Cyber-Ark®

Security That Empowers People™

# Complying with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53

## *An Assessment of Cyber-Ark's Solutions*

September 2011

# Table of Contents

# EXECUTIVE SUMMARY

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 provides the recommended security controls for federal information systems and organizations. Cyber-Ark offers three solution suites that help agencies implement the necessary controls within NIST SP 800-53 to achieve FISMA compliance:

- **Privileged Identity Management (PIM) Suite** – comprehensive lifecycle management for privileged, shared and application accounts across the datacenter.
- **Privileged Session Management (PSM) Suite** – isolates, controls and monitors privileged sessions on servers, databases or virtual environments, providing a pre-integrated solution with PIM.
- **Sensitive Information Management (SIM) Suite** – manages and protects sensitive information whether being shared within the organization or sent to external parties.

Cyber-Ark's solutions offer a preventative approach by introducing the necessary security controls to protect the organization's assets.

Privileged users are abundant in the enterprise environment. They can be categorized into the following four classes:

- Generic, shared or non-personal administrative accounts that exist in virtually every network device, operating system, database, or software application. These accounts hold “super user” privileges and are often anonymously shared among IT staff with no proper accountability. Some examples are: Windows Administrator user, UNIX root user and Oracle SYS account.
- Personal privileged accounts – the powerful accounts that are used by business users and IT personnel. These accounts have a high level of privileges and their use (or misuse) can significantly affect the organization’s business. Some examples are: the CFO’s user or a DBA account.
- Application accounts, which are used by applications to access databases and other applications. These accounts typically have broad access rights to underlying business information in databases.
- Emergency accounts – used by the organization when elevated privileges are required to fix urgent problems, such as in cases of business continuity or disaster recovery. Access to these accounts frequently requires managerial approval. These are often called: fire call ids, break-glass users, etc.

The main NIST SP 800-53 Control Families addressed by Cyber-Ark include:

Access Control –
The “Access Control” family is the foundation for the management of users and accounts. It addresses issues of account creation and assignment (e.g. who should be given an account?), as well as when and how accounts and privileges should be used. It therefore contains many guidelines regarding the special

care and attention that needs to be given to privileged accounts and their elevated access rights, as well as access to sensitive information stored in organization’s information systems.

*“Users requiring administrative privileges on information system accounts receive additional scrutiny by organizational officials responsible for approving such accounts and privileged access”*. Cyber-Ark's PIM suite provides an organization with a comprehensive solution for privileged account lifecycle management from discovering and securing the accounts to enforcing policies and auditing the use of them. Complementing the PIM suite, PSM gives organizations better control over privileged sessions, who can initiate sessions and for how long, enable privileged single sign on to sessions without divulging privileged credentials, e.g. to third parties having to access your network and continuously monitoring activity throughout the session.

Achieve NIST 800-53 compliance using pre-defined policies and workflows

As to access to sensitive information, the Access Control family specifies the Access Enforcement, Information Flow and other controls that prescribe how information should be controlled, encrypted, accessed, shared and so on. Cyber-Ark’s SIM suite provides a complete solution for storing and sharing sensitive information, whether inside the organization or with other entities.

Cyber-Ark successfully addresses and even exceeds the baseline requirements for Account Management, Access Enforcements, Separation of Duties, Concurrent Session Control, Session Lock and others. Cyber-Ark’s products emphasize the Least Privilege principal, by providing granular access control and effectively restricting privileged access throughout the organization.

<u>Audit and Accountability</u> –
The “Audit and Accountability” family ensures that the information required for auditing and, if necessary, rebuilding the chain of events is available on demand.
Both for access to sensitive information and for privileged actions, accountability cannot be achieved if anonymous access is used. That is why control “Content of Audit Records” (AU-3), lists the required data for each audit log record, and states that *“the information system produces audit records that contain sufficient information to, at a minimum, establish… (the) identity of any user/subject associated with the event”*. Cyber-Ark supports this requirement by extensively documenting any event in the system, be it access to stored information (in the case of the SIM Suite) or use of a privileged password (for PIM Suite), personalizing activity for full accountability.

All Cyber-Ark logs are properly time-stamped, cryptographically protected and stored in a tamper-proof vault, referenced to a specific user in the system and stored for as long a period as required by the organization. Cyber-Ark products can also generate alerts on specific occurrences and connect to organizational SIEM products, such as ArcSight to send CEF compliant syslog events.

<u>Identification and Authentication</u> –
Control “IA-2 Identification and Authentication (Organizational Users)” is the main control in this family and is needed for effective access control or audit. The control itself asserts that: *“The information system uniquely identifies and authenticates organizational users”*. This is especially true for privileged

and shared accounts, which are shared among the IT staff, diminishing accountability and exposing vulnerabilities due to password knowledge. Control "IA-5 Authenticator Management" is concerned with the management and use of authenticators, mainly passwords, in the organization. The control provides many requirements for password management, such as: ensuring their strength, defining their lifetime, refreshing/changing them periodically, protecting them, and managing their revocation. These requirements apply to all types of accounts, as specified in AC-2: "individual, group, system, application, guest/anonymous, and temporary". Often, knowing where these accounts exist can be a challenge. Cyber-Ark's auto-discovery capabilities identities where these accounts exists, whether on servers or virtual environments and continues to manage these throughout their lifecycle.

Cyber-Ark's PIM and PSM suites enable an organization to securely provide its users and applications with the exact privileges they need in order to complete their role

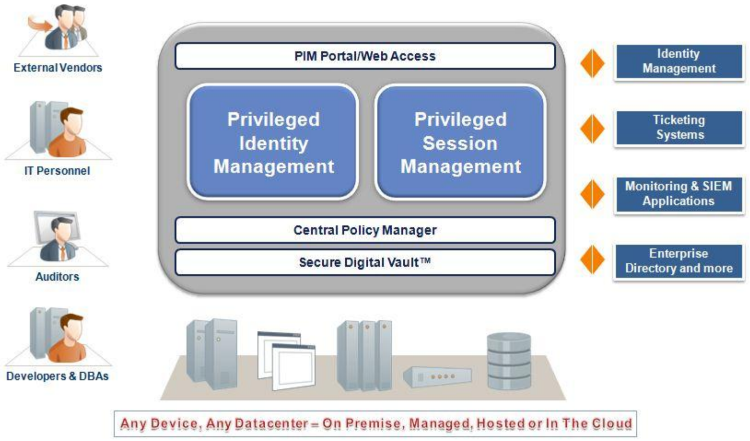
Control Enhancement (7) addresses the key problem of hardcoded, clear-text passwords in applications, by requiring that *"The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys"*.

Cyber-Ark's Application Identity Manager part of the PIM suite, uniquely addresses this area by eliminating hard-coded passwords and periodically replacing them with no system downtime, enhanced secure authentication and a secure cache mechanism in the event of a network outage.

This document provides an overview of the solution suites offered by Cyber-Ark and demonstrates how these solutions address the recommendations of NIST SP 800-53.

# CYBER-ARK SOLUTION OVERVIEW

Cyber-Ark's Privileged Identity Management (PIM) Suite and Privileged Session Management (PSM) Suites are an integrated, full lifecycle solution for centrally managing privileged and shared identities, privileged sessions as well as embedded passwords found in applications and scripts.


External Vendors
IT Personnel
Auditors
Developers & DBAs
PIM Portal/Web Access
Privileged Identity Management
Privileged Session Management
Central Policy Manager
Secure Digital Vault™
Identity Management
Ticketing Systems
Monitoring & SIEM Applications
Enterprise Directory and more
Any Device, Any Datacenter = On Premise, Managed, Hosted or In The Cloud

Privileged accounts, as well as the audit information associated with using them, must be protected according to the highest security standards. The Cyber-Ark PIM Suite utilizes the Patented Digital Vault®, validated as highly secure by independent security evaluators (such as ICSA Labs). This core technology is the heart of the PIM suite and was designed to meet the highest security requirements for controlling the "keys to the kingdom." The Digital Vault provides numerous underlying security capabilities for authentication, encryption, tamper-proof audit and data protection.

The Cyber-Ark PIM Suite includes the following products:

- **Enterprise Password Vault ®** – Cyber-Ark's award winning Enterprise Password Vault (EPV) enables organizations to enforce an enterprise policy that protects your most critical systems, managing the entire lifecycle of shared and privileged accounts across data centers.
- **Application Identity Manager™** – Cyber-Ark's market leading Application Identity Manager (AIM) fully addresses the challenges of hard-coded App2App credentials and encryption keys. The solution eliminates the need to store App2App credentials in applications, scripts or configuration files, and allows these highly-sensitive credentials to be centrally stored, audited and managed within Cyber-Ark's patented Digital Vault.
- **On-Demand Privileges Manager™** – On-Demand Privileges Manager (OPM) is the first unified solution for managing and monitoring superusers and privileged accounts under one roof. Usage of accounts such as 'root' users on UNIX is no longer anonymous and can now be controlled by pre-defined granular access control, where both the command itself and the output are recorded. On-Demand Privileges Manager also dramatically improves productivity in Windows environments to enforce a 'least privilege' policy on desktops.

To complement Cyber-Ark's market-leading **Privileged Identity Management Suite** and proactively protect privileged sessions, especially remote or third party access, Cyber-ark's **Privileged Session Management (PSM)** Suite is a central control point and allows you to isolate, control and monitor all privileged sessions whether on servers, databases or virtual machines. Together these two suites provide a holistic and preventative approach to managing risks associated with privileged accounts and activities.

**Sensitive Information Management (SIM) Suite**

1. **Sensitive Document Vault** provides a highly secure central storage with granular access control, segregation of duties and extensive monitoring capabilities when storing and sharing files within the organization.

2. **Governed File Transfer (GFT) Suite** enables encrypted transmission of sensitive files to third parties supporting a variety of transfer types. All transfer methods, ad-hoc, manual or automated processes are supported on the same secure Digital Vault platform for centralized management and control. This suite employs the patented highly-secure Digital Vault and secure transfer protocols (patented Vault Protocol[1]/ SSL / SSH) that encrypts and protects files at rest and in transit.

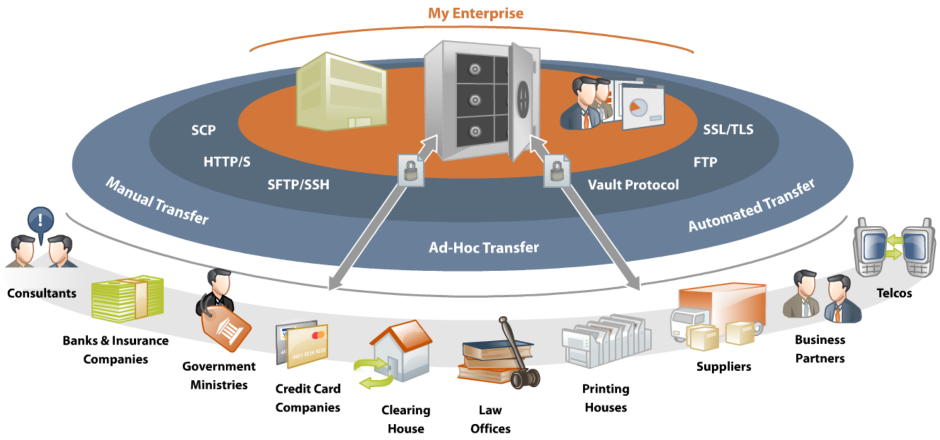


Figure 3: A unique approach for transferring files securely

Cyber-Ark's unique and patented Digital Vault technology, which includes multiple security layers such as encryption, authentication, access control, and strict auditing, is a core component of the underlying infrastructure for both the PIM, PSM and SIM suites, delivering an enterprise class solution for protecting and controlling access to sensitive information or privileged credentials.

[1] The patented "Vault Protocol" employs proven cryptographic algorithms and primitives.

# ADDRESSING NIST SP 800-53 RECOMMENDATIONS

The table below describes how Cyber-Ark's solutions help implement the controls described in NIST SP 800-53. For each family, **all the controls listed in the "Control Name" column are implemented by Cyber-Ark for LOW, MED and HIGH baselines**, as detailed in the NIST SP 800-53 Rev. 3

| CNTL NO. | CONTROL NAME | HOW DOES CYBER-ARK HELP? |
|---|---|---|
| **Access Control** | | |
| AC-2 | Account Management | Cyber-Ark's PIM and PSM suites provide an organization with the ability to automatically discover where privileged accounts exist on servers and virtual environments and securely provide it's users with only the necessary privileged access they need in order to complete their role based on pre-defined policies. Based on the policy, passwords can be "one-time" passwords and changed after a user has accessed them or any other automatic replacement frequency. 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.<br>By extending to the PSM Suite, organizations have:<br>• Control over session initiation on servers, databases or virtual infrastructure, including control regarding who can initiate sessions and for how long<br>• Privileged single sign on to sessions without divulging privileged credentials e.g. to third parties having to access your network remotely<br>• Dual control for session initiation<br>• Continuous monitoring capabilities on servers, databases and virtual environments that allow for forensic analysis and quicker remediation time<br>Separation of duties – The Vault infrastructure inherently provides separation of duties and allows users to be exposed only to information that is relevant to them (files, privileged credentials etc). The Vault is divided into safes which users can access based on their permissions without knowing of the existence of other safes. All Vault activity is logged and stored in tamper-proof format for audit.<br>Sensitive Information Management Suite provides organizations with the following:<br>• Users can create and share content through safes<br>• Scan Engine can be used to scan files for viruses |
| AC-3 | Access Enforcement | |
| AC-4 | Information Flow Enforcement | |
| AC-5 | Separation of Duties | |
| AC-6 | Least Privilege | |
| AC-7 | Unsuccessful Login Attempts | |
| AC-8 | System Use Notification | |
| AC-10 | Concurrent Session Control | |
| AC-11 | Session Lock | |
| AC-16 | Security Attributes | |
| AC-17 | Remote Access | |
| AC-20 | Use of External Information Systems | |

| CNTL NO. | CONTROL NAME | HOW DOES CYBER-ARK HELP? |
|---|---|---|
| AC-21 | User-Base Collaboration and Information Sharing | • Enforce Dual Control for accessing sensitive information<br>• Use File Categories to attach security attributes to information<br>• Automatically and securely transfer information between users and organizations |
| **Audit and Accountability** | | |
| AU-2 | Auditable Events | Cyber-Ark solution suites provide extensive audit records, including time stamps, addresses, user identifiers, event descriptions, success/fail indicators and more. Support is provided for the organization in identifying the important events and configuring the audit. Notable features include:<br>• Support for any storage size<br>• Support for any retention period as set by the organization<br>• Support for Syslog and XSL schemas<br>• Integration with SIEM and event log systems<br>• Alert on failures through the Notification Engine<br>• Audit records filtering by various parameters<br>• All logs are properly time-stamped and synchronized to Vault clock. NTP can be enabled if required.<br>• All audit information is protected in the Digital Vault<br>• All actions are personalized for full accountability<br>• Built-in reports e.g. entitlements, activity log, provisioning/deprovisioning and more<br>• Session recording for forensic analysis |
| AU-3 | Content of Audit Records | |
| AU-4 | Audit Storage Capacity | |
| AU-5 | Response to Audit Processing Failures | |
| AU-6 | Audit Monitoring, Analysis, and Reporting | |
| AU-7 | Audit Reduction and Report Generation | |
| AU-8 | Time Stamps | |
| AU-9 | Protection of Audit Information | |
| AU-10 | Non-repudiation | |
| AU-11 | Audit Record Retention | |
| AU-12 | Audit Generation | |
| AU-14 | Session Audit | |
| **Security Assessments and Authorization** | | |
| CA-3 | Information System Connections | Cyber-Ark's Application Identity Management solution uses the AIM Provider and SDK to remove all hard coded connection details to a remote data source such as a database and enables secure control over connections of various applications throughout the infrastructure. By eradicating the need to store application passwords embedded in applications, scripts or configuration files, these highly-sensitive passwords are now centrally stored, logged and managed within the Digital Vault. |

| CNTL NO. | CONTROL NAME | HOW DOES CYBER-ARK HELP? |
|---|---|---|
| **Configuration Management** | | |
| CM-2 | Baseline Configuration | Cyber-Ark supports baseline configuration and effectively enforces access restrictions for change as required by organizational policy.<br>The PIM solution enables access restrictions for changes throughout the organization, by controlling the access to passwords. Notable features include:<br>• Dual control - specify that access to highly sensitive passwords or policies requires confirmation by one or more authorized users<br>• Access confirmation or denial via a web-browser or a Smartphone<br>• Control what privileged and elevated commands a user can run based on 'least privilege' principle<br>• Accountability and auditability of all privileged activities<br>Privileged Session Management Suite enables:<br>• Monitoring and recording privileged sessions on servers, databases or virtual environments<br>• Session approval workflows<br>• DVR playback of recordings for review and analysis |
| CM-5 | Access Restrictions for Change | |
| CM-7 | Least Functionality | |
| **Contingency Planning** | | |
| CP-9 | Information System Backup | All Cyber-Ark products offer high availability, full disaster recovery capabilities and backup.<br>For Privileged Identity Management Suite this means that privileged credentials will always be 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.<br>For Sensitive Information Management Suite this means that sensitive information is never lost, always protected and transmissions are always automatically resumed. The Vault can also be rebuilt based on guidelines. |
| CP-10 | Information System Recovery and Reconstitution | |
| **Identification and Authentication** | | |
| IA-2 | User Identification and Authentication | With Cyber-Ark, every user is uniquely identified in the system and given the permissions and functions as assigned by the organization.<br>A variety of authentication methods for end users is supported, including: PKI, RADIUS, LDAP, RSA SecurID, Windows authentication, Oracle SSO and a robust |
| IA-3 | Device Identification and Authentication | |

| CNTL NO. | CONTROL NAME | HOW DOES CYBER-ARK HELP? |
|---|---|---|
| IA-4 | Identifier Management | infrastructure for integrating with most Web SSO or OTP solutions.<br>Device authentication is supported by IP authentication.<br>The Application Identity Manager (AIM) solution, part of the PIM Suite, also uses unique secure authentication parameters e.g. path, hash/signature, OS user or machine address.<br>Cyber-Ark's products are FIPS 140-2 compliant. |
| IA-5 | Authenticator Management | |
| IA-6 | Authenticator Feedback | |
| IA-7 | Cryptographic Module Authentication | |
| IA-8 | Identification and Authentication (Non-Organizational Users) | |
| **Incident Response** | | |
| IR-5 | Incident Monitoring | Cyber-Ark provides the necessary logs and notifications for effective Incident Monitoring and Reporting, sends alerts through the Notification Engine and connects to organizational SIEM. |
| IR-6 | Incident Reporting | |
| **Maintenance** | | |
| MA-4 | Non-Local Maintenance | PSM provides the ideal platform from which to securely provide external parties access to key systems in closely monitored and controlled environments:<br>• Record and store every privileged session in the tamper-proof Digital Vault for 24/7 video surveillance of sensitive systems.<br>• Privileged single sign on, a key capability in the PSM Suite, allows users to connect to privileged sessions without having to divulge the privileged password. This is critical when external vendors need to access your environment. |
| **Risk Assessment** | | |
| RA-5 | Vulnerability Scanning | The PIM Suite enables in-depth vulnerability scanning of organizational infrastructure integrating with vulnerability scanners and providing them with the required passwords on demand, thus ensuring that the scanner itself does not expose the organization to password-exposure risks. |

| CNTL NO. | CONTROL NAME | HOW DOES CYBER-ARK HELP? |
|---|---|---|
| **System and Services Acquisition** | | |
| SA-3 | Life Cycle Support | Cyber-Ark supports its customers and enables complete life-cycle management of the solution suites. Specifically:<br>• All Cyber-Ark products come fully documented<br>• Cyber-Ark products are highly acclaimed for their security engineering, including layered protection, security architecture, security training for developers and much more.<br>• Cyber-Ark products were tested by ICSA Labs<br>• Our products have all been internally and field tested and extensively used by hundreds of large customers, providing the highest security assurance.<br>• Cyber-Ark provides configuration management, change tracking, and security updates<br>• Cyber-Ark has a 95% maintenance renewal rate |
| SA-4 | Acquisitions | |
| SA-5 | Information System Documentation | |
| SA-8 | Security Engineering Principles | |
| SA-10 | Developer Configuration Management | |
| SA-11 | Developer Security Testing | |
| SA-13 | Trustworthiness | |
| **System and Communications Protection** | | |
| SC-2 | Application Partitioning | Cyber-Ark successfully addresses all the requirements for system and communication protection, whether related to transmission, architecture, cryptographic procedures and functions, etc. Specifically:<br>• Cyber-Ark separates the main Vault component from other components, isolating the main security function and ensuring application partitioning.<br>• Supports distributed architecture<br>• Session authenticity is ensured by SSL verification between the main interface (PVWA) and the Vault.<br>• The proprietary secure protocol (Vault Protocol) also preserves session authenticity.<br>• Cyber-Ark's products are FIPS 140-2 compliant.<br>• Cyber-Ark databases saves state and preserve consistency<br>• The architecture supports the use of thin nodes, enhancing the overall security<br>• Cyber-Ark facilitates creation of Honeypots that can be used to indicate possible breaches<br>• All information at rest is encrypted and well protected in the Vault<br>• Cyber-Ark components can run on Virtual Machines |
| SC-3 | Security Function Isolation | |
| SC-6 | Resource Priority | |
| SC-7 | Boundary Protection | |
| SC-8 | Transmission Integrity | |
| SC-9 | Transmission Confidentiality | |
| SC-10 | Network Disconnect | |
| SC-11 | Trusted Path | |
| SC-12 | Cryptographic Key Establishment and Management | |
| SC-13 | Use of Cryptography | |
| SC-23 | Session Authenticity | |
| SC-24 | Fail in Known State | |

| CNTL NO. | CONTROL NAME | HOW DOES CYBER-ARK HELP? |
|---|---|---|
| SC-25 | Thin Nodes | |
| SC-26 | Honeypots | |
| SC-28 | Protection of Information at Rest | |
| SC-30 | Virtualization Techniques | |
| SC-32 | Information System Partitioning | |
| **System and Information Integrity** | | |
| SI-4 | Information System Monitoring | Cyber-Ark ensures System and Information Integrity through:<br>• Internal components check – Cyber-Ark'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.<br>• The Notification Engine enables error handling.<br>• Retention policy is configurable<br>• All data is encrypted and verified |
| SI-6 | Security Functionality Verification | |
| SI-9 | Information Input Restrictions | |
| SI-10 | Information Accuracy, Completeness, Validity, and Authenticity | |
| SI-11 | Error Handling | |
| SI-12 | Information Output Handling and Retention | |

# CONCLUSION

With an increased focus on the insider threat and the rise in number of security incidents related to abuse of privileged accounts by both insiders and external wrongdoers, NIST appropriately included a great deal of improvements to SP 800-53 in its third revision. An unscientific but quick indicator is the leap in occurrences of the word “privileged” from 9 in the previous revision to 53 in the current one.

Whether an organization performs a methodological risk assessment process, or simply looks for a “quick fix” to secure the keys to its kingdom – privileged accounts are bound to be at the top of the priority list. Aspects of Privileged Identity Management are not limited to the controls listed in this document. For every implemented control, an organization has to identify the proper targets for that control, which may include privileged users.

While some aspects of Privileged Identity Management may be addressed procedurally or using present tools, many of these controls entail the use of a dedicated solution for the management and audit of privileged users. Control Enhancement AC-2 (1) calls for *“automated mechanisms to support the management of information system accounts”*. Cyber-Ark's Privileged Identity and Session Management Suites provide an end-to-end, continuous monitoring solution covering all the requirements mentioned in this document and more, while the Sensitive Information Management Suite secures all confidential files in transit and at rest between organizations.