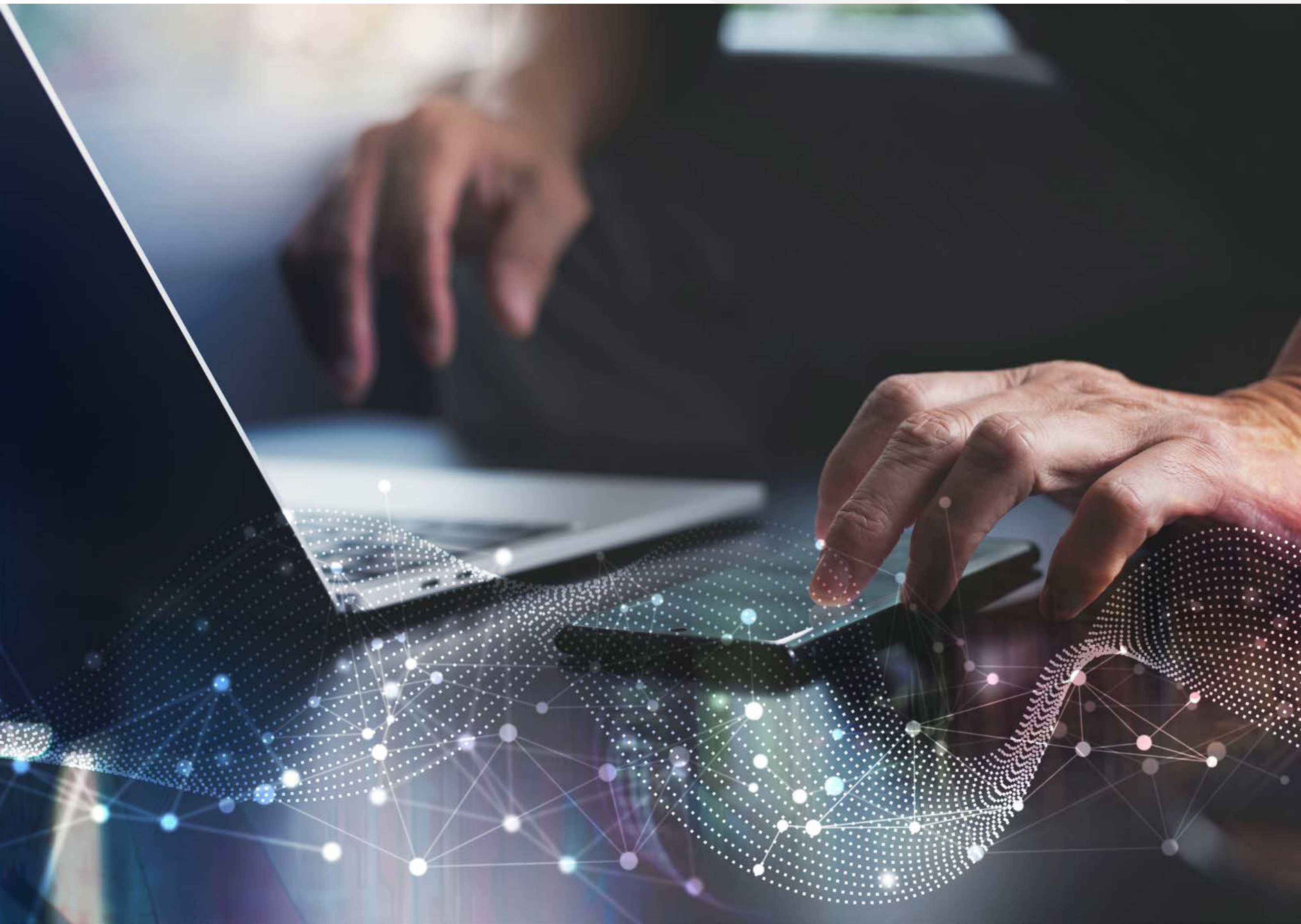
GUIDE

Managed Security Provider (MSP) OpenText Identity and Access Management (NetIQ) Partner Program Guide

March 2025



Contents

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 Managed Security Provider 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.

The OpenText Cybersecurity Managed Security Provider (MSP) 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
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
NetIQ Marketplace and User Groups

How to become a Managed Security Program Partner and Managed Security Provider

How to become a Managed Security Provider

Step 1: Register your company

- Complete a simple online company registration form.
- 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 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.
- 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 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™ NetIQ™ Identity and Access Management • IISO 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

OpenText Identity And Access Management (NetIQ) Managed Security Provider (MSP) Guide

OpenText™ NetIQ™ IAM secures organizations through a comprehensive set of identity and access services for workforce and customer identities. The OpenText NetIQ IAM solutions provide Managed Security Providers (MSP) with a unique opportunity to address the major challenges associated with securing and managing identities and access for employees, contractors, citizens, consumers, and devices in a hybrid world.

The OpenText NetIQ IAM portfolio offers an in-depth and robust IAM portfolio for Managed Security Providers (MSP).

The Managed Security Provider (MSP) can build a managed IAM offering from any of the capabilities as a single offering or as a combined IAM solution offering.

Managed Security Provider (MSP) program and licensing

Program entry

- An initial program buy-in of 1,000 Identities Licenses is required for entry into the IAM program . This is an annual subscription purchase buy-in.
- The OpenText licenses are managed on a Managed Identity model and underpinned by the OpenText ALA terms applicable to NetIQ.
- The program is a Pay-per-Use Model, encouraging growth and adoption across the full IAM portfolio offering.
- 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.

Licensing options

- **Subscription Term—Pay in Advance:** This option allows Managed Security Provider (MSP) Partners to purchase up front for a 12-to-60- month subscription term.
- **Pay-per-Use:** This option allows Managed Security Provider (MSP) Partners to pay quarterly in arrears, in a Pay-as-You-Grow model.

Pay as You Grow allows additional managed identities to be added as use cases or managed identity estates grow and billed quarterly.

- **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 the Partner's own internal business operations or functions.

Subscription term

1. Pricing is per Managed Identity.
2. Price is based on term duration and quantity purchased. Requires a Legal quote to confirm pricing.

Pay-per-use

1. Pricing is per Managed Identity.
2. PAM (Privileged Access Management) consumption will be determined via the PAM Console and reported in quantity of Administrators, Users, and Service Accounts.
3. At time of initial purchase, Managed Security Provider (MSP) Partner is obligated to complete an onboarding document committing to how Managed Identities are counted and reported to OpenText . Consumption usage measurement is ideally the same as Managed Security Provider (MSP) Partner utilized for invoicing end customer.
4. Consumption usage is reported quarterly via manual form (provided by OpenText to Managed Security Provider (MSP) Partner at time of order).
5. Managed Security Provider (MSP) Partner is required to report new customers with quantity of managed identities via the Deal Registration Form, with quantity of managed identities at time of onboarding a new customer.
6. Managed Security Provider (MSP) Partner is required to report departing customers via manual form (provided by OpenText to Managed Security Provider) with the regular quarterly reporting submissions.
7. Consumption usage is charged quarterly.
8. Managed Security Provider (MSP) Partner is obligated to provide a blanket purchase order for quarterly overages for the term of the contract . The blanket purchase order will include the agreed estimated usage fee amount, the period of service, and blanket purchase order identification and it must be signed.
9. Managed Security Provider (MSP) Partner will submit consumption usage to the OpenText MSSP Operations team quarterly.
10. Initial billing period will be amended considering business ramp up and OpenText Cybersecurity preference to transact in month two of OpenText Fiscal quarter.
11. Minimum quarterly invoice is $2,500; otherwise usage is held to forward periods.
12. Enablement to be provided to Managed Security Provider (MSP) Partner administrators for reporting once signed up to the program.

Pay-per-use reporting: During the Term, Managed Security Provider (MSP) Partner shall provide on a quarterly basis a consumption usage report that includes the number of managed identities by end customer.

The reporting template and reporting instructions will be provided to Managed Security Provider (MSP) Partner at time of order.

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.

Payment options:

- Pre-paid annually
- Pre-paid in advance
- Quarterly usage

SaaS Licenses: Require a minimum purchase of 1,000 SaaS Managed Identities per annum, as is available upon discussion with your MSP program manager in your geography.

License True-Ups: License true-ups will be required annually or contractually, based on reported consumption overage and install base growth.

Overage of 10% will be allowed:

- <10% corrections are addressed go-forward.
- >10% corrections are retroactive and applied go-forward with additional license purchases.

Managed Security Provider (MSP) Partners are required to provide to OpenText the end-customer invoices and contracts in the event of a license over-usage dispute.

Additional Definitions

- Managed Identity means an identity managed by or connecting through the licensed software.
- Database means application data, including table structure, stored procedure, and other functionality.
- Deployment means the software implementation plus the associated licensed software that is part of the Identity Intelligence Solution.
- User means a user object in a single directory tree (or other class of object that contains data representing a person, such as
- objects containing credit card information or PIN numbers) that has:
  (a) access or use rights to any portion of the Licensed Software, or
  (b) access or use rights to products (devices, hardware, or software)
  being managed by the Licensed Software, regardless of whether the user object is assigned to a person or device . User objects (or other classes of objects) representing the same person that are linked to each other within a single tree and/or linked across multiple trees count as only one user.
- Privileged credential means a credential that allows the user to perform advanced functions on whatever system they are accessing.

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

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 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 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.

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's 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.