

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

Unify<mark>Cloud</mark>™



Table of Contents

1 Objective	.3
2 Intended use and Target audience	.3
3 Introduction	.3
4 Compliance Control Requirements Used in CloudAtlas Cybersecurity	3
5 Data Collection	.3
6 User Login	.5
7 Data Management	.6
8 Dashboard	6
9 Azure Analysis	6
10 O365	.8
11 On-Premise	9
12 Report Download	9



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 Onpremises, 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 onpremises, 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 (<u>https://www</u>.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

Cite Cite	oudAtlas		
	FINALIST	User Login	
	MICROSOFT PARTNER OF THE YEAR	Select Language ▼	
	2022	Email address	
	- Xer	cyberuser@contoso.com	
	2021 - Finalist 2020 - Winner	Password	
	Modernizing Applications Solution Assessment		
		Remember me?	
	Microsoft Partner Microsoft Siler Secury Siler Data Center	I Accepted Terms and Conditions and Privacy-Policy Sign in	

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.

FINALIST	User Login
	Select Language V
2022	Email address cyberuser@contoso.com
2021 - Finalist 2020 - Winner	Password
Modernizing Applications Solution Assessment	
• • •	Remember me?
MICrOSOft Bartbor Gold Cloud Platform	✓ I Accepted Terms and Conditions and Privacy-Policy



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.

CloudAtlas	Soloci Languar	ya 😒	Data Synced on : 10 8-+	772	📕 📅 Sample Report 🔶 🚺 😭	Shapsh	65 FFT (2)	CyberUser
Welcome, CyberUser	The ability to successfully collect data a provide the best insights into your Cybe for discovery data along with answers tr to initiate our Cybersecurity assessmen	bout your or security s the surve	environment is a key prerequ ate. Please check that you h y questionnaire. This checkli	uisite f have p ist is a	that enables us to conduct analysis a provided the uploads or access nece a reminder of these prerequisites ne	and essary eded	Snap	shot
@ Dashboard v	On-Premise	Azure			0365		O365 Services	
📄 Data Management 🔍 🗸	Data Collection Guide Reviewed [Data C	ollection Guide Reviewed		Data Collection Guide Reviewed	2		
	Data Discovery Scan Done	App Cr	eation SOP Reviewed		App Creation SOP Reviewed			
💮 Zero Trust 🗸 🗸	Discovery Data Uploaded	AD Ap	Created		AD App Created	23		
E On-Premise Analysis	Questionnaire Completed	App Cr	edential Shared		App Credential Shared	2		
		Questi	onnaire Completed		Questionnaire Completed			
🔥 Azure Analysis 🛛 🗸 🗸					PowerShell Data Collected			
0 0385 Analysis 🔹 🗸	Do not show again				Submit			
(60) Power Apps Data >	1 W 55 U					nate:	an toboo	12,000
🕘 Reports 🔍 🗸			 (0) /0. 		L COV II MODERADE II I			
Contraction (Contraction)								

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.





ne / Data Management /	Upload Data			
Azure App				
App Authorized for :	Azure	☑ O365	App Creation Script	Download SOP Document
		Enter Tenant ID		
		Phone Review and Phone		
		Enter Client ID		
		Enter Secret Key		
		e ers mense stationers	CBreize	
			Test Connection	

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.

pp Authorized for :	Azure	Ø 0365	📥 App Creation Script	Download SOP Document
		Enter Tenant ID		
		Enter Client ID		
		Enter Secret Key		
		Azure and O365 Connected Successfully !!	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.



Unify<mark>Cloud</mark>™

Cloudsecurity Welcome.	<u>,</u>	On-Pre	emise Services	Azure	Services	0365 Service	5
CyberUser		Subscription Name	All Subscriptions	v			
🕑 Dashboard	~	Total Subscriptions	E Security Assessment Result Dat	a	🗰 Zero Trust		View
😑 Data Management	*	11	proposed services		Identities End	Points ApplicationsInfrastructure	Data Networks
🍈 Zero Trust	*	Total Services	on resource sevel proposed services on tenant level proposed services		Coptimal Zero Trust Implementati		
On-Premise Analysis	•		level data		Transaction of the second		
Azure Analysis	~	Total Security Issues	identityandaccess		o Zero Trust journey starte		
Questionnaire	>	199	compute		Traditiona Zero Trust no		
🔹 😭 Issue by policy	>	Total Defender Alert	Healthy Low Medium	High	initiated		
O Logging Status	>	4					
🗉 🛃 Monitoring Alerts	>	III Subscription-wise (SI	landard or Free) Tier	e Defender Data	• View	Vulnerability Assessment Data	• View
RBAC Dashboard	>						
- \land Arlvienr			Copyright @ 2022 UnifyClou	id All rights reserve	d. UnifyCloud CloudAtlas Co	nfidential.	

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







CloudAtlas	Select	Language 👻 Data Sy	vnced on : 02 Sep 2022	Sample R	eport 🔸 💽 Snap	shots PPT (2)	🗄 <u> </u>
Welcome, CyberUser	Cloudsecul This report provide detaile	ity Dashboard	y Dashboard.				Snapshot
	Home						
O Dashboard	. On-P	remise Services	A.	Azure Services		0365 Se	rvices
Main Dashboard							
On-Premise	Total Machines 733	Unknown Machines 0	AADGroup - Malware -	unerability			
Azure	Physical		D8 Instance - Update -				
0365	Machines 678	194	Registory - AAD User - Share - Firewall -				
Data Management			Antivirus - RunningApps -				
(ii) Zero Trust	Virtual Machines	Encrypted Disks	0 SSupport	2,000	4,000 6,000	8,000 1	0,000 12,000
On-Premise Analysis		Copyright © 2022	UnifyCloud All rights re	served. UnifyClo	ud CloudAtlas Confiden	tial.	

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.



Cloudsecurity	/ _	- Olioot Laing	Judge		
	O Re This repor	ecommendal	tion Re of Recomme	Azure V Please Select V Report 🛓 🎛 Questionnaire 🛓	Snapshot
	Home / R	eports / Recommend	dation		
Dashboard	× A •	Azure Recomme	endation		
Data Management		and recomme	inducion		
) Zero Trust	Sut	scription Name	All Subs	criptions	Ŷ
Zero Trust On-Premise Analysis	v Sut	Total Issue	All Subs	criptions v Environment Tag Select	v
Zero Trust On-Premise Analysis Azure Analysis	Šut Č	scription Name Total Issue 199	All Subs	criptions v Environment Tag Select Top 5 High Recommendation	Count
Zaro Trust On-Premise Analysis Azure Analysis O365 Analysis	sut Č	Total Issue 199 High 164	All Subs	criptions Environment Tag Select Environment Tag Select Commendation Features like up-to-date map of your data landscape with automated data discovery, sensitive data classification and end-to-end data lineage	Count 27
Zaro Trust On-Premise Analysis Azure Analysis O365 Analysis Dewer Apps Data	sut Sut X X X X X X	Total Issue 199 High 164	All Subs	criptions Environment Tag Select	Count 27 11
Zero Trust On-Premise Analysis Azure Analysis 0365 Analysis Power Apps Data Reports	Sut Sut	Total Issue 199 High 164 Medium 31	All Subs	criptions Environment Tag Select	 Count 27 11 11

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.

Report Download