Case Study: Enhancing Security with Zero Trust at a Manufacturing Company

Client: Manufacturing Industry

Timeline: 4 Weeks

Solution: Zero Trust Security Implementation with Microsoft Endpoint Manager

M by Matthew Goodchild

Client’s Challenges and Solution Provided

The manufacturing client had several security vulnerabilities and challenges, including:

- Lack of Control and Visibility: The client struggled with a lack of centralized control and visibility over their IT infrastructure, making it difficult to monitor and manage systems effectively.
- Inconsistent Automation: The absence of automated processes meant that security measures were not as responsive and proactive as needed.
- Security Concerns: The primary concern was their outdated security measures, which left the organization exposed to potential breaches and compliance issues.

CG Technologies implemented a comprehensive Zero Trust Security Model to enhance the client’s security posture. This solution involved:

- Microsoft Endpoint Manager & Intune Integration: In a hybrid Active Directory (AD) environment, CG Technologies deployed Microsoft Endpoint Manager with Intune to provide centralized management, monitoring, and security enforcement across all devices and endpoints.
- Custom Security Policies: To address the client’s unique needs, CG Technologies designed specific security policies that met their operational and compliance requirements.
- Hybrid AD Security Enhancement: The solution ensured that even devices outside the corporate network were securely managed, meeting the needs of a dynamic, mobile workforce.
- Microsoft Cloud Services for Zero Trust: Utilizing Microsoft’s cloud services, CG Technologies followed the Zero Trust security framework, ensuring continuous authentication, least-privilege access, and end-to-end encryption across all user interactions and devices.

Challenges Overcome, Project Outcomes, and Lessons Learned

Challenges Overcome:

- Endpoint Non-Compliance: During the deployment, some endpoints did not comply with the security policies set by the system.
- Solution: CG Technologies quickly replaced non-compliant endpoints and ensured all devices adhered to the security protocols.

Project Outcomes:

- Enhanced Security Posture: The client now enjoys a robust security environment with controlled access and continuous monitoring, minimizing the risk of security breaches.
- Peace of Mind & Compliance: With the implementation of the Zero Trust model, the client gained confidence that their data and systems were secure. The solution also ensured compliance with industry standards.
- Improved Efficiency: By automating security processes and policies, the client has reduced manual intervention, allowing internal teams to focus on more strategic tasks.

Key Metrics:

- Reduced Risk: Significant reduction in the risk of breaches and unauthorized access.
- Increased Compliance: Improved adherence to regulatory and security compliance standards.
- Cost Savings: A reduction in security-related incidents, leading to lower potential costs associated with breaches.

Lessons Learned:

- Adaptability to Endpoint Challenges: The need for flexibility when endpoints fail to comply highlighted the importance of proactive measures in ensuring all devices are secure from the outset.
- Custom Security Needs: Tailoring security solutions to the client's specific operational environment was critical in ensuring the solution met both technical and business requirements.

> "CG Technologies transformed our security infrastructure. Their Zero Trust solution gave us the confidence to focus on growing our business, knowing that our systems are secure. Their team's ability to quickly address and resolve endpoint issues ensured that the project was delivered on time and within budget." — Client, Manufacturing Industry