



# CYBERARK CONNECTOR FOR RADIANTONE IDENTITY ANALYTICS

## INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Radiant Logic

Website: [www.radiantlogic.com](http://www.radiantlogic.com)

Name of Product: CyberArk Connector for RadiantOne Identity Analytics

Version: DESCARTES

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 Radiant Logic flagship products is RadiantOne's platform component, Identity Analytics, which provides a turnkey solution for the audit and compliance control of user entitlements in the information system, such as accounts, roles, fine-grained access rights, etc.

RadiantOne Identity Analytics has been specifically designed for business sectors subjected to advanced compliance or security requirements, such as banking, insurance, healthcare and other sensitive industries. With RadiantOne Identity Analytics, customers can fully automate the retrieval and consolidation of user access rights on many disparate IT systems to provide a comprehensive entitlement map. A control plan can then be configured to automatically produce reports and analyses and take remediation actions.

In addition, RadiantOne Identity Analytics involves all the concerned parties as it manages schedules, distributes access reviews through the lines of business to the appropriate reviewers and continuously tracks progress.

## RADIANT LOGIC: THE LEADERS IN IDENTITY DATA MANAGEMENT AND ANALYTICS

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

 Received a large investment from TA Associates in 2021

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

 Rated 4.8/5.0 on Gartner Peer Insights™

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

 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

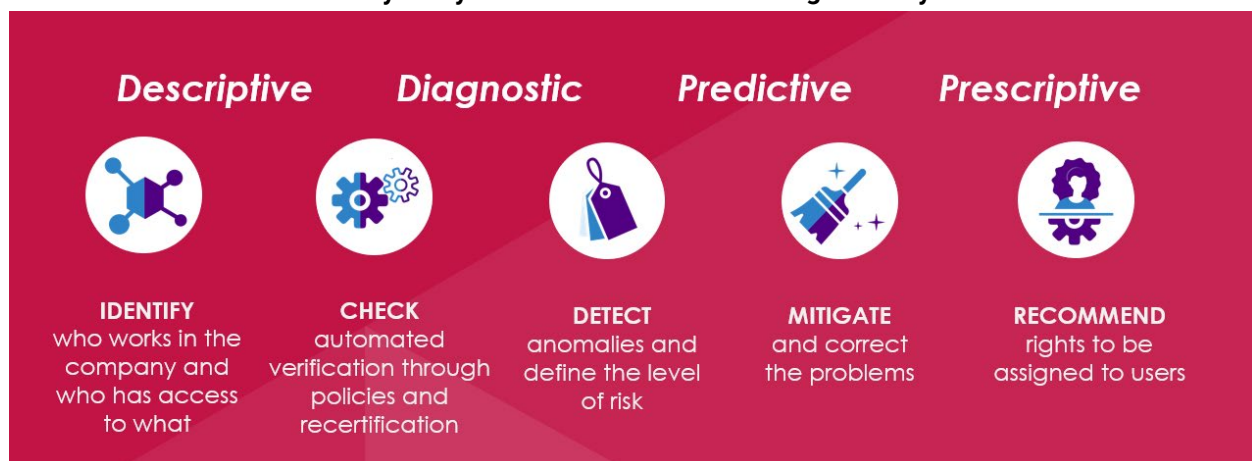
**RadiantOne Identity Analytics** is the ideal solution to:

- Align your employees to access standards and perform data cleansing
- Provide a 360° view of organizations, users, and entitlements (“Who has access to what? Who accessed what?”)
- Provide consolidated reporting data for stakeholders
- Measure and manage risks related to application and data access
- Carry out access reviews and recertification
- Automate reporting to internal and external auditors and senior management
- Continuously monitor access security

## KEY BENEFITS

**Secure and govern your whole environment with RadiantOne Identity Analytics:**

### Identity Analysis: the Science of Access Rights Analysis



**RadiantOne Identity Analytics Benefits:**

- Know and strengthen identity and access governance
- Solve data quality issues and mitigate security risks
- Automate access reviews through lines of business
- Benefit from an exhaustive vision of access rights which includes any data type (cloud, in-house applications, on site, etc.)
- Provide visibility to external auditors and internal controllers
- Ensure compliance for audits
- Continuously verify compliance with security policies
- Identify atypical situations in the systems and provide remediation through ITSM or IAM tools

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.

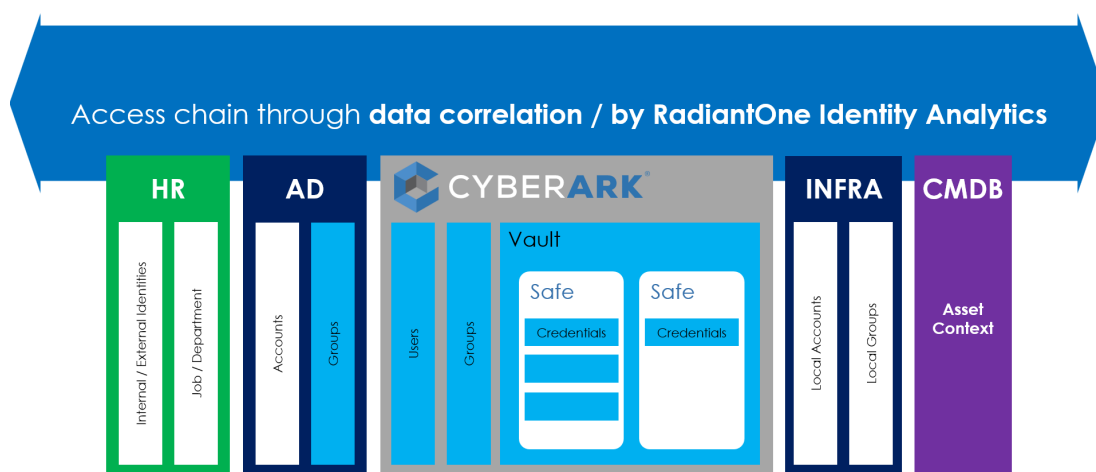
With its powerful analysis engine and award-winning patented data model, Radiant Logic addresses these issues by continuously automating controls and reviewing access to privileged accounts within the organization to ensure that only the people responsible for each technology silo have legitimate, privileged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

Review automation can also help to establish a recurring process asking Safe owners directly to check users accessing their safe and identify if these users are legitimate or not.

A review of orphaned accounts per application or technical owner can also be configured to identify if these are privileged accounts. In this way, it is easier to add them to the IAM and PAM process perimeter to secure and better control these privileged accesses.

## DATA CORRELATION, A KEY DIFFERENTIATOR

One of the key differentiators of RadiantOne Identity Analytics is its ability to automatically correlate multiple sources of data in order to rebuild the full access chain.



## PRODUCT DIAGRAM AND DESCRIPTION OF PRODUCT INTEGRATION

### 1. RadiantOne Identity Analytics Description and CyberArk Integration

When deploying the solution on-premises, all Identity Analytics components should be installed in the Mid-Tier or Central Server area. They can be installed on the same server or separately, depending on customer constraints and data volume. The components are the following:

#### Identity Analytics Client

The [identity analytics](#) studio or client is a client application that can be deployed on a Windows environment. The [identity analytics](#) client is used to configure the solution (reports, workflows and custom data collect). Web packages are prepared through the [identity analytics](#) client to deploy web instances of the solution. This interface is to be considered as a configuration interface during the “build” phase, as it is not needed during the “run” phase. This component can be installed on an end-user desktop (end points) and/or on a server (Mid-Tier or Central Server) accessible through RDP.

#### . Identity Analytics Server (Batch)

The [identity analytics server](#) is Java-based and can either be deployed on a Windows or a Linux environment.

This component can be triggered by a task scheduler to automate data loading processes on the [Identity Analytics](#) database.

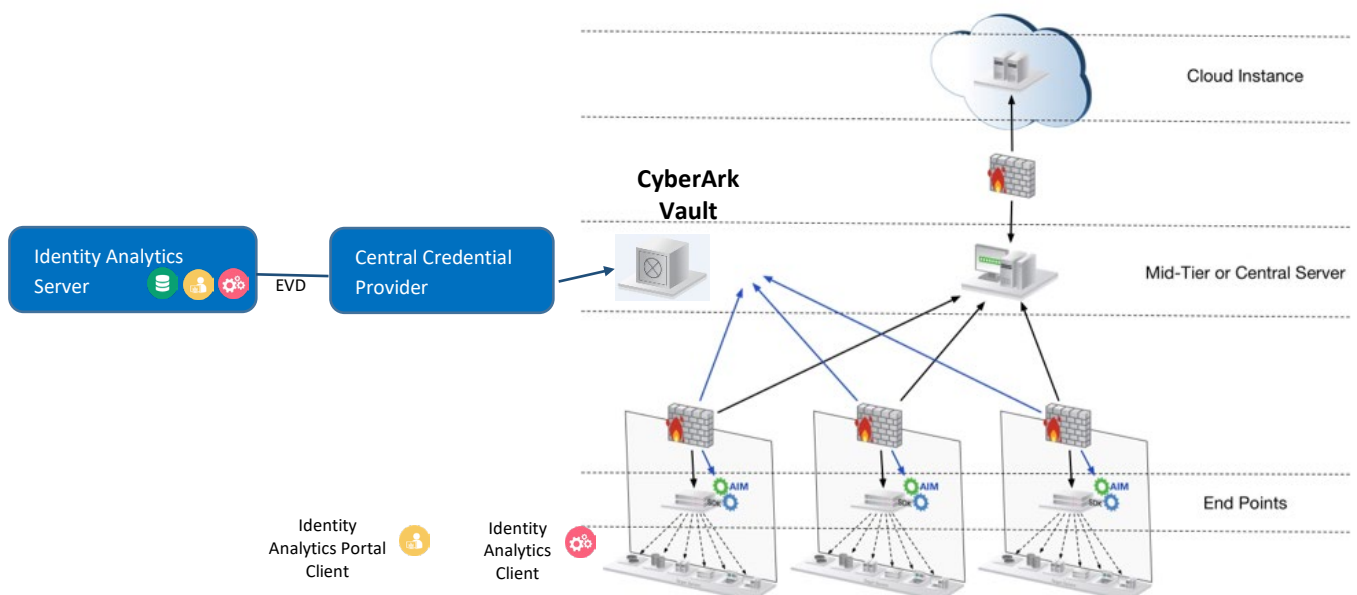
The loaded data comes from files automatically extracted regularly by the customer from systems to audit or from connectors (extraction scripts) provided by [Radiant Logic](#) and scheduled by the customer.

#### . Identity Analytics Portal

The [identity analytics portal](#) is a web application and is deployed on an Apache Tomcat web server and connected to the [identity analytics](#) database to leverage the data.

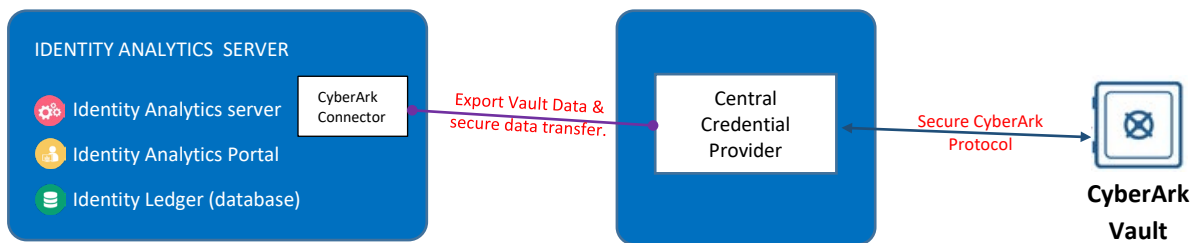
#### . Identity Ledger (Database)

The identity ledger is stored in a relational database. This database instance is accessed by the web portal, the analytics server, and the analytics client.

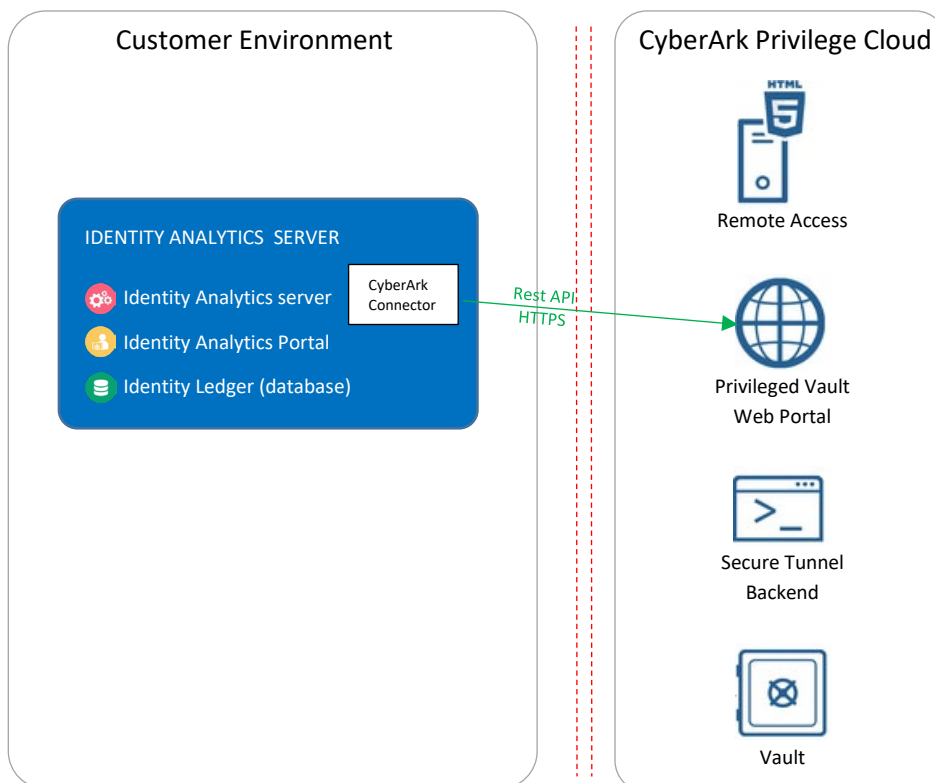


In a typical installation, the Identity Analytics Server and Portal are deployed on a same server. The Database is deployed remotely (SQL server/Oracle/Postgres), and the Identity Analytics Client is installed locally on the end-user computer of the RadiantOne administrator/integrator.

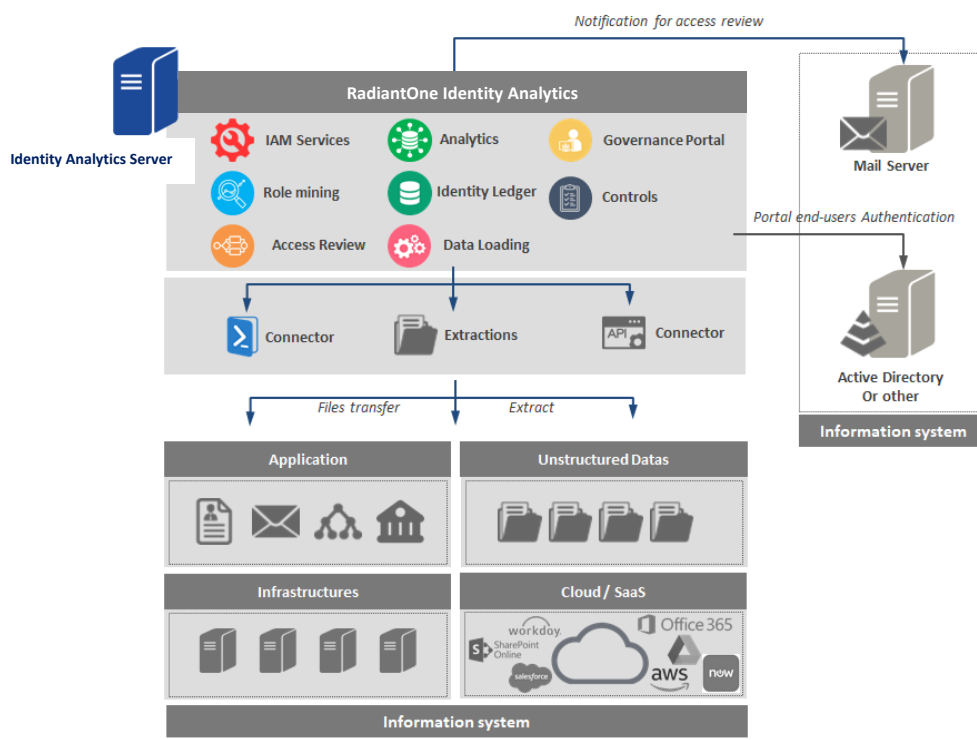
Schema of the RadiantOne Identity Analytics integration with CyberArk PAM:



Schema of the RadiantOne Identity Analytics integration with CyberArk Privilege Cloud:



## 2. Flow and Credential Retrieval in RadiantOne Identity Analytics



Here is the list of credentials that are used in the RadiantOne Identity Analytics environment:

- End-user logs in to access the Identity Analytics Portal client: SSO or synchronized with AD.
- Identity Ledger access (database): a dedicated owner account of the instance is used to import and browse data, used by the Identity Analytics Portal permanently, Identity Analytics server and Identity Analytics client on demand.
- Access accounts to Identity Analytics server environments (Linux or Windows), used on demand
- PVWA CyberArk access account to extract data (GET only) through the API when CyberArk Privilege Cloud is used, used on demand.
- CyberArk credentials to extract data through EVD when CyberArk PAM is on premise, used on demand.

The access from Identity Analytics Portal to the Identity Ledger (database) is a permanent connection. All other accounts can be used on demand during deployment and conception by the RadiantOne administrator/integrator.

During the “run” phase, the Identity Analytics client is no longer used. Connection between the Identity Analytics server and database is based on the data import frequency, typically once a week or once a month and automatically scheduled using batch. This is the same for the connection accounts to the CyberArk environment to extract data.

Access to the Identity Analytics Portal client can be done at any time by end users from their web browser using their AD/LDAP account login and password.

Regarding review and remediation, SMTP notification can be activated if needed to automatically notify review/re-certification actors and technical/application owners when an access review is pending or remediation actions require validation.

## PARTNER PRODUCT INSTALLATION AND INTEGRATION CONFIGURATION

Refer to the online documentation to install **RadiantOne Identity** Analytics in your environment: [Installation and deployment | Radiant Logic Documentation](#)

Once the RadiantOne Identity Analytics environment is fully installed and configured, download the CyberArk add-ons available in our Marketplace to deploy the CyberArk reporting:

<https://marketplace.radiantlogic.com/>

The following add-ons and their dependencies will be required:

1- For data extraction and collect

The add-on **bw\_ias\_cyberark** provides the CyberArk PAM data extraction agent using EVD for an on-premise CyberArk PAM environment. The agent is also able to extract data from CyberArk Privileged Cloud using REST/API. In addition, the agent federates all data coming from the various sources (HR, AD, LDAP, CyberArk, etc.). The add-on also manages the creation of the data cube in RadiantOne Identity Analytics, data correlation and the control plan rules.

Please follow the documentation provided with these add-ons to extract and collect data.

2- For reporting and dashboarding

The add-on **bw\_iap**: The PAM Booster is now part of this add-on. When PAM Booster is activated, this add-on provides standard reports and dashboards relative to CyberArk PAM or CyberArk Privileged Cloud. It includes search pages and detail pages for vaults, safes and credentials. The dashboards provide KPIs, graphs of users access chain, the control defect lists, and safe user access reviews among others.

## 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. These controls can be customized and defined depending on your context:

### 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.

### 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   |