CYBERARK®

WHITEPAPER

Addressing the Department of Defense's Zero Trust Framework with the CyberArk Identity Security Platform

A Technical Review of how Federal Agencies can Leverage CyberArk Identity Security Solutions to Align to the DoD's Zero Trust Reference Architecture.



Table of Contents

Introduction **3**

Pillar #1 – Users 4

Pillar #2 – Devices 4

Pillar #3 – Network

Pillar #4 – Applications 6

Pillar #5 – Automation: Security Automation and Orchestration Harmonious 7

Pillar #6 – Analytics: Security Visibility and Analytics 8

Zero Trust for Privileged Users 19

Zero Trust Privileged User Credential Boundaries 20

Zero Trust for Applications 20

Users/Analytics 25

Data/Devices 26

Applications/Automation 26

How To Get Started: Establishing Identity Security Success with the Cyberark Blueprint **26**

CyberArk's Commitment to the Federal Government 27

Conclusion **27**

Introduction

In the spring of 2021, the White House issued an executive order putting into place guidelines on how to improve the nation's cybersecurity stance. This requires federal agencies to modernize their approach to cybersecurity by becoming more transparent about cyber threats for protection. Government agencies are required to move toward a Zero Trust architecture, which calls for an "assume-breach" mindset and secures all cloud services. Federal agency heads must develop a plan for implementing the ZT Architecture and incorporate guidelines from the National Institute of Standards and Technology (NIST) as appropriate.

With the cybersecurity executive order in place, the U.S. Department of Defense recently published its Zero Trust Reference Architecture. What's important to note is that the newly revised DISA Zero Trust Architecture now includes the addition of privileged access management (PAM).

This technical whitepaper will outline the importance of PAM controls that are necessary to align with the DISA Zero Trust reference architecture and why federal agencies need to follow the government's recommendations for implementing a Zero Trust framework.

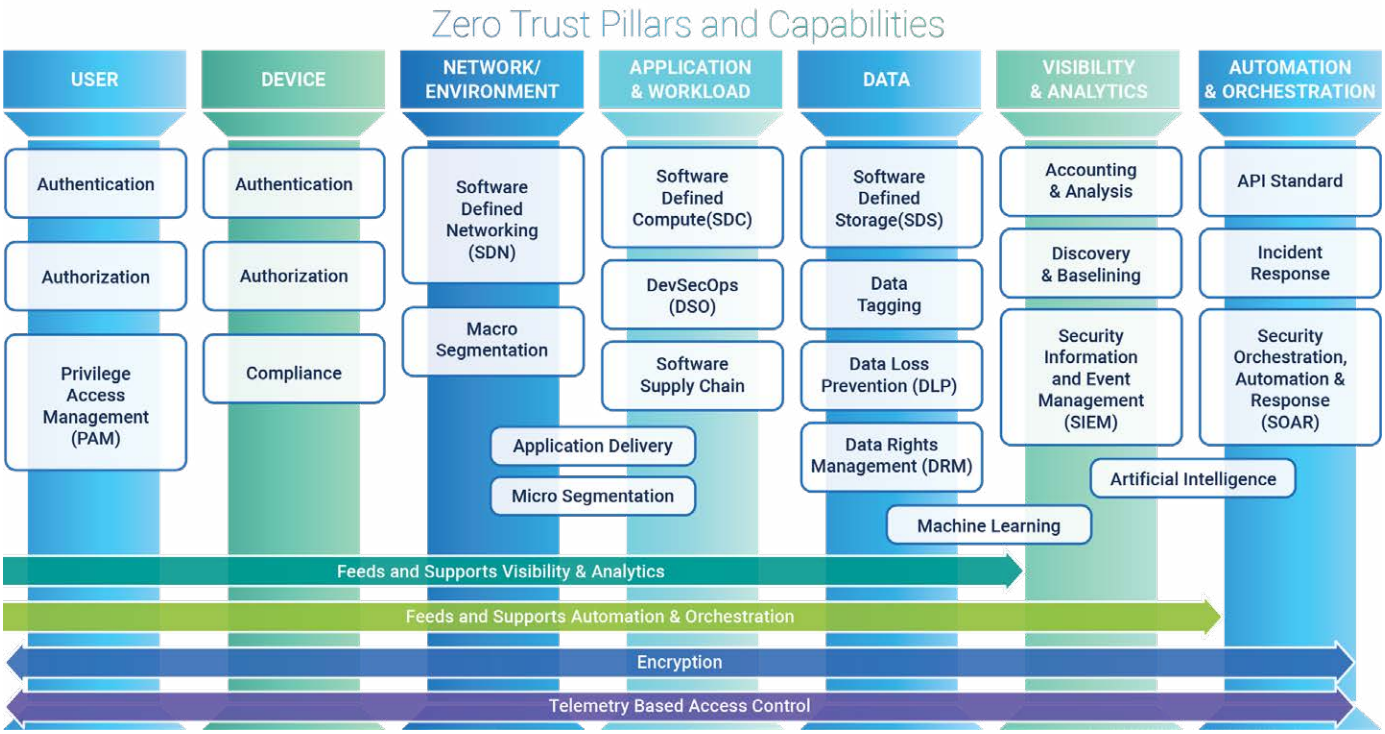
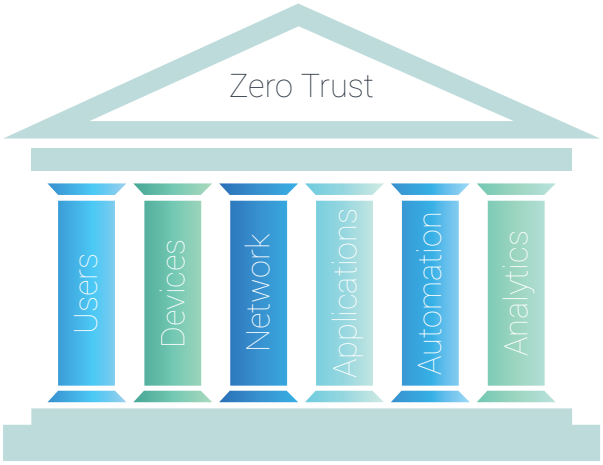


Figure 1: Zero Trust Pillars and Capabilities

Zero Trust can be thought of as a strategic initiative that, together with an organized framework, enables decision makers and security leaders to achieve pragmatic and effective security implementations. Zero Trust efforts need to incorporate, coordinate and integrate a challenging combination of policies, practices and technologies to succeed. A conceptual security model can be helpful to understand and organize these components, and one can see how CyberArk aligns directly to each of the six Zero Trust pillars below.



Six Pillars of a
Zero Trust Security Model

Figure 2: Six Pillars of a Zero Trust Security Model

Pillar #1 – Users

People/Identity Security - Ongoing authentication of trusted users is paramount to Zero Trust. This encompasses the use of technologies like Identity, Credential and Access Management (ICAM); Multi-Factor Authentication (MFA); and continuously monitoring and validating user trustworthiness to govern their access and privileges. Technologies for securing and protecting users' interactions, such as traditional web gateway solutions, are also important.

CyberArk Workforce Identity delivers next-gen access, helping protect organizations through a Zero Trust approach. With CyberArk Workforce Identity, organizations experience secure access everywhere, with reduced complexity and newfound confidence to adopt modern business models and deliver exceptional customer experiences.

Organizations can take a step toward Zero Trust architecture by strengthening access controls with frictionless secondary authentication for end users.

Workforce Identity MFA adds an extra layer of protection before granting access to corporate applications. Leveraging device, network and user behavior context, Workforce Identity helps intelligently assign risk to each access event and allows you to create dynamic access policies that are triggered when anomalous behavior is detected.

Specific to privileged identities or users, the associated access needs to be continuously monitored and validated in terms of user trustworthiness to govern access and privileges. Incorporating identity access with a least privileged approach is foundational to Zero Trust. Privileged identities should only be provided access to the systems when specifically required. Access should be as limited as possible, and access should be immediately revoked when it is no longer required. CyberArk Privileged Access Manager provides the foundational controls to secure privileged user access, both human and non-human (i.e., service accounts).

Pillar #2 – Devices

Device Security - Real-time cybersecurity posture and trustworthiness of devices is a foundational attribute of the Zero Trust approach. Some "system of record" solutions, such as Mobile Device Managers, provide data that can be useful for device-trust assessments. Additionally, other assessments should be conducted for each access request (e.g., examinations of compromise state, software versions, protection status, encryption enablement, etc.).

Traditional measures of security are not sufficient for today's new world. The sophistication and scale of cyber attacks is unlike any previous era. Most breaches involved the compromise of privileged accounts and credentials, and phishing attacks are often followed by malicious software installation, because of this it is imperative to ensure your endpoints are integrated with your identity and access management strategies. As devices are gateways to company data and resources, it is critical that one only allows access to corporate resources from trusted endpoints. CyberArk Workforce Identity can make sharing access from validated dual authenticated endpoints possible and seamless.

Pillar #3 – Network

Network Security - Some argue that perimeter protections are becoming less important for networks, workflows, tools and operations. This is not due to a single technology or use-case, but rather a culmination of many new technologies and services that allow users to work and communicate in new ways. Zero Trust Networks are sometimes described as "perimeter-less;" however, Zero Trust Networks attempt to move perimeters in from the network edge and segment and isolate critical information from other data. The perimeter is still a reality, albeit in a much more granular way. The traditional infrastructure firewall perimeter, or "castle and moat" approach, is not sufficient. The perimeter must move closer to the data in concert with micro-segmentation to strengthen protections and controls. Network security must expand as agencies grow their networks to partially or fully transition to Software Defined Networks, Software Defined Wide Area Networks and internet-based technologies. It is critical to (a) control privileged network access, (b) manage internal and external data flows, (c) prevent lateral movement in the network and (d) have visibility to make dynamic policy and trust decisions on network and data traffic. The ability to segment, isolate and control the network continues to be a pivotal point of security and is essential for a Zero Trust Network.

In addition to traditional network segmentation, CyberArk's privileged session management capabilities allow for implementation of tiered levels of access and credential boundary concepts across a multitude of devices. This concept is similar to Microsoft's ESAE/Red Forrest and Privileged Access Workstation (PAW) but with more accountability, more supported device/application types, lower costs and quicker time to productions.

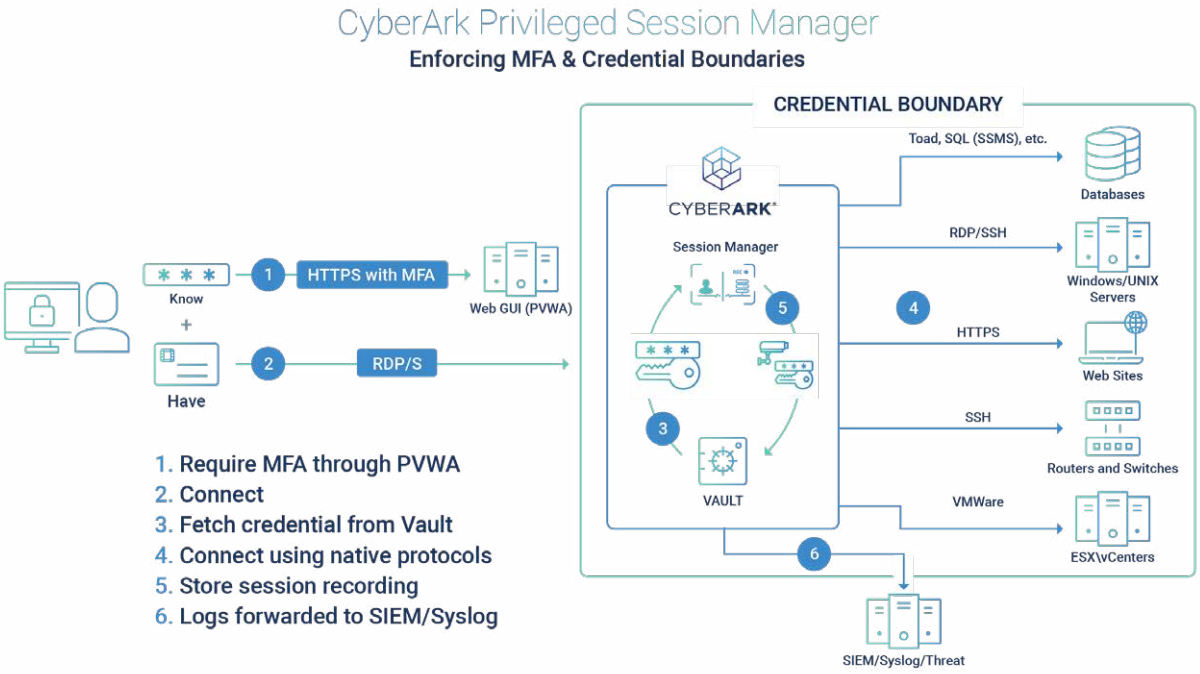


Figure 3: CyberArk Privileged Session Manager Enforcing MFA and Credential Boundaries

Pillar #4 – Applications

Application and Workload Security - Securing and properly managing the application layer, as well as compute containers and virtual machines, is central to Zero Trust adoption. Having the ability to identify and control the technology stack facilitates more granular and accurate access decisions. MFA is an increasingly critical part of providing proper access control to applications in Zero Trust environments.

CyberArk addresses Zero Trust for Applications in three different ways:

1. CyberArk Workforce Identity - The Workforce Identity Application Gateway is available as an add-on to the Workforce Identity Single Sign-On service. It provides an easy and secure way to access on-premises applications without requiring configuration of VPN clients, modification of firewall policies or changing of on-premises code. With Workforce Identity, IT teams can provide users SSO access to applications required to perform responsibilities and manage user identities across all applications and endpoints from a single console. Workforce Identity enforces Zero Trust by securing access to legacy applications with Workforce Identity MFA and configures per-application access based on user roles. Application Gateway enables you to prevent both inadvertent and intentional identity–related security breaches and manage access policies for all applications in one management interface

2. CyberArk Secrets Manager - Enterprises are increasingly adopting DevOps methodologies and automation to improve business efficiency and to accelerate innovation, while also leveraging commercial and internally developed applications. However, each application, automation tool and other non-human identity relies on some form of privileged credential to access sensitive resources. Additionally, application and IT environments can vary significantly within the organization — from highly dynamic, native cloud to largely static and even mainframe based. The privileged credentials used by applications need to be secured regardless of the application type and compute environment. These credentials pose a variety of challenges for IT security, operations and compliance teams. Application and other non-human credentials must be managed. In addition to eliminating hard-coded credentials in code and scripts, approaches and techniques, including strong authentication, least privilege, role-based access controls, credential rotation and audit, should also be used in a Zero Trust environment.

With Endpoint Privilege Manager's application control, least privilege and Zero Trust capabilities, IT operations and security teams can allow approved applications to run, while blocking malware, including ransomware. Unknown applications can run in "Restricted Mode," which prevents them from accessing corporate resources, sensitive data or the Internet.

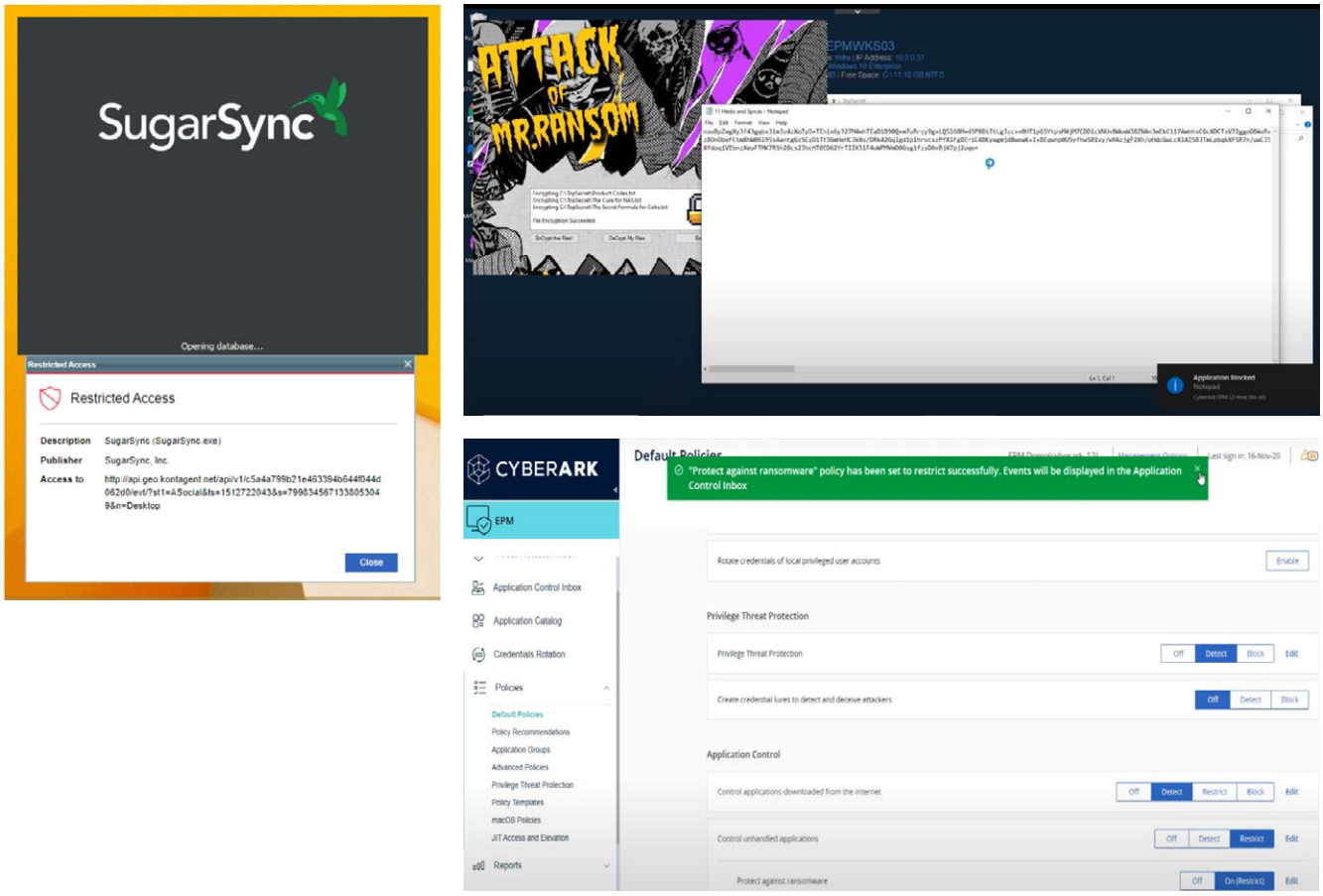


Figure 4: CyberArk Endpoint Privilege Manager allows an application to run in 'Restricted Mode.'

You can also send these applications to Endpoint Privilege Manager's cloud-based Application Analysis Service, which integrates with data feeds from CheckPoint, FireEye, Palo Alto Network and other services for additional analysis. The solution reduces security risk and configuration drift on endpoints, while reducing help desk calls from end users. Based on testing by the CyberArk Threat Research Labs team, the removal of local administrator rights combined with application control is extremely effective in helping to prevent ransomware from encrypting files.

Pillar #5 – Automation: Security Automation and Orchestration Harmonious

Zero Trust makes full use of security automation response tools that automate tasks across products through workflows, while allowing for end-user oversight and interaction. Security Operation Centers commonly make use of other automated tools for security information, event management, and user and entity behavior analysis. Security orchestration connects these security tools and assists in managing disparate security systems. When integrated, these tools can greatly reduce manual effort and event reaction times, while reducing costs.

CyberArk prides itself on the CyberArk C3 Alliance, a robust technology partnership ecosystem. With more than 300 integrations, CyberArk provides the ability to manage privileged credentials to your most critical applications. Utilizing CyberArk as an entry point to applications allows for a Zero Trust environment by enforcing "who" or "what" has access to the privileged credential required for secure, audited access in a Just-in-Time (JIT), just enough administration approach.

Pillar #6 – Analytics: Security Visibility and Analytics

Combatting threats that are invisible is a nearly impossible feat that challenges organizations, both public and private. Zero Trust leverages tools like security information management, advanced security analytics platforms, security user behavior analytics and other analytics systems to enable security experts to observe in real time, what is happening and orient defenses more intelligently. The focus on the analysis of cyber-related event data can help develop proactive security measures before an actual incident occurs.

CyberArk Privileged Access Manager delivers advanced analytics, based on patent-pending behavioral and deterministic algorithms, which helps detect anomalies when they occur. This is achieved by comparing the historical patterns of privileged access with the current behavior and use of privileged accounts. While there may be broader security analytics solutions on the market, such as SIEM and SOAR, realtime security intelligence solutions, having a specialized product offering that targets monitoring and rapid response of the misuse of privileged account usage, provides an RTSI approach to privilege management that is ahead of the curve when compared to more generalized approaches that are available in the market. Understanding the behavior of your privileged credentials enhances your Zero Trust model by automating trust by alerting on abnormal behavior.

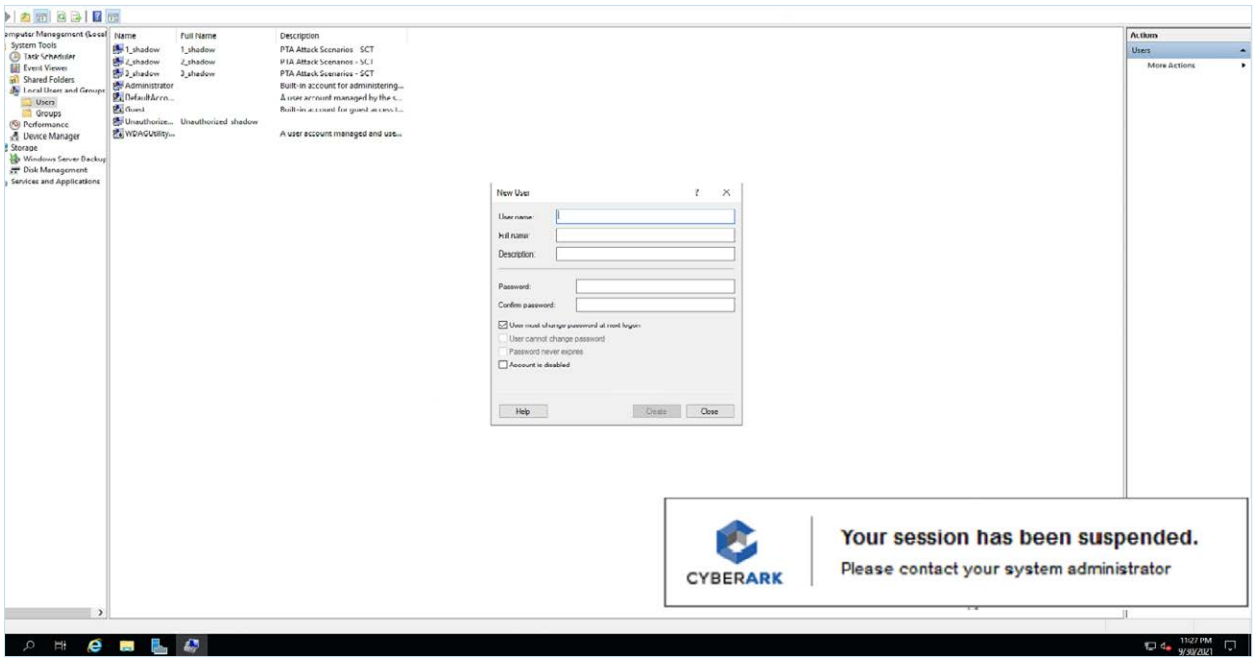


Figure 5: CyberArk Privileged Access Manager suspends a privileged session that presented high levels of risk.

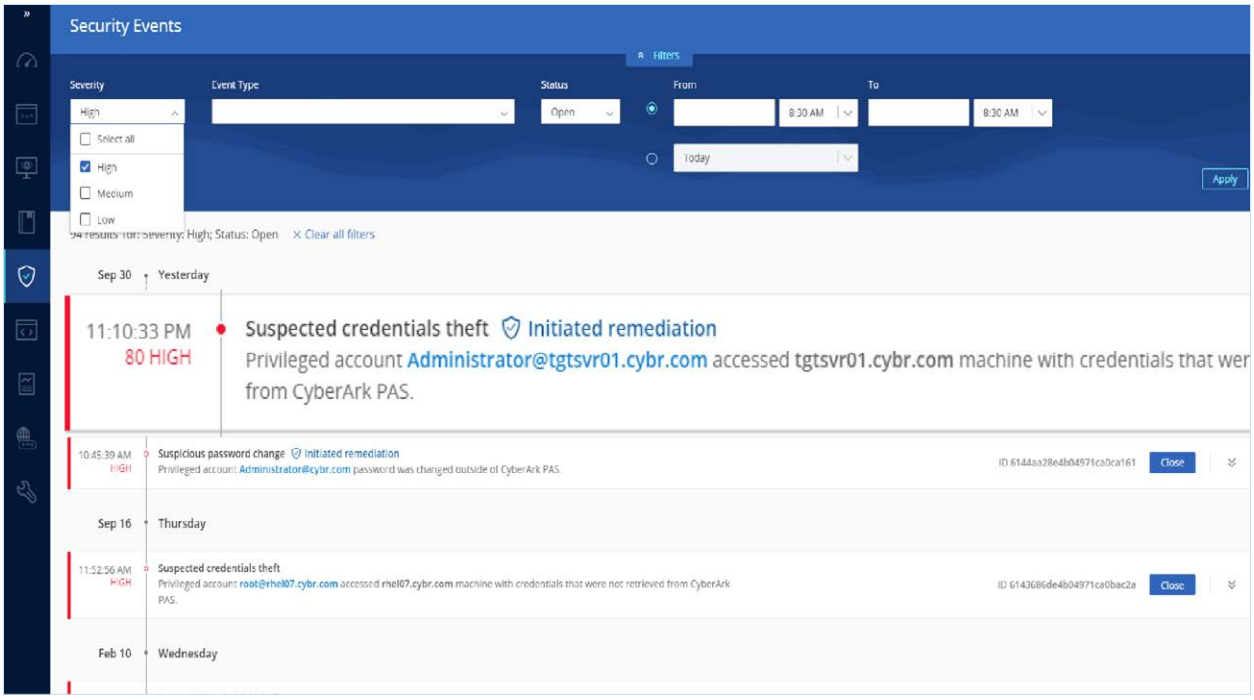


Figure 6: CyberArk Privileged Access Manager allows for the assignment of a risk score to privileged sessions, which can then be filtered by severity to streamline and improve audit review processes.

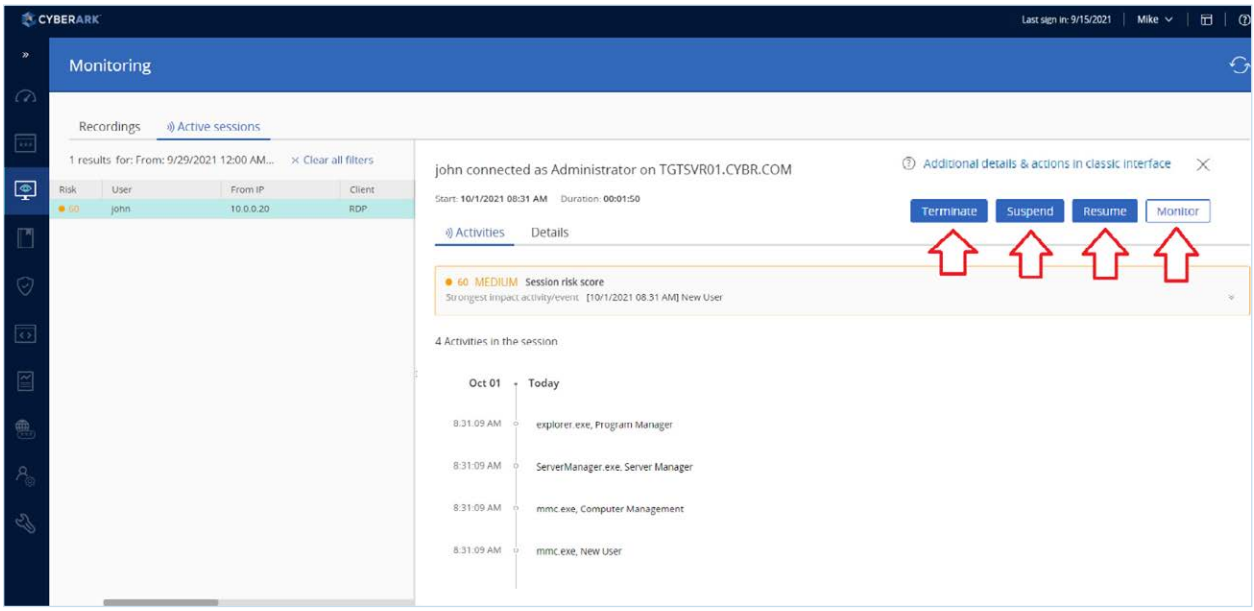


Figure 7: CyberArk Privileged Access Manager enables auditors to terminate, suspend, resume or monitor privileged sessions.

Compromised accounts is one of the leading causes of a data breach. CyberArk Workforce Identity leverages real-time security analytics to provide context-aware access decisions in real time. Trying to build an environment that combines authentication policies for users, roles, applications and devices, while ensuring secure access and preventing user productivity, is a massive security undertaking. Workforce Identity Analytics, which is based on user behavior, prevents credential-based attacks that serve as the core that fuels Workforce Identity SSO and MFA. Behavior-based scoring enables a frictionless user experience that is adjusted based on risk and improving productivity, while maintaining security.

This next section leverages the latest draft of NIST SP 800-207, Zero Trust Architecture, describing CyberArk's approach to the Zero Trust tenants defined within the publication.

2.1. All data sources and computing services are considered resources.

CyberArk assists agencies in classifying access to devices based on their level of criticality. By grouping assets into safes (logical access containers) within CyberArk, agencies can control who has access to what credentials based on the principles of least privilege. Agencies determine which devices are most critical and implement the necessary level of controls in order to retrieve or leverage that credential, for example, multi factor, approval from a manager or multiple managers, etc.

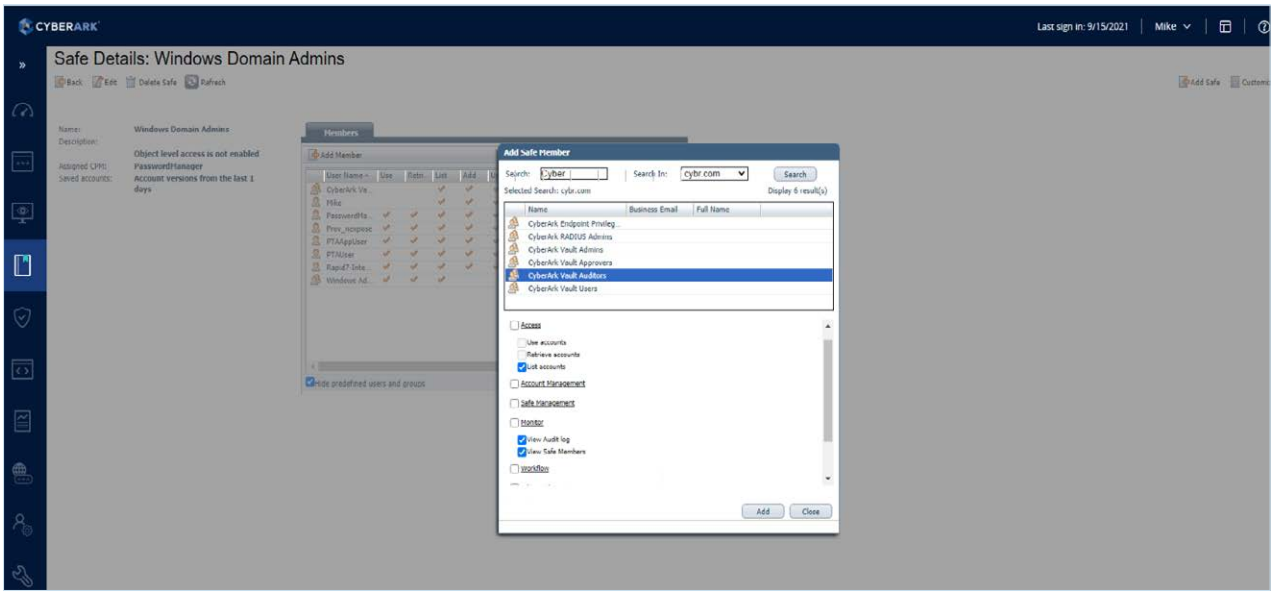


Figure 8: CyberArk provides granular permissions to be assigned to specific members of a "safe" within the CyberArk Digital Vault.

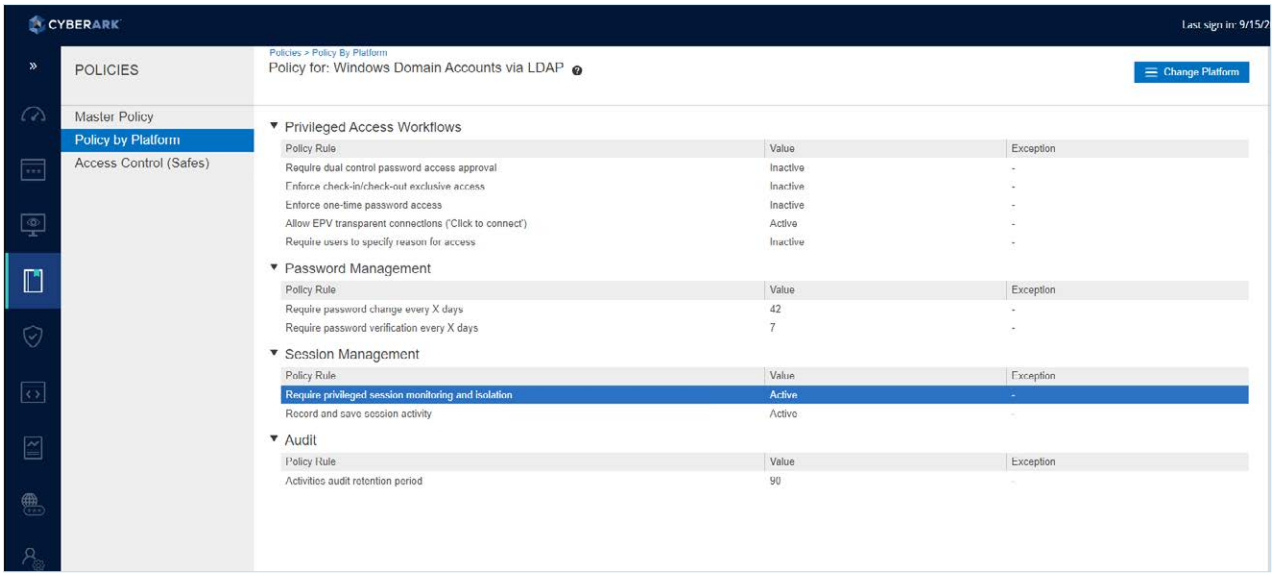


Figure 9: Here we can see platform policies associated with a particular safe.

By securely storing privileged credentials in a hierarchical manner and by re-authenticating users at each request, CyberArk is helping to implement zero trust for privileged access to devices and constantly reverifying access at multiple points (logon, during sessions, etc.).

2.2 All communication is secured regardless of network location. Network location does not imply trust. Access to individual enterprise resources is granted on a per-session basis.

Whether deployed on-premises, in the cloud, or in a hybrid environment, CyberArk helps provide end-to-end security.. CyberArk has invested heavily in designing and building security measures directly into our products. By leveraging built-in security capabilities and adhering to the CyberArk Digital Vault security standard, CyberArk customers can significantly strengthen the security of their PAM solution to mitigate the risk of a system compromise.

At the core of all CyberArk PAM solutions is the Digital Vault, which contains a highly secure database that stores privileged account credentials, access control policies, credential management policies and audit information. To protect both the Digital Vault database itself and the data stored within it, CyberArk has designed a multi-layered encryption hierarchy that uses FIPS 140-2 compliant encryption. Symmetric encryption is completed using an AES-256 key, and asymmetric encryption is completed using an RSA-2048 key pair. Each individual file and safe within the Digital Vault database is uniquely encrypted using a randomly generated encryption key.

As sensitive data is transmitted between systems, it can potentially be exposed to attackers who are eavesdropping inside the network. To help prevent these attackers from capturing privileged account credentials from intercepted traffic, CyberArk ensures all data to and from the Digital Vault is encrypted in transit.

The Digital Vault software employs a proprietary protocol to secure sensitive privileged account information as it is transmitted between CyberArk components. The proprietary session encryption mechanism uses a unique AES-256 session key and is FIPS 140-2 compliant. With this level of encryption in place, attackers inside the network may be able to see traffic flowing between CyberArk components, but the traffic will be undecipherable and thus useless to the attacker.

With CyberArk, network location is not an indicator of trust. Regardless of whether the user is on the enterprise network or remoting in via VPN, on-premise or in the cloud, users must still authenticate to CyberArk and are allowed access based on the policies in place. Once authenticated in, users are given access to their target endpoint via privileged session management capabilities with Privileged Access Manager. This trusted proxy allows users direct privileged access to the target endpoint, while also putting controls in place to monitor that session. Agencies can monitor the sessions in real time and terminate sessions based on suspicious activity. The use of privileged session management also helps create credentials boundaries and limit a user's ability to move laterally throughout the network without the proper authentication and approvals in place. Below is a diagram of how CyberArk allows for this architecture and protects against irreversible network takeover.

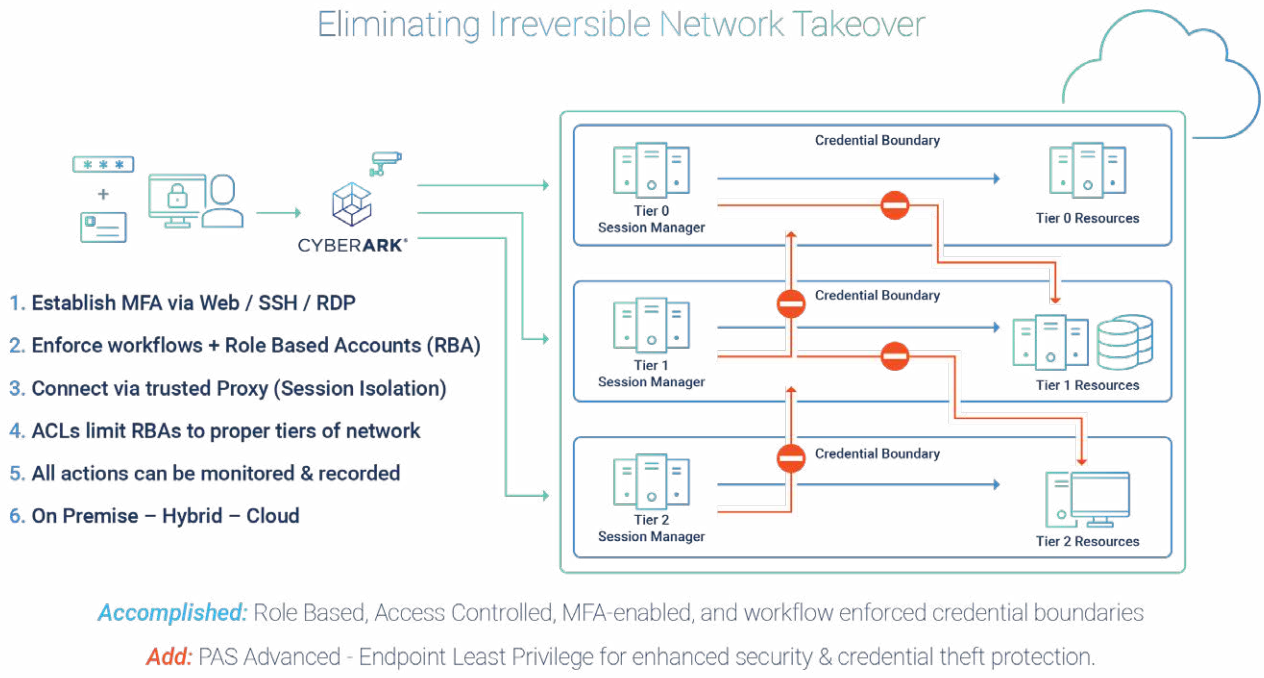


Figure 10: Elimating Irreversible Network Takeover

In addition, Privileged Access Manager's threat intelligence capabilities leverage a behavioral algorithm to monitor users' behavior and detect abnormal behavior in real time. CyberArk also can assign a risk score to sessions recorded through privileged session management. This allows for SOC teams and auditors to review the most at-risk sessions based on the behavior and commands executed inside said session. The solution integrates and pulls data from both CyberArk and SEIM tools to create a comprehensive overview of privileged activity in your environment.

Finally, leveraging adaptive MFA, Workforce Identity verifies the user with MFA/2FA, optionally blocks access from unmanaged devices and other conditions and limits access based on roles.

2.3. Trust in the requester is evaluated before the access is granted.

CyberArk certifies the identity of the requester in several ways before allowing the requester access to the privileged credentials or data. The CyberArk solution supports two layers of authentication: a primary layer and a secondary layer. The secondary layer is optional and can be set to increase the authentication strength according to your needs.

Primary authentication establishes an initial secure connection between the CyberArk interface and the CyberArk Vault server to grant access to users.

The CyberArk Vault supplies the following primary authentication options:

CyberArk Password Authentication	RADIUS Authentication	Oracle SSO (in PVWA)
LDAP Authentication	RSA SecurID Authentication (in PVWA)	SAML Authentication
NT/Windows Authentication	PKI Authentication (Personal Certificate)	Amazon Cognito Authentication

Secondary authentication strengthens the secure connection by adding an additional user identification procedure. This is mainly useful for forcing additional authentication in case of automatic authentication (SSO), such as Windows authentication, PKI authentication or Web SSO.

The following authentication methods can be used as primary authentication methods when applying secondary authentication methods:

NT/Windows Authentication	PKI Authentication (Personal Certificate)	SAML Authentication
RSA SecurID Authentication (in PVWA)	Oracle SSO (in PVWA)	Amazon Cognito Authentication

The following authentication methods can be used together with the above primary authentication methods as secondary authentication methods:

LDAP Authentication	RADIUS Authentication	CyberArk Authentication

In deployments within the federal government, CyberArk helps agencies achieve HSPD-12 compliance at LOA-4 by enforcing all users to authenticate via PIV/CAC before being granted access to CyberArk and the CyberArk safes that users have access to. The user authenticates to CyberArk with their PIV/CAC card, enters a PIN and then is brokered access to the target endpoint with elevated rights via a trusted proxy. All access to systems is controlled and monitored — should a user veer from their job role or expected task, CyberArk will have the ability to automatically alert and respond to that action.

This process also allows CyberArk to control access to systems on a per session basis and can limit the user to only the access to the allowed machine.

2.4. Access to resources is determined by dynamic policy—including the observable state of client identity, application and the requesting asset—and may include other behavioral attributes.

CyberArk provides best practices on implementing polices for access to credentials and information stored within CyberArk. The access controls are dynamic and are based on security best practices and integrations with leading identity governance solutions such as SailPoint. As rights are added or removed in AD, LDAP or the identity governance tool of the agency, CyberArk is automatically updated, and rights are adjusted based on the latest information. This ensures that users have the right level of access and permissions at all times. Access is automatically provisioned and deprovisioned in real time. When a person changes roles and leaves an agency, the access is automatically updated to reflect the change.

CyberArk Privileged Access Manager facilitates automatic full life-cycle management for Windows accounts and their service accounts in your enterprise, such as Windows Services, Scheduled Tasks, etc.

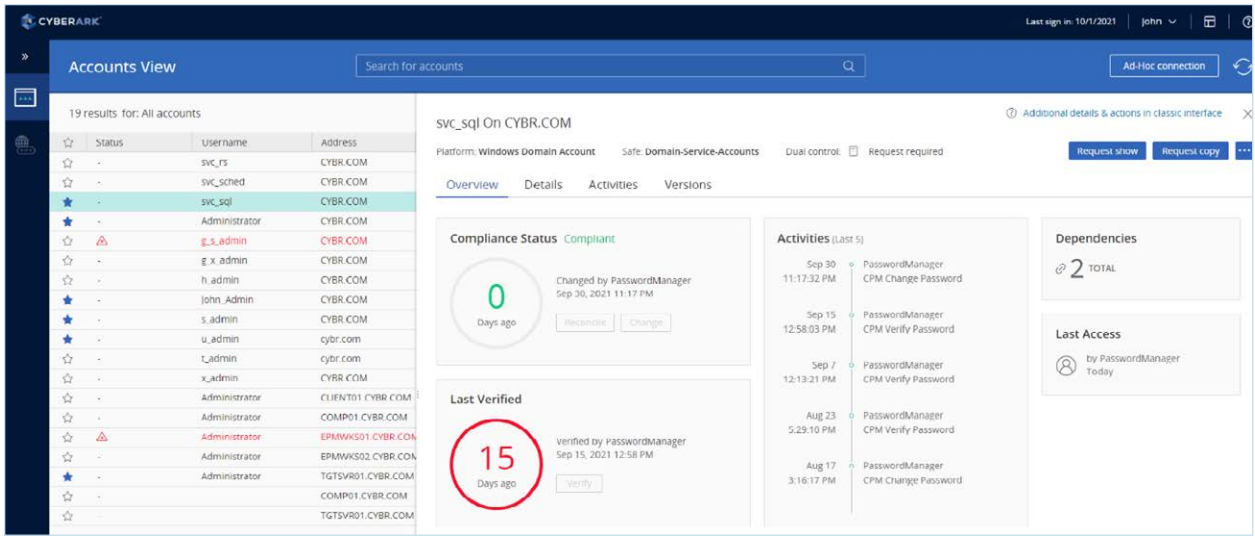


Figure 11: The 'Accounts View' highlights recent password rotation, dependencies, credential age compliance and when the account was last accessed.

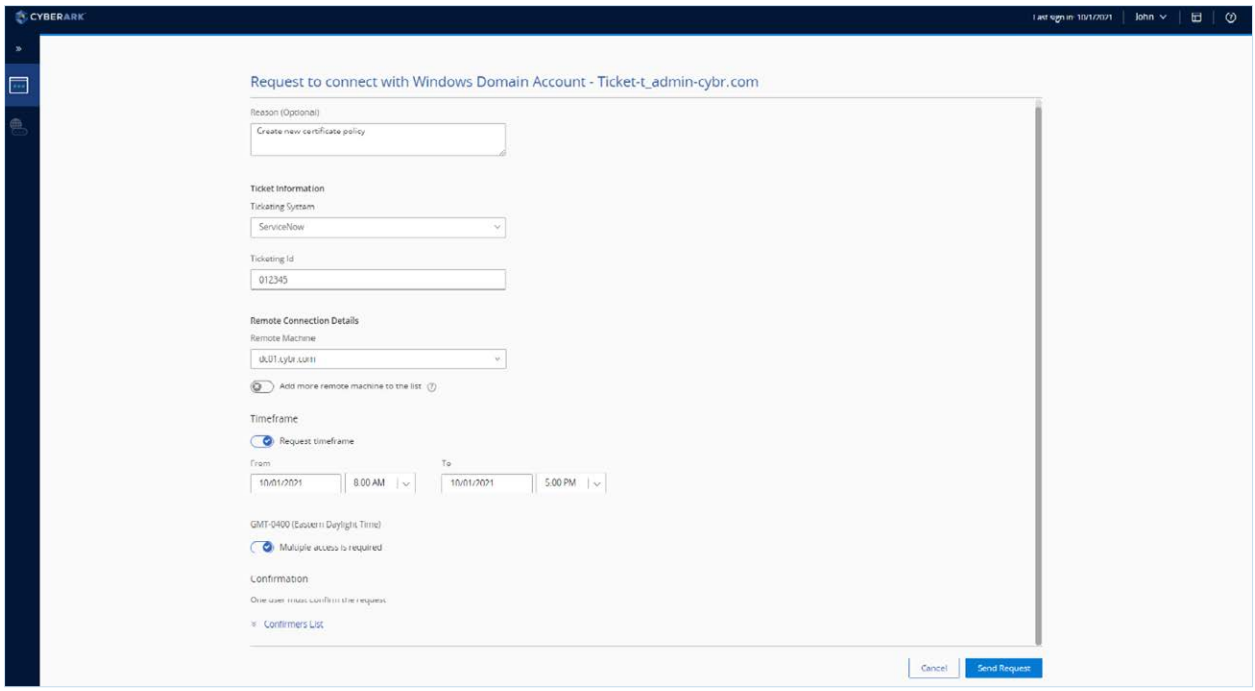


Figure 12: The CyberArk solution integreates seamlessly with ITSM solutions such as ServiceNow, to provide secure access for these privileged users.

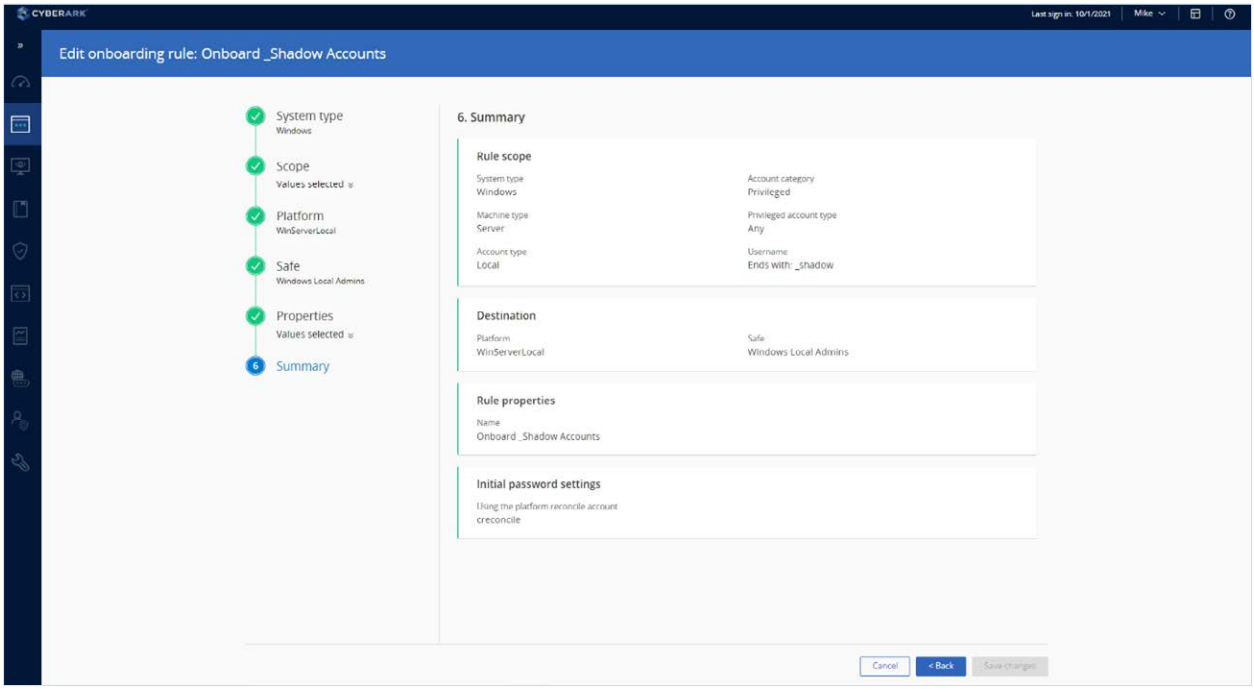


Figure 13: Example of an onboarding rule which provides scope, destination, properties and more.

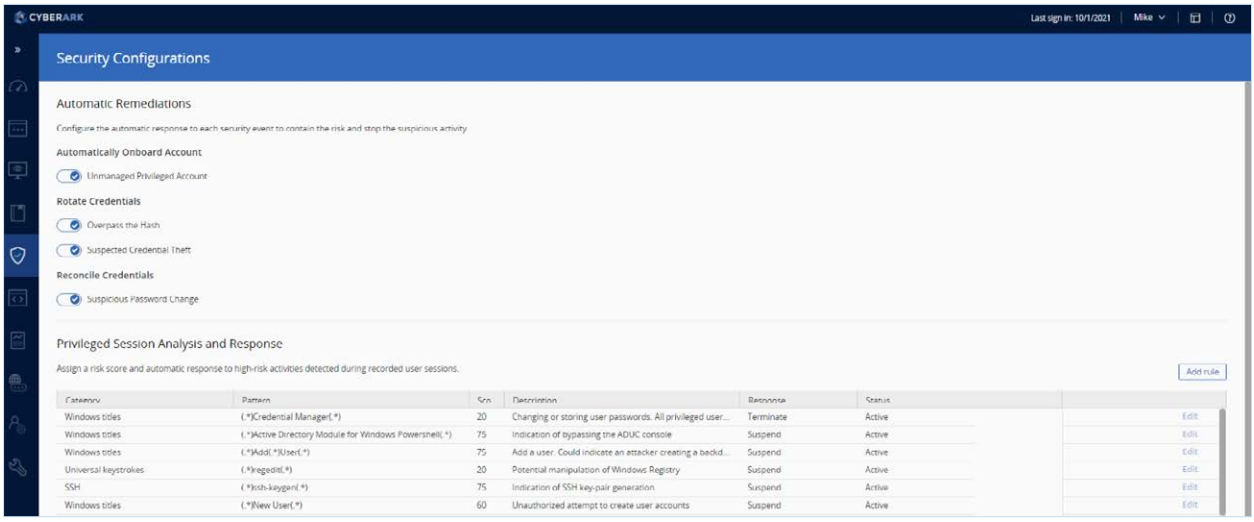


Figure 14: Automatic remediation capabilities allow for the configuration of automatic response to specific security events. to contain the risk and stop suspicious activity.

This ranges from provisioning to removal or archiving and includes all management tasks in between, ensuring complete control and secure management. This capability provides the following features:

- **Automatic provisioning for Windows local accounts** – Your enterprise's external directory can be integrated with the Password Vault to create, update and remove privileged accounts automatically in the Vault for Windows machines in Windows domains.
- **Automatic provisioning for VMware Unix/Linux guest machines Root accounts** – Your enterprise's vCenter directory can be integrated with the Password Vault to create, update and remove privileged accounts automatically in the Vault for Root or local accounts in VMware Unix/Linux guest machines.
- **Automatic provisioning for VMware ESX host Root accounts** – Your enterprise's vCenter directory can be integrated with the Password Vault to create, update and remove privileged accounts automatically in the Vault for Root accounts in VMware ESX host machines. This enables you to maintain the organization password policy across your vCenter environment.

- **Automatic provisioning for usages** – All local and domain service accounts can be detected and provisioned automatically in the Password Vault, where they benefit from all of CyberArk's standard account life-cycle management features. This greatly reduces administration overhead required by the IT personnel when machines are added or updated or when existing machines are removed from the external directory.
- **Flag domain or accounts used in Windows Services, Schedules tasks, etc., and are not currently managed by the PAM solution** – Accounts that have not been used for a while and/or are not currently managed in the Password Vault can be automatically identified and flagged. This prompts the PAM solution to notify and/or automatically start managing any potential shared/privileged domain/local account that is used in a Windows Service or other Windows usage, and is not currently managed by the PAM solution.
- **On-demand automatic detection and reporting** – Users can initiate specific automatic detection processes for local and domain service accounts and generate a report of all the detected service accounts, with or without provisioning them in the Vault.
- **Auditing automatic detection activities** – A record of all automatic detection activities is maintained in the Vault, and a report can be generated at any time with all these details, providing a full audit of every account and usage that is detected and/or provisioned in the Vault.

2.5. The enterprise ensures that all owned and associated devices are in the most secure state possible and monitors assets to ensure that they remain in the most secure state possible. No device is inherently trusted.

Within the CyberArk Workforce Identity solution, you can set a conditional rule that can be applied, restricting access only from devices enrolled into Workforce Identity. Device enrollment can be restricted only to administrators, to ensure approved device enrollments.

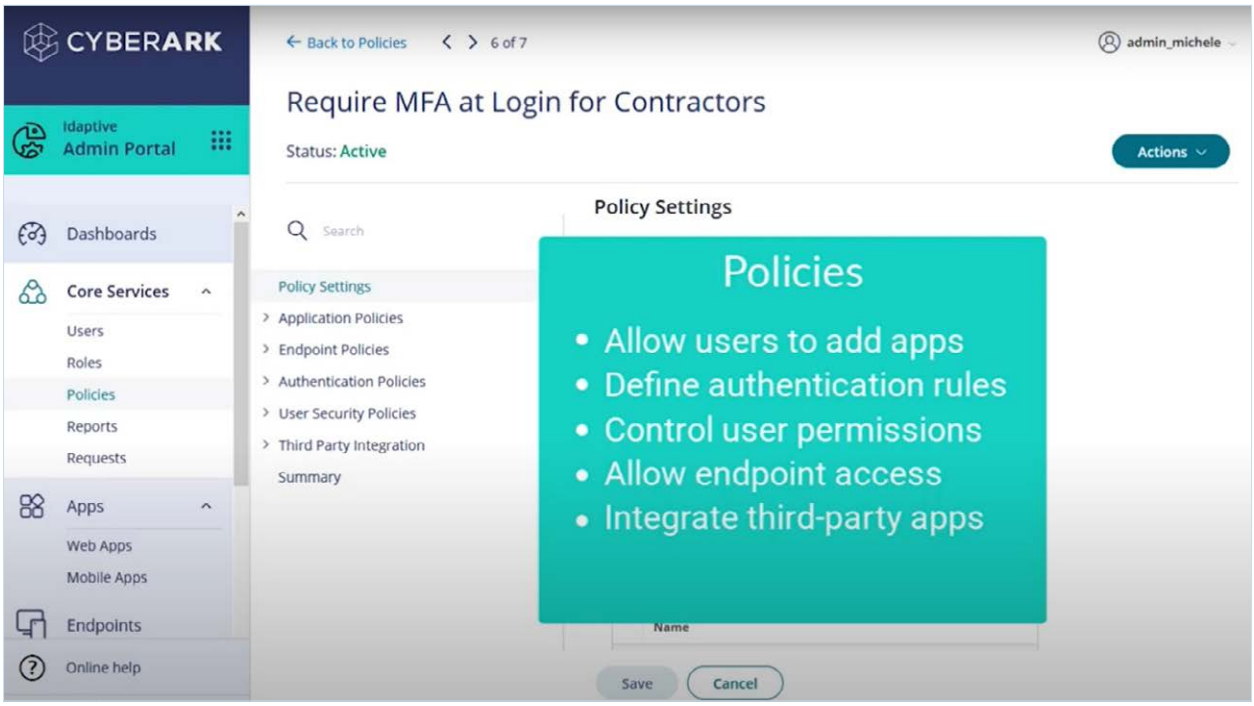


Figure 15: CyberArk Workforce Identity provides visibility to different policies, with a high-level overview of each.

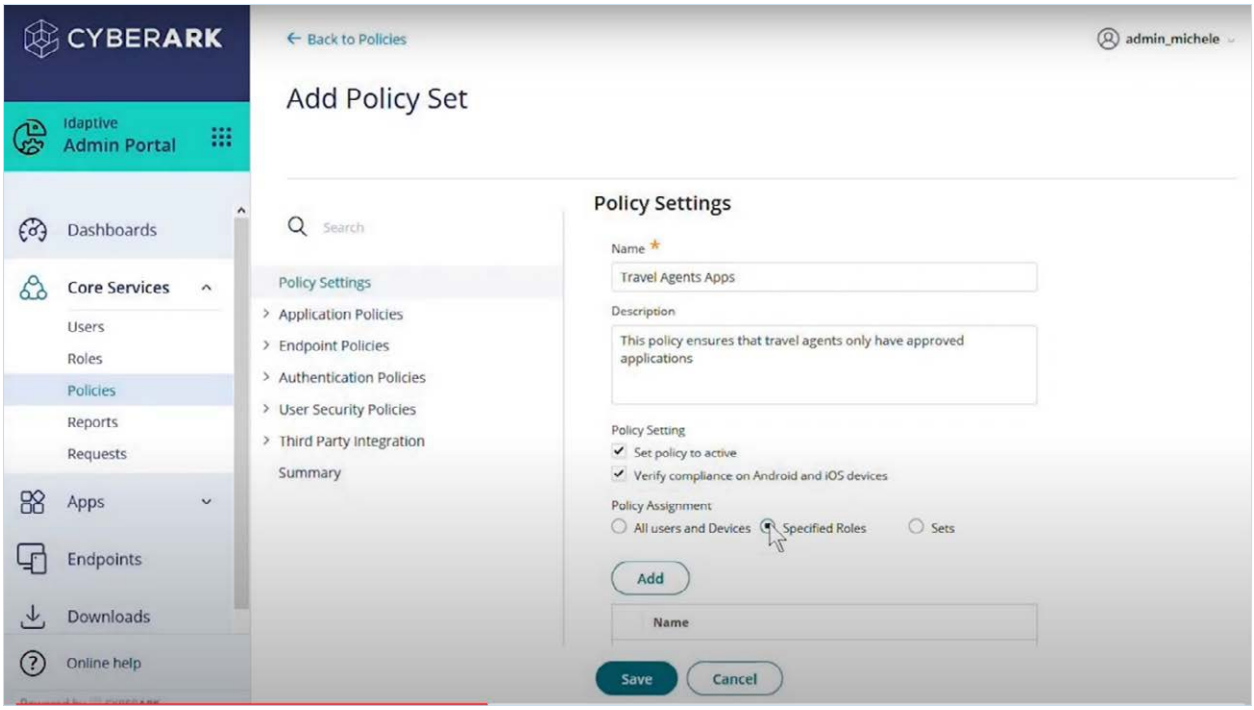


Figure 16: CyberArk Workforce Identity allows for policy assignments across all users and devices, as well as specified roles.

In addition, CyberArk integrates with marketing-leading Network Access Control tools like ForeScout to ensure that only compliant devices are on the network. Once the device is deemed compliant, its privileged access can be enrolled into CyberArk and managed to ensure access is fully controlled and monitored.

2.6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed. This is a constant cycle of obtaining access, scanning and assessing threats, adapting and continually re-evaluating trust in ongoing communication.

CyberArk allows for dynamic access after providing a high degree of assurance that the user requesting access or elevation should have the rights to do so. This is verified with every elevation and once elevated, CyberArk's threat analytics server continually verifies access and actions performed in a session. Should a user perform a task their job role forbids, their access will be stopped in real time. CyberArk's core JIT capabilities allow for temporary elevation to carry out tasks that require administrative rights on many target types. CyberArk enables users to request temporary access as well and can integrate with ticketing systems like ServiceNow, Remedy, etc. to ensure there is no standing access for administrators, while still allowing for automated approval workflows to ensure that users are not hindered by security.

2.7. The enterprise collects as much information as possible about the current state of network infrastructure and communications and uses it to improve its security posture.

CyberArk's account feed is the next-generation workflow of discovering and provisioning privileged accounts. This workflow is aligned with business processes to simplify and accelerate the deployment and management of privileged account security. The accounts feed process is divided into three main steps:

- **Discover** – Automate privileged account discovery, which is designed to quickly locate critical accounts and credentials.

- **Analyze** – Provide an easy view of all discovered accounts that enables you to analyze, determine which account is no longer needed and can be deleted, and assess the risk of each account.
- **Provision** – The scope of the accounts to manage can be provisioned in the Vault in a simple and intuitive way.

CyberArk scans your machines according to the defined source, such as Active Directory or a CSV file, to discover privileged accounts in your organization (such as Windows and Unix accounts) and their dependencies (such as Windows Services). This gives you a clear and comprehensive picture of existing accounts in your organization.

The Privileged Access Manager solution uses the CyberArk Central Policy Manager (CPM) scanner to run account discoveries. A scanner is installed with each CPM in your environment, enabling you to scan all distributed networks in your organization.

When scanning a specified domain, the CPM scanner automatically retrieves information about discovered accounts that is stored in trusted domains, without requiring additional permission. Likewise, the CPM scanner can retrieve information about discovered accounts from trusted domains in the forest trust. However, in order to discover accounts (not just information about them) in domains that are not specified as the source, the user who runs the discovery requires permissions in those domains.

All the detected accounts are displayed in the pending accounts page in the PVWA, where they can be **viewed and onboarded**, based on pre-defined critiera. Account discoveries can be scheduled to run automatically, once or at regular intervals, streamlining account management and ensuring that the pending account list contains the most up-to-date details about the privileged accounts in your environment. Users can view recurring discoveries and see when they last ran, when they'll next run and how long each one took.

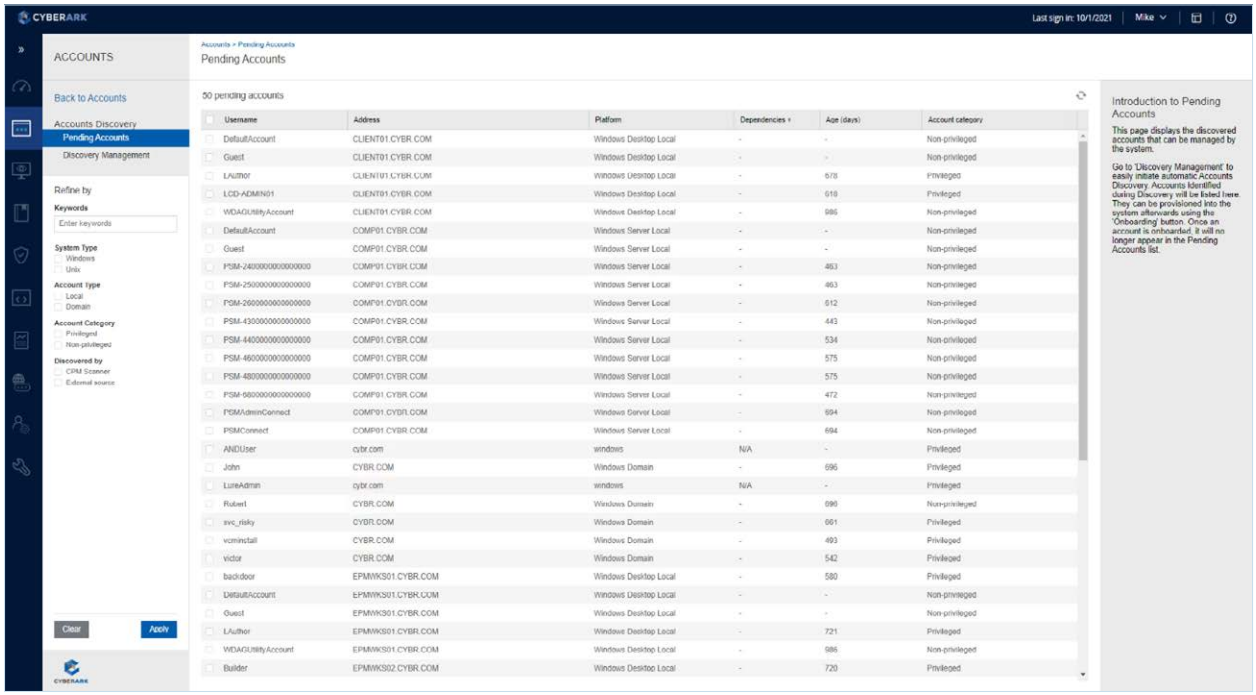


Figure 17: An example of pending accounts that have been discovered.

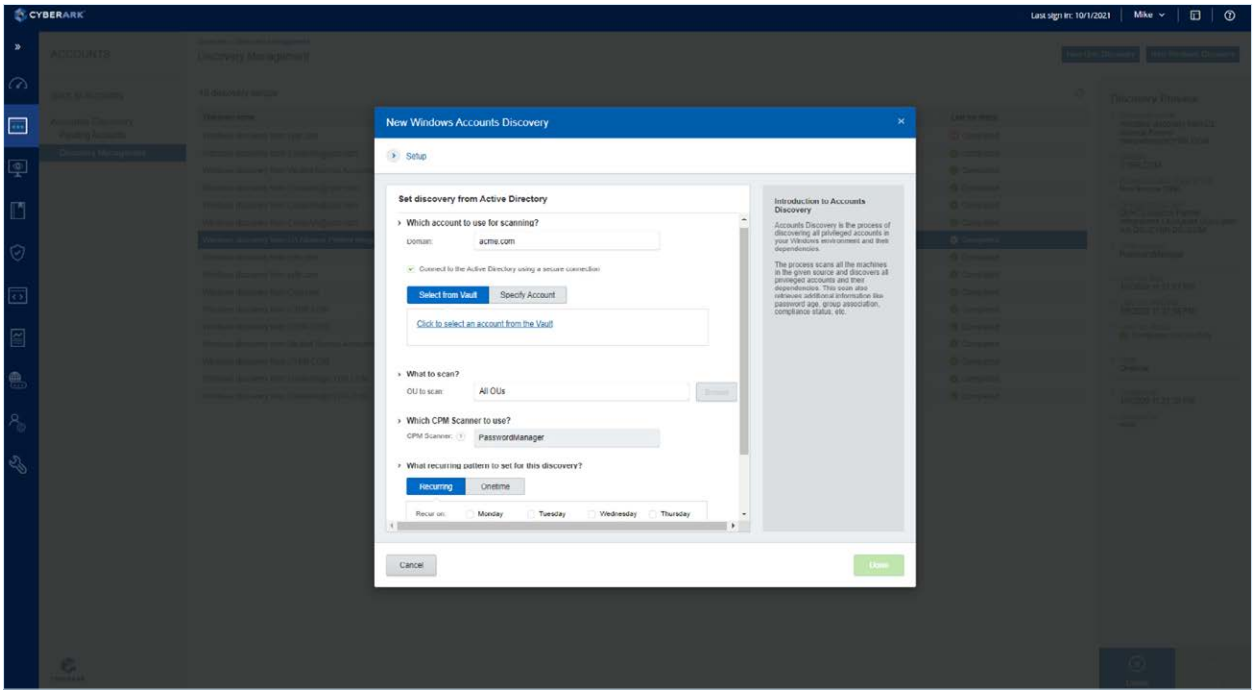


Figure 18: An example of creating a new accounts discovery scan.

Managing the privileged access of devices is critical once the device is compliant and allowed on the network. CyberArk can also integrate with state of the art Network Access Control tools (i.e., ForeScout) to automatically on-board privileged credentials once the devices is deemed to be in compliance.

Zero Trust for Privileged Users

CyberArk enables the ability to centrally secure and control access to privileged credentials based on administratively defined security policies. Automated privileged account credential (password and SSH key) rotation eliminates manually intensive, time consuming and error-prone administrative tasks, ultimately safeguarding credentials used in on-premises, hybrid and cloud environments.

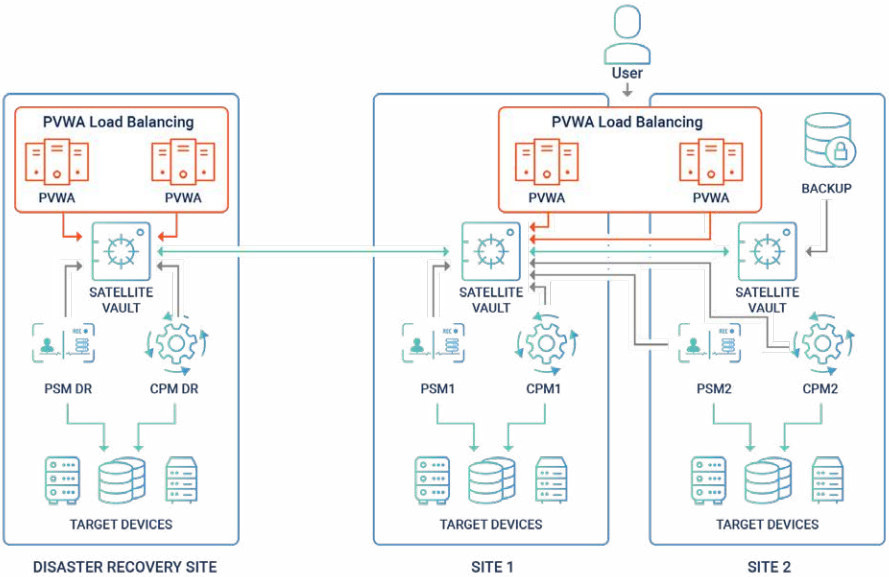


Figure 19: A standard CyberArk Zero Trust Architecture.

Zero Trust Privileged User Credential Boundaries

CyberArk helps provide secure privileged user session isolation and create credential boundaries, giving only the right people access to the privileged resources. Monitoring and recording capabilities enable security teams to view privileged sessions in real-time, automatically suspend and remotely terminate suspicious sessions and maintain a comprehensive, searchable audit trail of privileged user activity. Native and transparent access to multiple cloud platforms and web applications provides a unified security approach with increased operational efficiency.

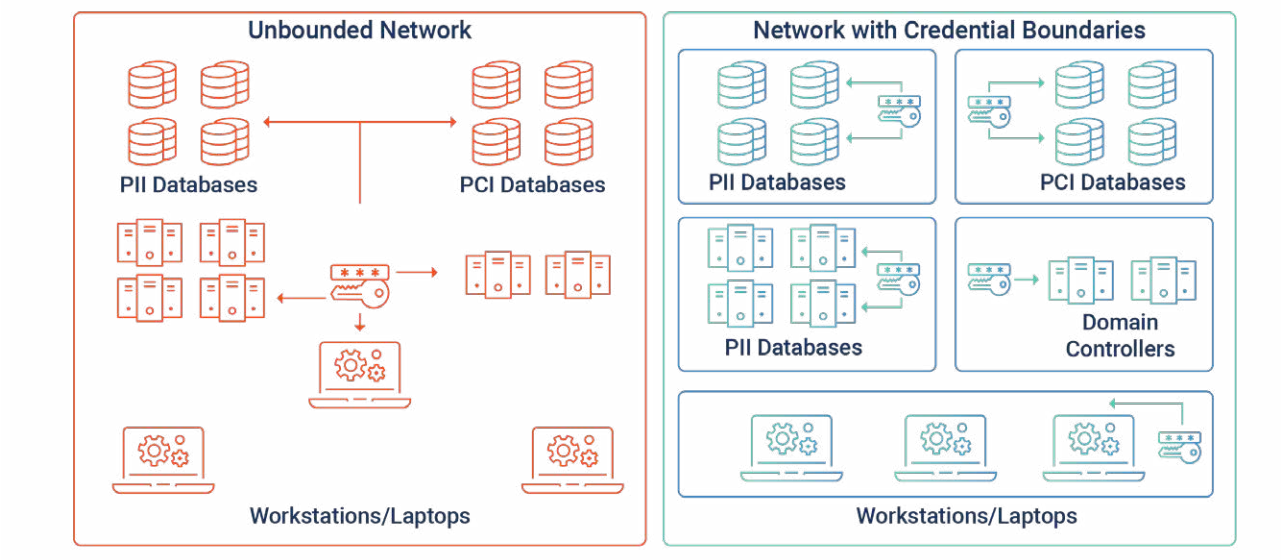


Figure 20: Mitigating privileged risk through established credential boundaries.

Zero Trust for Applications

CyberArk Endpoint Privilege Manager provides "allow" and "deny" list capabilities that quickly identify and block malicious applications. Leveraging CyberArk's Application Risk Analysis to quickly determine risk associated with any application streamlines policy definitions and aids in preventing malicious applications from running in the environment.

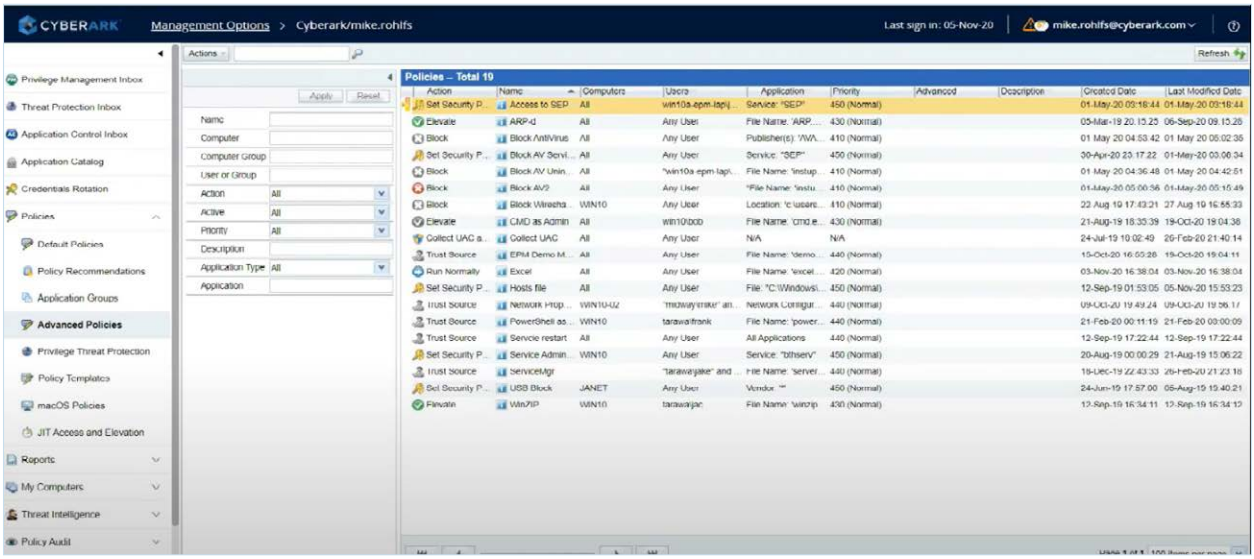


Figure 21: An example of CyberArk Endpoint Privilege Manager application control policies.

Deployment/Enforcement Mechanism					
Policy creation Mechanism	Device/Gateway Based	Enclave Based	Resource Portal Based	Device Application Sandboxing	Other
Identity Governance	Gov-A	Gov-B	Gov-C-CyberArk PAM is a policy based solution that focuses on the delegation of Privilege Resources to trusted Privileged users (established by the enterprise). CyberArk integrates with SailPoint which allows for the certification and recertification of those users. CyberArk Workforce Identity allows for you to utilize 2 factor authentications with all of your uses to ensure only trusted users have access to your resources.	Gov-D	Gov-O
Micro-Segmentation	Seg-A	Seg-B-CyberArk PAM solutions allows for the creation of Credential Boundaries that segment the access to Privileged resources by Credentials, only allowing specific trusted users to policy designated privileged resources	Seg-C	Seg-D	Seg-O
Network Infrastructure/ Software Defined Perimeters	Per-A	Per-B-CyberArk PAM solutions allows for the creation of Credential Boundaries that segment the access to Privileged resources by Credentials, only allowing specific trusted users to policy designated privileged resources.	Per-C- CyberArk End Point Privileged Manager provides Zero Trust value by allowing only Trusted applications on endpoints. The same solution has Blacklist and Greylist (sandboxing capabilities)	Per-D- CyberArk End Point Privileged Manager provides Zero Trust value by allowing only Trusted applications on endpoints. The same solution has Blacklist and Greylisting (Sandboxing) capabilities. CyberArk Workforce Identity allows for two factor authentications for all of your end users and end user resource. This enhances the Zero Trust framework	Per-O
Other Mechanism	Oth-A	Oth-B	Oth-C	Oth-C	Oth-O

This next section details how CyberArk solutions are mapped with the DHS Continuous Diagnostics and Mitigation (CDM) capabilities in the context of the Zero Trust Pillars.

The Zero Trust pillars introduce a framework that is reflected in the Continuous Diagnostics and Mitigation (CDM) program.

The United States Federal Government Continuous Diagnostics and Mitigation (CDM) Program is a dynamic approach to fortifying the cybersecurity of government networks and systems that CyberArk has both pioneered in the PAM space and also embraced for the adoption and continuous innovation in forwarding leaning technologies that elevate identity-based security.

The Department of Homeland Security developed the CDM program to support government-wide and agency-specific efforts to implement adequate and risk-based cybersecurity. The program completion is based on four phases: Asset Management, Identity and Access Management, Network Security Management and Data Protection Management.

The goal of CDM Phase II was to give agencies better visibility and security into Identity management across their networks. CDM Phase II-PRIV reduces potential loss of confidentiality, integrity and availability of data through better privileged access management. The challenge many organizations face in this area is that administrators often have broad access to multiple systems, which either cannot be multi-factor enabled or must utilize shared accounts. With the enforcement of the privileged account access control, an organization can ensure that personnel who are granted access to privileged accounts receive only the appropriate amount of access commensurate to performing their job functions and duties. Thus, a system administrator who only needs access to certain machines and specific tools to perform their job can be limited to such access with granularity and ease.

The table below maps the Zero Trust Pillars to the DHS CDM capabilities from these four phases.

ZT Pillar	CDM Capabilities	Description	CyberArk Solution
Users	Manage Trust in People Granted Access	Assesses the inherent risk to an Agency from insider attacks for the purposes of granting trust to users and authorizing each user for certain attributes.	Workforce Identity , Privileged Access Manager, Endpoint Privilege Manager, Endpoint Privilege Manager
	Manage Security Related Behavior	Ensures that authorized users with or without special security responsibilities exhibit the appropriate behavior for their role.	
Devices	Hardware Management	Discover unathorized or unmanaged hardware on a network	Secrets Manager
	Software Management	Discover unauthorized or unmanaged software on a network	Endpoint Privilege Manager
	Configuration Settings Management	Ensures that authorized security configuration benchmarks exist and contain acceptable value(s) for each relevant configurable setting for each IT asset type.	Privileged Access Manager, Endpoint Privilege Manager, Endpoint Privilege Manager
	Vulnerability Management	Discove and support remediation of vulnerabilities in IT assets on a network as defined in NIST SP 800-53 controls	

ZT Pillar	CDM Capabilities	Description	CyberArk Solution
Network	Credentials and Authentication Management	Ensures that only proper credentials are authenticated to systems, services and facilities.	Privileged Access Manager, Secrets Manager
	Managing Privileges User Access Capability	Provides an agency the assurance that users and systems have access to, and control of, only the appropriate resources. The capability identifies access beyond what is needed to meet business requirements.	Privileged Access Manager, Endpoint Privilege Manager
	Network Protection	Limits, prevents and/or allows the removal of unauthorized network connections/access via devices such as firewalls that sit at a boundary and regulate that flow of network traffic. It also includes the use of encryption to protect traffic that must cross logical boundaries and addresses physical access systems that limit unauthorized user physical access to Federal Government facilities.	Privileged Access Manager, Endpoint Privilege Manager
Applications	Credentials and Authentication Management	Ensures that only proper credentials are authenticated to systems, services and facilities.	Secrets Manager
	Managing Account Access Capability	Provides an agency the assurance that users and systems have access to, and control of, only the appropriate resources. The capability identifies access beyond what is needed to meet business requirements.	Workforce Identity, Privileged Access Manager, Endpoint Privilege Manager, Secrets Manager
	Design and Build in Security	Describes preventing exploitable vulnerabilities from being effective in the software/system while in development or deployment.	

ZT Pillar	CDM Capabilities	Description	CyberArk Solution
Automation	Manage Events	Describes preparing for events/incidents, gathering appropriate data from appropriate sources, and identifying incidents through analysis of data.	Privileged Access Manager
	Operate, Monitor and Improve	Describes audit data collection and analysis, incident prioritization and response, and post-incident activities (e.g., information sharing).	
Analytics	Data Protection	Provides data protection functions through cryptography, masking/ obfuscation, or access control. This CDM Capability includes user and entity behavioral analytics that support detection of suspected compromised accounts (people or application), endpoint devices, data exfiltration, and insider access abuse (including excessive or unauthorized access to data, functions, and privilege abuse) and provide context for security investigations.	Privileged Access Manager, Workforce Identity, Endpoint Privilege Manager

ZT Pillar	CDM Capabilities	Description	CyberArk Solution
Data	Data Discovery and Classification	Supports data protection functions through data identification, data classification and data tagging.	N/A
	Data Loss Prevention	Provides data protection functions through data loss prevention capabilities to include data protection policy management and data protection security orchestration.	N/A
	Data Protection	Provides data protection functions through cryptography, masking/ obfuscation or access control. This CDM Capability includes user and entity behavioral analytics that support detection of suspected compromised accounts (people or application), endpoint devices, data exfiltration and insider access abuse (including excessive or unauthorized access to data, functions and privilege abuse) and provide context for security investigations.	Privileged Access Manager, Endpoint Privilege Manager
	Data Spillage	Provides data breach/ spillage response actions.	N/A
	Information Rights Management	Provides data protection functions through information rights management capabilities using fine-grained access control to encrypted data.	Privileged Access Manager, Endpoint Privilege Manager,

CyberArk also views the definitions of these categories as fluid in the sense that each layer of security must overlay with one another to provide a cohesive and encompassing solution. Rather than providing point solutions or focusing only on one element of the Identity framework, CyberArk approaches identity as a whole. In doing so, CyberArk's portfolio of technologies allows security teams to manage and monitor user access from the moment of connection through the lifecycle of their engagement with Federal assets. Below we have summarized how we would group and overlay these various elements of Zero Trust to ensure a resilient and robust Identity Security posture.

Users/Analytics

Managing security based on User Related Behavior: CyberArk solutions empower federal agencies to quickly identify and disrupt abnormal behaviors with customized behavioral analytics technology that detects and alerts on abnormal, suspicious privileged account behavior.

Data/Devices

Manage credentials and authentication: CyberArk solutions help federal agencies secure and manage privileged credentials with a multi-layered solution that fully protects, manages and monitors privileged passwords and SSH keys in a tamper-proof digital vault

Applications/Automation

Manage account access/manage privileges: CyberArk solutions help IT and security teams achieve the balance between security and operational needs by enabling end-user productivity while controlling privileges for security reasons.

How To Get Started: Establishing Identity Security Success with the Cyberark Blueprint

CyberArk has developed a prescriptive blueprint to help organizations establish and evolve an effective PAM program. The CyberArk Identity Security Blueprint is designed to defend against three common attack chain stages used to steal data and wreak havoc. Simple, yet comprehensive, the CyberArk Blueprint provides a prioritized, phased security framework that closely aligns PAM initiatives with potential risk reduction, helping federal agencies address their greatest liabilities as quickly as possible.

The CyberArk Blueprint was built with contemporary organizations and extensibility in mind. It prescribes PAM controls and best practices for organizations using conventional on-premises infrastructure and software development methods, as well as for agencies embarking on digital transformation projects such as migrating infrastructure to the cloud, adopting CI/CD practices, optimizing processes through robotic process automation or implementing SaaS solutions for business-critical applications.

The CyberArk Blueprint reflects the combined knowledge and experience of CyberArk's global Sales, Sales Engineering, Security Services and Customer Success organizations. As the undisputed leader in Identity Security, CyberArk is uniquely positioned to deliver a thorough and effective PAM blueprint:

- CyberArk solutions are trusted by 7,000+ customers, including more than 50% of the Fortune 500, across a wide range of industries including financial services, insurance, manufacturing, healthcare and tech.
- CyberArk's Incident Response and Red Team have been front and center in helping both the public and private sector recover from some of the largest breaches of the 21st century. Additionally, CyberArk draws on the insights of its Threat Research and Innovation Lab.
- CyberArk Security Services and Customer Success organizations have decades of real-world implementation and support experience, and have a detailed, first-hand understanding of PAM risks and best practices.
- CyberArk is widely recognized as a leader in PAM in all major industry analyst reports.

Learn more by visiting **www.cyberark.com/blueprint**.

CyberArk's Commitment to the Federal Government

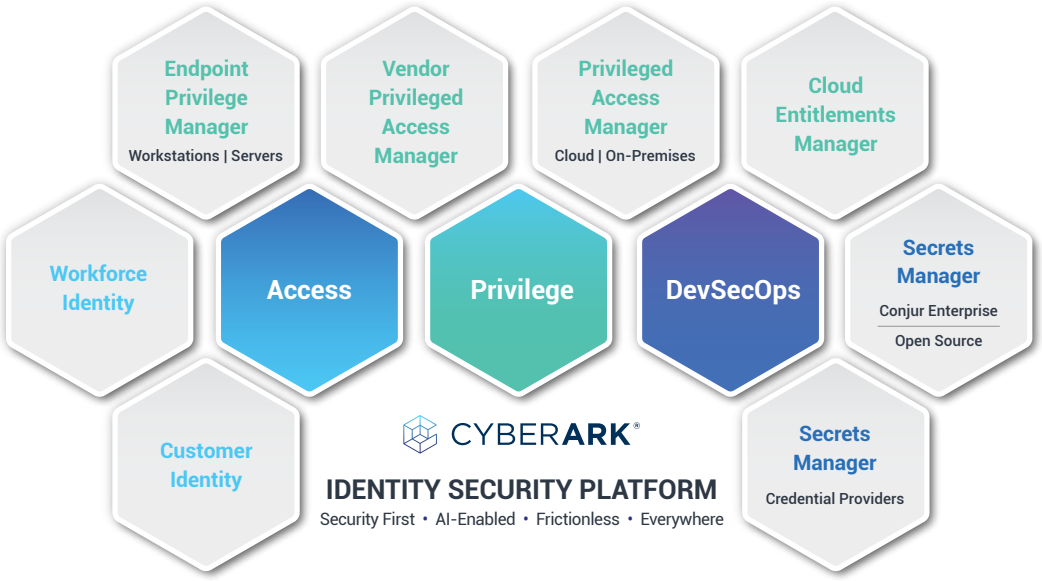
The CyberArk Privileged Access Manager Solution has been independently validated and awarded an Evaluation Assurance Level (EAL) 2+ under the Common Criteria Recognition Agreement (CCRA). We've received the U.S. Army Certificate of Networthiness (CoN) enabling the streamlined implementation of the CyberArk 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). Prioritizing both obtaining and maintaining these certifications demonstrates CyberArk's continued commitment to helping federal government agencies proactively protect privileged users and credentials across networks.

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 that 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

Through CyberArk's Identity Security Platform, federal agencies can introduce the necessary controls that both mitigate the risk of advanced cyber attacks and align to the requirements of the Department of Defense's Zero Trust Reference Architecture. CyberArk is the recognized Identity Security market leader and the most widely deployed PAM solution in the federal government. As a growing, publicly traded company on the NASDAQ stock exchange, CyberArk continues to drive growth with strategic investments bringing innovation to the cybersecurity segment as the threat landscape evolves. CyberArk is uniquely positioned for continued R&D investment and demonstrates commitment to delivering cybersecurity solutions with the highest level of efficacy. The maturity and breadth of the CyberArk solution provides the federal government with a comprehensive roadmap for their PAM program. The company's stability and commitment to the federal government as demonstrated by government certifications, accreditations and ATOs make CyberArk a strategic and long-term security partner to the federal government.



WHY CYBERARK

Most Complete and Extensible Identity Security Platform
Solving the full range of hybrid to multi-cloud identity challenges with a security-first approach.

Architected for the Federal Government
Built and ready platform that enables digital business and supports the workforce of governmental agencies.

Broadest Integration Support
Most out-of-the box integrations to solve identity security across federal government agencies.

Identity Security Innovator
Pioneered the key solution to solve the hardest IT security problem. Continues to lead the market with dynamic solutions to address new and emerging threats.

Proven Expertise in Securing Identities
Long tail of experience and tenure with federal government agencies provides the deepest and widest institutional knowledge of identity security challenges.

.

LEARN MORE

About CyberArk

CyberArk is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security offering for any identity – human or machine – across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets.

CYBERARK®

©Copyright 2021 CyberArk Software. All rights reserved. No portion of this publication may be reproduced in any form or by any means without the express written consent of CyberArk Software. CyberArk®, the CyberArk logo and other trade or service names appearing above are registered trademarks (or trademarks) of CyberArk Software in the U.S. and other jurisdictions. Any other trade and service names are the property of their respective owners.

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. U.S., 10.21 Doc. 308725

THIS PUBLICATION IS FOR INFORMATIONAL PURPOSES ONLY AND IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER WHETHER EXPRESSED OR IMPLIED, INCLUDING WARRANTY OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, NON-INFRINGEMENT OR OTHERWISE. IN NO EVENT SHALL CYBERARK BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND IN PARTICULAR CYBERARK SHALL NOT BE LIABLE FOR DIRECT, SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE OR LOSS OF USE, COST OF REPLACEMENT GOODS, LOSS OR DAMAGE TO DATA ARISING FROM USE OF OR IN RELIANCE ON THIS PUBLICATION, EVEN IF CYBERARK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.