Manage Privileges Securely with Universal Privilege Management

With more people working from home, innocent mistakes can be damaging.

In 2019, government and military agencies experienced 83 data breach incidents, exposing more than three million sensitive records. While those kinds of numbers probably don't surprise some, it might be less obvious what many of these data loss incidents have in common: the abuse of privileged credentials. According to Forrester Research, 80 percent of data breaches are connected in some way to compromised privileged credentials, such as passwords, tokens, keys, and certificates.

Privileged credentials for various types of IT administrators provide elevated access and permissions across accounts, applications, and systems. In many ways, however, all users with access to government applications and data have privileged credentials, especially while they are actively accessing government resources. When these credentials are abused, hackers can have free rein to move laterally within the environment, stealing data, changing settings, and doing damage.

The growth of privileged credential abuse over the past several years is startling, but it shouldn't be surprising. For federal agencies, much has changed. The pace of cloud adoption has increased significantly. New cloud instances can be easily spun up, creating new privileged identities that need to be onboarded and managed. While cloud computing provides many benefits, it can reduce network visibility, obscure perimeters, and make it more difficult to manage policies and enforce least privilege.

There are also millions of endpoint devices accessing these systems, due to both the growth of bring your own device (BYOD) and Internet of things (IoT). Internet-connected sensors are common throughout government today for everything from smart buildings to asset monitoring to data collection.

Today's IT environment also includes more remote users than ever before, due to both the organic growth of telework and the current work-from-home situation that Coronavirus has forced. Remote workers can sometimes make innocent mistakes that can easily turn into big problems. Writing down and sharing passwords, sending files to personal email, failing to log off, logging in over unsecure WiFi, or downloading onto an external memory stick can all cause major issues. According to a recent BeyondTrust report, nearly two-thirds of organizations believe they have or may have experienced a breach due to misused or abused employee access.

And then there is the government's massive contractor workforce. The BeyondTrust report found that 58 percent believe they have suffered a breach due to vendor access, and only 29 percent are very confident that they even know how many third-party vendors are accessing their systems. Other reports have corroborated these findings.

"These contractors are not government employees, and they come and go as prime contracts

change," said Kevin Gordon, chief sales & marketing officer at Swish, a provider of technology solutions and engineering services to the federal government. "It's a huge undertaking for an agency to manage privileged access to particular databases and applications."

All of these factors make it more difficult than ever to know who and what is accessing an agency's systems and data at any given time. That leads to privilege misuse or abuse, both intentional and unintentional.

"The question is how to secure the entire environment when it isn't contained in one location or by one person or even by one device or entity," said Craig McCullough, vice president of public sector at BeyondTrust. "What's needed is a more holistic approach to privileged access management that gives security professionals absolute control over every privilege in their environment, so they can secure their entire universe of privileges."

A holistic approach to privilege management

That new, more holistic approach is called Universal Privilege Management (UPM). This model brings together the important aspects of managing privileges under one umbrella. Universal privilege management enables agencies to granularly secure, manage, and audit all privileged access on-premise or in the cloud for employees, remote workers, vendors, machines, and more. Together, the tools that make up universal privilege management can drastically reduce the attack surface and windows of exposure, and improve auditing and visibility, all while boosting mission productivity.

"It goes far beyond just securing passwords," McCullough explained. "It's a modern approach that secures every user, every session and every asset across the entire environment. You're securing the entire universe of privilege that you see, in a holistic, strategic, and productive fashion."

Universal privilege management is comprised of three solution pillars: privileged password management, endpoint privilege management, and secure remote access.

Privileged password management discovers, onboards, manages, and audits every privileged account, both human and non-human, and tracks every session. Security personnel should also be able to pause or terminate active privileged sessions as necessary.

Endpoint privilege management grants rights to the right user or application at the time needed, to do what needs to be done. The moment a user no longer needs access, it is automatically revoked. Access also can be revoked if the system detects that a user is performing an action considered out of the norm.

Secure remote access secures, manages, and audits remote access for personnel and vendors, ensuring the right level of access for each user and session. It also allows users to connect from anywhere, to anywhere, to any device, without a VPN.

In one recent case, a major federal agency chose a secure remote access solution from BeyondTrust and Swish to reduce the number of complex security tools, which not only inhibited user productivity, but were nearly impossible to manage. The solution unified all privileged access management use cases into one integrated platform. It reduced risk by providing complete coverage over all users, assets and accounts and was easy to deploy, manage, and integrate with existing security tools. The customer was able to quickly deploy the secure remote access solution and enable third-party integrations so they could move forward on achieving their strategic federal agency objectives. Now the federal agency's IT team can easily grant, control, audit, and revoke third-party access. They are also seeing improvement in IT support ticket resolution.

> **"It goes far beyond just securing passwords. It's a modern approach that secures every user, every session and every asset across the entire environment. You're securing the entire universe of privilege that you see, in a holistic, strategic, and productive fashion."**
>
> —CRAIG MCCULLOUGH
> VICE PRESIDENT OF PUBLIC SECTOR AT BEYONDTRUST

It's okay to start small

If budget and other resources are stretched, it's okay to start with the solution that addresses your agency's most pressing needs. However, the best long-term vision is to deploy a solution that is part of a broader platform, and not a point solution. Adding a siloed solution could add more complexity and integration issues to your environment down the line. By choosing BeyondTrust's universal privilege management platform, an agency that wants to start by protecting privileged access from third parties or eliminating administrative rights from users can do so without implementing a full password management solution at first, McCullough explained. "Over time, the agency can then enhance the level of protection across their organization in a way that meets their budget and needs."

That's the path that one large federal department is taking. The department chose to implement a secure remote support solution to help ensure that it could keep pace with a planned expansion of personnel and duties. Swish and BeyondTrust worked together to implement the solution, which has also enabled the department to effectively manage the current unexpected remote access requirements caused by COVID-19 without impacting productivity. Since it worked so well, the department is currently considering the next phase of deployments under the universal privilege management model.

"By looking at cybersecurity as a whole, agencies can better devise a comprehensive strategy that will fully protect them, and universal privilege management should be part of that strategy," Gordon said. "Whether achieving compliance for DOD's new cyber framework, or managing a complicated identity lifecycle for a civilian agency, universal privilege management is the path forward."

Swish

BeyondTrust