Solution Brief

Managed Detection and Response (MDR) for Endpoint

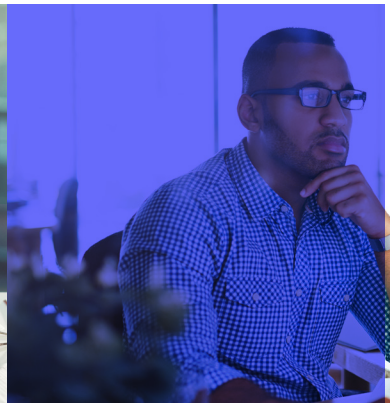
Powered by Microsoft® Defender for Endpoint

Introduction

BlueVoyant Managed Detection and Response (MDR), powered by Microsoft Defender for Endpoint, consists of monitoring and management of endpoint software deployments and the performance of threat hunting and incident response actions as needed. Monitoring services include 24×7 collection, storage, reporting, and customer notification of security events and device health events. This service is supported by the BlueVoyant technology platform, a cloud-based ingestion, processing, and analysis system.

This web-based platform generates reports based on the alerts that are analyzed by experts in BlueVoyant's Security Operations Center (SOC). Managed Detection and Response (MDR) for Endpoint includes a proven implementation methodology and tools for simplified reporting and analysis that are provided to you through BlueVoyant's client portal.

BlueVoyant



Standard Features

Indicator Enrichment
Indicators of compromise associated with detections within the monitored environment are automatically extracted, scored, and enriched, leveraging open source and proprietary Threat Intelligence. Enriched indicators assigned a reputation Wavelength portal.

Malware Prevention
Deployed endpoint software will automatically prevent the execution of suspicious or known malicious software, often preventing the outbreak or spread of malware. Through blacklist policy management, delivery of unique signatures and threat intelligence indicator matching, BlueVoyant can deny, terminate, and block operations remotely.

Endpoint Response
BlueVoyant will take a specific set of actions at the completion of an investigation: quarantine, delete, whitelist, monitor, or blacklist. Depending on your services, if an advanced investigation with live/real-time response is needed, BlueVoyant may perform remote intrusion response activities.

Health Monitoring
BlueVoyant will monitor installed endpoint agent communications using the technology platform. BlueVoyant will monitor log sources and will generate an alert when a log source's output has not been received in a specified interval.

Threat Detection
Advanced endpoint software will be used to expand enrichment and enhanced behavioral correlations. Depending on your services, BlueVoyant will proactively and iteratively search through events to detect and isolate advanced threats that evade existing security solutions.

Outage Prevention
All third-party vendor patches and upgrades will be assessed for their security, stability, and functionality by BlueVoyant prior to client deployment to ensure they are supported and won't cause outages.

Ready to get started? Learn more here.

About BlueVoyant
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 nearly 1,000 clients across the globe.

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

BlueVoyant