Boosting Security Through MFA, O365, and Vulnerability Fixes

Enhancing security, efficiency, and resilience across the organization

Client Snapshot

NASCO-OP is a member-owned non-profit serving as an exclusive purchasing cooperative for the North American recycling industry. Founded in 1959 and headquartered in New Philadelphia, Ohio, the organization provides high-quality recycling products and supplies from leading manufacturers at competitive prices to its members.

Testimonial

> *"It's been a pleasure working with you. I'm very pleased with the initial risk assessment earlier this year, and the completion of these 3 projects. I actually sleep a little more soundly now that our security is tightened"*
>
> **-Gabe Lawrence**
> **IT Manager**

THE CHALLENGE: RISING SECURITY THREATS

NASCO-OP needed to reduce its cybersecurity risk and improve its overall security infrastructure. To identify where improvements were needed, they requested a network security assessment.

- **Cybersecurity Risk:** Existing systems required improvements to better protect against potential threats.
- **Need for Security Assessment:** Gaps in the network were not fully visible without a formal review.
- **Maintaining Business Continuity:** Security improvements had to be implemented without disrupting daily operations.
- **Strengthening Processes:** Existing procedures needed updating to enhance overall protection.

PROJECT GOALS

- ✓ Reduce cybersecurity risk and protect the organization's critical systems.
- ✓ Strengthen security infrastructure and overall protection.
- ✓ Identify vulnerabilities to understand where improvements are needed.
- ✓ Ensure improvements support business continuity without disruption.

VELONEX TECHNOLOGIES

☎ 800-245-5210

🌐 www.velonexit.com

✉ contact@velonexit.com

Boosting Security Through MFA, O365, and Vulnerability Fixes

Enhancing security, efficiency, and resilience across the organization

SOLUTIONS OVERVIEW

The project focused on improving NASCO-OP's cybersecurity posture and reducing their attack surface. Velonex Technologies worked closely with the client to assess vulnerabilities, implement security improvements, and remediate critical issues without disrupting business operations.

The project included:

- **Network Security Assessment**: Conducted an in-depth review of policies, LAN, workstations, networking equipment, router/firewall, mobile devices, data, remote access, email, and physical security.
- **Microsoft 365 Security Improvements:** Created policies, enabled application security features, improved identity and email security, and upgraded users to modern authentication.
- **Multi-Factor Authentication (MFA) Implementation:** Reviewed requirements with the client, enabled MFA on applications, and tested logins for administrators and standard users.
- **High-Severity Security Issue Remediation**: Addressed critical vulnerabilities, disabled weak ciphers and protocols, coordinated software updates with vendors, and verified all systems and user access post-implementation.

KEY WORKFLOWS IMPLEMENTED

Security Assessment Workflow

Reviewed existing policies, network infrastructure, devices, email, remote access, and physical security to identify vulnerabilities.

Microsoft 365 Security Workflow

Created and applied security policies, enabled application protections, and transitioned users to modern authentication.

Multi-Factor Authentication (MFA)

Configured MFA for applications, tested logins for administrators and standard users, and verified proper prompts.

Vulnerability Remediation

Addressed critical security issues, disabled weak protocols, applied software updates, and confirmed system and user functionality post-implementation.

Results

- Stronger cybersecurity
- Safer user access
- Streamlined security workflows
- Uninterrupted business operations