The key to securing **cloud resources**

As adversaries increasingly target IT administrators, privileged access management rises to the challenge

David McNeely
Chief Strategy Officer, Centrify

THE RECENT SURGE IN TELEWORK affects the vast majority of government employees, including IT teams. But it is a challenge to manage and secure servers and other infrastructure located inside agency data centers without being able to physically access those resources.

Given the restrictions on sending employees into government offices, many agencies are accelerating their move to cloud-based infrastructures, which essentially transfers the responsibility for physically managing servers to the cloud platform providers.

Moving to the cloud is a logical and essential step toward enabling remote IT employees to gain access to systems and data, but it also expands the systems an agency must manage and heightens the need to control access to them.

Guarding the keys to agency resources

At the same time that the number of systems that the IT team needs to log into is expanding, adversaries are increasing their efforts to breach government systems by phishing account information from authorized users.

That's because it's easier to steal a key to unlock a door than pick the lock. Adversaries try to convince IT team members to open a malicious email message or go to a website that infects the computer with malware and allows the adversary to compromise that user's credentials. Once inside the network, adversaries can go wherever that valid account is authorized to go.

Many agencies are moving to privileged access management products as the main method of controlling IT-level access to their systems because those tools are specifically designed to protect against that type of threat. Privileged access management focuses on securing and managing IT professionals' access to the inner workings of an agency's IT resources.

Rigorous enforcement on-premises and in the cloud

For cloud-based infrastructures, agencies need to make sure they are enforcing the same strong access controls they use for on-premises systems. For example, if an agency is required to use Personal Identity Verification cards for authentication, then those cards and any other security controls must be part of the process for authenticating IT users for access to cloud platforms and the applications that are being hosted on them.

Also, in an ideal setup, IT team members should only have access to the systems they need in order to do their jobs. In other words, they should be granted the least amount of privileges.

Agencies must deploy strong authentication and privileged access management to ensure that only authorized users have access to the systems that power their missions, whether those systems are on-premises or in the cloud. ■

David McNeely is chief strategy officer at Centrify.