely unchanged.

Challenges:

- Outdated OT components and default configurations introduce risk.
- Shared network between OT and IT systems increases exposure.

Device management and local autonomy

Scenario

- Endpoint, IoT, and OT devices are managed locally by IT teams at each facility.
- Local teams define patch frequency, configuration baselines, and policy enforcement.
- A variety of third-party antivirus solutions are used across different sites.

Challenges:

- Inconsistent management practices across facilities.
- Varying expertise levels among IT staff lead to delays in vulnerability remediation.
    - Example: Engineering laptops remained exposed to known software flaws for weeks after discovery.
    - Example: A contractor's unpatched laptop accessed internal engineering documentation via a cloud-based resource portal.

Local infrastructure and migration

Scenario

- Each facility hosts localized infrastructure services:
    - Microsoft SQL Server–based databases
    - Linux-based middleware servers
- These systems support production workflows and are being migrated to Azure VMs.

Challenges:

- Ensuring configuration consistency and security oversight during migration.

Security telemetry and monitoring

Scenario

- Security telemetry is processed locally at each facility.
- Telemetry is aggregated regionally using different SIEM and security tools.
- This reflects regional autonomy and differing operational requirements.
- Systems are tailored to local technology stacks and compliance needs.

Challenges:

- Decentralized telemetry systems limit integration.
- Varying tools and processes reduce consistency in threat detection and response.

Your role as a security architect

Analyze Litware Inc.’s current security posture and design a resilient Zero Trust architecture that:

- Strengthens endpoints and infrastructure security
- Does not compromise operational continuity