



PAM BOOSTER INTEGRATION GUIDE

DOCUMENT PURPOSE: THIS DOCUMENT PRESENTS HOW THE RADIANTONE IDENTITY ANALYTICS SOLUTION, PAM BOOSTER, INTEGRATES WITH CYBERARK PAM AND CYBERARK PRIVILEGE CLOUD SOLUTIONS.

Name of Company: Radiant Logic

Website: www.radiantlogic.com

Name of Product: PAM Booster

Version: March 2024

Date: 03/29/2024

PARTNER SOLUTION OVERVIEW

Radiant Logic was launched in 1995 with the invention of the virtual directory forever changing how organizations get the most value from their identity data. The company continued to innovate in the Identity and Access Management (IAM) sector and garnered customers from the Fortune 500 to government agencies. Brainwave GRC was acquired in 2023 allowing Radiant Logic to create the industry-first Identity Data Management and Analytics platform.

One of the Radiant Logic flagship products is “RadiantOne Identity Analytics.” RadiantOne’s platform component, Identity Analytics, embeds the PAM Booster, designed for CyberArk. PAM Booster provides a turnkey solution to streamline the administration and control of access rights to gain visibility into the configuration of the CyberArk Privileged Access Manager solution and/or CyberArk Privilege Cloud. It can be used by customers who have already deployed CyberArk or are doing so.

PAM Booster delivers everything needed to meet audit requirements and ensure regulatory compliance (ISO27001, PCIDSS, SOC, etc.) The service correlates employee information with CyberArk and LDAP/AD (groups and users) to enforce least privilege and need-to-know principles to ensure that the identity lifecycle is aligned with privileged access. In addition, the PAM Booster monitors the CyberArk environment, including LDAP/AD and CyberArk Identity, to detect unauthorized changes, avoid drift, and keep control of the CyberArk access chain. PAM Booster facilitates the communication of business KPIs related to the CyberArk deployment to stakeholders, such as C-level leadership, safe owners, line managers. No need to be a CyberArk expert to use PAM Booster.

RADIANT LOGIC: THE LEADERS IN IDENTITY DATA MANAGEMENT AND ANALYTICS



Inventor of the virtual directory and holder of multiple patents in identity



Named Gartner Cool Vendor multiple times (2013, 2016, 2022)



Managing over 50M identities and +280M objects in a single deployment



Received a large investment from TA Associates in 2021



Rated 4.8/5.0 on Gartner Peer Insights™



Selected by NIST's NCCoE for multiple cybersecurity implementations, including Zero Trust Architecture project

Deployed in 60 of the Fortune 500

- 6 of the 10 Top Healthcare Providers
- 6 of the 10 Top FIServe Institutions
- 28 of the Fortune 100

ACCOLADES

"At a high level, Radiant Logic helps organizations make sense out of complicated IAM infrastructure by providing a global view across the entire IT estate, such that every application can use it... Radiant Logic can be conceptually thought of as an 'Informatica for identity data'."
—Datos Insights

"Radiant eliminated integration as the roadblock to every new project."
— Insurance corporation

"Deploying Radiant Logic saved us over \$100M dollars in customization."
— Large healthcare conglomerate

PAM Booster is the ideal solution to:

- Align employee and access standards and perform data cleansing in AD/LDAP and CyberArk environments
- Provide a 360° view of organizations, users, entitlements, and associated history information for forensic analysis. Answer the questions, “Who has access to what?” and “Who accessed what?”
- Automate continuous access control for privileged accounts
- Detect and analyze the impact of configuration changes on CyberArk assets to suggest remediation based on the root cause
- Provide consolidated reporting data for stakeholders such as safe or line managers and C-level executives.

KEY BENEFITS

PAM Booster designed for CyberArk streamlines the administration and control of rights and provides visibility into your CyberArk PAM and Privilege Cloud system configuration. Key benefits are:

- Knowing and strengthening identity and access governance
 - An exhaustive vision of access rights which includes HR, LDAP/AD and CyberArk correlated data
- Less effort to produce and share reports
 - Share dashboards and reports with safe owners and C-level executives
 - Provide visibility to external auditors and internal controllers
 - Ensure compliance for audits
 - Continuously check the security policy compliance
- Improved accuracy corrective actions:
 - Solve data quality issues and mitigate security risks
 - Identify atypical situations and provide remediation suggestions.



When using CyberArk, the initial risks that exist at the privileged account level are controlled. However, some risks can remain at the CyberArk user account level. This means that user accounts are critical. Who has access to the CyberArk accounts in the company? Is this access legitimate? Are these accounts being managed properly and allocated appropriately?

For example, user account management for PAM is often delegated to third-party, LDAP solutions such as Active Directory. Therefore, adding a user account to a group allows it to access privileged accounts. A management error at this level can be fatal.

The automation of controls is essential to ensure that the right people have access to highly privileged, critical resources, considering the context of their identities, or the HR context. Here is a partial list of the controls that are frequently found in such environments:

- Are there people not from IT teams who have access to privileges using CyberArk? Which privileges do they have access to? What resources are involved, and is this legitimate?
- Are there people in R&D who access privileged accounts through CyberArk in production?
- Who can administer Active Directory groups that provide access to privileged accounts in CyberArk?
- Are there people who can both backup and restore the same perimeter in CyberArk which could allow them to commit fraud?
- Which people have changed jobs, departments or have left the company altogether and still have access to privileged accounts using CyberArk?

During the lifetime of the company, people leave, new jobs are created, and departments are reorganized. Digital transformation is also causing the rapid evolution of information systems. As a result of these changes, it is essential to be able to address these issues regarding access to the Privileged Accounts Management solution, such as CyberArk, and to regularly limit the risk of compromise.

With its powerful analysis engine and award-winning patented data model, Radiant Logic addresses these issues by continuously automating these controls and reviewing access to privileged accounts within the organization to ensure that only the people responsible for each technology silo have legitimate privileged access to it.

Changes inside and outside of CyberArk can affect risk and the security of credentials. The Identity context, AD, LDAP or even the CyberArk solution are managed by different teams. Each of these teams can work well within the scope of their responsibilities and make changes, creating risk without even knowing it.

This is why Radiant Logic embeds automated IT controls in PAM Booster. The objective of IT controls is to highlight the riskiest situations caused by these changes and provide the end user a ready-to-use analysis including the root cause and suggested remediations.

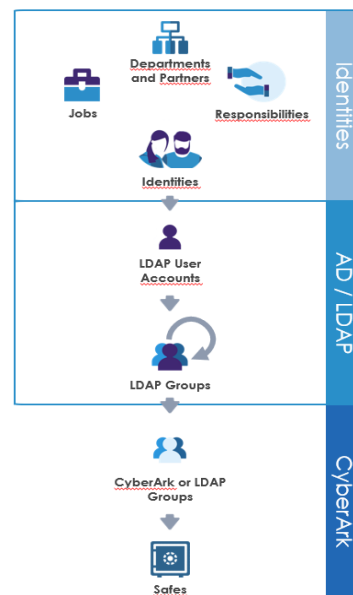
Ready-to-use, C-level dashboards, such as license usage and onboarding progress, are also provided in the solution. The end user can also create search queries and define new controls in business language on all the loaded resources. For example, he can look for contractors who have left the company but still have access to some specific secrets, or for developers who can administer safes in production. These results can be listed and have analytics applied to create and share new dashboards.

DATA CORRELATION, A KEY DIFFERENCIATOR

One of the key differentiators of RadiantOne is its ability to automatically correlate multiple sources of data to uncover the full access chain, from identities to credentials in safes and vice versa.

All the powerful investigations, the specialized IT controls, and other features available in PAM Booster use the access chain principle to provide the most accurate analysis to the end user.

This allows the highlighting of any unauthorized changes, the enforcement of the least privileged and need-to-know principles, and the creation of understandable dashboards that can be shared with stakeholders.



CONTROL PLAN DETAILS

PAM Booster allows the automation of controls to discover atypical situations relating to the company's organizational context. These controls are organized in two parts, one listing the risky situations and the other showing the data quality issues. The following controls are provided by default with a risk level. This is then used to compute a risk ranking per identity and account. It is also possible to define controls based on a specific context, if needed.

Risk controls

- Vault and safe user account owner left – risk level 4.
- Contractors without an expiration date that can manage a safe/vault – risk level 4.
- Users without an expiration date that can manage a safe/vault – risk level 3.
- Users that can manage both a safe and use its contents – risk level 3.
- Users with access to both a vault and access to a safe inside the vault – risk level 3.
- CyberArk credentials for which automatic password rotation is disabled (CPM) – risk level 3.
- Vault and safe orphaned user account – risk level 2.
- Users with at least one direct permission to a safe/vault (not through groups) – risk level 2.
- Users that can both audit and administer the same vault – risk level 2.
- Users that can both backup and restore the same vault – risk level 2.

Quality controls

- Empty safes.
- Dormant users with safe/vault access.
- Disabled users with safe/vault access.
- Technical/service accounts with safe/vault access.

- Empty groups that give access to safes/vaults.
- Groups with only disabled users giving access to safes/vaults.
- Groups with only one group giving access to safes/vaults.
- Groups with only one user giving access to safes/vaults.
- Vault and safe user accounts with direct ACL (not using groups).
- Vault and safe dormant user accounts (not used for more than 3 months).
- Vault and safe disabled user account.

PRODUCT DIAGRAM AND DESCRIPTION OF PRODUCT INTEGRATION

PAM BOOSTER DESCRIPTION AND CYBERARK INTEGRATION

PAM Booster is provided through Kubernetes or through the SaaS platform to provide rapid deployment and time to value. Each PAM Booster tenant is completely isolated per customer and databases and backup are fully encrypted. PAM Booster can also be installed in an on-site environment.

The service comes with data extraction connectors that allow the extraction of data from AD, LDAP and CyberArk, the gathering of all the data, including HR (Identity Context data), AD, LDAP, CyberArk data (CyberArk Identity, CyberArk Privilege Cloud, CyberArk PAM), and the uploading of it to the PAM Booster tenant of the customer in a secured and encrypted manner through HTTPS.

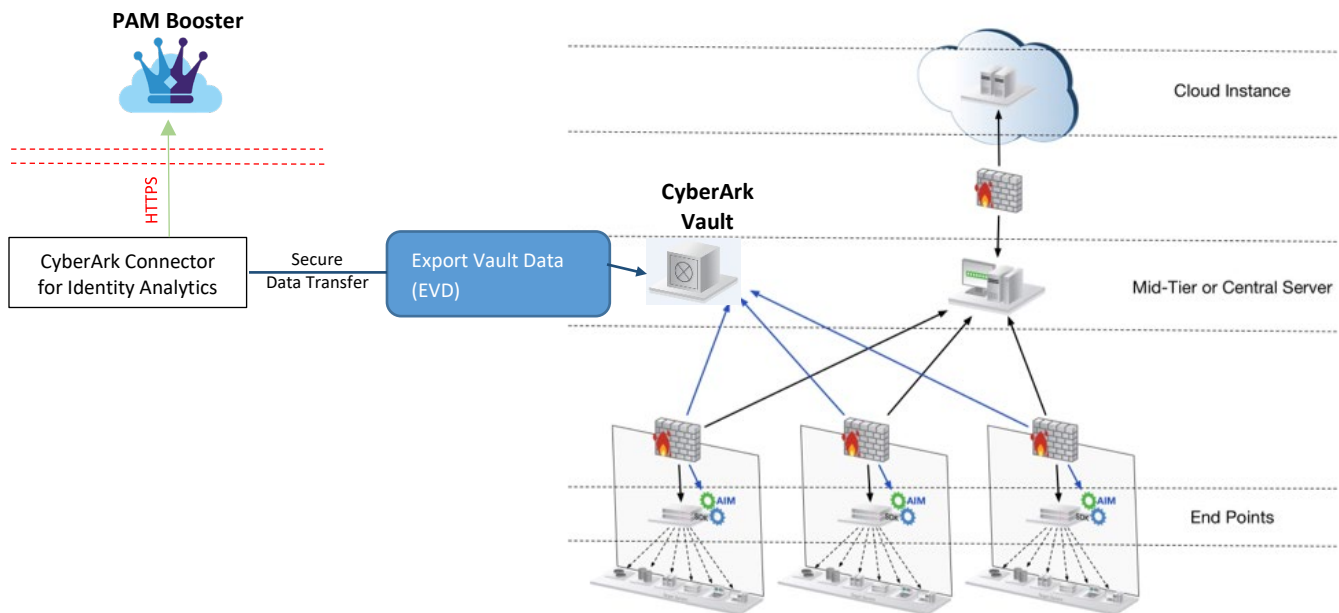
In a typical installation, the "CyberArk Connector for RadiantOne Identity Analytics" is deployed in a server with access to PVWA (or EVD for on-premises environments), and the connector is scheduled on a regular basis using the scheduling tool of the customer.

Data extracted using REST/API or EVD is stored in CSV files and are prefixed by the vault name. Here is the data requested and the method used to extract it:

DATA Type	From Application	Method	Description	Comments about the used method
Accounts	CyberArk PAM	EVD	List of all the accounts (secrets) in the vault.	EVD does not provide all information of a secret like the address, the username, the CPM flags and other attributes.
Group Members List Report	CyberArk PAM	EVD	The "Group Members List Report" contains a list of group members for each group in the vault.	
Groups List Report	CyberArk PAM	EVD	The "Groups List Report" contains a list of the groups in the vault and their location in the vault hierarchy.	Rest API has low performance.
User and Safe Activities Report	CyberArk PAM	EVD	The "User and Safe Activities Report" includes all the activities carried out by users on other users/groups/locations and all the operations carried out by users in the different safes in the vault. Each activity is marked as either a "User Activity" or a "Safe Activity".	Rest API does not provide safes and user activity logs.
Owners List Report	CyberArk PAM	EVD	The "Owners List Report" contains a list of owners of the safes in the vault and their permissions.	
Safes List Report	CyberArk PAM	EVD	List of all safes in the vault.	EVD has better performance than REST API but do not get all information like CPM flags.
Users List Report	CyberArk PAM	EVD	List of all users in the vault.	EVD has better performance than REST API but do not get all information like suspended and componentuser attributes.
LDAP directories config (PVWA)	CyberArk PAM & CyberArk Privilege Cloud	Manual export	Export the List of LDAP directories declared in the vault from PVWA.	Both REST API and EVD do not provide a way to extract LDAP directories configuration details. The only way is to export it manually from PVWA.
Get all Safes	CyberArk Privilege Cloud	REST API	List of all safes in the vault.	

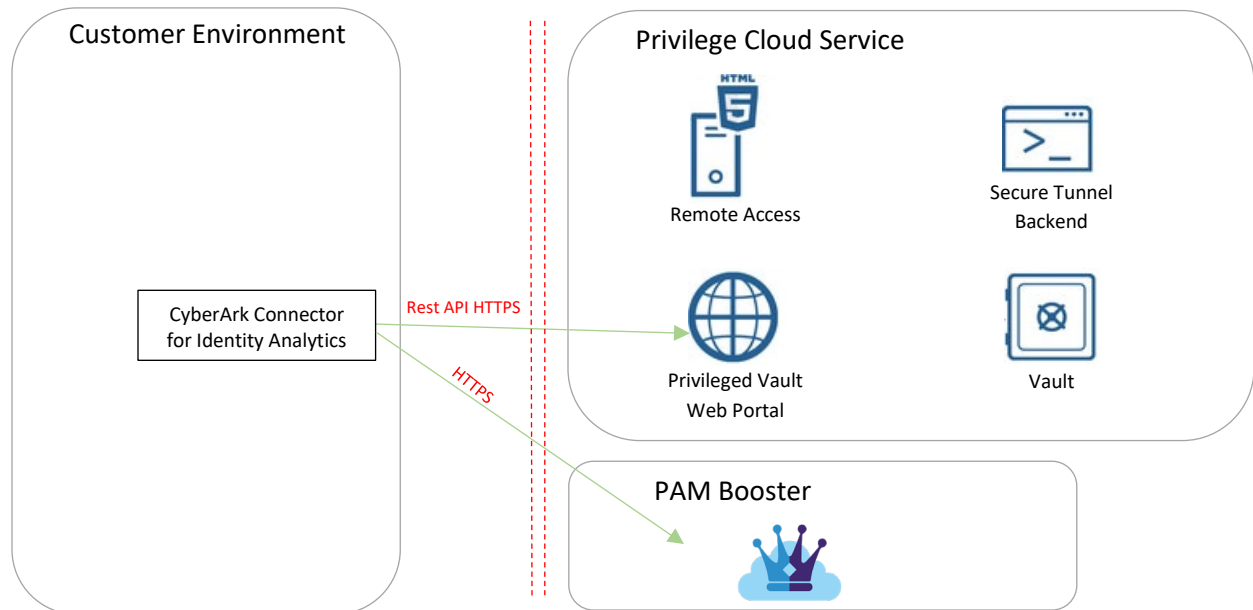
Get users	CyberArk Privilege Cloud	REST API	List of all users in the vault.	
LDAP mappings	CyberArk Privilege Cloud	REST API	List all LDAP mappings.	EVD does not provide LDAP mappings.
ADGroup	CyberArk Identity	REST API	Active Directory groups for the tenant	
ADUser	CyberArk Identity	REST API	Users belonging to Active Directory	
CDUser	CyberArk Identity	REST API	Users enrolled in the Cloud user service	
DSGroups	CyberArk Identity	REST API	Groups from all directory services used by the tenant	
DSUsers	CyberArk Identity	REST API	Users from all directory services used by the tenant	
Proxy	CyberArk Identity	REST API	Cloud connectors (proxies) that the tenant can use or is currently running	
Role	CyberArk Identity	REST API	All roles defined for the tenant	
Roles Members	CyberArk Identity	REST API	Get role members	
Roles Admin Rights	CyberArk Identity	REST API	Get assigned administrative rights associated of role	

Schema of the PAM Booster in SaaS integration with CyberArk PAM:



In CyberArk Privilege Cloud, the extraction method using Rest/API is the same as for the CyberArk PAM on-premises environment except that EVD is not available. Therefore, only the Rest/API is used.

Schema of the PAM Booster in SaaS integration with CyberArk Privilege Cloud:



FLOW AND CREDENTIAL RETRIEVAL IN RADIANTONE

End-user logins to access the PAM Booster tenant are done through SSO or synchronized with the Identity Provider of the customer. The password/secret of this user is not stored in PAM Booster but managed by the IDP and the client authentication referential.

Here is the list of credentials that is used in the Radiant One Identity Analytics solution:

- PVWA CyberArk access account to extract data (GET only) through the API, used on demand by the data extraction connector for CyberArk. This secret is stored in the client environment where the end customer centralized the data extraction using the CyberArk Central Credential Provider, or if CCP is not available, the Powershell tool PSCredential.
- CyberArk credentials to extract data through EVD when CyberArk PAM is on-site. Used on demand by the data extraction connector for CyberArk, this secret is stored in the client environment where EVD is used to extract data. It is created through the utility provided by CyberArk "CreateCredFile."

Connection between the RadiantOne data extraction connector and the PAM Booster through HTTPS is based on the data import frequency, typically once a week and automatically scheduled using batch. It is the same for the connection accounts to the CyberArk environment to extract data.

The access to the PAM Booster end-user interface can be done at any time by end users through HTTPS from their web browser using their account login and password. The recommended scenario is to interface the PAM Booster service with the preferred Identity Provider, be it Azure AD, Google, or Okta. We support SAML v2 and OpenID Connect. If MFA is mandatory in the identity domain, it will immediately benefit PAM Booster's authentication as well.

Regarding notifications, SMTP notification is activated to automatically notify the end user about the status of the data ingestion, if it succeeds or fails, when data is uploaded to the PAM Booster.

PAM BOOSTER INSTALLATION AND INTEGRATION CONFIGURATION

Refer to the online documentation to start using PAM Booster:

[Identity Analytics](#) | [Radiant Logic Documentation](#)

Once the Identity Analytics tenant is provided and PAM Booster activated, download the data extraction connector from the Radiant Logic marketplace and check the guides and documentation from there.

CYBERARK LICENSING REQUIREMENTS

PAM Booster works with CyberArk Privileged Access Manager and CyberArk Privilege Cloud.

The supported versions of CyberArk PAM are listed here: <https://docs.cyberark.com/Product-Doc/OnlineHelp/EOL/en/Content/End-Of-LifePolicy.htm>

CYBERARK IMPLEMENTATION GUIDANCE

Any deployment of the CyberArk PAM version listed above is supported by PAM Booster.
The three following items will have to be configured:

- For on-premises CyberArk PAM:
 - o Install and configure the EVD tool and add a user to extract data using EVD as listed in the table earlier in this document.
- For CyberArk Privilege Cloud:
 1. Set the maximum number of accounts that may be displayed in a view ("MaxDisplayedRecords") to the right value. The REST API configuration in PVWA should allow the export of the right number of secrets that the customer has. (For example, if the vault contains 42,000 credentials, the limit should be set to 50,000.)
 2. Add a user for the REST API in PVWA to be able to extract the required data as listed in the table earlier in this document.

TROUBLESHOOTING

LOG GATHERING

DATA EXTRACTION

In the zip file generated by the data extraction connector, there is a status file called "status.csv" and a "logs" folder containing one log file per extraction. The file "status.csv" contains one line per action and the result status. Regarding the CyberArk extraction, the file is named "ExtractCA_{timestamp}.log" and contains details of extractions according to the "-LogLevel" parameter.

Please contact your Radiant Logic Customer Success Manager or the support team if assistance is required.

PAM BOOSTER

The PAM Booster produces computer traces called Application Logs during its execution (use of functionalities by the end user). These Application Logs allow the monitoring of the good health of the PAM Booster and the proper execution of the functionalities. When SaaS deployment of the solution, the Application Logs can be consulted by the Support department to monitor the health of the PAM Booster or to qualify incidents.

In SaaS mode, any access to the PAM Booster production environments is tracked and monitored.

COMMON ERRORS: FILE VALIDATION ERRORS

When data is uploaded to the platform, it is analyzed. The format of each file is checked. If an error is detected, it is indicated in the Application Logs. A status indicates if all the files in the category are valid or if an error is detected.

In case of an invalid file, the corrections must be made outside the PAM Booster. Once this is completed, the whole ZIP file must be uploaded again onto the platform.

PARTNER CONTACT INFO

Business Contact	Name	Jeff Tishgart
	Email	jtishgart@radiantlogic.com
Technical Contact	Name	Damien Besson
	Email	dbesson@radiantlogic.com
Support Contact	Name	support
	Email	support@radiantlogic.com