WHITE PAPER

A RISK-BASED APPROACH TO INSIDER THREAT DETECTION FOR FEDERAL GOVERNMENT AGENCIES

Leveraging Privileged Access Security solutions to detect, alert, and respond to insider threats

CyberArk.com

Table of Contents

Executive Summary

Malicious insiders have been and continue to be a major threat to United States government. Regardless of motivation, when an insider decides to go rogue they can cause severe damage to an agency and in some cases, even adversely impact the state of national security. One big advantage a malicious insider has is they often already have an “all access pass” with the necessary privileges required to gain access to some of the government’s most sensitive applications, systems, and devices. This makes prevention and detection more nuanced as the actions taken by the privileged user often appear to be fully authorized activity. Insider threat programs have been mandated to prevent, detect, and respond to the threat of malicious insiders. This white paper will highlight how U.S. federal government agencies can put in place effective countermeasures to combat insider threats and provide granular level access to critical systems and applications, effectively manage authentication, and monitor all privileged access activity.

A Risk-based Approach to Security

Why focus on privileged accounts and access? Because it is important to take a wholistic approach to security. Protect the perimeter but also the keys to the kingdom – the privileged and administrative accounts. It is not only important to be in compliance but to also go a step further to stay ahead of the attackers. When privileged and administrative accounts are left unmanaged and unsecured, it becomes easy for malicious insiders to successfully carry out an attack, given the access they provide. These accounts have been exploited in every major attack affecting federal government agencies. Security frameworks such as the Council on Cyber Security Top 20 Critical Security Controls, NIST, and others have always maintained the importance of protecting, managing and monitoring privileged and administrative accounts. These accounts present a large security vulnerability when left unmanaged and unsecured.

Privileged user accounts should be a critical focus as, unlike regular authorized users, they have been given elevated access that allows them to access certain designated or all systems within an enterprise network. These accounts are designed to be used by system administrators to manage or troubleshoot network systems, run services, or allow applications to communicate with one another. The downside is that these same credentials, which are used to help keep the organization operating, can easily be unintentionally misused in an operator error, or maliciously used to cause significant damage to networks or for the exfiltration of sensitive data.

Federal government agencies are beginning to take a risk-based approach in securing their infrastructure and think like the attacker. As security tools and solutions are continually developed to protect agencies from existing vulnerabilities and threats, attackers are often one step ahead – thinking of new sophisticated ways to infiltrate an agency and disrupt operations, hold the agency for ransom, steal PII, and classified data. The first step in proactive protection is locking down the privileged access pathway to your most critical systems and applications.

Centralizing Access to Critical Infrastructure

Centralizing, securing and managing credentials used to access privileged accounts both on-premises and cloud-based environments is fundamental in securing your infrastructure. Instead of needing dozens or hundreds of sets of separate credentials to access necessary accounts, administrators need only one highly secure credential, which can be a password, token, certificate or other multi-factor authentication method of choice. This secure credential is used to allow the administrator to prove they truly are who they claim to be, and have the right to access other privileged accounts. Once logged in to the central console, administrators can seamlessly and securely access all their authorized privileged accounts from one place. During emergencies and one-off situations, automated workflows enable users to easily request and receive approval to access needed privileged accounts. This centralized approach enables greater security, improves interactions with IT systems and helps to simplify day-to-day tasks. This end user benefit is critical for any privileged access security project, and alleviates the administrative burden on the system administrators.

How does it work? After locating privileged user and application accounts and SSH keys, agencies should proactively secure, rotate and control access to their privileged account credentials. CyberArk provides a highly secure repository for storing sensitive account passwords and private SSH keys, and it supports strong access controls to help ensure that only authorized users, applications or systems are able to access these credentials. Using the CyberArk Digital Vault, organizations can centrally manage access to most all privileged accounts, including but not limited to those on *NIX systems, Windows systems, databases, and network devices, both on-premises and in the cloud.

To comply with some of the government's best practices, as well as to reduce the risk of a compromised credential, federal government agencies should proactively rotate privileged passwords and SSH keys. Using CyberArk Enterprise Password Vault, security teams can automate password and key pair rotation, set policies to rotate these credentials at regular intervals and rotate credentials on-demand as needed. When securing and managing privileged account credentials, it's important to keep in mind the nuanced differences between privileged user credentials and privileged application credentials. While both types of credentials require centralized security, rotation and access controls, the approaches should be slightly different in order to maintain user productivity and application availability.

Once user credentials are securely stored and managed in the Digital Vault, security teams should set policies to ensure that only authorized users are able to access authorized credentials. To do this, CyberArk solutions enable agencies to create access control policies based on individual users or user groups. Customizable workflows enable users to request access to credentials with elevated privileges as needed for business purposes, and integrations with IT ticketing systems are available to validate approvals. For added control, agencies can require multi-factor authentication before users may gain access to credentials in the Digital Vault. This not only helps to strengthen security, but also enforces strong authentication to protected systems, as required by some regulations and industry standards.

Effectively Managing Authentication

Traditional authentication is a knowledge-based process wherein the user knows in advance the necessary password or credentials to obtain access to the necessary systems. There are a few other techniques to properly authenticate via biometrics means or through Personal Identity Verification (PIV) or Common Access Cards (CAC). However, limiting authentication to only traditional methods creates a single point of failure to the agencies security. It is a best practice for both public and private organizations alike to implement multi-factor authentication to reduce the risk associated with insider threats. The implementation of multi-factor authentication solutions is a direct response to vulnerabilities associated with improperly secured privileged account credentials.

Using multi-factor authentication for all users and product administrators enables agencies to mitigate some of the common credential theft techniques such as basic key loggers or more advanced attack tools that are capable of harvesting plaintext passwords. CyberArk solutions integrate with a range of authentication solutions to provide an additional layer of authentication security. Multi-factor authentication can be enforced for all privileged accounts via the central login to the CyberArk solution. Single-sign-on to the CyberArk solution also provides secured and centralized authentication to resources throughout the organization. This can simplify a robust authentication implementation while enforcing strong authentication requirements across the agency.

Monitoring All Privileged Access Activity

In today's threat environment, agencies must not only proactively protect their critical systems and sensitive data, but they must also anticipate insider attacks that bypass proactive controls. The greatest risk associated with a compromised privileged account is that the attacker may be able to move freely around the environment to locate and access highly sensitive data. These accounts allow attackers to infiltrate systems in plain sight while deleting their tracks along the way, allowing the attackers to operate undetected for months. Without the ability to detect abnormal privileged access activity, advanced and inside attackers can exfiltrate sensitive data before an organization has even been made aware of the breach.

Cyber attackers behave differently than legitimate users. They log in at different times, from different locations, and access systems in different patterns. It's much more difficult for the attacker to hide from detection mechanisms that rely on behavioral pattern analysis. Privileged accounts are an agency's last line of defense against a cyber attack. Once these accounts are compromised, the attackers have everything they need to successfully locate and steal the targeted data. At this point in a breach, the only way to thwart the attack is to locate anomalous privileged access activity that indicates a compromise and restrict the impacted accounts.

CyberArk helps federal government agencies do just that. CyberArk Privileged Threat Analytics monitors all privileged user and account activity to establish a baseline of what is “normal.” The solution first aggregates specific data sets from security information and event management (SIEM) tools, taps traffic over the network, queries the Active Directory, and collects privileged account related activity from other CyberArk solutions. Using a self-learning, statistical analysis engine and correlation analysis, this solution is able to rapidly detect and alert on any information that falls outside of that norm, indicating a potential attack in progress. By alerting security teams to anomalous activity early, the solution enables agencies to accelerate incident detection times, reduces the window of opportunity for attackers, and gives security teams the opportunity to stop the attacker before they cause greater damage.

Recommended Steps for Insider Threat Mitigation

It’s hard to understand why an insider would undermine an agencies objectives, to reduce the risk of insider threats and limit potential damage, agencies should consider these five recommendations.

1. Reduce the attack surface to limit insider threat exposure: Restrict standard number of user privileges based on role to limit intentional or accidental damage. Control applications to reduce the risk of users becoming exploited.
2. Don’t leave credentials lying around: Store privileged credentials in a secure, central repository that supports strong access controls, multi-factor authentication, and full auditability. Change these credentials on a regular basis.
3. Limit the power of any one account: Segregate administrative duties based on least privilege principle, and role based access controls so that privileged users only have access to functions and capabilities commensurate with their roles and responsibilities. Only allow full administrative or root access when necessary.
4. Look for attackers disguised as authorized insiders: Attackers operating with privileged accounts will look like authorized insiders, but their behavior will likely be different. Monitor and analyze privileged user and account behavior to learn what’s normal to more easily identify anomalies that may indicate in-process attacks.
5. Do what you can to deter bad behavior: Inform users they are being monitored, and consistently audited for changes in employee behavior.

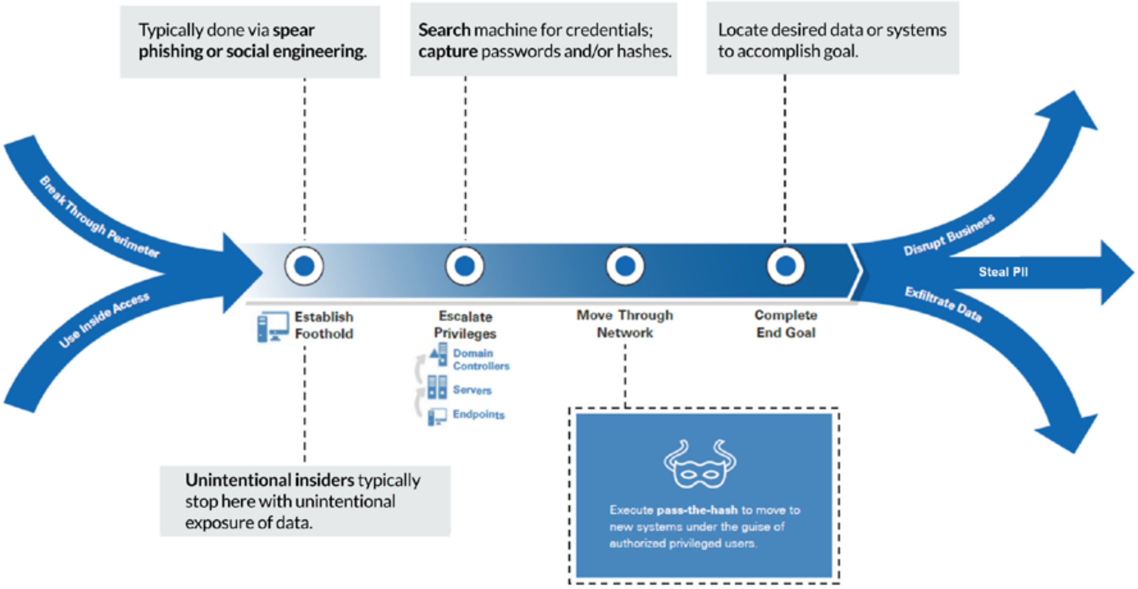
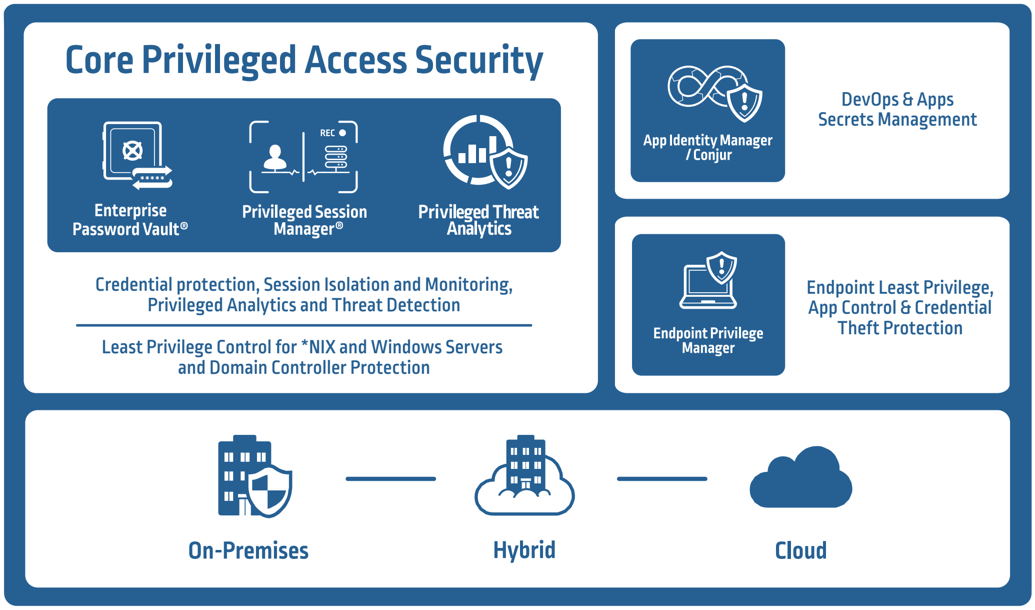

Typically done via **spear phishing or social engineering.**
Search machine for credentials; **capture** passwords and/or hashes.
Locate desired data or systems to accomplish goal.
Break Through Perimeter
Use Inside Access
Establish Foothold
Escalate Privileges
Domain Controllers
Servers
Endpoints
Move Through Network
Complete End Goal
Disrupt Business
Steal PII
Exfiltrate Data
Unintentional insiders typically stop here with unintentional exposure of data.
Execute **pass-the-hash** to move to new systems under the guise of authorized privileged users.

Figure 1. This chart shows a standard attack pathway malicious insiders use to execute their attack.

CyberArk Solutions Overview

The CyberArk Privileged Access Security solution enables agencies to secure, provision, manage, control and monitor all privileged access related activity. The solution is built on a common, Shared Technology Platform that delivers a single management interface, centralized policy creation and management, a discovery engine for provisioning new accounts, enterprise-class scalability and reliability, and the secure Digital Vault™. The individual products in the CyberArk Privileged Access Security Solution integrate with the Shared Technology Platform, enabling agencies to centralize and streamline management.


Core Privileged Access Security
Enterprise Password Vault®
Privileged Session Manager®
REC
Privileged Threat Analytics
Credential protection, Session Isolation and Monitoring, Privileged Analytics and Threat Detection
Least Privilege Control for *NIX and Windows Servers and Domain Controller Protection
App Identity Manager / Conjur
DevOps & Apps Secrets Management
Endpoint Privilege Manager
Endpoint Least Privilege, App Control & Credential Theft Protection
On-Premises
Hybrid
Cloud

The CyberArk Privileged Access Security Solution includes the following products:

- Core Privileged Access Security Solution
  - Centrally secure and control access to privileged credentials based on administratively defined security policies
  - Isolate and secure privileged user sessions, and protect target systems from malware on endpoints
  - Detect, alert and respond to anomalous privileged activity
  - Control least privilege access for *NIX and Windows
  - Protect Windows Domain Controllers
- Application Identity Manager™ eliminates hardcoded passwords and SSH keys from applications and scripts and replaces them with secure, dynamic credentials, with zero impact on application performance
- Conjur is a secrets management solution tailored specifically to meet the unique infrastructure requirements of native cloud and DevOps environments
- Endpoint Privilege Manager secures privileges on the endpoint and contains attacks early in their lifecycle

The CyberArk Privileged Access Security single-platform solution is uniquely positioned to help federal government agencies meet today's challenging security and compliance requirements. The CyberArk Privileged Access Security solution has been added to the U.S. Department of Defense (DoD) Unified Capabilities Approved Products List (UC APL). This designation identifies products that have undergone a rigorous testing process conducted by the DoD, which assures acceptable levels of information assurance (IA) and interoperability (IO) capabilities. CyberArk's Privileged Access Security Solution has been independently validated and awarded an Evaluation Assurance Level (EAL) 2+ under the Common Criteria Recognition Agreement (CCRA). Additionally CyberArk has received the U.S. Army Certificate of Networthiness (CoN) enabling the streamlined implementation of the CyberArk solution on the Army Enterprise Architecture/LandWarNet (LWN). You can visit the Army CoN website for more details on the CyberArk certification #201621511 (requires CAC for access). CyberArk's efforts to obtain and maintain these certifications demonstrates the company's commitment to helping federal government agencies and global enterprises secure privileged access.

Here are a few ways in which CyberArk can help meet security and compliance requirements in federal government agencies:

- FISMA/NIST SP800-53 – CyberArk solutions help federal government agencies comply with requirements related to the "Access Control", "Audit and Accountability" and "Identification and Authentication" control families.
- Department of Homeland Security CDM Program – Phase 2 of the Continuous Diagnostics and Mitigation (CDM) program features least privilege and infrastructure integrity requirements which can be addressed with CyberArk solutions.
- NERC – CIP – Requirements related to privileged access control, remote access management and access revocation in the regulation can be addressed with CyberArk solutions.
- HSPD-12 – The requirement to authenticate using a Personal Identity Verification (PIV) card can be easily implemented across all current and legacy systems with the seamless integration of CyberArk solutions and PIV cards.

Conclusion

To effectively protect against insider threats, federal government agencies should minimize user privileges to reduce the attack surface, lock down privileged credentials, and control and monitor privileged access, which are consistently targeted by advanced insider and external attackers alike. CyberArk's comprehensive solution for privileged access security offers proactive controls to reduce the risk of intentional and unintentional insider threats, as well as real-time monitoring and threat analytics to aid in detection.

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice.