**Company A & Company B Network Merger Documentation**

This document presents a comprehensive proposal for merging the network infrastructures of Company A and Company B. It integrates technical findings and recommendations derived from the provided risk assessments, network diagrams, vulnerability reports, and cybersecurity tools. The objective is to design a secure, scalable, and regulation-compliant hybrid architecture that addresses legacy system risks, supports zero trust principles, and remains within the $50,000 first-year budget constraint. Each section outlines identified problems, proposed solutions, and justifications for infrastructure decisions in line with modern cybersecurity best practices.

**BUSINESS REQUIREMENTS**

1. *Describe****two****current network security problems and****two****current infrastructure problems for each company, based on business requirements given in the scenario.*

**Company A**

**Network Security Problem 1** – No Network Authentication or Access Control Enforcement:

Company A lacks a RADIUS server or identity-aware network access control. Devices connect to the wired and wireless networks without authentication tied to user identity or device health. This exposes the internal LAN to unauthorized or unmanaged endpoints and violates Zero Trust principles.

**Network Security Problem 2** – Legacy Wireless Access Points with Poor Security Controls:

The network relies on two Meraki MR28 wireless access points, which are end-of-life and not centrally managed. These access points lack integration with any identity provider or policy enforcement engine, resulting in weak wireless security and a lack of visibility or control over connected devices.

**Infrastructure Problem 1** – Outdated Network Hardware:

The core switching infrastructure is built on Cisco 3750X switches, and the network edge is protected by a Cisco 7600 router, both end-of-life and unsupported by the vendor. These devices cannot accommodate modern routing features, security protocols, or software updates, making them a liability for performance and compliance.

**Infrastructure Problem 2** – Legacy Operating Systems in Production:

Company A still utilizes Windows Server 2012/2012R2 for critical roles such as application hosting, file sharing, and external-facing web services. These systems are nearing or past end-of-support, lack security patches, and are at odds with secure system baselines. Additionally, 14 laptops still run Windows 7, which is no longer supported and cannot be secured effectively.

**Company B**

**Network Security Problem 1** – No VLAN Segmentation for Internal Systems:

Despite having stacked switches and a corporate VLAN structure, Company B’s flat network design lacks logical segmentation for users, servers, printers, and guest access. Without proper VLAN boundaries, east-west traffic is unrestricted, increasing the risk of lateral movement in the event of an internal compromise.

**Network Security Problem 2** – Broad Attack Surface from Unmanaged Services and Open Ports:

The environment includes numerous exposed services such as FTP (ports 20, 21), RDP (3389), MariaDB (3306), and VMware (902, 8222) across internal systems. Many of these are hosted on Linux systems running varied web applications and databases, without evidence of a unified security policy or compensating controls like network segmentation, WAFs, or service isolation.

**Infrastructure Problem 1** – Workstations Running Unsupported Operating Systems:

Company B has 75 workstations across various platforms, including Windows XP and Windows 7. These systems are no longer supported and are incompatible with most modern endpoint detection and response (EDR) tools. Their presence introduces a significant vulnerability that affects the organization’s overall risk profile and violates fundamental compliance baselines (e.g., NIST, HIPAA, PCI).

**Infrastructure Problem 2** – Uncontrolled Server Sprawl and Mixed OS Deployment:

The Hyper-V environment includes over 20 virtualized servers spanning both Windows Server and multiple Linux distributions (Ubuntu, Debian). These include legacy Exchange servers post-migration, ElasticSearch clusters, Ruby on Rails apps, and databases running PostgreSQL and MariaDB. This complexity introduces high overhead for patching, monitoring, and configuration management, without centralized control, automation, or configuration baselines.

**VULNERABILITIES**

1. *Analyze the given network diagram and vulnerability scan for both companies by doing the following: 1. Describe two existing vulnerabilities for each company.*

Company A exhibits two critical vulnerabilities that present both operational and regulatory risks. The first is the continued use of unsupported operating systems, specifically, 14 laptops running Windows 7. Microsoft officially ended support for Windows 7, meaning these devices no longer receive security updates or patches. As a result, they are highly susceptible to known exploits such as EternalBlue, remote code execution, and privilege escalation. These endpoints represent a soft target for threat actors using phishing, lateral movement, or malware delivery as initial access vectors. The impact of compromise is high, especially given that these devices are likely connected to the internal production network without additional segmentation or endpoint detection. This vulnerability carries a high risk profile and a high likelihood of exploitation, given the widespread availability of automated tooling designed to exploit Windows 7 vulnerabilities.

The second vulnerability in Company A’s environment is an external-facing web server hosted in a demilitarized zone (DMZ) without application-layer protections. While a Fortinet firewall protects the server at the network level, there is no evidence of a web application firewall (WAF), intrusion prevention system (IPS), or reverse proxy performing deep packet inspection or traffic normalization. As a result, the server is exposed to application-layer threats such as SQL injection, cross-site scripting (XSS), and remote file inclusion, which can easily bypass traditional firewall policies. This is particularly concerning in a financial sector organization where public-facing systems are a prime target for attackers. The impact of a successful compromise would be severe, potentially leading to data loss, internal pivoting, or reputational damage. Given the absence of layered defenses and the prevalence of automated scanning tools, the likelihood of exploitation is moderate to high, and the overall risk is also high.

Company B also suffers from serious weaknesses that stem from architectural decisions and a lack of secure service design. One of the most pressing vulnerabilities is the exposure and continued use of insecure legacy protocols, including Telnet (port 23), FTP (ports 20/21), and RDP (port 3389). These services transmit credentials and data in plaintext, offering no encryption or protection from man-in-the-middle attacks. They are routinely targeted in credential harvesting campaigns, brute-force attacks, and ransomware operations. The risk is compounded by their presence on internal network segments that lack proper segmentation. This vulnerability poses a high impact. Credential theft or unauthorized access via these protocols can result in full domain compromise, and the risk and likelihood are both high due to the frequency with which these protocols are scanned and exploited in real-world attacks.

The second vulnerability in Company B’s network is the lack of centralized identity and access management. The environment does not use a federated identity provider, multi-factor authentication, or centralized access enforcement system. Instead, identity is handled in a fragmented, local manner across various Windows, Linux, and macOS systems. This decentralization significantly weakens the ability to monitor or control access, particularly in the event of credential theft or insider threats. This gap also has direct compliance implications in a network that manages sensitive medical provider and payment data. The impact of unauthorized access could include data leakage, regulatory penalties, and loss of customer trust. The risk level is high, and the likelihood of exploitation is moderate to high, especially given the commonality of credential compromise in targeted attacks.

**IMPACT, RISK, LIKELIHOOD**

1. *Analyze the given network diagram and vulnerability scan for both companies by doing the following: 2. Explain the impact, risk, and likelihood associated with each described vulnerability from part B1 as it relates to each company.*

In Company A’s environment, using unsupported Windows 7 endpoints introduces a clear and immediate security threat. These devices no longer receive security patches and are vulnerable to a wide range of publicly known exploits, including remote code execution and privilege escalation vulnerabilities. According to Company A’s internal risk analysis, these endpoints are part of the general user environment, meaning they are likely to interact with core applications, mapped drives, and internal resources. The impact of compromise is high, as these systems could be used as entry points for credential harvesting, lateral movement, or ransomware deployment. The likelihood of exploitation is also high due to the widespread availability of automated scanning tools and malware targeting unsupported operating systems. The overall risk associated with this vulnerability is classified as high.

The second vulnerability in Company A is the lack of application-layer protections for the external-facing web server in the DMZ. The network diagram shows that the web server is accessible from the public internet and only protected at the perimeter by a Fortinet NGFW. However, there is no mention of a web application firewall (WAF), intrusion prevention system (IPS), or reverse proxy to mitigate application-layer attacks. Without these defenses, the server is exposed to high-risk threats such as SQL injection, cross-site scripting, and remote file inclusion. The impact of successful exploitation is severe, particularly if the server provides access to backend systems or internal applications. The likelihood of exploitation is moderate to high based on its exposure and known attack trends against web infrastructure. The risk is therefore rated as high, due to the combination of exposed attack surface and lack of layered security.

Company B’s first major vulnerability is the active use of insecure legacy protocols, including Telnet (23), FTP (20/21), and RDP (3389), all identified in the network scan results. These services are unencrypted and known to transmit credentials in plaintext, making them easy targets for credential theft, man-in-the-middle attacks, and brute-force attempts. The vulnerability is amplified by the flat VLAN architecture shown in the network diagram and the lack of centralized monitoring. The impact of a successful attack is high, as attackers can gain access to critical internal systems, including file shares, application servers, or domain resources. The likelihood of exploitation is also high; attackers frequently scan for and target these ports due to their well-known weaknesses. Therefore, the risk associated with this vulnerability is unambiguously high.

The final vulnerability in Company B is the absence of centralized identity and access controls. According to the vulnerability report, there is no federated identity provider, no multi-factor authentication enforcement, and no unified directory service governing access across workstations, servers, or applications. This creates significant blind spots in access governance, particularly in an environment where systems span Windows, Linux, and macOS. The impact of compromise is extremely high without centralized controls; a single compromised credential could allow unrestricted access across multiple systems. Additionally, the lack of access visibility hinders incident response and violates key compliance requirements under HIPAA and PCI-DSS. The likelihood of unauthorized access is moderate to high, particularly in phishing or insider threat scenarios. The resulting risk is high due to organizational exposure and the criticality of handling data.

**TOPOLOGY DIAGRAM**

1. *Create a network topology diagram detailing the proposed merged network requirements.*

Check D482PA.vsdx for network topology.

**TOPOLOGY COMPONENTS**

1. *Identify the layer for all components in the topology diagram referencing the layers of the OSI model and TCP/IP protocol stack.*

|  |  |  |
| --- | --- | --- |
| **Device** | **OSI Layer** | **TCP/IP layer** |
| Firewall (FortiGate NGFW) | Layer 3/4/7 – Network/Transport/Application | Internet / Transport / Application |
| Servers (AWS: RDS, FSx, Beanstalk, Transfer Family, OpenSearch) | Layer 7 – Application | Application |
| Cabling (Cat5e) | Layer 1 – Physical | Network Access |
| VPN (FortiGate or SSL-VPN) | Layer 3/4/7 – Network/Transport/Application | Application |
| Laptops and Workstations | Layer 7 – Application | Application |
| Wireless Access Points (Aruba AP-535) | Layer 2/3 – Data Link / Network | Network Access |
| Switches (Aruba 2930F) | Layer 2 – Data Link | Network Access / Internet |
| Cloud RADIUS Service | Layer 7 – Application | Application |
| Okta Identity Platform | Layer 7 – Application | Application |
| AWS IAM Identity Center | Layer 7 – Application | Application |
| Monitoring Tools (CloudTrail, GuardDuty) | Layer 7 – Application | Application |

**RATIONALE**

1. *Explain the rationale for adding, deleting, or repurposing network components in the newly merged network topology diagram, including details of how each component addresses budgetary constraints.*

In designing the merged network topology for Companies A and B, strategic decisions were made to retain, replace, or repurpose hardware based on security needs and the defined budgetary constraint of $50,000. Rather than centralize infrastructure at a single location, both companies maintain their physical separation while leveraging cloud-based services and centralized identity to reduce technical debt and improve scalability.

One of the most critical upgrades was the replacement of Company A’s end-of-life Cisco 3750X switches and Cisco 7600 border router. These devices no longer receive firmware updates and lack modern capabilities such as VLAN tagging, secure remote access, and automated configuration management. They were replaced with Aruba 2930F 48G PoE+ switches, a modern alternative that supports VLANs, policy-based access control, and integration with identity-aware network enforcement. Priced at approximately $2,600 per unit (Hewlett Packard Enterprise, n.d.), four units were procured to cover Company A’s switching needs, totaling $10,400. This investment ensures secure network segmentation and long-term maintainability.

In addition, Company A’s legacy Meraki MR28 wireless access points were replaced with two Aruba AP-535 Wi-Fi 6 access points, which provide enterprise-grade wireless performance and integrate with cloud RADIUS for identity-based access control. The AP-535 supports modern encryption, advanced throughput, and centralized management features. Each unit is priced around $1,200 (CDW, n.d.), totaling $2,400 for two units. This upgrade replaces vulnerable, unsupported wireless infrastructure with a secure, scalable solution.

Both companies operate legacy Windows Server 2012/2012R2 instances for file storage, FTP, and application hosting. Rather than replacing these with new on-prem hardware, critical services were migrated to AWS-hosted platforms including RDS, FSx, Transfer Family, and Elastic Beanstalk. These services offer elasticity, built-in redundancy, and reduced management overhead. The deployment is scoped for minimal compute usage in year one, resulting in a projected cloud spend of $10,000 (Amazon Web Services, n.d.-a). This strategy reduces physical footprint while improving scalability and uptime.

The Fortinet FortiGate firewall at Company A and Sophos XG at Company B were retained. Both modern next-generation firewalls support VPN, deep packet inspection, and policy enforcement. Retaining these devices avoided unnecessary costs while maintaining strong perimeter defense. Similarly, Company B’s Aruba 2930F switches were also retained, as they match the upgraded infrastructure at Company A and remain within their supported lifecycle.

Both companies adopted Okta as the central identity provider to consolidate identity and access control, and it was federated with the AWS IAM Identity Center via SAML. Okta enables secure SSO, MFA, and device posture enforcement. With sufficient room remaining in the budget, the solution was scaled to include all 150 users for $10 per user per month, totaling $18,000 for the first year (Okta, n.d.). This full deployment eliminates fragmented access models, ensures every user is covered under centralized authentication, and simplifies user lifecycle management across cloud and on-prem environments.

Cloud RADIUS was also deployed at both physical locations to secure wireless access. Integrated with Okta, it provides user- and device-based enforcement at the network edge. JumpCloud’s cloud RADIUS platform was selected due to its native compatibility with Okta and low operational overhead. Licenses for all 150 users were included at $6 per user per month, totaling $7,200 for the year (JumpCloud, n.d.). This configuration ensures secure, identity-based Wi-Fi access across both environments without deploying and maintaining a dedicated on-prem RADIUS server.

The upgraded and newly adopted components include $10,400 for switches, $2,400 for wireless access points, $10,000 for AWS-hosted services, $18,000 for full Okta deployment, and $7,200 for cloud RADIUS. This brings the projected first-year cost to $48,000, keeping the total under the $50,000 budget. The design addresses high-priority security concerns, replaces only the most critical legacy systems, and enables scalable, identity-driven access control across physical locations and the cloud, ensuring full compliance and strategic flexibility.

**SECURE NETWORK DESIGN PRINCIPLES**

1. *Explain two secure network design principles used in the proposed network topology diagram.*

The proposed network architecture implements two foundational secure network design principles: Zero Trust architecture and network segmentation by role and function. These principles were selected to address known vulnerabilities in Company A and Company B’s legacy environments, while ensuring scalability and strong access control in a hybrid, cloud-integrated infrastructure.

The first principle, Zero Trust, is enforced throughout the entire network design. Under this model, no user or device is automatically trusted based on location, VLAN, or previous access. Every access request must be explicitly authenticated, authorized, and validated. In the proposed topology, this principle is operationalized by deploying Okta as the centralized identity provider, enforcing multi-factor authentication (MFA) and device posture checks for all 150 users across both physical sites. Okta is integrated with AWS IAM Identity Center via SAML, ensuring that access to cloud-hosted services such as RDS, FSx, Beanstalk, and Transfer Family is tightly controlled and audited. Additionally, Cloud RADIUS is deployed at each site to enforce identity-based authentication for Wi-Fi access, ensuring that even internal LAN access is restricted to known, compliant devices. These controls eliminate implicit trust across internal and external boundaries and enforce authentication at every access layer.

The second principle implemented is network segmentation, which restricts lateral movement and limits the blast radius of a potential compromise. Company A and Company B’s internal networks are segmented into dedicated VLANs such as user VLANs, server VLANs, guest VLANs, and printer VLANs using Aruba 2930F switches. These switches support policy-based VLAN tagging and access control, enabling isolation between functional groups. For example, guest users are segmented into an isolated VLAN without access to internal servers or production systems. Access between VLANs is governed by firewall rules on the FortiGate 800D and Sophos XG firewalls, ensuring that only explicitly authorized traffic (e.g., a specific port to a backend database) is allowed between zones. This segmentation strategy mitigates the risks identified in Company B’s legacy flat network design, which previously allowed unrestricted internal communication.

Together, these two principles form the backbone of a resilient, secure, and scalable network design that reduces attack surface, enforces least privilege, and aligns with modern enterprise security frameworks such as NIST SP 800-207 and CIS Controls.

**REGULATORY COMPLIANCE**

1. *Explain how the proposed merged network topology diagram addresses two regulatory compliance requirements that are relevant to the newly merged company, including the following in your explanation:*

*•   the name of the regulatory compliance requirement*

*•   Why the regulatory requirement is relevant to the newly merged company*

*•   How the proposed merged network topology diagram meets the regulatory requirement*

The proposed network topology was built with regulatory compliance in mind. Two relevant regulatory requirements for the newly merged organization are the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS). These regulations were selected based on the business operations and data sensitivities in each company’s legacy environment.

The first applicable regulation is HIPAA, which is relevant because Company B handles medical provider and patient-related data that may include electronic protected health information (ePHI). HIPAA requires organizations to implement administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of ePHI. The proposed network enforces HIPAA’s technical safeguard requirements through multiple mechanisms. All users authenticate using Okta with multi-factor authentication and device posture checks, satisfying access control mandates under HIPAA §164.312(a) (U.S. Department of Health and Human Services, 2013). Additionally, access to internal systems and cloud services is tightly logged through AWS CloudTrail, meeting audit control expectations defined in §164.312(b). Cloud RADIUS further secures wireless access by ensuring only verified users and devices can join internal networks. Sensitive systems previously hosted on local servers are migrated to HIPAA-eligible AWS services such as FSx and RDS. These natively provide encryption in transit and at rest to satisfy HIPAA’s transmission security requirements under §164.312(e).

The second regulation, PCI DSS, is relevant due to Company A’s role in the financial sector, which involves processing credit card or payment data. PCI DSS mandates that companies secure cardholder data through robust access controls, network segmentation, and encrypted transmission of sensitive data. The proposed architecture addresses PCI DSS Requirement 8 by enforcing all personnel's unique user identities and MFA through Okta (PCI Security Standards Council, 2022). Access is tightly scoped using group policies and integrated with AWS IAM Identity Center to ensure least privilege. Aruba switches and VLAN segmentation across both sites provide that the cardholder data environment (CDE) is logically isolated from general-purpose traffic, aligning with PCI DSS Requirement 1. In addition, AWS Elastic Beanstalk and RDS allow the company to meet encryption and logging requirements outlined in PCI DSS Requirements 10 and 11 by using AWS-native tools like CloudTrail and GuardDuty to monitor and report on access and anomalies.

By addressing HIPAA through authenticated identity controls, cloud-based encryption, audit logging, and meeting PCI DSS through segmentation, SSO, and secure system design, the proposed network ensures that both regulatory obligations are met using scalable, modern infrastructure. These controls also lay the groundwork for streamlined audits and future certification readiness.

**EMERGING THREATS**

1. *Describe two emerging threats that apply to the merged organization, including the following in the description:*

*•   potential network security risks of implementing the topology*

*•   potential performance impacts on the merged network after implementation of the proposed design*

*•   How to manage the identified potential security risks*

While the proposed merged network design significantly improves the security posture of both organizations, it introduces new potential threats, particularly related to cloud integration and centralized identity infrastructure. Two emerging threats applicable to the merged organization are: (1) identity-based attacks on federated access infrastructure, and (2) cloud service misconfigurations and data exposure. These threats could impact security and performance if not proactively mitigated.

The first emerging threat involves identity-based attacks, such as credential phishing, session hijacking, or exploitation of identity federation misconfigurations. Because the proposed design centralizes user authentication through Okta and federates that identity into AWS IAM Identity Center via SAML, attackers may target the identity infrastructure as a single point of compromise. A successful phishing campaign or token theft via session hijacking could grant unauthorized access to cloud services, bypassing traditional perimeter defenses. This creates a significant network security risk, as attackers could access sensitive data or deploy malicious services within the AWS environment.

Additionally, performance may be impacted during login spikes or failover scenarios. If Okta becomes temporarily unreachable or performance degrades, users across both sites may experience delays or be locked out of critical systems, particularly cloud-hosted services. To manage this threat, the organization must implement strict phishing-resistant MFA methods (e.g., WebAuthn or authenticator apps) and enforce device posture policies via Okta. Okta’s built-in anomaly detection and AWS’s session timeout and re-authentication policies should also be configured. Regular testing of the SAML trust and active monitoring of authentication logs are essential to detect abuse patterns early.

The second emerging threat involves cloud service misconfiguration, one of the most common and impactful causes of breaches in hybrid environments. As the merged organization migrates file storage, applications, and databases to AWS services (FSx, Transfer Family, RDS, Beanstalk), the risk of unintentionally exposing sensitive data increases. For example, an external actor could gain access to regulated or confidential data if an S3 bucket or RDS instance is misconfigured to allow public access or lacks proper IAM scoping.

These configuration errors may also introduce performance issues, particularly if cloud services are overprovisioned, undersecured, or misaligned with actual usage patterns. Poorly optimized instances can cause latency, degrade user experience, or lead to unexpected AWS billing spikes. To manage this threat, the organization must implement infrastructure-as-code (IaC) with automated security checks (e.g., AWS Config, CloudFormation with guardrails) and enable GuardDuty and CloudTrail for continuous monitoring and alerting. Access policies must follow the principle of least privilege, and all cloud resources should be subjected to regular audits using AWS Trusted Advisor or third-party tools like Prisma Cloud.

These risks can be addressed through hardened identity enforcement, cloud-native monitoring, and secure deployment pipelines that align with the organization's Zero Trust and compliance-focused architecture.

**SUMMARY RECOMMENDATIONS**

1. *Summarize your recommendations for implementation of this proposed merged network based on the scenario and budgetary requirements, including the following in the summary:*

*•   a cost-benefit analysis for on-premises and cloud infrastructure solutions*

*•   a justification for your recommendations to implement the proposed secure merged network design*

The recommended merged network design uses a hybrid approach to maximize cost-efficiency and security. Core infrastructure was redesigned to retain support for on-premises equipment where possible, replace only security-critical legacy hardware, and shift high-maintenance services to the cloud using AWS. This approach enables the merged organization to meet compliance and operational requirements while remaining within the $50,000 first-year budget.

A cost-benefit analysis of on-premises versus cloud infrastructure strongly supports this hybrid design. Replacing all end-of-life servers and maintaining on-prem file storage, FTP, and application servers would have cost over $30,000 in hardware, not including licensing, power, physical security, and IT overhead. These systems also require ongoing patching and backups, increasing operational risk and long-term maintenance costs. In contrast, migrating key services to AWS, including RDS, FSx, Beanstalk, and Transfer Family, reduces capital expenditure and shifts infrastructure management to a cloud provider with built-in compliance controls. These services are scoped to fit within a $10,000 annual usage budget, and provide encrypted data handling, backup automation, high availability, and fine-grained access control. The scalability and reduced management burden offer technical and financial advantages over legacy hardware.

On the identity and access side, deploying Okta across all 150 users provides a centralized, cloud-native platform for single sign-on (SSO), multi-factor authentication (MFA), and device posture enforcement. This investment $18,000 annually eliminates the need for fragmented domain controller infrastructure and hard-to-scale VPN authentication. Okta’s integration with AWS IAM Identity Center streamlines cloud access, aligns with Zero Trust principles, and simplifies access revocation and auditing across cloud and internal systems. Additionally, Cloud RADIUS, licensed for the same user base at $7,200, allows identity-based Wi-Fi authentication at each location without deploying and maintaining physical RADIUS servers.

The organization addresses known security gaps without unnecessary overhauls by selectively replacing only unsupported network equipment (Cisco 3750X switches and Meraki MR28 APs). Four Aruba 2930F switches and two Aruba AP-535 access points were procured for Company A, totaling $12,800. Company B’s supported switches and firewalls were retained, keeping hardware costs lean.

This approach balances capital and operational costs, targets known vulnerabilities, and positions the company for secure growth. It reduces technical debt, improves resilience, and integrates regulatory compliance directly into the infrastructure through encrypted cloud services, identity governance, and policy-driven access control, all while remaining $2,000 under budget.

**SOURCES**

*45 CFR 164.312 -- Technical safeguards. (n.d.). https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.312*

*AWS Pricing Calculator. (n.d.). https://calculator.aws/*

*Epson EcoTank Pro ET-5850 All-in-One Multifunction Printer - C11CJ29201 - All-in-One Printers - CDW.com. (n.d.). CDW.com. https://www.cdw.com/product/hpe-aruba-ap-535-wireless-access-point/5899424*

*JumpCloud. (2025, May 20). Pricing - JumpCloud. https://jumpcloud.com/pricing*

*Payment Card Industry Data Security Standard: Requirements and Testing Procedures (Version 4.0). (2022). PCI Security Standards Council. https://www.pcisecuritystandards.org/documents/PCI-DSS-v4\_0.pdf*

*Plans and pricing | Okta. (n.d.). https://www.okta.com/pricing/*

*PROVANTAGE: HPE JL262A#ABA Aruba 2930F 48G POE+ 4SFP Switch. (n.d.). https://www.provantage.com/hpe-jl262a-aba~7HEWN41W.htm*