Solution Brief

BlueVoyant's MXDR for Microsoft Onboarding Service

Implementation and optimization of Microsoft Sentinel and Defender XDR for BlueVoyant Managed XDR (MXDR) service

Is your Microsoft Sentinel + Defender XDR optimally deployed?

Properly implementing and optimizing a SIEM plus XDR strategy using Microsoft Sentinel and Defender XDR while operating a 24×7 Security Operations Center (SOC) is challenging. It requires converging and streamlining multiple security tools to function as a cohesive system. Cross-source data correlation is essential for detecting sophisticated multi-vector threats before they mutate, establish lateral movement, and evade detection. Successful SIEM and XDR integration demands specialized expertise to optimize resource allocation and prevent the introduction of security gaps or hidden vulnerabilities.

BlueVoyant's MXDR for Microsoft Onboarding Service provides Microsoft-certified expert deployment of Microsoft Sentinel and Defender XDR for onboarding readiness of BlueVoyant Managed XDR (MXDR) service. Our approach begins with comprehensive environmental assessment, followed by expert-led system hardening and baseline configuration, utilizing BlueVoyant's extensive library of proprietary playbooks and detection rules. It includes a detailed assessment of your risks, guidance on how to best leverage Microsoft Sentinel and Microsoft Defender XDR with E5/A5//G5 license. That can include implementation and configuration assistance to best meet the requirements of your unique environment.

Based on your business needs, you may choose from a Standard or Premium deployment offering. Additionally, this service will be used as part of your BlueVoyant Managed XDR (MXDR) service for Microsoft onboarding.

Delivered Outcomes

> Apply best practices from 1,000+ global deployments to effectively deploy your optimized configuration

> Apply BlueVoyant's IP to expertly reduce log ingest costs by 30% or more

> Access and activate key log sources to improve MXDR detection and investigation

> Utilize over 350 pre-built data connectors and 1,000 analytic rules to expedite deployment

> Converge Microsoft Defender XDR and Microsoft Sentinel into a unified solution

BlueVoyant

Features

Microsoft Sentinel Deployment

We assess your current SIEM, Azure tenancy, and security controls, identify key log sources, and establish a project timeline. Our experts then customize and tune data connectors, tailor analytic rules, and develop data visualizations with BlueVoyant Workbooks, which are complemented by response automation using BlueVoyant playbooks.

Microsoft Defender XDR Deployment

Deployment and implementation of security features within the Microsoft Defender XDR product suite, which are included in the Microsoft 365 E5/A5 & G5 Security licenses. This includes Defender for Endpoint; Defender for Identity; Defender for Office 365; Defender for Cloud Apps; Microsoft Entra ID Identity Protection and Microsoft Entra ID Password Protection.

CIS-Based Maturity Workshop

Includes four phases:

1. Brief overview of where we have been and where we are headed in cybersecurity
2. Illustrations of how various factors influence risk
3. Review of our expert approach to identifying key cyber strengths and vulnerabilities
4. An exercise to clarify your strengths and vulnerabilities, resulting in a findings and recommendations report

BlueVoyant Defender Assessment

Function app deployed in your Azure tenant that utilizes existing Microsoft tools to weekly evaluate your Secure Score and detailed configuration data.

Feature	BlueVoyant MXDR for Microsoft Standard Deployment	BlueVoyant MXDR for Microsoft Premium Deployment
Microsoft Sentinel Deployment		✓
Microsoft Defender XDR Deployment	✓	✓
CIS-Based Maturity Workshop	✓	✓
BlueVoyant Defender Assessment	✓	✓

Maximize your Microsoft Security investment

Start here.

BlueVoyant delivers a comprehensive cloud-native security operations platform that provides real-time threat monitoring for networks, endpoints, and supply chains, extending to the clear, deep, and dark web. The platform integrates advanced AI technology with expert human insight to offer extensive protection and swift threat mitigation, ensuring enterprise cybersecurity. Trusted by more than 1,000 clients globally, and the 2024 Microsoft Worldwide Security Partner of the Year, BlueVoyant sets the standard for modern cyber defense solutions.

BlueVoyant