Managed Security Provider (MSP) OpenText Security Operations Partner Program Guide

August 2025



Contents

About OpenText Cybersecurity 3

OpenText Cybersecurity MSP Partner Program Introduction 3

- Managed Security Provider Program Benefits 4

How to Become a Managed Security Provider Partner and Managed Security Provider Requirements 5

- How to Become a Managed Security Provider 5
- Managed Security Provider Program Requirements 6

Security Operations Managed Security Provider Guide 7

- Security Operations Pay as You Grow Managed Security Provider Licensing Models 8
- Security Operations Managed Security Provider Program 10
- Additional Terms and Conditions 20

About OpenText Cybersecurity

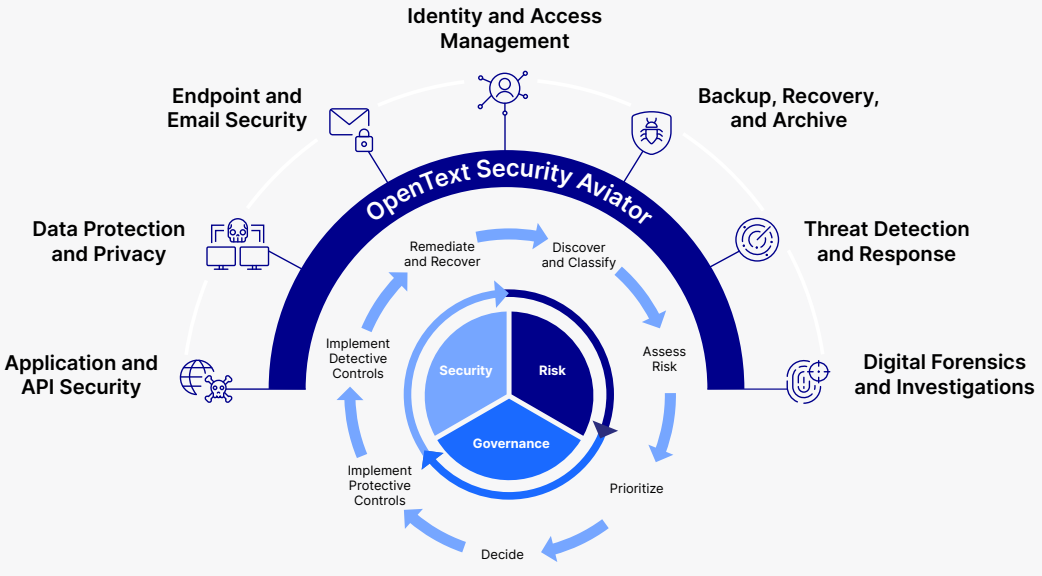
OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified/end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high-efficacy products, a compliant experience and simplified security to help manage business risk.

OpenText Cybersecurity MSP Partner Program Introduction

As technology evolves and customers' requirements continue to shift, all areas of IT are impacted. Managed Security Providers experience pressure to improve service quality and costs, both internally and from end customers. To meet expectations and drive high customer value, Managed Security Providers must provide solutions that improve the customer experience, IT agility, and profit margins. We recognize that the Managed Security Provider marketplace is evolving rapidly and our Partners are aligning their respective strategies to expand their business to leverage this growing business opportunity.

The goal of the Managed Security Provider is to build, serve, and retain customers via **outcome-based security service offerings**. Additionally, Managed Security Providers must offer solutions that deliver the consumer-like digital experience that end customers expect today. Machine learning, analytics, intelligent automation, and personalization are all important components of a modern solution that can solve issues. For Managed Security Providers to become trusted Partners, they must understand their customers' desired business outcomes, the nuances of their business, and their specific needs.

OpenText Cybersecurity: Comprehensive Cybersecurity Coverage



	The OpenText Cybersecurity Managed Security Provider (MSP) Program provides access to proven, industry-leading software with flexible licensing options designed to help you address the different needs of your customers in a rapidly changing marketplace. OpenText is Managed Security Provider Ready.

Revenue-Generating Solutions	• Rich, deep, and broad product portfolio built on service delivery flexibility
	• Use cases for Services Providers
	• Market-Leading Software
	  • Application Security
	  • Security Operations
	  • Data Privacy & Protection
	  • Identity & Access Management

Pay-as-You-Grow Models	• Flexible Business Models • CapEx and OpEx Models • Perpetual Licenses • PPU (Pay Per Use) & PPU payment in arrears (depending on portfolio) • Subscription/Term Licenses • Access to SaaS • MSP Terms
Go-to-Market Partnerships	• Collaborative Sales and Marketing • Access to Partner Portal and Program Benefits • Education and Enablement • Marketing Support

Managed Security Provider Program Benefits

MSP Program Benefits

- Unique Product SKU Access for MSP
- Partner Portal
- Partner Directory Listing
- Partner Events
- Training and Certifications
- Partner Webcasts
- Partner Leadership Forum
- OpenText MSP logo

- Quarterly Business Review
- Joint Business Planning
- MSP Partner Manager and Architect
- Initiative-based Market Development Funds
- Security Operations Marketplace and User groups

How to Become a Managed Security Provider Partner and Managed Security Provider Requirements

How to Become a Managed Security Provider

STEP 1: REGISTER YOUR COMPANY

- Complete a simple online company registration form available at: https://microfocus.my.site.com/s/?language=en_US.
- For Partners seeking to procure through Distribution, agree to the standard OpenText Tier 2 click-through terms and conditions.
    - Or if you wish to procure directly from OpenText, an extended due diligence process is required.

      Note: *Direct Buy Reseller (DBR) applications are by invitation only. Please allow 2 weeks for processing time.*
- All Managed Security Providers are required to have an active OpenText Partner Agreement that includes a Managed Security Provider Addendum.
- Legal and Regulatory screening (processing time is typically less than 48 hours).
- Upon successfully completing your company onboarding, you will receive a Partner Registration Complete and Welcome Onboard email containing a copy of your agreement and Partner Account Number.
- Managed Security Providers are not allowed to sell to Managed Security Providers. In other words, MSP-to-MSP models are not allowed.

STEP 2: REGISTER AS A PARTNER USER FOR OPENTEXT PARTNER PORTAL ACCESS

- Complete a simple online company registration form available at: https://microfocus.my.site.com/s/?language=en_US.
- Use your Company Partner Account Number (optional) or we will try to match you based on your corporate email domain and country.

Upon registration, you will receive an email with a "validate my email" link to then log into the Portal.

Please contact your MSP GEO Sales leader, Partner Business Manager, or Alliance Business Manager if additional assistance is needed.

Managed Security Provider Program Requirements

Requirements
Applicable to Security Operations • ISO Certified Data Center • 24×7 Security Operations Center (SOC) • Certified SOC Analysts and Administrators
End Customer Support
Managed Security Services Catalog Offering
Portfolio-Specific Sales Accreditation
Portfolio-Specific Technical Accreditation
Press Release or Social Media Announcement
Display OpenText MSP logo
Executed Managed Services Agreement
Managed Security Provider Skills Assessment
Quarterly Business Plan, Marketing Plan, and Business Plan Review

Security Operations Managed Security Provider Guide

This guide describes the Security Operations offering applicable to Managed Security Providers.

Security Operations is a leading provider of security and compliance management solutions used by corporations and government agencies worldwide to protect their online assets from cyberthreats and risk. Security Operations products help Managed Security Providers monitor and manage their End Customer's business by providing comprehensive visibility into activity across their IT infrastructure.

Security Operations Capabilities are available to Managed Security Providers under the **ONE Security Operations Managed Security Provider Program.** This program provides all Security Operations capabilities, under a single Program Model, covered in the next section of this guide.

Security Operations Capabilities

Capability	What it Delivers	MSSP Business Value
Security Information & Event Management	A powerful, intelligent SIEM backed by an open architecture and powerful real-time correlation.	Centralizes your security operations and detects "known" threats in real-time.
Log Management and Threat Hunting	Comprehensive log management and search solution that eases compliance burdens and accelerates forensic investigation.	Gain centralized log storage that powers intelligent investigation and compliance
Security Data Platform	Collect, normalize, enrich, and distribute event data from 480+ source types.	Leverage more insightful, and cost-effective data to efficiently produce better threat insights.
User and Entity Behavior Analytics	Anomaly detection that learns normal behavior for each entity and identifies the most unusual or suspicious activity.	Detect complex or "unknown" threats, such as insider threats or targets attacks.
Security Orchestration, Automation and Response	Seamless orchestration of both technology and people, automation and incident management	Improve efficiency in responding to cyberattacks in security operations.

Security Operations powers the following capabilities for Managed Security Providers:

Type of MSP Offering Examples	
Security Event Monitoring and Response	Firewall Management
Enhancing EDR Core Behavioral Signals	Extended Detection and Response as a Service (XDR)
Incident Response	IOT Threat Management
Reporting for compliance use case across log and data sources	Secure Data Logging
Threat Core Behavioral Signals Services	Unified Threat Management
Security Operations as a Service	Identity and Access Event Tracking
	Security Operations and Threat Response Automation (SOAR)

Security Operations Pay as You Grow Managed Security Provider Licensing Models

- Perpetual licenses
- PPU (Pay Per Use)
- Subscription/Term licenses
- Access to SaaS Subscription licenses
- MSP terms

Dedicated Perpetual Model

This Managed Security Provider Model offers perpetual licenses and pricing for Managed Security Provider (MSP) Partners to provide services to a single dedicated Named End Customer. The End Customer must be disclosed.

Internal Use: No Internal Use is allowed with Managed Security Provider Licenses. Internal Use means installation, access, and use of the Eligible Products by Partner for the purpose of running or supporting Partner's own internal business operations or functions.

Transfer: Two (2) years after purchase, Managed Security Provider (MSP) Partner may be entitled to transfer the Perpetual License to the Named End Customer as defined in the initial order document. Transfer must comply with the OpenText Software License Transfer (SLT) policy. Managed Security Provider (MSP) Partner may not re-use perpetual licenses for any other Named End Customer.

Pricing: Eligible Security Operations products in this model are priced in the in-country list price for perpetual software licenses, appliance, and support.

Support: Annual 24×7 Support and Content Update Subscription is required for all Security Operations licenses.

Invoicing: Software license, appliance, and first year support are billed in advance. Licenses are required to be under support for the duration of the Managed Security Provider's agreement with named end customers.

Security Operations Pay-Per-Use Subscription Models

This Managed Security Provider Model is designed for Partners who require a leveraged and repeatable solution deployed in their SOC to support multiple end customers through a single technology configuration. It offers one (1) and three (3) year subscription (term) licenses for specific Security Operations products in a PPU usage-based price model, enabling Managed Security Provider Partners to provide services to multiple end customers.

Security Operations SaaS Subscription Models

This Managed Security Provider Model offers SaaS Subscription and Pricing for Managed Security Provider (MSP) Partners to provide services to their customers.

- Currently applicable to Security Log Analytics and Core Behavioral Signals Core Behavioral Signals for CrowdStrike (SaaS).

Internal Use: No Internal Use is allowed with Managed Security Provider Licenses. Internal Use means installation, access, and use of the Eligible Products by Partner for the purpose of running or supporting Partner's own internal business operations or functions.

MSP Terms

- **End Customer Registration:** The Managed Security Provider (MSP) Partner agrees to register new end customers within 10 days of executing a managed security services contract with such End Customer by completing and submitting the "Security Operations Customer User Registration Form." The registration shall include the estimated consumption in EPS/day (and include GB/day if the MSP Partner is leveraging the Security Operations Classic Model), the term of the contract signed with the End Customer. Registration forms will be provided at time of order and submitted to MFI-msspcyberres@opentext.com.
- **End Customer Onboarding:** 90 days are provided as the onboarding period for any new end customers. Managed Security Provider (MSP) Partner agrees to onboard any and all registered end customers onto the Security Software Platform within 90 days of the registration. Managed Security Provider Partner will provide notification if there is a delay in the onboarding process that would extend beyond the stipulated period.
- **End Customer Termination:** Managed Security Provider (MSP) Partner agrees to notify OpenText within five (5) business days if the End Customer contract is terminated before Managed Security Provider Partner begins servicing the End Customer.

- **Connectors:** Managed Security Provider (MSP) Partner may install standard Security Operations Connectors Software and custom connectors developed by Managed Security Provider Partner using the FlexConnector Software and CONAPP Software (collectively, the "Connectors") at the End Customer's facilities. However, any right and license to the Connectors will extend only to Managed Security Provider (MSP) Partner. The End Customer will have no license rights whatsoever with respect to the Connectors or any other Products provided herein. Customer has no ability to access the Connector for the purposes of forwarding events to a non-MSP supported application or platform.
- **Security Operations SOC Location Form:** Managed Security Provider (MSP) Partner must communicate to OpenText the location of all Security Operations Centers (SOC) by completing and submitting the "Security Operations SOC Locations Form." If a new SOC is assembled, Managed Security Provider Partner must notify OpenText.

  The Security Operations SOC Location Form will be provided at time of order and is to be submitted MFI-msspcyberres@opentext.com. In addition, Managed Security Provider (MSP) Partners must provide documentation verifying that each SOC or Data center from which Managed Security Services (MSS) are provided using Security Operations products has at least one current industry-standard certification (e.g., ISO, ADC, Uptime Institute).

Security Operations Managed Security Provider Program

The Security Operations Managed Security Provider Program provides the **Security Operations and beyond capabilities**, under **a single Program Model**.

Security Operations Is Managed Security Provider Ready	
Low Entry Cost	• Low-cost annual or 3-year option • Unlimited usage in a PPU model
Single Platform Pay as You Grow	Deploy all Security Operations capabilities in a single-cost EPS PPU model. Includes: • Security Log Analytics, ESM, Behavioral Signals, Threat Hunting, SOAR, Transformation Hub, SmartConnectors and OpenText Management Center. • Upfront Subscription SKU's available • Logger as EPS model – purchased separately as an add-on • Galaxy Community Edition
Simplicity	• PPU or Subscription Options

Prices may vary by country and must be confirmed by a OpenText legal quote. This base package, comprising multiple product licenses, must be re-purchased at the end of each one (1) or three (3) year term.

Note: *It is highly recommended that new Managed Security Provider (MSP) Partners also purchase OpenText Flex Credits, which can be leveraged for SIOC ("Security Core Behavioral Signals and Operations Consulting") Services and for OpenText Education Training Units.*

- Flexible Credits are a OpenText service currency that provides a flexible way to obtain additional short-term services. Flexible Credits can be purchased up front or at any time during the life of your contract to provide you with a source of funding for the services you need, when you need them. Flexible Credits can be redeemed anytime during the 12-month period from purchase for Support, Education and Training, or Consulting services.
- www.microfocus.com/media/guide/micro_focus_flexible_credits_guide.pdf

Product Code	Product Description
SU-AA065	• Flexible Credit—Flexible Service Offerings

Product Code	Description	Features
SB-AE005	Security Operations Managed Security Managed Security Provider Pay Per Use Platform Subscription SW E-LTU	• Can be purchased for 1 or 3 years. 1 or 3 year term starts upon e-delivery. Required to purchase again after the term is expired. Non-Discountable. **Includes:** • Production, Non-Production, and High Availability • 24×7 Technical Support • Core Behavioral Signals • Security Log Analytics • ESM • OpenText Management Center • Sentinel • Smart Connectors • Transformation Hub • Compliance packs for ESM and Security Log Analytics Quarterly EPS usage is collected and billed separately. Recommended to add Flexible credits (SU-AA065) for Professional Services and Education.
SB-AE007	One Security Operations Logger Add-on for Managed Security Provider Pay Per Use Platform subscription SW E-LTU	Must own SB-AE005 MSP Platform SKU. Co-term the expiration date of this ADD-ON to match the SB-AE005 Platform SKU. Non-Discountable. **Includes:** • 24×7 Technical Support • Logger 10,000 EPS capacity • Logger Compliance Insight packs Quarterly usage is collected and billed separately. If additional Logger capacity is needed, additional Logger licenses are required to be purchased.

Product Code	Description	Features
SB-AE009	Security Operations ESM APHA Add-on for Managed Security Managed Security Provider Pay Per Use per Instance Subscription SW E-LTU	Must own SB-AE005 MSP Platform SKU. Co-term the expiration date of this ADD-ON to match the SB-AE005 Platform SKU. Non-Discountable. Includes: • 1 license for ESM Active Passive High Availability. Purchase the QTY needed for each Active Passive Instance. This is not unlimited. Active Passive High Availability is defined as 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. **If the data is not in sync, then purchase this license.**

- If SB-AE005 MSP PPU Platform subscription is expired, Partner will lose access to contacting Technical Support and the ability to download updates, patches, and fixes.
- In this model (Security Operations Subscription Term Model), license key capacity may be exceeded. It will be captured via Managed Security Provider (MSP) Partner Quarterly EPS usage reports and made available to OpenText. As such, there are no capacity add-on licenses.
- Security Operations ALL in model will include the following versions:
  - ESM v7.5 and higher
  - Security Log Analytics v1.2 and higher
  - Core Behavioral Signals v6.3 and higher
  - Transformation Hub v3.5 and higher
  - Logger Add-On sold separately
  - Sentinel v8.5 and higher
  - Smart Connectors v8.2 and higher
  - ArcMC v3.0
  - The licenses in this model are considered Class 1. Class 1 provides free non-production licenses. Description of the Non- production use rights available can be found at: Non-Production Licensing Guide.

Usage Reporting

Over the course of the subscription Term, Managed Security Provider (MSP) Partners are invoiced for usage based on event ingestion (measured in average EPS by day) against certain named Products. For invoicing to occur, Partners are required to submit usage tracking reports to Security Operations's billing team in a timely manner. Below is an overview of reporting and related Partner requirements.

During the Term, Managed Security Provider (MSP) Partner shall provide on a quarterly basis a Usage Report for each of the following product instances deployed in production under the Pay-Per-Use license:

- Security Operations Platform—tracks usage for Security Log Analytics & Core Behavioral Signals Standard Edition
- Enterprise Security Manager
- Logger
- Sentinel

Each of the above Products provides the Managed Security Provider (MSP) Partner a Usage Report that is described in the Reporting Guide. For each Product, the Guide describes how to navigate to and run the Usage Report.

The Reporting Guide can be found within the OpenText Marketplace, under Security Operations Utilities and Tools:

https://marketplace.opentext.com/cybersecurity/category/arcsight

Usage reports track each Product instance's average ingested EPS by day. EPS is metered on a post-filter and pre-aggregation basis. The pre-aggregation event count method counts device events and ignores any aggregation or consolidation performed by the Connectors.

The Security Operations Platform tracks usage for Security Log Analytics and Core Behavioral Signals Standard Edition (SE). The Platform provides a common event store to Security Log Analytics and Core Behavioral Signals Standard Edition (SE). Event ingestion is measured against the common event store. Events ingested into the Platform are always counted once, even if both Security Log Analytics and Core Behavioral Signals Standard Edition (SE) are deployed. The Security Operations Platform Usage Report consolidates the usage reporting requirement for deployed Security Log Analytics and Core Behavioral Signals Standard Edition (SE) instances.

Managed Security Provider (MSP) Partner shall submit Usage Reports for each Pay-Per-Use licensed Product instance covering the entire quarter that just ended within ten (10) business days after quarter end.

Reports are to be sent to: MFI-msspcyberres@opentext.com.

See the following table for **Standard Price Tiers**. Price tiers are applied to each day. For example, if the average EPS for a given day is 12,500 EPS, then the corresponding Price Per EPS is $0.10 and the extended price is calculated as 12,500 EPS x $0.10 $/EPS = $1,250. The total extended price from all three reports is calculated and adjustments, if any, are applied. The highest value single report will result in the invoiced amount.

ESM/Security Log Analytics/ Core Behavioral Signals/ Sentinel/Logger EPS/Day Tier	Price Per EPS/Day—USD
0–10,000	$0.12
10,001–50,000	$0.10
50,001 +	$0.08

Example:

A Managed Security Provider (MSP) Partner has the following deployment:

- Enterprise Service Manager—Instance A
- Enterprise Service Manager—Instance B
- Security Log Analytics
- Core Behavioral Signals Standard Edition

A single instance of the Security Operations Platform hosts both Security Log Analytics and Core Behavioral Signals SE. At the beginning of a quarter, Managed Security Provider (MSP) Partner produces a Usage Report covering the previous quarter for each deployed Product instance, resulting in three distinct Usage Reports. Recall that the Security Operations Platform produces a single Usage Report for Security Log Analytics and Core Behavioral Signals SE.

Managed Security Provider (MSP) Partner emails all three reports to the OpenText billing team.

Once the billing team receives the reports, a per EPS price is assigned for each day and then the extended price is calculated. The total extended price from all three reports is summed and adjustments,if any, are applied. The highest value single report will result in the invoiced amount. The Billing team sends the invoice to Managed Security Provider (MSP) Partner.

Reports are to be sent to MFI-msspcyberres@opentext.com.

Invoicing

Within (5) five business days of receiving each quarterly Usage Report from Managed Security Provider (MSP) Partner, OpenText will review and calculate the Usage Fees. Managed Security Provider (MSP) Partner is obligated to provide a blanket purchase order for quarterly usage for the term of the contract. The blanket purchase order will include the agreed estimated usage fee amount, the period of service, include blanket purchase order identification and be signed. OpenText will invoice for the agreed fees using the Blanket Purchase Order no later than ten (10) business days after receiving the quarterly usage report.

Should Managed Security Provider (MSP) Partner choose to pre-pay for usage fees, OpenText and Managed Security Provider (MSP) Partner will agree on 12-month estimated EPS Usage to be pre-billed.

Note: *Quarterly Usage Reports are still required for pre-pay orders.*

Managed Security Provider (MSP) Partner will send OpenText a purchase order for the annual estimated amount and OpenText will invoice promptly thereafter. If actual usage fees are less than pre-billed usage fees in the final 12 months of the contract term, Managed Security Provider (MSP) Partner does not have a right to refund or right to carry forward the balance of pre-billed usage fees. If the Managed Security Provider Agreement terminates other than by OpenText, and if usage fees have been pre-billed, Managed Security Provider (MSP) Partner assumes forfeiture of the unused balance and does not have the right to a refund. If usage overage occurs during the pre-pay period, Managed Security Provider (MSP) Partner will be invoiced for any such overage.

Payment Method	Product Code	Description	Description
Pre-Pay	SP-AH858	Security Operations Managed Security, Managed Security Provider Pay Per Use Program Usage Fee, Upfront Billing SW E-LTU	• Use this SKU to pay in advance for any of the usage for both the Classic and Security Operations TERM models. • Manual pricing based on the signed contract.
Post-Pay	SP-AH857	Security Operations Managed Security, Managed Security Provider Pay Per Use Program, Usage Fee Billing SW E-LTU	• This SKU will be used for billing quarterly in arrears for all the usage for both the Classic and Security Operations Term models. • Manual pricing is used based on the signed contract.

SECURITY OPERATIONS CLASSIC SUBSCRIPTION TERM MODEL

Base Package can be purchased for either 1 or 3 years and will grant entry into the Security Operations Classic program. Prices may vary by country and confirmed by a OpenText legal quote. This onboarding bundle, comprising multiple SKU's and includes the following:

- 1 ESM license (which includes three instances: Production, Non- Production, and High-Availability)
- 2 ADP licenses (25 GB capacity for each instance)
- 24×7 Support with Content, one (1) or three (3) years billed up front
- Not renewable: Once subscription term ends, Managed Security Provider (MSP) Partner must re-purchase base package.

Note: *It is highly recommended that new Managed Security Provider (MSP) Partners also purchase OpenText Flex Credits, which can be leveraged for SIOC ("Security Intelligence and Operations Consulting") Services and for Education Training Units to be used toward Security Education courses.*

For pricing, ask your Sales Representative for a budgetary quote.

Product Code	Description	Features
SP-AL094	**Base Package:** Security—Security Operations Managed Security, Managed Security Provider, Pay Per Use Entry Platform, Classic Suite SW E-LTU	Can be purchased for 1 or 3 years. Non-renewable, needs to be re-purchased after term expires. Contains the following: • ESM 10,000 EPS (for production, non-production, and HA instances) • Logger for 2 instances at 25 GB each • ArcMC quantity 1 • Smart Connectors Recommended to add Flexible credits (SU-AA065) for Professional Services and Education.

Product Code	Description	Features
ESM and Data Platform Additional Instance and Capacity Licenses		
SP-AL095	Security Operations Managed, Security Managed Security, Provider Pay Per Use, Enterprise Security Manager, 10,000 EPS Additional Instance Classic SW E-LTU	Must own SP-AL094 MSP Classic Entry suite. This SKU is an add-on and should be co-termed the SP-AL094. Provides entitlement for 10,000 ESM EPS for 1 additional instance. Non-renewable. Needs to be re-purchased when the term is expired.
SP-AL096	Security Operations Managed, Security Managed Security, Provider Pay Per Use Security, Data Platform 25 GB/day, Additional Instance Classic SW E-LTU	Must own SP-AL094 MSP Classic Entry suite. This SKU is an add-on and should be co-termed the SP-AL094. Provides entitlement for 25 GB for Logger for 1 additional instance.
SP-AL097	Security Operations Managed, Security Managed Security, Provider Pay Per Use Security, Data Platform Additional 25 GB/day Capacity Classic SW E-LTU	Must own SP-AL094 MSP Classic Entry suite. This SKU is an add-on and should be co-termed to the SP-AL094. Provides entitlement to 50k Security Log Analytics EPS. Usage is collected quarterly in arrears. Purchase of the Security Log Analytics R8100 or R8000 appliance(s) are HIGHLY recommended. Non-renewable and needs to be re-purchased when term expires.
SC-AB138	Security Operations Managed Security Service Provider Pay Per Use SECURITY LOG ANALYTICS 50k EPS ADD-ON for CLASSIC Suite Subscription SW E-LTU	Must own SP-AL094 MSP Classic Entry suite. This SKU is an add-on and should be co-termed to the SP-AL094. Provides entitlement to 50k Security Log Analytics EPS. Usage is collected quarterly in arrears. Purchase of the Security Log Analytics R8100 or R8000 appliance(s) are HIGHLY recommended. Non-renewable and needs to be re-purchased when term expires.

Flexible Credits are a OpenText service currency that provides a flexible way to obtain additional short-term services. Flexible Credits can be purchased up front or at any time during the life of your contract, to provide you with a source of funding for the services you need, when you need them. Flexible Credits can be redeemed anytime during the 12-month period from purchase, for Support, Education and Training, or Consulting services.

See microfocus.com/media/guide/micro_focus_flexible_credits_guide.pdf.

Product Code	Product Description
SU-AA065	Flexible Credit—Flexible Service Offerings

1. If SP-AL094 MSP PPU Platform subscription is expired, Managed Security Provider (MSP) Partner will lose access to contacting Technical Support and the ability to download updates, patches, and fixes. This is non-renewable and will need to be purchased again.
2. In this model, Managed Security Provider (MSP) Partner may NOT exceed the license key capacity. If additional EPS is needed, please use the SKU list above and co-term to expire at the same time as your Platform subscription.
3. This model will entitle Managed Security Provider (MSP) Partner to older versions that OpenText still supports. If Managed Security Provider (MSP) Partner is running an older version of Logger and ESM, please upgrade them so they can transition to the new Security Operations model.
4. There is **no migration plan** to move current Managed Security Provider (MSP) Partners from the Security Operations Classic Model onto the Security Operations Subscription Term Model. If a Managed Security Provider (MSP) Partner desires to move to Security Operations, it must be purchased. No credits or refunds will be provided for purchases under the Security Operations Classic Model.

Reporting

During the Term, Managed Security Provider (MSP) Partner shall provide on a quarterly basis the EPS (across all EMS instances) and the GB (across all ADP instances) used by each End Customer within that month.

Within (10) ten business days after the end of each quarter, Managed Security Provider (MSP) Partner shall submit two consolidated reports as follows:

- Monthly EPS/Day Usage Report for every ESM instance
- Monthly GB/Day Usage Report for every ADP instance

Determination of Quarterly Services Usage Fees will be calculated as follows:

EPS/Day Tier for ESM	Price Per EPS/Day—USD
0–1000	$0.10
1001–2500	$0.09
2501–5000	$0.08
5001–10000	$0.07
10001+	$0.06
50,001+	$0.08

GB/Day Tier for ADP	Price Per 5 GB/Day—USD
0–50	NO CHARGE
51–500	$2.00
501+	$1.00

The Reporting Guide can be found within the OpenText Marketplace, under Security Operations Utilities and Tools:

https://marketplace.opentext.com/cybersecurity/category/arcsight

Quarterly usage reports are to be sent to: MFI-msspcyberres@opentext.com.

- For the purpose of determining usage charges, EPS/day is calculated as an average of events per second processed at the ESM in a 24-hour period. There is no size restriction while considering an event. The usage charges on the ADP platform are calculated as total data ingested across all ADP instances at 5 GB increments.
- Logger version 6.1 and later contains a default report that calculates the Daily Byte Count, including Gigabytes per day. The byte counts are based on the Post Filtered and Aggregated event size provided by the SmartConnectors (Device Event Class ID: agent:050).
- For the avoidance of doubt, these charges are tiered (not cumulative).
- There is no byte-size limitation when considering an event.

Invoicing

Within (5) five business days of receiving each quarterly Usage Report from Managed Security Provider (MSP) Partner, OpenText will review and calculate the Usage Fees. Managed Security Provider (MSP) Partner is obligated to provide a blanket purchase order for quarterly usage for the term of the contract. The blanket purchase order will include the agreed estimated usage fee amount, the period of service, include blanket purchase order identification and be signed. OpenText will invoice for the agreed fees using the Blanket Purchase Order no later than ten (10) business days after receiving the quarterly usage report.

Should Managed Security Provider (MSP) Partner choose to pre-pay for usage fees, OpenText and Managed Security Provider (MSP) Partner will agree on 12-month estimated EPS Usage to be pre- billed. Quarterly usage reports are still required for pre-pay orders. Managed Security Provider (MSP) Partner will send OpenText a purchase order for the annual estimated amount and OpenText will invoice promptly thereafter.

Payment Method	Product Code	Description	Features
Pre-Pay	**SP-AH858**	Security Operations Managed Security Managed Security Provider Pay Per Use Program Usage Fee Upfront Billing SW E-LTU	Use this SKU to pay in advance for any of the usage for both the Classic and Security Operations models. Manual pricing is based on the signed contract.
Post-Pay	**SP-AH857**	Security Operations Managed Security Managed Security Provider Pay Per Use Program Usage Fee Billing SW E-LTU	This SKU will be used for billing quarterly in arrears for all the usage for both the Classic and Security Operations models. Manual pricing is used based on the signed contract.

If actual usage fees are less than pre-billed usage fees in the final 12 months of the contract term, Managed Security Provider (MSP) Partner does not have the right to a refund or the right to carry forward the balance of pre-billed usage fees. If the Managed Security Provider Agreement terminates other than by Micro Focus, and if usage fees have been pre-billed, Managed Security Provider (MSP) Partner assumes forfeiture of the unused balance and does not have the right to a refund. If usage overage occurs during the pre-pay period, Managed Security Provider Partner will be invoiced for any such overage.

Additional Terms and Conditions

This Program Guide and the information contained herein are subject to change without notice.

Prices may vary by country and must be confirmed by a OpenText legal quote.

This OpenText Partner Program Guide constitutes an addendum to your OpenText Partner Agreement. In the event of any conflict between the terms of this Guide (“Terms”) and the OpenText Partner Agreement, these Terms take precedence regarding OpenText Partner specialization requirements and related Program benefits.

Capitalized terms not otherwise defined in these Terms are defined in the OpenText Partner Agreement.

Unless requested to accept these Terms online or otherwise, you agree that your participation in this Partner Program (“Program”) constitutes acceptance of, and is governed by, these Terms:

Warranty and Intellectual Property

The only warranties for products and services of OpenText and its affiliates and licensors are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. OpenText shall not be liable for technical or editorial errors or omissions contained herein.

This document contains confidential and/or legally privileged information. It is intended for OpenText and channel partner internal use only. If you are not an intended recipient as identified on the front cover of this document, you are strictly prohibited from reviewing, redistributing, disseminating, or in any other way using or relying on the contents of this document.

Your company's role as a OpenText Authorized Partner may provide access to intellectual property of OpenText and its affiliates. Partners must properly access, use, and help protect our intellectual property, which includes, but is not limited to, this Partner Program Guide, datasheets, service descriptions, collateral, selling guides, service delivery guides, firmware, software updates/upgrades and downloads, and software tools owned by OpenText and its affiliates.

Program Participation

Participation in the Program shall automatically end when your OpenText Partner Agreement terminates.

OpenText Partner Program participation is at the single legal entity level. Aggregated legal entities, such as buying groups, franchisee/ franchisor networks, holding companies, and associated businesses are not eligible. Individual companies that are part of these groups may be eligible at the individual legal entity level if program participation requirements are met.

Partner Eligibility—Compliance

Compliance with anti-corruption laws is an important part of our mission to conduct our business in all cultures and countries with trust, respect, and integrity. Furthermore, compliance with these laws serves to maintain our positive reputation, delight our customers, and grow our relationship with you.

A requirement of the OpenText Partner Legal and Regulatory Compliance Program is the periodic completion of a Due Diligence Questionnaire and Key Personnel List and submission of the Anti- Corruption Compliance Declaration. Furthermore, completion of the program requirements is mandatory for participation in the OpenText Partner Program.

To maintain good standing with Micro Focus, Partners must complete all Legal and Regulatory Compliance Program requirements. Partners that do not meet the Software compliance requirements may forfeit their OpenText Partner Program benefits.

Code of Conduct

At OpenText International plc and the OpenText group companies, we are committed to maintaining the highest ethical standards in our business dealings around the world. Our Code of Conduct sets out the standards that guide our business practices and govern our behavior.

This Code of Conduct is applicable to OpenText channel partners, their employees, temporary employees, agents, independent contractors, and subcontractors. A OpenText channel partner is any party selling OpenText products, including distributors, OEMs, resellers, agents, and any other party to a OpenText Partner or channel agreement. A OpenText channel partner

also includes any party providing services directly or indirectly to OpenText in support of OpenText business, such as system integrators, logistics companies, and other Managed Security Providers to OpenText supporting Micro Focus' business with its customers. A breach of this Code of Conduct will be considered a breach of the channel partner's contract with OpenText and may lead to the termination of the business relationship with. OpenText and its channel partners are required to comply with all anti-corruption laws, such as the US Foreign Corrupt Practices Act, as well as the U.K. Bribery Act, the Canadian Federal Government and public sector rules on gift- giving, hospitality, and other benefits. OpenText channel partners must take special care in dealing with public sector customers, which include employees at all levels of government, government agencies, crown corporations, and publicly funded institutions such as hospitals, public utilities, and educational institutions.

Copyright © 2025 Open Text • 08.25 | 264-000089-002