CYBERARK | UBERETHER IAM ADVANTAGE PARTNER

The power of privileged access management

Privileged credentials are essential to agency operations but need special protection from attackers

James Imanian | CyberArk

Adversaries are always evolving and innovating, with recent developments including the theft of post-authorization cookies or access tokens. Industry is also innovating to provide controls that can keep adversaries from entering networks that way. But beyond having the appropriate controls in place, agencies need to shift their emphasis from trying to keep bad actors out because they may already be in. And attackers can do the most damage when they compromise a privileged credential.

Assuming a network has already been breached is a core tenet of zero trust, and privileged access management is a foundational element of such an approach. By limiting the exposure of privileged credentials, agencies can improve their ability to detect credential theft and block an attacker's lateral movement within government networks.

Automating workflows and orchestrating security actions

A privileged access management solution like CyberArk's can both send and receive signals from security policy enforcement points to help a zero trust solution make decisions about access. Agencies can rotate important passwords and even record and analyze privileged sessions if necessary. In addition, privileged access management can support agencies' efforts to automate workflows and orchestrate actions to achieve desired outcomes. Such tools can greatly reduce manual efforts and event reaction times while reducing costs.

An identity and access management solution should be integrated into an ecosystem that can deal with both human and machine identities. Our research has shown that the average organization has 45 machine identities to every human identity. Therefore, even a small organization with 1,000 employees may have 45,000 machine identities to manage and secure.

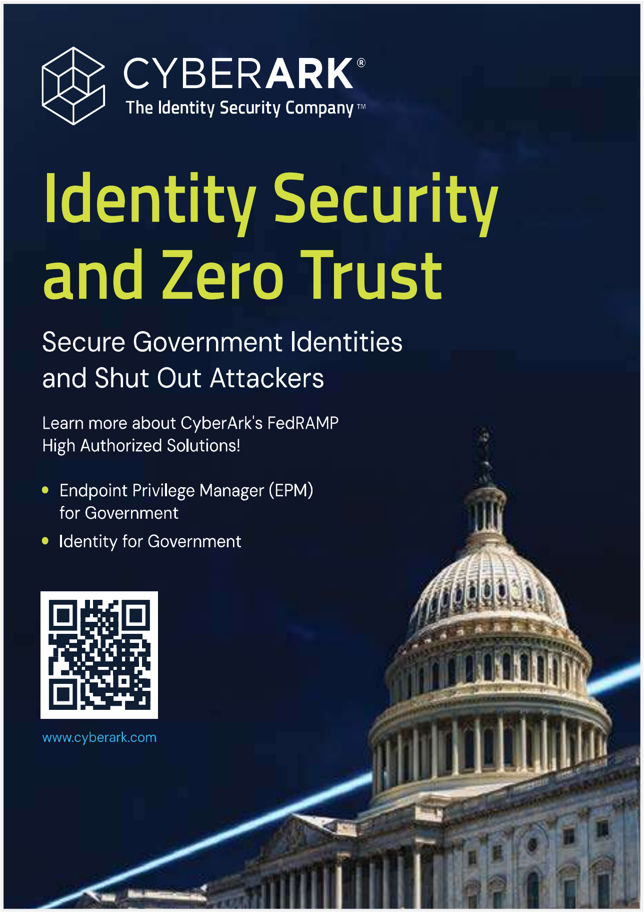
UberEther's IAM Advantage stack is a comprehensive, scalable zero trust solution, and CyberArk is a proud partner in that effort. IAM Advantage allows for multifactor authentication and role-based access. As agencies advance in their zero trust journeys, they can add just-in-time and just-enough access functions. Furthermore, IAM Advantage incorporates privileged session management, data encryption and key management for both human and machine identities on the network.

Enabling threat detection and response

Most attackers these days don't break into networks. They sign in with a compromised credential. That's why it's vital to integrate identity and access management into a security stack like IAM Advantage that can detect threats and enable organizations to respond appropriately with automated workflows and orchestration of their tools.

A zero trust architecture integrates the best security policies, practices and technologies and is most effective when leveraging privileged access management. With CyberArk and IAM Advantage, agencies can prevent attackers from using privileged credentials to access government networks. This greatly increases the probability of agencies successfully executing their missions.

James Imanian is senior director of the U.S. Federal Technology Office at CyberArk.


CYBERARK®
The Identity Security Company™
Identity Security and Zero Trust
Secure Government Identities and Shut Out Attackers
Learn more about CyberArk's FedRAMP High Authorized Solutions!
• Endpoint Privilege Manager (EPM) for Government
• Identity for Government
www.cyberark.com