THE MILLER GROUP
TECHNOLOGY SOLUTIONS

Solutions & Success
The Inside Story

The Miller Group Ranks 5/5 Stars For Critical Cybersecurity Project

www.themillergroup.com

The development and maintenance of Security Policies is an integral part of any business' cybersecurity posture.

Security policies set the standard for the implementation of all controls associated with managing the risk associated with an organization's cybersecurity plan.

This is especially important when it comes to managing cybersecurity in the cloud. The way your data is protected is of the utmost importance when it can, in theory, be accessed from any Internet-connected device.

This is precisely why this manufacturing firm got in touch with The Miller Group.

The Problem

According to the Cloud Security Firm RedLock and its Cloud Security Trends report, more than 50% of businesses that use cloud services have unintentionally exposed at least one of these services to the public.

This growing trend of unsecured cloud configurations is due to businesses neglecting known vulnerabilities in the cloud, or failing to properly assess their cloud environment to discover unseen security risks.

That's why this manufacturing firm enlisted our expert support. They needed to make their Azure Active Directory (AAD) infrastructure match the security policies that are in place in their local Active Directory.

The Solution

To manage this project, we carefully developed a plan to implement Intune Mobile Device Management and related security policies.

This ensures that company devices already enrolled in AAD will automatically have these new policies applied. We also added Defender for Business to provide spam and virus filtering for all incoming emails at the firm.

The policies in place were based on our previous recommendations to the firm:

- Require MFA authentication for all users
- Limit the number of Global Admin accounts
- Block legacy authentication
- Deploy Windows Hello for Business
- Control who can create new Microsoft Teams accounts
- Configure their OneDrive sync client to automatically sign in using the computer login credentials and silently move Windows known folders to OneDrive
- After a timed-out session, force a screen saver and require a password lock
- Remove admin rights to prevent users from changing these settings
- Disable Autoplay
- Require all enrolled devices to have active antivirus

The Result

As a result of this project, this manufacturing firm's AAD infrastructure now matches our range of cybersecurity best practices. Their users can now work more securely, with the confidence that company data is not being put at risk.

"It is a pleasure to work with the TMG team," says Sherman, a member of the firm's staff.

Our expert team carried out the project on time and according to plan, which is why this firm's staff rated our service 5/5 stars.