



CYBER**ARK**®

// LOGPOINT

Endpoint Privilege Manager

Integration Guide

Logpoint

<https://www.logpoint.com/en/>

Logpoint Version: 7.2.3.

Date: May 31, 2020

Partner Product Overview

Logpoint enables organizations to convert data into actionable intelligence, improving their cybersecurity posture and creating immediate business value. Our advanced SIEM, UEBA and Automation and Incident Response technologies, simple licensing model and market-leading support organization empower our customers to build, manage and effectively transform their businesses.

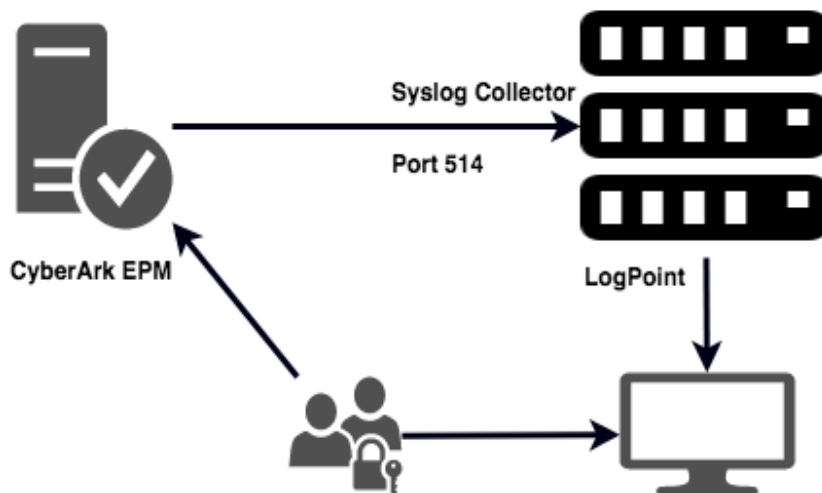
We provide cybersecurity automation and analytics that create contextual awareness to support security, compliance, operations and business decisions. In other words, we offer unified simplicity in a complex world.

Key Benefits

- Automated policy creation
- Privilege management
- On-demand privilege elevation
- Application control
- Greylisting
- Behavioral analysis
- Threat detection capabilities
- Automated policy updates

Product diagram and description of the integration

CyberArk Endpoint Privilege Manager can integrate with SIEM to send audit logs through third-party applications and create a complete audit picture of privileged account activities in the enterprise SIEM solution.



Installation of CyberArk Endpoint Privilege Manager v6.1:

Reference EPM CyberArk Endpoint Privilege Manager Solution Guide and review the chapters on “Enabling Third-Party Event Forwarding” and “Understanding Syslog Messages.”

1. Download the CyberArk Endpoint Privilege Manager Solution Guide from [Logpoint Help Center](#).
2. Install the package by importing the .pak file to Logpoint under *Settings >> System >> Applications*.
3. Add the required device in Logpoint.
4. Create a **Normalization Policy** then add the required CyberArk Endpoint Privilege Manager packages.
5. Create a relevant **Routing Policy**.
6. If required, create an **Enrichment Policy**.
Create a new enrichment policy under *Settings >> Configurations >> Enrichment Policies*
7. Create a **Processing Policy** with the previously created normalization policy, routing policy and enrichment policy. If the enrichment policy is not required, select **None** for the same.
8. Create a **Log Collection Policy** and configure the **Syslog Collector** by adding the processing policy created in step no 7.
9. Assign the log collection policy to the device.

Supported Versions

CyberArk Endpoint Privilege Manager supported with Logpoint in this configuration is:

- CyberArk Endpoint Privilege Manager version 6

Configuration of Sources

Expected Log format

- Semicolon delimited key-value pairs

Log Format:

```
<134>Oct 10 06:01:13 LP2: /EventInfo/Header/setId="xxxxxx-xxxx-xxxx-xxxx-xxxxxx";/EventInfo/Header/setName="WINLP2";/EventInfo/Header/agentId="xxxxxxxx-xxxx-xxxx-xxxx-xxxxxx";/EventInfo/Header/computerName="xxxxxx";/EventInfo/Header/eventId="976";/EventInfo/Event/ZeroTouchEvent[reliability]="2";/EventInfo/Event/FileInfo[targetType]="3";/EventInfo/Event/FileInfo[owner]="NT AUTHORITY\SYSTEM";/EventInfo/Event/FileInfo[reqExecLevel]="";/EventInfo/Event/FileInfo/Description="TODO: <File description>";/EventInfo/Event/FileInfo/Hash="SHA1##595AB96F28B1AA58E08C6EA9053C235974B5FE36";/EventInfo/Event/FileInfo/Path="C:\Program Files\NCR APTRA\Advance LP\VPITCPIPCOMServer.exe";/EventInfo/Event/FileInfo/LocType="FIXED";/EventInfo/Event/FileInfo/Size="319488";/EventInfo/Event/FileInfo/ModifTime="1305465119600000000";/EventInfo/Event/FileInfo/V1="-Embedding";/EventInfo/Event/FileInfo/V2="TODO: <File description>";/EventInfo/Event/FileInfo/V3="1.0.0.1";/EventInfo/Event/FileInfo/V4="TODO: <Product name>";/EventInfo/Event/FileInfo/V5="1.0.0.1";/EventInfo/Event/FileInfo/V6="TODO: <Company name>";/EventInfo/Event/ActionInfo[targetId]="{xxxxxxxx-xxxx-xxxx-xxxx-xxxxxx}";/EventInfo/Event/ActionInfo[policyId]="241";/EventInfo/Event/ActionInfo[policyAction]="1";/EventInfo/Event/ActionInfo[count]="1";/EventInfo/Event/ActionInfo[user]="S1A28501\SSTAuto1";/EventInfo/Event/ActionInfo[userIsAdmin]="False";/EventInfo/Event/ActionInfo[timeFirst]="131514082549299775";/EventInfo/Event/ActionInfo[timeLast]="131514082549299775";/EventInfo/Event/ActionInfo/PolicyName="Default Policy: Monitor Access";/EventInfo/Event/FileOrigin[version]="1";/EventInfo/Event/FileOrigin[preexisted]="true"
```

Parsed values

```
2020/04/27 05:19:50
log_ts=2020/04/27 05:19:13 ~ user= ~ device_ip= ~ device_name= ~ col_type=syslog ~ sig_id=7863355 ~ repo_name= ~ severity=6 ~ facility=16 ~ event_id=976 ~ policy=Default
Policy: Monitor Access ~ datasize=319488 ~ hash=595AB96F28B1AA58E08C6EA9053 ~ workstation= ~ agent_id= ~ algorithm=SHA1 ~ application_version=1.0.0.1 ~ col_ts=2020/04/27
05:19:50 ~ collected_at=LogPoint ~ command_line_argument=Embedding ~ count=1 ~ description=TODO: <File description> ~ end_ts=2011/09/04 12:53:45 ~ file_description=TODO: <File description> ~ file_origin_version=1 ~
file_version=1.0.0.1 ~ is_user_admin=False ~ location_type=FIXED ~ logpoint_name=LogPoint ~ modify_ts=2011/05/15 13:11:59 ~ norm_id=CyberArkEPM ~ organization=TODO: <Company name> ~ owner=NT
AUTHORITY\SYSTEM ~ path=C:\Program Files\NCR APTRA\Advance LP ~ policy_action=1 ~ policy_id=241 ~ pre_existed=true ~ product=TODO: <Product name> ~ reliability=2 ~ set=WINLP2 ~ set_id= ~
start_ts=2011/09/04 12:53:45 ~ target_id= ~ target_type=3 ~
<134>Apr 27 05:19:13 LP2: /EventInfo/Header/setId="
"/EventInfo/Header/setName="WINLP2"/EventInfo/Header/agentId="
"/EventInfo/Header/computerName="
"/EventInfo/Header/eventId="976"/EventInfo/Event/ZeroTouchEvent[reliability]="2"/EventInfo/Event/FileInfo[targetType]="3"/EventInfo/Event/FileInfo[owner]="NT AU
THORITY\SYSTEM"/EventInfo/Event/FileInfo[reqExecLevel]=""/EventInfo/Event/FileInfo/Description="TODO: <File description>"/EventInfo/Event/FileInfo/Hash="SHA1##595AB96F28B1AA58E08C6EA9053C235974B5FE36"/EventI
fo/Event/FileInfo/Path="C:\Program Files\NCR APTRA\Advance LP\Server.exe"/EventInfo/Event/FileInfo/LocType="FIXED"/EventInfo/Event/FileInfo/Size="319488"/EventInfo/Event/FileInfo/ModifTime="130546511960
000000"/EventInfo/Event/FileInfo/V1="-
Embedding"/EventInfo/Event/FileInfo/V2="TODO: <File description>"/EventInfo/Event/FileInfo/V3="1.0.0.1"/EventInfo/Event/FileInfo/V4="TODO: <Product name>"/EventInfo/Event/FileInfo/V5="1.0.0.1"/EventInfo/Event/FileInfo
/V6="TODO: <Company name>"/EventInfo/Event/ActionInfo[targetId]="{
}"/EventInfo/Event/ActionInfo[policyId]="241"/EventInfo/Event/ActionInfo[policyAction]="1"/EventInfo/Event/ActionInfo[count]="1"/EventInfo/Event/ActionInfo[user]="
\SSTAuto1"/EventInfo/Event/ActionInfo[userIsAdmin]="False"/EventInfo/Event/ActionInfo[timeFirst]="131514082549299775"/EventInfo/Event/ActionInfo[timeLast]="131514082549299775"/EventInfo/Event/ActionInfo/PolicyName="Default Policy: Monitor Access"/EventI
nfo/Event/FileOrigin[version]="1"/EventInfo/Event/FileOrigin[preexisted]="true"
```

Partner contact info

Business Contact	Name	Edy Almer
	Email	eal@logpoint.com
	Tel	
Technical Contact	Name	Basudev Raut
	Email	brv@logpoint.com

	Tel	
Support Contact	Name	Santosh Baral
	Email	sab@logpoint.com
	Tel	