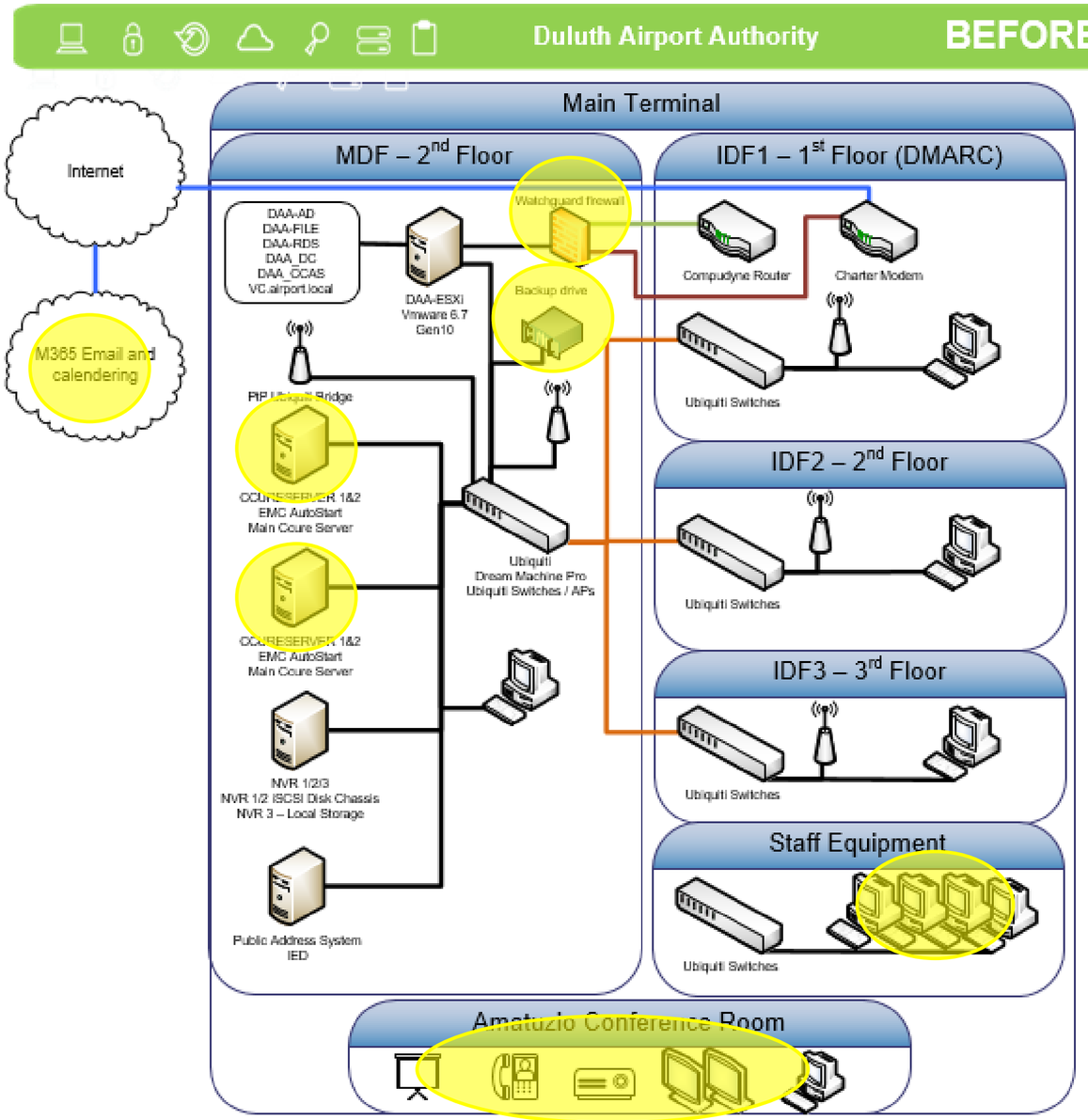
Duluth Airport Authority

Board Update

CITON

Infrastructure Resiliency

Where we started … (January 2021)

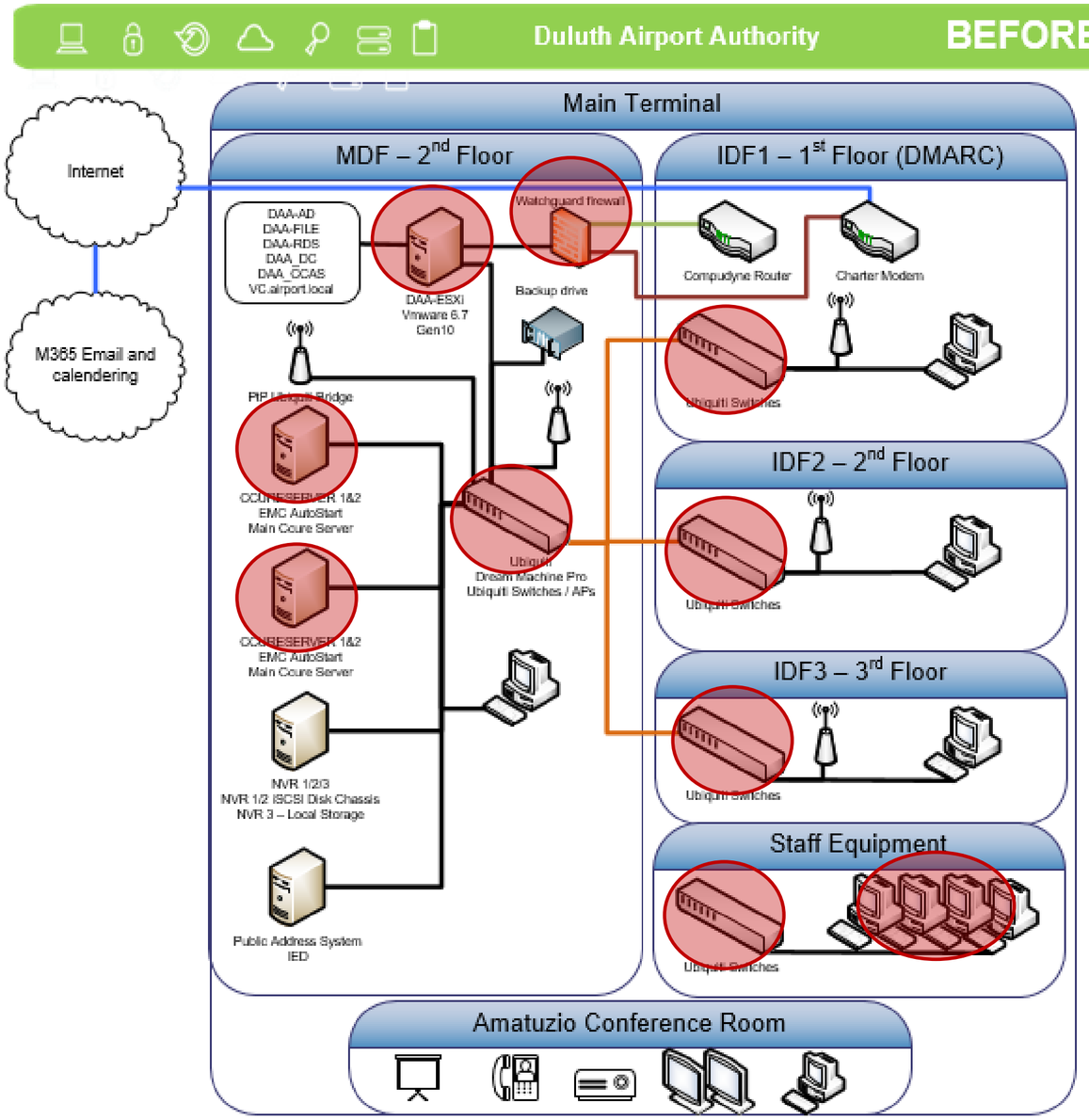


- CCure Servers – badging system – on aging, out of support, hardware and software.
- Backup drive with data, but no local or cloud business continuity.
- Aging firewall, not owned by DAA.
- No backups of data in M365 cloud – email, calendars, files, etc.
- Multiple staff computers well beyond fit for purpose – up to 12.5 years old.
- Difficult to use, inconsistent conference room with limited functionality.

SPECIALIZING IN CREATIVE SOLUTIONS FOR
209 West First Street, Duluth, MN 55802 P 218 720 4435 F 218 722 1231 www.citon.com
Custom Computers + Workstations | Servers + Storage | Network + Wireless Infrastructure
Hosted Email and UC | Layered Enterprise Security | Data Center | Managed IT

Infrastructure Vulnerabilities

Where we started … (January 2021)



- CCure Servers – badging system – operating system and software out of support – no updates no security patches.
- Firewall without advanced filtering and logging, and without SIEM/SOC.
- Main server software behind on patching, firmware and security updates.
- Older accounting server behind on patching, firmware and security updates.
- Multiple staff computers operating systems out of support, no security patches. Others behind on patches.
- Switch and wireless infrastructure behind on patches.
- Remote connections to DAA network and to M365 missing multi-factor authentication.

SPECIALIZING IN CREATIVE SOLUTIONS FOR
209 West First Street, Duluth, MN 55802 P 218 720 4435 F 218 722 1231 www.citon.com
Custom Computers + Workstations | Servers + Storage | Network + Wireless Infrastructure
Hosted Email and UC | Layered Enterprise Security | Data Center | Managed IT

Infrastructure Vulnerabilities

Before …

(January 2021)

Duluth Airport Authority
Vulnerability Scan Results and Reccomendations
April 2021

Always On™
CITON
COMPUTER CORP

Vulnerability Scan Overview: Scan Date: 2-23-2021

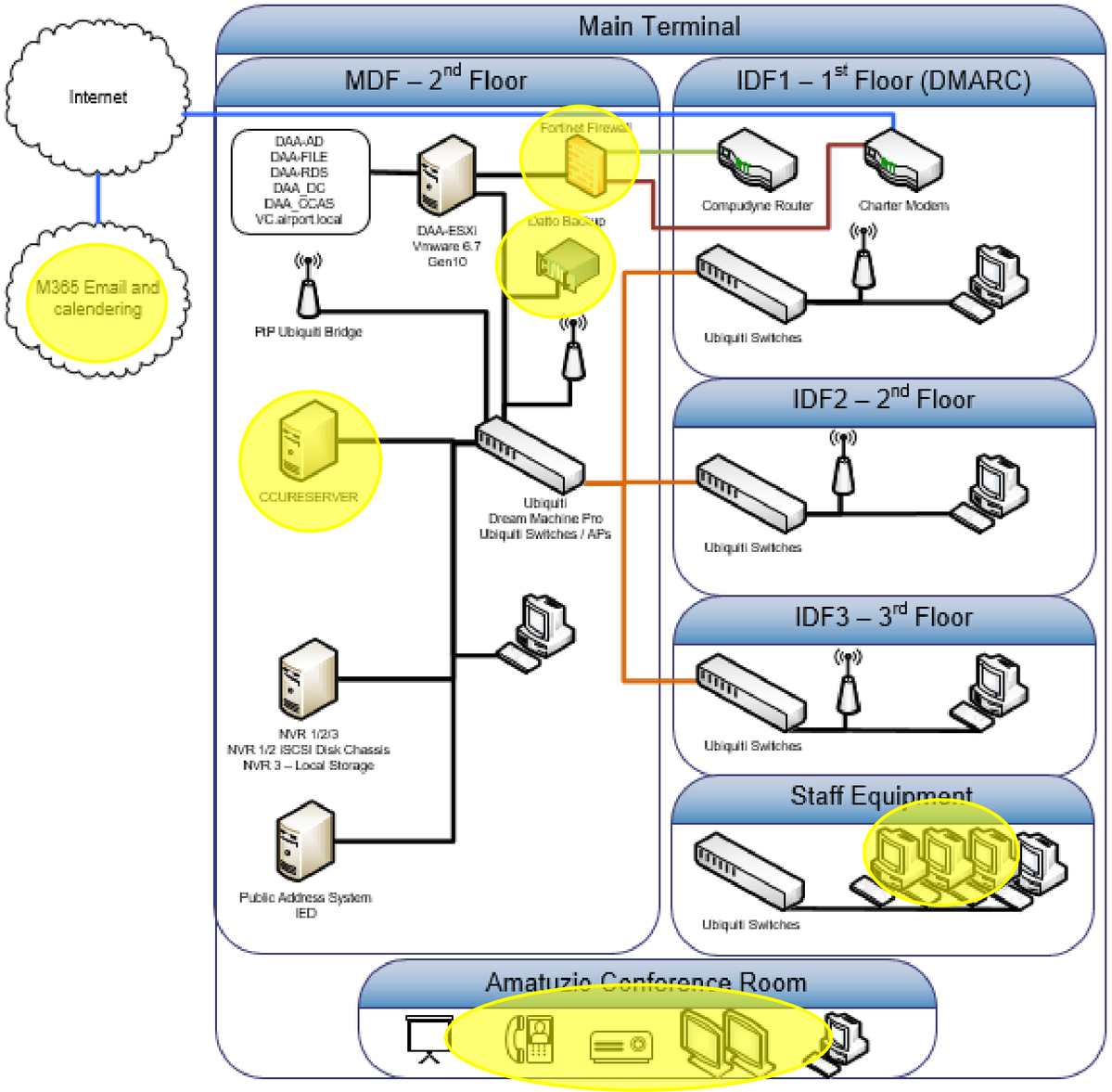
Risk Level	# of Risks	Risk Overview:
Critical	198	Server 2008, unsupport Adobe Flash, unsupport SQL, Windows 7, old versions of Chrome,
High	228	Adobe Reader, Group policy security issues, ILO Vulnerability - firmware update?
Medium	406	Self-signed and weak cipher certificates, security feature bypasses, openSSH, vulnerable webapp, RDS man-in-the-middle
Low	22	ftp clear text, terminal services not FIPS compliant, SSH issues
None	4230	
(blank)		
Grand Total	**5084**	

Initial vulnerability scan showed 854 vulnerabilities in the environment.

Infrastructure Resiliency

Where we are now … (July 2021)

Duluth Airport Authority **AFTER**



- CCure Servers – badging system – Hardware replaced with new equipment and new virtualized server.
- New backup device providing local file restoration and both local and cloud business continuity.
- New, DAA owned firewall installed
- M365 cloud backups implemented
- Aging computers replaced. Laptops now have docking stations so employees can use same computer at home and office – reducing cost of multiple computers per employee.
- New temporary camera and microphone system increases ease and usability of conference room.

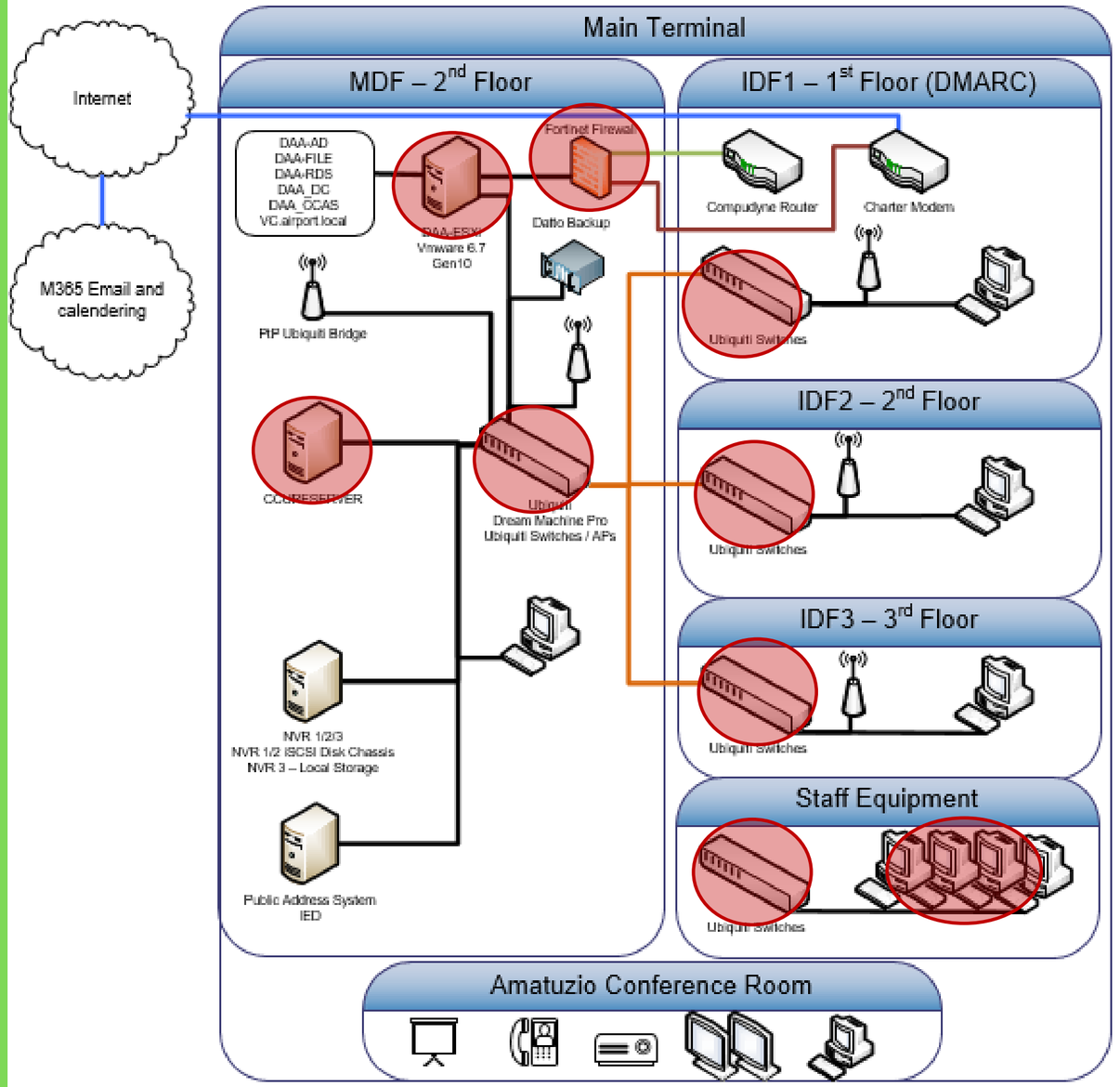
SPECIALIZING IN CREATIVE SOLUTIONS FOR
209 West First Street, Duluth, MN 55802 P 218 720 4435 F 218 722 1231 www.citon.com
Custom Computers + Workstations | Servers + Storage | Network + Wireless Infrastructure
Hosted Email and UC | Layered Enterprise Security | Data Center | Managed IT

Infrastructure Vulnerabilities

Where we are now … (July 2021)

Duluth Airport Authority **AFTER**

Always On:™ CITON COMPUTER CORP



- CCure Servers – new badging system servers are updated, fully patched, and on current, supported software.
- New firewall has web content filtering, intrusion prevention and detection, backups, and logging.
- Main server is patched, updated and maintained.
- Older, insecure accounting server has been archived and shut down.
- Unsupported operating systems on staff computers have been replaced, and systems are patched and updated.
- Switch and wireless equipment has been updated and patched.
- Remote connections to DAA network use secure VPN with MFA, and M365 logins now use MFA.

SPECIALIZING IN CREATIVE SOLUTIONS FOR
209 West First Street, Duluth, MN 55802 P 218 720 4435 F 218 722 1231 www.citon.com
Custom Computers + Workstations | Servers + Storage | Network + Wireless Infrastructure
Hosted Email and UC | Layered Enterprise Security | Data Center | Managed IT

Infrastructure Vulnerabilities

Where we are now … (July 2021)

Duluth Airport Authority
Vulnerability Scan Results and Reccomendations
April 2021

Always On™ CITON COMPUTER CORP

Vulnerability Scan Overview: Scan Date: 2-23-2021

Risk Level	# of Risks	Risk Overview:
Critical	198	Server 2008, unsupport Adobe Flash, unsupport SQL, Windows 7, old versions of Chrome,
High	228	Adobe Reader, Group policy security issues, ILO Vulnerability - firmware update?
Medium	406	Self-signed and weak cipher certificates, security feature bypasses, openSSH, vulnerable webapp, RDS man-in-the-middle
Low	22	ftp clear text, terminal services not FIPS compliant, SSH issues
None	4230	
(blank)		
Grand Total	**5084**	

Of the 854 vulnerabilities initially identified, 739 of them (86%) have been resolved. Remaining are in the process of being resolved.

Policy, Procedure and Process

Where we are now … (July 2021)

- ✓ Created network diagrams
- ✓ Created DAA service overview listing all technology related systems, contractors, contacts and contract information, along with catalog of actual contracts.
- ✓ Implemented Firewall Security Policy
- ✓ Created a data backup and retention policy
- ✓ Revamped and expanded Business Continuity plan
- ✓ Created 5-year IT budget, including capital expenditure plan, monthly services and annual costs.
- ✓ Implemented and deployed real-time dashboard displaying service and project metrics, results of end user satisfaction surveys, and information regarding equipment health, security, performance, and inventory.
- ✓ Revised employee hiring and termination procedures to include technology-related security measures and best practices.

Typical Risk Management Framework

Always On:™
CITON COMPUTER CORP

Ongoing Risk Assessment

Identify Risk

Develop Risk Mitigation Plans

Clear and Concise Risk Visibility

Implement Risk Mitigation Plans

Remediation Tools/Processes

What does comprehensive managed service and cybersecurity look like today?

Managed Support Services from Citon

- 24x7x365 Monitoring & Alerting
- Help Desk Services
- Available Onsite Support
- Backup System Management
- Quarterly Business Reviews
- Firewall Management
- Server & Network Management

- Enhanced Network Monitoring
- Virtual IT Management
- Spam Filtering
- Web Content Filtering
- Anti-Virus / Anti-Ransomware
- Security Policy creation & review
- Multi-Factor Authentication (MFA)
- Vulnerability Scanning

- Security Awareness Training
- Dark Web Scanning
- Endpoint Detection & Response
- Network Detection and Response
- Microsoft Cloud Detection & response
- Windows Drive Encryption
- O365 Backup
- Email Encryption

- MSP 1.0
- Next Gen MSP

Always On:

CITON COMPUTER CORP

Intelligence thru Technology since 1994

It starts with your backup:

Any IT policy requires a best-in-class backup. At Citon we have created a comprehensive backup solution and backup process to protect your data.

Security Table Stakes:

End of Support Operating systems and Firewalls that are "fit for purpose" are fundamental requirements in 2021. Look out for older firewalls and "end of support" operating systems like Windows 7 and Server 2008 which increase security risks.

Summary of Next Generation Services

✓ **24x7x365 Monitoring & Alerting**	Custom solution with Citon built "logic and flow" to monitor & alert.
✓ **Help Desk Services**	Duluth based team of IT Champions, expertly trained to support customer's needs.
✓ **Available Onsite Support**	Rapid Response Team trained and knowledgeable in a huge variety of IT related disciplines.
✓ **Backup System Management**	Backup performance testing and validation.
✓ **Quarterly Business Reviews**	Performance & SLA overview, SWOT summary & technology roadmap.
✓ **Firewall Management**	Firewall tuning and optimization, firmware updates &VPN management.
✓ **Server & Network Management**	Proactive maintenance and patches, uptime maximization.
✓ **Enhanced Network Monitoring**	Robust monitoring platform featuring threshold alerts and automated configuration backup.
✓ **Virtual CIO**	Impact based service that is designed to align IT with corporate goals. Includes, budgeting, security reviews and strategic IT Planning.
✓ **Spam Filtering**	Best in Class spam filtering and message management.
✓ **Web Content Filtering**	Improve security by blocking access to malicious websites. Prevents malware downloads, uses automatic intelligence to perform targeted threat analysis.
✓ **Anti-Virus / Anti-Ransomware**	Leading AV/AR platform. Provides protection via multiple layers of security to protect against botnets, viruses, ransomware, malware & zero-day threats.
✓ **Security Policy Creation & Review**	Best Practice & compliance requires creation and maintenance of a corporate security policy.
✓ **Multi Factor Authentication (MFA)**	MFA maximizes user login security for specific applications which are required for best practices and compliance.
✓ **Vulnerability Scanning**	Broad, deep toolset designed by security professionals. Provides visibility into vulnerabilities.
✓ **Security Awareness Training**	Comprehensive end-user training on how to identify potentially malicious or suspicious email or other requests.
✓ **Dark Web Scanning**	Automated discovery of stolen user account entries from customers domain and available for sale on the dark web.
Endpoint Detection & Response	Managed detection and response. Advanced threat detection, Instant response and remediation
Network Detection & Response	Network detection, threat identification. Monitoring, analysis and reporting. With, or without SOC support
Microsoft Cloud Detection & Response	Managed Security solution for O365, Azure AD, and OneDrive - Google available
Windows Drive Encryption	Full volume disk encryption. Protect data by applying AES, cipher block chaining. Requires Domain and Windows Pro, Edu or Enterprise subscription
✓ **O365 Backup**	Reliably & securely backup Microsoft 365 to ensure critical programs used are protected. Google workspace also available
Email Encryption	Industry standard email encryption for securing transmissions that contain sensitive data

TRUST ALLIANCE℠

CompTIA ISAO Proud Member

www.citon.com

Service by the numbers:

First 5 months

(Feb –June 2021)

Average Response Time	Average Resolution Time	Average User CSAT	# Service tickets and alerts	Workstation Health	Server Health
29.26 minutes	**2.75** hours	**4.0** Out of 4	**173**	**97%**	**94%**

What is coming next for the Duluth Airport Authority?

- ✓ Add SIEM (Security Information and Event Management) to firewall at minimum, with 24x7 SOC (Security Operations Center)
- ✓ Replace existing Wireless Internet service that is not properly secured to roof, with fiber Internet that is more resilient and faster speeds.
- ✓ Discuss overall organizational security and create corporate Security Policy
- ✓ Re-run vulnerability scan
- ✓ Review additional cybersecurity precautions;
  - ✓ Endpoint Detection and Response
  - ✓ Cloud Detection and Response
  - ✓ Hard drive encryption
  - ✓ Email encryption

Q&A