Overcome Hybrid Workforce Cyber Security Challenges with Multi-layered Approach

According to several recent studies, the majority of workplaces in the United States support a hybrid workforce. While this model has been shown to increase productivity and promote a better work-life balance, it does present challenges. As the nature of work continues to evolve, companies need to adjust their hybrid workforce cyber security to protect vital business assets.

Hybrid Workforce Cyber Security Challenges

Even as the world moves out of pandemic mode, the nature of work has changed in fundamental ways. While the number of fully remote employees continues to drop, many companies remain committed to hybrid work for the foreseeable future. This means that organizations must address the ongoing challenges of securing that workforce.

These challenges include:

- Expanded attack surfaces – Remote workers use different devices, networks, and applications to access corporate data and systems, which increases the number of potential entry points for hackers.
- Unsecured and vulnerable hardware – Along with remote work comes an increase in the number of employees using personal devices outside the control of IT. In many cases, these

devices have not been properly secured or updated with the latest patches and antivirus software.

- Lack of security talent – The cyber security skills gap continues to grow. With a global workforce shortage of 3.4 million people, companies lack sufficient in-house security expertise. At the same time, remote work has caused a substantial increase in support requests and cyber risk.

- Susceptibility to phishing attacks – With more distractions and less access to security resources, remote workers prove more likely to fall victim to phishing attacks.
- Poor data practices and procedures – Remote workers often store, transfer, or dispose of data in insecure ways. This includes using unencrypted USB drives, sending sensitive data through email, or using shadow IT.
- Disconnected security solutions – The average SMB uses at least four different tools for vulnerability management. Security teams find it difficult to keep up with product management and security logs. And lack of integration among the solutions means tech personnel have insufficient context and analytics to pinpoint indicators of compromise.

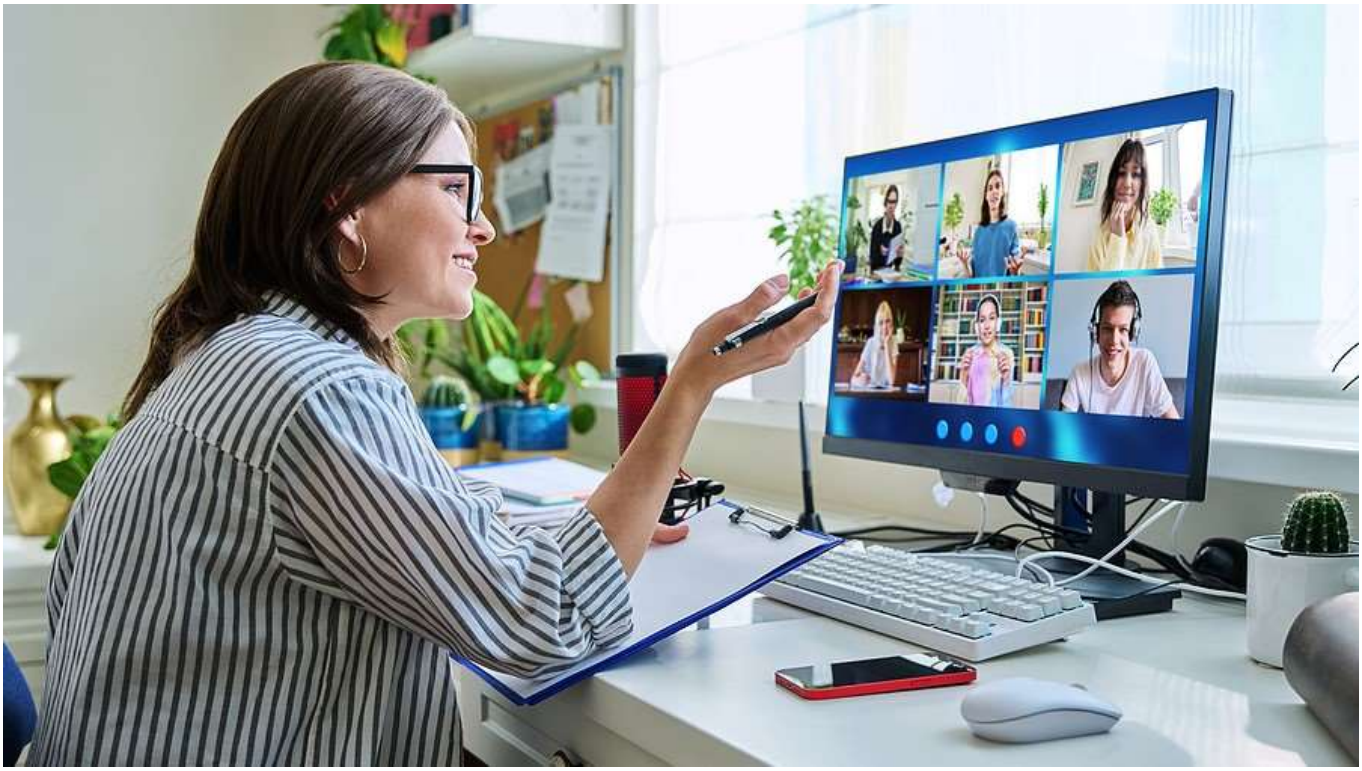
Common Attack Vectors

The prevalence of remote work has changed the nature of the cyber battle ground. As more data and applications move to the cloud, traditional network security models based on static perimeters and zones of trust become obsolete and ineffective.

Attackers have become adept at operating in this environment. Knowing the most common attack vectors will help organizations build their defenses accordingly.

Compromised credentials and social engineering top the list of typical attacks. This includes phishing and business email compromise (BEC). Hackers will also frequently exploit vulnerabilities in third-party software. And they will find entry points to insert ransomware and other malware.

To counter these threats and strengthen hybrid workforce cyber security, organizations need to take a multi-layer approach. This includes tools from multi-factor authentication (MFA) to endpoint protection, improved email security and more. To defend against targeted and sophisticated attacks, a zero-trust strategy proves essential.



Zero Trust Network Access

In the zero trust model, organizations address risk by taking a "never trust, always verify" approach to extending access. With effective zero trust, the system grants access to services based on contextual factors from the user and their device. Trust is established when a service or resource is accessed, and revoked when the access is no longer needed or authorized.

One of the key enablers of zero trust is micro-segmentation. This technique allows organizations to isolate and protect their workloads at a granular level. For instance, micro-segmentation could address a cloud-based application such as a CRM, isolating sensitive workloads such as financial information or customer data.

In the CRM example, sales and technical support likely require broad access in certain circumstances, while engineering teams will require less. Security policies can even restrict access based on factors such as the location of the device requesting access.

Partner with Security Experts

Defending your organization against today's sophisticated threats does not necessarily require costly, bleeding-edge security tools. The cyber security experts at eMazzanti will help you choose and appropriately deploy a comprehensive security strategy targeted to your business needs.

Begin by blocking known threats and preventing unauthorized access with MFA, endpoint protection and network firewalls. Take a step further with phishing protection, email filtering, risk-based authentication and advanced anti-malware. Or enhance your security posture with zero trust. Whichever security tier you choose, eMazzanti has the expertise you need.