CYBERARK®

WHITEPAPER

NIST SP 800-53 Revision 5

Meeting the Requirements of Effective Security Controls with CyberArk

Table of Contents

Executive Summary

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 and associated publications provide guidance for the selection of security and privacy controls for information systems and organizations. While the catalog is written from a U.S. Federal Government perspective, organizations around the world use the controls as part of the NIST Risk Management Framework because they provide a freely available and comprehensive set of tools and processes.

Revision 5 of the control catalog provides the next generation of security and privacy controls and supports a proactive and systematic approach to cybersecurity. These controls are a vital foundation for important compliance initiatives (such as those for protection of Controlled Unclassified Information, or CUI, and conformance to the U.S. Cybersecurity Maturity Model Certification (CMMC) program) and enable valuable infrastructure improvements (such as implementation of Zero Trust architecture).

NIST has also released criteria for validating that the controls are correctly implemented (SP 800-53A) and for ensuring that the controls are appropriate, depending on the sensitivity and criticality of the systems protected. That criteria calls for testing security solutions to confirm efficacy and examining results for the many important security, privacy and supply-chain controls to be implemented — results that are readily seen and proven through the CyberArk solutions.

This whitepaper illustrates how CyberArk addresses the NIST SP 800-53 Revision 5 requirements in its products.

CyberArk solutions help federal agencies implement effective controls for privileged and administrative identities and access to sensitive information.

Protecting the Privileged Identities

In most organizations today, typical IT environments are comprised of hundreds or thousands of servers, databases, virtual machines, network devices and applications, all controlled and managed by a variety of privileged and administrative identities, such as:

- **Shared administrative accounts –** "super user" privileges often anonymously shared among IT staff. Examples include Windows Administrator, UNIX root, an Oracle SYS account or AWS Root Access. They can be used to modify system and service configurations, access entire databases, change security settings on network devices, gain control over applications, reconfigure audit logs and so on.
- **Application and service accounts –** machine identities found in virtually every piece of hardware, software and application within an organization, including virtual environments. These accounts typically have broad access rights to underlying information and are a particular source of cyber risk when credentials are "hard coded" or embedded in application code.
- **Emergency accounts –** elevated privileges used to fix urgent problems, such as in cases of business continuity or disaster recovery. They are often called break glass, fire call or fireIDs.
- **Identities used for operational access –** dedicated accounts — or cloud Identity and Access Management (IAM) roles — created specifically for the purpose of operational, administrative access in ephemeral, cloud-hosted infrastructure. In the wrong hands, this operational access can be used to steal data, launch cryptomining operations or take cloud-hosted systems and applications offline.

Inadequate security controls for privileged and administrative identities, including those that are poorly implemented or maintained, create significant risks for an organization. For example, without the benefit of a privileged access management solution, it is difficult to sufficiently monitor usage of privileged identities. With shared or generic accounts, systems do not usually track which individual users log in as administrators — merely that an administrative login occurred. Privileged account credentials like admin passwords or SSH keys can be more susceptible to compromise because they are typically changed less frequently than personal non-privileged accounts, if at all.

Administrative, application or break-glass accounts can often be impossible to disable due to the high potential for disruption to business. Moreover, manual processes to manage and update these accounts are costly and prone to error. These challenges demonstrate the need for effective security planning, including application of robust security controls and control enhancements. For example, control enhancement AC-2 (1), Automated System Account Management, helps to support the management of system accounts and contributes to an effective Zero Trust Architecture solution.

Organizations also face a growing need for secure, authorized access to their most sensitive information. Current trends, such as the rise of mobile workforces and expanding use of service providers, further increase the risks that sensitive information will fall into the wrong hands. Organizations must know exactly who is accessing and sharing confidential files, documents and reports, and balance availability with security.

These challenges are accentuated by increased implementation of virtualization, containerization and microservices. The dynamic and distributed nature of these environments depends upon authentication mechanisms, yet those same mechanisms represent an attractive target for external attackers and malicious insiders. These risks are amplified with widespread adoption of cloud-first strategies and DevOps.

Implementing Effective and Efficient Controls with CyberArk Solutions

Security control implementation, as part of an overarching security plan and operation, helps organizations manage risk and protect the enterprise. While many entities must use these controls to achieve compliance with contractual or regulatory requirements, the primary purpose of the effective implementation of controls is to ensure that adequate safeguards are in place to protect security and privacy of critical resources. These controls must be efficient, too, to ensure that those safeguards can be applied in cost-effective and practical ways.

> Predefined policies and workflows help streamline the implementation of controls.

Demonstrating that effectiveness and efficiency in accordance with assessment and monitoring activities (such as those described in SP 800-53A) is an important element of maintaining a secure solution.

To help agencies implement the necessary controls for managing the risks of privileged and administrative identities and access to sensitive information, CyberArk solutions:

- **Manage and control access to all privileged accounts –** including automating password changes and rendering hard-coded application credentials invisible to all developers and administrators
- **Isolate, control and monitor privileged access –** to sensitive servers, databases or virtual machines
- **Enforce least privilege access across an organization –** from employee workstations to the public cloud
- **Thoroughly authenticate all identities, workforce and privileged –** with adaptive multifactor authentication

Realizing Key Benefits

With CyberArk solutions, federal agencies can implement effective and efficient controls to:

- Control privileged activities and access to sensitive information
- Protect critical assets
  - Including key infrastructure (on-premises and in the cloud) like operating systems, servers, databases and other information and technology, such as private/sensitive data and industrial control systems middleware
- Secure cloud environments
  - Securely manage standing privileged access for shared accounts in cloud environments
  - Securely provision access just in time for federated access in cloud environments
- Achieve consistent enforcement of policy across the entire organization
  - Replace ineffective and inefficient manual processes with reliable automated solutions

- Ensure comprehensive audit logging
  - Track individual administrators' command-level activities
  - Record sessions to sensitive business applications for workforce identities
- Increase situational awareness and visibility over privileged users and sensitive documents
- Reduce overhead and increase productivity
  - Decrease or reassign staff to more productive work
- Detect advanced threats with real-time session monitoring of privileged access and activity
- Leverage existing investments
  - Streamlined integration with an organization's identity infrastructure, including directories, provisioning, monitoring, security and authentication systems
- Support a Zero Trust approach that protects privileged access in areas affected by supply-chain risk and other third-party considerations
- Safeguard information using tamper-proof storage based on FIPS 140 (Federal Security Requirements for Cryptographic Modules) validated cryptography

Addressing the Controls

A majority of the NIST SP 800-53 controls addressed by CyberArk solutions are among those included in the control baselines from NIST SP 800-53B. That guide describes selected controls that, if correctly implemented and determined to be effective, meet security and privacy requirements defined by applicable laws, executive orders, policies, regulations and directives. Those privacy and security baselines provide a starting point for effective security, and CyberArk helps to apply many of those control families, including the following.

Access Control

The Access Control family deals with managing and enforcing access rights, as well as authorizing and restricting access to information. It covers issues of account creation and assignment, as well as when and how credentials should be used. Therefore, it contains many guidelines regarding the special care and attention that needs to be given to privileged accounts and their elevated access rights. For example, the Account Management control guidance states, "Users requiring administrative privileges on information system accounts receive additional scrutiny by organizational officials responsible for approving such accounts and privileged access."

CyberArk solutions can be used to address the full set of access control recommendations as they relate to managing privileged and administrative identities, including shared/group accounts, for meeting or even exceeding baseline requirements. This includes comprehensive privileged account lifecycle management, discovering and securing the accounts, enforcing access control policies and auditing privileged access. Organizations can also control privileged sessions, including who can initiate sessions and for how long, as well as restrict and monitor third-party access to privileged accounts used for operations on infrastructure or sensitive business applications.

For accessing sensitive information, the Access Control family specifies several controls regarding how information should be controlled, encrypted, accessed and shared. CyberArk provides a complete solution for storing and sharing sensitive information, whether inside the organization or with other entities.

Audit and Accountability

The Audit and Accountability family involves determining audit events and ensuring those events are adequately recorded and analyzed, and the audit records are reliable and protected. The control "AU-3: Content of Audit Records" specifically addresses the requirement for individual accountability. It lists the required data for each audit record and states, "The information system generates audit records containing information that establishes what type of event and the identity of any individual associated with the event."

CyberArk solutions helps organizations to meet the requirements of the Audit and Accountability family by providing extensive audit logging for events involving privileged accounts and access to sensitive information. Examples include logging the use of a privileged password or the transfer of a sensitive file, including the identity of the individual, recording sessions to web applications and sensitive windows infrastructure, and logging all commands in sessions to Linux infrastructure.

All CyberArk logs are properly time stamped, cryptographically protected and stored in the tamper-proof digital vault, referenced to a specific user in the system and stored for as long as required by the organization. CyberArk products can also generate alerts on specific occurrences and feed into Security Information and Events (SIEM) products, including HP ArcSight, McAfee ESM and RSA enVision.

Identification and Authentication

In today's hybrid and multi-cloud world, identity is the new perimeter. Because identities can be an attack path to an organization's most valuable assets, the Identification and Authentication family encompasses controls related to establishing and verifying the identity of users. The control "IA-2: Identification and Authentication (Organizational Users)" requires users be uniquely identified. The control asserts, "The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users)." It can be challenging to meet this requirement, especially for privileged accounts that are shared among the IT staff. Shared accounts diminish accountability and create vulnerabilities. The control "IA-5 Authenticator Management" is concerned with the management and use of authenticators, such as passwords. The requirements include ensuring authenticator strength, defining their lifetime, updating them periodically, protecting them and managing their revocation. CyberArk Privileged Access Manager solutions allow organizations to set custom organizational policies for the length, strength and rotation frequency of all such credentials.

For privileged and administrative accounts, CyberArk solutions uniquely identify all users, including individual use of shared accounts. Complete lifecycle management for privileged account passwords is provided, helping organizations meet the authentication management requirements.

IA-5 Control Enhancement (7) addresses the key problem of hard-coded, clear-text passwords in applications by requiring that "[the] organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys." CyberArk solutions eliminate hard-coded passwords. They ensure periodic password refresh with no system downtime and provide enhanced secure authentication and a secure cache mechanism in the event of a network outage.

Incident Response

The incident response controls ensure that an enterprise is adequately prepared to detect, respond to and recover from various security and privacy events. In addition to CyberArk's solutions that help the organization protect against many known attack vectors, threat analytics provide real-time incident detection and containment capabilities. Integrated with recordings of all privileged sessions, threat analytics provide risk scores to accelerate review and response to suspicious activity. CyberArk supports important solutions to many of these controls, including management of Insider Threats, Incident Monitoring and Automated Reporting.

Supply Chain Risk Management

SP 800-53 Rev. 5 includes a new SR family of controls focused on supply chain risk management policy and procedures. Several of these controls were previously included in other control families. Because organizations are increasingly interconnected and rely more heavily than ever on external service providers and other third-party partners, it remains imperative that supply chain risks be considered part of an overarching risk universe.

CyberArk provides multiple solutions to support a defense-in-depth methodology, such as Remote Access, which provides secure privileged access for external vendors that need to access critical internal systems and products for securing the software development/DevOps software supply chain. All privileged sessions conducted by remote vendors are enabled just in time, eliminating the risk of adding unnecessary standing access to critical systems. Simultaneously, all vendor sessions are fully monitored. The effectiveness of these solutions is demonstrated as organizations follow the assessment procedures, methods and monitoring as described in NIST SP 800-53A.

Confronting Advanced Threats

NIST continues to highlight the importance of preparing for and confronting advanced persistent threats (APTs). NIST defines an APT as "an adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives." APTs work to pursue objectives over an extended period of continuous adaptation; if organizations are to thwart such attacks, they must be equally adaptive and alert.

NIST has published SP 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information (CUI), which focuses on requirements to help prepare and defend against APTs. SP 800-53 also provides specific guidance regarding APTs and points out several key controls to consider. NIST has also published SP 800-171A and 172A publications that describe assessment criteria regarding methods for protecting CUI. It describes procedures by which assessors and monitors prove solution effectiveness through examining operations, interviewing personnel and partners, and testing the security mechanisms. These assessments demonstrate that CyberArk solutions support the implementation of many of the recommendations applicable to APTs, including:

- AC-6 (9) Least Privilege | Log Use of Privileged Functions
  - CyberArk solutions audit all access to privileged functions.
- CM-5 (4) Access Restrictions for Change | Dual Authorization
  - CyberArk provides "Dual Control," which requires that an additional authorized administrative user approve requested actions before being granted such things as configuration changes.
  - Dual Control is available via the CyberArk mobile application.
- SC-29 Heterogeneity
  - CyberArk products integrate with the full range of diverse operating systems, applications, databases, security appliances, network devices, directories, virtual machines and storage found in today's IT environments.
- SC-51 Hardware-Based Protection (that includes the former Rev 4 control SC-34 (3) Non-Modifiable Executable Programs)
  - CyberArk technology uses hardware-based protection mechanisms.

"Assurance" is another important aspect of defending against APTs. It advises that as organizations become susceptible to APTs, increased levels of assurance may be required. Many controls related to assurance are clustered in the Systems and Services Acquisition (SA) family. CyberArk can address many of the SA controls. The company provides proven technology that is certified by ICSA labs and FIPS 140 compliant. CyberArk solutions are based on highly acclaimed security engineering principles and best practices.

Overall, CyberArk solutions can help organizations implement a wide range of controls from each of the control families. The following sections in this document detail how CyberArk solutions address the controls of NIST SP 800-53 Rev. 5 and provide an overview of the product suites offered by CyberArk.

Addressing NIST SP 800-53 REV. 5 Recommendations and Assessments

As part of the NIST Risk Management Framework for Information Systems and Organizations, SP 800-53 Revision 5 recommends that organizations determine security controls by first categorizing information systems. This categorization is based on the potential impact of certain events that could jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions and protect individuals. By first categorizing information systems as low impact, moderate impact or high impact, organizations then select controls supplemented with control enhancements to attain "LOW," "MOD(ERATE)" or "HIGH" security baselines (based in the companion SP 800-53B publication). They can then tailor the controls to their own requirements, including the use of additional control enhancements provided in the catalog.

The table below describes how CyberArk solutions help organizations implement the controls and control enhancements provided in NIST SP 800-53 Revision 5. CyberArk solutions can be used to help meet or exceed LOW, MOD or HIGH baselines. Assessments, as described in SP 800-53A, demonstrate through observation and interviews that these solutions achieve the right level of risk management. For each control family, the table lists selected controls that can be addressed with CyberArk solutions and provides an explanation of how. Where applicable, some information on specific control enhancements is also provided.

Family: ACCESS CONTROL	
Describes controls to manage how access and authorization policies and procedures, including those applying the principle of least privilege, are implemented, enforced and monitored	
AC-1 POLICY AND PROCEDURES Involves development of an access control policy as well as procedures to facilitate implementation of policy and associated controls, including periodic reviews and updates	With CyberArk solutions, organizations can consistently implement policy and procedures and effectively implement automated controls for privileged access and access to sensitive documents. Predefined policies and workflows help streamline implementation of controls. Built-in, audit-ready reports enable efficient reviews and flexible architecture, and management environments provide support for updating controls. Privileged access management (PAM) solutions provide multiple layers of customization for policies governing access to privileged credentials.

Family: ACCESS CONTROL	
AC-2 ACCOUNT MANAGEMENT Covers full range of activities related to managing accounts	CyberArk provides comprehensive solutions for automating all the processes associated with privileged account lifecycle management. Identifying accounts is supported through the auto discovery function, while accounts can also be uploaded in bulk to CyberArk either manually or via automation. Automatic discovery and provisioning of accounts ensures that even accounts hidden in services, scheduled tasks, application pools or local administrator groups are discovered and managed securely according to organizational policy. All account information is held within CyberArk's patented digital vault. Assigning account managers is facilitated using "safes" within the vault; group managers are provided with restricted access to account information for their particular workgroup. For establishing conditions for group or role membership, organizations can leverage the group structure already created in their LDAP database, such as Active Directory. Granular account control for privileged identities is provided; in addition to group and role membership, additional privileges and attributes can be specified for individual accounts. Through LDAP integration, account changes (including creation, modification or removal) are automatically propagated to the information held in the vault. Entities can set up alerts for when users are transferred or terminated. All usage of privileged accounts is authorized and monitored. For example, before using their account, users must log in; all major authentication methods are supported, including CyberArk's own multifactor authentication capabilities. Further, "Dual Control" requires that an additional authorized user approve requested actions before granting them. All privileged access is recorded and audit logs protected in tamper-proof storage. Organizations can also do real-time monitoring of privileged sessions and in certain cases, automatically terminate risky sessions as they occur.
	Reviewing accounts for compliance with account management requirements is securely enabled by allowing auditors to log in and access audit logs and usage reports, etc. without giving them access to account credentials. CyberArk solutions also handle the requirement to reissue shared/group account credentials when individuals are removed from the group. The account administrator can be automatically notified when an individual is removed from a group in LDAP and immediately change the shared/group password, or the system can be set up to issue a one-time password so that every time an account is used, the password is reissued. This control has many control enhancements, all of which can be addressed by CyberArk solutions for managing privileged accounts, including: • Automated system account management • Removal of temporary/emergency accounts • Disable inactive accounts • Automated audit actions • Role-based schemes • Restrictions on use of shared/group accounts • Shared/group account credential termination • Usage conditions • Account monitoring/atypical usage • Disable accounts for high-risk individuals

Family: ACCESS CONTROL	
AC-3 ACCESS ENFORCEMENT Deals with enforcing approved authorizations for logical access to information and system resources in accordance with policies	CyberArk's policy-based solutions help automatically enforce privileged access rights so that only authorized privileged users or applications can gain logical access to the information or system resources they are entitled to access. 800-53 Rev. 5 adds five new enhancements for this control, including Restrict Access to Specific Information Types, that are directly supported by CyberArk privileged access management. Many of the control enhancements can be supported by CyberArk solutions, such as: • Dual authorization • Mandatory access control • Discretionary access control • Security-relevant information • Role-based access control • Revocation of access authorization • Access enforcement by systems and applications
AC-5 SEPARATION OF DUTIES Involves defining the separation of duties of individuals and ensuring access authorizations support defined separation of duties	The patented digital vault technology inherently supports separation of duties, allowing users to access only information that is relevant to them (files, privileged credentials, etc.). The vault is divided into safes that are accessed by users based on their specific permissions and without knowledge of the existence of other safes
AC-6 LEAST PRIVILEGE Covers the concept of least privilege, which allows only authorized accesses for users (and processes acting on behalf of users) that are necessary to accomplish assigned tasks	With CyberArk solutions, organizations can restrict users and applications to only the necessary privileged access required to perform their assigned tasks, based on pre-defined policies. Workflows such as dual approval of password usage, email notifications and ticketing system integration for ticket validation and reasoning are just some of the many workflows that can be implemented to support least privilege. Simultaneously, additional CyberArk solutions provide least privilege on endpoints via removal of local admin rights and application control settings, as well as the ability to implement least privilege policies in the public cloud via detection and removal of excessive permissions. Many of the control enhancements can be addressed by CyberArk solutions, including: • Authorize access to security functions • Network access to privileged commands • Separate processing domains • Privileged accounts • Privileged access by non-organizational users • Review of user privileges • Privilege levels for code execution • Auditing use of privileged functions • Prohibit non-privileged users from executing privileged functions

Family: ACCESS CONTROL	
AC-7 UNSUCCESSFUL LOGIN ATTEMPTS **AC-8 SYSTEM USE NOTIFICATION** **AC-9 PREVIOUS LOGON NOTIFICATION** **AC-10 CONCURRENT SESSION CONTROL** **AC-11 DEVICE LOCK** **AC-16 SECURITY AND PRIVACY ATTRIBUTES** Deals with limiting the number of invalid logon attempts, displaying notifications before granting access, notifying user of date/time of last access, restricting the number of concurrent sessions, locking session after inactivity and associating security attributes with information	CyberArk solutions support implementation of the following controls for the use of privileged accounts and access to sensitive documents within the vault: • Detection of anomalous logon attempts • Configurable automatic session termination • Failed logon attempts • System use notification • Previous logon (access notification) • Concurrent session control • Session lock • Security attributes
AC-17 REMOTE ACCESS **AC-18 WIRELESS ACCESS** Calls for establishing usage restrictions and authorizations for remote and wireless access	CyberArk solutions enable secure remote access through a web portal or wirelessly from a mobile device — privileged users can access their privileged accounts to retrieve privileged credentials as well as request or approve workflows. Organizations can isolate and protect critical IT assets from potential endpoint malware and avoid exposing privileged credentials, either to internal users or to external or outsourced vendors. CyberArk's Vendor Privileged Access Manager expands remote access capability by offering detailed access and just-in-time provisioning to remote vendors and other third-party users that must access either privileged accounts or web applications hosting sensitive data. The solution provides fast, easy and secure privileged remote access using cloud-based MFA with full session monitoring.
AC-20 USE OF EXTERNAL SYSTEMS Ensures terms and conditions are established for allowing authorized individuals to access external information systems or to process, store or transmit organization-controlled information using external information systems.	CyberArk provides a central platform for secure file transfers between organizations.

Family: ACCESS CONTROL	
AC-21 INFORMATION SHARING Applies to sharing information that is restricted in some manner (i.e., sensitive information) and is intended to facilitate information sharing in particular circumstances, including when employing automated mechanisms to help make information-sharing decisions	To facilitate sharing of sensitive information with an organization's business partners, suppliers and subcontractors, CyberArk provides a single platform enabling ad-hoc, manual or automated file transfer. The platform isolates sensitive data sent over the internet, allowing organizations to exchange sensitive information securely and efficiently. The solution is available as a self-hosted solution or as a cloud delivery model. CyberArk's platform can help organizations implement the following control enhancements: • Automated decision support • Information search and retrieval
AC-24 ACCESS CONTROL DECISIONS Relates to establishing procedures for ensuring access control decisions are applied to each access request prior to access enforcement	With CyberArk solutions, for each access request, the user is uniquely identified and their authorizations are validated (such as group membership in an LDAP directory) prior to granting access.

Family: AWARENESS AND TRAINING	
Contains controls for security awareness and training for end users and personnel with assigned security roles and responsibilities	
AT-3 ROLE-BASED TRAINING	CyberArk provides comprehensive training courses — ranging from privileged account administration to applications development — and can create specific programs to meet the unique needs of an organization.

Family: AUDIT AND ACCOUNTABILITY	
Covers controls related to generating, protecting and reviewing audit records and ensuring accountability	
AU-1 POLICY AND PROCEDURES	CyberArk solutions enable organizations to effectively implement automated controls for generating, protecting and reviewing audit records. All privileged users and applications are uniquely identified and their activities logged, ensuring full accountability for individuals regarding privileged actions and access to sensitive information.
AU-2 EVENT LOGGING	
AU-3 CONTENT OF AUDIT RECORDS	
AU-4 AUDIT LOG STORAGE CAPACITY	
AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES	

Family: AUDIT AND ACCOUNTABILITY	

AU-6 AUDIT RECORD REVIEW, ANALYSIS AND REPORTING
AU-7 AUDIT RECORD REDUCTION AND REPORT GENERATION
AU-8 TIMESTAMPS
AU-9 PROTECTION OF AUDIT INFORMATION
AU-10 NON-REPUDIATION
AU-11 AUDIT RECORD RETENTION
AU-12 AUDIT RECORD GENERATION
AU-14 SESSION AUDIT
	With CyberArk solutions, more than 150 different types of audit events can be recorded. Some examples include:
	• Update Owner – tracks top-level ownership and administration over specific items in the vault
	• Add Group Member – tracks when users are added to groups, which helps determine if a new member inadvertently gains over-wide access
	• Report Run – tracks when reports are run, which is useful for proving that auditors were supplied with specific reports with a timestamp
	• CPM Reconcile Password – tracks when password changes were made outside of the vault, which can detect potential malicious activity
	• Retrieve Password – tracks every time a user or application accesses a password in the vault
	Ensuring individual accountability is specifically addressed in the control, "AU- 3 Content of Audit Records," which lists the required data for each audit record, including the type of event and the identity of any individual associated with the event.
	This can be especially difficult for shared administrative accounts, which typically log the use of the account without associating the use with an individual. CyberArk solutions track all administrative actions by individual users.
	Content of event logs can be configured to include information on user identifiers, event descriptions, success/fail indicators and more. CyberArk's team can support the organization in identifying the important events and configuring the audit.
	When it comes to tracking privileged activity and gaining access to sensitive information, CyberArk solutions help organizations to meet the full set of requirements of the audit control family based on extensive audit capabilities, such as:
	• Recording individual user identities that access shared privileged accounts for full accountability
	• Supporting any audit storage size
	• Alerting on failures through the Notification Engine
	• Filtering audit records by various parameters
	• Providing a complete range of built-in audit reports
	• Delivering session recording and command logging for forensic analysis
	• Integrating with SIEM and event log systems including HP ArcSight, McAfee ESM, IBM/QRadar and RSA enVision for complete correlational analysis
	  ◦ Support for Syslog and XSL schema
	• Integrating with ITSM ticketing systems for change management and incident management, including Service Now and ZenDesk
	• Delivering customized telemetry dashboards to help organizations track compliance with organizational policies for specific teams and IT system types
	• Timestamping all logs synchronized to the vault clock
	  ◦ NTP can be enabled if required
	• Protecting audit information with cryptographic storage in a tamper-proof vault
	• Supporting any retention period as set by the organization
	• Generating alerts on specific occurrences

Family: ASSESSMENT, AUTHORIZATION AND MONITORING

Includes controls for assessing and authorizing security controls including authorizing connections within and between systems and ensuring ongoing assessments

CA-3 INFORMATION EXCHANGE **CA-7 CONTINOUS MONITORING** **CA-9 INTERNAL SYSTEM CONNECTIONS**	CyberArk solutions support the authorization of system interconnections and the secure exchange of information by providing secure control over connections of various applications throughout the infrastructure. For continuous monitoring, detailed session recordings and audit logs simplify protection, detection and response. CyberArk solutions monitor privileged access and provide audit logs in real time to SIEM solutions and security data analytics systems. Real-time monitoring of privileged sessions is also supported, providing details of all activity throughout a session and terminating a session.

Family: CONFIGURATION MANAGEMENT

Covers controls for managing the configuration of information systems

CM-2 BASELINE CONFIGURATION **CM-3 CONFIGURATION CHANGE CONTROL** **CM-5 ACCESS RESTRICTIONS FOR CHANGE** **CM-6 CONFIGURATION SETTINGS**	Configuration management ensures that critical assets, including operating systems, servers, databases, virtual machines, applications, firewalls, security systems, network devices, routers, etc. are always properly configured. The ability to make configuration changes must be restricted to authorized privileged users. CyberArk solutions help maintain baseline configurations and support the implementation of oversight of configuration change control by ensuring that only authorized users can gain access to system configurations. All access is monitored and records retained. Organizations can effectively enforce access restrictions for change as required by organizational policy by controlling access to administrative passwords. "Dual Control" can specify that access to highly sensitive passwords or policies requires confirmation by one or more authorized users.
CM-7 LEAST FUNCTIONALITY	Additionally, CyberArk solutions provide an audit record of which individual privileged users use administrative passwords to make configuration changes. Organizations can also monitor and record privileged sessions involving changes to configuration settings. Session approval workflows and DVR-like playback of recordings for review and analysis can be implemented. CyberArk solutions can control what privileged and elevated commands a user can access based on the "least privilege" principle. CyberArk can even be used to automatically terminate sessions that enter forbidden commands, depending on organizational preference.

Family: CONTINGENCY PLANNING

Covers controls involved with contingency planning

CP-9 SYSTEM BACKUP **CP-10 SYSTEM RECOVERY AND RECONSTITUTION**	All CyberArk products offer high availability, full disaster recovery capabilities and backup. Privileged credentials are always accessible and available for the requesting systems, even in network outages. Password versioning and reconciliation capabilities further enhance the criticality of being able to access systems with privileged credentials, based on enterprise policy. For sensitive information management, CyberArk's platform helps ensure that information is never lost and always protected, and transmissions are always automatically resumed. The vault can also be rebuilt based on guidelines.

Family: IDENTIFICATION AND AUTHENTICATION	
Covers controls involved with uniquely identifying users, processes and devices, and with applying various authentication methods to verify those identities as a prerequisite to allowing access to system resources	
IA-1 POLICY AND PROCEDURES Covers development of an identification and authentication policy and procedures to facilitate implementation of policy and associated controls	CyberArk solutions help organizations consistently implement identification and authentication policy and procedures and effectively implement automated controls for privileged identities. The CyberArk Telemetry tool helps organizations track utilization of key PAM policies and capabilities like privileged session management for specific IT platforms, helping them quickly close gaps in policies. Cloud Entitlements Manager can also identify privileged accounts in AWS that are not protected with MFA.
IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) Ensures that the information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users)	CyberArk directly offers authentication and identification of users, including adaptive single sign-on and multifactor authentication. With CyberArk solutions, every privileged user is uniquely identified in the system. The use of shared accounts is no longer anonymous, and instead, each individual privileged user is uniquely identified. Shared accounts such as Windows Administrator, UNIX root, an Oracle SYS account or Cisco Enable user are controlled by predefined granular access control. CyberArk solutions fully address the challenges of hard-coded, embedded credentials in applications, scripts or configuration files, and allow these highly sensitive identifiers to be centrally stored, audited and managed. Many of the control enhancements are directly applicable to the functionality of CyberArk solutions, including: • Network access to privileged accounts • Local access to privileged accounts • Group authentication • Network access to privileged accounts — separate device and replay resistant • Acceptance of PIV credentials • Hardware token-based authentication
IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION Requires the unique identification and authentication of devices before establishing a connection	CyberArk Identity cloud agents support strong MFA for boot screen and lock screen of Windows and macOS devices with features such as: • Risk-based adaptive MFA • Support for MFA on RDP/RDS access to Windows servers • Self-service password reset based on authentication challenges to minimize IT helpdesk support and costs • MFA for offline devices, with the ability to lock and wipe Windows and macOS devices if they are stolen • Flexible authentication factors, such as OTP, SMS, email, mobile push, FIDO2 keys (such as Yubikey), etc. All of CyberArk's products use highly secure cryptographic methods for establishing connections between components and storing or transmitting information and are FIPS 140 compliant. For example, every connection to the digital vault, where all the privileged account information is securely stored, has to be authenticated. It uses a strong two-way challenge and response authentication protocol (SRP). CyberArk's solutions use unique secure application authentication methods for applications requesting credentials. This includes enforcing limitations like machine address, OS user, application path and runtime signature. Control enhancements supported by CyberArk solutions include: • Cryptographic bidirectional authentication • Dynamic address allocation • Device attestation

Family: IDENTIFICATION AND AUTHENTICATION	
IA-4 IDENTIFIER MANAGEMENT Requires organization to manage information system identifiers	Common device identifiers mentioned include MAC, IP addresses or device-unique tokens. CyberArk solutions support authentication using passwords, SAML, RSA SecurID tokens, RADIUS, USB tokens (e.g., Aladdin's) or PKI digital certificates. Further, connections to the digital vault can be restricted by IP address.
IA-5 AUTHENTICATOR MANAGEMENT Covers management of information system authenticators such as passwords and other types of authenticators	CyberArk solutions support a variety of authentication methods for end users to access the digital vault, including passwords, PKI, RADIUS, SAML, LDAP, RSA SecurID, Windows authentication, Oracle SSO and a robust infrastructure for integrating with most Web SSO or OTP solutions (in addition to CyberArk Identity SSO). The solutions provide automated privileged password management, including automatically changing passwords based on an organizationally defined timeframe or when membership in a group changes. Complete lifecycle management for privileged account passwords helps organizations meet the full range of requirements, including ensuring password strength, defining their lifetime, updating them and managing their revocation. Passwords are stored using the CyberArk Digital Vault technology, which protects them from unauthorized disclosure and modification. And all passwords are also protected with strong encryption, both in transit and at rest. Many modern applications, containers and devices rely on insecure authentication. CyberArk solutions help apply recommendations such as those described in NIST SP 800-190 Application Container Security Guide and help eliminate weaknesses such as hard-coded, clear-text passwords, replacing those with secure authentication and a secure cache mechanism (for use in the event of a network outage). Many of the control enhancements are supported, including: • Password-based and PKI-based authentication • Automated support for password strength determination • Protection of authenticators • No embedded unencrypted static authenticators
IA-6 AUTHENTICATOR FEEDBACK Ensures information system obscures feedback of authentication information during authentication	With CyberArk solutions, authentication information is obscured — for example, by displaying asterisks when users input passwords.
IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION Requires implementation of mechanisms for authentication to a cryptographic module that meets requirements of applicable federal laws, regulations and standards	All of CyberArk's products are compliant with the NIST Security Requirements for Cryptographic Modules (FIPS-140) criteria.
IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) Ensures that the information system uniquely identifies and authenticates non-organizational users and processes	CyberArk solutions uniquely identify any third parties (e.g., contractors) provided with a privileged account and provide the ability to grant access without revealing any privileged passwords. Further, non-organizational users who remotely connect to privileged accounts do so through a proxy, so their session is encrypted and isolated from the internal network, mitigating third-party risks.
IA-9 SERVICE IDENTIFICATION AND AUTHENTICATION Ensures that organizations identify and authenticate services using security safeguards	For authenticating services, the digital vault technology is ICSA validated and designed to meet the highest security, audit and compliance requirements for managing App2App accounts. CyberArk delivers a complete infrastructure to centralize the management of credentials to resources with a comprehensive set of abilities for managing service accounts.

Family: IDENTIFICATION AND AUTHENTICATION	
IA-10 ADAPTIVE AUTHENTICATION Provides for flexible supplemental authentication techniques or mechanisms under specific circumstances or situations	CyberArk supports adaptive multifactor authentication, which is a method for using contextual information and business rules to determine which authentication factors to apply to a particular user in a particular situation. Adaptive authentication supports additional or increased security based on behavior or context, such as after consecutive login failures, attempts from a different physical location or temporal factors (e.g., unusual day of the week or time-of-day requests).
IA-11 RE-AUTHENTICATION Requires users and devices to re-authenticate when requesting access under predefined circumstances	With CyberArk solutions, organizations can require re-authentication for privileged users or applications based on timeframes or when users request to initiate additional sessions. As with adaptive authentication, CyberArk enables organizations to determine the unique authentication requirements that apply to a broad set of contextual factors, circumstances and user behavior. This dynamic solution also enables a risk-based approach that applies more stringent requirements to high-value resources and less rigorous criteria for those that are categorized as less critical or sensitive. CyberArk Identity also offers continuous authentication for sessions to sensitive web applications or cloud management consoles, requiring users who leave their desktops or do not show an active presence to re-authenticate.

Family: INCIDENT RESPONSE	
Contains controls related to a comprehensive incident response program	
IR-5 INCIDENT MONITORING	CyberArk solutions provide the necessary logs and notifications for effective incident monitoring and reporting, including sending alerts through the notification engine and connecting to an SIEM from vendors that include Splunk, HP ArcSight, McAfee ESM and RSA enVision. For example, CyberArk's privileged threat detection and response mechanisms continuously monitor the use of privileged accounts that are managed in the CyberArk Privileged Access Manager platform, as well as accounts that are not yet managed by CyberArk, and look for indications of abuse or misuse of the CyberArk platform. The solution also looks for attackers who compromise privileged accounts by running sophisticated attacks, such as Golden Ticket. CyberArk exchanges incident information with multiple sources (receiving alerts and sending detection data), including CyberArk, SIEM and network sensors, to rapidly detect indications of compromise and identify malicious privileged activity. This approach: • Detects and alerts in real-time with automatic response to detected incidents • Identifies privileged access related anomalies and malicious activities with the ability to detect in-progress attacks • Adapts threat detection to a changing risk environment with self-learning algorithms • Correlates incidents and assigns threat levels • Enhances the value of existing SIEM solutions with out-of-the-box integrations • Improves auditing processes with informative data on user patterns and activities
IR-6 INCIDENT REPORTING	

Family: MAINTENANCE

Includes controls regarding information system maintenance

MA-2 CONTROLLED MAINTENANCE	For maintenance, CyberArk provides the ideal platform from which to securely provide external parties with access to key systems in closely monitored and controlled environments. Organizations can record and store every privileged session in the tamper-proof digital vault for 24/7 video surveillance of access to sensitive systems. CyberArk Remote Access is specifically designed to provide fast, easy and secure privileged access for external vendors that need to perform preventative or corrective maintenance from non-local sources.
MA-4 NON-LOCAL MAINTENANCE	

Family: PLANNING

Covers controls for security planning

PL-8 SECURITY AND PRIVACY ARCHITECTURES	CyberArk's professional services consulting team includes top subject-matter experts who can help organizations to architect secure and efficient solutions for managing and controlling privileged access and access to sensitive documents. The core functionality of CyberArk solutions includes centralized management of privileged identities and access to sensitive information.
PL-9 CENTRAL MANAGEMENT	

Family: PERSONNEL SECURITY

Contains controls related to personnel security

PS-4 PERSONNEL TERMINATION	With CyberArk solutions, organizations can ensure that upon termination of individual employment, privileged users' access to privileged passwords is immediately disabled. All changes in the organization's LDAP directory (e.g., Active Directory) are immediately propagated to the digital vault. CyberArk Identity's lifecycle management capabilities also directly integrate with HRIS systems, allowing organizations to rapidly provision and deprovision users as they join/leave/change roles within a company. For personnel transfers, all modifications to an individual's access authorizations are also immediately propagated to the vault. Further, organizations can proactively set up the use of one-time passwords, which would ensure terminated or transferred users could not use previously issued passwords. As organizations enable and authorize external providers, CyberArk helps support rapid and effective identity management updates for external personnel changes. CyberArk Remote Access is specifically designed to provide fast, easy and secure privileged access for external personnel who need to access internal systems. Adaptive authentication helps quickly detect and adjust based on changes to external personnel behavior, such as access requests at unusual date/time, or from an unusual geolocation.
PS-5 PERSONNEL TRANSFER	
PS-7 EXTERNAL PERSONNEL SECURITY	

Family: RISK ASSESSMENT

Includes controls regarding risk assessment

RA-5 VULNERABILITY MONITORING AND SCANNING	CyberArk solutions help to protect the integrity of vulnerability scanning systems by ensuring that only those with authorized privileged credentials can gain access to these systems. Also, a detailed log is kept so that organizations will have a complete record of scan requests. CyberArk integrates with leading products and services such as Qualys, Tenable and Rapid7 to enable deep, authenticated scans while continuing to protect the privileged credential needed to scan IT systems.
RA-7 RISK RESPONSE	This newly added control points out, "Organizations have many options for responding to risk, including mitigating risk by implementing new controls or strengthening existing controls, accepting risk with appropriate justification or rationale, sharing or transferring risk, or avoiding risk." Frequently, the findings from security and privacy assessments, monitoring and audits include opportunities for improvement of identification and authentication controls. Application of CyberArk solutions will help the organization mitigate risks and close these gaps, leading to overall improvement of cybersecurity and privacy protections.

Family: SYSTEM AND SERVICES ACQUISITION

Contains controls for system and services acquisition

SA-3 SYSTEM DEVELOPMENT LIFE CYCLE	CyberArk helps implement controls for system and services acquisition. The company fully supports its customers and enables complete lifecycle management of the product suites. Specifically: • All CyberArk SaaS solutions are SOC 2 Type 2 Certified. • CyberArk Privileged Access Manager is certified on the DODiN Approved Product List. • CyberArk's products are highly acclaimed for their security engineering, including layered protection, security architecture, security training for developers and much more. • The company provides configuration management, change tracking and security updates. • The products have all been internally and field tested and extensively used by hundreds of large customers, providing the highest security assurance. • To help ensure proper implementation and usage of the product suites, CyberArk provides comprehensive training for users and administrators and offers additional support through professional services. • CyberArk's products are validated by ICSA Labs and FIPS 140 compliant. • Through the publication of our own corporate security standards in our corporate trust center, all organizations can easily verify product security. • CyberArk can provide customized development professional services.
SA-4 ACQUISITION PROCESS	
SA-5 SYSTEM DOCUMENTATION	
SA-8 SECURITY AND PRIVACY ENGINEERING PRINCIPLES	
SA-9 EXTERNAL SYSTEM SERVICES	
SA-10 DEVELOPER CONFIGURATION MANAGEMENT	
SA-11 DEVELOPER TESTING AND EVALUATION	
SA-16 DEVELOPER-PROVIDED TRAINING	
SA-20 CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS	

Family: SYSTEM AND COMMUNICATIONS PROTECTION

Includes controls regarding system and communications protection

SC-2 SEPARATION OF SYSTEM AND USER FUNCTIONALITY	CyberArk successfully addresses a wide range of the requirements for system and communications protection, including transmission, architecture, cryptographic procedures and functions.
	
	Specifically, CyberArk solutions:
	
	• Separate the main vault component from other components, isolating the main security function and ensuring application partitioning
	• Enable system components to reside on the internal network, helping to ensure protection from DoS attacks
	• Can block access to system components based on subnet or IP address
	• Ensure session authenticity by SSL verification between the main interface (PVWA) and the vault and through use of the proprietary secure protocol
	• Use FIPS 140 validated cryptography
	• Supports the use of PKI (Public Key Infrastructure) certificates for trustworthy user identification and secure connections
	• Save database states and preserve consistency
	• Have been architected with the use of thin nodes, enhancing the overall security
	• Protect all information at rest with encryption in the vault
	  ° Encryption algorithms supported include AES-256 and RSA-2048
	  ° Hardware Security Module (HSM) integration
	• Support heterogeneous environments
	  ° Integrate with the full range of operating systems, applications, databases, security appliances, network devices, directories, virtual environments and storage
	• Are designed to run in virtualized environments, enabling the use of virtualized techniques for concealment and misdirection
	• Enable information system partitioning; components can be set up to reside at diverse geographic locations
	• Employ hardware-based protection to ensure non-modifiable executable programs
	• Support distributed architecture
	• Facilitate process isolation using “safes” within the vault; each safe is assigned a separate address space

SC-3 SECURITY FUNCTION ISOLATION	
SC-4 INFORMATION IN SHARED SYSTEM RESOURCES	
SC-5 DENIAL-OF-SERVICE PROTECTION	
SC-7 BOUNDARY PROTECTION	
SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY	
SC-10 NETWORK DISCONNECT	
SC-11 TRUSTED PATH	
SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	
SC-13 CRYPTOGRAPHIC PROTECTION	
SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES	
SC-23 SESSION AUTHENTICITY	
SC-24 FAIL IN KNOWN STATE	
SC-25 THIN NODES	
SC-28 PROTECTION OF INFORMATION AT REST	
SC-29 HETEROGENEITY	
SC-30 CONCEALMENT AND MISDIRECTION	
SC-32 SYSTEM PARTITIONING	
SC-34 NON-MODIFIABLE EXECUTABLE PROGRAMS	
SC-36 DISTRIBUTED PROCESSING AND STORAGE	
SC-39 PROCESS ISOLATION	

Family: SYSTEM AND INFORMATION INTEGRITY

Includes controls regarding system and communications protection

SI-3 MALICIOUS CODE PROTECTION	CyberArk helps organizations meet the requirements for system and information integrity through an internal components check. CyberArk's Vault checks the internal firewall, as well as the crypto functionality and other security functions. In case of failure, the system will stop its operation to ensure security and integrity. The Notification Engine enables error handling. All system information is encrypted and verified, and the retention policy is configurable. CyberArk provides a security intelligence solution that allows organizations to detect, alert and respond to anomalous privileged activity indicating an in-progress attack. Real-time monitoring helps provide continuous protection for privileged access, as well as automatic suspension and termination of privileged sessions if any activity is deemed suspicious. Integration with many well-known third-party SIEM solutions provides rapid and accurate alerts on unusual activity and ensures timely notification and reporting.
SI-4 SYSTEM MONITORING	
SI-5 SECURITY ALERTS, ADVISORIES AND DIRECTIVES	
SI-6 SECURITY AND PRIVACY FUNCTION VERIFICATION	
SI-10 INFORMATION INPUT VALIDATION	
SI-11 ERROR HANDLING	
SI-12 INFORMATION MANAGEMENT AND RETENTION	

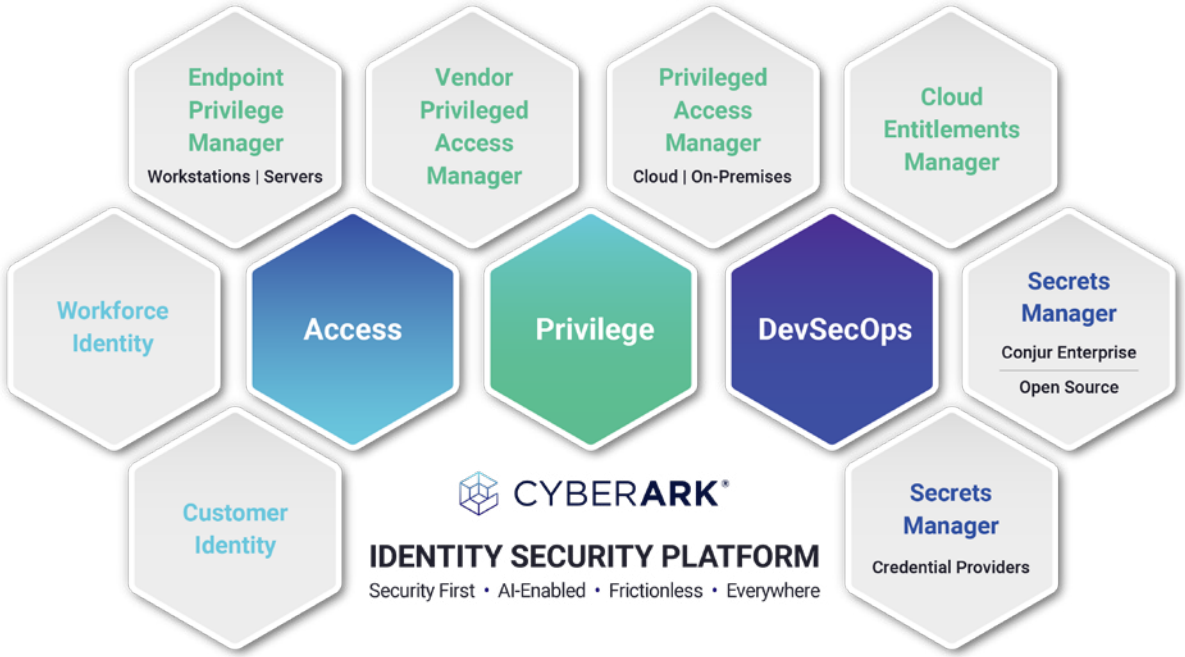
Family: SUPPLY CHAIN RISK MANAGEMENT

Includes controls regarding supply chain risk management policy and the associated supply chain risk management controls

SR-3 SUPPLY CHAIN CONTROLS AND PROCESSES	SP800-53 Rev. 5 includes a new family of controls related to Supply Chain Risk Management. CyberArk provides multiple solutions to support a defense-in-depth methodology, such as Remote Access, which provides secure privileged access for external vendors who need to access critical internal systems, and products for securing the software development/DevOps software supply chain. CyberArk solutions enable a proactive, holistic approach to securing privilege throughout your supply chain, including DevOps, hybrid and native cloud environments inherent to the software supply chain. Specifically: • CyberArk Secrets Manager solutions integrate with popular tools and container platforms to provide a comprehensive solution for securing secrets and other credentials in DevOps environments. • CyberArk Endpoint Privilege Manager enforces least privilege on the endpoint early in the lifecycle. It enables revocation of local administrator rights and implements application controls while minimizing impact on user productivity. • CyberArk Privileged Access Manager enables organizations to secure the privileged credentials and secrets used across their entire enterprise, including the development environments that are driving the organization's digital transformation. • CyberArk Cloud Entitlements Manager allows organizations to implement least privilege for all identities within their multi-cloud environments, including removing excessive permissions granted to additional software applications. • CyberArk Adaptive Multifactor Authentication facilitates implementation of a broad range of secondary authentication methods across the organization.

CyberArk Solution Overview

CyberArk's Identity Security Platform is built on the pillars of management for Access, Privilege and DevSecOps to deliver authentication, authorization, access and audit in an integrated, seamless manner — enabling security at every step in the Identity Security lifecycle. Our intelligent approach balances the need for better security with end-user productivity. CyberArk solutions leverage real-time intelligence and analytics to create a context-based, adaptive approach to the Identity Security lifecycle — for all identities, across all systems and apps, using any device. To mitigate the risk of a serious breach, enterprises need to adopt a security solution with consistent controls that specifically address their privileged access exposure.



The CyberArk Identity Security Platform solution is uniquely positioned to help federal government agencies meet today's challenging security and compliance requirements. The CyberArk Privileged Access Manager 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 capabilities.

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

- **FISMA/NIST SP 800-53 –** CyberArk solutions help federal government agencies comply with requirements, including those related to the "Access Control," "Audit and Accountability" and "Identification and Authentication" control families. The effectiveness of these solutions is proven through the examination, interviews and tests as described in SP 800-53A. The controls addressed, including those described above, address many of the important controls described in the LOW, MOD or HIGH, and Privacy starter baselines in SP 800-53B.

- **Executive Order (EO) 14028 –** CyberArk aids in the achievement of agency requirements for Zero Trust Architecture, Cloud Security and Supply Chain protections. CyberArk integration and solutions enable rapid and effective achievement within the EO's tight deadlines.
- **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.
- **Cybersecurity Maturity Model Certification (CMMC) –** CyberArk solutions (including access control, identity management and remote workforce protections) enable compliance with the Department of Defense CMMC model for protection of Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). This is largely based on NIST SP 800-171 and SP 800-172 requirements — guidelines for which CyberArk and its integration partners have a proven track record.

Conclusion

The Federal Information Security Modernization Act (FISMA) provides a comprehensive framework for safeguarding information resources. As these agencies work to protect those resources, including through security and privacy controls as described in NIST SP 800-53, CyberArk solutions help effectively and efficiently meet the full range of requirements regarding privileged accounts. The solutions are enterprise proven in large and mid-sized government and commercial organizations. CyberArk is the global leader in Identity Security.

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®