

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

August 1, 2022—Version 1



Contents

About OpenText Cybersecurity	3
OpenText Cybersecurity Managed Security Provider Program Introduction	4
How to Become a Managed Security Provider Partner and Managed Security Provider Requirements	5
OpenText Data Security as a Service Managed Security Provider (MSP) Program	7
OpenText Structured Data Manager License Models, Usage, and Pricing	9
OpenText Structure Data Manager Managed Security Provider (MSP) Licensing Models	11
OpenText Core Data Discovery & Risk Insights License Models, Usage and Pricing	14
OpenText Core Data Discovery & Risk Insights Program Requirements	15
OpenText Core Data Discovery & Risk Insights Licensing Options	16
OpenText Core Data Discovery & Risk Insights Options	18
OpenText Core Data Discovery & Risk Insights Trial/PoC	19
OpenText Core Data Discovery & Risk Insights Managed Security Provider (MSP) Partner Technical Requirements	19
Additional Terms and Conditions	21

About OpenText Cybersecurity

OpenText Cybersecurity line of business. We bring the expertise of one of the world's largest security portfolios to help our customers navigate the changing threat landscape by building both cyber and business resilience within their teams and organizations. We are here to help enterprises accelerate trust, reliability, and survivability through times of adversity, crisis, and business volatility. We are a part of a larger set of digital transformation solutions that fight adverse conditions so businesses can continue to run today, keep the lights on, and transform to grow and take advantage of tomorrow's opportunities.

Strengthen Your Cyber Resilience

CyberRes
A Micro Focus Line of Business

Enhance resilience to emerging threats such as data privacy and secure cloud transformation.

Data Privacy Protection

- Data Discovery
- Data Insight
- Data Protection
- Data Usage Monitoring
- Data Minimization



Voltage



Fortify

Application Security

- Software Resilience for Modern Development
- Holistic AppSec Platform
- Securing the Software Supply Chain

Identity and Access Management

- Zero Trust with Intelligent Access Governance
- Adaptive Access and Automation
- Protect Unstructured Data from Unauthorized Access
- Centrally Manage Security Policy Controls



NetIQ



ArcSight

Security Operations

- 360° Analytics for Threat Detection
- Threat Hunting and Response Automation
- Advanced Threat Research and Visualization

CyberRes

OpenText Cybersecurity Managed Security Provider 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.

The OpenText Cybersecurity Managed Security Provider (MSP) Partner 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 Cybersecurity is Managed Security Provider Ready:

Revenue-Generating Solutions	• Rich, deep, and broad product portfolio built on service delivery flexibility • Use cases for Managed Security 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) & Pay Per Use Payment in Arrears (depending on portfolio) • Subscription/Term Licenses • Access to SaaS • Managed Security Provider 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

Unique Product SKU Access for Managed Security Provider

Partner Portal

Partner Directory Listing

Partner Events

Training and Certifications

Partner Webcasts

Partner Leadership Forum

OpenText MSP logo

Quarterly Business Review

Joint Business Planning

Managed Security Provider Partner Manager and Architect

Initiative-Based Market Development Funds

OpenText Data Security 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://microfocuspartner.force.com/s/>.
- 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 for two 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, Managed Security Provider-to-Managed Security Provider 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://microfocuspartner.force.com/s/>.
- Use your Company Partner Account Number (optional), or we will attempt 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 Managed Security Provider Geo Sales leader, Partner Business Manager, or Alliance Business Manager if additional assistance is needed.

Managed Security Provider Program Requirements

Applicable to OpenText Data Security

- ISO Certified Data Center
- 24x7 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

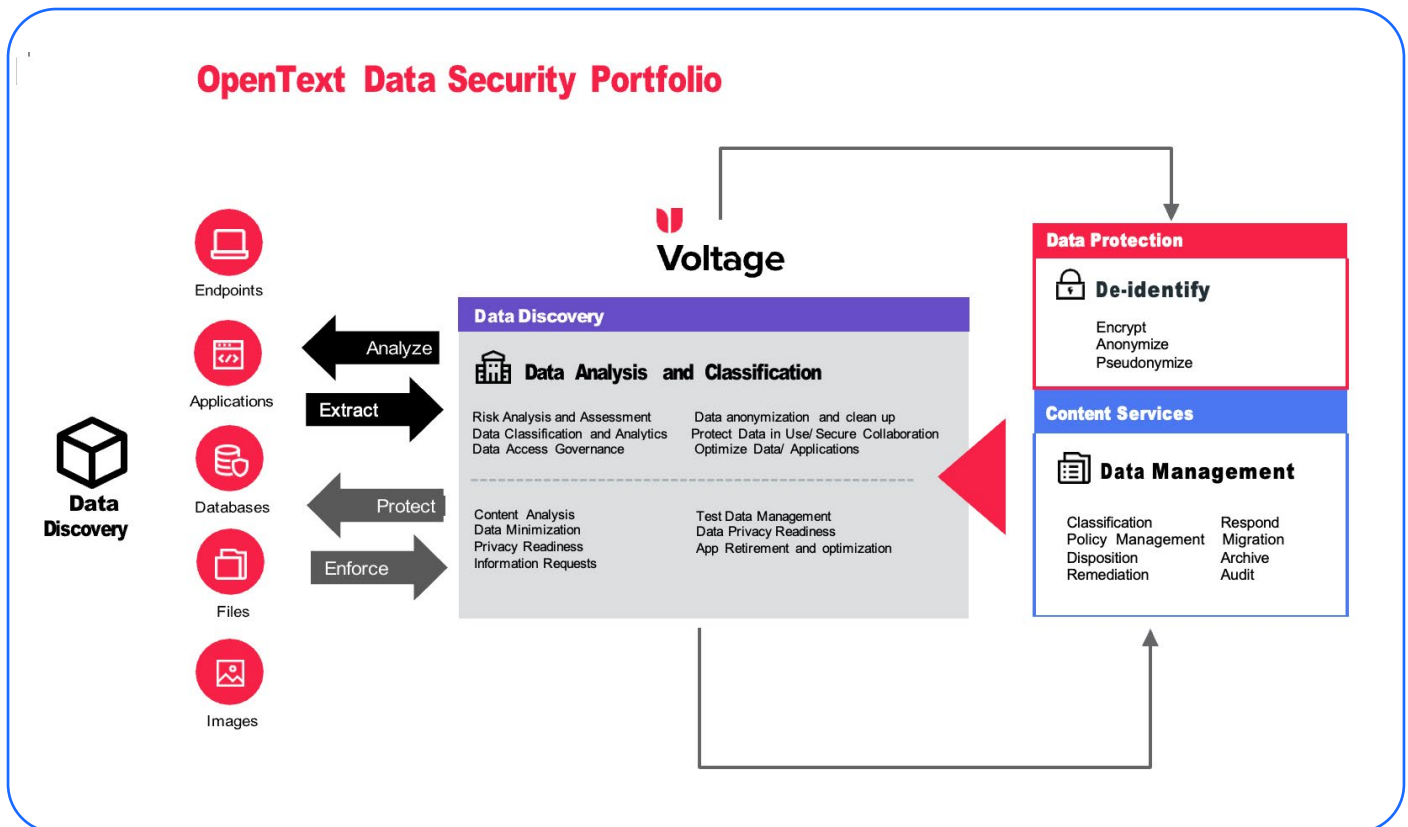
Managed Security Provider Skills Assessment

Quarterly Business Plan, Marketing Plan, and Business Plan Review

OpenText Data Security as a Service Managed Security Provider (MSP) Program

OpenText Data Security as a Service Managed Security Provider (MSP) Guide

This guide describes the OpenText Data Security offering applicable to Managed Security Providers.



The OpenText Data Security solutions provide Managed Security Providers (MSPs) with a unique opportunity to address the major challenges associated with data privacy and protection in a Managed Security Offering.

For Managed Security Providers (MSPs) offering OpenText Data Security capabilities, we empower the following:

Selling strategies | It all starts with data discovery...



Data Clean Up/ Smart Migration

- Detect redundant, trivial and out of date information
- Defensibly delete data
- Optimize storage, reduce total cost of operations
- Additional Path to Data Discovery and Data Privacy and Data Protection use cases



Privacy Risk Assessment

- Cloud-based, or pre-packaged for fast time-to-value
- Short-term licensing available
- Random Sampling and visualization of Sensitive Data
- Additional Path to Data Discovery and Data Protection use cases



Data Discovery

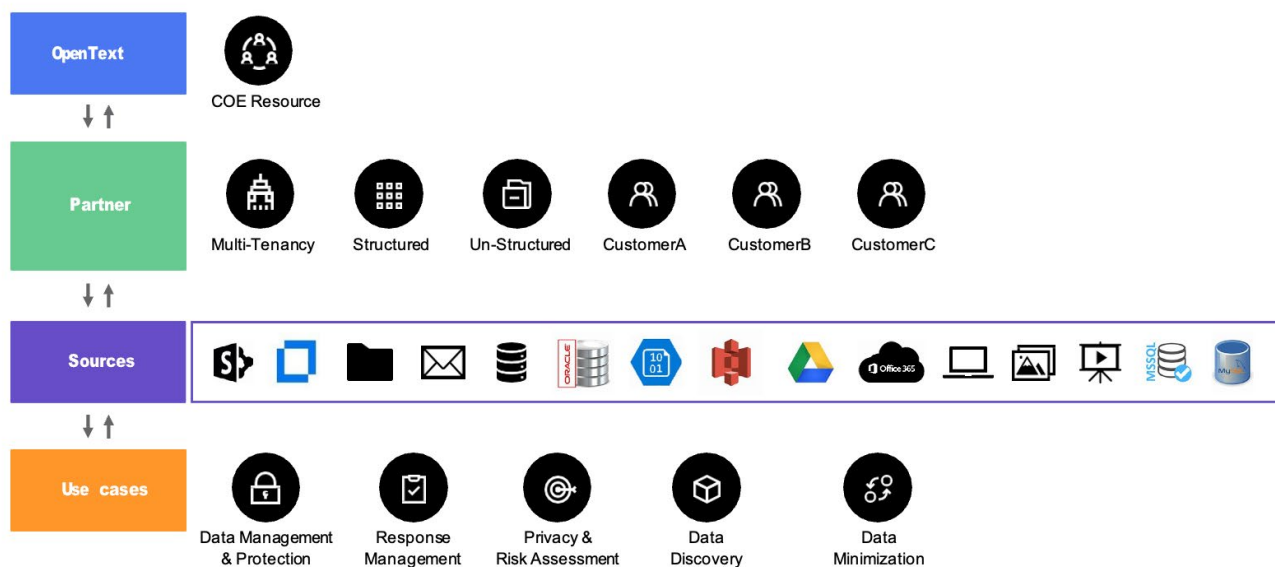
- Start with unstructured data
- Single Source of truth for managing Data Lifecycle
- Support Data Privacy Readiness, business purpose and contextually aware PII detection
- Broader OpenText data security portfolio upsell around

The following OpenText Data Security solutions are currently available in the OpenText Data Security Managed Security Provider (MSP) program:

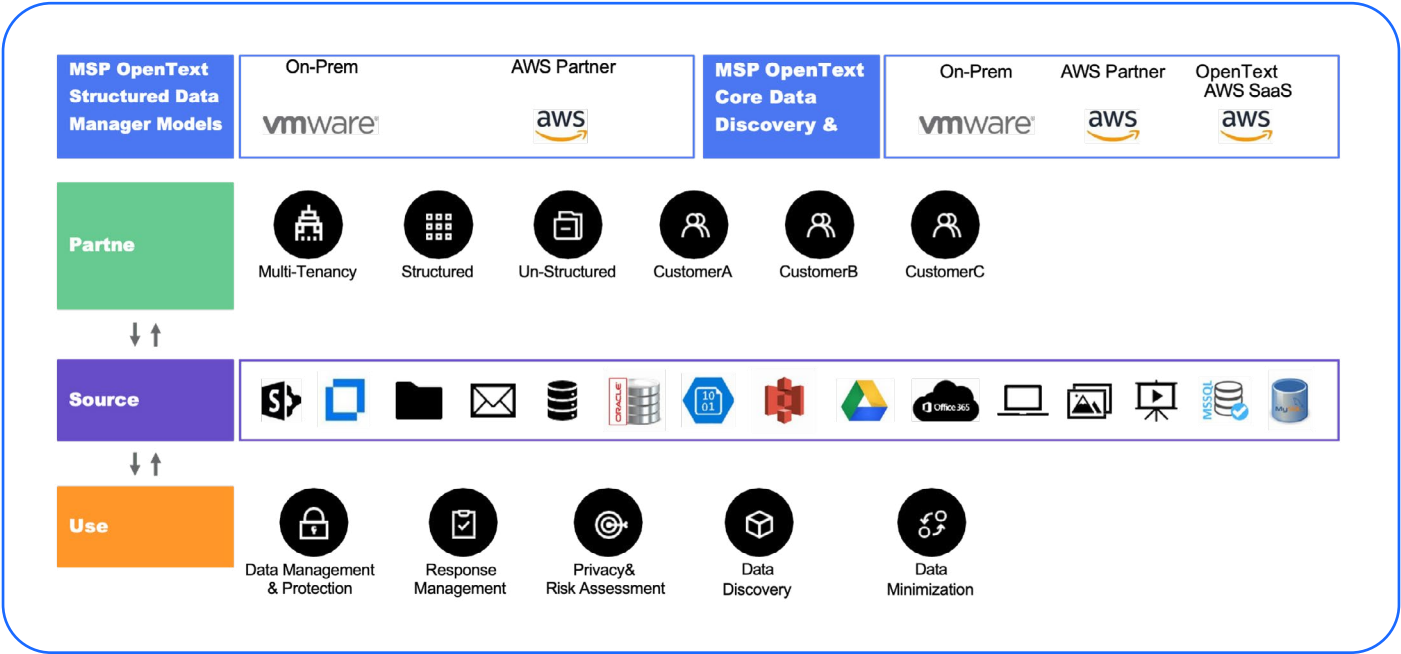
1. OpenText Structured Data Manager Solutions
2. OpenText Core Data Discovery & Risk Insights

This is offered as a multi-tenant capability as depicted below to address structured and unstructured data:

MSP model overview



In addition, these solutions are available in various deployment options/ scenarios. Please consult your Managed Security Provider (MSP) Geo Business Manager on the right deployment model for your region and business offering/ business case.

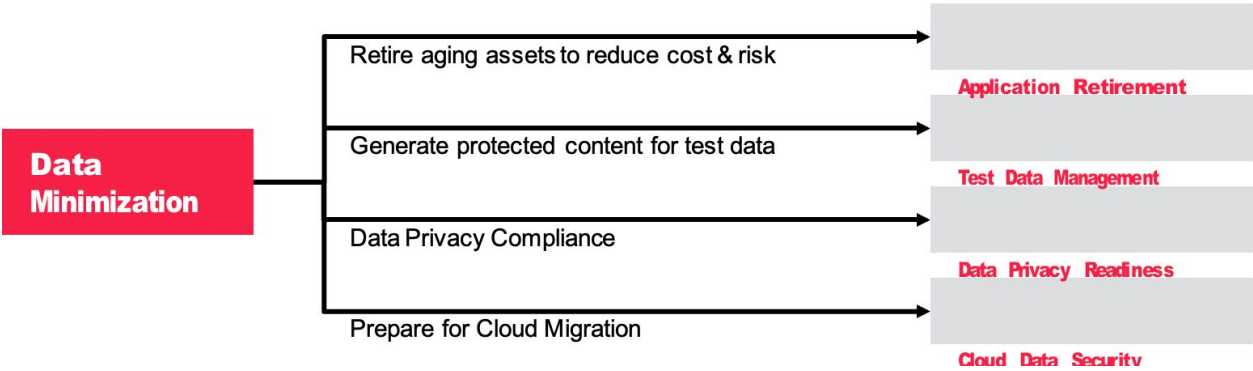


OpenText Structured Data Manager License Models, Usage, and Pricing

Discover and protect sensitive data, preserve its business value, and manage the life cycle of information held in databases. OpenText Structured Data Manager reduces the total cost of ownership of application infrastructure, increases business productivity, raises information value, and mitigates the risks associated with tightening compliance requirements.

Data Security as a Service | OpenText Structured Data Manager for MSP Powered Offering

Addressing multiple challenges



Structured Data Manager application archiving solution effectively migrates eligible transactions off of your Oracle, Microsoft SQL Server, IBM DB2, Sybase, or other JDBC-accessible databases while seamlessly preserving data access and integrity to support long-term retention and access requirements.

Features and Benefits

OpenText Structured Data Manager provides unmatched flexibility to harness the power of a holistic approach to information management with the following built-in integrations:

- **OpenText Content Manager:** Captures, manages, helps secure, and disposes of information according to corporate and compliance policies.
- **OpenText Data Privacy & Protection (DPP) Foundation:** Enables OpenText Structured Data Manager to protect sensitive data as it moves across the IT ecosystem, at rest, in motion and in use, without gaps in security.
- **OpenText Analytics Database:** Provides high-performance analytics so you can gain better business insights from your information.
- **Amazon S3:** Leverage as storage to continue to lower costs and increase ROI for your cloud investment.

Structured Data Manager is certified for multiple open system databases and is designed to leverage vendor-specific database capabilities to help you simplify operations, increase application archiving performance, and reduce maintenance. This native API and deep integration approach ensure that once the database archiving modules are designed and implemented, you can run them on a regular basis (monthly or quarterly) to fully maintain your databases and monitor your archiving jobs just like any other data center task. Each archiving operation is launched as a single job; in the event of an error, the job engine handles recovery tasks and relaunches the job, as required.

Discover and Analyze | Structured Data Management



Key Product Features and Differentiators

- Connect to all types of environments and manage them all in one interface
- Fast scanning performances
- Risk Index is calculated within the table and is customizable
- Grammars are all managed through the UI

Structured Data Management

- OpenText Structured Data Manager-in-a-Box/Accelerator augmenting DPIA and Data Assessment Services. It serves as enabler/accelerator for Data Protection and Data Management Services.
- Flexible License Deployment (AWS Cloud, On-prem, MSP) for Data Management programs/initiatives.

OpenText Structure Data Manager Managed Security Provider (MSP) Licensing Models

This Licensing Model is designed for Managed Security Provider (MSP) Partners who require a leveraged and repeatable solution deployed to support multiple end customers through a single technology configuration. It offers software and licenses for OpenText Structured Data Manager products in a subscription term or usage-based price model, enabling Managed Security Provider (MSP) Partners to provide services to multiple end customers.

Program entry

- A non-discountable Annual Base Package cost of \$5,000 USD
- (1 year) or \$15,000 USD (3 years) will grant entry into this OpenText Data Security program. Prices may vary by country and confirmed by a OpenText legal quote. This base package, comprised of multiple product licenses, must be repurchased at the end of each one (1) or three (3) year term.
- SKU-SB AF180
- The Annual Base Package will deliver 3 databases limited to 100 tables, as part of the initial program start-up.

Licensing Options

- **Pay in advance**—This option allows Managed Security Provider (MSP) Partners to pre-purchase upfront anticipated consumption, with a quarterly draw down off the pre-purchase balance. Once the pre-purchase amount is consumed, partner is obligated to repurchase or convert to pay-per-use (for a new term duration). Any remaining pre-purchase balance at end of Annual Base Package term is forfeited.
- **Pay-per-Use**—This option allows Managed Security Provider (MSP) Partners to pay by Data Source per quarter. A signed blanket Purchase Order is a requirement to facilitate quarterly billings and usage invoicing. The blanket purchase order will include the agreed estimated usage fee amount, the period of service, the blanket purchase order identification, and be signed.

Pricing is per source. One source = one Production database instance (identified in the setup configuration). A source production database instance is represented by a connection to a running RDBMS on a virtual or physical server.

Data Source Definition: Structured Data Manager licensing is per source instance of an RDBMS when used for production purposes. On the same physical or virtual server, you can have multiple instances of an RDBMS running.

Examples:

- **Oracle:** An instance of Oracle RDBMS.
- **SQL Server:** An instance of SQL Server RDBMS. You can have multiple what Microsoft calls databases in the same instance. These are, in fact, catalogs or schemas inside the instance.
- **DB2:** An instance of DB2 RDBMS.
- **PostgreSQL:** An instance of PostgreSQL RDBMS.
- **Hadoop Thru Hive or MangoDB:** Here you may have a cluster with multiple data sets. These data lakes or data warehouses are usually hosting data that came from some other production RDBMS. If you already have a license of the source feeding the lake, then you only count Hive as 1 data source. Otherwise, you need to understand how many sources are feeding the lake or the warehouse.
- **Special case:** Excel files and Access files: Multiple files will be considered as one source depending on their sizes.

Perpetual Licenses: These are not an option for Managed Security Provider (MSP) Partner use and may not be purchased for such use under this program.

Internal Use: No Internal Use is allowed with Managed Security Provider (MSP) 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.

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

Product code	Product description	Term	List Price
SB-AF180	OpenText Structured Data Manager Platform per Source Database Subscription SW E-LTU	Can be quoted as 12- to 60-month Subscription Term or Pay-per-Use	Price based on term duration and quantity purchased
SB-AF181	OpenText Structured Data Manager Query Server per Source Database Subscription SW E-LTU	Can be quoted as 12- to 60-month Subscription Term or Pay-per-Use	Price based on term duration and quantity purchased
SB-AF182	OpenText Structured Data Manager, OpenText Core Data Discovery & Risk Insights and OpenText DPP Integration Module per Source Database Subscription SW E-LTU	Can be quoted as 12- to 60-month Subscription Term or Pay-per-Use	Price based on term duration and quantity purchased
SB-AF183	OpenText Structured Data Manager, OpenText Test Data Management Module per Source Database Subscription SW E-LTU	Can be quoted as 12- to 60-month Subscription Term or Pay-per-Use	Price based on term duration and quantity purchased
SB-AF184	OpenText Structured Data Manager, Data Privacy Manager per Source Database Bundle Subscription SW E-LTU	Can be quoted as 12- to 60-month Subscription Term or Pay-per-Use	Price based on term duration and quantity purchased

Subscription Term:

1. Pricing is per source. One source = one Production database instance. A source production database instance is represented by a connection to a running RDBMS on a virtual or physical server.
2. Price is based on term duration and quantity purchased. Requires a SFdC quote to confirm pricing.

Pay-per-Use:

1. Pricing is per source. One source = one Production database instance. A source production database instance is represented by a connection to a running RDBMS on a virtual or physical server.
2. Pay-per-Use leverages the same Product Code as Subscription Term. Pay-per-Use is selected by modifying the "Sales Event" attribute in SFdC Quote Configuration.

Product code		
SB-AF180	OpenText Structured Data Manager Platform per Source Database Subscription SW E-LTU	Quarterly in-arrears price per source
SB-AF181	OpenText Structured Data Manager Query Server per Source Database Subscription SW E-LTU	Quarterly in-arrears price per source
SB-AF182	OpenText Structured Data Manager OpenText Core Data Discovery & Risk Insights and OpenText DPP Integration Module per Source Database Subscription SW E-LTU	Quarterly in-arrears price per source
SB-AF183	OpenText Structured Data Manager Test Data Management Module per Source Database Subscription SW E-LTU	Quarterly in-arrears price per source
SB-AF184	OpenText Structured Data Manager Data Privacy Manager per Source Database Bundle Subscription SW E-LTU	Quarterly in-arrears price per source

Pay-per-Use Reporting: During the Term, Managed Security Provider (MSP) Partner shall provide on a quarterly basis a usage report that includes the number of sources by end customer. Managed Security Provider (MSP) Partner will run supplied Usage Script, which will provide an inventory of Data Sources cumulatively. Partner is responsible for identifying the unique data sources.

The reporting template and reporting instructions will be provided to Managed Security Provider (MSP) Partner at time of order. Quarterly Usage Reports are to be submitted to: msspcyberres@microfocus.com

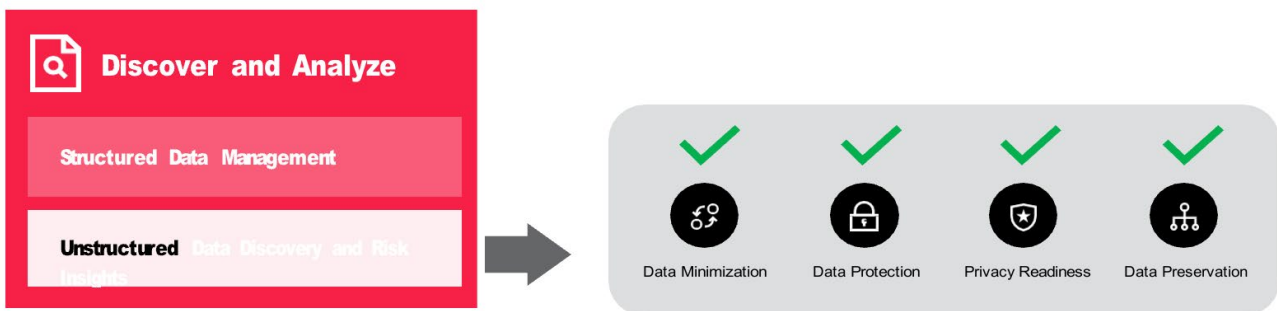
Invoicing: Within (5) five business days of receiving each quarterly Usage Report from Managed Security Provider (MSP) Partner, OpenText will review and calculate the Usage Fees and send a quarterly invoice. OpenText shall book and invoice the usage fees against the blanket purchase order for the Quarterly Invoice Amount no later than ten (10) business days after submission of the Quarterly Invoice Amount fees, to the Managed Security Provider (MSP) Partner.

OpenText Core Data Discovery & Risk Insights License Models, Usage and Pricing

OpenText Core Data Discovery & Risk Insights is a leading provider of data discovery and data protection solutions focusing on data minimization, sensitive data detection, and data privacy and protection activities on unstructured data. OpenText Core Data Discovery & Risk Insights helps Managed Security Provider (MSP) Partners monitor and manage their end customer's unstructured data stores, providing comprehensive visibility into data value, data risk, and lifecycle management of high-value and sensitive data.

Discover and Analyze | Unstructured Data Discovery and Risk Insights

Key OpenText Core Data Discovery & Risk Insights powered use cases



The following are OpenText Core Data Discovery & Risk Insights capabilities currently available to Managed Security Provider (MSP) Partners under the Service Provider Program:

- OpenText Core Data Discovery & Risk Insights includes: metadata and full content analysis, and unique abilities to detect PII (Personal Identification Information) and sensitive data, dynamic tagging, risk-based analytics dashboards, collaborative workspaces, and protective actions to take on data including disposition, legal hold, and collection.
- OpenText Core Data Discovery & Risk Insights supports the most common unstructured document repositories, including Office 365, Teams, SharePoint Online, SharePoint, Exchange, Google Drive, and NT file shares. Additional connectors can be delivered by OpenText in a paid engagement.
- OpenText Core Data Discovery & Risk Insights supports multi-tenant deployment options for the Managed Security Provider (MSP) out of the box. OpenText Core Data Discovery & Risk Insights can be deployed on Amazon Web Services or at Managed Security Provider (MSP) Partners.
- OpenText Core Data Discovery & Risk Insights can be used in conjunction with OpenText Content Manager and on premises deployments, but these are not currently included in the Service Provider Program agreement.

OpenText Core Data Discovery & Risk Insights for MSP Powered Catalog



OpenText Core Data Discovery & Risk Insights Program Requirements

Any Managed Security Provider (MSP) Partner wishing to order OpenText Core Data Discovery & Risk Insights for use in their data center (running VMware) or instance of AWS must meet the following business requirements specifically for their Managed Security Provider (MSP) Business:

- ISO Certified Data Center
- 24x7 Operations and Support model
- Analysts and Administrators staff that meet OpenText Core Data Discovery & Risk Insights skills and qualifications (see OpenText Core Data Discovery & Risk Insights Service Provider (SP) Partner Technical Requirements)
- End Customer Support
- Service Level Agreements (SLA)
- Data Privacy knowledge

Version currency—The Managed Security Provider (MSP) Partner will patch and update OpenText Core Data Discovery & Risk Insights environments within 90 days of the latest release or patch from OpenText. The patches will be made available on the Customer Support Portal or through the Customer Success Manager.

Managed Security Provider (MSP) Partner must communicate to OpenText the location of all data centers by completing and submitting the “OpenText Core Data Discovery & Risk Insights Locations Form.” The form will be provided at time of order. If a new data center is assembled, Managed Security Provider (MSP) Partner must notify OpenText.

All data centers must have built-in resiliency (e.g., production and staging facilities set up) prior to going live with the service. OpenText Core Data Discovery & Risk Insights Locations Form will be provided at time of order and is to be submitted to: msspcyberres@microfocus.com.

In addition, Managed Security Provider (MSP) Partners must provide documentation verifying that each data center from which Managed Security Services (MSS) are provided using OpenText Core Data Discovery & Risk Insights has at least one current industry-standard certification (e.g., ISO, ADC, Uptime Institute).

OpenText Core Data Discovery & Risk Insights Licensing Options

Local data center or partner private cloud (such as AWS) options

These models are designed for Managed Security Provider (MSP) Partners who require a leveraged and repeatable solution deployed in their data center or partner local cloud to support multiple end customers through a single technology configuration.

Program Entry

- A non-discountable Upfront Annual Base Package cost of
- \$5,000 USD (1 year) (OpenText Core Data Discovery & Risk Insights Entry Fee 5TB Service Provider Multi-User Subscription SW E-LTU) will grant entry into this OpenText Data Security program. Prices may vary by country and confirmed by a OpenText legal quote. This base package, comprised of multiple product licenses, must be repurchased at end of each one (1) or three (3) year term.
- OpenText delivers licenses for the Managed Security Provider (MSP) Partner to install in Private Cloud. Partner is responsible for installation and maintaining environment in synchronization with current releases.
- The Annual Base Package will deliver 5TB of Service/yr of service is included. Unlimited ingestion capacity & tenant creation.

Subscription Term—Pay in advance: This option allows Managed Security Provider (MSP) Partners to purchase upfront for a 12-to- 60-month subscription term.

Pay-per-Use: This option allows Managed Security Provider (MSP) Partners to pay by Data Source per quarter, overage is per TB, and captured per quarter. A signed blanket Purchase Order is a requirement to facilitate quarterly billings and usage invoicing. The blanket purchase order will include the agreed estimated usage fee amount, the period of service, include blanket purchase order identification, and be signed.

Perpetual Licenses: Are not an option for Managed Security Provider (MSP) Partner use and may not be purchased for such use under this program.

Transfer: Managed Security Provider (MSP) Partner is not entitled to transfer the Products to any of the Managed Security Provider (MSP) Partner's end customers.

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

OpenText Core Data Discovery & Risk Insights Subscription Term and Pay-per-Use

Subscription Term:

- Price is based on term duration and quantity purchased. Requires a SFdC quote to confirm pricing.

Pay-per-use:

- Pricing is charged per GB usage in any given quarter.
- Quarterly billing in arrears for usage.
- A signed blanket Purchase Order is a requirement to facilitate quarterly billings and usage invoicing. The blanket purchase order will include the agreed estimated usage fee amount, the period of service, include blanket purchase order identification, and be signed.

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, and send a quarterly invoice. OpenText shall book and invoice the usage fees against the blanket purchase order for the Quarterly Invoice Amount no later than ten (10) business days after submission of the Quarterly Invoice Amount fees, to the Managed Security Provider (MSP).

Reporting: During the Term, Managed Security Provider (MSP) Partner shall provide quarterly usage per GB (across all instances) over that period in total and by each end customer.

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

- Quarterly GB Usage Report for every tenant/ end customer

Reporting Template and instructions will be provided to Managed Security Provider (MSP) Partner at time of order. Quarterly usage reports are to be submitted to: msspcyberres@microfocus.com.

OpenText Core Data Discovery & Risk Insights Options

SaaS options are available on a case-by-case basis, in limited geographies and in discussion with the Managed Security Provider (MSP) Geo Sales Leader.

- SaaS options are available on a Volume Pre-Pay Flex credit or consumption Pay-per Use basis, with minimum monthly and annual commitment levels.
- Both SaaS Flex credit as well as SaaS consumption requires an upfront Annual Program Fee of \$5,000.00, which is defined in the table below.
- Mix and match is not possible between the two options.

Both options are detailed below:

	SaaS Flex—Upfront Volume Pre-Pay Purchase	MSSP Business Value
Program fee	• \$5,000 annual program fee • OpenText delivers a single SaaS Flex environment with multi-tenant rights	• \$5,000 annual program fee • OpenText delivers a single SaaS environment with multi-tenant rights
Tenant fee	• Fee per tenant created (draw down off pre-pay value) • Partner is responsible for requesting tenants via Support Tickets	• Fee per tenant created (contributes monthly to quarterly billing) • Partner is responsible for requesting tenants via Support Tickets
Partner requirements	• Partner is responsible for Customer Success management function of its customers and SaaS set up • Set up of customer's users tenants • Professional services to the customer's 1st Line support	• Partner is responsible for Customer Success management function of its customers and SaaS set up • Set up of customer's users tenants • Professional services to the customer's 1st Line support
Annual SaaS contractual commitment	\$100,000	\$50,000
Consumption expectations	Ingestion capacity is limited up to available Upfront Volume Pre-Pay Purchase balance from upfront purchase. Usage draw down is reported monthly. The Annual SaaS contractual commitment establishes a "draw-down" account available for the next 12 months. As ingestion or consumption occurs, the associated delivery fees as established in the order schedule are calculated and the calculated value will be "drawn down" from the Flex dollar balance. As the "draw-down" account approaches 10% of capacity, or the end of the 12-month period approaches, the partner will have the opportunity to make an additional investment of at least \$50,000.	Ingestion capacity is unlimited. Usage drawdown is calculated and invoiced quarterly in arrears. As ingestion or consumption occurs, the associated delivery fees as established in the Legal Quote are calculated and the calculated value is reported to the Managed Security Provider (MSP). OpenText shall book and invoice the usage fees against the blanket purchase order for the Quarterly Invoice Amount no later than ten (10) business days after submission of the Quarterly Invoice Amount fees, to the Managed Security Provider (MSP).
Dedicated OpenText Core Data Discovery & Risk Insights instance	• Transacted with an upfront purchase order only. Not available for activation via a consumption request. Can be mixed with the Entry package and Flex Express Model. • Dedicated Instance set-up fee \$10,000 applies.	• Transacted independently as an upfront order only. Not available for deployment via a consumption request. • Dedicated instance set-up fee of \$10,000 applies.

OpenText Core Data Discovery & Risk Insights Trial/PoC

Ideally suited for privacy impact assessments and short-term engagements such as PoCs or trials, the OpenText Core Data Discovery & Risk Insights Managed Security Provider (MSP) Trial/ PoC model is:

- Single (Dedicated end-customer) use only. End-customer must be disclosed upfront.
- Pay as you go with no upfront commitments (with purchase order).
- Sold in 10TB blocks.

Pricing, license entitlement, and contract terms are valid for one year and can be configured for 1 to 12 months.

SC-AB136	OpenText Core Data Discovery & Risk Insights Volume Package 10TB Service Provider Subscription SW E-LTU
-----------------	---

Support: Annual 24×7 Support and Content Update Subscription is included in all OpenText Core Data Discovery & Risk Insights subscription licenses.

Professional Services and Education

Flex Credits: Flexible Credits are a OpenText service currency that provide a flexible way to obtain additional short-term services. Flexible Credits can be purchased upfront 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

OpenText Core Data Discovery & Risk Insights Managed Security Provider (MSP) Partner Technical Requirements

Set up, maintain, monitor, and manage a diverse group of technologies consumed by a cloud-native, broad-scale application. Proactively provide elevated levels of availability and performance of the application and its environment, striving to deliver best-in-class reliability and QoS (Quality of Service). This includes both operations of existing monitoring and management technologies, but also active contributions to the investigation and implementation of additional components.

Managed Security Provider (MSP) Partner Skill Sets and Qualifications

- Significant practical experience managing hybrid application infrastructure; equally comfortable in working with *nix and Windows.
- Practical experience managing cloud infrastructure, including cloud-native SaaS offerings in conjunction with cloud-operated but self-controlled components.
- Knowledge of multiple environment experience will be helpful.
Example: AWS, Azure, OpenStack, On-Premises virtualization such as vCenter, etc.
- Experience designing, communicating, implementing, enforcing, and auditing modern security best practices for both application and infrastructure.
- Practical experience in operating high-availability SaaS production environments.
Rapid and effective incident response using a follow-the-sun model with fellow team members.
- Comfortable working in a global, geographically diverse company; must be able to communicate primarily in English.

Managed Security Provider (MSP) Partner Technical Skills

- Experience in scripting (bash and PowerShell preferred. Python, ruby, etc., a plus).
- Experience with Docker containers (specifically on *nix, Windows containers a plus).
- Familiarity with container orchestration and scheduling technologies (Mesos\ Marathon and Kubernetes).
- Knowledge and management skills with large-scale indexing systems—Elasticsearch.
- Knowledge and technical skills in managing and maintaining RDB systems (PostgreSQL and MS SQL).
- Knowledge and management skills with message queuing systems (RabbitMQ).
- Knowledge and management skills with platform monitoring and reporting systems (Netdata and Grafana).
- Knowledge and management skills with scaling and load-balancing technologies (haproxy, Apache as a reverse proxy, etc.).
- Knowledge and management skills with lower-level infrastructure services (Active Directory, Certificates, SMTP, Routing, etc.).
- Experience with traditional enterprise IT virtualization technologies (VMware).
- Familiarity with platform automation technologies (chef, salt, puppet, etc.).
- Familiarity with other enterprise infrastructure systems (SharePoint, Exchange, etc.).

Training Requirement

Managed Security Provider (MSP) Partners must verify that at least one individual has completed all four of the following OpenText training courses. Completion is required prior to onboarding to the OpenText Core Data Discovery & Risk Insights Managed Security Provider (MSP) Partner Program.

- OpenText Data Security L300
- OpenText Core Data Discovery & Risk Insights L320
- OpenText Core Data Discovery & Risk Insights L340
- OpenText Core Data Discovery & Risk Insights PoC Readiness, Level 360

Additional Terms and Conditions

This Program and Guide content are subject to change without notice.

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:

Trademarks

© 2022 OpenText or one of its affiliates. OpenText and the OpenText logo, among others, are trademarks or registered trademarks of OpenText or its subsidiaries or affiliated companies in the United Kingdom, United States, and other countries. All other marks are the property of their respective owners.

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. The information contained herein is subject to change without notice.

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 an 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 OpenText, 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.

Resources

**Enterprise Cybersecurity
Solutions & Services | OpenText**

[Visit OpenText
Cybersecurity Cloud ›](#)

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 OpenText's 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. 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.