Strategies to Secure the Hybrid Workforce and Power Collaboration

Hybrid work has become a fixture of today's workplace. A recent study suggests that nearly one third of companies allow hybrid work, while another third have remained 100 percent remote. Remote collaboration has been shown to increase productivity and worker satisfaction. However, the need to secure the hybrid workforce presents challenges.

In a traditional office setting, IT departments have significant control over both the network and the devices that connect to it. However, outside the corporate security umbrella, devices may miss essential updates, as well as critical maintenance and monitoring. Additionally, while the cloud simplifies collaboration, it also expands the attack surface and introduces new risks.

To protect against cyber attack and keep data safe in a hybrid setting, organizations need to revisit their cyber security strategies. This begins with a renewed commitment to cyber security best practices. Beyond basic security, companies should move toward a zero trust approach, revisit security policies and educate their users.

Start with Basic Cyber Security to Secure the Hybrid Workforce

While tools continue to evolve, several basic principles of cyber security become even more important in a hybrid work environment. These include:

- Encryption – The organization shares responsibility for encryption with the cloud provider. Talk with your cloud provider to ensure encryption of your data both in transit and at rest. Highly sensitive data may require more sophisticated encryption methods.
- Patching – Review your organization's patch management strategies to make sure that patches to software and firmware are applied quickly. With thousands of applications and devices, this can prove challenging. Automate patching where possible. Your managed services provider (MSP) can help.
- Backups – While systems like Microsoft 365 include data protection features, these built-in features have limitations. Implement a comprehensive, automated data backup and restore plan.
- Risk assessments and pen testing – Regular risk assessments and penetration testing highlight security vulnerabilities in the organization. Use this information as the foundation for designing a security strategy.

Strengthen Access Management with Zero Trust and Least Privilege

The prevalence of cloud collaboration has made zero trust security an imperative. Because hybrid work stretches far beyond traditional boundaries, this "never trust, always verify" approach requires authentication for every transaction. As a key component of zero trust, implementing MFA should rank high on the organization's security priority list.

While zero trust emphasizes verifying identity for every access request, the principle of least privilege minimizes risk by limiting access. That is, a user should have only the access they need to complete their job. Tools such as Azure AD allow the security team to enforce conditional access based on the user's role, location, device, and other factors.

Automate Security Policies

To strengthen and protect hybrid work, organizations should take time to update cyber security policies. These include policies governing data access, passwords, data retention, encryption and other actions that determine how data is created, shared, and stored. They also include BYOD policies governing the devices used to access company data and services.

Automating security policies improves security by reducing dependance on workers to remember and apply critical security controls. For instance, organizations can tag sensitive data and apply sharing restrictions, encryption or data retention policies according to data classification.

Build a Security Aware Workforce

Successful hybrid work requires employees that understand their role in keeping data secure. Targeted, engaging security awareness training can change employee behavior. Combining regular training with phishing simulations significantly improves the organization's ability to withstand common cyber threats.

Essential Partnerships Pave the Way to Secure Collaboration

Hybrid work has opened the door to unprecedented opportunities for collaboration. But the many benefits of collaborating in the cloud come with increased security risk. Addressing that risk requires new skills and tools that many organizations do not yet have. Fortunately, MSPs help fill the skills gap with deep expertise and cutting-edge tools to match the risks.

For example, the cyber security consultants at eMazzanti will help your organization navigate the powerful but complex security controls in Microsoft 365. In addition to consulting on access management and policy automation, they can help educate your users and implement tools such as MFA and cloud backups.