Solution Brief

Microsoft Advanced Log Routing Service with ADX

Cost-effective alternative to storing all your logs on Microsoft Sentinel

The combination of Microsoft and BlueVoyant can deliver complete cyber security for almost any organization. By combining Microsoft with BlueVoyant, resource requirements are reduced, security operations are simplified, and overall security becomes more effective.

Although there are countless benefits to combining Microsoft and BlueVoyant, one challenge remains for larger organizations – the cost of storing all logs on Microsoft Sentinel, regardless of detection value.

BlueVoyant Microsoft Advanced Log Routing with ADX is a managed service for organizations, where monthly data storage is not measured in gigabytes but terabytes. It brings a standardized way to store logs on a lower-cost Azure ADX cluster and does that without impacting security efficacy. Only logs with threat detection value are duplicated to Microsoft Sentinel.

Key Differentiators

- Manage Microsoft Sentinel log storage costs
- Improve the overall value of Microsoft investments
- Reduce data and resource burden while streamlining security operations
- Retain more logs longer with a cost-effective log storage solution
- Retain ownership, control, and access to logs
- Have logs available longer for forensics, investigation, compliance, and hunting purposes.

Manage Costs

Store logs with lower-security value in a more cost-efficient ADX cluster instead of Micorosft Sentinel to help manage costs.

Retain Control

The client owned ADX cluster is fully accessible, and logs are searchable to aid with forensics, compliance, investigation, hunting, etc.

Be More Efficient

The BlueVoyant Log Collector and the ADX cluster are continually monitored, optimized, and managed by BlueVoyant MXDR 24×7 services.

BlueVoyant

Features

Implementation and initial configuration of our BlueVoyant-managed Log Collector and client-owned ADX cluster. Monitoring includes health, misconfiguration, configuration drift, continuous data connections, and malicious events.

Store all logs on the ADX destination for investigation, forensics, compliance, hunting, etc.

Logs with high-detection security value are duplicated entirely and sent to Microsoft Sentinel.

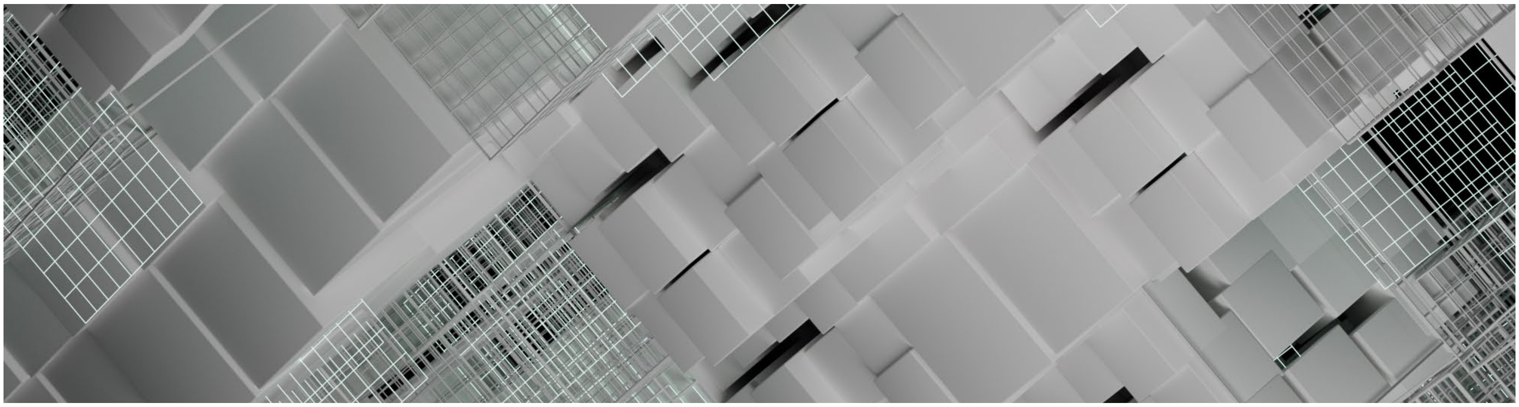
BlueVoyant templates for filtering logs at time of ingest via DCR or ITT

Implementation of ADX specific functions in Microsoft Sentinel to enable searching of the data retained in ADX.

Microsoft Sentinel ADX workbook for monitoring the ADX solution.

Log sources include,

- Syslog sources sent to BlueVoyant-managed Log Collector
- Microsoft Defender XDR Advanced Hunting Events for supported tables
- Microsoft Sentinel Logs in standard tables (If applicable for long-term retention)
- Other log sources that natively support export to Azure Data Explorer, Azure Event Hub, or Azure Data Lake Storage



To learn more about BlueVoyant and how we can help you with manage Sentienl storage cost with ADX, please work with your BlueVoyant representative or BlueVoyant partner. You can also visit us at **bluevoyant.com** for additional information and more contact options.

BlueVoyant