Privileged Account Security for Unix/Linux Environments

Privileged accounts and credentials in Unix/Linux environments often provide access to an organization's most critical systems, applications and data. To protect these accounts, organizations should look for controls that centralize the security, management and monitoring of all privileged account activity.

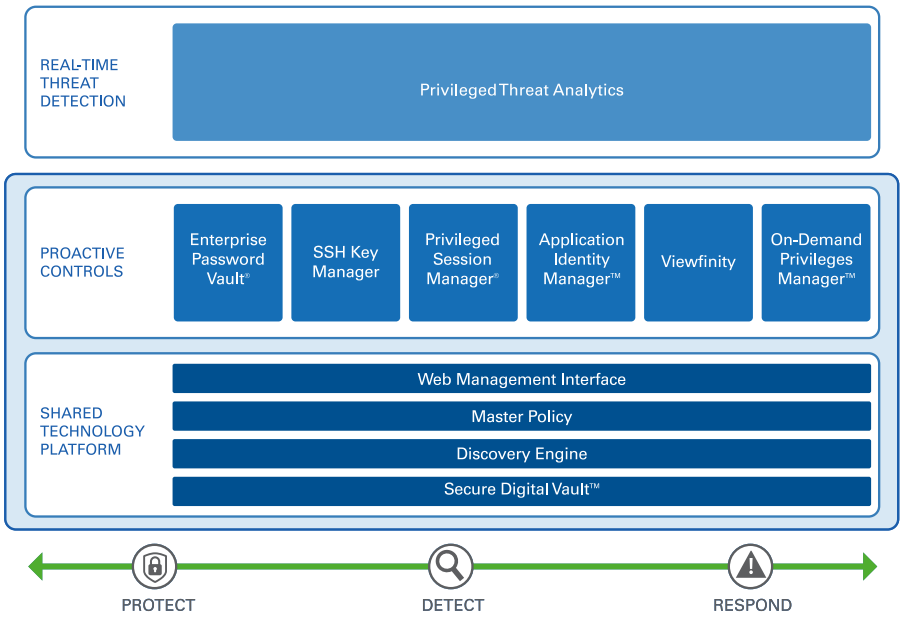
Unix and Linux systems often house an organization's most critical applications and most sensitive data. Yet, due to the inherently siloed nature of these systems, many organizations struggle to effectively and efficiently secure, control and monitor privileged accounts and credentials in their Unix/Linux environments. As a result, these sensitive accounts and credentials, which can be used to access sensitive data, change system settings, and delete audit logs, are often left unprotected from malicious and unauthorized users.

To protect Unix/Linux accounts and credentials in a uniform and effective way, organizations need controls that centrally manage privileged accounts throughout the enterprise, secure and rotate privileged account credentials, proactively secure privileged user sessions and continuously monitor privileged accounts to detect anomalous activity.

The CyberArk Privileged Account Security Solution

CyberArk is the trusted expert in privileged account security. Designed from the ground up for security, the CyberArk Privileged Account Security Solution centralizes and secures privileged account information, enforces least privilege and monitors activity to detect threats. To make security usable for system administrators, CyberArk solutions enable users to securely access authorized accounts on Unix and Linux systems while working natively within their preferred remote access tools.

Every product in the CyberArk Privileged Account Security Solution is stand-alone and can be managed independently while still sharing resources and data from the common infrastructure. Working together the products provide a complete, secure solution.



Why CyberArk?

CyberArk is the only security company focused on eliminating the most advanced cyber threats; those that use insider privileges to attack the heart of the enterprise. Dedicated to stopping attacks before they stop business, CyberArk proactively secures against cyber threats before attacks can escalate and do irreparable damage. The company is trusted by the world's leading companies to protect their highest value information assets, infrastructure and applications.

Privileged Account Security Capabilities for Unix/Linux Environments

Strong security of privileged account information – *Shared Technology Platform*
At the core of CyberArk's solution is the CyberArk Digital Vault, which centrally secures all privileged account information. Multiple layers of built-in security help to ensure the strongest levels of protection for an organization's most sensitive assets.

Centralized and granular policy management– *Shared Technology Platform*
Master Policy serves as a centralized policy engine, from which organizations are able to set granular policies for all managed users, accounts and credentials throughout on-premises, cloud and ICS environments. Organizations can create policies to automatically scan Unix and Linux environments to discover new privileged accounts and credentials and optionally provision them to the Digital Vault.

Centralized privileged account management and provisioning – *Privileged Session Manager, On-Demand Privileges Manager*
Active Directory (AD) bridging capabilities enable organizations to connect Unix/Linux administrators to AD through the CyberArk Digital Vault. Based on role and policy, CyberArk can automatically provision and deprovision local user accounts on Unix/Linux systems, as well as apply least privilege policies to these accounts. This helps to simplify the management of privileged users while enabling users to easily access all their authorized accounts using AD credentials.

Password and SSH key security and management – *Enterprise Password Vault, SSH Key Manager, Application Identity Manager*
CyberArk solutions enable organizations to proactively secure, rotate and control access to privileged user and application credentials. The solution tracks the use of these credentials to help organizations clearly report on privileged access throughout the IT environment.

Least privilege enforcement with detailed audit – *On-Demand Privileges Manager*
CyberArk's centralized and secure alternative to sudo eliminates unneeded root privileges while still allowing privileged users to run authorized administrative commands and elevate privileges when necessary, based on policy. Unified auditing links superuser sessions to individual users, and recording capabilities enable organizations to securely and easily document all activity that occurs during root sessions.

Session security with a native user experience– *Privileged Session Manager*
CyberArk can establish privileged user sessions on a dedicated, secure jump server to help protect target systems from malware on endpoints and enable privileged account access without exposing sensitive credentials. Unix/Linux users are able to establish these sessions directly from their preferred remote access tools, meaning they do not have to leave their native environments.

Tamper-resistant audit of privileged user activity – *Privileged Session Manager*
Monitoring and recording capabilities built into CyberArk's secure jump server enable security teams to document all activity that occurs during privileged user sessions. Recordings are stored in the Digital Vault, which supports strong access controls to prevent users from altering their audit trails. Security teams can optionally watch sessions in real-time to gain the opportunity to spot suspicious activity and immediately terminate the session.

Targeted alerts to notify security teams of potential in-progress attacks – *Privileged Threat Analytics*
By continuously monitoring and analyzing privileged account activity, CyberArk's threat analytics solution detects anomalous activity that could indicate an in-progress attack. The solution generates critical privileged account intelligence with a combination of built-in algorithms designed by privileged account security experts. Targeted alerts enable organizations to quickly identify malicious privileged activity and take immediate action to disrupt and respond to attacks.

Start Assessing Your Privileged Unix/Linux Accounts Today

CyberArk DNA™ (Discovery and Audit) is a free assessment tool that can help organizations understand the scope of privileged account security risks in Unix, Linux, Windows and ESX environments. DNA discovers the location and status of privileged accounts, SSH keys, service accounts, hard-coded application credentials and insecure sudo configurations to help organizations prioritize projects, build a business case and plan for a privileged account security project.

Specifications

Encryption Support:
- AES-256, RSA-2048
- HSM integration
- FIPS 140-2 validated cryptography

High Availability:
- Clustering support
- Multiple Disaster Recovery sites
- Integration with enterprise backup systems

Access and Workflow Management Integrations:
- LDAP directories
- Identity and Access Management solutions
- Ticketing and workflow systems

Multi-lingual Portal:
- English, French, German, Spanish, Russian, Japanese, Chinese (Simplified and traditional), Brazilian Portuguese, Korean

Authentication Methods:
- Username and Password, LDAP, Windows authentication, RSA SecurID, Web SSO, RADIUS, PKI and smart cards

Monitoring:
- SIEM integration, SNMP traps, Email notifications

Sample Supported Managed Devices:
- Operating Systems: Windows, *nix, RHEL, Solaris, IBM iSeries, Z/OS, CentOS, OVMS, HP Tandem, MAC OS, ESX/ESXi, XenServers
- Windows Applications: Service accounts including SQL server service accounts in cluster, Scheduled Tasks, IIS Application Pools, COM+, IIS Anonymous Access, Cluster Service
- Databases: Oracle, MSSQL, DB2, Informix, Sybase, MySQL and any ODBC compliant database
- Security Appliances: CheckPoint, Nokia, Juniper, Cisco, Blue Coat, IBM, TippingPoint, SourceFire, Fortinet, WatchGuard , Industrial Defender, Acme Packet, Critical Path, Symantec, Palo Alto
- Network Devices: Cisco, Juniper, Nortel, HP, 3com, F5, Alactel, Quintum, Brocade, Voltaire, RuggedCom, Avaya, BlueCoat, Radware, Yamaha
- Applications: SAP, WebSphere, WebLogic, JBOSS, Tomcat, Oracle ERP, Peoplesoft, TIBCO, Cisco
- Directories: Microsoft, Sun, Novell, UNIX vendors, RSA, CA
- Remote Control and/ Monitoring: IBM, HP iLO, Sun, Dell DRAC, Digi, Cyclades, Fijitsu
- Virtual environments: VMware vCenter and ESX
- Storage: NetApp
- Generic Interfaces: any SSH/Telnet device
- Windows registry any web application e.g. Facebook, Twitter, LinkedIn
- WMI remote command execution
- ODBC - passwords stored in database tables
- Configuration files (flat, INI, XML) - e.g. application server configuration files or any application/script configuration file