# 5 Endpoint Security Best Practices that Provide Security When Remote Work Takes Center Stage

With the majority of employees working from home this spring, organizations have encountered new challenges. The increased burden on corporate networks can result in diminished performance and productivity. More important, remote connections increase the security risk. Endpoint security best practices help to mitigate that risk and protect the organization.

Endpoints include any devices that connect to the network. Every connection represents a possible point of access for cyber criminals. Endpoint security, therefore, acts as the front line of cyber security for the organization. An effective endpoint security solution uses a multi-faceted approach to detect and minimize threats and control system access.

## Mobile Workforce Broadens Attack Surface

In recent years, remote work has become the norm. Even before COVID-19 sent the bulk of the workforce home, end users regularly conducted business via mobile device. As a result, the network perimeter has largely disappeared. Consequently, traditional centralized security no longer provides adequate protection for the mobile workforce on its own.

In addition to company-owned devices, many organizations have instituted bring-your-own-device (BYOD) policies. And as employees use personal phones and tablets to connect to enterprise systems, security teams struggle to manage access.

The explosion in privacy regulations since GDPR took effect in 2018 has further complicated the security environment. To achieve compliance, organizations need to demonstrate that they have

secured mobile data. That can prove extremely challenging with data traveling to and from thousands of devices.

With such a wide attack surface, organizations need to employ endpoint security best practices to keep sensitive data safe. Here are a few of those best practices to consider.

## 1. Invest in Mobile Device Management

With so many devices connecting to the network, IT departments turn to mobile device management (MDM) systems to manage device-level security. MDM determines which devices can access the network and enforces policies. It manages encryption, monitors for security and regulatory compliance and provides for remote wiping of a lost or stolen device.

For instance, with MDM, organizations can require that mobile devices meet specific security standards before being allowed network access. They can also enforce acceptable use policies determining application access and block risky activities.

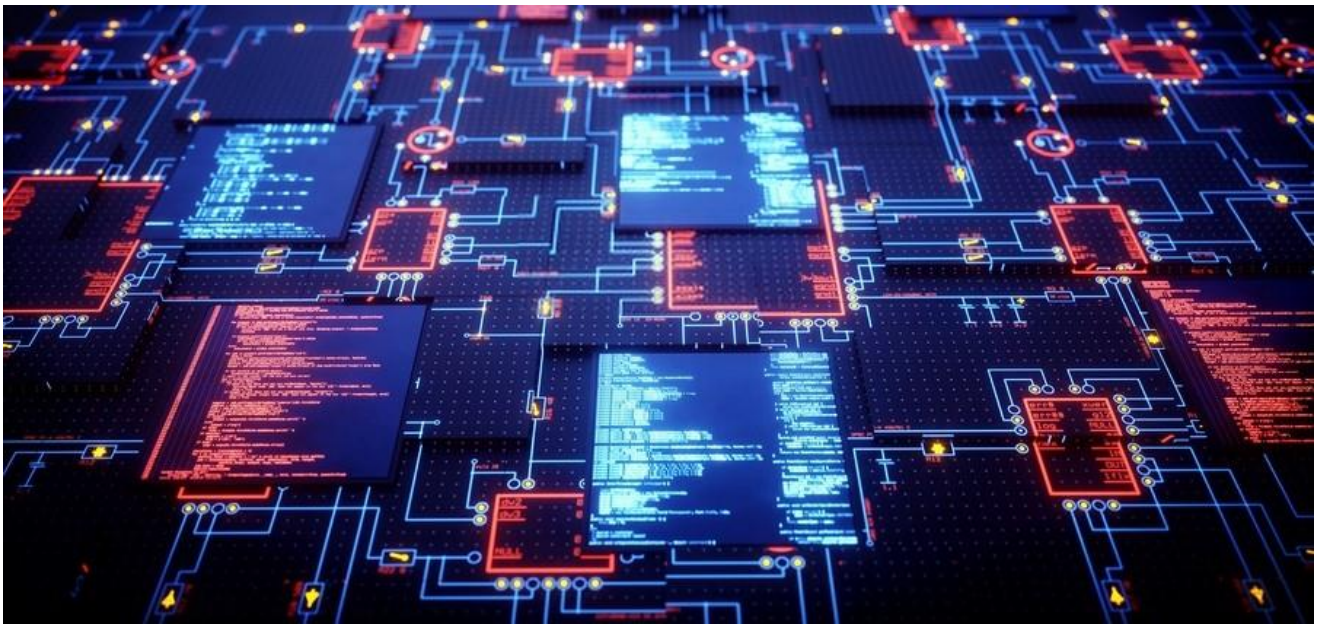
## 2. Implement Application Control

With application control, organizations gain visibility into and control over the applications in use across the enterprise. They can whitelist trusted applications and/or blacklist applications that may prove a risk to the organization. This not only helps keep the system secure, but it also facilitates data discovery for purposes of regulatory compliance.

## 3. Strengthen Access Management

Take a layered approach to access management. Start with automatically enforcing strong password policies. Then bolster defenses with multi-factor authentication (MFA). To achieve a balance between security and usability, define access based on risk.

For instance, system administration activities present greater risk, as do connections from certain locations. Define risk-based access that requires MFA for these and other higher risk activities.



## 4. Stay Up to date

Out-of-date devices and applications increase the likelihood of attack, and not all mobile devices receive updates in a timely manner. Put policies in place to ensure that patches get applied quickly. In particular, make sure that antivirus, antimalware and firewalls stay up-to-date. An anti-virus last updated two months ago provides little protection from this week's threats.

## 5. Double Your Protection with EPP and EDR

Endpoint protection platform (EPP) solutions work to prevent known attacks, such as malware and ransomware. On the other hand, endpoint detection and response (EDR) solutions work to discover and respond to attacks that slip past the defenses.

Even with updated antivirus, breaches will happen. A good EDR solution monitors endpoints for unusual behavior and helps the organization to stop zero-day attacks in their tracks. By using EPP and EDR in tandem, organizations benefit from breach prevention, detection and remediation.

## Implement Endpoint Security Best Practices

Businesses of all sizes have moved into a mobile-first environment without much preparation. Navigating security challenges with a vastly increased security perimeter can prove a daunting task. Contact eMazzanti Technologies today to prioritize and implement endpoint security best practices for your organization.