Onboarding Document for CyberSecurity

Version 1.0

UnifyCloud™

Document Review & Approval

	Prepared by	*Reviewed by*	*Approved by*
Name	Sukanya.R		
Company	UC		
Role	Tech Writer		
Date	03/01/2023		

Version	Date	Prepared by	Changes made
1.0	03/01/2023	Sukanya.R	Prepared the first draft of Onboarding Document

Table of Contents

Objective

This Cybersecurity Onboarding document aids in comprehending the CloudAtlas Cybersecurity Onboarding standards and login procedures. It also includes an overview of the distinct dashboards available in On-premises, Azure, and Office 365 environments.

Intended use and Target audience

This document is intended for reference with the target audience, including company internal personnel, customers, and partners.

Introduction

CloudAtlas Cybersecurity is a service from UnifyCloud that analyzes IT environments' security using various security frameworks, benchmarks, and baselines.

Compliance Control Requirements Used in CloudAtlas Cybersecurity

Azure:

- Microsoft Cloud Security Benchmark v1.0
- ISO 27001
- ACSC Essential 8
- CERT NZ

O365:

- CIS Benchmark for O365

On-premise:

- CIS v1.7
- NIST CSF
- ACSC Essential 8

Data Collection

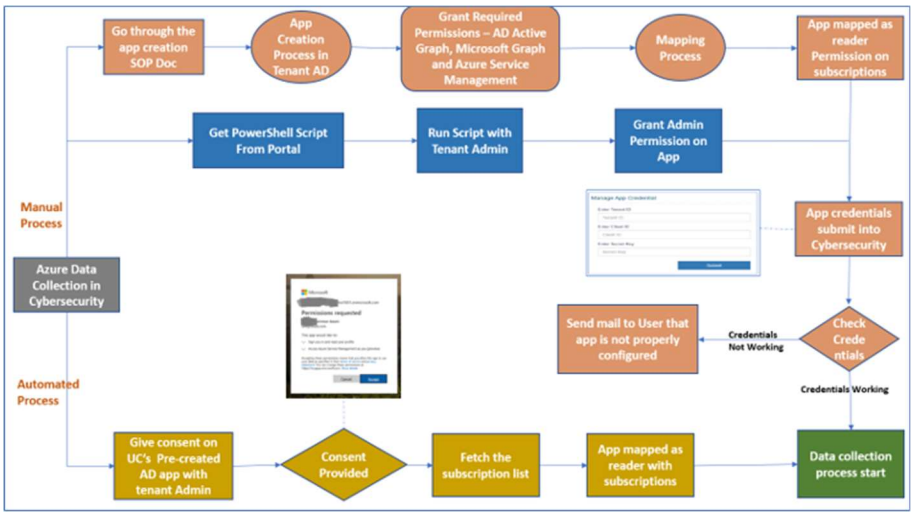
This gives a brief explanation of how data is gathered and processed from various signal sources in on-premises, Azure, and/or Office 365 systems.
In CloudAtlas Cybersecurity, we conduct analysis for the following environments:

- Azure
- O365
- On-premises

We use a variety of tools to in order to collect as much representative data as possible for each environment. This Data Collection Document contains instructions for 3 environments – Azure, O365 and OnPremise.

Azure

We make advantage of Microsoft's graph APIs for Azure data collecting. These APIs will request authorization from the Azure AD app. Both "Manual" and "Automated" process flows are available for data collection in the Azure environment.

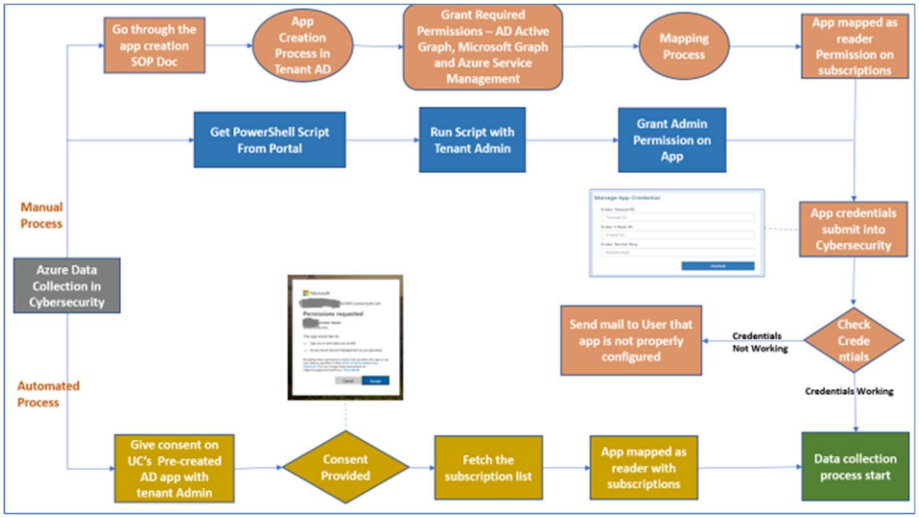


To capture data from the subscription, the Azure AD app needs a reader role on the subscription. It takes 24-48 hours for the graph APIs to pull data from the subscription thanks to an automated procedure executed by a web job.

The tenant's Azure subscriptions' key settings for each resource are gathered, and security analysis is provided. We perform data analysis using RBAC rules, compliance frameworks, and tool recommendations.

O365

For O365 data collecting, we use Microsoft graph APIs as well as PowerShell.



These APIs obtain authorization from the Azure AD app. The data collection process flow in the O365 environment can take one of two paths: "Manual" or "Automated."

On-Premise

For on-premise data collection, we use these discovery tools:

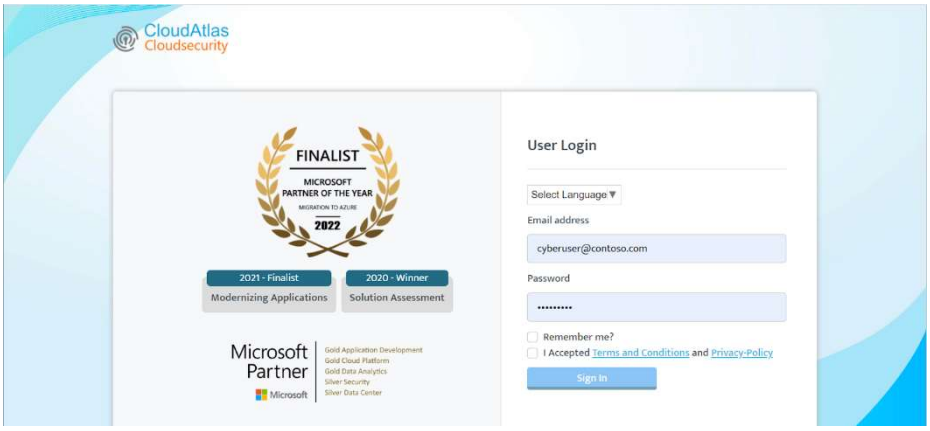
Lansweeper
Lansweeper finds & gathers information on all assets, and provides end-to -end visibility. Lansweeper data, reports and settings are stored in a database. The database is hosted in either the Microsoft SQL LocalDB or Microsoft SQL Server.Depending on how much scanned data is actually recorded, a database's size can vary significantly. However, on average, we advise setting aside 1GB of disc space for every 100 Windows machines.

Movere
The tenant's Movere account is necessary to start the environment's discovery using Movere. The Movere console needs to be set up for discovery. When this console is installed and the environment-scanning application has all the necessary permissions.

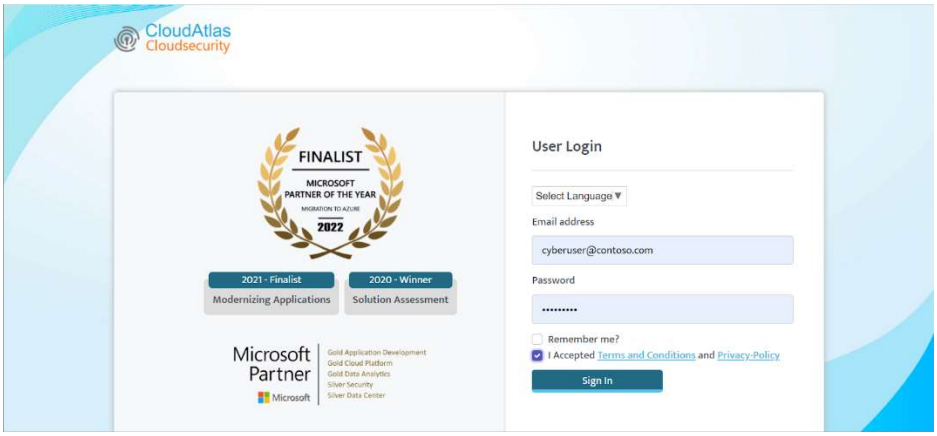
The scan can be started, and the Movere site (https://www.movere.io) will display the results and any updates.Following scanning, all data should be extracted in CSV format, compressed, and uploaded to CloudRecon.

Note: UnifyCloud processes data transfer from CloudRecon to the CloudAtlas Cybersecurity service

User Login



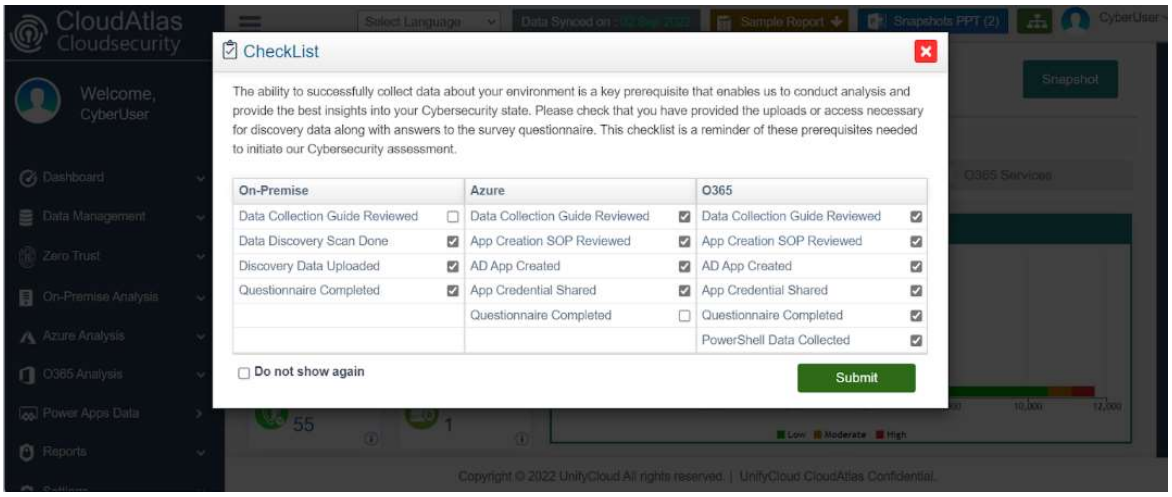
Step 1. Go to the CloudAtlas Cybersecurity Portal https://crcybersecurity.azurewebsites.net/. The login window appears, as shown in Figure 1: CloudAtlas Cloudsecurity Login Window.



Step 2. Enter the login credentials, Username, and Password, and accept the Terms and conditions and Privacy policy

Note: you can select the language of choice; it is also available in Chinese(Simplified), Japanese and Korean.

Step 3. Click sign-in, You will be redirected to the CloudAtlas cybersecurity Dashboard.



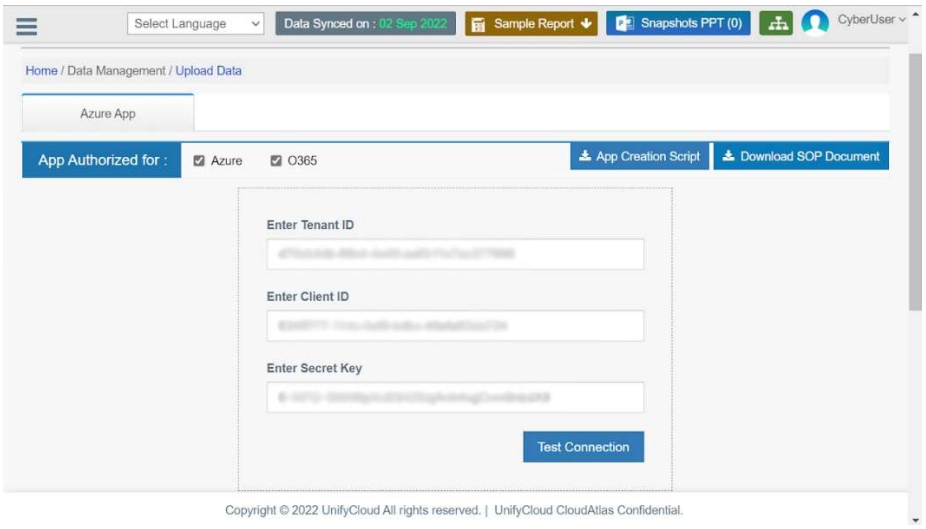
Note: The Checklist is the first feature you'll notice on the Dashboard page. The Checklist's purpose is to successfully collect data from the customer environment, conduct analysis, and deliver the finest insights into cybersecurity.

The Checklist also serves as a free reminder of the requirements for initiating the cybersecurity assessment.

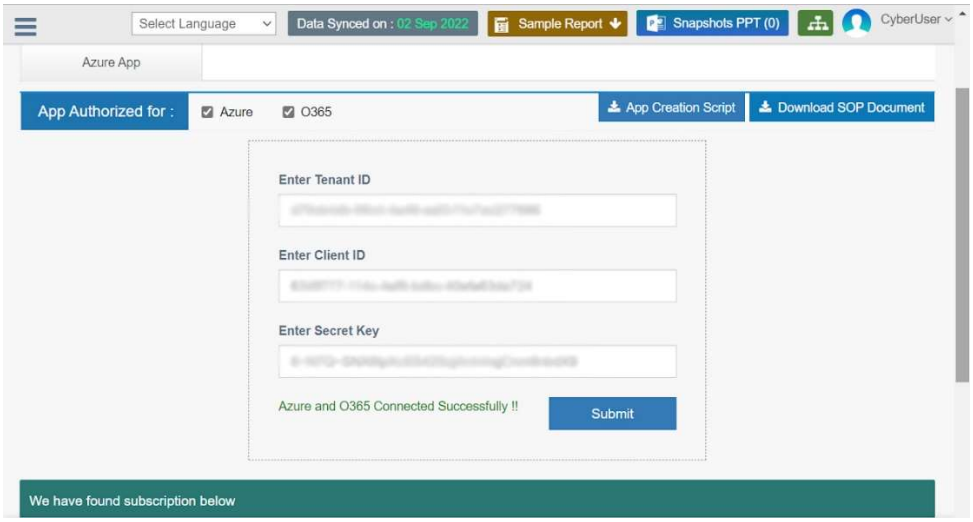
The Checklist provides credentials from all the three domains, such as On-Premise, Azure, and 0365. Next, select the relevant functionalities needed to conduct cybersecurity analysis from the three domains and click on the submit option.

Data Management

This dashboard provides a detailed description of Cybersecurity Data Capture. In the App Authorized Credential, submit the following information such as Tenant ID, Client ID, App Key {Secret Key].
You can also download App creation Script and SOP documents.



You can proceed with the Test connection. Upon completion it will deliver a message such as “Azure and O365 Connected Successfully !!”
Then you can proceed with Submit.

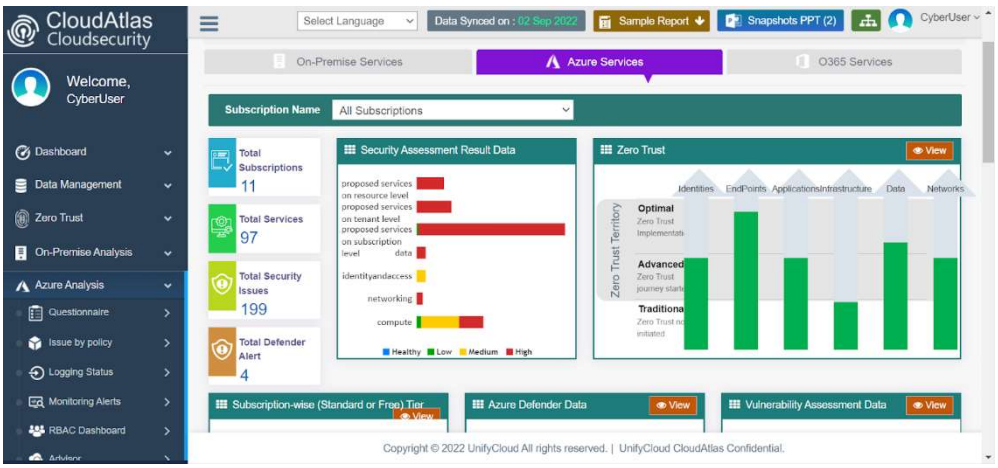


Dashboard

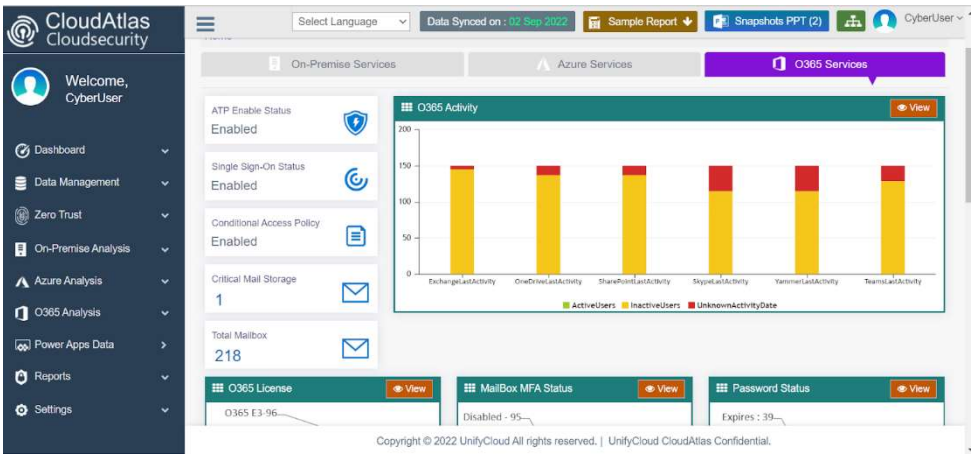
A dynamic dashboard is included with CloudAtlas Cybersecurity. The administrator can use the dashboard application to analyze and monitor the configurations of all Cybersecurity subscriptions, monitor security issues, detect potential vulnerabilities, and offer alerts and recommendations.

Azure Analysis

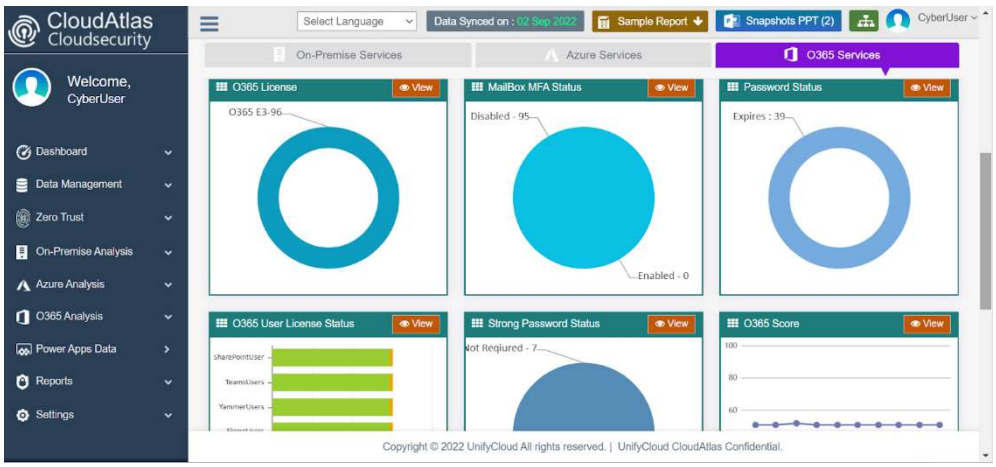
In this Azure Dashboard we showcase the total number of subscriptions and services, security issues and vulnerabilities on different services running under the Tenant subscriptions.



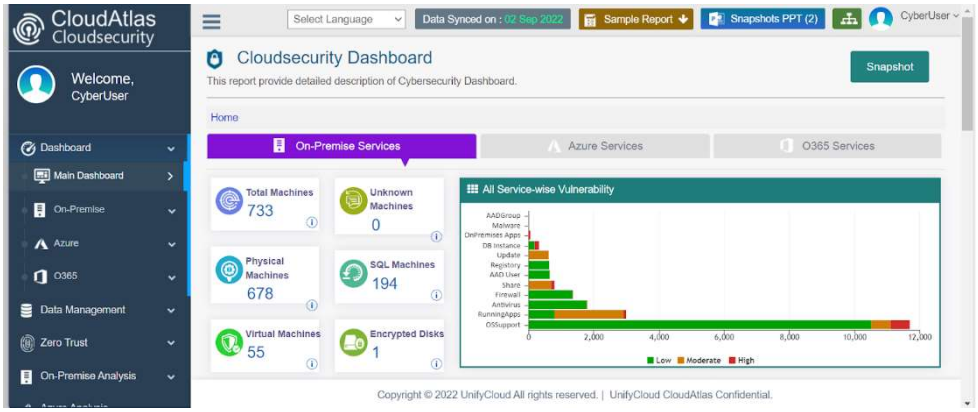
O365



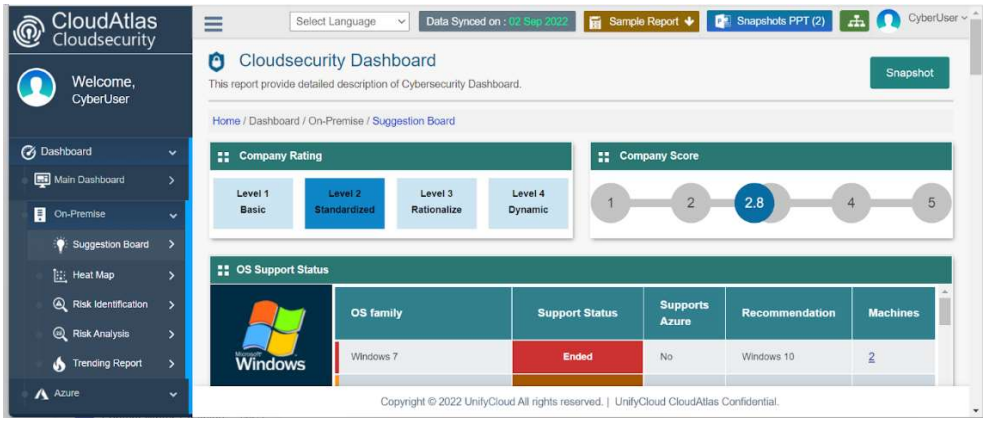
In this Dashboard , we show different issues which would leave the tenant O365 data susceptible to risk, the details about the failed resources and the overall O365 activities



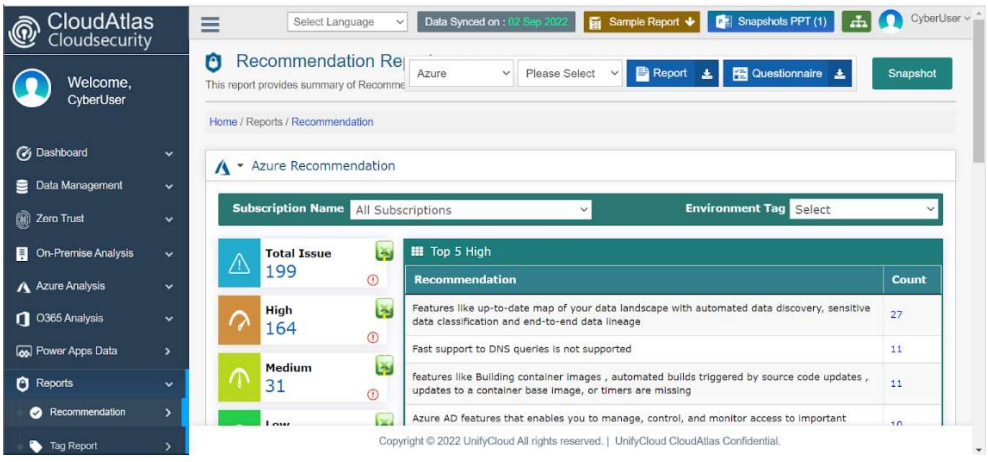
On-Premise



This dashboard illustrates the security issues that impact the environment's services. It includes information about the encryption status, the service-specific vulnerability status, and the availability of antivirus.



Report Download



Under the menu "Cybersecurity Report-> Recommendation, the user can select the environment from the dropdown and download the report. Under this dropdown, all the environments the user has selected for security analysis will appear.