Beyondsoft Advanced Cloud Protection with Microsoft XDR and Zero Trust Deployment: 8-Week Implementation

Beyondsoft will deploy a collection of best of breed solutions from Microsoft to address security challenges regarding Extended Detection and Response (XDR), Security Information and Event Management (SIEM/SOAR), Identity and Access Management and Device Management.

What are Beyondsoft Advanced Cloud Protection Services?

Our Deployment services help you get the most out of your Microsoft investment. We provide hands-on assistance with onboarding and setting up the optimal configuration for your specific Microsoft Security solutions. Our goal is to ensure a smooth and fast implementation that meets your security needs.

We will analyze your environment and conduct two **CIS Security Assessments**: one for Microsoft Azure and one for Microsoft 365. Based on the results, we will work with you to configure and deploy Microsoft Solutions to a pilot group of users, devices, and servers.

Our Microsoft certified experts will help you overcome various security challenges with Microsoft's top-notch solutions. These solutions cover **Extended Detection and Response (XDR)**, **Security Information and Event Management (SIEM/SOAR)**, **Identity and Access Management**, and **Device Management**. You will get comprehensive protection for endpoints, email, identities, and cloud apps with **Microsoft Defender XDR**. You will also get a cloud-native SIEM/SOAR solution that collects, analyzes, and responds to security threats across your hybrid environment with **Microsoft Sentinel**. Moreover, you will get a cloud-based identity and access management service that enables secure sign-in, multi-factor authentication, and identity governance for your users and applications with **Microsoft Entra ID** (formerly Azure Active Directory). Finally, you will get a cloud-based service that helps you manage and secure your mobile devices, apps, and data with **Microsoft Intune**.

What does the Beyondsoft Advanced Cloud Protection service include?

An initial cybersecurity assessment based on the CIS Foundations Benchmark V.2 for Microsoft Azure and Microsoft 365 will be performed. Then the following Microsoft solutions will be configured for your organization and up to 100 users, devices and servers will be onboarded across these solutions.

- **Microsoft Sentinel.**
  - Log integration with Microsoft 365 Defender.
  - Standard Connectors for other data sources.
  - Alerts management.
  - Workbooks deployment.
  - Playbooks deployment.
  - Cost optimization management.
- **Defender for Endpoint.**
  - Endpoint detection and response.
  - Automated Investigation and Response.
  - Next-generation protection.
  - Attack surface reduction.
  - Mobile Cyberthreat Protection.
  - Core Vulnerability Management.
  - Device Discovery.
  - Device Inventory.
  - Foundational CSPM
- **Defender for Identity.**
  - Identity threat detection.
  - Identity threat investigation.
  - Identity threat response.
  - Identity security posture.
- **Defender for Office 365.**
  - Safe Attachments.
  - Safe Links.
  - Advanced Anti-phishing.
  - Impersonation Protection.
- **Defender for Cloud Apps.**
  - Cloud Discovery.
  - Information Protection.
  - Data Loss Protection.
  - Threat Detection.
  - Conditional Access App Control.
- **Microsoft Entra ID.**
  - AD Connect and single sign-on.
  - Multifactor authentication.
  - Conditional access.

- Identity protection.
- Access reviews.
- Self-service password reset.
- Privileged identity management.
- **Microsoft Intune.**
  - Mobile Device Management (MDM) for Windows, iOS and Android.
  - Mobile Application Management (MAM) for BYOD devices.
  - Integration with Microsoft Defender for Endpoint.
  - Configuration Policies.
  - Compliance Policies.
  - Application Management.
  - Windows Autopatch.
  - Windows Autopilot.
  - Windows BitLocker.

Overall Project Outline:

- One-week Cybersecurity assessments and Planning Phase.
- Three-week Deployment Phase.
- Three-week Onboarding and Fine-Tuning Phase.
- One-week Knowledge Transfer with Security Administration Workshops

Additional Details:

- All terms, conditions, final scope and pricing are custom to each engagement and must be accepted before start of engagement.
- Up to 100 devices can be onboarded across all solution deployed.

Customer Requirements:

- Paid or trial licenses of all products related to this offer.
- Supply computers and mobile devices for onboarding Intune.
- Azure costs when applicable.