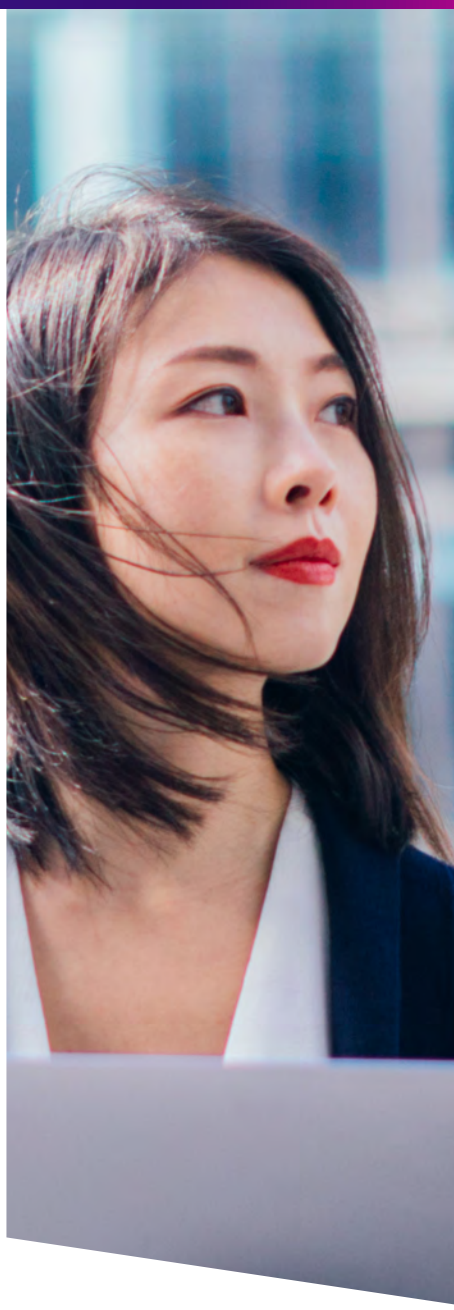
DATASHEET

Microsoft Sentinel Accelerator – Basic



What are BlueVoyant Accelerator Services?

With BlueVoyant's Microsoft Security Accelerator services, you don't need to be an expert to take your security and compliance posture to the next level. Our Accelerator 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 Accelerator (Basic) 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, Azure Active Directory - SignIn logs, is also included. While this log source is billable by Microsoft, it has a low volume.

Azure Activity Logs	Defender for Cloud Apps*
Office 365	Azure Activity
Defender for Endpoint*	Azure Identity Protection
Defender for Office 365*	Microsoft Defender for Cloud*
Defender for Identity*	Microsoft Defender for Cloud*

*Alerts Only

In addition to the listed Microsoft sources onboarding into Microsoft Sentinel above, you may select up to five (5) additional Log Source Types, as long as they are in the 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

Following setup, BlueVoyant will conduct 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
- Deployment of a set of 3 playbooks for Microsoft Sentinel in customer's Microsoft Sentinel subscription
- Knowledge Transfer: Introduction to KQL and Azure Functions

Additional Details

- Typically Basic Accelerator Sentinel deployments take 10 days, subject to customer's resource availability to supply devices and log sources.

WHY CUSTOMERS CHOOSE BLUEVOYANT

Delivery Expertise

200+ 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, 600+ proprietary alert rules, Threat Intelligence, Automation and AI capabilities.

Data Privacy and Cost Optimization

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

About BlueVoyant

When it comes to compliance, you need an experienced partner.

As the **2021 Managed Detection Response Microsoft Security 20/20 Award Winner**, along with BlueVoyant's status as a **Microsoft Gold Partner** with an **Advanced Specialization in Cloud Security and Threat Protection** and **founding member of Microsoft Intelligent Security Alliance (MISA)**, our mission is to proactively defend organizations of all sizes against today's sophisticated attacks and accelerate detection and response with Microsoft.

BlueVoyant®

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