A better approach to **telework security**

Privileged access management and cloud-based security are essential for protecting a remote workforce

Morey J. Haber
CTO and CISO, BeyondTrust

THE CORONAVIRUS PANDEMIC quickly prompted the transition to telework. However, remote working may remain the new reality for many agencies long after the threat of the virus has subsided.

This large-scale shift to working from home introduces interesting challenges for government agencies. How do they secure a growing number of remote devices while keeping employees productive? How do they enforce least privilege while allowing end users to perform necessary tasks? How do agencies secure devices, access and systems when the network perimeter has been stretched to support large numbers of remote workers?

Some IT leaders have committed to VPNs or remote desktop access, both of which can be difficult to secure and scale. Devices are still at risk when they're not connected to the VPN or remote access technology because of vulnerabilities in the home network. For example, agencies can't protect against a family member or housemate using an employee's home computer. They may also not be able to enforce whether or not basic software, such as antivirus or OS, is up-to-date on a personal device.

The situation fundamentally requires a shift to the cloud. Cloud-based tools can monitor a managed resource more effectively in all environments. With that always-on approach to security, IT administrators can see and respond to potential threats in real time as they arise.

The most basic form of privileged access management involves storing credentials in a vault. Today, that's only a partial solution at best. People need privileged access for applications, databases, remote support and managing resources in the cloud or even on social media. How do you secure privileged access when those users are not in a government building?

The best approach accomplishes three primary goals:

1. Secure privileged accounts and credentials by adding a layer of complexity, never exposing the password to the user and rotating credentials after each use.

2. Enforce least privilege and ensure every identity, endpoint and session only have the precise privileges needed for the finite duration of time needed to perform an authorized activity. (BeyondTrust's 2020 Microsoft Vulnerabilities Report found that removing admin rights would mitigate 77% of all critical Microsoft vulnerabilities in 2019.)

3. Secure the remote access pathways that connect to the corporate network. This includes granular control of privileges and complete session monitoring and auditing.

To protect and empower this changing work environment, agencies should avoid inappropriately vetted cybersecurity and remote access tools, which are almost never enterprise-grade and tend to only introduce additional security vulnerabilities and backdoors. Instead, agencies should rely on solutions from trusted vendors that understand the challenges facing government agencies and are certified against the appropriate security controls. ■

Morey J. Haber is CTO and chief information security officer at BeyondTrust.