

Ontinue Consulting Services Statement of Work

Consulting Services



Table of Contents

1.	About Consulting Services.....	3
2.	Engagement Overview & Scope.....	3
2.1.	Engagement Overview.....	3
2.2.	Engagement Scope.....	3
2.2.1	Within Engagement Scope.....	3
2.2.2	Outside Engagement Scope.....	3
3.	Technology & Prerequisites.....	4
3.1.	Technology License Requirements.....	4
3.2.	Permission Requirements.....	4
4.	Engagement Phases.....	4
4.1.	Kickoff Roles & Responsibilities.....	4
4.2.	Engagement Phases.....	4
5.	Engagement Delivery.....	5
5.1.	Engagement Delivery Roles & Responsibilities.....	5
5.2.	Engagement Mechanics.....	5
6.	Commercial Terms.....	5
6.1.	Fees.....	5
6.2.	Microsoft Funding.....	5
6.3.	Scope Overage.....	6
6.4.	Microsoft Partnership Attribution.....	6
6.4.1	CPOR – Claiming Partner of Record.....	6
7.	Schedule A – Consulting Services Packages.....	6



1. About Consulting Services

Ontinue Consulting Services are a catalog of fixed-price, package-based engagements that help Customer implement the Ontinue Services and adopt Microsoft security features. Ontinue's consultants deliver Consulting Services remotely, working alongside Customer's team through discovery sessions, workshops, and configuration assistance for the defined Consulting Service package selected by Customer.

Ontinue's obligation to perform the Consulting Services is conditional on Customer procuring one or more Consulting Service packages in an Order and agreeing to pay the applicable fees as specified in the Order. Ontinue will provide only the specific Consulting Service package(s) identified in Customer's Order. This Statement of Work, together with the applicable Order referencing a Consulting Services package, is incorporated into the Multi-Services Agreement available at www.ontinue.com/msa, or such other agreement between Ontinue and Customer covering the subject matter of this Statement of Work (the "Agreement").

This document covers the following:

Section	Description
Engagement Overview & Scope	The catalog of available Consulting Service packages, and what is and is not included across all packages.
Technology & Prerequisites	The licenses, environment access, and permissions Customer must provide to support any Consulting Services engagement.
Engagement Phases	How a Consulting Service engagement begins and progresses.
Engagement Delivery	How Consulting Service engagements are delivered and closed out, including roles, mechanics, deliverables, and package-specific activities.
Commercial Terms	How Consulting Services are priced, including Microsoft Funding availability.

2. Engagement Overview & Scope

2.1. Engagement Overview

Consulting Services are provided on a fixed-price basis and are delivered remotely from a location determined by Ontinue. Each Consulting Service package addresses a specific implementation objective and is delivered through a defined set of discovery sessions, workshops, and configuration activities. The catalog of available Consulting Service Packages is outlined in Schedule A. Schedule A outlines all of the Consulting Services that Ontinue offers, but the Consulting Services which Customer receives will be specified in the applicable Order.

2.2. Engagement Scope

2.2.1 Within Engagement Scope

- The Ontinue and Customer in-scope activities specified in the selected package

2.2.2 Outside Engagement Scope

- Azure and/or Microsoft 365 setup and configuration work outside of what is required for the selected package
- Formal training, support, or certifications



- Direct incident response services; if a security breach is identified during an engagement, Ontinue will collaborate with and support Customer's designated Incident Response vendor(s), but does not act as that vendor
- Any additional exclusions specified for the selected package

3. Technology & Prerequisites

Technology, licensing, and access prerequisites vary by Consulting Service package. Common prerequisites across most packages are listed below:

3.1. Technology License Requirements

Technology	License	Comments
Microsoft 365	Minimum Microsoft 365 E5 Security or E5 Compliance, depending on package	Trial licenses may be used with Ontinue's authorization
Microsoft Azure	Active Azure subscription and tenant	Required for packages involving Microsoft Sentinel

3.2. Permission Requirements

- Customer assigns Ontinue role-based access appropriate to the selected package, provided via a Customer-managed account, PIM-managed identity, or Teams remote screen-sharing
- Exact roles required are defined per package

4. Engagement Phases

This section describes how an engagement begins and progresses.

4.1. Kickoff Roles & Responsibilities

Key Party	Contact / Entity	Kickoff Responsibilities
Ontinue	Consulting Services	Arrange and lead the Project Kickoff and Discovery session; confirm engagement scope and timeline.
Customer	IT Security Operations	Ensure attendance of relevant personnel at the Kickoff session; submit and obtain approval for any required Change Requests prior to engagement commencement; provide environment access and licenses.

4.2. Engagement Phases

Phase	Outcome	Typical Duration
Kickoff & Discovery	Engagement scope, timeline, and roles confirmed; Customer completes the applicable discovery questionnaire	1 session
Workshops & Configuration	Package-specific workshops and configuration activities delivered	Varies by package
Next Steps & Close-Out	Next-steps recommendation document delivered; Proof of Execution submitted to Microsoft where applicable; engagement formally closed	1 session



5. Engagement Delivery

This section describes the expected engagement from each party during delivery of the Consulting Services.

5.1. Engagement Delivery Roles & Responsibilities

Key Party	Contact / Entity	Delivery Responsibilities
Ontinue	Consulting Services	Lead workshop sessions per the selected package; provide best-practice recommendations aligned to Customer's environment and stated goals.
Customer	IT Security Operations	Ensure attendance of relevant personnel at workshop sessions; honor reasonable requests for information within 1 business day; accept responsibility for any Azure consumption or license charges resulting from the engagement.

5.2. Engagement Mechanics

- **Environment Access:** Ontinue consultants may require access to Customer's environment to deliver the engagement. Ontinue provides best-practice recommendations but primarily follows Customer's direction; Customer is solely responsible for the direction and instructions it provides, and Ontinue is not liable for following that direction.
- **Scope Change:** Ontinue will endeavor to complete the engagement within the estimated timeframe. Any extension due to Customer delays, expanded work requested by Customer, or reasons outside Ontinue's control may result in additional charges at Ontinue's then-current daily security consultant rate, subject to a change order prior to Ontinue commencing or continuing such work.
- **Language & Delivery Location:** All services, communication, and documentation are delivered in English. All Consulting Services are delivered remotely, from a location determined by Ontinue.

6. Commercial Terms

6.1. Fees

Consulting Services are provided on a fixed-price basis, payable in advance.

6.2. Microsoft Funding

Packages marked as Funding Available may qualify for funding from Microsoft ("Microsoft Funding"), subject to Ontinue confirming Customer's eligibility. Microsoft Funding is based on the fixed price quoted by Ontinue and reflects the current state of Customer's environment and Ontinue's assessment of project scope. Microsoft Funding is conditional on:

- Ontinue's delivery of all in-scope items for the package;
- Customer completing Microsoft's customer feedback/questionnaire form; and
- Submission of the workshop's proof of execution and feedback form to Microsoft.

If Ontinue is unable to successfully claim Microsoft Funding due to a delay or failure by or on behalf of Customer, Ontinue reserves the right to charge Customer the quoted amount without the Microsoft Funding discount.



6.3. Scope Overage

Efforts or deliverables required beyond the scope covered by the selected package, or beyond any Microsoft Funding available, are provided on a time-and-materials basis following rescoping with the Ontinue project team, per the Scope Change terms in Section 5.

6.4. Microsoft Partnership Attribution

As part of delivering Consulting Services, Ontinue will register as Claiming Partner of Record (CPOR) for the Microsoft workload(s) it helps implement or configure, and will attribute its Microsoft Partner Network (MPN) ID via Partner Admin Link (PAL) for in-scope Azure workloads. No action is required from Customer for either designation.

6.4.1 CPOR – Claiming Partner of Record

CPOR enables Microsoft to identify and recognize those partners who are helping Customer's achieve business objectives and realize value in the cloud. Once a partner associates to a workload or subscription, they will obtain access to usage and/or sold seats data. Access to such data enables partners to monitor active usage while providing Customer's with recommendations on how to maximize usage. Partners will not have access to any other Customer data. Additionally, the CPOR association helps Microsoft understand the ecosystem of service providers, and also helps Microsoft determine how to refine the tools and programs needed to best support our common Customer's. There is no action required for Customer. As part of this engagement Ontinue will claim CPOR for the workload(s) they assist in implementing and configuring

7. Schedule A – Consulting Services Packages

Package Category	Package Name
Discovery	Ontinue Zero Trust Discovery Package
	Ontinue AI Security Discovery Package
Workshop	Ontinue Microsoft Threat Protection Workshop Package
	Ontinue Microsoft Defender for Cloud Workshop Package
	Ontinue Microsoft Sentinel Workshop Package
	Ontinue Microsoft Data Security Workshop Package
Accelerator	Ontinue Microsoft Defender for Cloud Accelerator Package
	Ontinue Microsoft Sentinel Accelerator Package
Deployment	Ontinue Microsoft XDR Deployment Package
	Ontinue AI Security Deployment Package
	Ontinue Microsoft Purview Deployment Package
	Ontinue Microsoft Entra ID Deployment Package
	Ontinue Microsoft iSOC Deployment Package
Readiness	Ontinue Microsoft Defender for Office 365 Readiness Package
	Ontinue Microsoft Purview Readiness Package

Nonstop SecOps

Questions? Let's talk.

European HQ

Grubenstrasse 54, 8045 Zürich,
Switzerland

Düsseldorf Office

Speditionstraße 2, 40221
Düsseldorf, Germany

North America HQ

450 Maple Street, Redwood City,
CA 94063, USA

Vienna Office

Kohlmarkt 8-10, 1010 Wien, Austria

UK Office

9 Holborn, London EC1N 2LL, United
Kingdom

APAC Office

World Trade Tower, Sector 16, Noida
201301, India

Toronto Office

6060-3080 Yonge St, Toronto ON
M4N 3N1, Canada

 Continue

Ontinue

Ontinue Zero Trust Discovery Package Consulting Services

Version: v1.00

Effective Date: 24.08.2026



Table of Contents

- 1. About Zero Trust Discovery..... 3
- 2. Engagement Scope..... 3
 - 2.1. Ontinue In-Scope Activities..... 3
 - 2.2. Customer In-Scope Activities..... 3
- 3. Engagement Outputs..... 4
- 4. Assumptions, Dependencies, Constraints..... 4



1. About Zero Trust Discovery

An evaluation of Customer's security posture across the identity, device, data, and network pillars against Microsoft baselines. Ontinue runs the automated Microsoft Zero Trust Assessment script against Customer's tenant to audit configurations, detect risks, and identify security gaps, then delivers a detailed findings report and an executive readout with a prioritized roadmap to accelerate Zero Trust maturity.

2. Engagement Scope

2.1. Ontinue In-Scope Activities

- Arrange and lead up to 1 x 1hr Project Kick-Off and Discovery session
- Complete the Ontinue Security Strategy Review, up to 3 x 2hr sessions
- Perform a review of Customer's current security posture, covering:
 - Microsoft licenses (required, as the license level determines the scope of the scan below)
 - Identity: Entra ID
 - Devices: Intune, Entra ID
 - Data: Purview
 - Network
 - Infrastructure
 - Security Operations: Microsoft Defender for Identity, Microsoft Defender for Office 365, Microsoft Defender for Endpoint, Microsoft Defender for Cloud Apps
 - SIEM/SOAR: Microsoft Sentinel
 - AI (optional)
- Review Secure Score and present the reported recommendations
- Generate the Zero Trust Report by running the official Microsoft Zero Trust Assessment PowerShell script in Customer's tenant
- Generate next steps recommendations with high, medium, and low priority options and timelines, using the Microsoft Zero Trust Assessment website and a customized PDF report
- Review all findings with Customer in a readout of the Zero Trust Report
- Arrange and lead the Project Close-Out session

2.2. Customer In-Scope Activities

- Attend up to 1 x 1hr Project Kick-Off and Discovery session
- Complete the Ontinue Security Posture Questionnaire
- Assign the following permissions for Ontinue: Security Administrator, Compliance Administrator, Global Reader, Intune Administrator, and Reader on Azure subscriptions
- Provide licenses to support Ontinue activities, or authorization to use trial licenses (minimum Microsoft 365 E5 Security required)
- Ensure someone with Global Administrator privileges attends the call to run the required scripts
- Meet the following technical prerequisites:
 - PowerShell 7 or later (required)
 - Zero Trust Assessment PowerShell module
 - Stable internet connectivity
 - Local storage for the script report output
 - Admin consent, if required
- Arrange or perform any required proxy, firewall, or network changes to support Ontinue activities



- Provide all infrastructure needed for any additional roles (as required)
- Support screenshot generation for the report
- Honor all reasonable requests for information within 1 business day
- Accept full responsibility for all Azure, consumption, and license charges resulting from the engagement
- Ensure attendance of relevant personnel at the Project Close-Out session

3. Engagement Outputs

Output	Owner	Sign-off Required
Next Steps Recommendation Document	Ontinue	No

4. Assumptions, Dependencies, Constraints

Item	Type
Customer has an active Azure subscription	Assumption

Nonstop SecOps

Questions? Let's talk.

European HQ

Grubenstrasse 54, 8045 Zürich,
Switzerland

Düsseldorf Office

Speditionstraße 2, 40221
Düsseldorf, Germany

North America HQ

450 Maple Street, Redwood City,
CA 94063, USA

Vienna Office

Kohlmarkt 8-10, 1010 Wien, Austria

UK Office

9 Holborn, London EC1N 2LL, United
Kingdom

APAC Office

World Trade Tower, Sector 16, Noida
201301, India

Toronto Office

6060-3080 Yonge St, Toronto ON
M4N 3N1, Canada

 **Continue**

Ontinue

Ontinue AI Security Discovery Package Consulting Services

Version: v1.00

Effective Date: 24.08.2026



Table of Contents

- 1. About AI Security Discovery..... 3
- 2. Engagement Scope..... 3
 - 2.1. Ontinue In-Scope Activities..... 3
 - 2.2. Customer In-Scope Activities..... 3
- 3. Engagement Outputs..... 4
- 4. Assumptions, Dependencies, Constraints..... 4



1. About AI Security Discovery

A consulting engagement that aligns Customer's business goals, regulatory needs, and ROI targets with a roadmap for AI adoption. Delivered through interactive workshops and an offline audit of Customer's Microsoft E5 Defender suite (Entra ID, MDE, Intune, MDI, MDO, MDCA, MDC), Ontinue assesses feature fit and projected cost for Microsoft Security Copilot and evaluates the underlying infrastructure. Concludes with an executive readout covering the top five security issues, key configuration gaps, and a plan to deploy Security Copilot safely.

2. Engagement Scope

2.1. Ontinue In-Scope Activities

- Arrange and lead up to 1 x 1hr Project Kick-Off and Discovery session
- Discuss organizational readiness and objectives, up to 2 x 2hr sessions, covering:
 - Business goals and priorities
 - Current gaps
 - Desired future state
 - Goals for usage
 - Industry and regulatory landscape
 - ROI requirements
- Review Microsoft Security Copilot features and gaps, 1 x 2hr session, covering:
 - Current capabilities
 - Missing requirements, based on the readiness and objectives discussions
 - Cost, based on the proposed level of usage
- Complete a Tenant Security Review of the Microsoft security tools in use within Customer's E5 Defender suite. The review is performed offline, up to 5hrs, and covers:
 - Microsoft Defender for Endpoint
 - Intune
 - Microsoft Defender for Identity
 - Microsoft Defender for Office 365
 - Microsoft Defender for Cloud Apps
 - Microsoft Defender for Cloud
 - Entra ID
- Review the Tenant Security Review findings with Customer, 1 x 1hr session, covering:
 - The top five issues found
 - Gaps in the current configuration
 - Readiness to deploy Microsoft Security Copilot

2.2. Customer In-Scope Activities

- Attend up to 1 x 1hr Project Kick-Off and Discovery session
- Complete the Ontinue Security Posture Questionnaire
- Assign the following permissions for Ontinue: Security Administrator, Compliance Administrator, Global Reader, Intune Administrator, and Reader on Azure subscriptions
- Provide licenses to support Ontinue activities, or authorization to use trial licenses (minimum Microsoft 365 E5 Security required)
- Arrange or perform any required proxy, firewall, or network changes to support Ontinue activities
- Provide all infrastructure needed for any additional roles (as required)



- Support screenshot generation for the report
- Honor all reasonable requests for information within 1 business day
- Accept full responsibility for all Azure, consumption, and license charges resulting from the engagement
- Ensure attendance of relevant personnel at the Project Close-Out session

3. Engagement Outputs

Output	Owner	Sign-off Required
Next Steps Recommendation Document	Ontinue	No

4. Assumptions, Dependencies, Constraints

Item	Type
Customer has an active Azure subscription	Assumption

Nonstop SecOps

Questions? Let's talk.

European HQ

Grubenstrasse 54, 8045 Zürich,
Switzerland

Düsseldorf Office

Speditionstraße 2, 40221
Düsseldorf, Germany

North America HQ

450 Maple Street, Redwood City,
CA 94063, USA

Vienna Office

Kohlmarkt 8-10, 1010 Wien, Austria

UK Office

9 Holborn, London EC1N 2LL, United
Kingdom

APAC Office

World Trade Tower, Sector 16, Noida
201301, India

Toronto Office

6060-3080 Yonge St, Toronto ON
M4N 3N1, Canada

 **Continue**

Ontinue

Ontinue Microsoft Threat Protection Workshop Package Consulting Services

Version: v1.00

Effective Date: 24.08.2026



Table of Contents

- 1. About Microsoft Threat Protection Workshop.....3
- 2. Engagement Scope.....3
 - 2.1. Domain Coverage by Package Size.....3
 - 2.2. Domain 5: Secure your devices and endpoints.....3
 - 2.2.1. Continue In-Scope Activities.....3
 - 2.3. Domain 3: Defend against email threats.....4
 - 2.3.1. Continue In-Scope Activities.....4
 - 2.4. Domain 2: Protect your identities and access.....4
 - 2.4.1. Continue In-Scope Activities.....4
 - 2.5. Customer In-Scope Activities.....5
- 3. Engagement Outputs.....5
- 4. Assumptions, Dependencies, Constraints.....5



1. About Microsoft Threat Protection Workshop

A hands-on engagement with Microsoft Defender XDR, deployed to up to 25 workstations and/or 5 users, so Customer sees it detect and respond to real threats. XS covers one domain of Customer's choice: Protect your identities and access, Defend against email threats, or Secure your devices and endpoints; S covers Defend against email threats and Secure your devices and endpoints; M covers Protect your identities and access, Defend against email threats, and Secure your devices and endpoints.

2. Engagement Scope

2.1. Domain Coverage by Package Size

Package Size	Domains Included
XS	One domain of Customer's choice: Domain 2 (Protect your identities and access), Domain 3 (Defend against email threats), or Domain 5 (Secure your devices and endpoints)
S	Domain 3 (Defend against email threats) and Domain 5 (Secure your devices and endpoints)
M	Domain 2 (Protect your identities and access), Domain 3 (Defend against email threats), and Domain 5 (Secure your devices and endpoints)

2.2. Domain 5: Secure your devices and endpoints

2.2.1 Continue In-Scope Activities

- Arrange and lead the Project Kick-Off and Discovery session
- Arrange and lead Workshop sessions covering:
 - Microsoft Defender for Endpoint (Windows workstations)
 - Microsoft Defender for Cloud Apps
- If present: review the existing Defender for Endpoint configuration in Customer's production environment
- If present: review the existing Intune compliance policies in Customer's production environment
- If present: provide recommendations on Intune and Defender for Endpoint configuration and policies
- Configure or verify the following Microsoft Defender XDR configurations:
 - Turn on auditing within the Microsoft 365 Compliance Portal or via PowerShell
 - Configure file monitoring within Defender for Cloud Apps
 - Configure the Office 365 App Connector within Defender for Cloud Apps
 - Enable the malware detection policy in Defender for Cloud Apps
- Onboard up to 25 Windows 10/11 workstations into Microsoft Defender for Endpoint via Intune, if not already onboarded
- Create relevant device groups (if required)
- Configure email notifications (if required)
- Enable the following advanced features: Live Response, Show User Details, Office 365 Threat Intelligence Connection, Defender for Cloud Apps
- Configure role-based access controls (if required)
- Configure device proxy and internet connectivity settings (if required)



- Create a Microsoft Defender Vulnerability Management security baselines assessment
- Deliver Microsoft Security, Microsoft Defender for Endpoint, and Defender for Cloud Apps deep-dive demonstrations
- Generate screenshots from Defender workspaces for the Microsoft Proof of Execution
- If required: decommission any configurations performed during the workshop
- Arrange and lead the Threat Check Results and Next Steps session
- Arrange and lead the Project Close-Out session

2.3. Domain 3: Defend against email threats

2.3.1 Continue In-Scope Activities

- Arrange and lead the Project Kick-Off and Discovery session
- Arrange and lead Workshop sessions covering Microsoft Defender for Office 365
- Review the current email security console and policy sets, including:
 - Mail flow reports
 - Priority user identification
 - Custom filtering rules
 - Allow and block lists to migrate to Defender for Office
- Review Exchange Online mail flow rules
- Review Exchange Online mail flow connectors
- Review Exchange Online Protection settings
- Design and configure one policy set each for: anti-phishing, anti-spam, Attack Simulation, Safe Links, and Safe Attachments
- Configure mail flow rules and policies
- Review Zero-hour Auto Purge (ZAP) in Defender for Office
- If required: decommission any configurations performed during the workshop
- Arrange and lead the Threat Check Results and Next Steps session
- Arrange and lead the Project Close-Out session

2.4. Domain 2: Protect your identities and access

2.4.1 Continue In-Scope Activities

- Arrange and lead the Project Kick-Off and Discovery session
- Arrange and lead Workshop sessions covering Microsoft Entra ID
- Review and configure Privileged Identity Management (PIM) for up to 10 users, covering:
 - Just-in-time privileged access to Entra ID and Azure resources
 - Time-bound access to resources using start and end dates
 - Approval requirements to activate privileged roles
 - Enforced multi-factor authentication to activate any role
 - Activation justification, to understand why users activate roles
 - Notifications when privileged roles are activated
 - Access reviews, to confirm users still need their roles
 - Audit history for internal or external audit
 - Prevention of removing the last active Global Administrator and Privileged Role Administrator role assignments
- Review out-of-box reports and insight dashboards
- Review token protection guidance and best practices



- If required: decommission any configurations performed during the workshop
- Arrange and lead the Threat Check Results and Next Steps session
- Arrange and lead the Project Close-Out session

2.5. Customer In-Scope Activities

- Ensure attendance of relevant personnel at the Project Kick-Off session
- Submit all Change Requests and receive required approvals prior to engagement commencement
- Ensure attendance of relevant personnel at the Workshop sessions
- Provide access to Microsoft 365 (Office 365) and Azure production tenants
- Provide remote access and permissions for the Ontinue project team, via a Customer-managed account, PIM-managed identity, or Teams remote screen-sharing
- Provide up to 25 Windows 10/11 workstations to onboard to Defender for Endpoint (must be non-critical workstations)
- Assign the following permissions for Ontinue: Security Administrator and Global Reader; Security Reader and Global Reader assigned during the workshops with a Customer-assigned login
- Provide licenses to support Ontinue activities, or authorization to use trial licenses (minimum Microsoft 365 E5 Security required)
- Arrange or perform any required proxy, firewall, or network changes to support Ontinue activities
- Provision the Defender for Cloud Apps portal, with integration enabled between Defender for Cloud Apps and the Microsoft Defender XDR portal
- Provide all infrastructure needed for any additional roles (as required)
- Support screenshot generation for the Microsoft Proof of Execution
- Complete the Microsoft end-of-engagement Customer questionnaire
- Honor all reasonable requests for information within 1 business day
- Accept full responsibility for all Azure, consumption, and license charges resulting from the engagement
- If required: request decommissioning of any configurations performed during the workshop
- Ensure attendance of relevant personnel at the Threat Check Results and Next Steps session
- Ensure attendance of relevant personnel at the Project Close-Out session

3. Engagement Outputs

Output	Owner	Sign-off Required
Next Steps Recommendation Document	Ontinue	No
Proof of Execution Document (submitted to Microsoft)	Ontinue	No
Customer Questionnaire Completion	Customer	No

4. Assumptions, Dependencies, Constraints

Item	Type
Customer has an active Azure subscription	Assumption
All configuration work must be completed in the Production Tenant, linked to the primary domain	Constraint

Nonstop SecOps

Questions? Let's talk.

European HQ

Grubenstrasse 54, 8045 Zürich,
Switzerland

Düsseldorf Office

Speditionstraße 2, 40221
Düsseldorf, Germany

North America HQ

450 Maple Street, Redwood City,
CA 94063, USA

Vienna Office

Kohlmarkt 8-10, 1010 Wien, Austria

UK Office

9 Holborn, London EC1N 2LL, United
Kingdom

APAC Office

World Trade Tower, Sector 16, Noida
201301, India

Toronto Office

6060-3080 Yonge St, Toronto ON
M4N 3N1, Canada

 Continue

Ontinue

Ontinue Microsoft Defender for Cloud Workshop Package Consulting Services

Version: v1.00

Effective Date: 24.08.2026



Table of Contents

- 1. About Microsoft Defender for Cloud Workshop..... 3
- 2. Engagement Scope..... 3
 - 2.1. Domain Coverage by Package Size..... 3
 - 2.2. Domain 1: Secure your infrastructure..... 3
 - 2.2.1. Continue In-Scope Activities..... 3
 - 2.3. Domain 6: Manage your security posture..... 3
 - 2.3.1. Continue In-Scope Activities..... 3
 - 2.4. Customer In-Scope Activities..... 4
- 3. Engagement Outputs..... 4
- 4. Assumptions, Dependencies, Constraints..... 4



1. About Microsoft Defender for Cloud Workshop

A hands-on pilot of Microsoft Defender for Servers, deployed to up to 5 Windows Servers, so Customer sees it detect and respond to real threats. XS covers Secure your infrastructure; S and M cover Secure your infrastructure and Manage your security posture.

2. Engagement Scope

2.1. Domain Coverage by Package Size

Package Size	Domains Included
XS	Domain 1 (Secure your infrastructure)
S	Domain 1 (Secure your infrastructure) and Domain 6 (Manage your security posture)
M	Domain 1 (Secure your infrastructure) and Domain 6 (Manage your security posture)

2.2. Domain 1: Secure your infrastructure

2.2.1 Continue In-Scope Activities

- Arrange and lead the Project Kick-Off and Discovery session
- Arrange and lead Workshop sessions covering:
 - Microsoft Defender Portal
 - Defender for Servers
 - Microsoft Sentinel and Defender for Cloud integration
 - Microsoft Defender for Cloud Apps
 - Defender for Cloud Compliance Manager
 - Defender for Cloud cost estimation
- If present: review the existing Defender for Servers configuration in Customer's production environment
- If present: review the existing Compliance Manager policies in Customer's production environment
- If present: provide recommendations on Defender for Servers configuration and policies
- Onboard up to 5 Windows Servers into Microsoft Defender for Cloud (2019 and newer)
- Demonstrate the Microsoft Defender for Cloud options available in the Defender portal
- Review the cloud recommendations already available in the Defender portal
- If required: decommission any configurations performed during the workshop
- Arrange and lead the Threat Check Results and Next Steps session
- Arrange and lead the Project Close-Out session

2.3. Domain 6: Manage your security posture

2.3.1 Continue In-Scope Activities

- Arrange and lead the Project Kick-Off and Discovery session
- Arrange and lead Workshop sessions covering:
 - Defender for Cloud Security Posture Management
 - Security Exposure Management
 - Microsoft Defender Portal



- If present: review the existing Cloud Security Posture Management configuration in Customer's production environment
- Review the cloud recommendations already available in the Defender portal
- If required: decommission any configurations performed during the workshop
- Arrange and lead the Threat Check Results and Next Steps session
- Arrange and lead the Project Close-Out session

2.4. Customer In-Scope Activities

- Complete and return the Defend Against Threats Workshop Discovery Questionnaire
- Ensure attendance of relevant personnel at the Project Kick-Off session
- Submit all Change Requests and receive required approvals prior to engagement commencement
- Ensure attendance of relevant personnel at Workshop sessions
- Provide access to Microsoft 365 (Office 365) and Azure production tenants
- Provide remote access and permissions for the Ontinue project team, via a Customer-managed account, PIM-managed identity, or Teams remote screen-sharing
- Assign the following permissions for Ontinue:
 - Security Administrator (PIM role), for the XDR portal
 - Security Administrator (subscription-based RBAC), for Defender for Cloud
 - Global Reader (subscription-based RBAC), for Defender for Cloud
 - Contributor for the Microsoft Sentinel subscription (subscription-based RBAC), for Microsoft Sentinel portal access
- Provide a Microsoft Azure subscription for Sentinel configuration
- Provide licenses to support Ontinue activities
- Enable Defender for Servers Plan 1 for a minimum of 5 Windows servers
- Arrange or perform any required proxy, firewall, or network changes to support Ontinue activities
- Provide all infrastructure needed for any additional roles (as required)
- Support screenshot generation for the Microsoft Proof of Execution
- Complete the Microsoft end-of-engagement Customer questionnaire
- Honor all reasonable requests for information within 1 business day
- Accept full responsibility for all Azure, consumption, and license charges resulting from the engagement
- If required: request decommissioning of any configurations performed during the workshop
- Ensure attendance of relevant personnel at the Threat Check Results and Next Steps session
- Ensure attendance of relevant personnel at the Project Close-Out session

3. Engagement Outputs

Output	Owner	Sign-off Required
Next Steps Recommendation Document	Ontinue	No
Proof of Execution Document (submitted to Microsoft)	Ontinue	No
Customer Questionnaire Completion	Customer	No

4. Assumptions, Dependencies, Constraints

Item	Type
Customer has an active Azure subscription	Assumption



Item	Type
All configuration work must be completed in the Production Tenant, linked to the primary domain	Constraint

Nonstop SecOps

Questions? Let's talk.

European HQ

Grubenstrasse 54, 8045 Zürich,
Switzerland

Düsseldorf Office

Speditionstraße 2, 40221
Düsseldorf, Germany

North America HQ

450 Maple Street, Redwood City,
CA 94063, USA

Vienna Office

Kohlmarkt 8-10, 1010 Wien, Austria

UK Office

9 Holborn, London EC1N 2LL, United
Kingdom

APAC Office

World Trade Tower, Sector 16, Noida
201301, India

Toronto Office

6060-3080 Yonge St, Toronto ON
M4N 3N1, Canada

 Continue

Ontinue

Ontinue Microsoft Sentinel Workshop Package

Consulting Services

Version: v1.00

Effective Date: 24.08.2026



Table of Contents

- 1. About Microsoft Sentinel Workshop..... 3
- 2. Engagement Scope..... 3
 - 2.1. Domain Coverage by Package Size..... 3
 - 2.2. Domain 4: Detect and respond to external attacks..... 3
 - 2.2.1. Continue In-Scope Activities..... 3
 - 2.3. Domain 5: Secure your devices and endpoints..... 4
 - 2.3.1. Continue In-Scope Activities..... 4
 - 2.4. Customer In-Scope Activities..... 4
- 3. Engagement Outputs..... 5
- 4. Assumptions, Dependencies, Constraints..... 5



1. About Microsoft Sentinel Workshop

A hands-on pilot of Microsoft Sentinel, run as collaborative workshops. XS and S cover Detect and respond to external attacks; M covers Detect and respond to external attacks and Secure your devices and endpoints.

2. Engagement Scope

2.1. Domain Coverage by Package Size

Package Size	Domains Included
XS	Domain 4 (Detect and respond to external attacks)
S	Domain 4 (Detect and respond to external attacks)
M	Domain 4 (Detect and respond to external attacks) and Domain 5 (Secure your devices and endpoints)

2.2. Domain 4: Detect and respond to external attacks

2.2.1. Continue In-Scope Activities

- Arrange and lead the Project Kick-Off and Discovery session
- Arrange and lead Workshop sessions covering the activities below
- If present: review the existing Sentinel implementation in Customer's production environment
- Enable Sentinel in Customer's production environment, unless already enabled
- Configure or verify a selection of the following data sources within Microsoft Sentinel:
 - Entra ID
 - Entra ID Protection
 - Microsoft Defender for Endpoint
 - Microsoft Defender for Cloud Apps
 - Microsoft Defender for Office 365
 - Microsoft 365
 - Microsoft Defender XDR
 - Azure Activity
 - Security events via the legacy agent
- Optional: configure the Continue MDR Sentinel Baseline, including:
 - Azure Lighthouse, for data visibility for the Continue team
 - Resource provider registration in the subscription, for MDR onboarding
- Deliver Microsoft Sentinel deep-dive demonstrations covering:
 - Sentinel installation
 - Data connector configuration
 - Using workbooks for data visualization
 - Threat hunting with KQL
 - Incident analysis
 - Automation
- Arrange and lead the Threat Check Results and Next Steps session (Remote)
- Optional: decommission configuration and licenses at the end of the engagement
- Arrange and lead the Project Close-Out session (Remote)



2.3. Domain 5: Secure your devices and endpoints

2.3.1 Continue In-Scope Activities

- Arrange and lead the Project Kick-Off and Discovery session (Remote)
- Arrange and lead Workshop sessions (Remote) covering:
 - Microsoft Defender for Endpoint (Windows workstations)
 - Microsoft Defender for Cloud Apps
- If present: review the existing Defender for Endpoint configuration in Customer's production environment
- If present: review the existing Intune compliance policies in Customer's production environment
- If present: provide recommendations on Intune and Defender for Endpoint configuration and policies
- Configure or verify the following Microsoft Defender XDR configurations:
 - Turn on auditing within the Microsoft 365 Compliance Portal or via PowerShell
 - Configure file monitoring within Defender for Cloud Apps
 - Configure the Office 365 App Connector within Defender for Cloud Apps
 - Enable the malware detection policy in Defender for Cloud Apps
- Onboard up to 25 Windows 10/11 workstations into Microsoft Defender for Endpoint via Intune, if not already onboarded
- Create relevant device groups (if required)
- Configure email notifications (if required)
- Enable the following advanced features: Live Response, Show User Details, Office 365 Threat Intelligence Connection, Defender for Cloud Apps
- Configure role-based access controls (if required)
- Configure device proxy and internet connectivity settings (if required)
- Create a Microsoft Defender Vulnerability Management security baselines assessment
- Deliver Microsoft Security, Microsoft Defender for Endpoint, and Defender for Cloud Apps deep-dive demonstrations
- Generate screenshots from Defender workspaces for the Microsoft Proof of Execution
- If required: decommission any configurations performed during the workshop
- Arrange and lead the Threat Check Results and Next Steps session (Remote)
- Arrange and lead the Project Close-Out session (Remote)

2.4. Customer In-Scope Activities

- Ensure attendance of relevant personnel at the Project Kick-Off session (Remote)
- Submit all Change Requests and receive required approvals prior to engagement commencement
- Ensure attendance of relevant personnel at Workshop sessions (Remote)
- Provide access to Microsoft 365 (Office 365) and Azure production tenants
- Provide remote access and permissions for the Continue project team, via a Customer-managed account or PIM-managed identity
- Assign the following permissions for Continue: Contributor for the Microsoft Sentinel subscription
- Provide licenses to support Continue activities, or authorization to use trial licenses (minimum Microsoft 365 E5 Security required)
- Arrange or perform any required proxy, firewall, or network changes to support Continue activities
- Provide all infrastructure needed for any additional roles (as required)
- Support screenshot generation for the Microsoft Proof of Execution
- Complete the Microsoft end-of-engagement Customer questionnaire



- Honor all reasonable requests for information within 1 business day
- Accept full responsibility for all Azure, consumption, and license charges resulting from the engagement
- Ensure attendance of relevant personnel at the Threat Check Results and Next Steps session (Remote)
- Ensure attendance of relevant personnel at the Project Close-Out session (Remote)

3. Engagement Outputs

Output	Owner	Sign-off Required
Next Steps Recommendation Document	Ontinue	No
Proof of Execution Document (submitted to Microsoft)	Ontinue	No
Customer Questionnaire Completion	Customer	No

4. Assumptions, Dependencies, Constraints

Item	Type
Customer has an active Azure subscription	Assumption
All configuration work must be completed in the Production Tenant, linked to the primary domain	Constraint

Nonstop SecOps

Questions? Let's talk.

European HQ

Grubenstrasse 54, 8045 Zürich,
Switzerland

Düsseldorf Office

Speditionstraße 2, 40221
Düsseldorf, Germany

North America HQ

450 Maple Street, Redwood City,
CA 94063, USA

Vienna Office

Kohlmarkt 8-10, 1010 Wien, Austria

UK Office

9 Holborn, London EC1N 2LL, United
Kingdom

APAC Office

World Trade Tower, Sector 16, Noida
201301, India

Toronto Office

6060-3080 Yonge St, Toronto ON
M4N 3N1, Canada

 Continue

Ontinue

Ontinue Microsoft Data Security Workshop Package Consulting Services

Version: v1.00

Effective Date: 24.08.2026



Table of Contents

- 1. About Microsoft Data Security Workshop.....3
- 2. Engagement Scope.....3
 - 2.1. Domain Coverage by Package Size.....3
 - 2.2. Domain 7: Protect your data.....3
 - 2.2.1. Continue In-Scope Activities.....3
 - 2.3. Domain 5: Secure your devices and endpoints.....4
 - 2.3.1. Continue In-Scope Activities.....4
 - 2.4. Domain 8: Secure AI.....5
 - 2.4.1. Continue In-Scope Activities.....5
 - 2.5. Customer In-Scope Activities.....5
- 3. Engagement Outputs.....6
- 4. Assumptions, Dependencies, Constraints.....6



1. About Microsoft Data Security Workshop

A hands-on pilot of Microsoft Purview, demonstrating how it discovers, monitors, and protects sensitive data. XS and S cover Protect your data; M covers Secure your devices and endpoints, Protect your data, and Secure AI.

2. Engagement Scope

2.1. Domain Coverage by Package Size

Package Size	Domains Included
XS	Domain 7 (Protect your data)
S	Domain 7 (Protect your data)
M	Domain 5 (Secure your devices and endpoints), Domain 7 (Protect your data), and Domain 8 (Secure AI)

2.2. Domain 7: Protect your data

2.2.1 Continue In-Scope Activities

- Arrange and lead the Project Kick-Off session
- Arrange and lead the Discovery session, covering:
 - A walkthrough of the Microsoft Purview Portal
 - Understanding Customer's data protection requirements
 - Defining the search criteria for Automated Discovery
 - Defining Sensitive Info Types
 - Defining Sensitivity Labels
 - Defining Data Loss Prevention policies
 - Defining the Insider Risk Management policy
 - Assigning Data Security Check team members to appropriate roles
- Configure up to 2 Sensitive Info Types
- Create up to 5 Sensitivity Labels
- Configure and verify that audit logging is enabled within the Microsoft Purview Portal
- **Exchange configuration:**
 - Create a content search for Automated Discovery to identify stale data in Exchange Online
 - Create a content search for Automated Discovery to identify specific keywords in data stored in Exchange Online
 - Configure Automated Discovery to search for Sensitive Info Types
 - Create up to 3 additional content searches, as per Customer requirements
- **SharePoint Online:**
 - Create a content search for Automated Discovery to identify stale data in SharePoint Online
 - Create a content search for Automated Discovery to identify credit card numbers in data stored in SharePoint Online
 - Create a content search for Automated Discovery to identify specific keywords in data stored in the Microsoft 365 tenant
 - Create a content search for Automated Discovery to identify Sensitive Info Types
 - Create up to 3 additional content searches, as per Customer requirements
- **Teams:**



- Create a Data Loss Prevention policy for Data Loss Prevention for Teams, to search for Sensitive Info Types
- Create up to 2 additional Data Loss Prevention policies, as per Customer requirements
- **Insider Risk:**
 - Enable and run Insider Risk Analytics
 - Create an Insider Risk Management policy based on users performing exfiltration activities that exceed defined thresholds
 - Create an Insider Risk Management policy that triggers on Data Loss Prevention policy matches
 - Create up to 2 additional Insider Risk Management policies, as per Customer requirements
- Turn on Windows device monitoring
- Configure Automated Discovery to search for out-of-box Sensitive Info Types
- Configure Automated Discovery to search for Sensitive Info Types
- Arrange and lead the Project Close-Out session

2.3. Domain 5: Secure your devices and endpoints

2.3.1 Continue In-Scope Activities

- Arrange and lead the Project Kick-Off and Discovery session
- Arrange and lead Workshop sessions covering:
 - Microsoft Defender for Endpoint (Windows workstations)
 - Microsoft Defender for Cloud Apps
- If present: review the existing Defender for Endpoint configuration in Customer's production environment
- If present: review the existing Intune compliance policies in Customer's production environment
- If present: provide recommendations on Intune and Defender for Endpoint configuration and policies
- Configure or verify the following Microsoft Defender XDR configurations:
 - Turn on auditing within the Microsoft 365 Compliance Portal or via PowerShell
 - Configure file monitoring within Defender for Cloud Apps
 - Configure the Office 365 App Connector within Defender for Cloud Apps
 - Enable the malware detection policy in Defender for Cloud Apps
- Onboard up to 25 Windows 10/11 workstations into Microsoft Defender for Endpoint via Intune, if not already onboarded
- Create relevant device groups (if required)
- Configure email notifications (if required)
- Enable the following advanced features: Live Response, Show User Details, Office 365 Threat Intelligence Connection, Defender for Cloud Apps
- Configure role-based access controls (if required)
- Configure device proxy and internet connectivity settings (if required)
- Create a Microsoft Defender Vulnerability Management security baselines assessment
- Deliver Microsoft Security, Microsoft Defender for Endpoint, and Defender for Cloud Apps deep-dive demonstrations
- Generate screenshots from Defender workspaces for the Microsoft Proof of Execution
- If required: decommission any configurations performed during the workshop
- Arrange and lead the Threat Check Results and Next Steps session
- Arrange and lead the Project Close-Out session



2.4. Domain 8: Secure AI

2.4.1 Ontinue In-Scope Activities

- Arrange and lead the Project Kick-Off and Discovery session
- Arrange and lead Workshop sessions covering Microsoft Agent 365
- Review how Agent 365 enables controls across:
 - Microsoft Entra ID
 - Microsoft Defender
 - Microsoft Purview
 - Microsoft Intune
- Review Current Agents in Customer Tenant
- Review user permission for creating agents
- Create one Agent 365 Blueprint template
- Create up to 1 Agent Instance
- Setup up to 1 Managed Tool Set
- Configure up to 2 existing AI agents with controls in Agent 365
- Verify:
 - Existing behavior
 - Identity
 - Observability
 - Tooling
 - Notifications
 - Configuration
 - Confirm deployment readiness
- If required: decommission any configurations performed during the workshop
- Arrange and lead the Project Close-Out session

2.5. Customer In-Scope Activities

- Complete and return the Data Protection Engagement Questionnaire
- Ensure attendance of relevant personnel at the Project Kick-Off session
- Ensure attendance of relevant personnel at the Discovery session
- Submit all Change Requests and receive required approvals prior to engagement commencement
- Provide access to Microsoft 365 (Office 365) and Azure production tenants
- Provide remote access and permissions for the Ontinue project team, via a Customer-managed account or PIM-managed identity
- Assign the following permissions for Ontinue: Compliance Administrator and Global Reader. Additional roles may be required and will be defined with justification
- Provide or facilitate access to additional toolsets for Ontinue. Additional toolsets may be required and will be defined with justification
- Provide licenses to support Ontinue activities, or authorization to use trial licenses (minimum Microsoft 365 E5 Compliance required)
- Arrange or perform any required proxy, firewall, or network changes to support Ontinue activities
- Provide all infrastructure needed for any additional roles (as required)
- Honor all reasonable requests for information within 1 business day
- Complete the Microsoft end-of-engagement Customer questionnaire
- Accept full responsibility for all Azure, consumption, and license charges resulting from the engagement



- Ensure attendance of relevant personnel at Purview working sessions with Infrastructure and Data teams
- Ensure attendance of relevant personnel at the Next Steps session
- Ensure attendance of relevant personnel at the Project Close-Out session

3. Engagement Outputs

Output	Owner	Sign-off Required
Next Steps Recommendation Document	Ontinue	No
Proof of Execution Document (submitted to Microsoft)	Ontinue	No
Customer Questionnaire Completion	Customer	No

4. Assumptions, Dependencies, Constraints

Item	Type
Customer has an active Azure subscription	Assumption
All configuration work must be completed in the Production Tenant, linked to the primary domain	Constraint

Nonstop SecOps

Questions? Let's talk.

European HQ

Grubenstrasse 54, 8045 Zürich,
Switzerland

Düsseldorf Office

Speditionstraße 2, 40221
Düsseldorf, Germany

North America HQ

450 Maple Street, Redwood City,
CA 94063, USA

Vienna Office

Kohlmarkt 8-10, 1010 Wien, Austria

UK Office

9 Holborn, London EC1N 2LL, United
Kingdom

APAC Office

World Trade Tower, Sector 16, Noida
201301, India

Toronto Office

6060-3080 Yonge St, Toronto ON
M4N 3N1, Canada

 **Continue**

Ontinue

Ontinue Microsoft XDR Deployment Package Consulting Services

Version: v1.00

Effective Date: 24.08.2026



Table of Contents

- 1. About Microsoft XDR Deployment..... 3
- 2. Engagement Scope..... 3
 - 2.1. Ontinue In-Scope Activities..... 3
 - 2.2. Customer In-Scope Activities..... 3
- 3. Engagement Outputs..... 4
- 4. Assumptions, Dependencies, Constraints..... 4



1. About Microsoft XDR Deployment

Ontinue deploys Defender protection across up to 10,000 workstations and servers (Mac, Linux, and Windows), including Defender for Identity and a basic Intune setup for Defender for Endpoint deployments.

2. Engagement Scope

2.1. Ontinue In-Scope Activities

- Arrange and lead 1 x 2hr Microsoft Defender for Endpoint overview session, presenting the advanced deployment guide and the areas of assistance covered below
- Arrange and lead 5 x 2hr Microsoft Defender for Endpoint deployment workshops
- Import and analyse existing Group Policy configurations, and provide a recommended approach
- Identify and configure up to 4 Conditional Access policies for Windows user devices
- Configure best practice policies for Microsoft Defender for Endpoint in the initial deployment stage:
 - ASR rules (up to 4)
 - AV policies (up to 2)
 - BitLocker
- Configure Conditional Access policies to drive preferred client and user behaviour during the initial deployment stage
- Onboard up to 25 Windows 10/11 devices in the initial deployment stage
- Onboard up to 250 Windows 10/11 devices in the full rollout
- Assist with enablement and installation of Microsoft Defender for Endpoint:
 - Up to 250 Windows endpoints (Intune)
- Review Customer-deployed policies for servers:
 - Up to 25 Windows servers (Microsoft Defender for Cloud Servers)
 - Up to 25 Windows VDI instances (Microsoft Defender for Cloud Servers)
- Manage rollout, for a maximum of 8hrs per week over a maximum of 2 weeks; additional onboarding hours available via Change Request
- Assist Customer in troubleshooting device onboarding to Defender for Endpoint, for a maximum of 8hrs; additional troubleshooting hours available via Change Request
- Assist Customer in the removal of their current endpoint protection solution
- Install Microsoft Defender for Identity on up to 5 servers

2.2. Customer In-Scope Activities

- Ensure attendance of relevant personnel at the 1 x 2hr Microsoft Defender for Endpoint overview session
- Ensure attendance of relevant personnel at the 5 x 2hr Defender for Endpoint deployment workshops
- Provide a list of in-scope workstations and servers, including for each: name, OS version, location (Azure, AWS, GCP, or on-premises), server role, server criticality, and device management method (GPO, Azure Arc, Ansible, etc.)
- Provide remote access and permissions for the Ontinue project team, via a Customer-managed account or PIM-managed identity
- Assign the following permissions for Ontinue: Security Administrator, Intune Administrator, and Global Reader. Additional roles may be required and will be defined with justification



- Provide or facilitate access to additional toolsets for Ontinue as required. Additional toolsets may be required and will be defined with justification
- Provide licenses to support Ontinue activities: Defender for Servers P1 as a minimum
- Submit all Change Requests and receive required approvals prior to engagement commencement
- Arrange or perform any required proxy, firewall, or network changes to support Ontinue activities
- Collaborate with Ontinue on the high level project plan
- Honor all reasonable requests for information within 1 business day
- Accept full responsibility for all Azure, consumption, and license charges resulting from the engagement
- Prepare and provide Ontinue with access to all in-scope servers
- Prepare Microsoft Defender for Cloud Servers policies via Intune
- Schedule the removal of the current endpoint protection solution from target endpoints to coincide with Defender for Endpoint onboarding. Defender for Endpoint will run in passive mode during any period where both the current solution and Defender for Endpoint are in place
- Collaborate with Ontinue on Microsoft Defender for Cloud Servers policy issues, in both the initial deployment stage and the full rollout
- Conduct testing of onboarded endpoints within 1 week of deployment

3. Engagement Outputs

Output	Owner	Sign-off Required
Deployment Design Document	Ontinue	No

4. Assumptions, Dependencies, Constraints

Item	Type
Customer has an active Azure subscription	Assumption
All configuration work must be completed in the Production Tenant, linked to the primary domain	Constraint

Nonstop SecOps

Questions? Let's talk.

European HQ

Grubenstrasse 54, 8045 Zürich,
Switzerland

Düsseldorf Office

Speditionstraße 2, 40221
Düsseldorf, Germany

North America HQ

450 Maple Street, Redwood City,
CA 94063, USA

Vienna Office

Kohlmarkt 8-10, 1010 Wien, Austria

UK Office

9 Holborn, London EC1N 2LL, United
Kingdom

APAC Office

World Trade Tower, Sector 16, Noida
201301, India

Toronto Office

6060-3080 Yonge St, Toronto ON
M4N 3N1, Canada

 Continue

Ontinue

Ontinue AI Security Deployment Package Consulting Services

Version: v1.00

Effective Date: 24.08.2026



Table of Contents

- 1. About AI Security Deployment..... 3
- 2. Engagement Scope..... 3
 - 2.1. Continue In-Scope Activities, Assessment..... 3
 - 2.2. Continue In-Scope Activities, Data Protection Readiness..... 3
 - 2.3. Continue In-Scope Activities, Posture Review..... 3
 - 2.4. Continue In-Scope Activities, Security Copilot..... 4
 - 2.5. Continue In-Scope Activities Agent 365 Enablement..... 4
 - 2.6. Customer In-Scope Activities..... 4
- 3. Engagement Outputs..... 5
- 4. Assumptions, Dependencies, Constraints..... 5



1. About AI Security Deployment

A consulting engagement that prepares Customer's environment for secure enterprise AI adoption. Ontinue evaluates Customer's current Microsoft Purview configuration to prevent data oversharing and protect sensitive content as AI tools query the environment, then optimizes Microsoft Security Copilot enablement and deploys Agent 365 governance controls, establishing a configured control plane for Customer's AI agents and data estate.

2. Engagement Scope

2.1. Ontinue In-Scope Activities, Assessment

- Arrange and lead up to 1 x 1hr Project Kick-Off and Discovery session
- Discuss organizational readiness and objectives, up to 2 x 2hr sessions, covering:
 - Business goals and priorities
 - Current gaps
 - Desired future state
 - Goals for usage
 - Industry and regulatory landscape
 - ROI requirements
- Review Microsoft Security Copilot features and gaps, 1 x 2hr session, covering:
 - Current capabilities
 - Missing requirements, based on the readiness and objectives discussions
 - Cost, based on the proposed level of usage
- Complete a Tenant Security Review of the Microsoft security tools in use within Customer's E5 Defender suite. The review is performed offline, up to 5hrs, and covers:
 - Microsoft Defender for Endpoint
 - Intune
 - Microsoft Defender for Identity
 - Microsoft Defender for Office 365
 - Microsoft Defender for Cloud Apps
 - Microsoft Defender for Cloud
 - Entra ID
- Review the Tenant Security Review findings with Customer, 1 x 1hr session, covering:
 - The top five issues found
 - Gaps in the current configuration
 - Readiness to deploy Microsoft Security Copilot

2.2. Ontinue In-Scope Activities, Data Protection Readiness

- Review and discuss Microsoft Defender Vulnerability Management add-on licenses (optional)
- Produce a Purview C.A.M.P. report (optional)
- Compliance Manager: complete up to 1 framework step and create the corresponding report

2.3. Ontinue In-Scope Activities, Posture Review

- Review Security Exposure Management
- Security Exposure Management: connect third party connections, where available (optional)
- Cloud Security Posture Management: review Foundation versus Full
- Cloud Security Posture Management: review cost for full adoption



- Review Sentinel logs

2.4. Continue In-Scope Activities, Security Copilot

- Review Security Copilot Compute Unit (SCU) requirements, including the timeline of SCU usage for Security Copilot
- Enable Security Copilot, including:
 - SCU configuration
 - Microsoft Agent Store review
 - Continue agent enablement
 - Phrase commands, up to 5 examples with a readout

2.5. Continue In-Scope Activities Agent 365 Enablement

- Review how Agent 365 enables controls across:
 - Microsoft Entra ID
 - Microsoft Defender
 - Microsoft Purview
 - Microsoft Intune
- Review Current Agents in Customer Tenant
- Review user permission for creating agents
- Create one Agent 365 Blueprint template
- Create up to 1 Agent Instance
- Setup up to 1 Managed Tool Set
- Configure up to 2 existing AI agents with controls in Agent 365
- Verify:
 - Existing behavior
 - Identity
 - Observability
 - Tooling
 - Notifications
 - Configuration
 - Confirm deployment readiness
- Arrange and lead the Project Close-Out session

2.6. Customer In-Scope Activities

- Attend up to 1 x 1hr Project Kick-Off and Discovery session
- Complete the Continue Security Posture Questionnaire
- Assign the following permissions for Continue: Security Administrator, Compliance Administrator, Global Reader, Intune Administrator, and Reader on Azure subscriptions
- Provide licenses to support Continue activities, or authorization to use trial licenses (minimum Microsoft 365 E5 Security required)
- Arrange or perform any required proxy, firewall, or network changes to support Continue activities
- Provide all infrastructure needed for any additional roles (as required)
- Support screenshot generation for the report
- Honor all reasonable requests for information within 1 business day
- Accept full responsibility for all Azure, consumption, and license charges resulting from the engagement
- Ensure attendance of relevant personnel at the Project Close-Out session



3. Engagement Outputs

Output	Owner	Sign-off Required
Next Steps Recommendation Document	Ontinue	No
Proof of Execution Document (submitted to Microsoft)	Ontinue	No
Customer Questionnaire Completion	Customer	No

4. Assumptions, Dependencies, Constraints

Item	Type
Customer has an active Azure subscription	Assumption
All configuration work must be completed in the Production Tenant, linked to the primary domain	Constraint

Nonstop SecOps

Questions? Let's talk.

European HQ

Grubenstrasse 54, 8045 Zürich,
Switzerland

Düsseldorf Office

Speditionstraße 2, 40221
Düsseldorf, Germany

North America HQ

450 Maple Street, Redwood City,
CA 94063, USA

Vienna Office

Kohlmarkt 8-10, 1010 Wien, Austria

UK Office

9 Holborn, London EC1N 2LL, United
Kingdom

APAC Office

World Trade Tower, Sector 16, Noida
201301, India

Toronto Office

6060-3080 Yonge St, Toronto ON
M4N 3N1, Canada

 Continue

Ontinue

Ontinue Microsoft Purview Deployment Package Consulting Services

Version: v1.00

Effective Date: 24.08.2026



Table of Contents

- 1. About Microsoft Purview Deployment.....3
- 2. Engagement Scope..... 3
 - 2.1. Continue In-Scope Activities, Microsoft Purview..... 3
 - 2.2. Continue In-Scope Activities, Defender for Cloud Apps..... 3
 - 2.3. Customer In-Scope Activities..... 3
- 3. Engagement Outputs.....4
- 4. Assumptions, Dependencies, Constraints..... 4



1. About Microsoft Purview Deployment

Ontinue deploys Purview end-to-end: DLP, Sensitivity Labels, Classifiers, and Insider Risk, plus a baseline report of the environment.

2. Engagement Scope

2.1. Ontinue In-Scope Activities, Microsoft Purview

- Arrange and lead the Discovery session (Remote), including a walkthrough of the Microsoft Purview Portal and understanding Customer's data protection requirements
- Onboard up to 5 test Windows 10/11 devices for endpoint DLP
- Provision up to 5 Sensitivity Labels and up to 2 label policies
- Configure the deployment template
- Implement 1 of up to 4 Endpoint DLP policies
- Show and tell up to 4 on-premises DLP policies
- Deploy and configure 1 MIP Scanner and Microsoft SQL Server Express instance (required)
- Enable email encryption for test users, including encryption based on 1 content type
- Enable reporting and automatic classification for up to 3 pre-production file folders, to avoid user impact
- Demonstrate end-to-end functionality

2.2. Ontinue In-Scope Activities, Defender for Cloud Apps

- Arrange and lead the Discovery session (Remote): show and tell to level-set the team, understand the current cloud app estate, review any existing MDCA/CASB configuration, and designate up to 50 sanctioned apps
- Review and propose changes to the existing MDCA implementation
- Guide the deployment of up to 4 native API integrations
- Configure up to 5 Conditional Access App Control rules for featured apps
- Configure up to 50 sanctioned and unsanctioned apps
- Configure up to 5 File MDCA policies and up to 10 MDCA policies
- Guide the configuration of IP locations

2.3. Customer In-Scope Activities

- Ensure attendance of relevant personnel at the Discovery sessions (Remote)
- Submit all Change Requests and receive required approvals prior to engagement commencement
- Provide access to the Microsoft 365 (Office 365) production tenant
- Provide remote access and permissions for the Ontinue project team, via a Customer-managed account or PIM-managed identity
- Assign the following permissions for Ontinue: Compliance Administrator, Content List Viewer, Security Administrator, and Global Reader
- Provide licenses to support Ontinue activities (minimum Microsoft 365 E5 Compliance required)
- Deploy and configure 1 Windows Server 2016 or newer
- Deploy and configure 1 Microsoft SQL Server Express instance
- Perform any software changes or configurations required for API integrations
- Arrange or perform any required proxy, firewall, or network changes to support Ontinue activities
- Honor all reasonable requests for information within 1 business day



- Accept full responsibility for all Azure, consumption, and license charges resulting from the engagement

3. Engagement Outputs

Output	Owner	Sign-off Required
Microsoft Purview Design Document	Ontinue	No

4. Assumptions, Dependencies, Constraints

Item	Type
Customer has an active Azure subscription	Assumption
All configuration work must be completed in the Production Tenant, linked to the primary domain	Constraint

Nonstop SecOps

Questions? Let's talk.

European HQ

Grubenstrasse 54, 8045 Zürich,
Switzerland

Düsseldorf Office

Speditionstraße 2, 40221
Düsseldorf, Germany

North America HQ

450 Maple Street, Redwood City,
CA 94063, USA

Vienna Office

Kohlmarkt 8-10, 1010 Wien, Austria

UK Office

9 Holborn, London EC1N 2LL, United
Kingdom

APAC Office

World Trade Tower, Sector 16, Noida
201301, India

Toronto Office

6060-3080 Yonge St, Toronto ON
M4N 3N1, Canada

 **Continue**

Ontinue

Ontinue Microsoft Entra ID Deployment Package Consulting Services

Version: v1.00

Effective Date: 24.09.2026



Table of Contents

- 1. About Microsoft Entra ID Deployment..... 3
- 2. Engagement Scope..... 3
 - 2.1. Continue In-Scope Activities..... 3
 - 2.2. Customer In-Scope Activities..... 3
- 3. Engagement Outputs..... 4
- 4. Assumptions, Dependencies, Constraints..... 4



1. About Microsoft Entra ID Deployment

Ontinue deploys the Entra ID P2 identity protection capabilities: Privileged Identity Management, Privileged Access Management, risk-based Conditional Access, and alerting and reporting.

2. Engagement Scope

2.1. Ontinue In-Scope Activities

- Arrange and lead the Project Kick-Off and Discovery session, covering:
 - A show and tell to level-set the team
 - A review of the current multi-factor authentication deployment
 - A review of Conditional Access based on group, location, or device status
- Arrange and lead deployment workshops covering the activities below
- Configure the integration with Microsoft Defender for Cloud Apps
- Review and configure Privileged Identity Management (PIM) for up to 10 users, covering:
 - Just-in-time privileged access to Entra ID and Azure resources
 - Time-bound access to resources using start and end dates
 - Approval requirements to activate privileged roles
 - Enforced multi-factor authentication to activate any role
 - Activation justification, to understand why users activate roles
 - Notifications when privileged roles are activated
 - Access reviews, to confirm users still need their roles
 - Audit history for internal or external audit
 - Prevention of removing the last active Global Administrator and Privileged Role Administrator role assignments
- Configure Privileged Access Management (PAM) for up to 10 users
- Create risk-based Conditional Access policies within Entra ID Protection
- Configure alerts and reporting within the Entra ID P2 license set
- Review out-of-box reports and insight dashboards
- Review token protection guidance and best practices
- Arrange and lead the Project Close-Out session

2.2. Customer In-Scope Activities

- Ensure attendance of relevant personnel at the Project Kick-Off session
- Submit all Change Requests and receive required approvals prior to engagement commencement
- Ensure attendance of relevant personnel at the deployment workshops
- Provide access to the Microsoft 365 (Office 365) production tenant
- Provide remote access and permissions for the Ontinue project team, via a Customer-managed account or PIM-managed identity
- Assign the following permissions for Ontinue: Security Administrator, Privileged Role Administrator, and Global Reader
- Provide licenses to support Ontinue activities (minimum Entra ID P2 required for all users in scope)
- Arrange or perform any required proxy, firewall, or network changes to support Ontinue activities
- Maintain at least 2 emergency access accounts, excluded from the Conditional Access policies created during the engagement
- Honor all reasonable requests for information within 1 business day



- Accept full responsibility for all Azure, consumption, and license charges resulting from the engagement
- Ensure attendance of relevant personnel at the Project Close-Out session

3. Engagement Outputs

Output	Owner	Sign-off Required
Design document updated with Microsoft Entra ID P2	Ontinue	No

4. Assumptions, Dependencies, Constraints

Item	Type
Customer has an active Azure subscription	Assumption
All configuration work must be completed in the Production Tenant, linked to the primary domain	Constraint

Nonstop SecOps

Questions? Let's talk.

European HQ

Grubenstrasse 54, 8045 Zürich,
Switzerland

Düsseldorf Office

Speditionstraße 2, 40221
Düsseldorf, Germany

North America HQ

450 Maple Street, Redwood City,
CA 94063, USA

Vienna Office

Kohlmarkt 8-10, 1010 Wien, Austria

UK Office

9 Holborn, London EC1N 2LL, United
Kingdom

APAC Office

World Trade Tower, Sector 16, Noida
201301, India

Toronto Office

6060-3080 Yonge St, Toronto ON
M4N 3N1, Canada

 Continue

Ontinue

Ontinue Microsoft iSOC Deployment Package Consulting Services

Version: v1.00

Effective Date: 24.09.2026



Table of Contents

- 1. About Microsoft iSOC Deployment..... 3
- 2. Engagement Scope..... 3
 - 2.1. Ontinue In-Scope Activities..... 3
 - 2.2. Customer In-Scope Activities..... 3
- 3. Engagement Outputs..... 4
- 4. Assumptions, Dependencies, Constraints..... 4



1. About Microsoft iSOC Deployment

Ontinue deploys Microsoft iSOC: Microsoft Sentinel and Microsoft Defender XDR integrated into the unified Microsoft Defender portal, with Security Copilot and automated investigation enabled.

2. Engagement Scope

2.1. Ontinue In-Scope Activities

- Arrange and lead the Project Kick-Off and Discovery session
- Arrange and lead enablement sessions covering the activities below
- Review the existing Microsoft Sentinel implementation in the Customer's production environment, where present
- Enable the unified Microsoft Defender portal and platform ingestion
- Deploy Microsoft Defender for Endpoint on up to 25 devices
- Deploy Microsoft Defender for Servers on up to 5 servers (Optional)
- Deploy Microsoft Defender for Identity on up to 1 domain controller (Optional)
- Enable up to 2 Shadow IT policies in Microsoft Defender for Cloud Apps (Optional)
- Configure or verify a selection of the following telemetry sources within Microsoft iSOC:
 - Microsoft Entra ID
 - Microsoft Entra ID Protection
 - Microsoft Defender for Endpoint
 - Microsoft Defender for Cloud Apps
 - Microsoft Defender for Office 365
 - Microsoft 365
 - Microsoft Defender XDR
 - Azure Activity
 - Windows Security Events via the Azure Monitor Agent (AMA)
- Review and create device groups in the Microsoft Defender portal (Optional)
- Configure Microsoft Defender XDR Unified role-based access control (RBAC):
 - Create Microsoft Entra ID security groups for each iSOC access level
 - Assign the appropriate permissions to the iSOC groups
 - Enforce Privileged Identity Management (PIM) for elevated iSOC groups
 - Create and deploy a dual-layer, group-based permission model for Security Copilot access
- Enable AI and automated response (Security Copilot and automated investigation and response)
- Deliver Microsoft iSOC deep-dive demonstrations covering:
 - Automated investigation and response
- Validate telemetry and SOC operations workflows
- Arrange and lead the Threat Check Results and Next Steps session
- Arrange and lead the Project Close-Out session

2.2. Customer In-Scope Activities

- Ensure attendance of relevant personnel at the Project Kick-Off and Discovery session
- Submit all Change Requests and receive required approvals prior to engagement commencement
- Ensure attendance of relevant personnel at the enablement sessions
- Provide access to the Microsoft 365 (Office 365) and Azure production tenants
- Provide remote access and permissions for the Ontinue project team, via a Customer-managed account or PIM-managed identity



- Assign the following permissions for Ontinue: Contributor on the Microsoft Sentinel subscription, and Security Administrator
- Provide licenses to support Ontinue activities, or authorization to use trial licenses (minimum Microsoft 365 E5, or Microsoft 365 E3 with the Microsoft 365 E5 Security add-on)
- Provide Security Copilot capacity (included entitlement or provisioned Security Compute Units)
- Arrange or perform any required proxy, firewall, or network changes to support Ontinue activities
- Provide all infrastructure needed for any additional roles, as required
- Complete the Microsoft end-of-engagement Customer questionnaire
- Honor all reasonable requests for information within 1 business day
- Accept full responsibility for all Azure consumption and license charges resulting from the engagement, including Microsoft Sentinel ingestion, Microsoft Defender for Servers, and Security Copilot capacity
- Ensure attendance of relevant personnel at the Threat Check Results and Next Steps session
- Ensure attendance of relevant personnel at the Project Close-Out session

3. Engagement Outputs

Output	Owner	Sign-off Required
Next Steps Recommendation Document	Ontinue	No

4. Assumptions, Dependencies, Constraints

Item	Type
Customer has an active Azure subscription	Assumption
Customer must have minimum of M365 E5 licenses	Assumption
All configuration work must be completed in the Production Tenant, linked to the primary domain	Constraint

Nonstop SecOps

Questions? Let's talk.

European HQ

Grubenstrasse 54, 8045 Zürich,
Switzerland

Düsseldorf Office

Speditionstraße 2, 40221
Düsseldorf, Germany

North America HQ

450 Maple Street, Redwood City,
CA 94063, USA

Vienna Office

Kohlmarkt 8-10, 1010 Wien, Austria

UK Office

9 Holborn, London EC1N 2LL, United
Kingdom

APAC Office

World Trade Tower, Sector 16, Noida
201301, India

Toronto Office

6060-3080 Yonge St, Toronto ON
M4N 3N1, Canada

 **Continue**

Ontinue

Ontinue Microsoft Defender for Office 365 Readiness Package Consulting Services

Version: v1.00

Effective Date: 24.08.2026



Table of Contents

- 1. About Microsoft Defender for Office 365 Readiness.....3
- 2. Engagement Scope..... 3
 - 2.1. Continue In-Scope Activities.....3
 - 2.2. Customer In-Scope Activities..... 3
- 3. Engagement Outputs.....4
- 4. Assumptions, Dependencies, Constraints..... 4



1. About Microsoft Defender for Office 365 Readiness

Ontinue brings Customer's Defender for Office 365 setup in line with Ontinue best practices and completes all required Ontinue SPI tasks, ensuring the ION for EPP service add-on can be onboarded.

2. Engagement Scope

2.1. Ontinue In-Scope Activities

- Arrange and lead the Project Kick-Off and Discovery session
- Arrange and lead 4 x 2hr Microsoft Defender for Office workshops
- Review the current email security console and policy sets, covering:
 - Mail flow reports
 - Priority user identification
 - Custom filtering rules
- Catalog allow and block lists to migrate to Defender for Office
- Review Exchange Online mail flow rules
- Review Exchange Online mail flow connectors
- Review Exchange Online Protection settings
- Design and configure one policy set each for:
 - Anti-phishing
 - Anti-spam
 - Attack Simulation
 - Safe Links
 - Safe Attachments
- Configure mail flow rules and policies
- Review Zero-hour Auto Purge (ZAP) in Defender for Office
- Deliver a 1 x 2hr knowledge transfer session to level-set the team
- Arrange and lead the Project Close-Out session

2.2. Customer In-Scope Activities

- Ensure attendance of relevant personnel at the Project Kick-Off session
- Submit all Change Requests and receive required approvals prior to engagement commencement
- Provide access to the Microsoft 365 (Office 365) production tenant
- Provide remote access and permissions for the Ontinue project team, via a Customer-managed account or PIM-managed identity
- Assign the following permissions for Ontinue: Security Administrator and Exchange Administrator
- Provide licenses to support Ontinue activities (minimum Microsoft Defender for Office P2 required)
- Arrange or perform any required proxy, firewall, or network changes to support Ontinue activities
- Update MX records, SPF, DMARC, and DKIM to reflect the requirements for Defender for Office, and perform any other DNS changes as required
- Honor all reasonable requests for information within 1 business day
- Accept full responsibility for all Azure, consumption, and license charges resulting from the engagement
- Ensure attendance of relevant personnel at the Project Close-Out session



3. Engagement Outputs

Output	Owner	Sign-off Required
Microsoft Defender for Office Design Document	Ontinue	No

4. Assumptions, Dependencies, Constraints

Item	Type
Customer has an active Azure subscription	Assumption
All configuration work must be completed in the Production Tenant, linked to the primary domain	Constraint

Nonstop SecOps

Questions? Let's talk.

European HQ

Grubenstrasse 54, 8045 Zürich,
Switzerland

Düsseldorf Office

Speditionstraße 2, 40221
Düsseldorf, Germany

North America HQ

450 Maple Street, Redwood City,
CA 94063, USA

Vienna Office

Kohlmarkt 8-10, 1010 Wien, Austria

UK Office

9 Holborn, London EC1N 2LL, United
Kingdom

APAC Office

World Trade Tower, Sector 16, Noida
201301, India

Toronto Office

6060-3080 Yonge St, Toronto ON
M4N 3N1, Canada

 **Continue**



Ontinue

Microsoft Purview

Readiness Package

Consulting Services

Version: v1.00

Effective Date: 24.08.2026



Table of Contents

- 1. About Microsoft Purview Readiness..... 3
- 2. Engagement Scope..... 3
 - 2.1. Continue In-Scope Activities, Microsoft Purview..... 3
 - 2.2. Continue In-Scope Activities, Defender for Cloud Apps..... 3
 - 2.3. Customer In-Scope Activities..... 3
- 3. Engagement Outputs..... 4
- 4. Assumptions, Dependencies, Constraints..... 4



1. About Microsoft Purview Readiness

Ontinue brings Customer's Purview setup in line with Ontinue best practices and completes DLP and IRM configuration tasks, ensuring the ION for DSM service add-on can be onboarded.

2. Engagement Scope

2.1. Ontinue In-Scope Activities, Microsoft Purview

- Arrange and lead the Discovery session, including a walkthrough of the Microsoft Purview Portal and understanding Customer's data protection requirements
- Run the C.A.M.P. report in Customer's tenant and review the results
- Co-develop a deployment process and project plan with Customer
- Help create an overall data security governance plan for Customer, covering both structured and unstructured data
- Onboard up to 5 test Windows 10/11 devices for endpoint DLP
- Provision up to 5 Sensitivity Labels, based on Ontinue best practice, and up to 2 label policies
- Perform data discovery based on current usage per department
- Communicate any data security changes to the broader business
- Edit or create Microsoft Defender for Endpoint policies as needed, and test all hardened policies before deployment
- Implement 1 of up to 4 Endpoint DLP policies
- Deploy and configure 1 MIP Scanner and Microsoft SQL Server Express instance (required)
- Configure the MIP Scanner job template (non-environment change scan)
- Show and tell up to 10 on-premises DLP policies
- Provision and deploy Ontinue Critical Insider Risk Policies
- Provision the Purview connector for data security log ingestion
- Configure up to 5 Log Analytics playbooks for high-level alerting to a Customer source (e.g. helpdesk), covering DLP and Sensitivity Labelling only
- Enable Purview-based email encryption for test users, including encryption based on 1 content type
- Enable reporting and automatic classification for up to 3 pre-production file folders, to avoid user impact
- Demonstrate end-to-end functionality

2.2. Ontinue In-Scope Activities, Defender for Cloud Apps

- Arrange and lead the Discovery session: show and tell to level-set the team, understand the current cloud app estate, review any existing MDCA/CASB configuration, and designate up to 50 sanctioned apps
- Review and propose changes to the existing MDCA implementation
- Guide the deployment of up to 4 native API integrations
- Configure up to 5 Conditional Access App Control rules for featured apps
- Configure up to 50 sanctioned and unsanctioned apps
- Configure up to 5 File MDCA policies and up to 10 MDCA policies
- Guide the configuration of IP locations

2.3. Customer In-Scope Activities

- Ensure attendance of relevant personnel at the Discovery sessions



- Submit all Change Requests and receive required approvals prior to engagement commencement
- Provide access to the Microsoft 365 (Office 365) production tenant
- Provide remote access and permissions for the Ontinue project team, via a Customer-managed account or PIM-managed identity
- Assign the following permissions for Ontinue: Compliance Administrator, Content List Viewer, Security Administrator, and Global Reader
- Provide licenses to support Ontinue activities (minimum Microsoft 365 E5 Compliance required)
- Deploy and configure 1 Windows Server 2016 or newer (2019 or newer recommended)
- Deploy and configure 1 Microsoft SQL Server Express instance
- Arrange or perform any required proxy, firewall, or network changes to support Ontinue activities
- Honor all reasonable requests for information within 1 business day
- Accept full responsibility for all Azure, consumption, and license charges resulting from the engagement

3. Engagement Outputs

Output	Owner	Sign-off Required
Microsoft Purview Design Document	Ontinue	No

4. Assumptions, Dependencies, Constraints

Item	Type
Customer has an active Azure subscription	Assumption
All configuration work must be completed in the Production Tenant, linked to the primary domain	Constraint

Nonstop SecOps

Questions? Let's talk.

European HQ

Grubenstrasse 54, 8045 Zürich,
Switzerland

Düsseldorf Office

Speditionstraße 2, 40221
Düsseldorf, Germany

North America HQ

450 Maple Street, Redwood City,
CA 94063, USA

Vienna Office

Kohlmarkt 8-10, 1010 Wien, Austria

UK Office

9 Holborn, London EC1N 2LL, United
Kingdom

APAC Office

World Trade Tower, Sector 16, Noida
201301, India

Toronto Office

6060-3080 Yonge St, Toronto ON
M4N 3N1, Canada

 **Continue**