Additional License Authorizations

For OpenText Security Analytics software
products – Standard Edition Model

Products covered

These are the products covered under this ALA. If your product is **not** listed below please review the December 2018 version of ALA.

This Additional License Authorizations document ("ALA") set forth the applicable License Options and additional specific software license terms that govern the authorized use of the software products specified below, and are part of the applicable agreement (i.e., Micro Focus End User License Agreement; and/or any separate agreement that grants Licensee a license to such products (e.g., Customer Portfolio Terms or other Master Agreement); and/or Quotation) (the "Applicable Agreement"). Capitalized terms used but not defined herein shall have the meanings set forth in the Applicable Agreement. All products below are delivered electronically, and as such, any reference to software delivery methods that are stated on the purchase order other than electronic are void.

Products	**Non-production software class***	**Subscription license Non-production software class****
OpenText Enterprise Security Manager (ArcSight Enterprise Security Manager (ESM) Standard Edition)	Class 1	Class 1
OpenText Logger (ArcSight Logger Standard Edition)	Class 1	Class 1
OpenText Behavioral Signals (ArcSight Intelligence Standard Edition)	Class 1	Class 1
ArcSight Investigate Standard Edition	Class 1	Class 1
OpenText SIEM Management Center (ArcSight Management Center (ArcMC Software)	Class 1	Class 1
OpenText Secuirty Log Analytics (ArcSight Recon Standard Edition)	Class 1	Class 1
OpenText SIEM Data Platform (Security Open Data Platform (SDP))	Class 1	Class 1
Third Party Destination add-on per Target	Class 1	Class 1
Transformation Hub	Class 1	Class 1
OpenText L8000 Logger (ArcSight L8000 for Logger Server*)	Class 3	N/A
OpenText R8000 Security Log Analytics (ArcSight R8000 for Recon Server*	Class 3	N/A
OpenText R8100 Security Log Analytics (ArcSight R8100 for Recon Server*)	Class 3	N/A
OpenText C8200 Connector Hosting appliance (ArcSight C8200 Sled Appliance*)	Class 3	N/A
OpenText E8400 for ESM appliance (ArcSight E8400 Sled Appliance*)	Class 3	N/A
OpenText EC8300 appliance	Class 3	N/A
OpenText DB8400 appliance	Class 3	N/A
OpenText W8300 appliance	Class 3	N/A
OpenText L7700 for Logger appliance (ArcSightL7700 for Logger Gen10 Server*)	Class 3	N/A
OpenText E7700 for ESM appliance (ArcSightE7700 for ESM Gen10 Server*)	Class 3	N/A
OpenText C6700 Connector Hosting Appliance (ArcSight C6700 Gen10 for Connector Hosting Server*	Class 3	N/A
OpenText ThreatHub Feed Plus (ArcSight ThreatHub Feed Plus)	Class 3	Class 3
OpenText User Behavior Monitoring (ArcSight User Behavior Monitoring)	Class 1	Class 1

*Appliances are physically shipped.
**Additional licenses solely for non-production use may be available as specified in the Non-Production Licensing Guide found at opentext.com/about/legal/software-licensing depending on the non-production software class specified above. Any such non-production licenses will be subject to the Non-Production Licensing Guide and the applicable License Option terms and conditions set forth in this ALA.

Definitions

These are the new revised definitions for the newly repackaging products only. If you own the products that are on a different model please review the **December 2018 version of ALA**.

Term	Definition
Active Passive High Availability (APHA)	A failover system that is actively replicating the primary Instance of ESM and must be sized at the same hardware capacity as the production instance. If the primary ESM server fails, the other server can rapidly take over for it.
Actor	Any Entity being monitored by software. See “Managed Entity” for further definition.
Appliance	An Instance of software loaded and pre-configured on a Server.
Application Server	A software framework that provides both facilities to create web applications and a server environment to run them.
Asset	A single IT Device imported or created within the software.
Cloud	A generic reference to infrastructure, platforms, or applications that are hosted or run outside of an organizations’ on-premise or data center environment.
Cluster	A set of loosely or tightly connected computers that work together so that they can be viewed as a single system.
Cold Standby System	A standby, Non-Production System, which is not up and running. If the production system breaks down, or needs to be taken out of service, it is required to be switched on and start the Cold Standby System in order to take over for the Production system. A Cold Standby System, for the purposes herein shall be considered a functional component of the production implementation though its use limited to moments of schedule service outages or failure situations.
Collector	A generic Connector component that focuses on collection of data via a generalized method not reserved or designated for an explicit Device, Application, or System. This form of Connector typically has a one-to-many relationship with the number of sources that it is collecting data from. An example of a Collector is Syslog.
Connector	A component within the OpenText solution that is intended to facilitate data acquisition and integration capabilities between OpenText and other Devices, Systems and Applications.
Destination	An OpenText CyberSecurity Products product that receives Events via Connectors or the Transformation Hub. Examples include but are not limited to ESM, Logger, OpenText Behavioral Signals, OpenText Security Log Analytics and Investigate.
Device	An addressable Asset, physical or virtual, including, but not limited to, routers, switches, bridge, hub, Server, handheld equipment, mobile equipment, printer etc., that resides within the range defined for interrogation and asset tracking. Generally considered a source of Events.
Entity or Managed Entity	A generic reference to a person or non-person within the context of behavioral analytics. Typically seen with the acronym UEBA or User Entity Behavioral Analytics as a means of drawing a distinction between human and non-human actor analysis. Examples of available Managed Entities include: User Accounts, Projects, shared drives, Machines, domain controllers, IP Address, Resources, Servers, Websites Printers, and Files.
Event	Includes any identifiable occurrence that has significance for system hardware, software, data or anything else relevant to operations of an environment.
Event Broker (also known as Transformation Hub)	Refers to the OpenText Transformation Hub component. This component an enterprise-scale high performance message delivery bus, including raw data normalization and enrichment capabilities used in security operations.
Event Forwarding	The act of retransmission of a collected Event from one OpenText SIEM component or product to either another OpenText SIEM, or 3rd party, component or application.
Events Per Day (EPD)	The total number of events generated in a twenty-four hour clock period. The clock is calculated based on UTC time starting at 00:00:00 and ending at 23:59:59, regardless of any local times that may be in use.

Term	Definition
Events Per Second (EPS)	Events Per Second, refers to a consumption or performance metric used to indicate both a level of expected performance that the SIEM should operate at as well as measurable metric of consumption for licensing purposes. The total number of events generated in a twenty-four hour clock period. The clock is calculated based on UTC time starting at 00:00:00 and ending at 23:59:59, regardless of any local times that may be in use.
Forwarding Connector	An OpenText SIEM Connector that enables the receiving of events from a source ESM installation and sends them to a secondary destination such as another ESM installation, non-ESM location, Transformation Hub, or an OpenText Logger installation.
Gigabytes (GB)	Refers to Gigabytes. A Gigabyte has two definitions of size based on Decimal and Binary methods of computation. The Decimal representation for 1 GB equals = 10003 or 1,000,000,000 bytes. The Binary representation for 1 GB equals = 10243 or 1,073,741,824 bytes. For the purposes of OpenText licensing discussions. The calculations between Events Per Day and Gigabytes Per Day is based on the Decimal representation of 1 GB.
Gigabytes per Day GB/per day *or* GB/d	Gigabytes Per Day. The total size of storage represented in GB collected in a twenty-four hour clock period. For the purposes of this document, the clock period shall be considered 00:00 - 23:59 utilizing standard 24 hour UTC time.
Guest Data	Any data posted on Topics within Transformation Hub, which is not generated by a SmartConnectors, FlexConnector, forwarders or Transformation Hub Connector and is made available to Targets as a pass through.
High Availability	Hot Standby System. Refers to a method of deployment where the Device, application, or System is implemented and configured in a manner that has a reasonable expectation of being constantly available. This term is generally reserved for implementations that must meet or exceed availability thresholds of 99% or greater.
Hot Standby System	A designated function within a High Availability or disaster recovery configuration. This function describes the context that the designated system is always in a perpetual ready state to service the requests or needs of users. Traditionally traits of a Hot Standby system are: Always on; Data/content/configuration is continuously synchronized with the active system, however the actual ability to fulfill the requests or needs of users, is disabled until the identified failure of the primary or active system.
Individual	Denotes a single person or Entity as distinguished from a group or class, and also, distinguished the person or Entity from a partnership, corporation, or association.
Ingestion	The act of receiving and consuming data through any OpenText supported collection component, mechanism, or function for the purposes of security operations analysis.
Instance	A unique instantiation of a component that provides a common set of functionality within an Implementation of the software or overall solution. Examples include, but art not limited to, multiple Instances of a connector used to service high volumes of Events, or multiple Instances of ESM. An Instance may run in a standalone manner or work in conjunction with other component Instances. By default an OpenText Implementation will contain a minimum of a single Instance of the installed application or components.
Integration Connector	A Connector that has a primary responsibility of facilitating the exchange of information between two applications, typically where one is part of the OpenText CyberSecurity family of products. Unlike ingestion Connectors, Integration Connectors focus on, but are not limited to, the passing of synthesized information, command and control capabilities, as well as state information. Examples include, but are not limited to, connections with ITSM solutions, CMDBs, IAM solutions, etc.
Key Server	A computer, typically an Appliance that receives and subsequently serves existing cryptographic keys to users or other programs. The users' programs can be working on the same network as the Key Server or on another networked computer. The Key Server may also include a function or capability that participates in.
Licensed Capacity	The total EPS that results from one or more capacity purchase transactions. For Example, the organization makes an initial purchase of 1,000 EPS. In a subsequent purchase transaction another 2,500 EPS is acquired. In this example, the Licensed Capacity is 3,500 EPS.

Term	Definition
Licensed EPS	Licensed EPS, is calculated based on Post-Filtered and Pre-Aggregated Events, and is counted on a rolling 45 day calendar. To establish a statistical median. The relevant metric for consuming licenses is by Moving Median Events per Second (MMEPS).
Moving Median Events per Second (MMEPS)	The median value is the SEPS value that is a number in statistics that identify the middle of a data set. The Moving Median Events Per Second (MMEPS) is the Median SEPS value calculated by shifting the evaluation window one day every twenty-four hours keeping 45 days as the dataset. The clock definition for a day used for this calculation is defined by UTC time 00:00:00 to 23:59:59 regardless of local times that may be in use.
Multiplexing	The act of inserting a component within an input or output flow chain with the intent of making multiple individual Devices, Systems, or applications appear to be a single data stream or connection regardless of intent or intended purpose. In such situations, when a multiplexing technology is utilized within the ingestion data flow each Device, application, or System is to be counted separately and subject to any applicable licensing terms and conditions. In situations where multiplexing technology is utilized with the output or routing of data that derives either from one or more OpenText applications or components, as well as any Guest Data that may be introduced to the Transformation Hub component, then each Target shall be counted separately and is subject to the applicable licensing terms and conditions for routing to non OpenText CyberSecurity family of products, or Micro Focus product destinations.
Non-compliance Finding	Results when an organization's MMEPS values exceed their Licensed Capacity for a minimum of forty-five consecutive days. This value is derived by taking the median value across the total consecutive days of non-compliance.
Not for Resale (NFR)	Refers to Not For Resale. A packaging and delivery term that denotes that the packaged software or solution, regardless of delivery method, may not be resold by the holder typically under any condition. Most commonly a classification of software made available by Micro Focus to its partners.
Nodes	Any physical or virtual Device within a network of other devices that can send, receive, and/or forward information.
Non-Production	A designation for specific computing environment within an organization that is not responsible for the delivery of the day-to-day operations of the business, rather reserved for other purposes such as development, testing, etc. May also be a designation of a component, application, or system that is installed and running in an environment that is not associated with the day-to-day physical operations and service delivery of the organization. This would typically refer to instances installed in a lab environment for evaluation, development, testing, etc.
Per Account	An organizational entity that is in an active contract with Micro Focus for an OpenText related product or service.
Post-Filtered	A designation of an Event that has not been removed for collection or analysis by a filter, regardless of the filter's location.
Pre-Aggregated	Denotes that the Event is counted as a singular entity, if it is counted, post- filtering. The aggregation capability of OpenText is the ability to roll up or summarize the occurrence of multiple Events into a singular Event for the purpose of efficiency. To be counted pre-aggregation means that if ten of the same Events occur and are aggregated into a singular Event, then the ten Events are counted as ten unique Events not one singular Event.
SaaS Subscription	Refers to Software as a Service, or an application that is delivered in an environment that is hosted outside the user's environment. The consumer of the application does not have a perpetual right to the software and pays for accesses for a given period of time that renews at the application publisher's defined interval.
Server or SVR	Means any designated computer system in which an Instance or Instances of the software is installed.
Subflow	A Subflow is a type of Workflow that is invoked by another Workflow.
Sustained EPS *or* SEPS	The "constant" Events Per Second that the system sustained within the twenty-four hour clock period. It normalizes peaks and valleys and gives a better indication of use. The formula used for this calculation is (EPD/(60*60)*24). For the purposes of this document, the clock period shall be considered 00:00 - 23:59 utilizing standard 24 hour UTC time.

Term	Definition
System	A set of applications, components, Devices working together.
Target	-A Non-OpenText CyberSecurity family of products to third party destination of the data leaving any of the Micro Focus products, including but not limited to the Transformation Hub, SmartConnectors, or Logger, via Event forwarding.
Terabyte (TB)	Refers to Terabytes. A Terabyte has two definitions of size based on Decimal and Binary methods of computation. The Decimal representation for 1 TB = 10004 equals or 1,000,000,000,000 bytes. The Binary representation for 1 TB equals 10244 or 1,099,511,627,776 bytes.
Topic	A Kafka topic storage location for messages.
User	A reference to a specific persons, Device, application, or System that engages in some way with the application with the intent to make use of one or more of the application's capabilities or functions.
Vertica Stored Data	Means the uncompressed data that is stored in a Vertica database, as if it such uncompressed data had been exported from the database in text format.
Workflow	A Workflow is an end-to-end process that automates typically manual tasks like invoking a script, calling a REST API, running an executable or any other programmatic method. Each Workflow is comprised of one or more Workflow Steps, and a Workflow can have nested Workflows – referred to as Subflows.
Workflow Step	A Workflow Step is a programmatic processing task comprised within a Workflow.

Software Specific License Terms

Software products with software specific license terms are described below.

For the avoidance of doubt, the Vertica database is only permitted for use as included in OpenText SIEM Platform Customer is prohibited from using Vertica as a stand-alone product or in conjunction with any other OpenText or third-party products.

As of **May 1, 2019** the following licensing model has been introduced:

OpenText Enterprise Security Manager (ESM) (ArcSight Enterprise Security Manager (ESM) Standard Edition)

ESM provides an event collection, aggregation, monitoring and analytics solution that enables users to ingest events from a variety of sources via the OpenText family of SmartConnectors and Transformation Hub part of the SIEM Data Platform. ESM facilitates real-time monitoring of events providing notification in one more user-defined conditions. As part of ESM's analysis capabilities, it provides real-time analytics consisting of event correlation and pattern detection of events across a range of one or more data sources. The results of the performed analysis are made known to the user through continuous monitoring and notification capabilities, as well as a comprehensive set of reporting capabilities.

Key points for ESM

- OpenText Enterprise Security Manager (ESM) Standard Edition is licensed by ingestion capacity measured in EPS that is calculated post-filter, pre-aggregation. Ingestion capacity is sold in tiers of: 100, 250, 500, 1000, 2500, 5000, 10000, 25000 and 50000. ESM, through use of the Forwarding Connector, may forward events to locations such as but not limited to high tier ESM implementations. When forwarding events from ESM, leveraging the Forwarding Connector, the only limits imposed are a result of hardware or performance constraints of the ESM software. No other limits are imposed.
- Users are included regardless of access via consoles or web users. Users and Devices are no longer counted or considered a relevant metric.

- No rights to forward data outside of OpenText SIEM Platform products without a separate purchase of Third-Party Destination per Target license. Use of Multiplexing technologies between OpenText SIEM Platform products and Third-Party Targets is not permitted.
- The software may be installed without licensing impact, regardless of the number of Instances.

Software	Offering Includes
OpenText Enterprise Security Manager (ESM)	▪ Enterprise Security Manager (v7.0 and higher) ingestion capacity in Licensed EPS ▪ Transformation Hub (v3.0 and higher) equivalent Licensed EPS capacity to ESM ▪ OpenText Management Center (v2.9 and higher) for centralized OpenText infrastructure management ▪ SmartConnectors 7.11.0 and higher

OpenText Security Logger (ArcSight Logger Standard Edition)

Logger provides an event collection, aggregation, analysis, and storage solution that enables customers to ingest events from a variety of sources inlcuding but not limited to the OpenText family of SmartConnectors and Transformation Hub, and self-contained collectors. Once ingested, logs are stored in an immutable long-term compressed data store for use in various search, compliance, auditing and reporting activities as required.

Key points for Logger Standard Edition

- Logger Standard Edition is licensed by ingestion capacity measured in EPS that is calculated post-filter, pre-aggregation. Ingestion capacity is sold in tiers of: 100, 250, 500, 1000, 2500, 5000, 10000, 25000 and 50000. Forwarding data only limited to the hardware or performance constraints of the Logger software.
- No rights to forward data outside of OpenText SIEM Platform products without a separate purchase of Third-Party Destination per Target license. Use of Multiplexing technologies between OpenText SIEM Platform products and Third-Party Targets is not permitted.
- GB/d is no longer a relevant metric.
- The software may be installed without licensing impact, regardless of the number of Instances

Software	Offering Includes
OpenText Security Logger	▪ Logger (v6.7 and higher) ingestion capacity in Licensed EPS ▪ Transformation Hub (v3.0 and higher) equivalent Licensed EPS to Logger ▪ OpenText Management Center Instance (v2.9) for centralized OpenText infrastructure management ▪ SmartConnectors 7.11.0 and higher

OpenText Behavioral Signals Standard Edition (ArcSight Intelligence Standard Edition)

OpenText Behavioral Signals provides security analytics capabilities whereby Managed Entities such as user accounts, workstations, and servers, are scored for risk based on the scope and scale of anomalies observed. It uses online unsupervised machine learning, which means that the solution automatically builds baseline data for all behaviors being monitored (aka, models). The actual models that are triggered are determined by the type of data being ingested as well as the data attributes that are present in the data.

OpenText Behavioral Signals Standard Edition package includes Behavior Signals and the following OpenText infrastructure components: Transformation Hub, OpenText Management Center (SIEM Management Center) and the SmartConnectors.

Examples of available Managed Entities are:

- User Accounts
- Projects
- Shared drives
- Machines (aka, workstations)
- Domain Controllers
- IP Addresses
- Resources
- Servers
- Websites
- Printers
- Files

Key points for OpenText Behavioral Signals Standard Edition

- OpenText Behavioral Signals Standard Edition is licensed by Managed Entities in the following six tiers: 1) 500 to 5000, 2) 5001 to 25,000, 3) 25,001 to 100,000, 4) 100,001 to 500,000, 5) 500,001 to 1,000,000 and 6) over 1,000,001.
- License compliance will be measured against the number of User Accounts reported by the Behavioral Signals user interface. For example, if a deployment of the product is licensed for 5,000 Managed Entities, it will be deemed in compliance if 5,000 or fewer "Users" are reported by the user interface.
- No rights to forward data outside of OpenText products without a separate purchase of Third-Party Destination per Target license. Use of Multiplexing technologies between OpenText products and Third-Party Targets is not permitted.
- The software may be installed without licensing impact, regardless of the number of Instances.
- Third-party business Behavior Signals or data query tools may be used to access and perform ad hoc queries on the embedded database systems. Extending the database schema beyond the intended use of the OpenText product is not permitted.

Software	Offering Includes
OpenText Behavioral Signals	▪ OpenText Behavior Signals Licensed by Managed Entities ▪ Transformation Hub (v3.2 and higher) Licensed in EPS to Entity tier purchased ▪ OpenText Management Center Instance (v2.9 and higher) for centralized OpenText SIEM infrastructure management ▪ SmartConnectors 7.15 and higher

OpenText Behavioral Signals OpenText Behavior Signals is licensed by the number of Managed Entities purchased. Transformation Hub is bundled with this product OpenText Behavior Signals and will have the following EPS capacity relative to the Entity tier they are purchased under.

Entities are tiered using the following framework and the tiers also designate the capacity allocated to Transformation hub.

Entities	
500 to 5000	Transformation Hub will have an EPS capacity of 15,000.
5001 to 25000	Transformation Hub will have an EPS capacity of 50,000.
25001 to 100,000	Transformation Hub will have an EPS capacity of 100,000.
100,001 to 500,000	Transformation Hub will have an EPS capacity of 150,000.
500,001 to 1,000,000	Transformation Hub will have an EPS capacity of 350,000.
1,000,001+	Transformation Hub will have an EPS capacity of 500,000.

ArcSight Investigate Standard Edition

Arcsight Investigate Standard Edition is a high-capacity, threat-investigation solution that enables users to search through and analyze vast amounts of event data for anomalies associated with such entities as users, IP addresses, and network assets. Information yielded from a search can help users detect and investigate breaches.

Key points for Investigate Standard Edition

- Investigate Standard Edition is licensed by ingestion capacity measured in EPS that is calculated post-filter, pre-aggregation. Ingestion capacity is sold in tiers of: 100, 250, 500, 1000, 2500, 5000, 10000, 25000 and 50000.
- This LTU does not permit the use of Vertica Premium Edition on a standalone basis, such as but not limited to, using third-party business Behavior Signals tools, loading data directly into the database or performance ad hoc queries independent of OpenText Security Investigate.
- No rights to forward data outside of OpenText products without a separate purchase of Third-Party Destination per Target license. Use of Multiplexing technologies between OpenText products and Third-Party Targets is not permitted.
- The software may be installed without licensing impact, regardless of the number of Instances.

Software	Offering Includes
OpenText Investigate Standard Edition	▪ Investigate (v2.3 and higher) ingestion capacity in Licensed EPS ▪ Transformation Hub (v3.0 and higher) equivalent Licensed EPS to Investigate ▪ OpenText Management Center Instance (v2.9) for centralized OpenText infrastructure management ▪ Vertica - 2 TBs for every 100 Investigate EPS (250 tier will receive 4 TBs) – limited for Investigate use only ▪ SmartConnectors 7.11.0 and higher

OpenText Management Center (SIEM Management Center) Software per Instance

OpenText Management Center Software is a centralized security management center that manages large deployments of OpenText solutions such as an OpenText Logger, OpenText Investigate, OpenText ESM, OpenText SmartConnector, OpenText Connector Appliances and Transformation Hub through a single interface. Automates log collection and log management.

Key points for OpenText Management Center Software

- When included in the Standard Edition license for ESM, Investigate and Logger OpenText Management Center per Instance software product is limited only by hardware capacity. The software may be installed without licensing impact, regardless of the number of Instances.
- When purchased for connector hosting services (e.g., Appliance) SIEM Management Center requires concurrent or prior purchase of a Connector Hosting server (example C6700 server).

OpenText Security Log Analytics (ArcSight Recon Standard Edition)

OpenText Security Log Analytics is a log search and log management tool that increases SOC analyst effectiveness by making billions of logged events available for quick and easy search and visualization. Security Log Analytics helps SOC analysts gain a deeper understanding of specific alerts and hunt for hidden security threats. Log Analytics Security Log Analytics collects device logs by leveraging OpenText’s Connector and Transformation Hub products for log collection, routing, and enrichment. Once collected logs are persisted into OpenText’s security information model and optimized for search. Security Log Analytics provides an easy-to-understand search language to search logs and retrieve datasets that can be further explored by creating custom charts or selecting from a chart library. Security Log Analytics also supports log archival and compliance use cases.

Key points for OpenText Security Log Analytics

- Security Log Analytics is licensed by ingestion capacity measured in EPS that is calculated post-filter, pre-aggregation. Ingestion capacity is sold in tiers of 100, 250, 500, 1000, 2500, 5000, 10000, 25000 and 50000.
- No rights to forward data outside of OpenText SIEM Platform products without a separate purchase of Third-Party Destination per Target license. Use of Multiplexing technologies between OpenText SIEM Platform products and Third-Party Targets is not permitted.
- The software may be installed without licensing impact, regardless of the number of Instances.

- Third-party business intelligence or data query tools may be used to access and perform ad hoc queries on the embedded database systems. Extending the database schema beyond the intended use of the OpenText product is not permitted.
- It is highly recommended that you purchase the Security Log Analytics Appliance (R8000 or R8100) to ensure a successful implementation of Security Log Analytics.

Software	Offering Includes
OpenText Security Log Analytics Standard Edition	▪ Security Log Analytics (v1.0 and higher) ingestion capacity in Licensed EPS ▪ Transformation Hub (v3.3 and higher) equivalent Licensed EPS to Investigate ▪ OpenText Management Center Instance (v2.95) for centralized OpenText infrastructure management ▪ SmartConnectors 8.0.0 and higher

SIEM Data Platform (SDP)

Using an open architecture, SIEM Data Platform (SDP) centralizes security data ingestion, infrastructure configuration management and monitoring, and data queuing, transformation and routing to OpenText analytics ecosystems like Enterprise Security Manager (ESM), Logger and Investigate, or to third party software.

Key points for SIEM Data Platform

- SIEM Data Platform is licensed by ingestion capacity measured in EPS that is calculated post-filter, pre-aggregation. Ingestion capacity is sold in tiers of: 100, 250, 500, 1000, 2500, 5000, 10000, 25000 and 50000. Forwarding data only limited to the hardware or performance constraints of the SDP software.
- When deployed with a Connector hierarchy where one or more Connectors is forwarding data to a higher tier Connector, that is in turn forwarding the same data to the Transformation Hub, the aggregated EPS may not exceed the Licensed EPS capacity of the Destination products (i.e. ESM and Logger).
- SIEM Data Platform may be used independently from ESM, Logger or Investigate for the purposes of data ingestion, transformation and routing from one or more sources to one or more Targets. Any use of the SDP that involves the routing of data to a Target must be licensed via the OpenText Third Party Destination per Target license SKU. Minimum of 1 license required.

Software	Offering Includes
SIEM Data Platform (SDP)	▪ Event Broker renamed Transformation Hub (v3.0 and higher) ingestion capacity in Licensed EPS ▪ OpenText Management Center Instance (v2.9) for centralized OpenText infrastructure management ▪ SmartConnectors 7.11.0 and higher

OpenText SmartConnectors

OpenText SmartConnectors are designed to retrieve data from Servers or other Event sources in customer environments, normalize that data, and feed it into OpenText products. Unless licensed under the Third-Party Destination per Target license, SmartConnectors may not be used to feed event data into any non-OpenText products.

- The following Connectors are included under the SmartConnector entitlements:
  - FlexConnector which is a software development product (“SDK”) that enables monitoring of Devices not supported by the subset that was formerly ArcSight software OpenText software.
  - Quick Flex Parser Tool generates parser file used in FlexConnector framework.
  - Connector Load Balancer provides a “connector-smart” load balancing mechanism by monitoring the status and load of the SmartConnectors.

Connector Trials: When the OpenText SmartConnectors or FlexConnector are used in a trial environment, the connector may only be used for the purposes of supplying the product(s) on trial with the necessary data to perform an appropriate and comprehensive evaluation of the product(s). It may not be used for any other purposes, nor may its data be shared with any other system(s), applications, etc. that are not part of the OpenText product(s) under trial evaluation. All rights to use of the connectors shall terminate at the end of the trial evaluation period.

Third Party Destination add-on per Target

The Third Party Destination add-on per Target license provides the entitlement rights to forward Event data to a Non-OpenText product.

Key points for Third Party Destination Add-On per Target

- A Third Party Destination license is required for any data placed on the Transformation Hub that was not placed by an OpenText family connector, collector or product.
- Requires prior or parallel purchase of either Logger, ESM, Investigate or SIEM Data Platform.
- QTY 1 is required for each unique Target.

Transformation Hub

Transformation Hub is part of the OpenText family of products that provides an enterprise message delivery bus, raw data normalization, enrichment, and transformation capabilities for security operations.

Key points for Transformation Hub

- The entitlement for Transformation Hub is included in the “Standard Edition” products and SIEM Data Platform. Licenses are equivalent to the Licensed EPS for the “Standard Edition” or SIEM Data Platform (SDP) product which includes the Transformation Hub.

OpenText ThreatHub Feed Plus (CyberRes Galaxy Threat Acceleration Program Plus per Account (GTAP Plus))

OpenText ThreatHub Feed Plus is a package that provides timely, high fidelity threat Behavior Signals services.

It explores the threats to a specific business and threat environment over a wide trajectory, allowing for the development and design of appropriate mitigations for new threats. It consists of a periodically updated threat feed provided by OpenText and its accompanying threat related reports.

Key points for OpenText ThreatHub Feed Plus

- Sold Per Account, maximum would be for 3 concurrently running instances.
- Subscription based only for 1,2 or 3 years, no perpetual licenses.

OpenText User Behavior Monitoring (ArcSight IdentityView)

OpenText’s User Behavior Monitoring (OpenText UBM) is an add-on solution that utilizes the same analytics engine used within OpenText ESM. OpenText UBM protects organizations from Insider Threats by monitoring employees, partners, and other trusted identities. OpenText UBM allows organizations to monitor and report on roles and privileges granted to users on monitored systems, providing enhanced visibility of user activity by linking the user, role, and group information in Microsoft Active Directory with actual activity logged across the enterprise. By analyzing what each user does and comparing those actions to the user’s roles, UBM can detect potentially risky activity, including data theft and unauthorized access to confidential information, strengthen internal controls, and improve overall compliance.

Key points for OpenText User Behavior Monitoring (UBM)

- Pre-requisite is that you own or purchase in parallel OpenText Enterprise Security Manager (ESM)
- OpenText ESM is licensed by Events per Second and OpenText User Behavior Monitoring is licensed by Actor which is defined as a Managed Entity.

Appliances

As of **May 1, 2019**, OpenText's appliances are sold separately from the software (see matrix below). Customers can add capacity using the older model, if they are not on the latest versions.

Appliance	Offering Includes
OpenText L8000 for Logger Server	Hardware Appliance for Logger only, preloaded with the applicable Logger image. Software is licensed separately. Server can be used for production, non-production or HA purposes. Red Hat operating system included. Capacity of up to 30,000 EPS depending on event size and other variables. Only for Logger Software Versions 7.3 and higher.
OpenText Security Log Analytics R8000 Server	Hardware Appliance for Security Log Analytics only, preloaded with the applicable Security Log Analytics image. Software capacity is licensed separately. Server can be used for production, non-production or HA purposes. Red Hat operating system included. Capacity of up to 5,000 EPS depending on event size and other variables. Only for Security Log Analytics Software Versions 24.2 (v1.6) and higher
OpenText Security Log Analytics R8100 Server	Hardware Appliance for Security Log Analytics only, preloaded with the applicable Security Log Analytics image. Software capacity is licensed separately. Server can be used for production, non-production or HA purposes. Red Hat operating system included. Capacity of up to 20,000 EPS depending on event size and other variables. Only for Security Log Analytics Software Versions 24.2 (v1.6) and higher
OpenText C8200 Sled Appliance	Hardware Appliance for OpenText Management Center (SIEM Management Center) only, preloaded with the applicable SIEM Management Center image. Software licensed separately – SIEM Management Center Per Instance (Part number SP-AI209). Server can be used for production, non-production or HA purposes. Red Hat operating system included. Capacity of up to 40,000 EPS depending on event size and other variables. Only for SIEM Management Center Software Versions 24.3 (v3.2.5) and higher. Enclosure is sold separately and can hold a maximum of 4 Sleds.
OpenText E8400 Sled Appliance	Hardware Appliance for ESM only, preloaded with the applicable ESM image. Software capacity is licensed separately. Server can be used for production, non-production or HA purposes. Red Hat operating system included. Capacity of up to 25,000 EPS depending on event size and other variables. Only for ESM Software Versions 24.3 (v7.8) and higher. Enclosure is sold separately and can hold a maximum of 4 Sleds.
OpenText EC8300 Sled Appliance	Hardware Appliance for ESM only, preloaded with the applicable ESM image. Built to be a correlator within an ESM distributed correlation configuration. Software capacity is licensed separately. Server can be used for production, non-production or HA purposes. Red Hat operating system included. Capacity of up to 50,000 EPS depending on event size and other variables. Only for ESM Software Versions 24.3 (v7.8) and higher. Enclosure is sold separately and can hold a maximum of 4 Sleds.
OpenText DB8400 Sled Appliance	Hardware Appliance for ArcSight software only, preloaded with applicable Vertica image. Server can be used for production, non-production or HA purposes. Red Hat operating system included. Only for ArcSight Software Version 25.1 and higher. Enclosure is sold separately and can hold a maximum of 4 Sleds.
OpenText W8300 Sled Appliance	Hardware Appliance for ArcSight software only, preloaded with applicable images for SOAR, UI, Kubernetes, and THub functions and capabilities. Server can be used for production, non-production or HA purposes. Red Hat operating system included. Capacity for up to 25,000 EPS for Transformation Hub depending on event size and other variables. Only for ArcSight Software Version 25.1 and higher. Enclosure is sold separately and can hold a maximum of 4 Sleds.

Appliance	Offering Includes
OpenText E7700 for ESM RHEL Gen10 Server	Hardware Appliance for ESM only, preloaded with the applicable ESM image. Software is licensed separately. Server can be used for production, non-production or HA purposes. Max capacity of 25,000 EPS. Only for Software Versions 7.2 and higher.
OpenText C6700 for Connector Host RHEL Gen10 Server	Hardware Appliance for Connector hosting only, preloaded with the applicable Connector Appliance image. Software is licensed separately. Server can be used for production, non-production or HA purposes. Max capacity of 10,000 EPS. Only for Software Versions 2.93 and higher.

Appliances -Risk of Appliance Data Loss

Although the ArcSight Appliances are designed with redundant capabilities to reduce the risk of data loss or corruption, there are no guarantees. Customers should regularly back up their appliances, as Micro Focus is not liable for any unrecoverable data resulting from hardware failure or data corruption.

License Compliance Measurement

As of **May 1, 2019** OpenText has adopted the following method as a means to assess and evaluate whether there has been a violation of the ALA by a customer:

Overview

In the due course of proper utilization of a SIEM solution, activities and events may conspire where an organization may briefly exceed their licensed EPS. Examples of legitimate business reasons for these events include, but are not limited to:

- Organized attack by an outside entity upon the organization
- Configuration and tuning as a result of implementation of new operational use cases
- Onboarding new Devices, Application Servers, Systems, etc. that temporarily result in an event spike while proper tuning is then carried out

How Compliance Is Calculated

In attempting to account for conditions that occur within the due course of business that may result in temporary overages exceeding the Licensed Capacity, the Moving Median Events Per Second (MMEPS) is calculated and it is this value that is evaluated against the total Licensed Capacity.

Assessment of Compliance

Should an organization’s MMEPS calculation exceed their Licensed Capacity for less than five days, and then the MMEPS value returns to less than the Licensed Capacity then this shall not constitute a violation of the license agreement.

If an organization’s MMEPS calculation should exceed their Licensed Capacity exceeding the 5 concurrent day threshold, the organization shall have up to 45 days to contact Micro Focus and address the overage without incurring an infraction. Should the overage go for 45 consecutive days with no correction, this shall be considered a Non-compliance Finding.

Any organization found to be in breach of the license agreement shall be responsible for the difference between the Licensed Capacity and the Non-compliance Finding. An organization may be found liable for multiple Non-compliance Findings. Penalties may be assessed independently for each Non-compliance Finding identified.

Excluded Events

Any events that are generated by an OpenText Collector, Connector, User Interface, Correlator, etc. (generally referred to as OpenText Component) for the purposes of diagnostics, systems monitoring, auditing, etc. shall not be counted or considered in evaluation of license compliance. These events are there so that the customer may properly diagnose and troubleshoot issues either alone or with the assistance of Technical Support.

Additional license terms

	Term
A. Complete Product	You shall install and use the software as authorized in the applicable agreement and this ALA only as a complete product and may not use portions of such software on a standalone basis separate from the complete software or separate from the Server if delivered as an Appliance unless expressly authorized in the Supporting Material, specifications or an applicable agreement.
B. Additional Software License terms	You shall not access the embedded Oracle database or any other third-party product embedded in the OpenText software with applications other than the OpenText software.
C. Performance Information	You will not (and will not instruct, authorize or allow any third party to) publicly disseminate any performance information or analysis (including, without limitation, benchmarks and performance tests) from any source relating to the software.
D. Security and Network Acknowledgements	You acknowledge and agree that the software (i) accumulates and organizes security information that, in the wrong hands, could serve as a blueprint of your security system and its vulnerabilities and that any disclosure of such information could result in substantial harm to you and others. You will be solely responsible for any disclosure of such information; and (ii) is designed to give the user emergency administrator-level control over your computer network, with the ability to dynamically Security Log Analytics figure or disable network infrastructure devices, change network topology and exclude network access. Such networking products should be used only by users who have been trained in the use of such networking products. Improper use of such networking products may result in significant network damage or downtime. You assume all risks associated with the operation of such networking products.
E. Additional third party terms	You shall not (and will not instruct, authorize or allow any third party to) create, modify, change the behavior of, classes, interfaces, or sub packages that are in any way identified as “java”, “javax”, “sun” or similar convention as specified by Oracle in any naming convention designation. In the event that you create an additional API(s) which: (a) extends the functionality of a Java Environment; and (b) is exposed to third party software developers for the purpose of developing additional software which invokes such additional API, you must promptly publish broadly an accurate specification for such API for free use by all developers. Oracle and Java Trademarks and Logos. You may not use an Oracle America, Inc. name, trademark, service mark, logo or icon. You acknowledge that Oracle owns the Java trademark and all Java-related trademarks, logos and icons including the Coffee Cup and Duke (“Java Marks”) and agrees to: (a) comply with the **Java Trademark Guidelines**; (b) not to do anything harmful to or inconsistent with Oracle’s rights in the Java Marks; and (c) assist Oracle in protecting those rights, including assigning to Oracle any rights acquired by you in any Java Mark. Source Code. Software may contain source code that, unless expressly licensed for other purposes, is provided solely for reference purposes pursuant to the terms of your license. Source code may not be redistributed unless expressly provided for in the terms of your license. Third Party Code. Additional copyright notices and license terms applicable to portions of the software are set forth in the Third Party Copyright Notices and License terms and the THIRDPARTYLICENSEREADME.txt file contained therein that can be accessed from the ancillary.txt file or user documentation. OPSJ Runtime System software and technical data rights granted herein include only those rights customarily provided to commercial end use customers. This customary commercial license in technical data and software is provided in accordance with FAR 12.211 (Technical Data) and 12.212 (Computer Software) and, for Department of Defense purchases, DF AR 252.227-7015 (Technical Data-Commercial Items) and DFAR 227.7202-3 (Rights in Commercial Computer Software or Computer Software Documentation).

	Term
F. Logger Back-ups	The archiving functionality of OpenText Logger must be enabled for the product to back up data on a daily basis. In the unanticipated event in which data corruption occurs, the backup data will help you to restore the data for search and reporting purposes.
G. Control Workflows	The OpenText Control component supports management and administration of OpenText components, including, but not limited to, Connectors and Destinations. Control’s orchestration engine runs Workflows. The license to run Workflows by this orchestration engine is limited to Connectors and Destinations for the purposes of managing and administering them. If the targeted Node is not a Connector or Destination, the license does not entitle running a Workflow launched by Control on it.

opentext.com/about/legal/software-licensing

Latest version of software licensing documents

5200-1969, February 27, 2025; replaces 5200-1960 (January 20, 2025)