Microsoft 365 cyber risk assessment

Frequently asked questions

ASCERIS

About this document

The purpose of this document is to explain how we conduct cyber risk assessments of Microsoft 365 environments, and to answer frequently asked questions.

Frequently asked questions

What does the assessment involve?

As part of the assessment, we connect to your Microsoft 365 environment and collect configuration and activity information, which is then assessed and risk-rated under a broad range of areas such as multi-factor authentication, legacy authentication blocking, audit logging, and users with unusual activity patterns.

What are your checks and risk rating assessments based on?

The checks we conduct as part of the assessment are based on our experience of investigating hundreds of Microsoft 365 cyber security incidents, and provide practical recommendations for improving your security posture.

What is the output?

We prepare a Microsoft 365 cyber risk assessment report, which describes our observations and recommendations. We offer to schedule a follow-up call with you to discuss the report and answer any questions you may have.

How long will it take to start the assessment?

We can begin collecting data as soon as an administrator user is set up for us on your Microsoft 365 environment, which usually takes around five minutes. We provide a guidance document that specifies the step-by-step process for setting up an administrator account with the permissions we need.

How much time will you need from us during the assessment?

The time required on your part is minimal. We need a web-based form to be completed, and an administrator account needs to be provisioned for us.

How long does the assessment typically take?

The overall timing is largely dependent on the data collection stage and the number of user accounts in the environment. Small assessments can be completed relatively quickly, while assessments for large environments can take a few weeks. The following table provides a typical schedule for the assessment of a large environment.

Phase	Task	Typical timeline
Project kick-off and onboarding	We send the kick-off email to you, which includes our FAQ document and a link to a short questionnaire on the web.	Week 1
	You complete the questionnaire, which provides us with details of your Microsoft 365 environment, existing security controls, and who should sign the terms and conditions.	Week 1
Terms and conditions	We circulate our terms and conditions document via DocuSign for your signature. This document describes the objectives of the risk assessment and covers our data protection and confidentiality obligations.	Week 1
Access and verification	When the terms and conditions are signed we provide a step-by-step guide to you, which describes how you can provide us with access to your Microsoft 365 environment (usually an account with the minimum permissions for the assessment).	Week 1
	You share the relevant Microsoft 365 credentials with us, and we verify access.	Week 1
Assessment execution	We conduct the Microsoft 365 assessment, which includes data collection and processing, and a wide range of checks against your environment.	Week 2 to 3
Report creation and delivery	We prepare a report and share it with you by email.	Week 4
Report walkthrough	We conduct a walkthrough session with you to review the report and address your questions.	Week 4

How long do you need to use the administrator account?

We need the administrator account for the duration of the assessment, to collect log data and to review information in the administrator portals of your environment. The account can be removed after you receive our report.

Which user accounts are included in the activity analysis?

For most environments, we include all user accounts in data collection and analysis.

Is there a limit on the number of users?

No, there is no limit on the number of accounts in an environment. For environments with a very large number of users, we will restrict the timeframe of the activity under review in order to deliver the assessment in a timely manner.

How will you gather data?

We collect information using read-only PowerShell commands and manual observations in the administrator portals of your environment. We use the Graph API PowerShell functionality of Microsoft 365 to run certain read-only commands. When these commands are run, an Azure application maintained by Microsoft will appear in your Microsoft Entra ID portal under the *Enterprise Applications* section. It is named *Microsoft Graph Command Line Tools* and has the icon displayed to the right.

Is there any risk to our systems?

No. All of the tools we use for data collection are read-only, i.e. we do not run any commands that could alter data or configuration in your environment. Our analysis will not cause any performance impact to your users. Microsoft automatically throttles excessive traffic, which ensures that there is no performance impact across Microsoft 365 as a whole as a result of our data collection.

Do you collect personal data?

To conduct our proactive assessment, we collect the following low-sensitivity data sources: tenant configuration settings; user login activity; administrative changes; mailbox rules; email forwarding information; and autoreply information. The data we collect that relates to an individual is therefore very limited and incidental, and is typically business-related rather than personal (e.g. professional email addresses). We intentionally exclude phone numbers when we collect account configuration information, on that basis that they may be personal phone numbers. We do not collect the content or metadata of emails or files.

Is the data collected sent to any third-party location?

The data is collected directly onto our own cloud-based systems, where it is processed and reviewed. We use third-party APIs to provide us with contextual information, but only IP addresses are made available to these commercial third-party services.

What privileges does the administrator account need?

We require a new user account on your environment with certain administrator roles. The account does not require any product licenses, so should not incur any costs from Microsoft.

The simplest way of providing the access we need is to assign the minimum permissions we require to access all data that may be relevant, with the least effort from your team. Our account setup guide therefore requests the following roles: *Global Reader; Exchange Administrator; Compliance Administrator;* and *Cloud Application Administrator*.

We can work with an even more restricted set of permissions, but this may mean that we ask you to collect some data for us, or that we do not review certain configuration settings. The following table sets out the purpose for each administrative role, and provides alternatives where available.

Administrative role	**Data that we collect using this role**	**Alternative**
Global Reader	Tenant-level configuration data except for some mailbox-related configuration data	None – the *Global Reader* role is essential
Global Reader + *Compliance Administrator*	As above, plus user activity data to assess user-level events such as logins and app consent events	None – the *Compliance Administrator* role is essential for user activity analysis
Global Reader + *Compliance Administrator* + *Exchange Administrator*	As above, plus mailbox-specific data such as mailbox rules	You can run a PowerShell script we provide to collect the required data
Any of the above + Cloud Application Administrator	No additional data – we request the Cloud Application Administrator so that we can deploy and consent to the *Microsoft Graph Command Line Tools* application for you	You can deploy and consent to the *Microsoft Graph Command Line Tools* application

If you choose to deploy and consent to the *Microsoft Graph Command Line Tools* application, the process depends on whether your environment uses the admin consent workflow. If it is enabled on your environment, you must approve an application consent request when we begin collecting data. If it is not enabled, we provide a PowerShell command for you to run, which registers the app and specifies the scopes we will use.