Datasheet

Microsoft Sentinel Deployment Service - Enterprise

What are BlueVoyant Deployment Services?

With BlueVoyant's Microsoft Security Deployment Services, you don't need to be an expert to take your security and compliance posture to the next level. Our Deployment Services are designed to get you up and running quickly and to maximize your investment in Microsoft with hands-on services that include onboarding and baseline configuration services for the implementation of specific Microsoft Security solutions.

BlueVoyant will perform a detailed analysis of your environment(s) and provide actionable security insights leveraging the BlueVoyant catalog of pre-built playbooks and alert rules. The service includes a detailed assessment of your risks, guidance on how best to leverage Microsoft-powered solutions, and/or deployment and configuration assistance to best meet the requirements of your unique situation. The services are delivered by BlueVoyant Microsoft certified experts who specialize in Microsoft 365 Defender, Microsoft Defender for Cloud, and Microsoft Sentinel.

What does the Microsoft Sentinel Deployment Service for Enterprise service include?

Onboarding of the following Microsoft log sources into Microsoft Sentinel are included, as they are free of charge from Microsoft. An additional log source, Microsoft Entra ID - SignIn logs, is also included. While this log source is billable by Microsoft, it has a low volume.

- Azure Activity Logs
- Office 365
- Defender for Endpoint*
- Defender for Office 365*
- Defender for Identity*
- Defender for Cloud Apps*
- Microsoft Entra ID
- Entra ID (Azure) Identity Protection
- Microsoft Defender for Cloud*

*Alerts Only

The Microsoft Sentinel Deployment Services for Enterprise is enterprise-ready to onboard a variety of vendor security software and technologies. In addition to the included sources above, you may select any other Log Source Types, as long as they are in BlueVoyant Data Connectors Library. Types of suggested logs:

- Infrastructure logs (via Syslog/CEF with Log Collector)
- Other Cloud Logs (i.e., AWS Cloudtrail, GCP)
- SaaS applications (i.e., SalesForce, GSuite)
- Non-Microsoft Endpoint Security tools (i.e., Crowdstrike, McAfee)
- Other Security Controls (PAM/PIM solutions, DLP, NAC)
- Azure PaaS
- Windows Events; Security Events

Following setup, BlueVoyant will conduct a cost analysis and optimization workshop as well as a knowledge transfer exercise related to queries and Azure Functions.

Key Services Delivered

- Connector Configuration: BlueVoyant will onboard customer log sources into Microsoft Sentinel for both on-premises and Cloud devices
- Deployment of Alert Rules from the BlueVoyant catalog
- Microsoft Sentinel Cost Analysis and Optimization
- Deployment of a set of three (3) playbooks for Microsoft Sentinel in customer's Microsoft Sentinel subscription
- Customized Playbook automations via Azure LogicApps
- ITSM Integration via playbooks/email
- Customization of Workbooks to customer requirements
- Knowledge Transfer: Introduction to KQL and Azure Functions
- Develop additional custom content included in scope
- New Data Connectors, as required

Why Clients Choose BlueVoyant for Microsoft

Delivery Expertise

Hundreds of Sentinel deployments, battle-tested processes, and proprietary IP to quickly deploy and configure security solutions.

Increased security and visibility

Powered by our team of security experts, massive library of proprietary alert rules, Threat Intelligence, Automation and AI capabilities.

Data Privacy and Cost Optimization

Our customers keep security data in their own environment, ensuring stronger compliance and reducing cost.

About BlueVoyant

- Winner - Security MSSP of the Year in the Microsoft Security Excellence Awards for 2023
- Winner - 2023 and 2022 Microsoft US Security Partner of the Year
- Winner - 2021 Microsoft Security 20/20 Partner Awards for "Top MDR Team"
- Microsoft MXDR Verified Partner

BlueVoyant combines internal and external cyber defense capabilities into an outcomes-based cloud-native platform by continuously monitoring your network, endpoints, attack surface, and supply chain, as well as the clear, deep, and dark web for threats. The full-spectrum cyber defense platform illuminates, validates, and quickly remediates threats to protect your enterprise. BlueVoyant leverages both machine-learning-driven automation and human-led expertise to deliver industry-leading cybersecurity to more than 900 clients across the globe.

To learn more about BlueVoyant, please visit our website at **www.bluevoyant.com** or email us at **contact@bluevoyant.com**