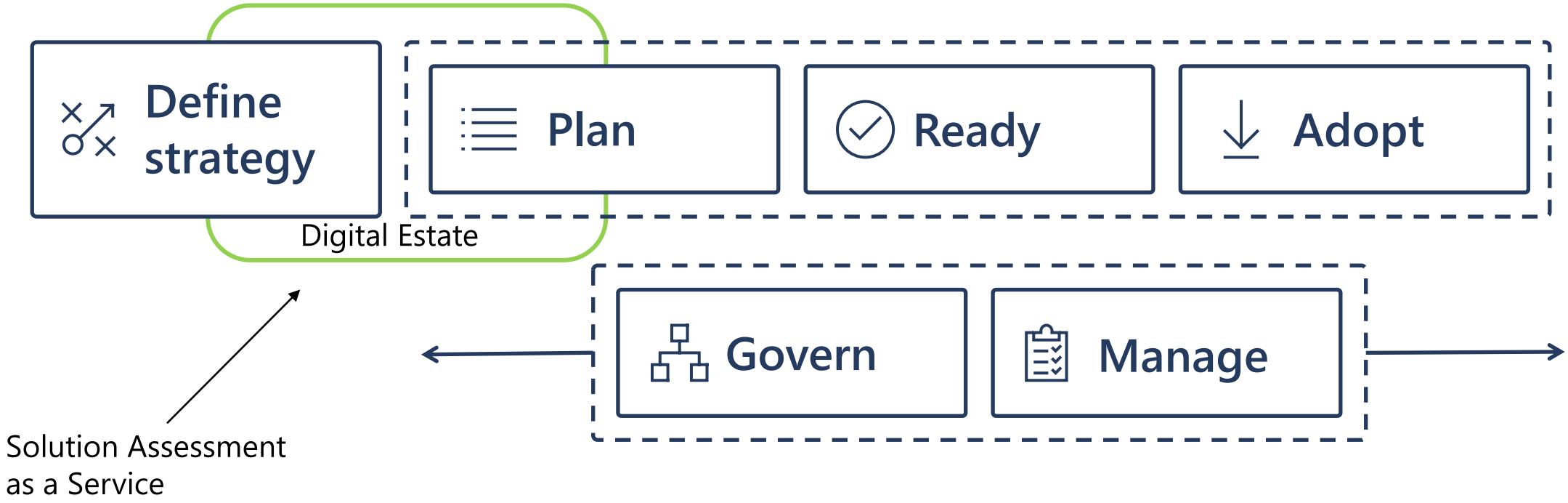
Microsoft | Solution Assessments

Solution Assessments as a Service

Cloud Adoption Framework



Using data to drive better decisions

Microsoft Solution Assessments use the power of data-driven recommendations and actionable steps to help customers improve productivity, reduce costs, and optimize their investments

Valuable insights

Get expert recommendations for your technology journey so you can make the best decisions for your business

Trusted partnership

We'll help you find the right Microsoft partner to drive your digital transformation

Peace of mind

Rest easy knowing you are staying ahead of your organization's security needs

Solution Assessment – the Value

Provides customers with an in depth understanding of the **opportunities** available in their environments to improve productivity, reduce cost and optimize investments.

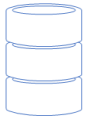
- A Solution Assessment is a set of proven processes that delivers a comprehensive view of a tangible data insights, inventory, usage, and risks, ultimately enabling organizations to **regulate costs and resources, manage business, and align IT investments with business needs.**
- Solution Assessment provide data based **real data** on existing infrastructure, **security** threats and **migration** options including **TCO** views
- From a **security** standpoint, a Solution Assessment helps organizations identify and counter potential threats by ensuring that end-of-life products get decommissioned and that product updates and security patches are applied in a timely way.

Planning

Prepare environment for tool deployment

Identify key points of contact and process owners

Identify scope of workloads & applications



Data collection

Deploy toolset/s:

Azure Migrate, Movere, Cloud Pilot, DMA, SQL script

Data Collection for 5-30 days

Data analysis

Review and validate all collected data, complete analysis and prepare **Business Case**

TCO

Final recommendations

Present our results, recommendations, and next steps through an overview presentation and detailed set of outputs

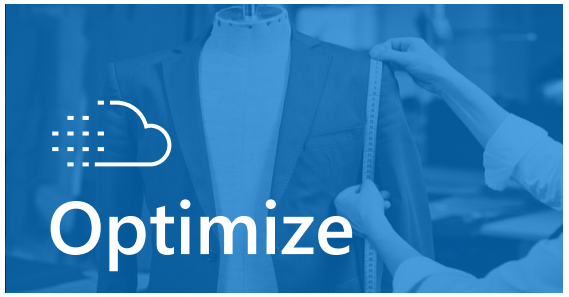
HOW: Solution Assessment – as a Service model

What do I have?

What should I do?

How shall I do it?

How can I optimize?



Partner

Microsoft as a service

Discovery Tool
Migration Tool – Data Collection
Data analysis

Final Assessment Report
Recommendations &
Action Plan
Workshop
Migration Action Plan and **sign off**

Migration in Execution

"Tailored" Cloud Project
Consumption monitoring
Cost Control & Governance
Managed Service

UnifyCloud CSAT MOVERE CAST Software Intelligence for Digital Leaders

Solution Assessment | as a Microsoft service - Offering

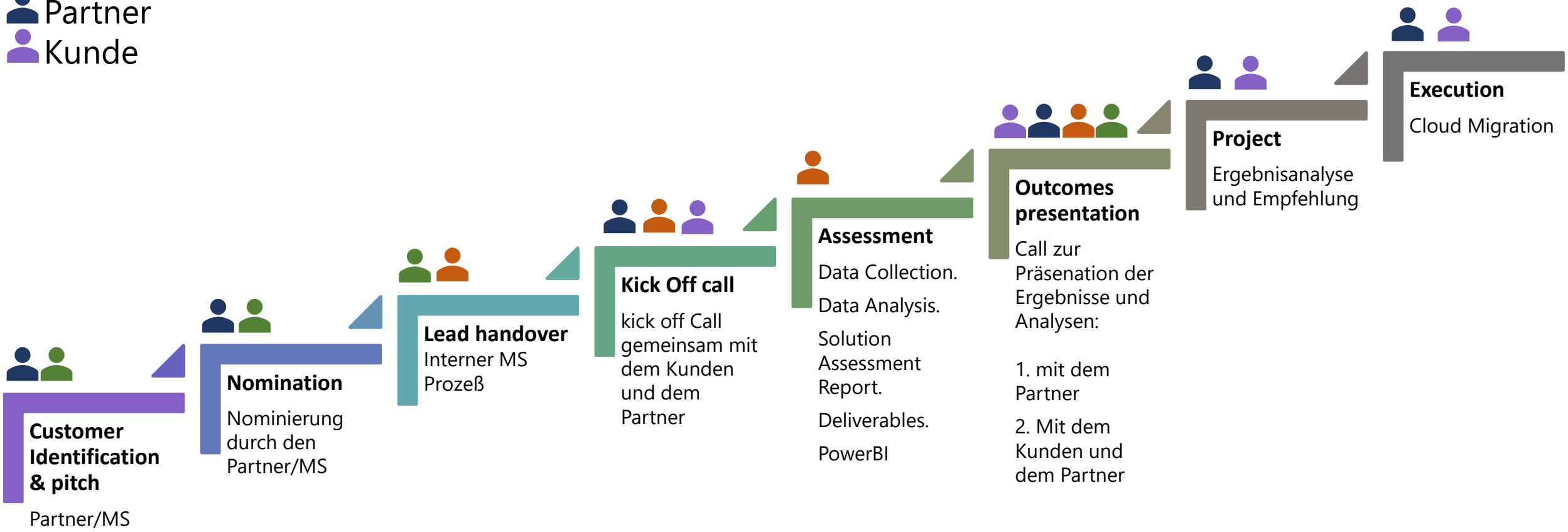
Microsoft

General Portfolio for FY21:

1. **Data & Infrastructure Migration**: Helps customers modernize their server & data storage and provide recommendations for migration to Azure
2. **Application Modernization**: Assists customers identify and prioritize applications for cloud modernization
3. **Data and AI Assessment:** Transforming data- analytics according to the Maturity Model
4. **Cloud Security**: Helps customers understand security risks in their IT Infrastructure and how to solve issues
5. **Workplace Modernization**: Provides the customer with a detailed prioritized set of recommendations of their overall cloud-ready capabilities in relation to their desktop cloud migration strategy
6. **Business applications:** Provides customers with Dynamics CRM on premise and Dynamics AX Assessment migration options in D365.

Solution Assessment Ablauf

Microsoft
Solution Assessment Consultant
Partner
Kunde



Solution Assessments - Zusammenfassung

	Data & Infrastructure Bei Modernisierung von Server und Rechenzentren; Empfehlungen zur Azure Migration	**Cybersecurity** Umfassender Einblick in die Cybersecurity Infrastruktur	**Application Modernization** Bewertung von Applikationen als PaaS in Azure	**Workplace Modernization** Migration zu oder Implementierung einer Software as a Service (SaaS) - Strategie
Idealer Kandidat	Kunden mit älterer HW & SW Kunden mit Cloud Strategie Kunden die bis dato kaum oder gar keine Erfahrung mit der Cloud haben	Kunden die ihr Sicherheitsrisiko evaluieren wollen	Azure Kunden die PaaS Lösung in Betracht und/oder einer Modernisierung ihrer Lösung	"Dark on cloud" On-premise zu Office365/M365 Alternde Hardware (Surface Opportunity)
Dauer	2-4 Wochen	2-3 Wochen	1-5 Wochen	2 - 3 Wochen
Tools	Movere	CSAT	CloudPilot	CSAT, Movere
Inputs	Server Hardware und Software Inventur mit Performance Metrik	Hardware und Software Inventur Ergänzend mit einem Fragebogen	Scannen von Kunden Applikationen (3-5 Applikationen/Source Code)	Hardware- und Softwareinventar, einschließlich Aktualisierungszyklen, Versionen, Betriebssystemen und Patches
Ergebnisse "Deliverable"	PowerBI-Report, inklusive TCO Analyse, Network Mapping und Usage and Consumption Grafik	Basisanalyse des aktuellen Cybersecurity Status sowie Ermittlung von Schwachstellen. Roadmap basierend auf einem Maturity Model (CIS Controls). TCO Analyse und Migrationplan.	Ermittlung der Applikations-Readiness für Azure, inclusive der erwarteten Kosten, einer Referenz Architektur und einem Modernisierungsplan.	Eine detaillierte und priorisierte Reihe von Empfehlungen zu einer Desktop-Cloud-Migrationsstrategie unter Berücksichtigung des Surface-Geräteportfolios TCO Analyse und Migrationsplan.

Data and Infrastructure Migration Assessment as a Service

by a Solution Assessment Consultant (remote)

Assessment Überblick

End-to-End Analyse der gesamten und aktuellen Infrastruktur (Bereitstellung, Nutzung, etc.) und Empfehlungen zur Modernisierung der Server & Rechenzentrumsumgebung mit einer optimierten Azure Migration.

Assessment Tool

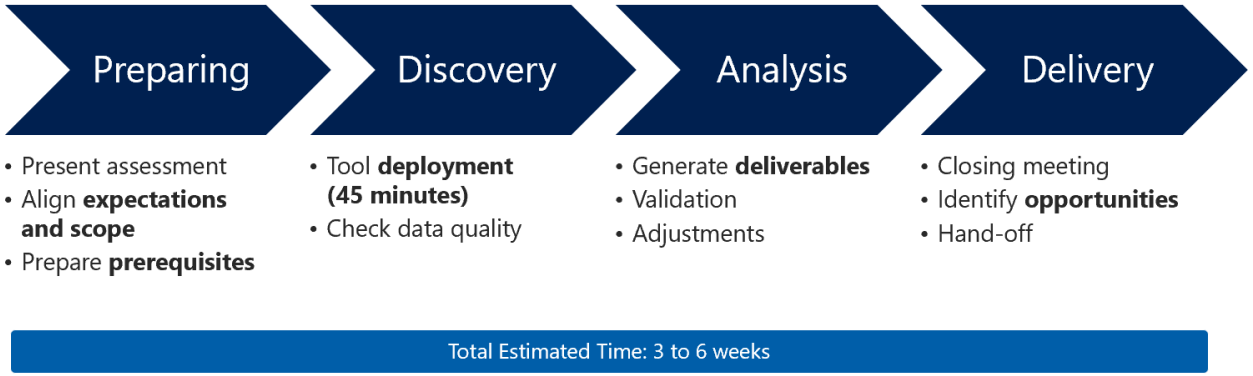
Zur Datenerfassung wird das Microsoft Tool Movere, eine Software-as-a-Service (SaaS) Lösung herangezogen. Movere erkennt, scant und sammelt automatisiert die Daten der IT Umgebung. (Installieren der Movere Konsole: Deployment Requirements)

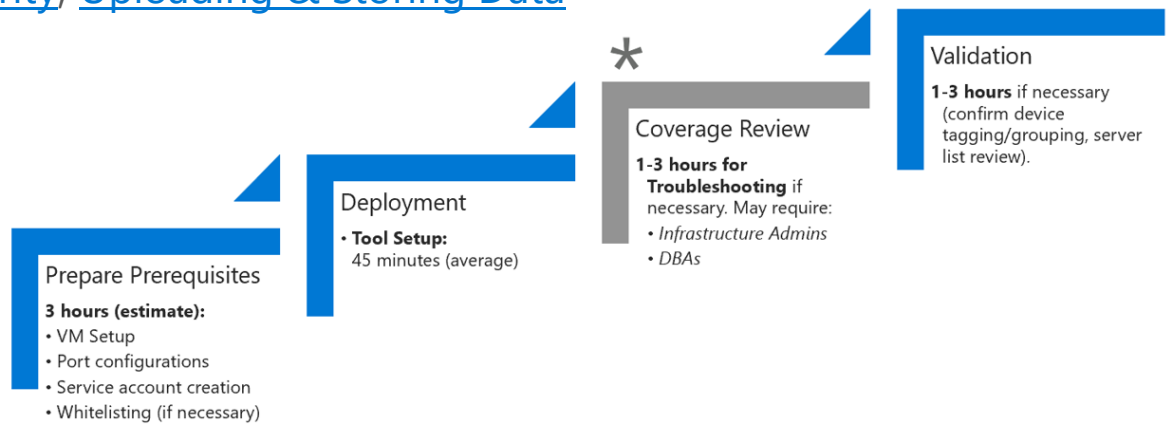
Assessment Ergebnis

Die Zugriffsrechte auf das Movere Webportal, wo die Daten liegen, werden vom Administrator (= Kunde) verwaltet. Eine umfassend Analyse aller Ergebnisse und Empfehlungen warden dem Kunden präsentiert und zur Verfügung gestellt (Power BI + Zusammenfassung als Power Point)

Datenschutz

Nach dem Assessment wird das Tenant für 16 Tage gesperrt, wonach sämtliche Daten automatisch gelöscht werden. Als Administrator kann der Kunde jederzeit Daten löschen. Movere Security; Uploading & Storing Data





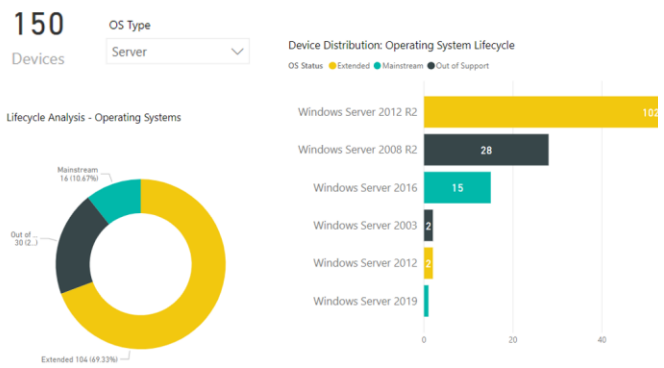
Data and Infrastructure Migration Assessment as a Service

by a Solution Assessment Consultant (remote)

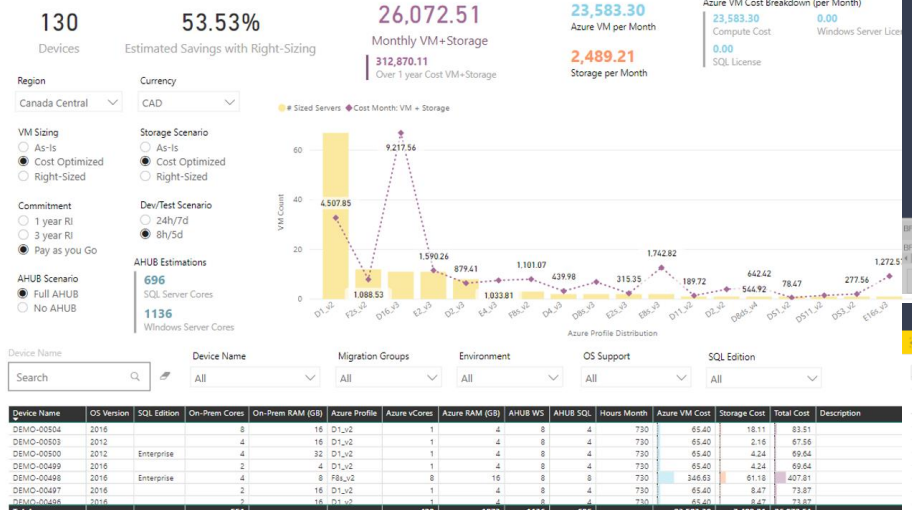
Microsoft

MOVERE

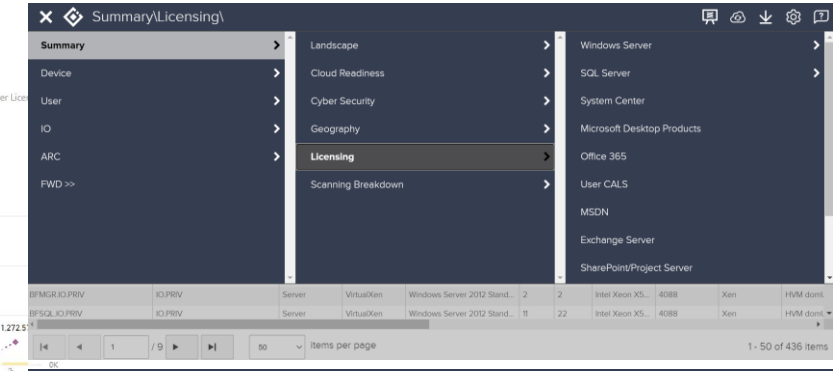
Operating Systems Lifecycle



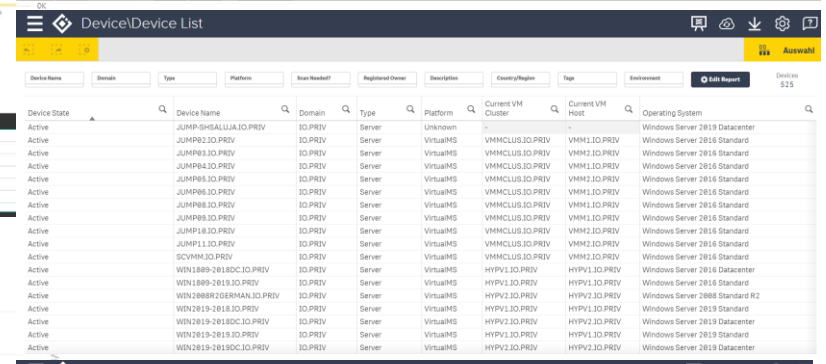
Azure Projections



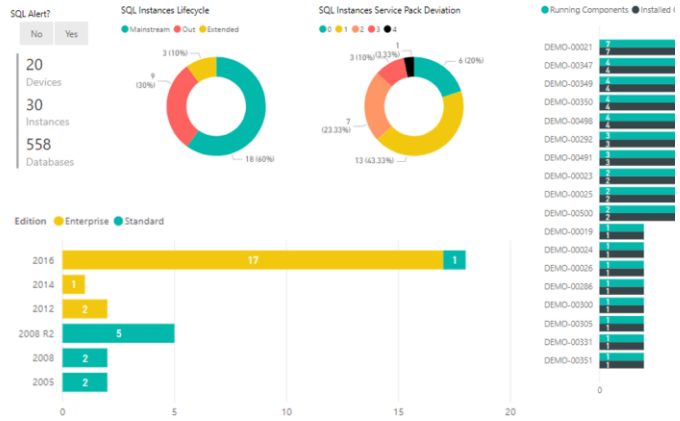
Summary\Licensing\



Device\Device List



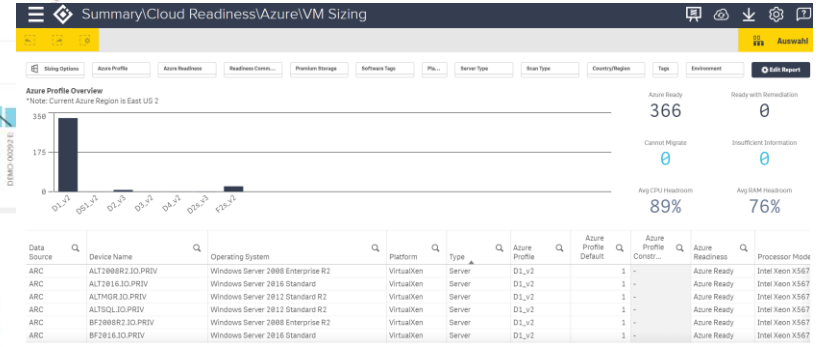
SQL Overview



Storage & IOPS Analysis

Azure storage profiles are available as "Standard" and "Premium". And this is where IOPS becomes a key factor. If a disk's IOPS exceeds 500 or has a throughput greater than 60MB per second during an ARC scan, then Movere will recommend Premium storage SKUs. *More information at: Movere: Cloud Storage Sizing & Pricing*

Summary\Cloud Readiness\Azure\VM Sizing



Modern Workplace Assessment as a Service

by a Solution Assessment Consultant (remote)

Assessment Überblick

Das Assessment zeigt umfassend die Möglichkeiten auf, um die Produktivität zu verbessern, Kosten zu senken und Investitionen zu optimieren.

Assessment Tool

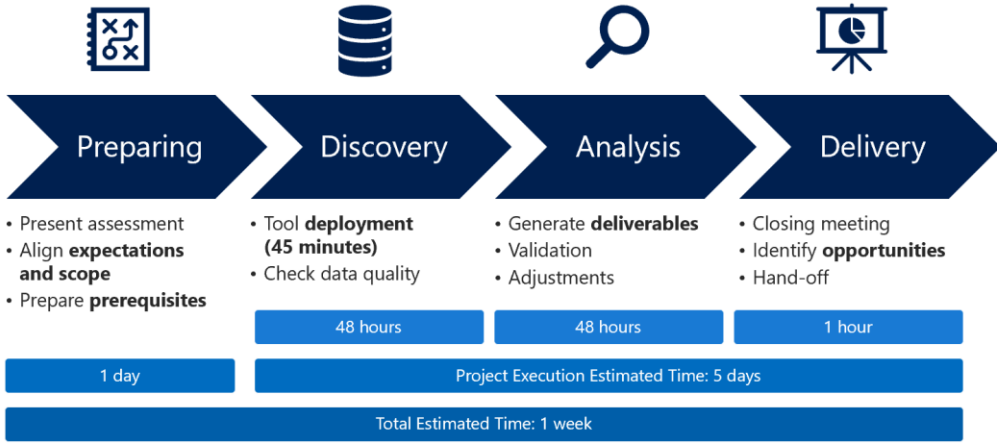
Zur Datenerfassung wird das Microsoft Tool Movere, eine Software-as-a-Service (SaaS) Lösung herangezogen. Movere erkennt, scant und sammelt automatisiert die Daten der IT Umgebung. (Installieren der Movere Konsole: Deployment Requirements)

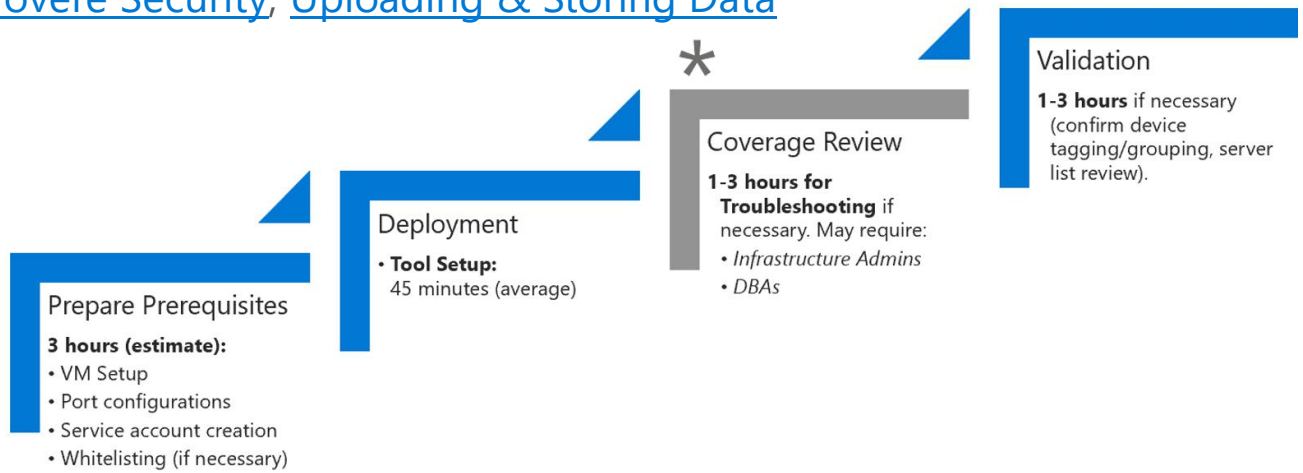
Assessment Ergebnis

Die Bewertungen bieten datenbasierende Empfehlungen, mit denen Kunden umsetzbare Schritte für digitale Transformationen, Cloud-Migrationen und Prozessverbesserungen ermitteln können.

Datenschutz

Nach dem Assessment wird das Tenant für 16 Tage gesperrt, wonach sämtliche Daten automatisch gelöscht werden. Als Administrator kann der Kunde jederzeit Daten löschen. Movere Security; Uploading & Storing Data



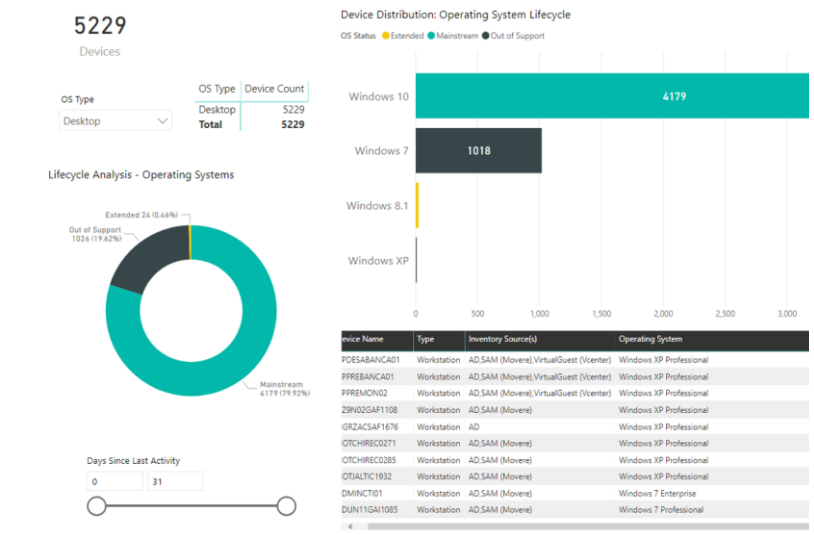


Modern Workplace Assessment as a Service

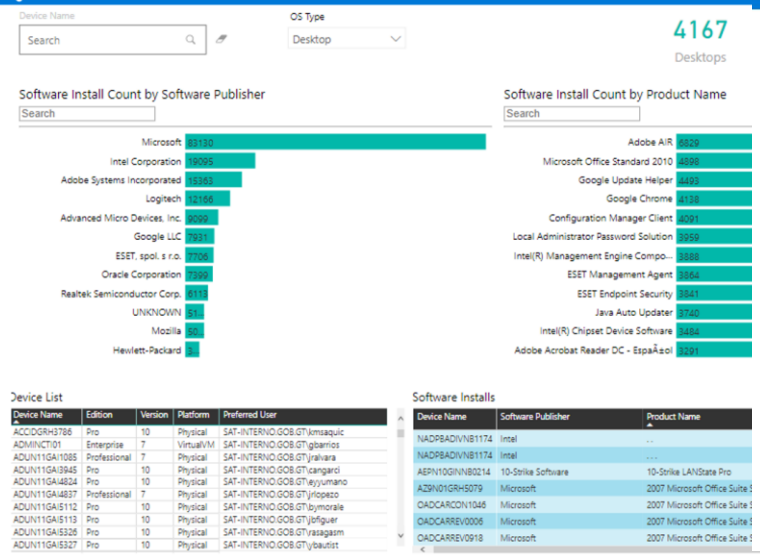
by a Solution Assessment Consultant (remote)

Microsoft

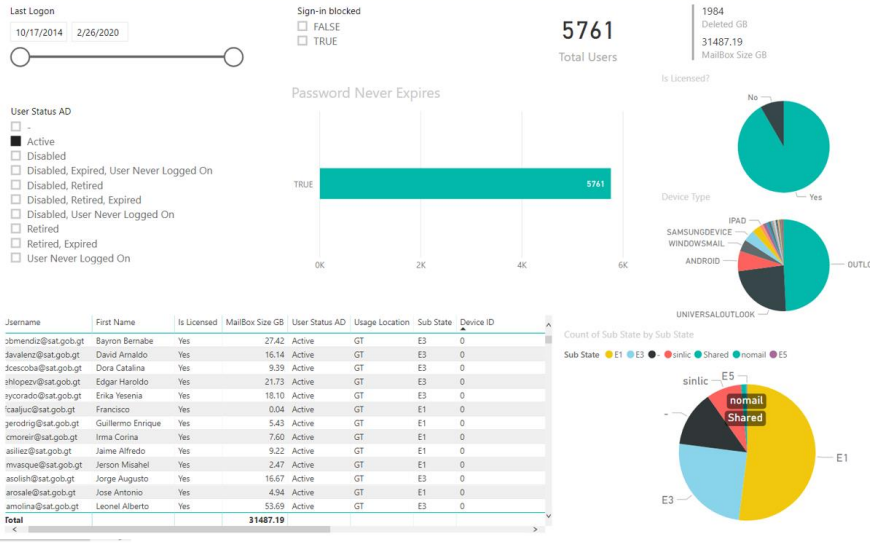
Lifecycle (Desktops)



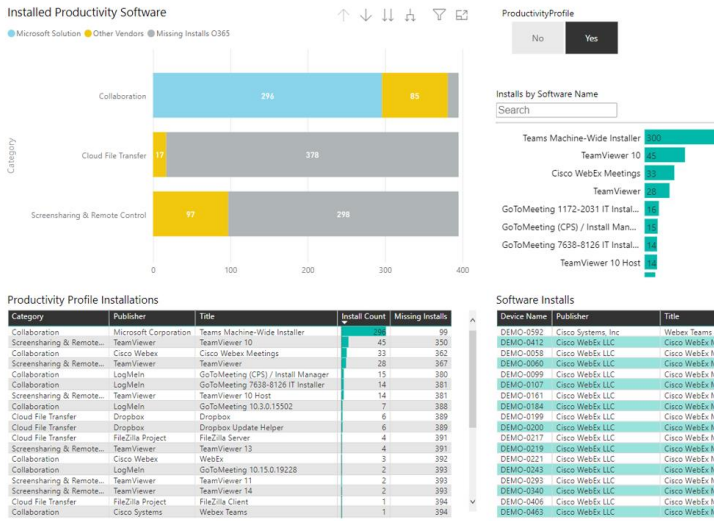
Application Discovery Status(Desktops)



Office 365 - Users

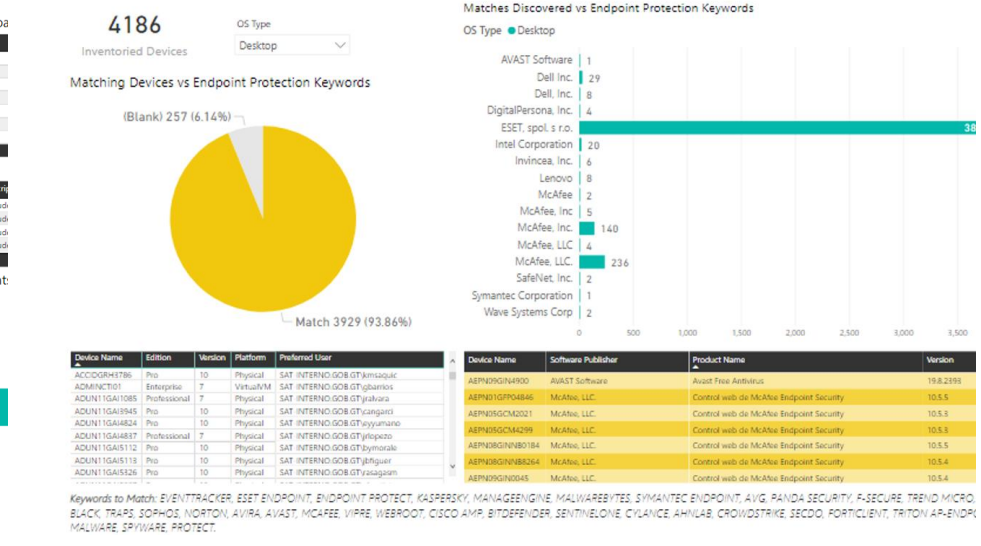


Productivity Profile



O365 Assignements

Antivirus and Antimalware Software Discovered(Desktops)



Application Modernization Assessment as a Service

by a Solution Assessment Consultant (remote)

Assessment Überblick

Das Assessment hilft Kunden dabei, Anwendungen für die Cloud-Modernisierung zu identifizieren und zu priorisieren.

Assessment Tool

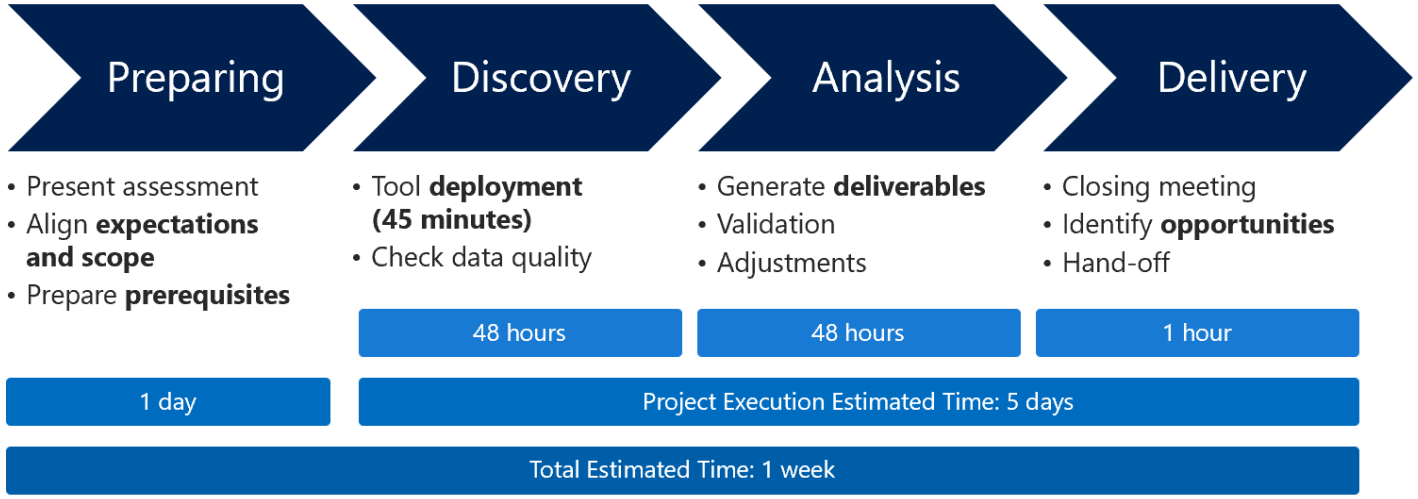
Das Tool CloudPilot, von UnifyCloud, ermittelt genau die Migrationskosten für Azure PaaS und IaaS und gibt bis zur Codezeile detaillierte Empfehlungen, welche Codeänderungen vorgenommen werden müssen.

Assessment Ergebnis

CloudPilot ist eine statische Code-Analyse zum Scannen des Sourcecodes und verwendet Konfigurationsdaten, um einen detaillierten Bericht über Änderungen auf Codeebene bereitzustellen (Codeänderungen, Beispielersatzcode sowie Aufwand und Kosten für AKS, Azure App Service, VM, etc.) abgebildet.

Datenschutz

Datenschutz Richtlinien: Privacy Policy



Application Modernization Assessment as a Service

by a Solution Assessment Consultant (remote)

Microsoft

UnifyCloud

App Modernization: Assessment Overview

Assessed Apps **2**

Assessed DBs **2**

Application Name	Application Platform	Scan Date	Container Readiness	App Service Readiness	Virtual Machine Readiness
Demo App1	.Net	05-18-2020	75%	79%	79%
Demo App2	.Net	05-18-2020	74%	75%	79%

Database Name	Database Type	Source Platform
Demo Database1	SQL Server	On-Premise
Demo Database2	SQL Server	On-Premise

App Profile and Recommendations:

Demo App1: Web Application; 1 Component; 24296 Code Lines; .Net Platform

- **Azure App Service** is recommended
- **12** changes needed
- **66** hours of migration effort
- **S2** instance CAD **$ 206.13** (monthly)

Demo App2: Web Application; 4 Components; 11454 Code Lines; .Net Platform

- **Azure App Service** is recommended
- **25** changes needed
- **161** hours of migration effort
- **S2** instance CAD **$ 206.13** (monthly)

Database Profile and Recommendations:

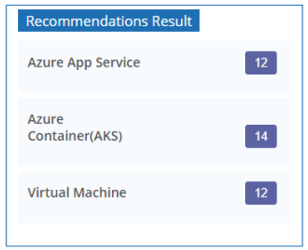
Demo Database1: MSSQL; Express Edition; v15.0.2070.41

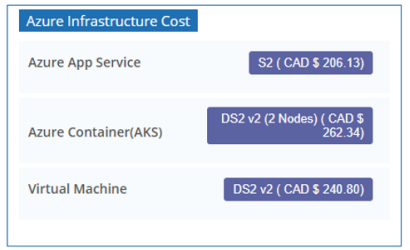
- **SQL Database (vCore)** is recommended.
- **7** changes needed.
- **22** hours of migration effort.
- **Gen 5 – 2 vCore** database CAD **$ 529.62** (monthly)

Demo Database2: MSSQL; Express Edition; v15.0.2070.41

- **SQL Database (vCore)** is recommended.
- **8** changes needed.
- **26** hours of migration effort.
- **Gen 5 – 2 vCore** database CAD **$ 529.62** (monthly)

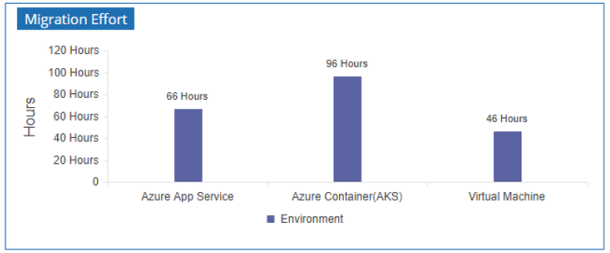
App Modernization: Overview (Demo App)

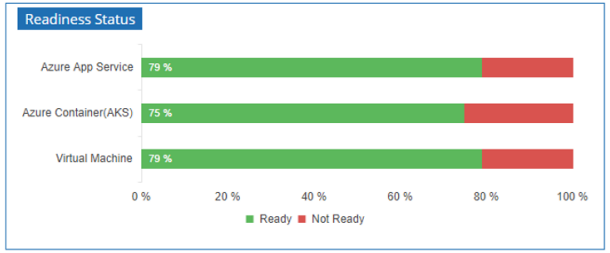




Recommended Application Platform: Azure App Service enables you to build and host web applications in the programming language of your choice without managing infrastructure. It offers auto-scaling and high availability, supports both Windows and Linux, and enables automated deployments from GitHub, Visual Studio Team Services, or any Git repo.
More Info...

Why: This application is a good choice to move to Azure App Services, as it has no blockers & has additional features without any cost.
Other Option: Azure Container Instance, Azure Kubernetes Service, Service Fabric and Virtual Machine.





Sample summary table for Key Recommendations

Code Block	Line	Hours	Impact	Reason for change
<authentication mode="Windows" />	74	24	Optional	Application using Windows Authentication for Identity. Windows Authentication is not supported on the cloud, use other recommended authentication scheme for identity
N/A	N/A	1	Optional	AppSettingsSection is used for storing sensitive information of application.
<sessionState mode="InProc" timeout="40" />	60	4	Optional	In Proc, Session mode will not support when you scale up your Application.
Dim path2 As String = "D:\ABC\Apps\DemoApp1\Demo\tmp\Sample.pdf"	22	16	**Mandatory**	The Application uses Hard Coded Drive Path. These drive paths may not be accessible after deployment in Azure App Service.

Migration Blockers

Issue Details:	Action
Cross database queries using three- or four-part names not supported in Azure SQL Database	**Mandatory**

Impact: Queries or references using three- or four-part names not supported in Azure SQL Database. Three-part name format, [database_name].[schema_name].[object_name], is supported only when the database_name is the current database or the database_name is tempdb and the object_name starts with #.

Recommendation: Move the dependent datasets from other databases into the database that is being migrated. Migrate the dependent database(s) to Azure and use 'Elastic Database Query' functionality to query across Azure SQL databases. (more info)

Issue Details:	Action
BAK file (import/export) is not supported in Azure SQL Database	**Mandatory**

Impact: You can not restore database in Azure SQL Database using BAK file.

Recommendation: Convert BAK file into a BACPAC file and restore it manually (more info).

Cybersecurity Assessment as a Service

by a Solution Assessment Consultant (remote)

Assessment Überblick

Das Cybersecurity Assessment hilft Kunden dabei, potenzielle Risikobereiche zu identifizieren und bietet einen umfassenden Überblick zu ihrer Cybersicherheitsinfrastruktur, einschließlich der aktuellen Softwarebereitstellung und –nutzung.

Assessment Tool

Das Cyber Security Assessment Tool (CSAT) von QS Solutions bietet automatisierte Scans und Analysen für Einblicke in die Schwachstellen, basierend auf Daten aus der Unternehmensinfrastruktur und erstellt Empfehlungen sowie einen Aktionsplan.

Assessment Ergebnis

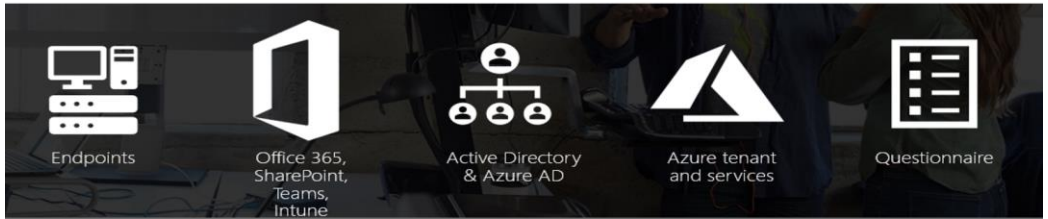
CSAT identifiziert die Bereiche wo empfohlen wird Maßnahmen zu ergreifen und liefert wichtige Erkenntnisse, um die richtigen Prozesse zur Reduzierung des Cyberrisikos zu etablieren.

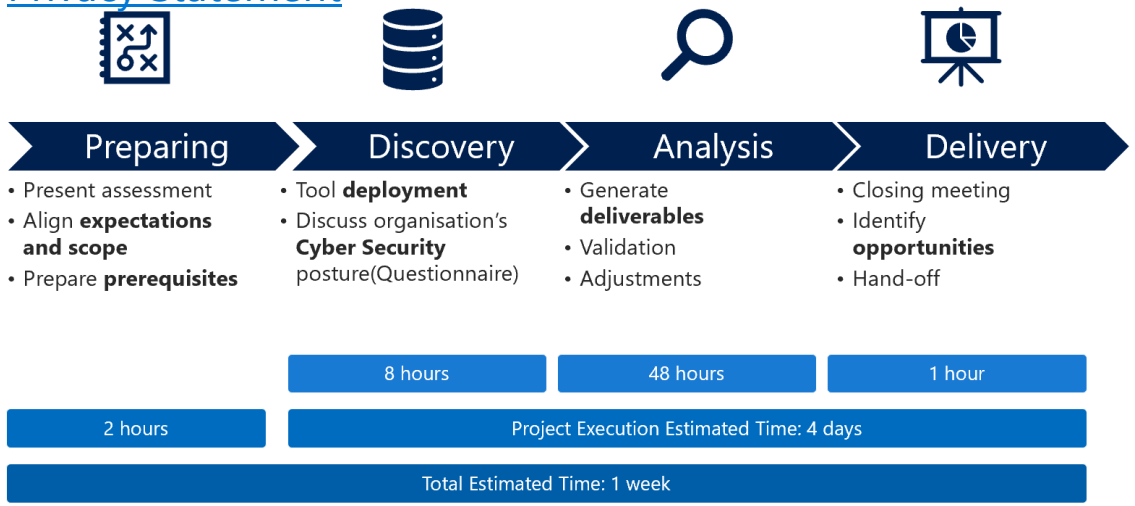
Datenschutz

Nach dem Scannen der Endpoints löschen sich die Agents automatisch. Privacy Statement

Cyber Security Assessment Tool (CSAT) collects relevant data from IT environment to assess your present status in terms of security and provides fact-based recommendations.

Additionally, a questionnaire is also used to collect information about policies and other key indicators.





Cybersecurity Assessment as a Service

by a Solution Assessment Consultant (remote)

Microsoft

CSAT

Action Plan to improve Cyber Security

Urgent priority Actions

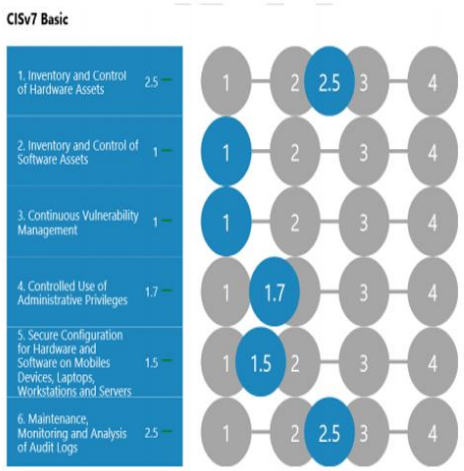
These are the urgent priority actions identified in the Assessment and detailed below in this report. We recommend that the following items are assessed and acted on as the first priority:

Priority	Action	Associated Software Products
Urgent		
2. Inventory and Control of Software Assets	• Embed a discovery tool for software asset management.	• Discovery tooling • Microsoft Endpoint Manager • Azure Security Center • Microsoft Cloud App Security • Microsoft Defender ATP
3. Continuous Vulnerability Management	• Implement a patch management process and tooling. Gain insights on the patch status of all systems • Gain continues insight on your specific regulatory requirements	• Microsoft Endpoint Manager • Windows Server Update Services (WSUS) • Azure Security Center • Azure Sentinel
4. Controlled Use of Administrative Privileges	• Setup personal admin accounts and enable multi-factor authentication for all external administrative access with just in time permissions	• Azure AD Privileged Identity Management (PIM) • Privileged Access Management (PAM) • Azure Multi-Factor Authentication • Azure Conditional Access
8. Malware Defense	• Enable the default tools for antivirus, anti-malware and DEP on the organization's systems.	• Microsoft Cloud App Security • Microsoft Defender ATP
12. Boundary Defense	• Enable DDoS protection on the external facing (web)services	• Azure DDoS Protection
13. Data Protection	• Enable encryption on the organization's main data sources.	• BitLocker • Microsoft Endpoint Manager
16. Account Monitoring and Control	• Define a standard password policy definition for all the applications and infrastructure services. Start implementing MFA on all systems, increase password length if MFA is not yet available	• Azure Multi-Factor Authentication (MFA) • Conditional Access
AD.2. Data Governance	• Define a labeling and classification policy and implement it.	• Azure Information Protection Scanner • Data Loss Prevention • Azure Information Protection P2

Quick wins

With the actions below, security improvements are visible, have direct benefits for Contoso and can be quickly deployed in the organization. Overview of the advised actions and products:

Topic	Action	Associated Software Products
Quick Wins		
(Azure) Active Directory Accounts	• Disable old/unused accounts • Implement Multi Factor Authentication (MFA) for all user accounts • Review External AAD users	• Azure MFA • Conditional Access • Azure AD reporting
Administrators	• Implement a process to regularly review administrator accounts and clean up old/unused accounts	• Azure Privileged Identity Management (PIM)
Applications	• Ensure that all applications are kept to up to date	• Intune
Secure Configuration	• Ensure SMB V1.0 is disabled	
Email Protection	• Implement the DMARC record	
Windows Updates	• Ensure that all the available security updates are deployed for the used Operating systems	• Intune • Azure Security Center
Antivirus	• Update the out	
Disk Encryption	• Enable disk en mobile device	
SharePoint Site Permissions and Externally Shared	• Create proced user permissi	
Protection against distributed denial-of-service (DDoS) attacks	• Ensure all exte DDoS attacks	
Protect your Sensitive assets	• Ensure all privi for administra	



Basic CIS Controls - Findings and Recommendations

The detailed findings below are associated with each of the six (6) Basic CIS controls, and lead to the following recommendations for Contoso:

Urgent				
Topic	**Question**	**Answer**	**Advice**	**Advised Products**
2. Inventory and Control of Software Assets	Are Discovery tools implemented to identify all software applications throughout the organization's infrastructure?	Basic (1) Not implemented	Embed a discovery tool for software asset management.	Microsoft Endpoint Manager, Azure Security Center, Cloud App Security, Microsoft Defender ATP
3. Continuous Vulnerability Management	Are Discovery tools implemented to identify any software vulnerabilities on systems within the infrastructure of the organization?	Basic (1) Not implemented	Implement vulnerability scan software. Scan for vulnerabilities regularly, especially on systems contain sensitive information.	Microsoft Endpoint Manager, Microsoft Defender ATP, Azure Security Center, Cloud App Security
3. Continuous Vulnerability Management	Has an automated patch management solution been implemented to continuously update all organization's systems?	Basic (1) Not implemented	Implement a patch management process and tooling. Gain insights on the patch status of all systems	Microsoft Endpoint Manager, Windows Server Update Services (WSUS), Azure Security Center
4. Controlled Use of Administrative Privileges	Does every administrator have a dedicated personal admin account, separated from their normal user account? The organization implemented multi-factor authentication (MFA) for all administrative access. Just in Time Access rules are applied to limit the default permissions.	Basic (1) Not implemented	Setup personal admin accounts and enable multi-factor authentication for all external administrative access.	Azure AD Privileged Identity Management (PIM), Privileged Access Management (PAM), Azure Multi-Factor Authentication
4. Controlled Use of Administrative Privileges	Does the organization have an entitlement review process to validate that each person with administrative privileges on servers, desktops, and laptops is authorized by a senior executive on a repeating schedule?	Basic (1) No process in place	Implement an entitlement and approval review process with Azure AD PIM Access Reviews for all accounts with administrative privileges, to regularly check these. Clean up old unused accounts.	Azure Privileged Identity Management (PIM), Azure AD Access Review
5. Secure Configuration for Hardware and	Are Discovery tools implemented to identify any misconfigured security settings on all of	Basic (1) Not implemented	Implement a configuration management tool, to check all	Microsoft Endpoint Manager, Microsoft

Microsoft | Solution Assessments