

Waterfall and CyberArk Overview and Diagram

Waterfall Unidirectional Security Gateways replace firewalls in industrial network environments, providing absolute protection to control systems and operations networks from attacks originating on external networks. Unidirectional Gateway solutions come in pairs: the TX appliance contains a laser, and the RX appliance contains an optical receiver. The Gateway pair can transmit information out of an operations network, but is incapable of propagating any virus, DOS attack, human error or any information at all back into the protected network.

Per the diagram below, clients can utilize CyberArk to monitor usage of privileged credentials in the OT network and send privileged user activity through the Waterfall Security unidirectional gateway to a SIEM and PTA for analysis and reporting. This provides a secure way for clients to combine the privileged user activity in both the IT and OT networks into one system for reporting and analysis.

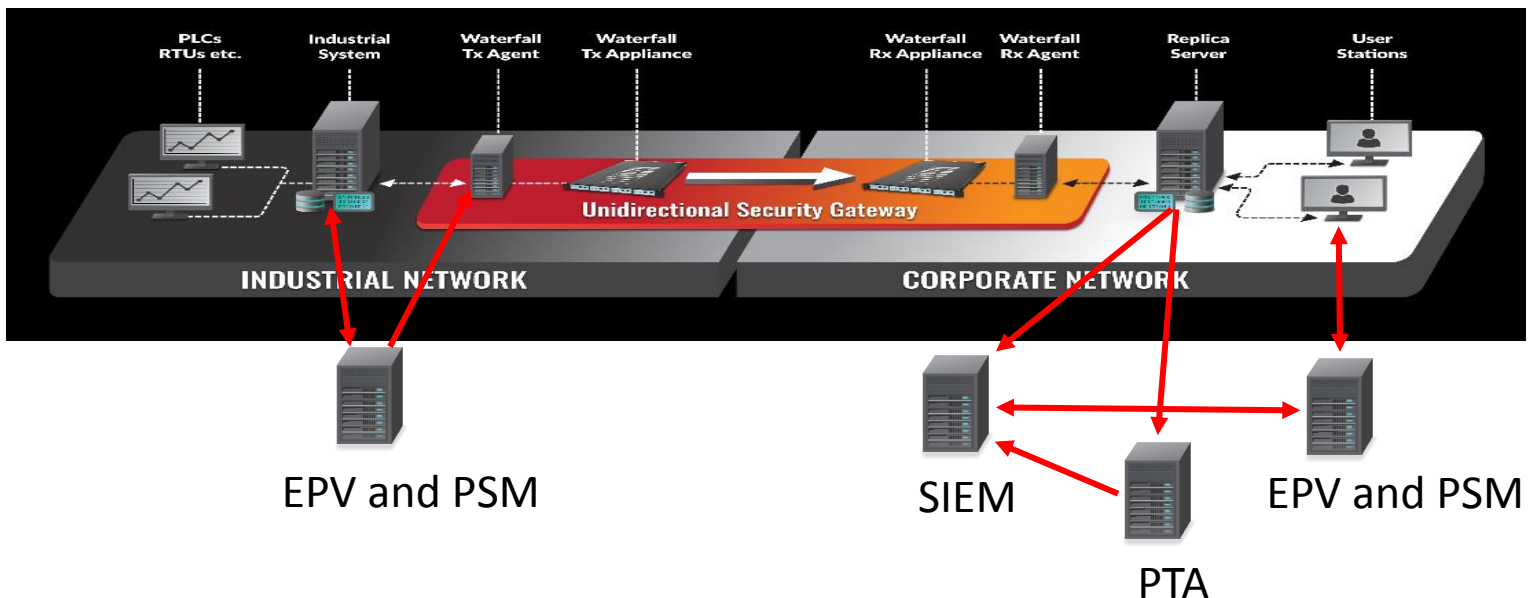


Diagram Overview:

1. Within the Industrial network, activity will be sent to the Waterfall Transfer agent
2. In addition, users will need to use EPV to authenticate within the Industrial Network, all of this activity will be sent to the Waterfall Transfer agent
3. The Waterfall Transfer agent will securely send the privileged user activity to the Waterfall RX agent and then to the Waterfall replica server securely through the unidirectional gateway
4. Within the corporate network, all user activity will be sent to the replica server including the IT privileged user activity from EPV
5. The Waterfall replica server will combine all of this activity and send the appropriate logs to PTA and SIEM
6. PTA will send any alerts that are identified to the SIEM

To Configure Waterfall Security Integration:

1. In DBParm.ini, configure the following parameters:

- **SyslogServerIP** – The IP address(es) of the Syslog servers where messages will be sent. Specify multiple values with commas.
- **SyslogServerProtocol** – Specifies the Syslog protocol that will be used to send audit logs. Specify either **TCP** or **UDP**. The default value is **UDP**.
- **SyslogServerPort** – The port used to connect to the Syslog server. The default value is **514**.
- **SyslogMessageCodeFilter** – Defines which message codes will be sent from the Vault to the SIEM application through Syslog protocol. You can specify message numbers and/or ranges of numbers, separated by commas.
For example, to specify messages 1,2,3,30 and 5-10, specify the following value: 1,2,3,5-10,30. By default, all message codes are sent for user and Safe activities, change the setting to send message codes 1-999 only. For a list of messages and codes, refer to the Privileged Account Security Reference Guide.
- **SyslogTranslatorFile** – Specifies the XSL file used to parse CyberArk audit records data into Syslog protocol.
- **DebugLevel** – Determines the level of debug messages. To include Syslog xml messages in the trace file, specify **SYSLOG(2)**.
- **UseLegacySyslogFormat** - Controls the format of the syslog message, and defines whether it will be sent in a newer syslog format (RFC 5424) or in a legacy format. The default value is **No**, which enables working with the newer syslog format. Specify multiple values with commas.

The following example shows a set of syslog properties that will send a single message to multiple syslog servers.

```
SysLogServerIP=192.168.1.1,192.168.2.2,192.168.3.3  
SysLogTranslatorFile=Syslog\Arcsight.sample.xsl  
UseLegacySyslogFormat=yes  
SyslogMessageCodeFilter=7,8,295
```

The following example shows a set of syslog properties that will send different syslog messages to multiple syslog servers.

```
SysLogServerIP=192.168.1.1,192.168.2.2,192.168.3.3  
SysLogTranslatorFile=Syslog\Arcsight.sample.xsl,Syslog\QRadar.xsl,  
Syslog\Arcsight.sample.xsl  
UseLegacySyslogFormat=yes,no,yes  
SyslogMessageCodeFilter=7,8,295|295-296|7
```

2. Copy the relevant XSL translator file from the Syslog subfolder of the Server installation folder to the location specified in the SyslogTranslatorFile parameter in DBParm.ini. During Vault installation or upgrade, the following sample XSL files are copied to the PrivateArk\Server\syslog folder:

- RSAenVision.sample.xsl
- Arcsight.sample.xsl
- QRadar.sample.xsl
- McAfeeESM.sample.xsl
- SyslogTranslator.sample.xsl
- RFC5424Changes.xsl

