Site Survey
Client: MyCo
Analyst: Chloe Kilroy
Completed on: 04-19-2025

MyCo Overview:

MyCo is a technology development company located in the Midwest. The company has recently had a security incident involving a break-in which resulted in data loss, account compromises, and the destruction of proprietary R&D data. MyCo has hired Chloe Kilroy as an analyst to propose changes to their infrastructure to prevent similar incidents in the future.

Risk Solutions Quick Overview:

1. FreeNAS 9.1 on 2017 hardware → TrueNAS Enterprise with ZFS, snapshots, off-site replication
2. MS SQL Server 2015 on aging hardware → MS SQL Server 2022 HA Cluster or Azure SQL Managed Instance
3. Single Web Server with no redundancy → Load-Balanced Web Cluster with NGINX/HAProxy
4. FTP Server for file transfers → SFTP Server or Azure Blob Storage with secure, signed access
5. EOL Client Systems (Windows XP/7, old Linux/macOS) → Windows 10/11, Ubuntu LTS, supported macOS + EDR tools deployed

Risk Solutions Breakdown:

Risk 1: EOL NAS Cluster Running FreeNAS 9.1

Problem:
The current NAS system is running FreeNAS version 9.1 on hardware that was purchased in 2017. This version of FreeNAS is end-of-life (EOL), which means it no longer receives security updates or vendor support. Running outdated storage software introduces vulnerabilities such as unpatched remote code execution exploits or privilege escalation flaws. The aging hardware also increases the risk of drive failure or system outages.

Solution:
Upgrade to TrueNAS Enterprise (the modern successor of FreeNAS) deployed on current, enterprise-grade NAS hardware with support for ZFS, snapshots, replication, and encryption. Alternatively, for off-site redundancy and scalability, consider AWS FSx for Windows File Server or Azure Files, which provide managed file storage with enterprise-grade encryption and availability.

Justification:
TrueNAS supports advanced data protection features like self-healing storage, RAID-Z, and automatic snapshotting. Transitioning to cloud-managed storage also eliminates single points of failure, ensures off-site accessibility, and provides seamless scalability without onsite maintenance. This upgrade also supports SMB and NFS protocols needed by development and internal services.

Product Links:
- TrueNAS Enterprise-Top-rated Primary Storage on Gartner Insights

Risk 2: EOL MS SQL Cluster (2015 version)

Problem:
The Microsoft SQL Server cluster is running the 2015 version, which has reached the end of its mainstream support lifecycle. This opens the door to unpatched vulnerabilities and poor compatibility with newer applications and integrations. The cluster also resides on aging hardware, compounding the risk of failure or service disruption.

Solution:
Upgrade the cluster to Microsoft SQL Server 2022 and deploy it on a new high-availability (HA) cluster using Windows Server Failover Clustering (WSFC). Alternatively, move to a cloud-hosted solution such as Azure SQL Database Managed Instance or Amazon RDS for SQL Server, which provides managed backups, failover, patching, and scalability.

Justification:
Upgrading ensures compliance, performance gains, and access to modern SQL features like intelligent query processing and better security auditing. Cloud-hosted options reduce the administrative burden and improve disaster recovery with automated backups and geo-redundant storage. They also free up physical datacenter space and energy consumption.

Product Links:
- Windows Server Failover Clustering with SQL Server

Risk 3: Web Server Runs on Aging Hardware without Redundancy

Problem:
The existing web server runs on outdated hardware with no failover or redundancy, meaning a single point of failure could take down public-facing services. If the server crashes or is

compromised, customer access to downloads, account services, and internal documentation will be interrupted.

Solution:
Deploy a redundant, load-balanced web server environment using Nginx or Apache HTTP Server on virtual machines across two availability zones or buildings. This setup can be enhanced with HAProxy for load balancing or use a cloud-based approach such as AWS EC2 + Elastic Load Balancer or Azure App Services.

Justification:
Load-balanced web clusters allow high availability and fault tolerance. If one server fails, traffic is redirected to healthy nodes. This setup improves uptime, scales with demand, and supports SSL/TLS for secure web communication. Using cloud infrastructure further enables auto-scaling, DDoS protection, and rapid deployment of patches.

Product Links:
- https://docs.nginx.com/nginx/admin-guide/installing-nginx/installing-nginx-open-source/
- https://docs.nginx.com/nginx/admin-guide/installing-nginx/installing-nginx-plus/

Risk 4: Use of Outdated FTP for Software Delivery

Problem:
The company relies on traditional FTP (File Transfer Protocol) for distributing software internally and externally. FTP transmits data, including credentials, in plaintext, making it easy for attackers to intercept and abuse. It's also difficult to manage permissions securely and lacks proper logging and access control.

Solution:
Replace FTP with a secure file transfer method, such as SFTP (SSH File Transfer Protocol), or adopt a cloud-based solution like AWS S3 with pre-signed URLs or Microsoft Azure Blob Storage with Shared Access Signatures (SAS). These solutions support encryption in transit and at rest, access expiration, and role-based access control (RBAC).

Justification:
SFTP is a drop-in replacement that works over SSH and is widely supported by automation tools and enterprise environments. Cloud options further enhance reliability and auditability while offloading the infrastructure maintenance. All access can be tracked, logged, and controlled programmatically, ensuring compliance with data handling best practices.

Product Links:
- https://learn.microsoft.com/en-us/azure/storage/blobs/secure-file-transfer-protocol-support

Risk 5: EOL Client Systems Throughout the Infrastructure

Problem:
Multiple departments continue to operate on legacy systems like Windows XP, Windows 7, and unsupported Linux distributions. These systems are no longer patched and are vulnerable to a wide range of exploits, such as SMBv1 vulnerabilities (e.g., EternalBlue), which can lead to ransomware outbreaks or remote access by attackers.

Solution:
Conduct a phased rollout of new client systems running current, supported OS versions. This includes:

- Upgrading Windows systems to Windows 11 or Windows 10 LTSC
- Standardizing Linux environments on Ubuntu 22.04 LTS or Debian 12
- Updating macOS systems to versions within Apple's supported range
    - Pair this with endpoint protection using EDR (Endpoint Detection & Response) tools like CrowdStrike, SentinelOne, or Microsoft Defender for Endpoint.

Product Links:

- https://learn.microsoft.com/en-us/intune/intune-service/protect/advanced-threat-protection-configure

Justification:
Modern OS versions receive regular security updates and support current encryption, authentication, and software deployment protocols. Centralized endpoint management further enhances detection, logging, and incident response capabilities. Replacing EOL devices is an upfront investment that significantly reduces the organization's attack surface and long-term operational risk.

Summary:

The five proposed risks can be implemented to MyCo's infrastructure as instructed above to improve MyCo's security posture and prevent future incidents from occuring. See the below updated logical drawing for assistance on implementing these remediations. Also see provided links for assistance with installation or product purchasing.

Logical Drawing: