# Security Health Checks as a core of your business strategy

February 26th, 2026



# Cybersecurity assessments as the core of your business strategy

**Business Risk**

**Cost Saving**

**Business Risk** and **Cost Saving** are the primary conversation starters to unlock all **cloud migrations** and **modernization** triggers.

# Security Health Check with FullScan & QuickScan

**Holistic view of the cybersecurity position** together with fact-based recommendations based on an internationally recognized **cybersecurity framework**.

Collect and analyze data from the **hybrid IT environment** in a short period of time to provide **data-driven recommendations**.

**Identify cost saving** elements to help organizations finance their security improvements and cloud migrations.

**Click here to watch explainer video**



Company score
based on **CIS controls v8**



Mapping to **NIS 2.0**
European guidelines & **Copilot Readiness**



Risk-based **action plan**
with improvement actions



Migration plans to improve cybersecurity
based on the **Zero Trust Architecture**



**Urgent Action** Items
and **Quick Wins**



**Total Cost of Ownership** for Security
and other relevant topics; e.g., Azure Migrate

# CISv8 maturity scores backed up by undisputable data

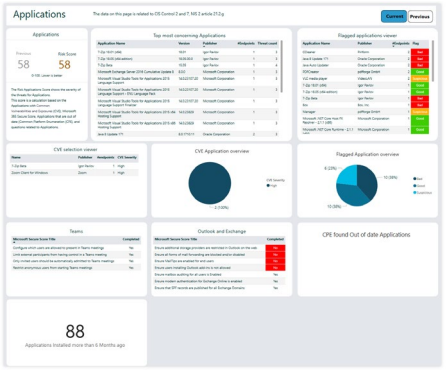
**Focus your sales effort** on the controls the customer is lacking security – these are your quickest sales.

Average maturity score **1.8**




## CISv8 Controls Summary

| | | Previous | Score |
|---|---|---|---|
| 1 | Inventory and Control of Enterprise Assets | 1.0 | 1.0 |
| 2 | Inventory and Control of Software Assets | 1.3 | 1.3 |
| 3 | Data Protection | 1.2 | 1.2 |
| 4 | Secure Configuration of Enterprise Assets & Software | 1.2 | 1.2 |
| 5 | Account Management | 1.5 | 1.5 |
| 6 | Access Control Management | 1.5 | 1.5 |
| 7 | Continuous Vulnerability Management | 1.3 | 1.3 |
| 8 | Audit Log Management | 1.7 | 1.7 |
| 9 | Email and Web Browser Protections | 1.5 | 1.5 |
| 10 | Malware Defenses | 1.3 | 1.3 |
| 11 | Data Recovery | 1.5 | 1.5 |
| 12 | Network Infrastructure Management | 1.2 | 1.2 |
| 13 | Network Monitoring and Defense | 1.7 | 1.7 |
| 14 | Security Awareness and Skills Training | 1.5 | 1.5 |
| 15 | Service Provider Management | 1.5 | 1.5 |
| 16 | Application Software Security | 1.8 | 1.8 |
| 17 | Incident Response Management | 1.5 | 1.5 |
| 18 | Penetration Testing | 1.0 | 1.0 |
| 19 | AQ 1. IT Governance | 1.2 | 1.2 |
| 20 | AQ 2. Data Governance | 1.7 | 1.7 |

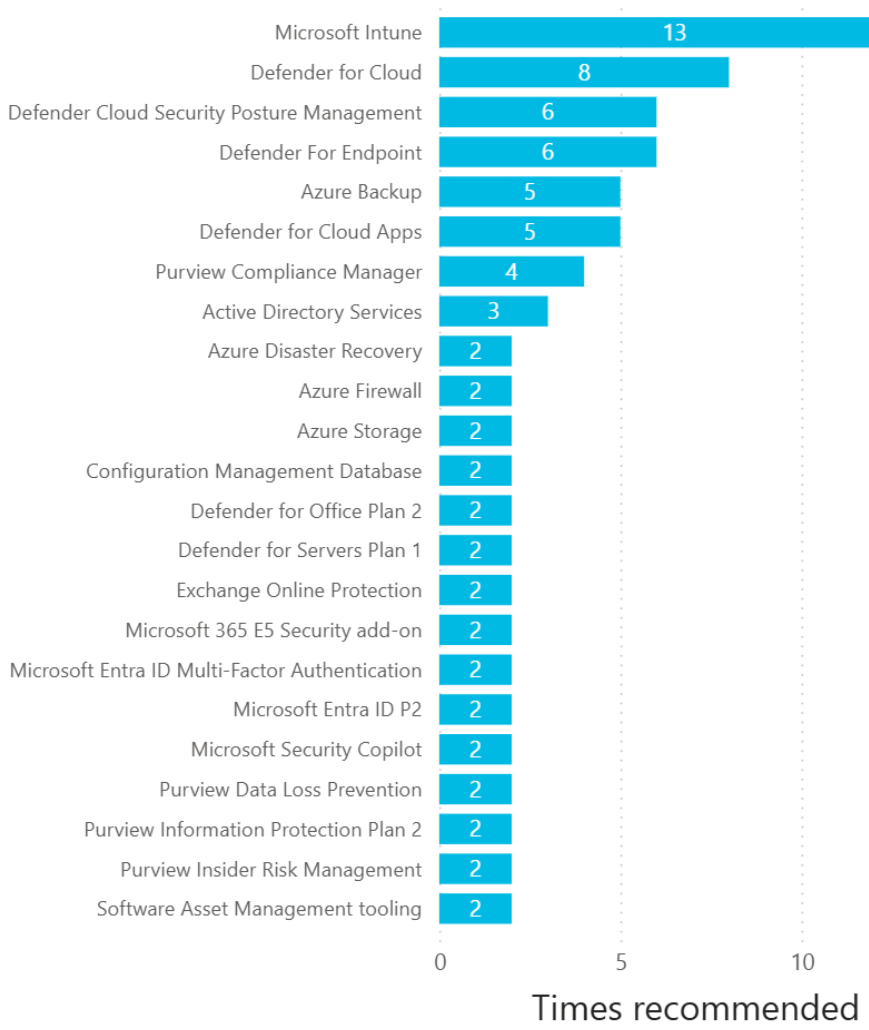





# Software Recommendations

Current | Previous

## Top 10 Advised Software




## Current Microsoft license overview

| Product | Consumed | Available |
|---|---|---|
| POWER BI (FREE) | 96 | 904 |
| MICROSOFT FLOW FREE | 91 | 19909 |
| ENTERPRISE MOBILITY + SECURITY E5 | 1 | 0 |
| MICROSOFT 365 BUSINESS BASIC | 1 | 0 |
| MICROSOFT 365 BUSINESS STANDARD | 1 | 0 |
| Microsoft 365 E5 | 1 | 0 |
| Microsoft_Intune_Suite | 1 | 0 |
| Office 365 Advanced GenThreat Protection (Plan 1) | 1 | 0 |
| Remote_Help_AddOn | 1 | -1 |
| Windows 10 Enterprise E5 | 1 | 0 |
| RMSBASIC | 0 | 2 |
| WINDOWS STORE FOR BUSINESS | 0 | 100 |

## Questionnaire

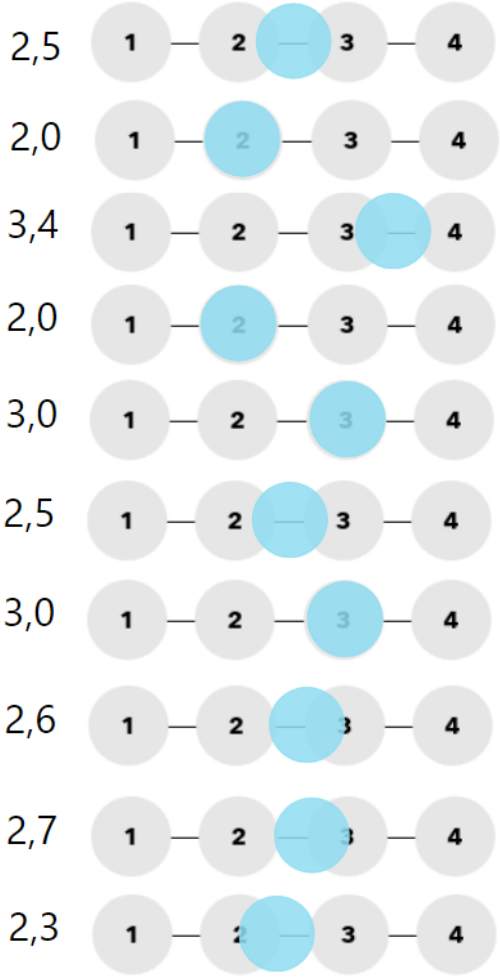
| Category | Topic | Question | Answer | Advice | Advised Product | Risk Score | NIS2 principle |
|---|---|---|---|---|---|---|---|
| CIS v8.1 | 09 | Are email attachments scanned in a sandboxed environment and what is your policy regarding the malicious attachments which are discovered? | Rationalized (3)Inbound emails are scanned for spam using real-time blacklisting and spam rules. File-type blocking and scanning for malware is applied to all email traffic. | Implement tooling to ensure real time phishing attacks are automatically stopped and ensure all attachments are scanned, in a sandboxed environment if necessary. Ensure all unwanted file types are blocked on all incoming and outgoing e-mail. | Exchange Online Protection; Defender for Office Plan 1 | 300 | A2: Risk Management; C2: Proactive Security event discovery; |
| CIS v8.1 | 09 | Are network-based URL filters (incl. DNS filtering) implemented, limiting a system's ability to connect to unapproved websites? | Standardized (2)URL, IP and DNS filters functionalities are being used, but not to the full extent of the IT infrastructure. | Use recommended practices for URL and DNS filters. Automatically updated category-based filters are preferred. All outbound internet traffic should be scanned. Consider to implement a proxy server that supports the recommended capabilities to protect devices that do not have built-in protection. | Defender for Endpoint; Defender for Cloud Apps; Azure Firewall; Microsoft Entra Suite [Microsoft Entra Internet Access] | 500 | B4: System Security; B5: Resilient Network and Systems |

# NIS2 maturity scores backed up by undisputable data

## NIS2 Measures Summary

This overview examines the CIS scores related to NIS2 but is not intended as a compliance score.

| | | |
|---|---|---|
| A | Policies on risk analysis and information security | 2,5 |
| B | Incident handling | 2,0 |
| C | Business continuity, such as backup management and disaster recovery, and crisis management | 3,4 |
| D | Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers | 2,0 |
| E | Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure | 3,0 |
| F | Policies and procedures to assess the effectiveness of cybersecurity risk-management measures | 2,5 |
| G | Basic cyber hygiene practices and cybersecurity training | 3,0 |
| H | Policies and procedures regarding the use of cryptography and, where appropriate, encryption | 2,6 |
| I | Human resources security, access control policies and asset management | 2,7 |
| J | The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate | 2,3 |



# NIS2 areas maturity scores backed up by undisputable data

## NIS2 Measure A

Policies on risk analysis and information security

| | | Score |
|---|---|---|
| 1 | Inventory and Control of Enterprise Assets | 1,0 |
| 2 | Inventory and Control of Software Assets | 1,3 |
| 3 | Data Protection | 1,8 |
| 4 | Secure Configuration of Enterprise Assets & Software | 1,8 |
| 7 | Continuous Vulnerability Management | 1,7 |
| 8 | Audit Log Management | 2,0 |
| 11 | Data Recovery | 3,5 |
| 14 | Security Awareness and Skills Training | 2,0 |
| 15 | Service Provider Management | 1,5 |
| 16 | Application Software Security | 2,0 |
| 17 | Incident Response Management | 2,0 |
| 18 | Penetration Testing | 1,0 |

## NIS2 Measure B

Incident handling

| | | Score |
|---|---|---|
| 8 | Audit Log Management | 2,0 |
| 13 | Network Monitoring and Defense | 1,3 |
| 17 | Incident Response Management | 2,0 |

## NIS2 Measure C

Business continuity, such as backup management and disaster recovery, and crisis management

| | | |
|---|---|---|
| 11 | Data Recovery | 3,5 |
| 17 | Incident Response Management | 2,0 |

## NIS2 Measure D

Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers

| | | |
|---|---|---|
| 8 | Audit Log Management | 2,0 |
| 15 | Service Provider Management | 1,5 |

# Microsoft 365 Copilot readiness security compliance

| Identity & Access Management | Available license | Status |
|---|---|---|
| Login to Microsoft Copilot with a single identity | O365 E3 ☑ M365 E3 ☑ M365 E5 ☑ | |
| Enforce MFA for Microsoft 365 access to use Copilot | O365 E3 ☑ M365 E3 ☑ M365 E5 ☑ | |
| Enable self-service password reset, change, and unlock for Microsoft 365 access | O365 E3 ☑ M365 E3 ☑ M365 E5 ☑ | |
| Implement Conditional Access policies based on identity, device and location for Microsoft 365 access | M365 E3 ☑ M365 E5 ☑ | |
| Enable real-time policy enforcement and instant access revocation for Microsoft 365 | M365 E3 ☑ M365 E5 ☑ | |
| Control access to Microsoft 365 and third-party cloud apps | M365 E5 ☑ | |
| Review access to content in Microsoft 365 - Copilot - to reduce oversharing | M365 E5 ☑ | |
| Require just-enough and just-in-time approval for admin roles managing Copilot app access | M365 E5 ☑ | |

| Endpoint Management | Available license | Status |
|---|---|---|
| Push/deploy the Microsoft 365 apps to devices and grant access to Copilot in these apps | O365 E3 ☑ M365 E3 ☑ M365 E5 ☑ | |
| Manage Microsoft 365 apps updates | O365 E3 ☑ M365 E3 ☑ M365 E5 ☑ | |
| Restrict the use of Microsoft 365, Teams, and Copilot on personal devices | O365 E3 ☑ M365 E3 ☑ M365 E5 ☑ | |
| Prevent saving files, including those generated by Copilot, if a device is lost | M365 E3 ☑ M365 E5 ☑ | |
| Revoke work access in noncompliant devices | M365 E3 ☑ M365 E5 ☑ | |

Legenda: ☑ **Completed** ☑ **Partially completed** ✗ Not completed

# Microsoft 365 Copilot readiness security compliance

| Data Security & Compliance | Available license | Status |
|---|---|---|
| Search Copilot-generated data by content, keyword, apply legal hold, and export search results and investigate incidents and respond to litigation | O365 E3 ☑ M365 E3 ☑ M365 E5 ☑ | |
| Audit logs for Copilot interactions | O365 E3 ☑ M365 E3 ☑ M365 E5 ☑ | |
| Apply a retention policy for Copilot interactions | O365 E3 ☑ M365 E3 ☑ M365 E5 ☑ | |
| Use Data Loss Prevention (DLP) policies to protect sensitive Copilot data in Microsoft 365 locations from exfiltration | O365 E3 ☑ M365 E3 ☑ M365 E5 ☑ | |
| Inherit sensitivity labels and cite them in Copilot output and references | O365 E3 ☑ M365 E3 ☑ M365 E5 ☑ | |
| Prohibit Copilot from summarizing or including data users cannot access in response messages | O365 E3 ☑ M365 E3 ☑ M365 E5 ☑ | |
| Exclude sensitive files without view permission from being processed by Copilot for those users | O365 E3 ☑ M365 E3 ☑ M365 E5 ☑ | |
| Label and protect Microsoft 365 content, used by Copilot | O365 E3 ☑ M365 E5 ☑ | |
| Detect business or code of conduct violations for Copilot prompts and responses | O365 E3 ☑ M365 E3 ☑ M365 E5 ☑ | |
| Prevent Copilot access to content encrypted with Double Key Encryption | O365 E3 ☑ M365 E3 ☑ M365 E5 ☑ | |
| Use ready-to-use machine learning trainable classifiers to identify sensitive information and create custom classifiers | O365 E3 ☑ M365 E3 ☑ M365 E5 ☑ | |

| Threat Protection | Available license | Status |
|---|---|---|
| Discovery and risk evaluation across 400+ AI apps in an organization | M365 E5 ☑ | |
| Ability to block or sanction the use of any discovered AI app in the organization | M365 E5 ☑ | |

# Overview of the full TCO analysis of this case

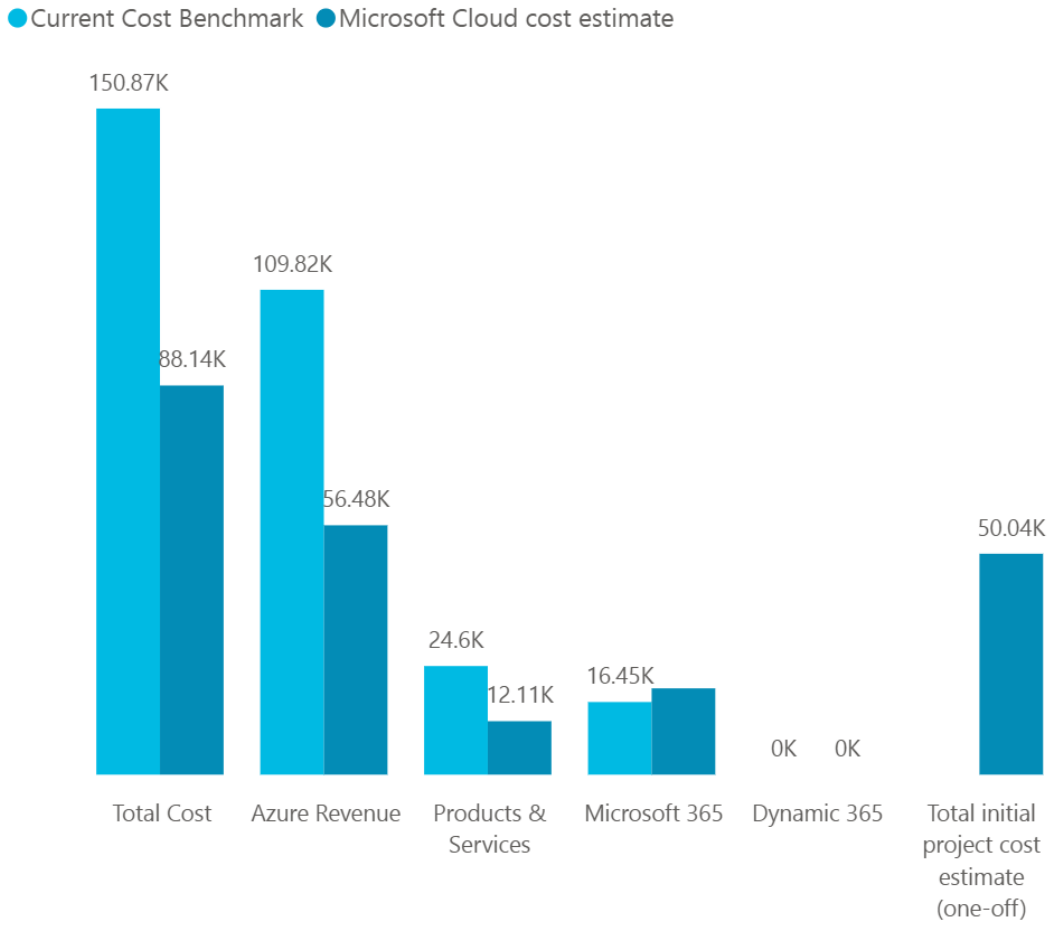
Current | Previous

CSAT conducted a security assessment of the entire infrastructure and based on the findings, an indicative TCO analysis was performed to compare the costs of the current infrastructure with those after migrating to the Microsoft Cloud, including the security upgrade. For more information, contact your partner.

## Revenue Table

| | Category | Currency | Benchmark | Estimate |
|---|---|---|---|---|
| 0 | Azure Revenue | EUR | 109815 | 56481 |
| 1 | • Azure Consumed Revenue | EUR | 101717 | 53310 |
| 2 | + Compute | EUR | 15699 | 10082 |
| 3 | + PAYG Windows Server Licensing | EUR | 151 | 59 |
| 4 | + VDI-AVD/CP | EUR | 5713 | 893 |
| 5 | + Storage | EUR | 4327 | 2073 |
| 6 | + Security | EUR | 4054 | 2140 |
| 7 | + Egress | EUR | 896 | 716 |
| 8 | + PAYG SQL Licensing | EUR | 70878 | 37348 |
| 9 | • License (CSP) | EUR | 8098 | 3171 |
| 10 | + CSP Windows Server Licensing | EUR | 8098 | 3171 |
| 11 | Microsoft 365 | EUR | 16451 | 19550 |
| 12 | + Office: Microsoft 365 | EUR | 6992 | 13242 |
| 13 | + Security | EUR | 9459 | 6308 |
| 14 | Dynamic 365 | EUR | 0 | 0 |
| 15 | + AX/CRM: Dynamics 365 | EUR | 0 | 0 |
| 16 | Products & Services | EUR | 24603 | 12111 |
| 17 | + Managed Services | EUR | 24603 | 12111 |
| 18 | Total Cost | EUR | 150869 | 88142 |
| 19 | Total initial project cost estimate (one-off) | | | 50035 |

## Holistic TCO Business Case Summary (Monthly)

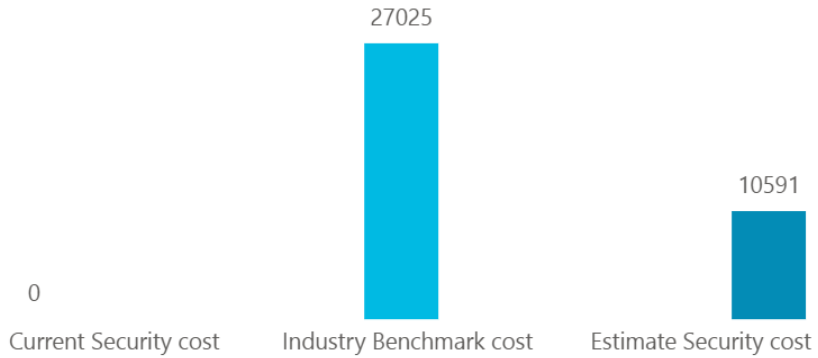


# Security TCO

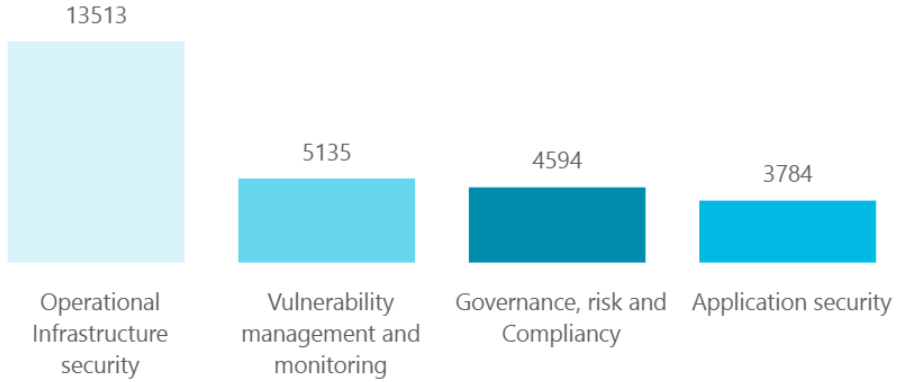
The objective of the CSAT recommendations is to increase the CIS maturity score of the current security environment to a value above 3. In this security TCO, a comparison is made between benchmark costs of companies that have reached such maturity levels with the security costs when the current security environment is migrated to the Microsoft Cloud.

Current | Previous

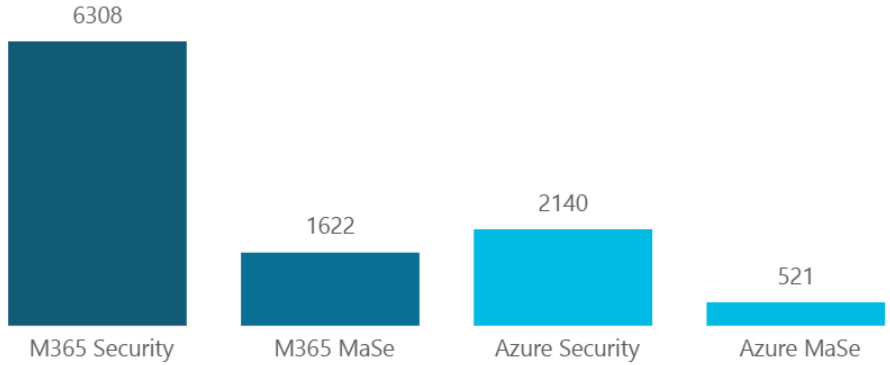
## Security TCO Analysis (monthly cost) EUR



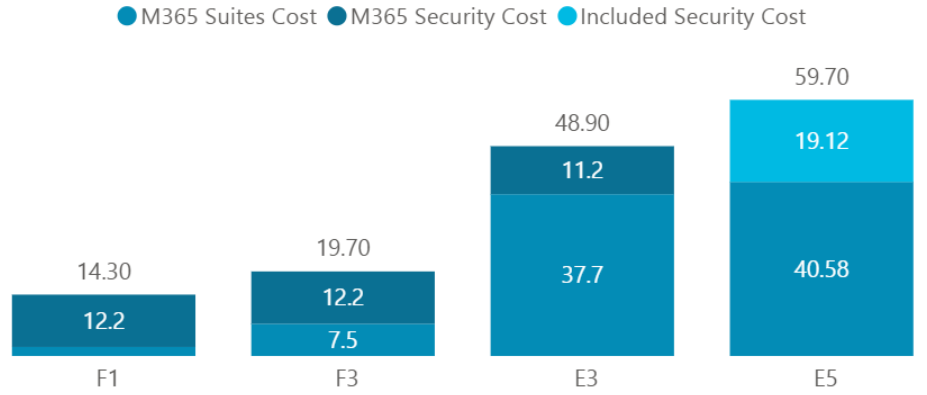

## Breakdown of the industry benchmark monthly security cost EUR



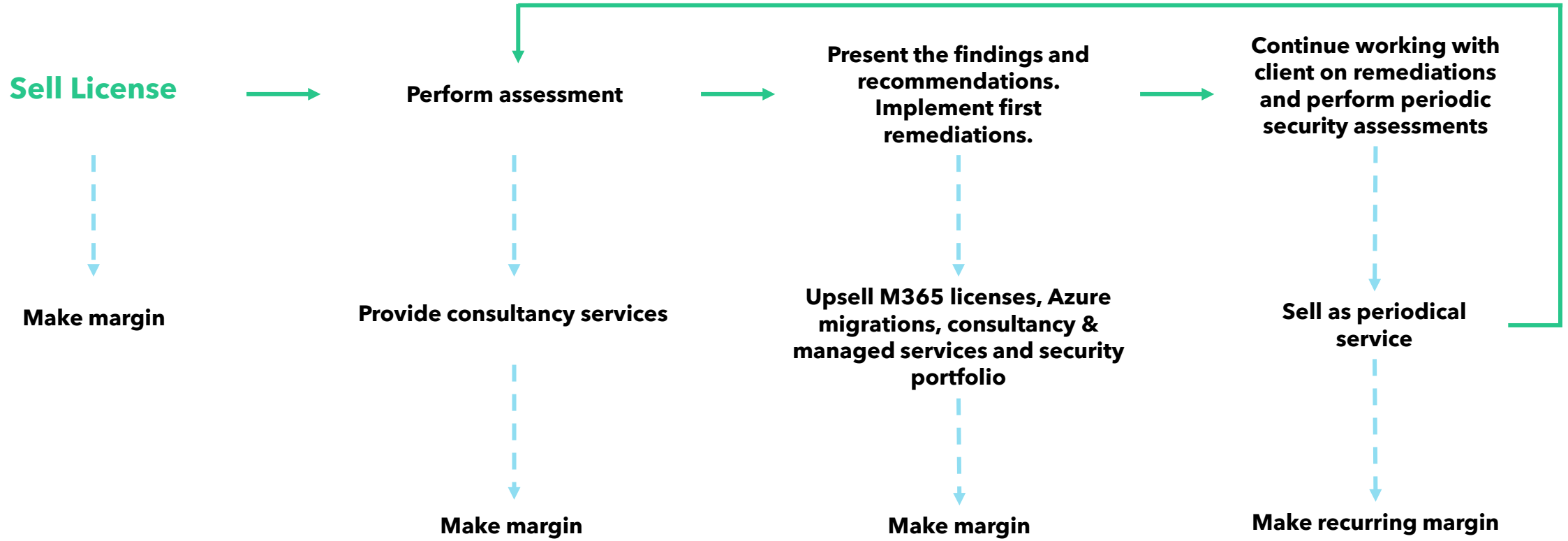

## Security Cost Summary (monthly cost) EUR




## Full price per user-type (monthly) EUR



# Sell 1st Security Health Check to jump into recurring revenue journey with the same client



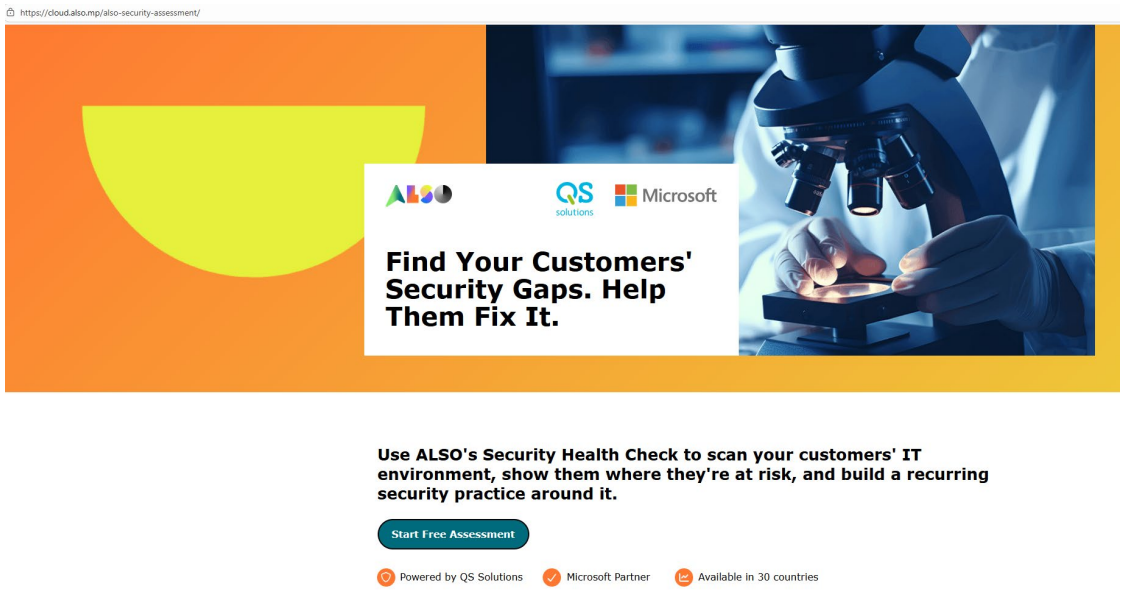

## High ROI

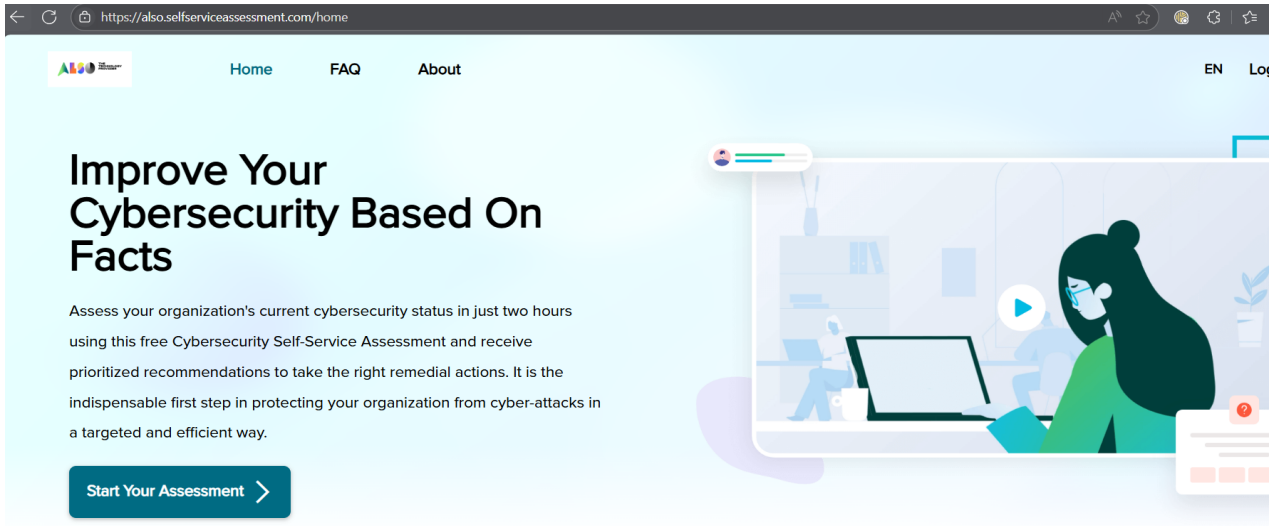
- ✓ Low investment in licenses
- ✓ Attractive subscription model to help grow managed services revenue
- ✓ High ROI in all segments; Enterprise, Corporate, Top SMB and SMB

# Value of Security Health Check

| For Customer | For Partner |
| --- | --- |
| • **Alignment** in between IT/Security and Business Managements.<br>• **Saves time, effort** and **budget** by focusing on what is urgent and relevant.<br>• Provides the **data-based evidence** required for regulations like NIS2. | • **Saves time** by providing automated investigations, reports and recommendations.<br>• Builds **strong relationship and trust** with customer<br>• **Creates opportunities** to upsell or/and deploy licenses, products and services.<br>• Third-party proof that the client needs to **upgrade licenses.** |

# Security Health Check with ALSO Self-Service Assessment




- **Fully self-service** via a web portal - no support needed
- **Easy to execute** and doesn't take a lot of time of a customer
- **Scan** for limited **datasets with most value**:
  - On-prem
  - Microsoft Cloud
- Easy to answer **questionnaire**
- Customer gets an **evaluation report**
- Partner gets a **qualified lead** hungry for more

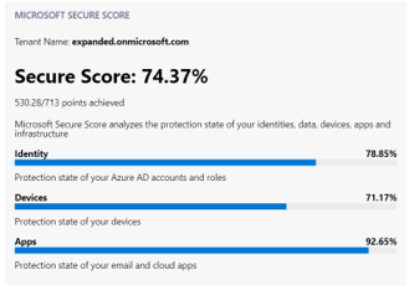
# Reports

## Microsoft and Azure Secure Score

The Microsoft Secure Score looks at multiple items within the Microsoft 365 and Azure environments. The score is based on the type of services being used in Microsoft 365 and compares them to a baseline established by Microsoft. The score shows in what level you are aligned with the best security practices. In the Self Service Essential assessment report you will find the recommendations to improve the scores.

### Microsoft Secure Score

The retrieved Microsoft Secure Score is as follows:




### Microsoft Defender for Cloud Secure Score

The retrieved Azure Secure Score is as follows:




## Assessment score

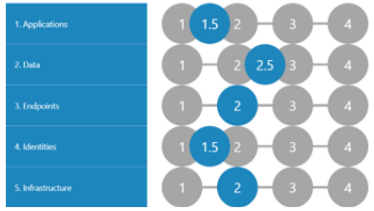
The overall assessment score is calculated based on the self-service assessment data collected in the assessment. The company score is shown below.




The score can be broken down into five topics. These topics are:

- **Applications** are the programs installed on your machines
- **Data** are for example e-mails and documents that are saved within the company
- **Endpoints** are for example the laptops, mobile phones and servers
- **Identities** are accounts that either people or workloads are using
- **Infrastructure** are all the services necessary to operate and manage IT services

The score for the individual topics from the self service assessment are shown below




The scores you see above are based on the following principle.

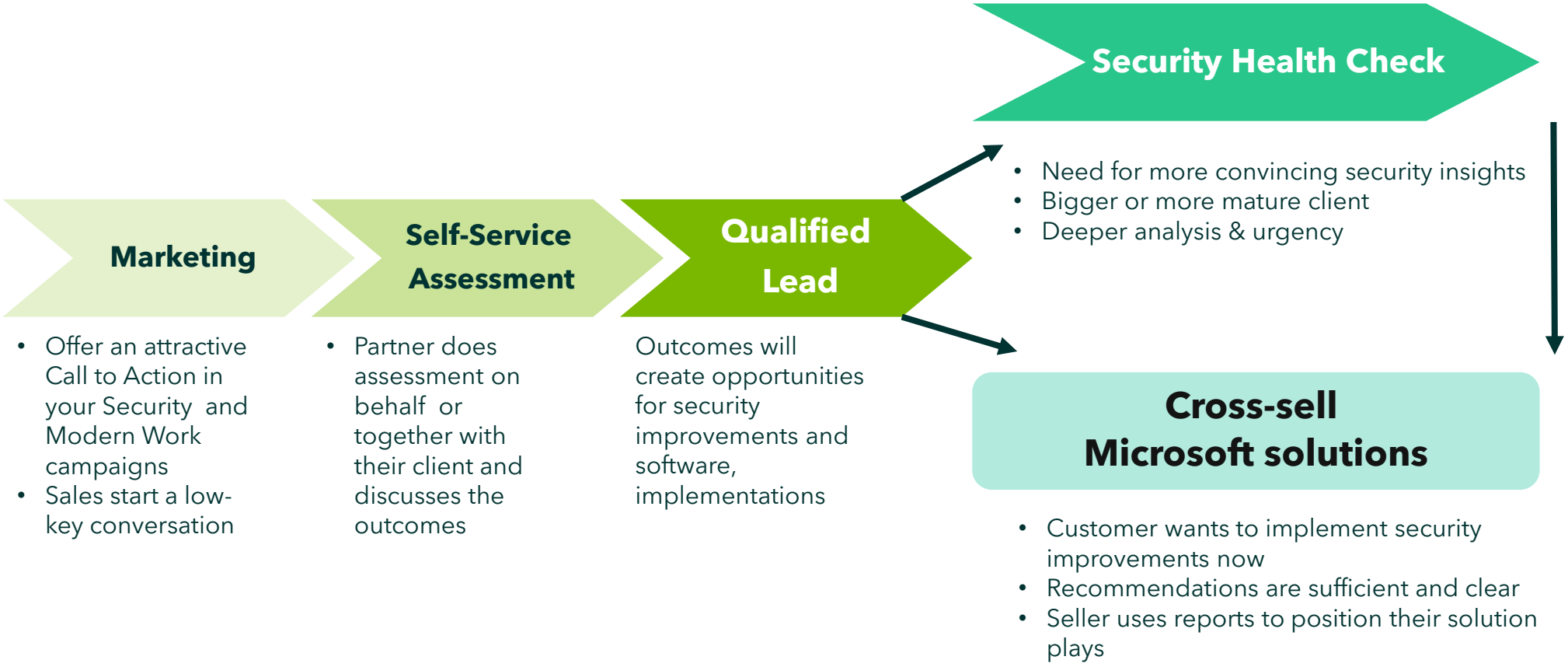



| High | | | | | |
|---|---|---|---|---|---|
| **Topic** | **Question** | **Answer** | **Advice** | **Advised Products** | **ZTA Zone** |
| 1. Applications | Do you have an inventory of all the used software in the company? | No | Implement a process to inventory the software used by the company both on-premises and cloud applications. | Software Asset Management [SAM] tooling; Microsoft Defender for Cloud Apps; Defender for | 2, 3, 5 |
| 2. Data | Is the data on the company devices (servers, laptops, mobile devices) encrypted? | No | Enable the built-in hardware encryption features of devices. For efficiency reasons, it is preferable to deploy and manage these settings with tooling. | Windows 10/11 BitLocker; Microsoft Endpoint Manager; Azure Storage; Microsoft Defender for Cloud; Defender for Endpoint Device Control; Customer Key | 2, 3 |

# Security Healthcheck Assesment Types

| | **Self Service** (2hrs) | **QuickScan** (1 day of consulting) | **FullScan** (3 days of consulting) |
|---|---|---|---|
| **TARGET GROUP** | SMB, Corporate-scale, Corporate | SMB (Up-to 300 employees) | Enterprise, Corporate and Top SMB; SMB with a higher need for security |
| **BASED ON** | **Light security assessment** which provides enough value for small SMB customers (<50 seats)<br><br>Based on a limited number of controls of the **Zero Trust Architecture** | **Quick check on the cybersecurity hygiene**<br><br>Based on the **CIS controls Implementation Group 1** | **Comprehensive cybersecurity assessment**<br><br>Based on the **CIS controls Implementation Group 1, 2, 3** |
| **OUTCOMES OF THE ASSESSMENT** | Upsell to<br>• Microsoft's Security solutions in M365 and Azure.<br>• Deeper Security Health Check Assessment<br>• Generate leads for full-service assessments | Upsell to<br>• Microsoft 365 Business Premium<br>• Azure migrations and Azure Consumption<br>• Consumed revenue by adding Azure Security<br>• Other security services | Upsell to<br>• Microsoft 365 E3+E5<br>• Sentinel<br>• Azure migrations and Azure Consumption<br>• Consumed revenue by adding Azure Security<br>• Other security services |
| **SCAN SOURCES IN SCOPE** | • Manual Endpoint Scan of Windows OS<br>• Local Active Directory<br>• Email DNS check<br>• Limited datasets of Microsoft 365 environment<br>• Limited datasets from the Azure tenant<br>• Questionnaire on basic security controls – no official framework<br><br>*Note: only analyzed and aggregated data is saved in the self-service platform. Assessment reports do not provide insights into details.* | • Basic Automated Endpoint Scan<br>• Local Active Directory<br>• Email DNS check<br>• Microsoft 365 environment<br>• Limited datasets from the Azure tenant<br>• Checked against CIS IG1 (basic security hygiene controls) | • Comprehensive Automated Endpoint Scan including Linux machines and network devices<br>• Local Active Directory<br>• Email DNS check<br>• Microsoft 365 environment<br>• Comprehensive scan of the Azure tenant<br>• SharePoint on-premises<br>• Google Workspace and AWS included<br>• Checked against the full CISv8 controls |

# GTM approach



# Examples of potential ROI

**On-prem client with 400 seats upgrading to Microsoft 365 E3 including first Azure Migration**

| Generated sales pipeline with FullScan | 400 seats |
|---|---|
| Security Health Check Services (Annual) | € 4,000 |
| Purchase Microsoft 365 E3 licenses (Annual) | € 190,000 |
| Azure Consumed Revenue (Annual) | € 16,000 |
| Implementation Services (One-Time) | € 60,000 |
| Managed Services (Annual) | € 16,000 |
| Potential revenue per year | **€ 286,000** |

**On-prem client with 100 seats upgrading to Microsoft 365 Business Premium including first Azure Migration**

| Generated sales pipeline with QuickScan | 100 seats |
|---|---|
| Security Health Check Services (Annual) | € 1,500 |
| Purchase M365 Business Premium licenses (Annual) | € 24,700 |
| Azure Consumed Revenue (Annual) | € 4,000 |
| Implementation Services (One-Time) | € 15,000 |
| Managed Services (Annual) | € 4,000 |
| Potential revenue per year | **€ 49,200** |

**M365 E3 client with 400 seats upgrading to M365 E5 including first Azure Migration**

| Generated sales pipeline with FullScan | 400 seats |
|---|---|
| Security Health Check Services (Annual) | € 4,000 |
| Purchase Microsoft 365 E5 licenses (Annual) | € 274,000 |
| Azure Consumed Revenue (Annual) | € 16,000 |
| Implementation Services (One-Time) | € 60,000 |
| Managed Services (Annual) | € 16,000 |
| Potential revenue per year | **€ 370,000** |

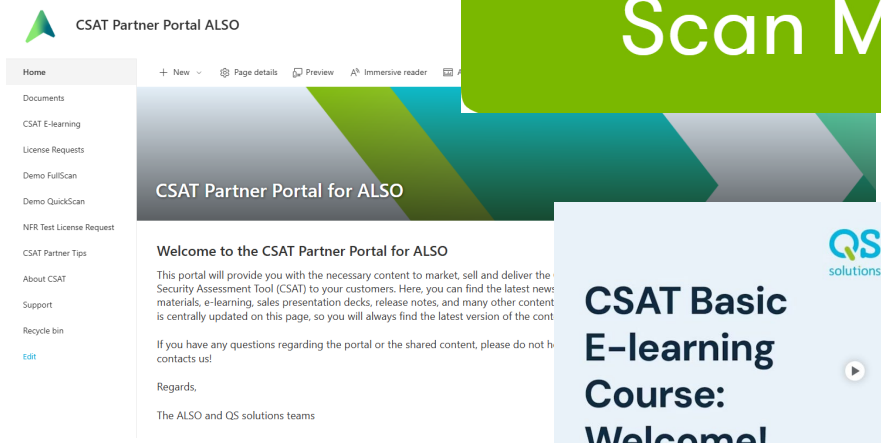
**M365 Basic client with 100 seats upgrading to M365 Business Premium including first Azure Migration**

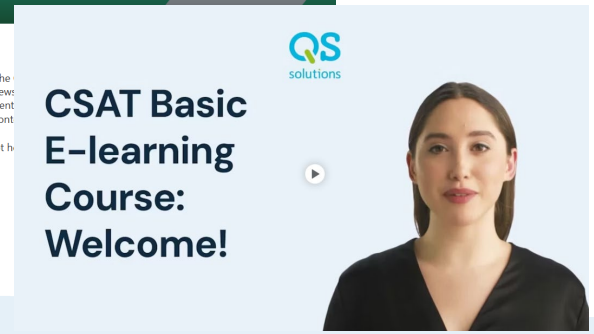
| Generated sales pipeline with QuickScan | 100 seats |
|---|---|
| Security Health Check Services (Annual) | € 1,500 |
| Purchase M365 Business Premium licenses (Annual) | € 22,000 |
| Azure Consumed Revenue (Annual) | € 25,000 |
| Implementation Services (One-Time) | € 25,000 |
| Managed Services (Annual) | € 7,000 |
| Potential revenue per year | **€ 80,500** |

# Next Steps:

1. Check FREE ALSO Self-Service Assessment
2. 1-on-1 introduction call to get you started
3. Complete Certification
4. Test Assessment in your own environment
5. First Customer Assessment

Scan Me



# Thank you!
# Reach out for more information



**Daria Barsukova**
Global Partner Manager
dariab@qssolutions.nl
linkedin.com/in/dariabarsukova/

# Relevant Links

- ALSO Landing Page
- QS Solutions x ALSO Landing Page
- QS Solutions x ALSO FAQs