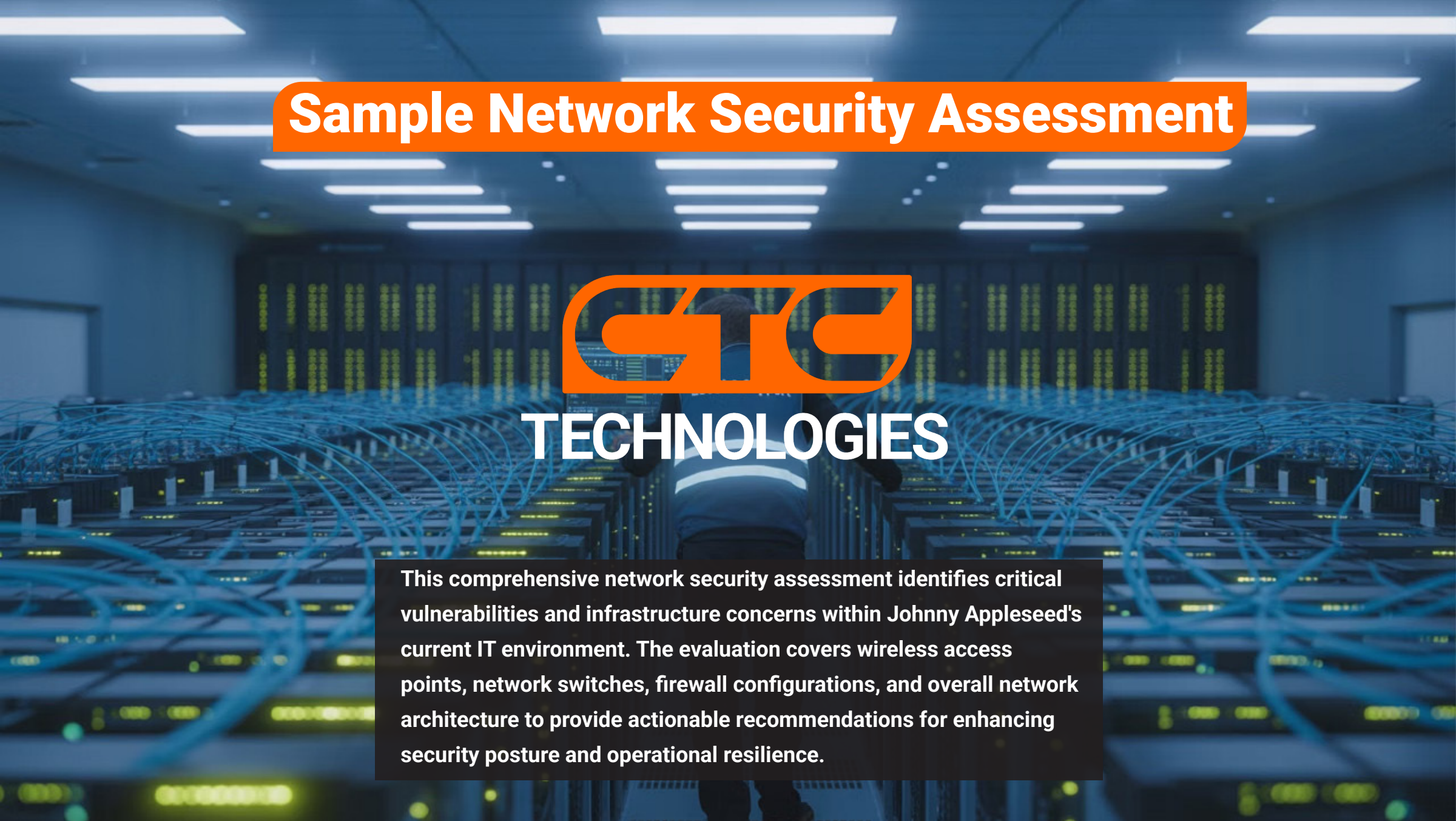
Sample Network Security Assessment



GTC TECHNOLOGIES

This comprehensive network security assessment identifies critical vulnerabilities and infrastructure concerns within Johnny Appleseed's current IT environment. The evaluation covers wireless access points, network switches, firewall configurations, and overall network architecture to provide actionable recommendations for enhancing security posture and operational resilience.

Executive Summary and Critical Findings

Johnny Appleseeds' network infrastructure presents several high-priority security vulnerabilities that require immediate attention. The assessment reveals a flat network architecture with insufficient segmentation, end-of-life hardware components, and firewall misconfigurations that expose the organization to significant cyber threats.

Critical issues include firewall rules allowing unrestricted WAN-to-LAN access, multiple end-of-support switches creating maintenance gaps, and a daisy-chained switching architecture lacking redundancy. These vulnerabilities collectively create potential attack vectors that could compromise network integrity and business operations.

The wireless infrastructure appears stable with modern access points, though management strategy clarification is needed. Email services show concerning volume patterns from backup systems that warrant investigation. Immediate remediation of high-priority firewall rules and development of a hardware refresh strategy are essential for maintaining security compliance and operational continuity.

High Priority Issues

- Unrestricted WAN-to-LAN firewall access
- Missing security profiles in policies
- Exposed PBS access from WAN

Infrastructure Concerns

- Multiple end-of-life switches
- Flat network architecture
- No switching redundancy

Operational Issues

- High CPU utilization on switches
- Disabled password complexity
- Excessive backup email volume

Wireless Infrastructure Assessment

The wireless network infrastructure consists of seven access points utilizing EnGenius EWS276-FIT and EWS377-FIT models. These are relatively modern enterprise-grade devices that support the latest wireless standards and provide adequate coverage for the current environment. The hardware appears to be in good operational condition with no immediate security concerns identified during the assessment.

However, several management questions require clarification to ensure optimal deployment and security posture. The current management approach4whether cloud-based, controller-based, or standalone4significantly impacts security policies, firmware updates, and centralized monitoring capabilities. Cloud-based management typically provides better security patch management and centralized policy enforcement, while standalone configurations may offer more granular control but require manual maintenance.

End-of-life planning for these devices is crucial for maintaining security compliance. While current models appear to be within their support lifecycle, establishing a proactive replacement schedule ensures continued vendor support and security updates. The organization should verify warranty status and plan for refresh cycles typically occurring every 5-7 years for enterprise wireless equipment.

Current Deployment

- 3 × EWS276-FIT access points
- 4 × EWS377-FIT access points
- No immediate security issues identified
- Modern enterprise-grade hardware

Outstanding Questions

- Management platform configuration
- End-of-life and support timeline
- Firmware update scheduling
- Security policy enforcement method

Network Switching Infrastructure Analysis

The network switching infrastructure presents significant concerns with multiple end-of-life devices creating security and operational risks. Seven switches comprise the current deployment, with four models showing expired or near-expired support lifecycles that demand immediate attention and planning for replacement or extended support arrangements.

The Cisco SG500-52P switches (4 units) reached end-of-support in April 2023, creating critical vulnerabilities as security patches and firmware updates are no longer available. Similarly, the SF300-24P switch expired software maintenance in October 2019, representing a severe security gap with over four years without updates. The SF220-24P and SG550X-48P switches expired software maintenance in July 2023 but retain hardware support until 2027, providing a window for migration planning.

Performance issues compound these lifecycle concerns, with high CPU utilization observed across multiple switches likely attributed to SNMP service overhead. While traffic flow appears unaffected currently, sustained high CPU usage can impact performance under load and may indicate configuration optimization opportunities. Password complexity being disabled across multiple devices creates additional authentication vulnerabilities that require immediate remediation through policy enforcement and configuration standardization.

7

Total Switches

Mixed vendor and model deployment

5

End-of-Support

Devices requiring immediate attention

4

High CPU Usage

Switches showing performance issues

Switch End-of-Life Timeline and Risk Assessment

The switching infrastructure end-of-life analysis reveals critical timelines that require immediate strategic planning and budget allocation. Current deployment includes devices spanning different support phases, from already expired maintenance windows to equipment approaching end-of-support within the next few years.

Immediate action items include the four Cisco SG500-52P switches that reached end-of-service-life in April 2023, eliminating access to security updates, bug fixes, and technical support. This creates significant compliance and security risks, particularly in regulated environments where current vendor support may be mandatory. The single SF300-24P switch presents the highest risk, having been without software updates since October 2019, making it vulnerable to known exploits and security vulnerabilities.

Medium-term planning should address the SF220-24P and SG550X-48P switches, which maintain hardware support through July 2027 despite expired software maintenance. This provides a 3-4 year window for planned replacement while maintaining some vendor relationship for hardware failures. The organization should prioritize replacement of the oldest and most vulnerable devices first, followed by a systematic refresh strategy for remaining equipment.

Device Model	Quantity	Software EOS	Hardware EOS
SG500-52P	4	April 2023	April 2023
SF300-24P	1	October 2019	October 2023
SF220-24P	1	July 2023	July 2027
SG550X-48P	1	July 2023	July 2027

Firewall Security Configuration Analysis

The FortiGate-100F firewall deployment contains several critical security misconfigurations that expose the network to significant threats. While the hardware platform is robust and current, policy implementation reveals fundamental security gaps that require immediate remediation to prevent potential breaches and maintain compliance with security best practices.

Rule 13 represents the most critical vulnerability, allowing unrestricted traffic from the WAN to reach any destination on the local LAN. This configuration essentially negates the firewall's primary security function and creates a direct pathway for external attackers to access internal resources. This rule must be immediately disabled or replaced with specific, restrictive policies that only allow necessary traffic to designated services.

Rule 6 permits PBS access from the WAN without IP restrictions, creating another high-risk exposure. External access to backup systems should be limited to specific trusted IP addresses or ranges, preferably through VPN connections rather than direct internet exposure. The absence of security profiles across firewall policies eliminates crucial protections like intrusion prevention, antivirus scanning, and application control that modern firewalls should provide.

Critical: Unrestricted WAN-to-LAN Access

Rule 13 allows any WAN traffic to reach internal LAN resources, creating direct attack pathway

High Risk: Exposed Backup System

Rule 6 permits PBS access from any WAN IP, should restrict to trusted sources only

Missing Security Controls

No security profiles implemented, losing IPS, antivirus, and application control protections

Network Architecture and Topology Concerns

The current network architecture exhibits a flat topology with switches connected in a daisy-chain configuration, creating multiple single points of failure and limiting scalability. This design approach, while simple to implement initially, introduces significant operational risks and performance limitations that impact both reliability and security posture.

The daisy-chain switching topology means that failure of any intermediate switch can isolate downstream devices, potentially causing widespread network outages. This architecture also creates suboptimal traffic flows, as communication between devices on different switch segments must traverse multiple hops, increasing latency and reducing available bandwidth. The lack of redundant links eliminates failover capabilities and prevents implementation of spanning tree protocols that could provide automatic recovery from link failures.

Network segmentation is virtually non-existent, with all devices operating on the same broadcast domain. This flat architecture eliminates security boundaries between different device types and user groups, allowing lateral movement for attackers who gain initial access to any network-connected device. Modern network security principles require microsegmentation to limit blast radius and contain potential security incidents. The current VPN implementation using SSL should be migrated to IPsec for improved security and performance characteristics.

Topology Issues

- Daisy-chained switch connectivity
- No redundant network paths
- Single points of failure
- Suboptimal traffic flows

Security Concerns

- Flat network architecture
- No network segmentation
- Unrestricted lateral movement
- SSL VPN instead of IPsec

Immediate Security Remediation Priorities

Critical security vulnerabilities require immediate attention to prevent potential network compromise and data breaches. The remediation timeline should prioritize firewall misconfigurations that create direct attack vectors, followed by infrastructure hardening measures that improve overall security posture. These actions can be implemented within days or weeks and provide significant risk reduction.

Firewall rule remediation must be the first priority, beginning with complete removal or restriction of Rule 13 that allows unrestricted WAN-to-LAN access. This rule should be replaced with specific policies that only permit necessary traffic to designated services using least-privilege principles. Rule 6 requiring PBS access should be modified to allow connections only from specific trusted IP addresses or implement VPN-based access instead of direct internet exposure.

Security profile implementation across all firewall policies will activate intrusion prevention, antivirus scanning, and application control features that provide crucial protection against modern threats. Password complexity enforcement on network switches must be enabled immediately, followed by configuration standardization across all devices.

1

Disable Critical Firewall Rules

Remove or severely restrict Rules 13 and 6 within 24-48 hours

2

Implement Security Profiles

Enable IPS, antivirus, and application control on all policies

3

Enable Password Complexity

Enforce strong authentication across all network devices

Strategic Infrastructure Modernization Plan

Long-term infrastructure modernization requires a comprehensive approach addressing hardware refresh cycles, network architecture redesign, and security enhancement initiatives. Hardware replacement strategy must prioritize the most vulnerable devices first, beginning with the SF300-24P switch that has been without security updates since 2019, followed by the four SG500-52P switches that reached end-of-life in April 2023. New switching infrastructure should implement redundant connectivity with ring or mesh topologies, eliminating single points of failure and providing automatic failover capabilities.

Modern managed switches with current firmware support and enterprise-grade security features will provide the foundation for improved network segmentation and monitoring. Network architecture redesign should implement VLAN segmentation to create security boundaries between different device types, user groups, and service tiers. This microsegmentation approach significantly reduces attack surface and contains potential security incidents. A single point of failure lies at the boundary of the network since the firewall is running in standalone mode without an HA device for failover. It's recommended to purchase an additional firewall with the same model to eliminate the single point of failure. The migration from SSL VPN to IPsec-based remote access will provide stronger encryption, better performance, and more granular access controls. Email service optimization should address the excessive Veeam backup notifications that may indicate configuration issues or potential system problems requiring investigation.

Phase 1: Critical Replacement

Replace end-of-life switches, implement basic network redundancy.

1

2

Phase 2: Architecture Redesign

Deploy VLAN segmentation, migrate to IPsec VPN, add firewall HA.

3

Phase 3: Ongoing Optimization

Implement continuous monitoring and address specific service issues like Veeam notifications.

Recommendations and Next Steps

The Johnny Appleseed network security assessment reveals a critical need for immediate remediation actions combined with strategic infrastructure planning to achieve a robust, secure, and resilient network environment. Success requires executive support, adequate budget allocation, and coordinated implementation across multiple technology domains to address both urgent vulnerabilities and long-term architectural improvements.

Immediate actions within the next 30 days must focus on the highest-risk firewall configurations that expose the network to direct attack. Removing unrestricted WAN-to-LAN access rules and implementing security profiles will provide substantial risk reduction with minimal operational impact. Simultaneously, enabling password complexity on network switches will address authentication weaknesses..

Strategic planning should prioritize hardware refresh cycles based on end-of-life status and security risk assessment. Budget allocation should account for not just hardware replacement costs but also professional services for architecture redesign, security policy development, and staff training on new technologies. Regular security assessments should be scheduled quarterly to monitor progress, identify emerging threats, and validate that implemented controls are functioning effectively in the evolving threat landscape.

Immediate Actions

- Remediate critical firewall rules 13 and 6
- Enable security profiles on all policies
- Implement password complexity requirements
- Investigate Veeam email volume issues

Short-term Goals

- Replace most critical end-oflife switches
- Design network segmentation strategy
- Develop hardware refresh budget proposal
- Plan redundant connectivity implementation

Long-term Strategy

- Complete infrastructure modernization
- Implement comprehensive network segmentation
- Migrate to IPsec VPN infrastructure
- Establish ongoing security assessment program

About CTC Technologies

We are dedicated to providing cutting-edge network security solutions and strategic IT infrastructure modernization. Your trusted partner for a secure and resilient digital future.

CTC TECHNOLOGIES

Phone
(734) 408-0200

Email
info@ctctechnologies.com

Website
www.CTCTechnologies.com

Address
7136 Jackson Rd, Ann Arbor, MI 48103

Our Services

Network Health and Security Assessments

Comprehensive evaluation of your network infrastructure to identify vulnerabilities, risks and overall health.

Network Security Services

Expert setup and ongoing management of firewalls for robust perimeter defense.

IT Infrastructure Refresh/Modernization

Strategic upgrades and implementation of cut-tingedge technologies for enhanced performance and security.

Cloud Security Solutions

Protecting your data and applications in cloud environments with advanced security measures.

Data Protection & Recovery

Implementing robust backup, recovery, and data loss prevention strategies.

Managed IT Services

Proactive monitoring, maintenance, and support to ensure optimal IT operations.

Low-Voltage and Fiber Optic Cabling

Professional installation and management of low-voltage and fiber optic cabling for reliable network connectivity.

Network Design and Architecture

Custom network infrastructure design, ensuring scalability, efficiency, and robust performance.

Wireless Site Surveys

Thorough analysis of your environment to determine optimal placement and configuration for wireless networks.

Wireless Network Design and Architecture

Designing secure and high-performing wireless solutions tailored to your specific business needs.