TECHNICAL DESIGN DOCUMENT

tikko
secure by design

Cristian Bogdan

version 1.0

Contents

Disclaimer: Fictional Case Study and Customization

This Technical Design Document (TDD) is based on a fictional case study involving the fictional company, ABC Solutions. The purpose of this document is to provide a general framework and illustrative example of how a comprehensive IT security and modernization solution might be structured. It is important to note that the details contained herein are entirely hypothetical and designed to serve as a guide for developing customized solutions for real-world scenarios.

Custom Tailoring

Each TDD should be specifically tailored to meet the unique requirements of individual customers. The strategies, technologies, and configurations presented in this document are illustrative and may not fully align with every organization's needs. The actual implementation will vary based on factors such as the customer's industry, existing infrastructure, regulatory requirements, and specific security concerns.

Open-Ended Framework

To ensure broad applicability, this TDD has been purposely left open-ended regarding certain aspects, such as the specific services provided by ABC Solutions. This approach is intended to prevent any misconceptions that the solution outlined here is not relevant to other organizations. As such, the document does not delve into the details of ABC Solutions' business operations, allowing it to serve as a flexible template applicable to a wide range of scenarios.

Technology Scope

The technologies and solutions highlighted within this document represent a subset of the many available options for enhancing IT security and infrastructure. While the technologies discussed are relevant and effective, they are not exhaustive. Customers are encouraged to consider additional or alternative technologies that may better align with their specific requirements and business goals.

In summary, this TDD serves as a starting point for designing and implementing IT solutions and should be adapted to reflect the unique context of each client. For a tailored solution, it is recommended to engage in a detailed assessment of the customer's needs and consult with experts to develop a plan that addresses their specific challenges and objectives.

Executive Summary

ABC Solutions, a mid-sized technology services provider, experienced a significant data breach leading to financial losses and operational disruption. This Technical Design Document (TDD) outlines a strategic plan to enhance cybersecurity through the implementation of advanced solutions, including Veeam's immutable backup for file servers, Palo Alto firewalls, Microsoft Defender, Azure AD integration, Data Loss Prevention (DLP), and Microsoft's Rapid Modernization Plan. The objective is to modernize and secure the IT infrastructure, integrate risk management practices, and ensure robust data protection.

Solution Architecture Overview

The proposed solution architecture includes:

- **Immutable Backup Solution**: Deploy Veeam Backup & Replication with immutable backup features for file servers.
- **Network Security**: Upgrade to Palo Alto firewalls with advanced threat prevention and Zero Trust principles.
- **Endpoint Protection**: Utilize Microsoft Defender for enhanced security across all Windows endpoints.
- **Identity and Access Management**: Integrate Azure AD with Privileged Identity Management (PIM) and Just-In-Time (JIT) access.
- **Data Loss Prevention (DLP)**: Implement DLP policies to safeguard sensitive data.
- **Microsoft Rapid Modernization Plan**: Align IT infrastructure with modern security and management practices.
- **Incident Response Plan**: Develop a comprehensive incident response strategy.
- **Employee Training**: Establish an ongoing cybersecurity training program.

Business Case

Implementing these solutions will:

- **Protect Data**: Secure critical data with immutable backups and DLP policies.
- **Enhance Security**: Improve overall security posture through advanced firewalls, endpoint protection, and modern identity management.
- **Modernize Infrastructure**: Align with Microsoft's Rapid Modernization Plan for optimized IT operations and security.
- **Ensure Compliance**: Meet regulatory requirements and industry standards.
- **Improve Response**: Strengthen incident response capabilities.

Requirements Summary

Backup Solution: Implement Veeam Backup & Replication with immutable backup functionality for file servers.

Network Security: Deploy Palo Alto firewalls in a high-availability configuration.

Endpoint Protection: Use Microsoft Defender on all Windows endpoints.

Identity Management: Integrate Azure AD with PIM and JIT for managing privileged access.

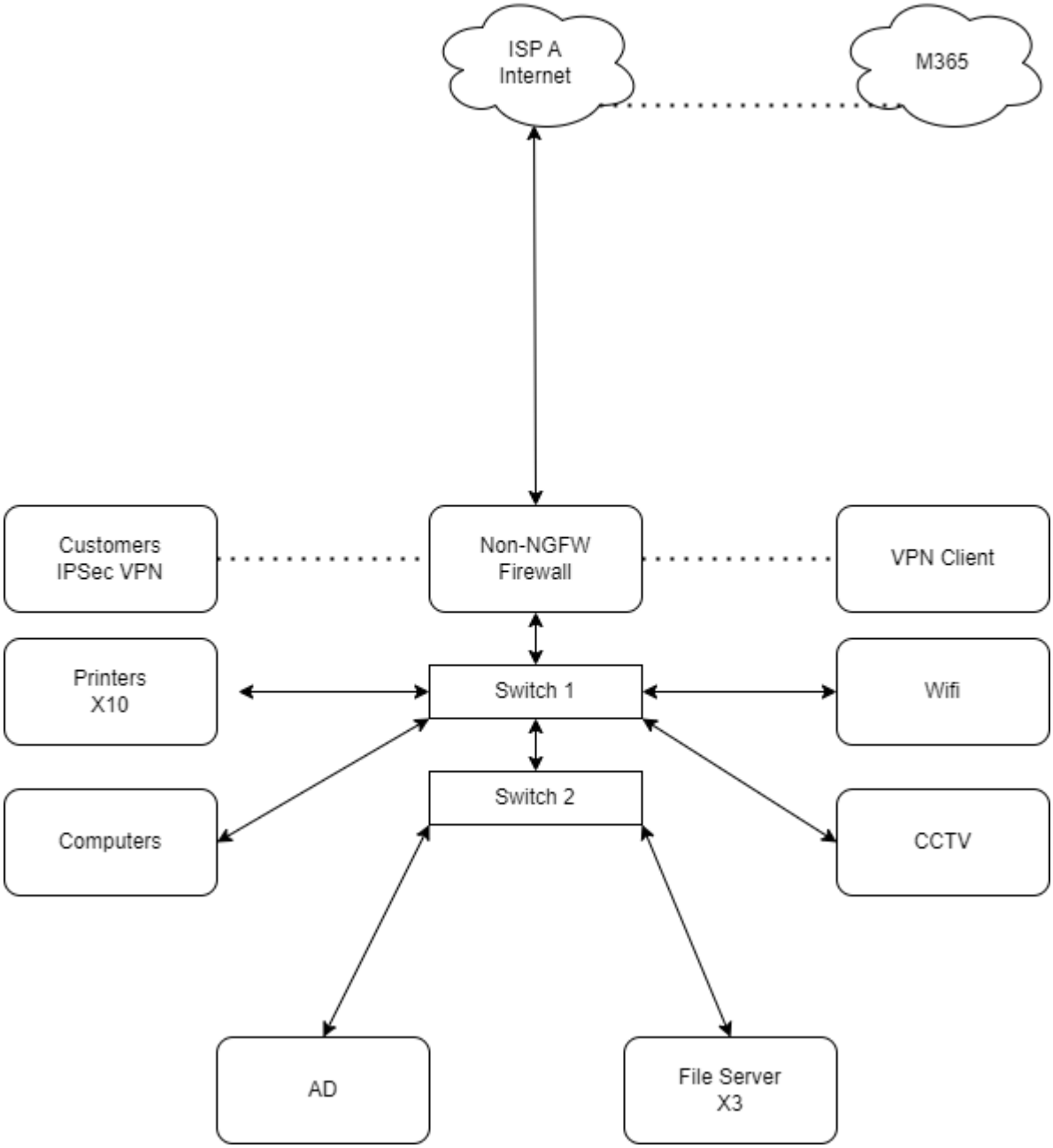
Data Loss Prevention: Deploy and manage DLP policies to protect sensitive data.

Modernization: Apply Microsoft's Rapid Modernization Plan to upgrade infrastructure.

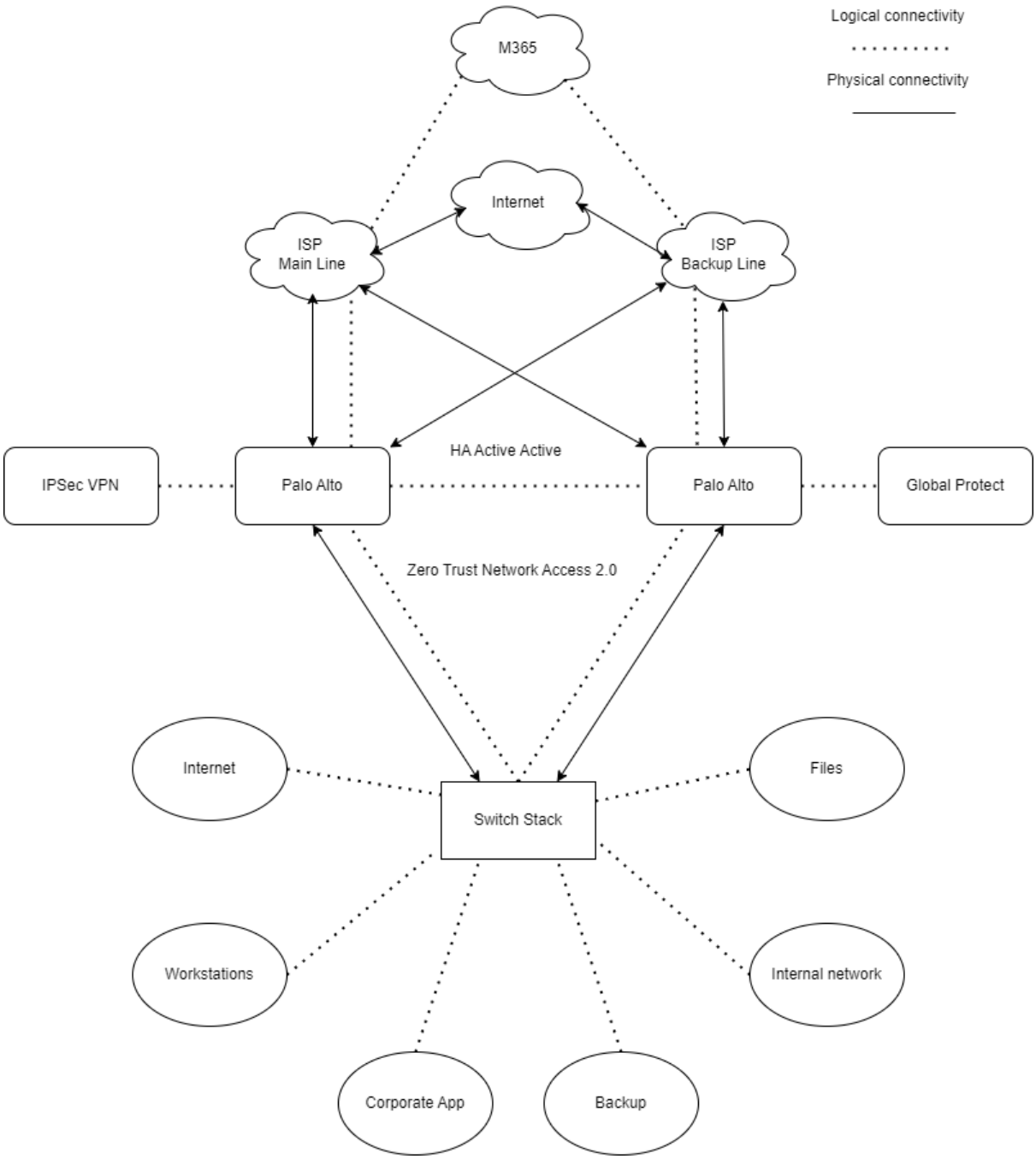
Incident Response: Develop and test a formal incident response plan.

Training and Awareness: Conduct comprehensive and ongoing cybersecurity training programs.

Current State Diagram



Desired State Diagram



High-Level Solution Design

Backup Solution

- **Veeam Immutable Backups**:
    - Deploy Veeam Backup & Replication with immutable backup settings.
    - Set up retention policies to prevent modification or deletion of backup data.
    - Use compatible immutable storage solutions for backup repositories.

Network Security

- **Palo Alto Firewalls**:
    - Deploy dual Palo Alto firewalls in a high-availability configuration.
    - Configure for Zero Trust network segmentation and IPsec connections.
    - Utilize advanced threat prevention features.

Endpoint Protection

- **Microsoft Defender**:
    - Deploy Microsoft Defender across all Windows endpoints.
    - Follow Microsoft Secure Score recommendations and configure attack surface reduction (ASR) and automated investigation and response (AIR).

Identity and Access Management

- **Azure AD Integration**:
    - Integrate Azure AD with on-premises Active Directory.
    - Implement PIM and JIT for privileged access management, with a maximum JIT access duration of four hours and requiring admin approval for elevation.

Data Loss Prevention (DLP)

- **DLP Implementation**:
    - **Policy Creation**: Develop DLP policies to monitor and protect sensitive data.

- **Policy Enforcement**: Apply policies across endpoints, file servers, and cloud services.
- **Monitoring and Alerts**: Configure alerts for policy violations and establish reporting mechanisms.

Microsoft Rapid Modernization Plan

- **Assessment and Planning**:
  - Evaluate current IT infrastructure and identify modernization needs.
  - Develop a roadmap for upgrading systems, applications, and security measures.
- **Modernization Execution**:
  - **Cloud Adoption**: Migrate suitable workloads and applications to the cloud.
  - **Automation**: Implement automation tools for management and deployment.
  - **Security Integration**: Ensure new systems are integrated with modern security practices.

Incident Response

- **Incident Response Plan**:
  - Develop a formal incident response plan outlining roles, procedures, and communication strategies.
  - Conduct regular drills to test the effectiveness of the response plan.

Employee Training

- **Training Programs**:
  - Deliver initial comprehensive cybersecurity training.
  - Implement ongoing training and phishing simulations, with increased frequency if necessary.

Detailed Solution Architecture

Immutable Backup Solution

Veeam Backup & Replication with Immutable Backup

- **Deployment**:
    - **Installation**: Install Veeam Backup & Replication software on designated backup servers.
    - **Immutable Backup Configuration**: Configure immutable backup settings to prevent modification or deletion of backups. This involves setting up backup repositories with immutability enabled and defining retention policies that comply with regulatory and organizational requirements.
    - **Storage Integration**: Integrate Veeam with immutable storage solutions, such as WORM (Write Once, Read Many) compliant storage or cloud storage with immutability support. Ensure that storage solutions are configured to support Veeam's immutable backup capabilities.
- **Backup Processes**:
    - **Backup Jobs**: Configure backup jobs for the file servers to ensure regular, automated backups. Define job schedules, backup windows, and retention periods based on business requirements.
    - **Recovery Testing**: Implement procedures for periodic recovery testing to validate backup integrity and recovery processes. Ensure that recovery from immutable backups meets the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) requirements.
- **Security Measures**:
    - **Encryption**: Ensure that backups are encrypted both at rest and in transit to protect data from unauthorized access.
    - **Access Controls**: Restrict access to backup management interfaces and storage to authorized personnel only. Implement multi-factor authentication (MFA) for backup systems.

Network Security

Palo Alto Firewalls

- **Deployment**:
    - **High-Availability Configuration**: Deploy two Palo Alto firewalls in a high-availability (HA) pair to ensure redundancy and reliability. Configure active-passive or active-active HA based on the network architecture and performance requirements.
    - **Network Segmentation**: Implement Zero Trust network segmentation using the Palo Alto firewalls. Define network segments (VLANs) to

isolate different types of traffic, such as internal, DMZ, and external traffic. Apply security policies based on the principle of least privilege.

- **Firewall Configuration**:
    - **Access Control Policies**: Create and enforce access control policies to regulate traffic between network segments. Define rules for inbound and outbound traffic, ensuring that only authorized connections are allowed.
    - **IPsec VPN Configuration**: Configure IPsec VPNs for secure remote access and client connections. Implement strong encryption standards and authentication methods to protect data in transit.
- **Threat Prevention**:
    - **Advanced Threat Detection**: Utilize Palo Alto's advanced threat prevention features, including intrusion prevention system (IPS), anti-malware, and URL filtering. Configure threat detection and prevention profiles to address common attack vectors.
    - **Logging and Monitoring**: Enable comprehensive logging and monitoring to track network traffic and detect potential security incidents. Integrate with a Security Information and Event Management (SIEM) system for centralized log management and analysis.

Endpoint Protection

Microsoft Defender

- **Deployment**:
    - **Microsoft Defender Configuration**: Deploy Microsoft Defender for Endpoint across all Windows endpoints. Configure policies to ensure comprehensive protection against malware, ransomware, and other threats.
    - **Secure Score Optimization**: Review Microsoft Secure Score recommendations and implement suggested improvements to enhance endpoint security. Configure settings for attack surface reduction (ASR) and automated investigation and response (AIR).
- **Endpoint Management**:
    - **Microsoft Endpoint Manager Integration**: Integrate Microsoft Defender with Microsoft Endpoint Manager (Intune) for centralized management and policy enforcement. Ensure that all endpoints are enrolled and compliant with security policies.
- **Advanced Features**:

- **Attack Surface Reduction**: Configure ASR rules to minimize potential attack surfaces by blocking potentially risky behaviours and applications.
- **Automated Investigation and Response**: Enable AIR capabilities to automatically investigate and respond to detected threats, reducing the time to remediation.

Identity and Access Management

Azure AD Integration with PIM and JIT

- **Azure AD Integration**:
  - **Synchronization**: Use Azure AD Connect to synchronize on-premises Active Directory with Azure AD. Ensure that user identities and attributes are accurately reflected in Azure AD.
  - **Conditional Access**: Implement Conditional Access policies to enforce security controls based on user identity, device compliance, and location.
- **Privileged Identity Management (PIM)**:
  - **Role Assignment**: Assign administrative roles within Azure AD using PIM. Define roles and permissions for both internal IT admins and client-related admins.
  - **Just-In-Time (JIT) Access**: Configure JIT access for privileged roles with a maximum duration of four hours. Ensure that requests for privileged access require approval from another authorized admin.
- **Access Reviews**:
  - **Regular Reviews**: Implement periodic access reviews to ensure that users have appropriate permissions, and that access is revoked when no longer needed.

Data Loss Prevention (DLP)

DLP Policy Implementation

- **Policy Creation**:
  - **Sensitive Data Identification**: Define and classify sensitive data types based on regulatory and organizational needs. Create DLP policies to monitor and protect this data across endpoints, file servers, and cloud services.

    - **Policy Configuration**: Configure DLP policies to detect and respond to potential data leaks. Set up rules for actions such as blocking access, encrypting data, or alerting administrators.

- **Policy Deployment**:
    - **Endpoint and Server Policies**: Deploy DLP policies to endpoints and file servers. Ensure that policies are applied consistently across all devices and storage locations.
    - **Cloud Integration**: Implement DLP policies for cloud-based applications and services to protect data stored and transmitted in the cloud.
- **Monitoring and Reporting**:
    - **Incident Management**: Configure alerts for DLP incidents and establish procedures for incident response and remediation.
    - **Reporting**: Set up reporting mechanisms to track DLP policy effectiveness and review incidents.

Microsoft Rapid Modernization Plan

Modernization Execution

- **Assessment**:
    - **Current State Evaluation**: Assess the current IT infrastructure, including hardware, software, and security measures. Identify gaps and areas for improvement.
    - **Modernization Roadmap**: Develop a roadmap for modernizing IT systems, including cloud adoption, automation, and security enhancements.
- **Cloud Migration**:
    - **Workload Assessment**: Evaluate which workloads and applications can be migrated to the cloud. Plan for migration, including data transfer, application reconfiguration, and testing.
    - **Cloud Services**: Leverage cloud services for scalability, flexibility, and cost-efficiency. Implement cloud-based security measures to protect data and applications.
- **Automation and Optimization**:
    - **Automation Tools**: Implement automation tools to streamline management and deployment processes. Use automation to enhance operational efficiency and reduce manual errors.

- **Security Integration**: Ensure that new systems and services are integrated with modern security practices and tools, including endpoint protection, identity management, and DLP.

On-Premises Server Management

File Servers and AD Server

- **File Servers**:
  - **Immutable Backup**: Secure file servers with Veeam immutable backups. Configure backup jobs and retention policies to ensure data protection.
  - **Encryption**: Implement encryption for data at rest and in transit. Ensure that backup data is also encrypted to prevent unauthorized access.
- **AD Server**:
  - **Hardening**: Harden the Active Directory server by applying security updates, enforcing strong authentication methods, and implementing MFA for administrative access.
  - **Integration with Azure AD**: Integrate with Azure AD for hybrid identity management. Configure synchronization and Conditional Access policies to enhance security.

Integration Architecture

Hybrid Identity Management

- **Azure AD Connect**:
  - Synchronize on-premises AD with Azure AD.
  - Implement Conditional Access policies.

Endpoint Management

- **Microsoft Endpoint Manager**:
  - Deploy and manage security policies across all endpoints.

Backup Integration

- **Veeam and Storage**:
  - Ensure Veeam integrates with immutable storage solutions.

DLP Integration

- **Cross-Platform Policies**:
    - Deploy DLP policies across endpoints, file servers, and cloud environments.

Data Architecture

Data Encryption

- **Encryption at Rest**:
    - Implement encryption for data on file servers and backup repositories.
- **Encryption in Transit**:
    - Ensure data in transit is encrypted between endpoints, file servers, and backup repositories.

Backup and Recovery

- **Immutable Backups**:
    - Use Veeam's immutable backup features and develop disaster recovery plans.

DLP Data Protection

- **Data Classification**:
    - Implement data classification schemes to apply appropriate DLP policies.

Security Architecture

Zero Trust Security Model

- **Principle of Least Privilege**:
    - Enforce least-privilege access controls.
- **Continuous Monitoring**:
    - Implement continuous monitoring of user and device compliance.

Advanced Threat Protection

- **Microsoft Defender**:

    - Utilize advanced threat protection features including ASR and AIR.
- **Palo Alto Firewalls**:
    - Leverage Palo Alto's advanced threat prevention capabilities.

Data Loss Prevention

- **DLP Policies**:
    - Implement and enforce DLP policies to protect sensitive data.

Infrastructure Requirements

Hardware

- **Palo Alto Firewalls**:
    - Deploy in high-availability configuration.
- **Endpoints**:
    - Ensure compatibility with Microsoft Defender and Endpoint Manager.

Software

- **Veeam Backup & Replication**:
    - Obtain licenses with immutability features.
- **Azure AD Licenses**:
    - Upgrade to Azure AD Premium P2 for PIM and JIT functionalities.

Network

- **Network Segmentation**:
    - Implement Zero Trust network segmentation.

Non-Functional Requirements

Performance

- **Backup and Recovery**:
    - Ensure backup and recovery processes meet performance and availability requirements.

Scalability

- **Endpoint Management**:
    - Plan for scalability in Endpoint Manager for growing device numbers.

Compliance

- **Regulatory Compliance**:
    - Ensure compliance with data protection regulations.

Transition and Implementation Strategy

Phased Implementation

- **Initial Phase**:
    - Implement Veeam immutable backups and upgrade network security with Palo Alto firewalls.
- **Subsequent Phases**:
    - Deploy Microsoft Defender, integrate Azure AD, implement DLP policies, and execute the modernization plan.

Testing and Validation

- **System Testing**:
    - Perform thorough testing of backup, endpoint protection, and DLP implementations.
- **User Acceptance Testing**:
    - Conduct user acceptance testing to ensure functionality meets business requirements.

Rollout Plan

- **Training**:
    - Deliver training sessions and develop ongoing awareness programs.
- **Support**:
    - Provide post-implementation support and monitor the performance of new systems.

Risks and Mitigations

Risk: Implementation Delays

- **Mitigation**:
    - Develop a detailed project plan and ensure resources are allocated appropriately.

Risk: Integration Challenges

- **Mitigation**:
    - Conduct thorough planning and testing to address integration issues.

Risk: Compliance Issues

- **Mitigation**:
    - Regularly review and update compliance measures and DLP policies.

Appendices

Appendix A: Veeam Immutable Backup Configuration Guide

- Detailed configuration instructions for Veeam Backup & Replication with immutable backup settings.

Appendix B: Palo Alto Firewall Configuration Guide

- Step-by-step configuration guide for deploying and managing Palo Alto firewalls.

Appendix C: Microsoft Defender Configuration and Best Practices

- Guidelines for configuring Microsoft Defender and implementing security best practices.

Appendix D: Data Loss Prevention (DLP) Policy Implementation Guide

- Instructions for creating, deploying, and managing DLP policies to protect sensitive data.

Appendix E: Incident Response Plan Template

- Template for developing an incident response plan, including roles, procedures, and communication strategies.

Appendix F: Employee Training Materials and Schedule

- Training materials, schedules, and content for initial and ongoing cybersecurity training programs.

Appendix G: Microsoft RAMP Implementation Guide

- Guidelines for applying Microsoft's Rapid Modernization Plan principles, including risk assessment, mitigation strategies, and continuous monitoring.

Overall Cost Estimate

Blueprint: £8,140 - £11,230

Materials: £84,000 - £104,000

Implementation: £24,280 - £33,180

Total Estimated Project Cost: £116,420 - £148,410

Summary

- **Blueprint**: £8,140 - £11,230
    - Includes high-level design, strategic planning, and documentation.
- **Materials**: £84,000 - £104,000
    - Covers hardware (firewalls), software licenses (Microsoft 365 E5), backup solutions (Veeam), and additional security tools.
- **Implementation**: £24,280 - £33,180
    - Involves configuring and deploying the solution, including roles for project management, cybersecurity consulting, systems engineering, and documentation.

This cost estimate provides a comprehensive view of the project, accounting for all major phases and necessary components. It ensures that each aspect of the project is adequately budgeted and planned for, from initial design to full implementation.

Overall Project Duration

Phase 1: 5-8 weeks

- **Description**: Initial consultation and blueprint development, including meetings with stakeholders, requirement gathering, high-level solution design, security architecture, integration architecture, and documentation.

Phase 2: 3-4 weeks (overlapping with Phase 1)

- **Description**: Procurement of materials such as Palo Alto firewalls, Microsoft 365 E5 licenses, Veeam backup solutions, and additional security tools, including vendor selection and ordering processes.

Phase 3: 10-15 weeks

- **Description**: Implementation phase involving infrastructure setup (firewalls, IPsec, Microsoft 365 E5, Microsoft Endpoint Manager, Veeam backups), security configuration (Zero Trust, PIM, JIT, Microsoft Defender, DLP), testing and validation of configurations, and employee training and awareness programs.

Phase 4: 2-3 weeks

- **Description**: Final review and handover, including reviewing the implemented solution, updating documentation, conducting final meetings with stakeholders, and transitioning support to operational teams.

Total Estimated Time

Total Duration: 20-28 weeks (Approximately 5-7 months)

Summary

The overall project duration, from the first contact with the client to project completion, is estimated to be around 5-7 months. This timeline includes all necessary phases such as initial consultation, blueprint development, procurement, implementation, testing, training, and final handover. This estimate provides a realistic view, accounting for task overlaps and dependencies, ensuring thorough planning and execution of the project.