

# Zero Trust Implementation Case Study: Enhancing Security for a Leading Manufacturing Firm

This case study examines how CG Technologies successfully implemented a Zero Trust security model for a mid-sized manufacturing company in the Greater Toronto Area, addressing critical security vulnerabilities and compliance challenges in just four weeks.

# Client Overview and Challenges

## About the Client

A mid-sized manufacturing company operating in a highly competitive and regulated industry within the Greater Toronto Area. The organization needed to modernize its IT security posture to respond effectively to increasing cyber threats and evolving compliance requirements in the manufacturing sector.

## Key Challenges

- Limited visibility and control over devices accessing the corporate network
- Manual endpoint management processes creating operational inefficiencies
- Security vulnerabilities stemming from outdated policies and infrastructure
- Inconsistent compliance and access control in a hybrid Active Directory environment

These security gaps exposed the organization to significant risks of data breaches and compliance violations, potentially impacting both operations and reputation in the manufacturing industry.



# Project Goals and Solution Approach

## Primary Objectives

- Strengthen overall cybersecurity posture across the organization
- Gain comprehensive visibility and control over all network endpoints
- Implement automated security management systems
- Ensure regulatory compliance in manufacturing operations

## Solution Framework

- Zero Trust security model implementation
- Microsoft Endpoint Manager and Intune deployment
- Hybrid Active Directory integration and optimization
- Custom security policy development and enforcement

## Implementation Timeline

The project was executed over a condensed four-week period, with careful planning to minimize disruption to manufacturing operations while maximizing security improvements. The timeline included assessment, implementation, testing, and training phases to ensure comprehensive adoption.

# Implementation Strategy and Components



## Zero Trust Model Deployment

Implemented the "never trust, always verify" approach across all network access points, requiring continuous authentication regardless of user location or device.



## Endpoint Management Integration

Deployed Microsoft Endpoint Manager with Intune to establish centralized visibility and control over all devices accessing corporate resources.



## Access Policy Development

Created granular role-based access controls and conditional access policies tailored to the manufacturing environment's specific operational requirements.



## User Training and Change Management

Conducted comprehensive training sessions to ensure smooth adoption and minimize resistance to new security protocols.

The implementation focused on balancing robust security with the practical needs of a manufacturing environment, where operational continuity and efficiency remain critical priorities.



# Challenges Overcome During Implementation

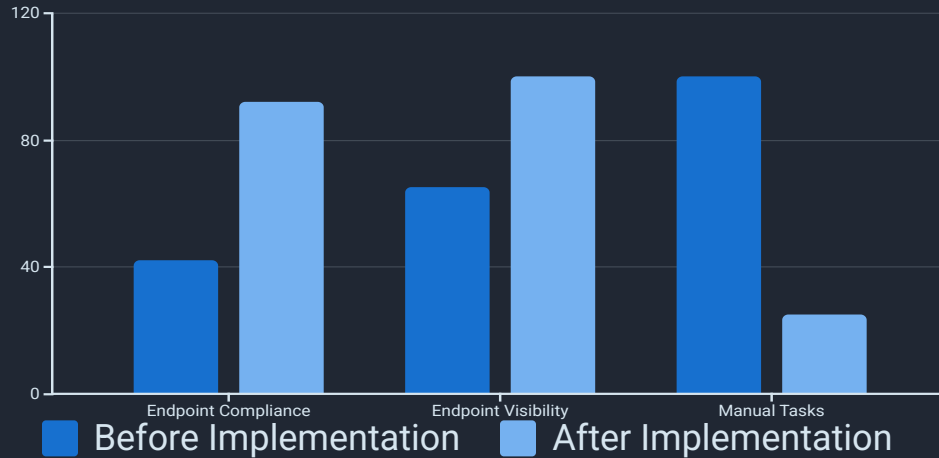
While the overall project proceeded smoothly, the CG Technologies team encountered significant compliance issues with a segment of legacy endpoints used in the manufacturing environment. These older systems, critical to specific production processes, were incompatible with modern security protocols but couldn't be immediately decommissioned.

To address this challenge, the team developed a phased replacement strategy for non-compliant devices, implementing temporary isolation measures to secure these endpoints while maintaining production capabilities. This approach ensured continuous operations while systematically upgrading the security infrastructure across all manufacturing systems.

The successful resolution demonstrated CG Technologies' ability to adapt security implementations to the unique constraints of manufacturing environments where legacy industrial systems are common.



# Measurable Outcomes and Benefits



## Key Performance Improvements

- **52% increase** in endpoint policy compliance within 2 weeks
- **100% endpoint visibility** through centralized monitoring
- **74% reduction** in manual endpoint configuration tasks
- Significantly improved threat detection times
- Enhanced regulatory compliance posture

Executive leadership reported increased confidence in their IT environment's integrity and resilience against modern cyber threats targeting manufacturing operations.

# Lessons Learned and Best Practices



## Hardware Assessment is Critical

Legacy manufacturing hardware can significantly impede security initiatives and must be thoroughly assessed early in the planning phase to develop appropriate migration or isolation strategies.



## User Education Drives Success

The success of Zero Trust models in manufacturing environments depends heavily on aligning technical implementation with comprehensive user awareness and change management programs.



## Hybrid Environment Considerations

Manufacturing environments with hybrid AD infrastructures require particularly careful planning to balance cloud-native security tools with existing on-premises infrastructure without disrupting operations.



## Industry-Specific Adaptation

Security frameworks must be adapted to address unique manufacturing requirements, including operational technology (OT) networks and industrial control systems that may interface with IT infrastructure.



# About CG Technologies



With over 30 years of experience, CG Technologies has established itself as a trusted IT managed services provider in Toronto, specializing in secure, scalable, and tailored IT solutions for businesses across all industries, with particular expertise in manufacturing environments.

Our proactive approach to technology management ensures client infrastructures are not only supported but positioned for growth and resilience against evolving threats.

Interested in similar results for your manufacturing organization? Contact CG Technologies today to discover how our team can help strengthen your security posture and future-proof your IT environment.

**[cgtechnologies.com](https://cgtechnologies.com)** | [sales@cgtechnologies.com](mailto:sales@cgtechnologies.com)