BEYONDSOFT®
beyond your expectations

Advanced Cloud Protection

We're accelerating your business goals

Let us help you #FutureProofYourBusiness

Beyondsoft

Who are we

30 years
delivering solutions to customers around the world

30,000+
Experts worldwide

10+
International 45 offices

3,000+
Customers

1,500+
Copyrights and patents

70
Delivery centers

~$1B
Revenue in 2022

Microsoft Solutions Partner
Infrastructure
Azure

Specialist
Windows Server and SQL Server
   Migration
Azure Virtual Desktop

Microsoft Solutions Partner
Modern Work

Microsoft Solutions Partner
Data & AI
Azure

Specialist
Infra and Database Migration

Microsoft Solutions Partner
Security

Specialist
Cloud Security
Identity and Access
   Management
Information Protection and
   Governance
Threat Protection

Microsoft Solutions Partner
Digital & App Innovation
Azure

Advanced Cloud Protection

Why invest in Advanced Cloud Protection?

Investing in cloud protection is essential due to the increasing reliance of businesses on cloud computing for storing sensitive data and running critical applications. As more organizational assets move to the cloud, they become potential targets for cyber attacks. Cloud environments face unique security challenges, such as data breaches, unauthorized access, and compromised credentials, which can lead to significant financial losses, reputational damage, and legal repercussions, especially with stringent data protection regulations in place. Main challenges today are:

Extended Detection and Response (XDR)

XDR aims to provide a comprehensive security posture by integrating various data sources like endpoints, networks, cloud, and email. The main challenge here is effectively integrating and correlating data from these disparate sources.

Security Information and Event Management/Security Orchestration, Automation, and Response

SIEM/SOAR systems are indispensable for real-time analysis and management of security alerts, enabling organizations to efficiently orchestrate response and automate security workflows, thus reducing the time to respond to incidents.

Identity and Access Management

One of the main challenges in IAM is achieving the right balance between robust security measures and user convenience. Organizations need to ensure that security measures do not become a barrier to efficient workflow while still maintaining a high level of security against unauthorized access.

Device Management

With the rise of remote work and BYOD, managing and securing a diverse range of devices across different locations is a significant challenge. The heterogeneity of device types, operating systems, and user environments adds complexity to device management, requiring flexible yet robust security and management solutions.

What We Do

We provide hands-on assistance with onboarding and setting up the optimal configuration for Microsoft Security solutions.

Microsoft Defender XDR

Defender for Endpoint.
Defender for Identity.
Defender for Office 365.
Defender for Cloud Apps.

CIS Security Assessment

Microsoft Azure Foundations Benchmark.
Microsoft 365 Foundations Benchmark.

Mincrosoft Intune

Cross-platform endpoint management. Mobile application management. Configuration, compliance, security and App Policies.

Microsoft Sentinel

Log integration with Defender XDR and Microsoft 365. Workbooks and playbooks deployment. Alerts and cost management.

Microsoft Entra ID

Conditional access, single sign- and MFA. Self-service password reset, access reviews, identity protection and privileged identity management.
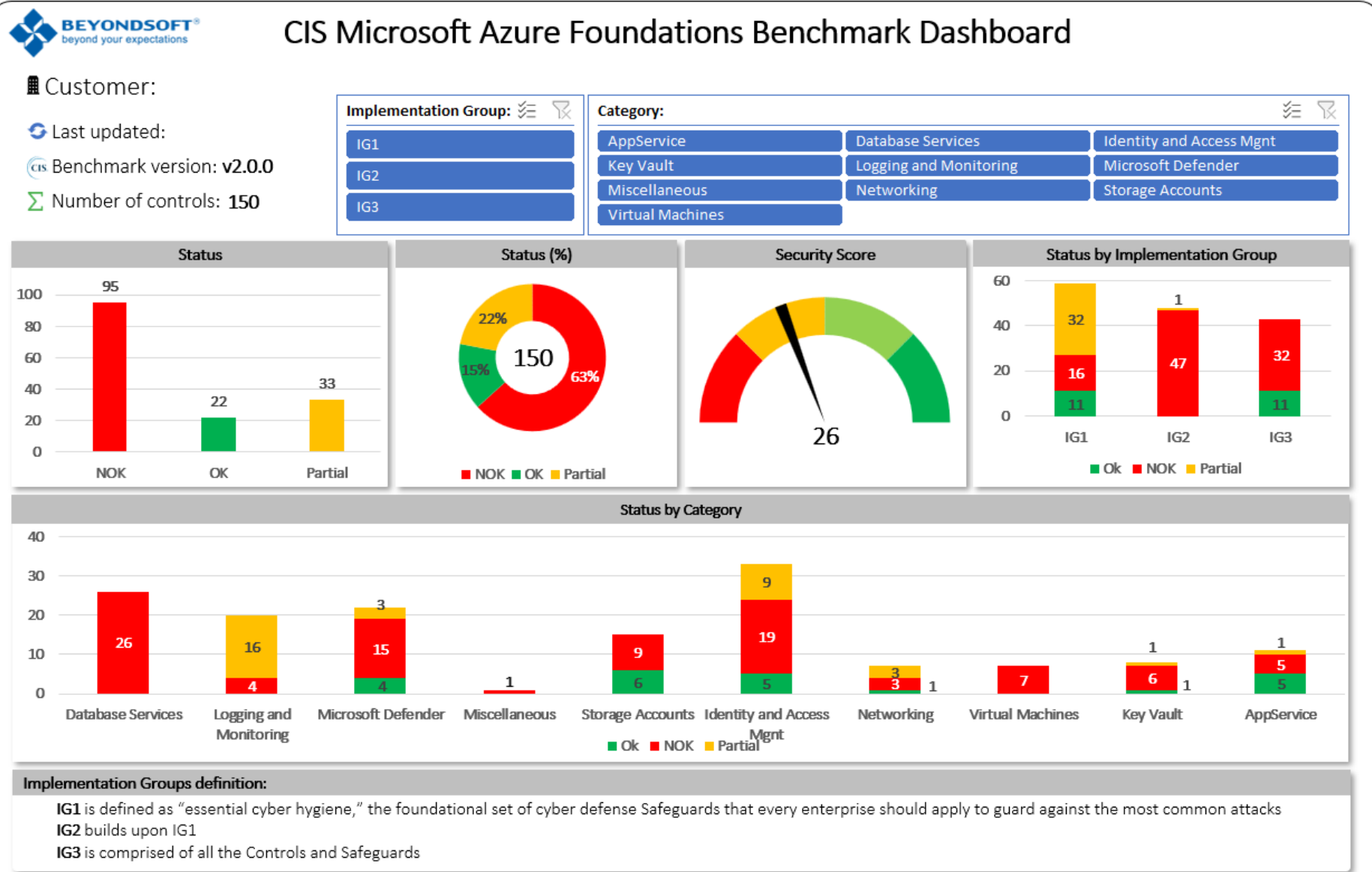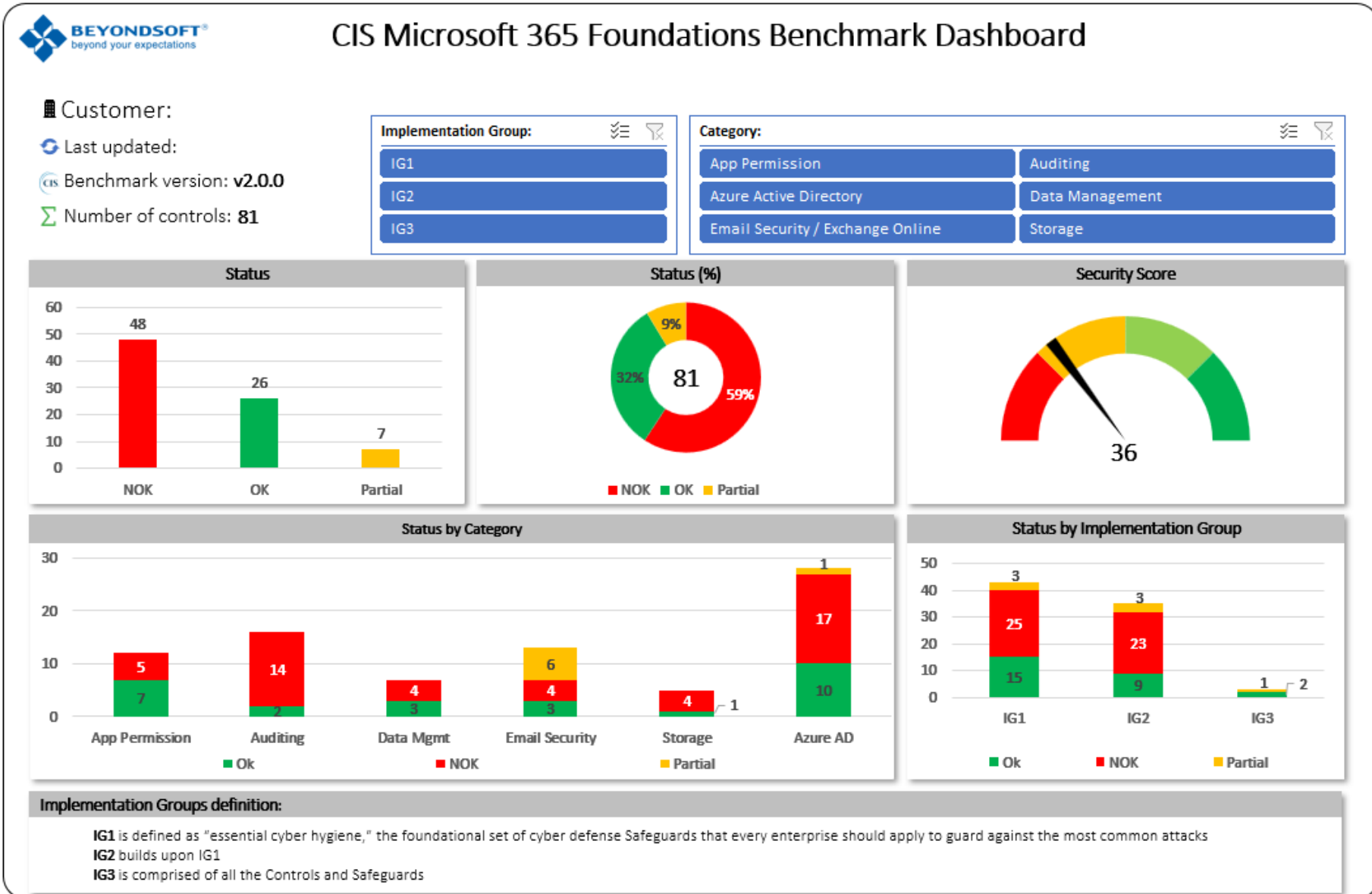
CIS Microsoft Azure Foundations Benchmark

CIS Microsoft Azure Foundations Benchmark Dashboard

CIS Microsoft 365 Foundations Benchmark

Implementation Plan

Phase 1	Phase 2	Phase 3	Phase 4

1 Week

3 Weeks

3 Weeks

1 Week

Assessment

Planning

Deployment

Onboarding users & devices

Fine Tuning

Admin Workshops
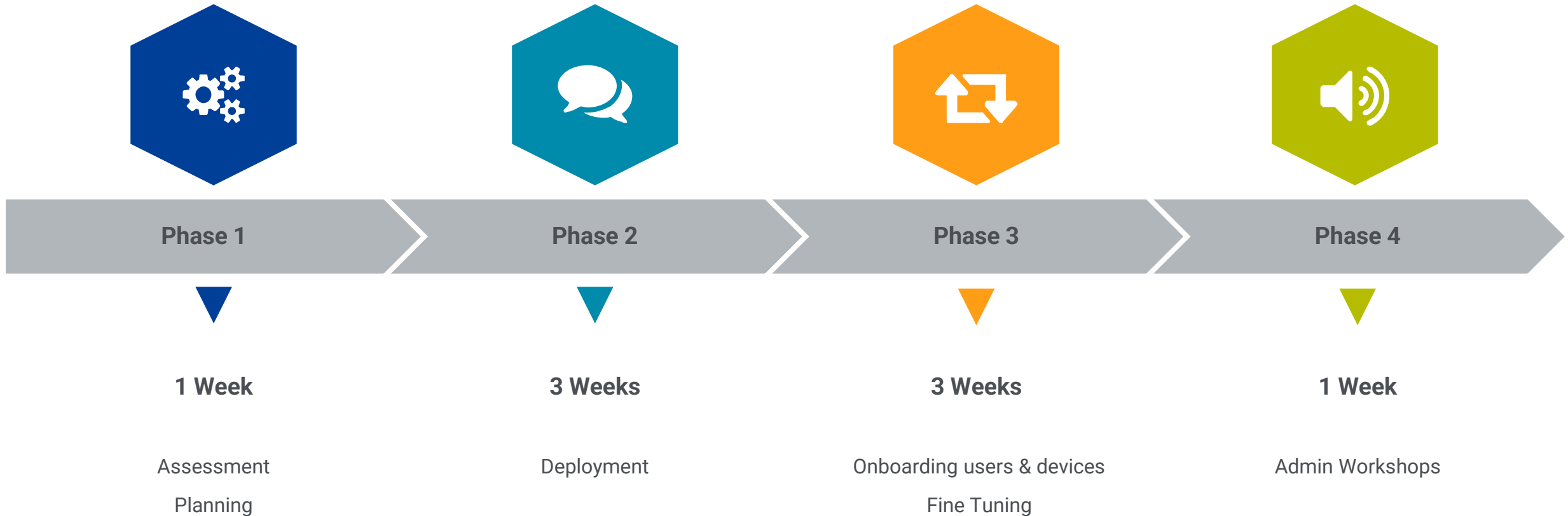
Implementation Benefits

Deployment services

Leverage Beyondsoft´s global experience for a rapid and smooth implementation of Microsoft XDR and Zero Trust solutions.

Improved security posture

Prevent, detect, and respond to threats across your endpoints, networks, cloud applications, emails, identities, and data.

Reduced costs

Cloud-based offers flexible pricing models that can lower the total cost of ownership compared to traditional security solutions.

Greater business agility

Enable your organization to securely adopt new technologies, such as remote work, BYOD, IoT, and multicloud, without compromising their security
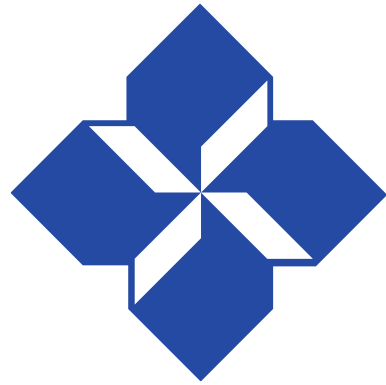

Increased efficiency

Microsoft XDR and Zero Trust solutions leverage automation, AI, and machine learning to provide faster and more accurate threat detection and response.

Let us help you to #FutureProofYourBusiness