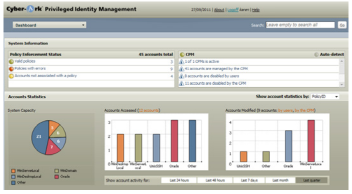
CYBERARK®

Privileged Identity and Session Management for Protecting Critical Infrastructure

Proactively protect your critical infrastructure by controlling privileged access and activity across your industrial control systems, while meeting the growing demands of compliance.



Cyber-Ark Privileged Identity Management   27/09/2011 | About | Logoff Karen | Help

Dashboard   Search: Leave empty to search all   Go

System Information

Policy Enforcement Status	45 accounts total
Valid policies	3
Policies with errors	9
Accounts not associated with a policy	4

CPM   Auto-detect

- 1 of 1 CPMs is active
- 41 accounts are managed by the CPM
- 8 accounts are disabled by users
- 11 accounts are disabled by the CPM

Accounts Statistics   Show account statistics by: PolicyID

Show account activity for: Last 24 hours | Last 48 hours | Last 7 days | Last month | Last quarter

Privileged Identity & Session Management delivers one central dashboard console for managing and monitoring all types of privileged accounts.

Why CyberArk?

CyberArk is the trusted expert in stopping cyber attacks before they stop business.

The Challenge

In today's environment, organizations which serve as national critical infrastructure, such as energy and water utilities, oil and gas companies, transportation authorities and others, spend a great deal of resources building defenses for securing their critical assets, assuring reliability, business continuity and meeting compliance requirements. In recent years, critical facilities have been integrating more general IT and COTS systems into their Operational Technology (OT) environments (e.g. SCADA, Industrial Control Systems, etc). This trend introduces many known risks from the IT environment into the OT environment – raising the risk level due to the critical infrastructure which this environment serves. Adding to the risk is the growing requirement from the business for Industrial control systems (ICS) originated data. This requires network connectivity into the segregated OT environment which was once physically isolated, introducing new risks and security considerations.

The typical operational environment is comprised of hundreds or thousands of servers, databases, desktops, virtual machines, SCADA RTUs and PLCs, network devices and applications, all controlled and managed by a variety of privileged and shared administrative identities, which are the most powerful identities in the organization. Ironically, the security, control and auditability of these privileged identities is often neglected, their usage difficult to monitor, and changing the passwords on a periodic basis is often hard to manage. In some cases, these identities are required not only by the internal IT/OT personnel, but also by external 3rd party vendors, and thus require extra care, such as secure remote access without exposing the credentials.

Unmanaged privileged identities pose the following challenges:

- Internal and External Threats. In many organizations, the same root or Administrator password is used across the production network, making it easier for a disgruntled insider to abruptly take down critical systems, access or steal sensitive information, or even take control of key systems. External threats are also increasingly penetrating the organization and targeting critical infrastructure, attempting to gain access to privileged accounts and cause detrimental damage.
- Audit and Accountability. Regulations in the different critical industries require organizations to provide accountability over who accessed shared accounts, what was done, and whether passwords are protected and updated according to a security policy that prohibits the usage of default or weak passwords.

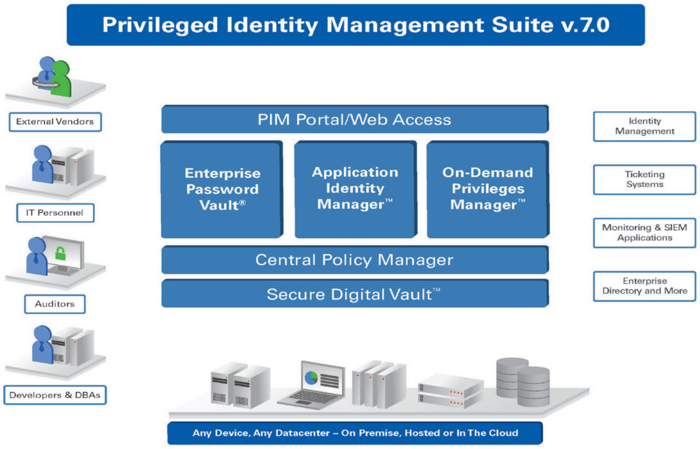
  Some regulatory examples for managing privileged identities include:

  - North America Electric Reliability Corporation - Critical Infrastructure Protection (NERC CIP)
  - Chemical Facilities Anti Terror Standards (CFATS)
  - U.S. Nuclear Regulatory Commission (NRC)
- Administrative Overhead. With hundreds of critical systems, privileged identities can be extremely time-consuming to manually update and report on and more prone to human errors. Moreover, inaccessibility of such a password by an on-call administrator may cause hours of delay in recovering from system failure.

The Solution

CyberArk's Privileged Identity Management (PIM) Suite is the industry-leading solution that secures, manages and tracks all privileged account access and activities associated with management of a critical operational environment.

Complementing the PIM Suite is CyberArk's Privileged Session Management (PSM) Suite that isolates privileged sessions connecting to sensitive target machines, preventing potential cyber attacks and controls and monitors all privileged activities on servers, databases or virtual environments with a


Privileged Identity Management Suite v.7.0
External Vendors
IT Personnel
Auditors
Developers & DBAs
PIM Portal/Web Access
Enterprise Password Vault®
Application Identity Manager™
On-Demand Privileges Manager™
Central Policy Manager
Secure Digital Vault™
Identity Management
Ticketing Systems
Monitoring & SIEM Applications
Enterprise Directory and More
Any Device, Any Datacenter – On Premise, Hosted or In The Cloud

zero-footprint solution. The pre-integrated suites share a common platform that together delivers a central command and control point for controlling and monitoring all privileged access and activities across your operational systems, creating a proactive approach to continuously protecting and securing critical assets.

The two Suites, engineered to work together from the ground up, allow you to better manage internal or external risks while improving workforce efficiency and meet audit and compliance requirements.

Benefits

- **A Preventative Approach Against Threats.** PIM manages, secures and controls access to all privileged accounts and makes hard-coded application credentials invisible to developers, database administrators, third parties and IT staff. PSM ensures continuous monitoring of who is accessing your critical infrastructure and gives a clear picture of what they are doing. The overall result is an improved security posture that eliminates default or weak credentials, controls privileged access and creates full accountability.
- **Meet Compliance and Audit Requirements with Confidence.** PIM and PSM Suites enforce corporate security policies and work flows to ensure compliance with regulatory needs and create easy to use, unified audit reports required by NERC-CIP, CFATS, NRC and more. By enforcing security policies around privileged accounts and easily being able to provide proof around activity, organizations are audit-ready and can save time when preparing for their next audit. Auditors enjoy the benefits of PIM & PSM with pre-scheduled reports and session recordings for forensic analysis and point in time playback.
- **Improve OT Efficiency with Automated Password Management.** Streamline and automate the process of managing thousands of privileged accounts on critical devices according to regulation or internal requirements. This allows for an extremely reliable and uninterrupted service, while ensuring the protection of critical infrastructure with no privileged credentials remaining static and vulnerable to abuse.
- **Improved Control over External Contractors.** Allow external contractors a secured and transparent connection into the network without divulging the password, while enabling full monitoring and recording capabilities. The ability to monitor sessions in real-time means you do not need to be physically next to the contractor and, in the event of suspicious activity, the session can be terminated.
- **Enterprise-Ready.** With industry leading performance, scalability and robustness, PIM and PSM can protect and manage up to hundreds of thousands of privileged accounts across a highly heterogeneous OT environment, with complex and distributed network architectures and integrate with core enterprise systems.
- **Fast and Easy Adoption Means Short Time to Value.** Quick to deploy with a proven track record of improving OT productivity. Our experience spans hundreds of enterprise customers in all verticals, including a third of the Fortune 50 and some of the top 50 energy companies worldwide, providing fast ROI.

CyberArk is helping more than 70 leading Energy companies meet the stringent compliance requirements in this sector.

1 in every 3 Fortune 50 companies have selected CyberArk.