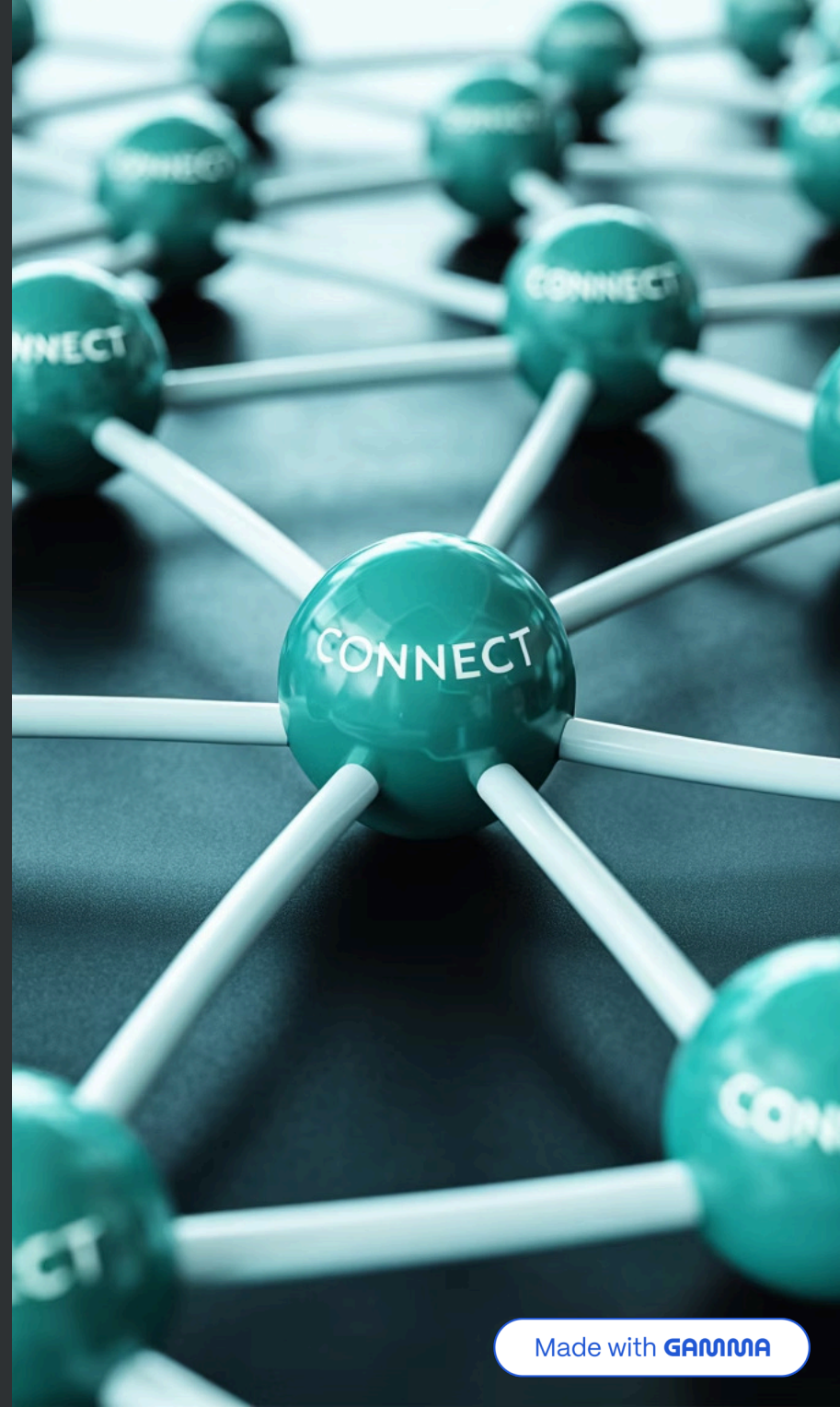
# IT Infrastructure for European Law Firm

A comprehensive network design for a European law firm, featuring robust security, redundancy, and GDPR compliance. This infrastructure supports legal operations with specialized VLANs, backup systems, and disaster recovery protocols.

By: Ysani Peña

# Table of Contents

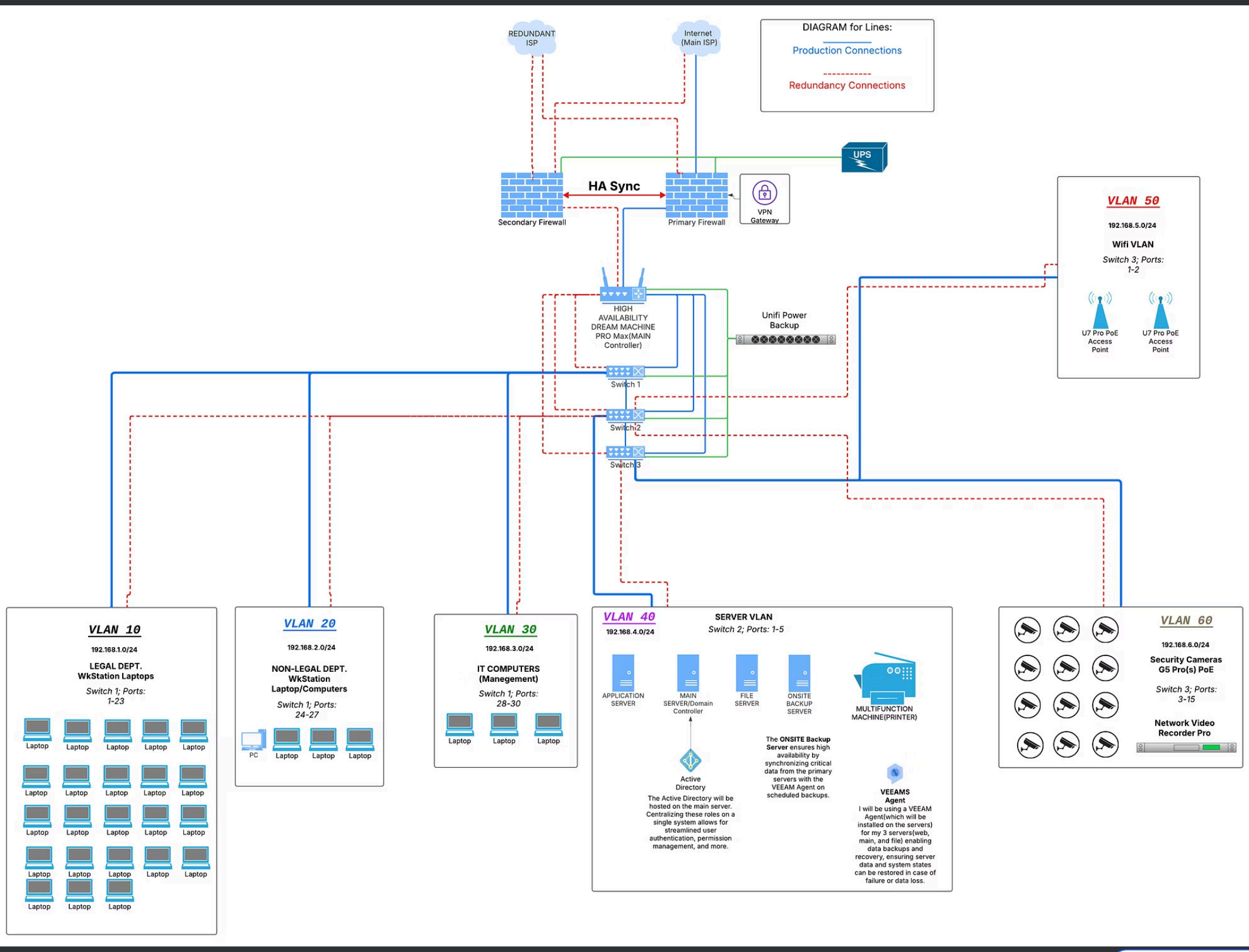




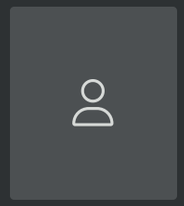
# Summary of Scenario: European Law Firm

- **Organization**: A small law firm with 30 employees specializing in corporate law.
- **Objective**: Create a secure IT environment to handle sensitive legal documents and client communications.
- **Regulatory Compliance**: GDPR (for European clients).
- **Constraints**: Budget of $100,000; data must be encrypted at **rest** and in **transit**.
- **Threat Model**: Data breaches, phishing.
- **Specific Needs**:
  - Encrypted file storage.
  - Secure email communication.
  - Backup system with off-site storage.

# Network Topology

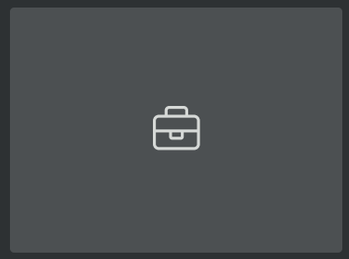


# VLANs



## VLAN 10 (Legal)

26 workstations (laptops) with access to legal documents (VLAN 40)

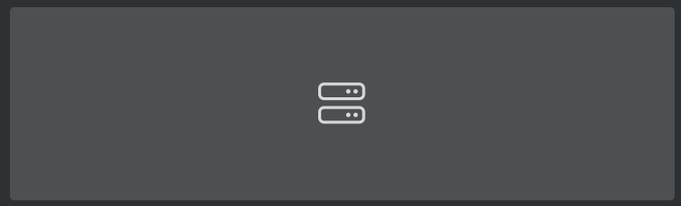


## VLAN 20 (Non-Legal)

4 workstations (3 laptops, 1 pc) accessing financial records/documents (VLAN 40) and limited security camera access (VLAN 60).

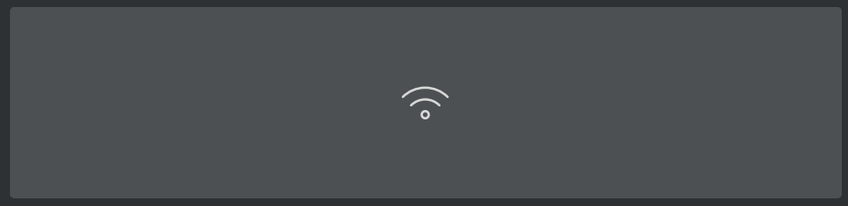
## VLAN 30 (IT)

3 workstations (laptops) with full access to all servers and devices.



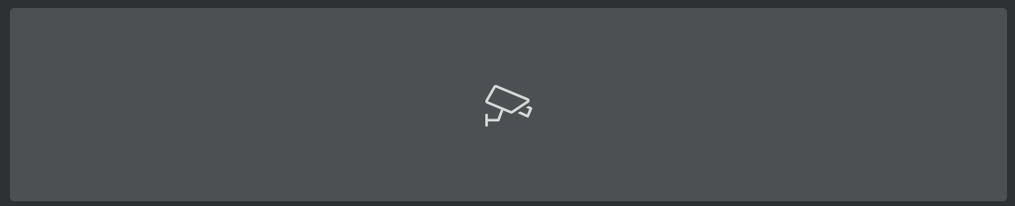
## VLAN 40 (Servers & Printer)

Contains all our critical servers and are accessed by other VLANs (RBAC)



## VLAN 50 (WiFi APs)

U7 Pro WiFi Access Points



## VLAN 60 (Security Cameras)

Accessible by IT & limited view for receptionist only

# Firewall & ISP




**Primary Firewall**: Fortinet FortiGate 200F (NGFW)

- $30,000
- 27Gbps Firewall Throughput
- 3.5Gbps Throughput NGFW
  - IPS, Web Filtering, Threat Protection, SSL Inspection

**Redundant Firewall**: Same model with HA (High Availability) Sync

- Automatically takes over in failure scenarios

**VPN** : Integrated into Fortinet firewall

- Secure remote access for employees/lawyers



**ISP Setup**

- **Main ISP**: BT Business (1Gbps fiber)
  - $6,240/year
  - 24/7 Support (Guaranteed 5-hour fix time)
  - Consistent & High Speed connectivity
- **Backup ISP**: Starlink Local Priority (500GB Plan)
  - $1000-$1500 (Hardware, one time cost)
  - $165/month (will only use/charge when main ISP goes down)

# Main Controller & Switches

- **Controller**: Dream Machine Pro Max (High Availability Pair)
  - $1,198
  - Supports 2,000+ clients & 200+ UniFi devices
  - 5Gbps IPS routing
- **Switches**: 3x UniFi Pro Max 48 PoE
  - $3,900
  - 48 ports, Layer 3 switching, 2.5GbE PoE++
  - Powers APs, cameras, and can for any potential additional PoE devices

# Switch Configuration

## Switch 1

Handles VLANs 10, 20, and 30 for workstation and management traffic.

Optimizes user access and administrative controls.

## Switch 2

Dedicated to VLAN 40 (Server VLAN) for high-speed access.

## Switch 3

Manages security cameras and Wi-Fi access points.

Keeps surveillance separate from business operations.

# Employee & IT Workstations


## ThinkPad X13 Gen 5 (Legal, Non-Legal, IT)

- CPU: Intel Core Ultra 5
- Windows 11 Pro
- 16GB RAM
- 512 GB SSD


## Dell OptiPlex Micro (Front Receptionist)

## CPU: Intel Core i5

- Windows 11 Pro
- 16 GB
- 512 GB SSD


# Servers

- **Main/Application/File Servers**: 3x Dell PowerEdge R650
  - $26,439 total
  - 64GB RAM
  - 3x 960GB SSD (RAID 5)
  - 10 Gb NIC
- **On-Site Backup Server**: Lenovo ThinkSystem SR650 V2
  - $2,923.83 total
  - Dual Xeon support (can handle two CPUs)
  - Up to 400TB of storage
  - RAID 0/1/5/10 options

# Printer

Lexmark MX722 All-in-One Laser Printer

- $3,269
- Print/Scan/Copy/Fax
- 70ppm
- WiFi + Ethernet, EPEAT Gold Certified

# Security Cameras & Access Points

## G5 Pro 4K Cameras

- Total $4,548 (12x)
- Long-range IR Night Vision
- 3x Optical Zoom
- PoE Powered

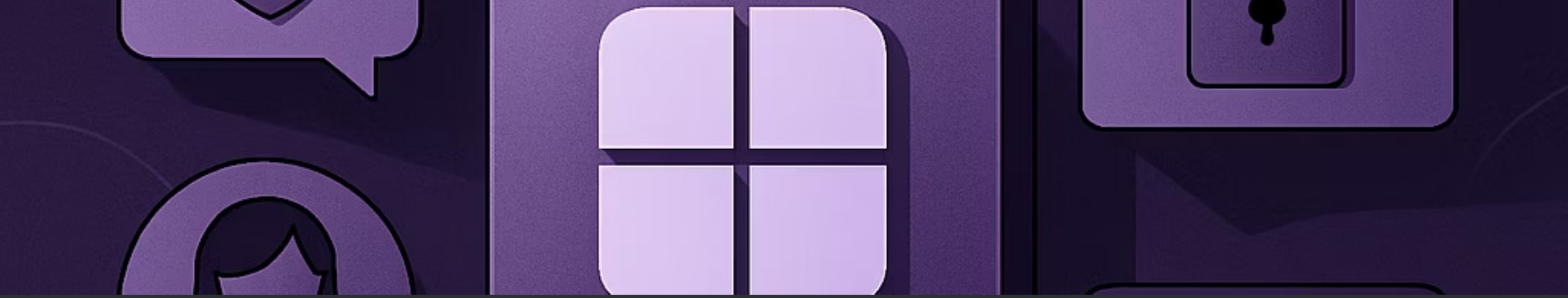
## UniFi U7 Pro PoE Access Points

- Total $736 (4x)
- Ceiling-mounted WiFi 7
- 6GHz Support

## Network Video Recorder Pro

- Total $1,495
  - $499 → NVR Pro
  - $996 (4x) → Seagate IRONWOLF 8TB HDD
- Can hold up to 7 HDDs

# Web Services



# Microsoft 365 Business Premium

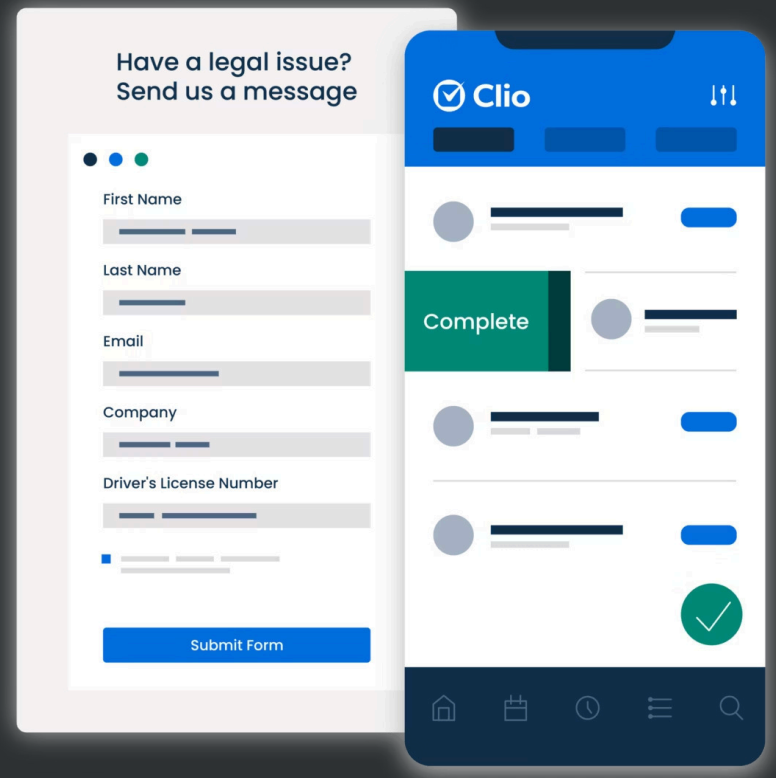
- **Cost:** ~$22/user/month → x30 users = $660/month ($7,920/yr)
- **Included Tools:** Outlook, Word, Excel, PowerPoint, Teams, Exchange, OneDrive
- **Security Features:**
  - Microsoft Defender for Office 365
  - Data Loss Prevention (DLP)
  - Endpoint Protection


# GDPR Monitoring Web Service – DPOrganizer

- **Cost:** $199/month → $2,388/year
- **Key Features:**
  - Data mapping and visualization tools
  - GDPR activity logs
  - Compliance reporting dashboards
  - RoPA
- Supports data protection documentation
- Helps satisfy GDPR’s accountability principle

# Secure Client Portal – Clio

- **Cost:** Starts at $49/user/month → $1,127/month ($13,524/yr) for 23 lawyers
- **Key Features:**
  - Client-facing document portal
  - E-signatures and secure file sharing
  - Case/matter organization tools
  - Time tracking, billing, and scheduling
- Fully encrypted and cloud-based
- Accessible to clients from anywhere



# Communication Tools

## Microsoft Teams (Internal Communication):

- **Cost:** Included with Microsoft 365 Business Premium
- **Features:**
  - Chat, video calls, file sharing
  - Integrated with Office apps (Word, Excel, OneDrive)
  - Private and group channels for departments
  - Secure communication with **end-to-end encryption**
- **Purpose/Justification:**
  - Centralized internal communication
  - Secure and efficient for staff collaboration

## Google Voice (External Communication):

- **Cost:**
  - Standard Plan: $20/user/month → $7,200/yr (30 users)
- **Features:**
  - Business phone number for the firm (single main number)
  - Employee personal numbers or **secondary numbers** for client calls
  - **Call forwarding**, **voicemail transcription**, and **SMS**
  - Works on smartphones and computers
- **Purpose/Justification:**
  - Modern alternative to landlines
  - Professional, flexible client communication
  - More **cost-effective** than setting up traditional phone lines

# Backups

# Critical Data for Backup

### Legal Documents

Client files, contracts, and sensitive case information.

### System Configurations & Security Camera Footage

Network/server configurations & after a certain time, back up camera footage

### Financial Records

Billing, payroll, and financial data.

### Application Server

Services for Employees

### Compliance & Audit Data

GDPR compliance records, audit logs and agreements

# Backup Approach/Types

## Full Backups

Weekly complete copies of all critical data.

Performed every Sunday at 10 PM.

Creates baseline for incremental backups.

## Incremental Backups

Daily backups of only changed data.

Performed every night at 10 PM.

Minimizes storage requirements while ensuring data protection.

# Backup Storage Solutions

## Primary Data

Stored on active servers

- Main Server
- File Server
- Application Server

## On-Site Backup Storage

Lenovo ThinkSystem SR650 Backup Server stores backups onsite using the VEEAM Backup Agent.

## Off-Site Backup Storage

VEEAM Backup Agent syncs encrypted backups to VEEAM Data Cloud Vault.

Provides disaster recovery capabilities for catastrophic failures.

# Veeam Backup and Replication


## Key Features of Veeam:

- **Automated Backups**
- **Incremental Backups**
- **Instant Recovery**
- **Data Integrity Checks**
- **Ransomware Protection**

**Veeam Agent:**

- Installed on servers to automate and manage backups
- Backs up **critical data** from local servers
- Sends backup data to the **Onsite Backup Server** for local redundancy

**Veeam Data Cloud Vault:**

- Acts as the **offsite backup** for data stored locally
- Enables **cloud replication** to ensure data availability even if local backups fail


# Backup Workflow

## Data Sources

File Server, Main Server, Application Server

## Encryption

VEEAM Backup Agent applies AES-256 encryption

## On-Site Backup

Data stored on Lenovo ThinkSystem SR650

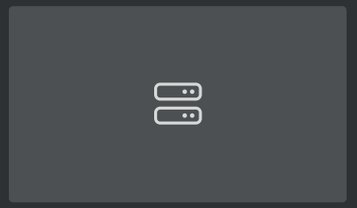
## Off-Site Backup

Data synced to VEEAM Data Cloud Vault

# Recovery Priorities

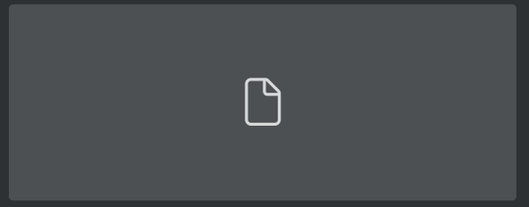
## Critical Infrastructures

Networking & Firewall



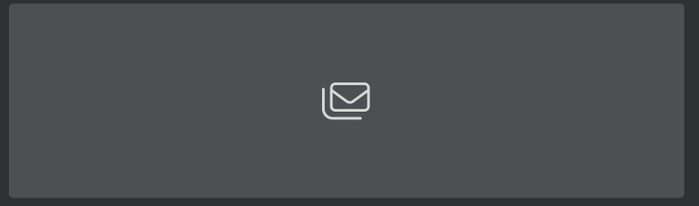
## Main Server/Domain Controller

Critical for authentication services and employee access.



## File & Application Server

Legal/Financial Data & Software (Clio, DPOrganizer)

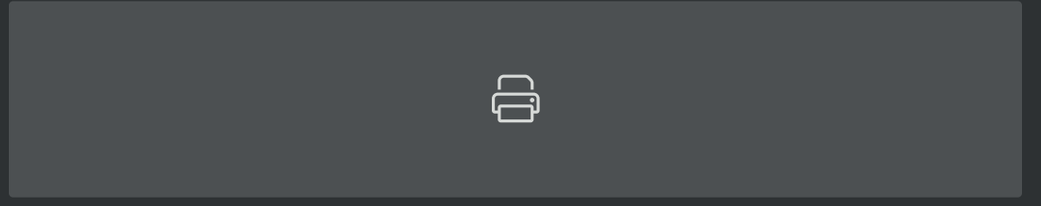


## Communication Systems

Important for client and internal communications.

## Backup Access

Verify that onsite and offsite backups are accessible



## Devices/Printer/Cameras

Verify employee devices are operational

# Recovery Time Objectives

## 2 hrs

File & Main Server

Critical for business operations

## 2–3h

System Configurations

Network functionality

## 4–6 hrs

Network Video Recorder Pro

Security Camera Storage Device

## 4 hrs

Application Server

Internal operations

# Backup Retention Policy

## On-Site Backups

Retained for 30 days

Provides quick access for recent recovery needs

Automatically purged after retention period

## Off-Site Backups

Retained for 90 days

Ensures longer-term disaster recovery capability

Stored in VEEAM storage in the cloud vault

## Legal & Financial Data

Retained for 7 years

Meets business needs and legal requirements

# Uninterruptible Power Supply & Generator

## CyberPower CP1500PFCLCD UPS

$220

1500VA / 1000W

Pure Sine Wave

LCD Display

## Generac GP9500E Tri-Fuel Generator

$1,099

Power Output: 9,500 W

Tri-Fuel: Gas, Propane, Natural Gas

## UniFi USP-RPS (Power Supply)

$515 (includes Smart Power Cables)

950W redundant power supply for rack-mounted UniFi devices

# Power Backup Strategy

### UPS for Firewalls:

- Maintains power during outages.
- Allows firewalls to stay online for critical network protection.

### UniFi USP-RPS for Switches and Controller:

- Provides backup power to switches and the main controller.
- Ensures continued network operation while power is restored.

### Generator for Full Infrastructure:

- Powers the entire system once manually activated.
- Provides long-term power until utility power is restored.

# Threat Model + Costs

# Addressing Threat Model

## Data Breaches Prevention

- SFTP for secure file transfer
- AES-256 (rest + transit)
- Server-side encryption and BitLocker
- Access Control Measures
- Advanced threat filtering and protection (NGFW)

## Phishing Prevention

- Recurring Employee training
- Secure email filtering (NGFW + Microsoft Defender)
- Multi-factor authentication → reduces credential compromise risk

# IT Infrastructure Cost Breakdown

## Hardware

**Total: $111,019.30**

- Servers, Firewalls, Switches, Controller
- ISPs (Main & Redundant)
- Laptops, Cameras, Printers
- HDD storage

## Annual Software/Cloud Services

**Total: $40,116/year**

- Microsoft 365 Business Premium
- Clio Client Portal
- DPOrganizer (GDPR Compliance)
- Google Voice
- Veeam Data Cloud Vault
  - (3-year plan)

## Generator/UPS

**Total: $1,834.00**

- CyberPower CP1500PFCLCD UPS
- Generac GP9500E Tri-Fuel Generator
- UniFi USP-RPS

TOTAL COST of INFRASTRUCTURE

**$152,969.39**

# Helpdesk

# OsTicket Video Demo

# Ticket Categorization

## Hardware Issues

Computer, printer or any hardware problems.

## Software Issues

Application errors or functionality problems.

## Network Issues

Connectivity, VPN, or access problems.

## Security Issues

Suspicious activity or access requests.

## General Inquiries

Information requests or guidance needed.

# Helpdesk Workflow Overview

### Ticket Submission

User submits request with required information.

### Classification

Auto-classification with manual review by IT staff.


### Resolution

IT staff addresses issue and documents solution.

### Closure

User verifies resolution and provides feedback.

# Password Reset Script

## Initial Response

"Thank you for contacting the IT Helpdesk. For security purposes, I'll need to verify your identity."

## Verification Request

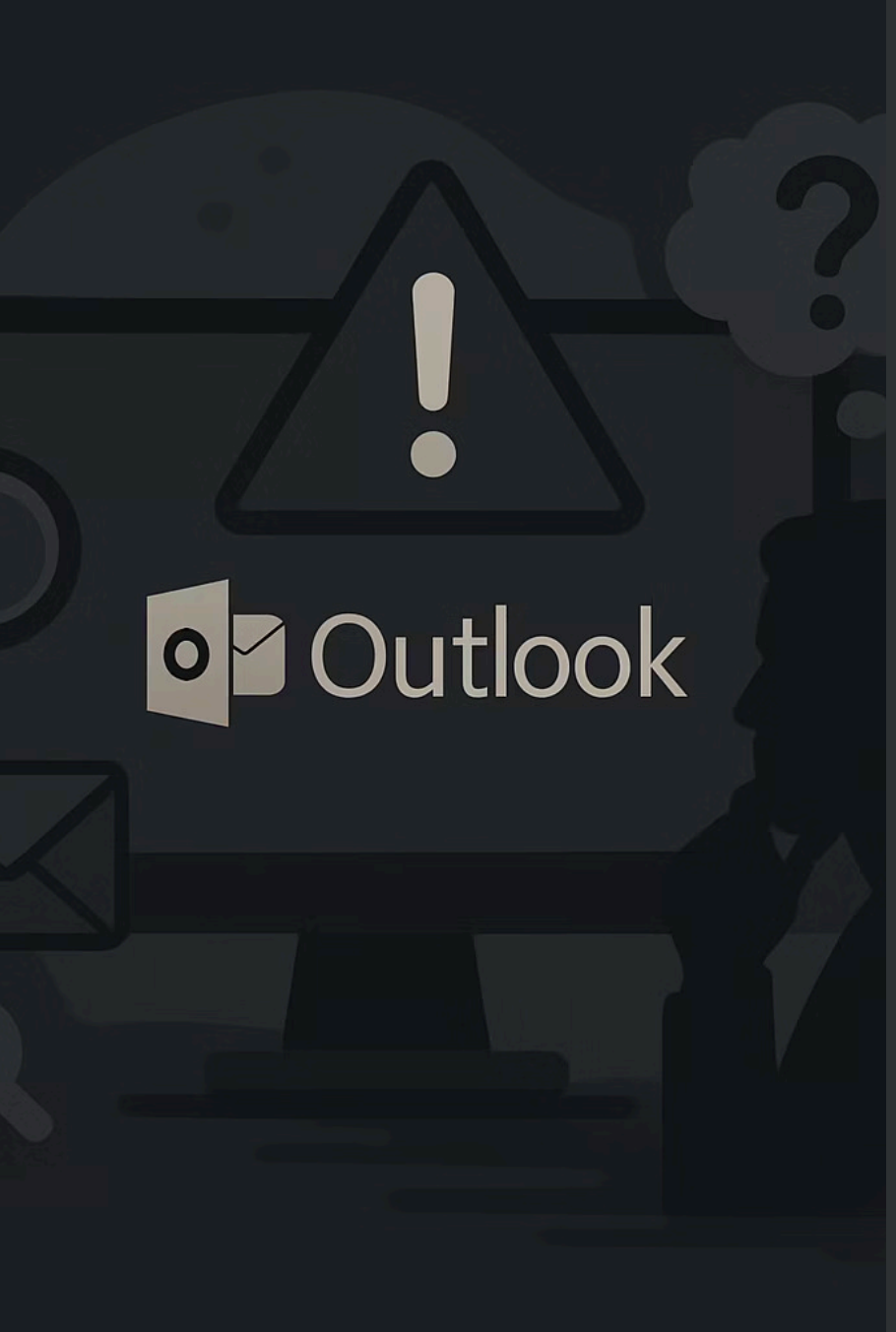
"Please provide your employee ID and the answer to your security question: [What was the name of your first pet?]"

## Resolution Process

"Once verified, I'll process your password reset and send you a link to reset your email password."

## Next Steps

"Please try logging back in and check that your password was successfully reset"




# Email Access Problem Script

## Initial Troubleshooting

"Let's troubleshoot your email access:"

### Web Access Check

"Can you access Outlook Web App at [outlook.office.com]?"

#### Error Information

"Are you receiving any specific error messages?"

##### Device Verification

"Does this affect outlook on other devices or just this one?"

# Escalation Triggers

## SLA Timeframe Exceeded

Ticket remains unresolved after defined resolution time.

## Multiple User Reports

Several users reporting identical issue indicates wider problem.

## Security Incident

Potential security breach requires immediate attention.

## VIP Impact

Senior staff or partners affected by IT issues.

# Severity Levels


### SEV1 (Very Critical)

Major system downtime or security breach

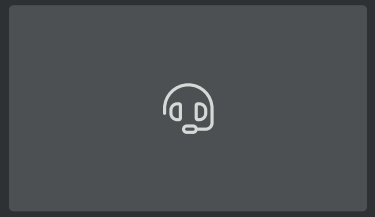
### SEV2 (High)

Significant degradation with limited impact

### SEV3 (Medium-Low)

Minor issues with available workarounds

# Escalation Path

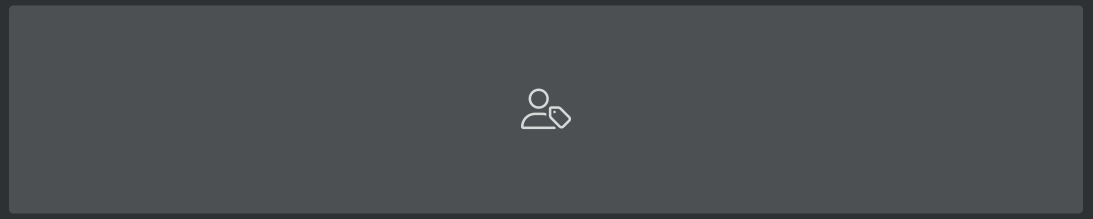


## Level 1: Helpdesk Technicians

Front-line support handling initial tickets and SEV3 issues.

## Level 2: Network Specialist/System Admin

Advanced network issues and server/application issues (SEV2/SEV1).



## Level 3: IT Director

Final escalation point for SEV1 with legal/financial risk.

# Escalation Communication Methods

## SEV3 Issues

Communication Method: Email/Teams

Priority: Non-urgent

Response Time: Same business day

Follow-up: As needed

## SEV2 Issues

Communication Method: Microsoft Teams

Priority: Urgent

Response Time: Within 1 hour

Follow-up: 2-hour updates

## SEV1 Issues

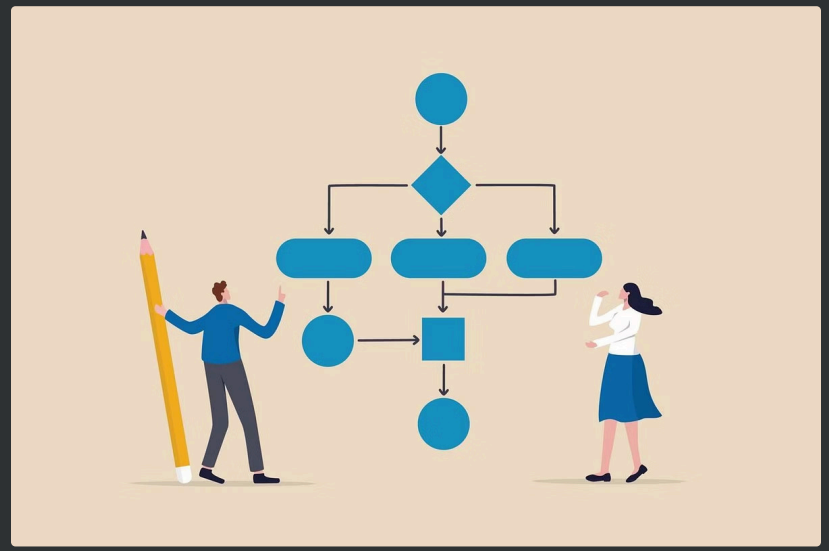
Communication Method: Phone/Teams

Priority: Mega-urgent

Response Time: Immediate

Follow-up: 30-minute check-ins

# Escalation Example Workflow



## Issue Identification

Multiple lawyers (VLAN 10) can't access files.

## Helpdesk Front-line

Helpdesk examine the issue and attempts to resolve issue and if not possible will escalate to next level.

## Initial Escalation

Escalates to Level 2 (Network Specialist/Sys Admin).

## Timing Protocol

Level 2 engages Level 3 after 30-60 mins if unresolved.

# Feedback and Improvement

### User Feedback

Collect satisfaction ratings and comments.

### Data Analysis

Review metrics and identify trends.

### Knowledge Base Update

Document solutions for future reference.

### Process Refinement

Implement improvements based on findings.

# Assessment

# Network Infrastructure

## Strengths

- Robust perimeter security with redundant Fortinet 200F firewalls
- Enhanced performance and access control via VLAN segmentation (VLAN 10–60)
- Efficient power delivery and traffic management with Pro Max 48 PoE Layer 3 switches
- Switch-level redundancy configured through switch stacking

## Weaknesses

- Clarity lacking on the specifics of switch-level redundancy
- No mention of DHCP Failover or Redundancy

## Improvements

- Implement Network Segmentation Monitoring and Threat Detection

# Backup Systems

## Strengths

- Hybrid on-site and off-site model ensures data redundancy
- Strong data protection with AES-256 encryption for data in transit and at rest (including BitLocker)
- VEEAM Agents protect file server, application server, and security footage backups
- Well-defined backup frequency (Weekly Full, Daily Incremental)
- Clear RTO objectives (2-4 hrs servers, 4–6 hrs camera system)
- Cost-effective and scalable cloud backups via Veeam Data Cloud Vault

## Weaknesses

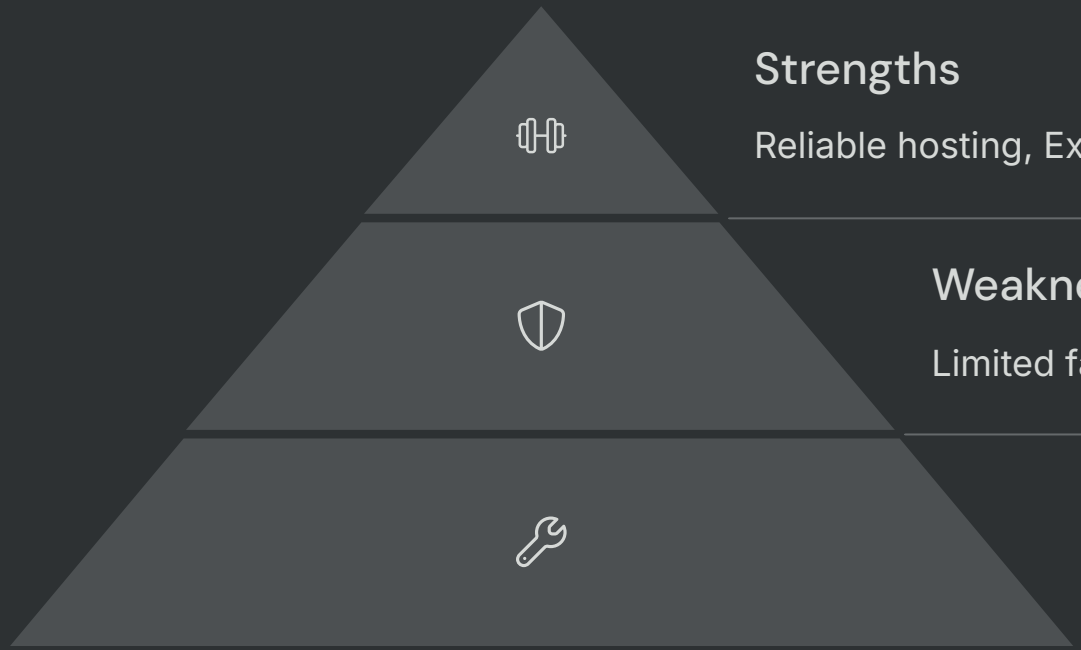
- Potential risk of exceeding on-site storage (SR650) with growing camera footage if not monitored
- No mention of regular test restores or backup validation procedures

## Improvements

- Schedule quarterly restore tests to validate backup integrity
- Set up automated storage monitoring alerts for the Lenovo SR650
- Evaluate long-term archival solutions specifically for security footage

# Web Services/Email

Our assessment of current web and email infrastructure components:



## Strengths

Reliable hosting, Exchange Online efficiency, isolated service roles

## Weaknesses

Limited failover details & DoS/DDoS protection details

## Improvements

Load balancer implementation, Fortinet DDoS protection

# Security Measures

## Strengths

- Excellent layered security provided by Firewall, VLANs, and RADIUS
- Proper departmental isolation using VLANs (Legal, Non-Legal, IT)
- Sensitive data further protected by BitLocker and AES-256 encryption

## Weaknesses

- No explicit mention of Intrusion Detection/Prevention Systems (IDS/IPS)
- Heavy reliance on a single server for centralized services like AD, DNS, DHCP, and RADIUS, creating a potential single point of failure

## Improvements

- Enable FortiGate IDS/IPS features
- Consider SIEM integration for alerting and detecting suspicious activity and threats
- If scaling demands, add a secondary domain controller (on a backup server)

# Scalability & Future-Readiness

## Strengths

- Modular switch infrastructure and server rack layout support physical expansion.
- Cloud-based email and offsite backups scale effortlessly with business growth.
- The three PowerEdge servers allow for future virtualization or container-based deployments (e.g., Hyper-V, Proxmox, Docker).

## Weaknesses (Potential Bottlenecks)

- Growing camera footage and user data could require more local or cloud storage within a couple of years.
- UPS units may limit coverage time if more systems are added without power infrastructure upgrades.

## Improvements

- Consider adding additional storage arrays (NAS) or utilizing cloud archive tiers.
- Look into more powerful UPS units

# CMM Framework

| Domain | Maturity Level | Evaluation |
| --- | --- | --- |
| Network Architecture | Level 4 | Managed VLAN segmentation, centralized management, and defined access controls. Minor redundancy improvements could elevate to Level 5. |
| Backup & Disaster Recovery | Level 4 | Managed Hybrid on-site/off-site VEEAM solution w/ encryption, and a schedule with clear RTO/RPO. Adding restore testing/reporting would bring to Level 5. |
| Server Infrastructure | Level 4 | Managed Enterprise-grade Dell and Lenovo servers with RAID, redundancy, and backup coverage. Lack of virtualization clustering or failover automation keeps this from Level 5. |
| Security Architecture | Level 3 | Defined VLANs, firewall layers, BitLocker, and RADIUS implemented. However, IDS/IPS, & SIEM integration can be specifically implemented and documented, which could increase this to a Level 4. |
| Email & Collaboration | Level 5 | Optimizing Migration to Microsoft 365 Business Premium enables fully managed, cloud-based email, premium features, and scalable licensing. |
| Scalability & Future Planning | Level 4 | Managed Infrastructure anticipates future growth with modular hardware and cloud services. More automation would elevate this to Level 5. |

# Suggestions & Implementations from IT Professional

## Internet Redundancy

**Finding:** Potential internet outage if primary ISP or firewall fails.

**Implementation:** Added secondary internet (Starlink) for failover; configured automatic failover routing on Fortinet.

## Dummy Switch Usage

**Finding:** Use of a dummy switch for load balancing

**Implementation:** Removed Dummy Switch (either kept for specific traffic or remove due to not desperately needing it for congestion control).

## Wi-Fi VLAN Design Simplification

**Finding:** Overcomplicated Wi-Fi VLAN setup (separate SSIDs in two vlans).

**Implementation:** Simplified to use single APs to broadcast the SSIDs.

## Firewall Redundancy Configuration

**Finding:** Not clear on firewall redundancy configuration.

**Implementation:** Configured Primary/Secondary Fortinet → seamless HA failover.

# QUESTIONS?