



ENDPOINT PRIVILEGE MANAGER

EPM Integration – Technical Documentation

Name of Company: Cigent Technologies, Inc

Website: <http://www.cigent.com/>

Name of Product: Dynamic Data Defense Engine (D3E)

Version: 1.4.23

Date: March 27, 2020

Contents

Overview	2
Key Benefits	2
Cigent Product Integration Architecture	3
CyberArk Integration.....	3
Integration Pre-requisites	3
Cigent Integration Configuration	4
Cigent D3E Installation.....	5
CyberArk EPM Installation	5

Overview

The Cigent Dynamic Data Defense Engine™ (D3E) is a new approach to data security, one that complements existing solutions and places the importance of protecting data above **all** else. D3E takes concepts used in threat containment and continuous authentication and applies them as close to the data stream as possible, bringing proactive protection directly to your data. D3E allows users to safely and easily access critically important information, even if the system is already compromised. The result is an unprecedented level of protection, detection, and response to cyberattacks, insider threats, and lost or stolen devices.

Cigent's management console is the centralized mechanism for monitoring, managing and controlling Cigent D3E deployments. Cigent's management console natively supports integration with CyberArk's Endpoint Privilege Manager's management console providing increased value and security to users of both solutions.

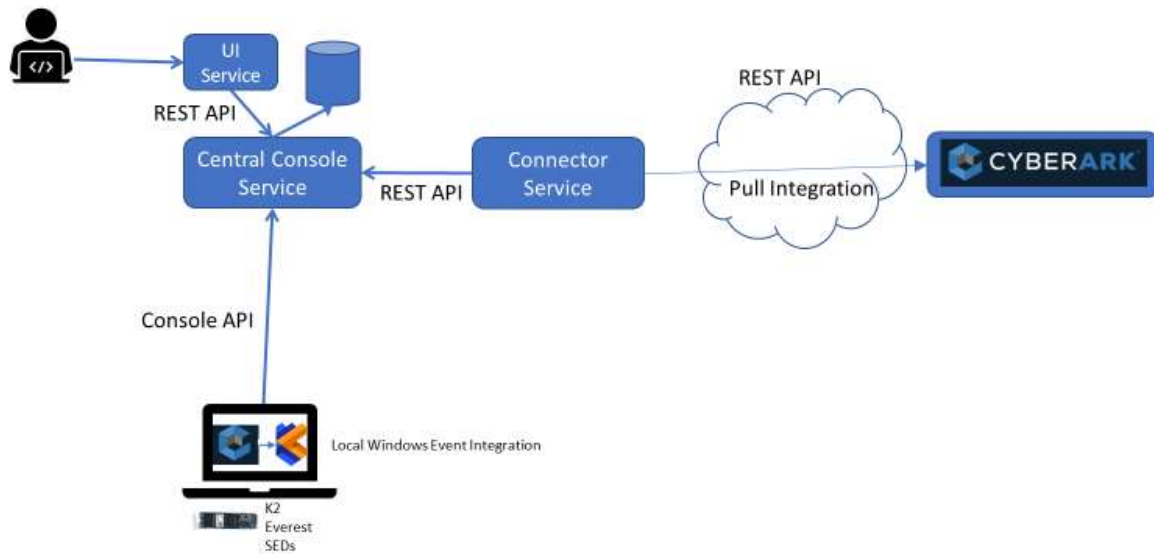
Key Benefits

Cigent D3E provides an additional response option for threats discovered by CyberArk's EPM solution. This response ensures files designated as sensitive by the end user are protected by adding a second factor authentication requirement to access the files during the heightened security state. End users can continue to access their files while in heightened security state and even clear the threat should they or their SOC determine the threat has been remediated.

Cigent Product Integration Architecture

The Cigent Management Console Connector Service communicates directly with the CyberArk EPM management console over the internet using CyberArk REST APIs. No additional software or infrastructure is required by the customer to enable this integration.

Cigent High Level Architecture



CyberArk Integration

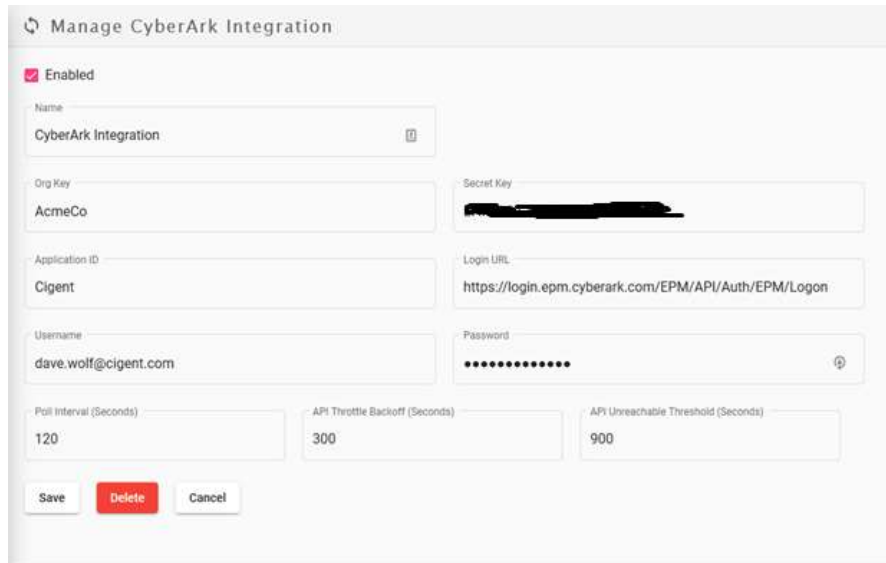
Cigent Management Console users can setup, activate and delete integrations to their CyberArk EPM autonomously. This integration is known as a pull integration as the Cigent Management Console will poll the CyberArk EPM console periodically to determine if any threats have been raised for devices under Cigent management. If so, an Active Lock enable request is immediately sent to the Cigent D3E endpoint to protect the user's sensitive files.

Integration Pre-requisites

Both Cigent D3E and CyberArk EPM endpoints need to be installed on devices on which users desire this additional layer of response.

Users must have administrative access to both Cigent and CyberArk's management consoles.

Cigent Integration Configuration



Navigate to <https://central.cigent.com/integrations>

Select 'New CyberArk EPM Integration' fill in the mandatory fields then click save.

MANDATORY FIELDS:

Name : Unique name for the Integration. This will appear on the home page along with health status.

Org Key : A unique alphanumeric. Can be the same as Name.

App ID: CyberArk required API field. This is the source application ID to distinguish between REST API calls from EPM and REST API calls from another application. Suggested value : Cigent (<https://docs.cyberark.com/Product-Doc/OnlineHelp/EPM/Latest/en/Content/WebServices/ServerAuthentication.htm>)

Secret Key : Unique key provided by Cigent. Contact support for a new key.

Login URL : Use <https://login.epm.cyberark.com/EPM/API/Auth/EPM/Logon> for CyberArk SaaS deployments. If you have an on premise deployment, enter an externally reachable URL.

Username/Password : Credentials to CyberArk with sufficient privileges to execute APIs. It is suggested to use a Service account rather than an administrator account.

Poll Interval : Interval in seconds to check for new threats. Suggested : 120, Minimum : 60

API Throttle Backup : Time in seconds to stop polling if throttled by CyberArk. Suggested : 300

API Unreachable Threshold : Time in seconds to raise Cigent alert if a successfully API connection could not be raised.

Cigent D3E Endpoint Installation

Refer to “D3E Quick Start and Evaluation Guide V6.pdf” for Cigent D3E installation guidance.

https://d3efiles.cigent.com/eval/D3E_Quick_Start_and_Evaluation_Guide_V6.pdf

CyberArk EPM Agent Installation

Refer to CyberArk EPM Agent installation documentation for guidance.

https://docs.cyberark.com/Product-Doc/OnlineHelp/EPM/Latest/en/Content/EPM_PET/AgentInstallation.htm.

No special setup or configuration of the CyberArk EPM Agent is required to enable integration.