# Network Security Risk Management Report

**Security Team**

April 16, 2023

## Abstract

This report evaluates the network security risks associated with the organizations IT infrastructure, focusing on the AT&T ISP Point-to-Point connectivity and diverse endpoint environment. It identifies critical vulnerabilities, assesses their likelihood and impact, and proposes mitigation strategies to ensure data confidentiality, integrity, and availability. The recommendations leverage advanced security solutions, including VPNs, network access control, malware protection, and physical security enhancements, to address risks such as unauthorized access, data breaches, and power disruptions.

# Contents

# 1 Introduction

In todays evolving threat landscape, robust network security is critical to protecting the organizations IT infrastructure. This report evaluates risks associated with the AT&T ISP Point-to-Point connectivity and diverse endpoint environment across departments, including Software Development, Quality Assurance, and Customer Support. By identifying vulnerabilities, assessing their impact, and proposing mitigation strategies, we aim to ensure data confidentiality, integrity, and availability while supporting operational efficiency.

# 2 Risk Identification

The organizations network faces several risks, including:

- **Unauthorized Access**: Weak authentication or lack of device visibility may allow unauthorized users or devices to access sensitive systems.
- **Data Breaches**: Exposure of data over public internet or unencrypted channels increases vulnerability to hacking.
- **Malware and Ransomware**: Diverse endpoints (e.g., Linux, Windows, macOS) are susceptible to malicious software.
- **Power Disruptions**: Lack of UPS power in critical facilities risks downtime and data loss.
- **Physical Security Gaps**: Open racks in data centers expose equipment to tampering.
- **Non-Compliant Devices**: BYOD policies without strict controls may introduce vulnerabilities.

# 3 Risk Assessment

The identified risks vary in likelihood and impact:

- **Unauthorized Access**: High likelihood due to diverse devices; high impact due to potential data exposure.
- **Data Breaches**: Moderate likelihood with public internet usage; critical impact on sensitive data.
- **Malware/Ransomware**: High likelihood given varied endpoints; severe impact on operations.
- **Power Disruptions**: Moderate likelihood; high impact on business continuity.
- **Physical Security Gaps**: Low likelihood but high impact if exploited.
- **Non-Compliant Devices**: Moderate likelihood with BYOD; moderate to high impact on network security.

# 4 Risk Mitigation Strategies

## 4.1 Network Access Control (NAC)

Aruba ClearPass provides a policy management platform to enforce network access across wireless, wired, and VPN networks:

- Delivers device visibility, policy control, and attack response.
- Redirects users to login pages for credential verification, ensuring authorized access.
- Uses RADIUS functionality to authenticate users/devices and assign VLANs dynamically.

## 4.2 Secure Remote Access

Cisco AnyConnect VPN ensures secure mobility:

- Prevents noncompliant devices from accessing the network using Cisco ISE.
- Uses SSL/TLS for encrypted tunnels, compatible with Windows, macOS, iOS, and Android.
- Operates over HTTPS ports (443), bypassing restrictive firewalls without specialized client software.

## 4.3 Data Encryption and Integrity

To protect data in transit:

- **AT&T Point-to-Point Connectivity**: Offers dedicated links with optional encryption, avoiding the public internet for enhanced security.
- **SFTP**: Uses SSH for encrypted file transfers over Port 22, with authentication via username/password or cryptographic keys.
- **HTTPS**: Ensures data integrity for customer-facing websites, protecting login credentials.

## 4.4 Malware and Ransomware Protection

Bitdefender GravityZone provides advanced endpoint security:

- Offers web-based analytics, dashboards, and reporting for risk assessment.
- Includes anti-ransomware protection by backing up and restoring targeted files.
- Defends against ransomware, phishing, zero-day attacks, and spyware.

## 4.5 Web Security and Content Filtering

Cisco Secure Web Virtual Appliance (SWAV) ensures secure web access:

- Restricts access to internal documentation websites.
- Provides malware protection through threat-intelligence infrastructure.

- Enforces web filtering policies to block malicious content.
- Performs SSL inspection to identify threats in HTTPS traffic.

### 4.6 Network Segmentation

To enhance security:

- **Cisco Catalyst Switches**: Use VLANs and ACLs to separate internal/external traffic.
- **Cisco NGFW**: Enforces access policies and inspects traffic, with a DMZ for external-facing servers.
- **Aruba ClearPass**: Dynamically assigns devices to VLANs based on authentication.

### 4.7 Power Protection

To mitigate power disruption risks:

- **APC Smart-UPS (Main Office)**: Supports servers and switches with intelligent battery management.
- **Eaton 5PX UPS (IT & Datacenter)**: Provides battery backup and remote management for network equipment.
- **Eaton 5SC UPS (Customer Support/Sales)**: Offers power protection with Advanced Battery Management.

### 4.8 Physical Security Enhancements

To address physical vulnerabilities:

- **Avigilon Cameras**: Deployed in data centers for monitoring.
- **Locked Cabinets**: Replace open racks, with keys managed by IT Director, Network/System Admins, CTO, and maintenance.
- **Eaton RS Enclosure**: Supports Cisco switches in the Sales building data center.

### 4.9 Logging and Auditing

SolarWinds Security Event Manager (SEM) ensures oversight:

- Analyzes logs to detect unauthorized access or policy violations.
- Provides compliance reports for HIPAA, PCI DSS, and other standards.
- Monitors configuration file integrity for unauthorized changes.

### 4.10 BYOD and Mobile Security

A BYOD policy with Apple iPhones ensures:

- Seamless integration with Cisco networks and security features.
- Mobile Application Management with encryption, access controls, and compliance monitoring.

- Data wipe policies for lost or noncompliant devices.

### 4.11 Collaboration and Customer Support

To support customer-facing teams:

- **Microsoft Teams**: Enables remote collaboration and issue escalation via dedicated customer channels.
- **Cisco AI Assistant**: Provides conversation summaries, burnout detection, and topic analytics for contact center agents.

## 5 Implementation Considerations

| Phase | Timeline |
|---|---|
| Risk Assessment | Weeks 1-2 |
| Solution Design | Weeks 3-4 |
| Hardware/Software Deployment | Weeks 5-8 |
| Employee Training | Weeks 9-10 |
| Ongoing Monitoring | Month 3 Onward |

Table 1: Implementation Timeline

Implementation will address the diverse endpoint environment:

- **Software Development**: Upgrade 67 Linux, 21 PC, 21 Mac to 109 Win11 PCs.
- **Quality Assurance**: Upgrade 22 Win8/10 PCs to 22 Win11 PCs.
- **Research and Development**: Upgrade 31 CentOS 6 to 31 Win11 PCs.
- **Network Administration**: Upgrade 7 Mac to 7 Win11 PCs.
- **System Administration**: Upgrade 6 Solaris, 3 Debian11 to 9 Win11 PCs.
- **Product Sales**: Upgrade 27 Win7 to 27 Win11 PCs.
- **Customer Support**: Upgrade 14 WinXP/Win7 to 14 Win11 PCs.
- **Financial**: Upgrade 8 WinXP to 8 Win11 PCs.

Standardizing on Windows 11 ensures compatibility with security solutions and consistent policy enforcement.

## 6 Conclusion

This report outlines a comprehensive strategy to mitigate network security risks within the organizations IT infrastructure. By leveraging AT&Ts Point-to-Point connectivity, Cisco, Aruba, and other advanced solutions, we address vulnerabilities, ensure compliance, and enhance operational resilience. The Security Team is prepared to collaborate with stakeholders to implement these recommendations, ensuring a secure and reliable network environment. For further details, contact the Security Team at cybersecurity@att.com or 1-800-555-1234.