SOLUTION BRIEF

Managed Detection & Response (MDR)

Microsoft Defender for Endpoint

The Challenge

With the ever-growing number of access points, it is becoming harder for organizations to stop incidents from becoming breaches. Microsoft Defender for Endpoint detects attacks and data breaches, and gives businesses insights and tools to prevent, detect, investigate, and respond to incidents. However, some businesses might not have the capacity or expertise to manage the security of their endpoints on their own.

The Solution

BlueVoyant provides Managed Detection and Response (MDR) for Microsoft Defender for Endpoint to help Microsoft customers detect, prevent, respond to and mitigate advanced attacks. Utilizing the breadth of threat protection capabilities built into Microsoft Defender for Endpoint, BlueVoyant provides organizations with a fully-managed, end-to-end advanced threat management service that includes:

- Ongoing policy management and tuning
- 24/7 security operations
- Endpoint monitoring
- Triage and investigation
- Real-time incident response
- Threat containment and mitigation
- Robust detection with advanced hunting

SOLUTION FEATURES

Ongoing Policy Consultation and Development - By utilizing Microsoft Defender for Endpoint, which is included in your E5 license or can be bought as a standalone, for threat detection and response, there is no need to deploy another third-party product into your environment for endpoint security. There is no agent to deploy, no compatibility issues, and no additional product cost.

Whether you are already using Microsoft Defender ATP or just getting started, we help you to quickly realize its value by applying our deep operational knowledge and expertise in Microsoft Defender for Endpoint deployments. Beyond initial set up, we continuously review and update your policies to whitelist applications, assets, and processes as your business changes over time.

Automated Alert Analysis - Microsoft Defender for Endpoint integrates into our cloud-native platform that utilizes security orchestration, automation, and response to triage, enrich, and integrate automation of alerts received from Microsoft Defender for Endpoint.

We use playbooks to simultaneously run dozens of queries and processes at machine speed and utilize intelligence from more than forty sources to identify indicators of compromise.

Managed Prevention Enhanced with Human Analysis - BlueVoyant's security operations center analyzes alerts received from Microsoft Defender for Endpoint. The combination of expert-level analysis coupled with Microsoft technology makes protection against new and unknown threats even more effective by eliminating the black magic typically associated with machine learning, and minimizing misses and false positives.

Customized Detections and Prevention - Cyber threats are always evolving, so your detections should do the same. We provide ongoing refinement of your detection policies based on real-time threat intelligence. Equipped with this intelligence, we proactively protect your organization from modern day threats by writing customized policies to neutralize sophisticated malware and stop lateral movement that could potentially evade standard detections.

Real-Time Response, Containment, and Mitigation of Threats - It is fast, real-time action that helps minimize the damage done by adversaries. We rapidly isolate affected assets, including hardware, to prevent lateral spread and manually remove malicious files. As new threats are detected and neutralized across our client base, they are added to the platform, enabling crowd-sourced protection that acts as a force-multiplier for enhancing detection and mitigation of threats.

Threat Hunting - Advanced adversaries can evade standard detection techniques and tools. We will proactively and iteratively search through events to detect and isolate advanced threats that evade existing security solutions. We will also conduct remote hunt missions on a regular basis that will perform manual and semi-automated activities for targeted data analysis to search for signs of advanced attacks and malicious behavior.

Root Cause Analysis - Remote root cause analysis is performed on all positively identified malicious activity. Identifying the nature of the attack, timeline, attack chain, and the attack's underlying persistence to help you understand how adversaries are trying to exploit your infrastructure.

KEY FEATURES

- Integrated global threat intelligence from over forty open, closed, and proprietary sources
- SOAR integration that automates Microsoft Defender for Endpoint alerts
- Rapid response to contain malicious attacks
- Real-time incident mitigation
- 24/7 support from a team of security experts
- Customized policy management, tuning, refinements

WHY CHOOSE BLUEVOYANT MDR FOR MICROSOFT DEFENDER FOR ENDPOINT

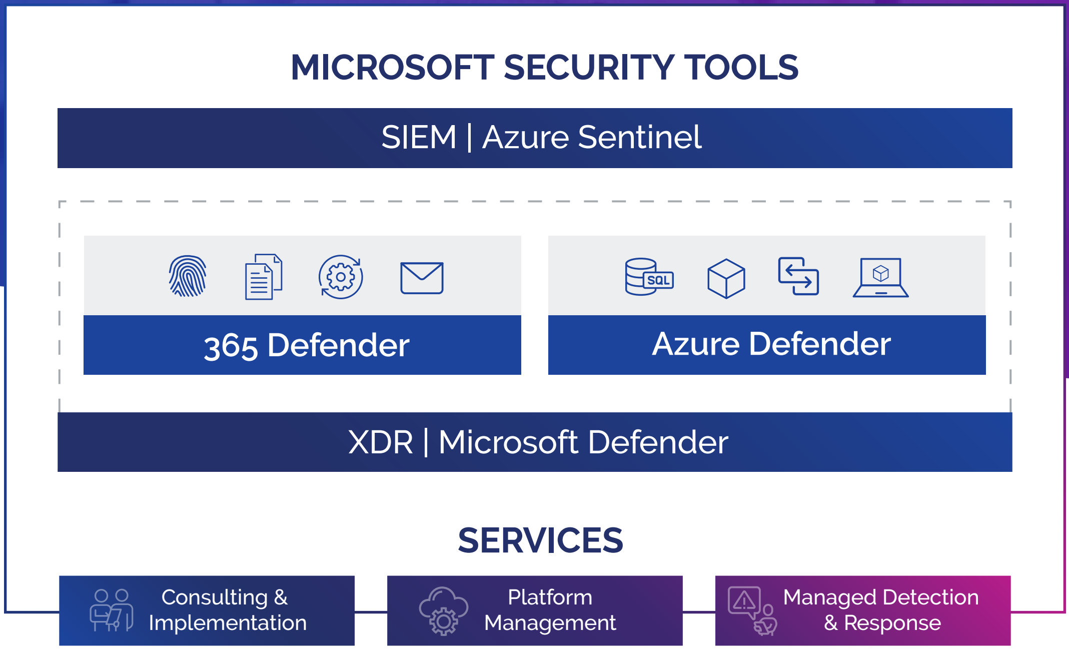
- Ongoing Technical Support and Customer Success
- Fast time to value
- Experience and recognition (Microsoft Gold Partner; Member of MISA)
- MDR platform built by cyber experts from the private sector, FBI, and NSA

The BlueVoyant Modern SOC supports the entire Microsoft security suite, including:

Microsoft Azure Sentinel
A cloud-based security information and event management (SIEM) tool.

Microsoft 365 Defender
An extended detection and response (XDR) platform designed to natively integrate with Azure Sentinel. (This includes all Microsoft 365 Defender services - for Endpoint, Office 365, Identity, and Cloud App Security).

Microsoft Azure Defender
A platform that provides XDR capabilities for infrastructure and cloud platforms including virtual machines, databases and containers.



MICROSOFT SECURITY TOOLS

SIEM | Azure Sentinel

365 Defender

Azure Defender

XDR | Microsoft Defender

SERVICES

Consulting & Implementation

Platform Management

Managed Detection & Response

Benefits

Reduce the level of risk faced by your organization

- 24x7 monitoring by our cyber security experts reduces your daily operational burden, allowing your team to focus on more strategic security activities.
- Automation and AI capabilities instantaneously identify and respond to the most serious threats.
- Incident responses that can’t be automated are tagged for evaluation by your team and can be integrated with your IT service management ticketing systems.
- A full array of regulatory compliance reporting capabilities so you know where you stand and can reduce the time needed to deliver audit reporting.

Benefits Continued

Fast time-to-value

- BlueVoyant has helped multiple customers design and implement Microsoft security tool deployments. Our well-defined and battle tested processes will have you up and running quickly.

Lower your total cost of ownership

- Deploy the Microsoft Security tools you already have access to as part of your M365 E3, E5, EMS or Business Premium License.
- Eliminate the time and cost of managing disparate security hardware and software technologies.

Optimize your cloud spend

- As part of every deployment, we will review all of your security log sources and as to which ones you need and which ones you don't. BlueVoyant customers can expect to see up to a 40% optimization in Azure log ingestion costs.

Ongoing Technical Support and Customer Success

- You will be assigned a Technical Customer Success Manager (CSM) during the onboarding process. Your CSM will serve as your primary point of contact into BlueVoyant and collaborate with both you and our internal teams to synthesize your feedback and ensure it is routed properly for action. Your CSM is laser-focused on ensuring that you are getting the most value out of your service at all times.
- As part of the MDR service, you will also have access to the BlueVoyant Security Operations Center 24x7. Every time you call, you'll speak to a human who will immediately address your concerns.

Gold
Microsoft Partner
Microsoft

Member of
Microsoft Intelligent Security Association
Microsoft

About BlueVoyant

BlueVoyant is an expert-driven cyber security services company whose mission is to proactively defend organizations of all sizes against today's constant, sophisticated attackers and advanced threats.

Led by CEO Jim Rosenthal, BlueVoyant's highly skilled team includes former government cyber officials with extensive frontline experience in responding to advanced cyber threats on behalf of the National Security Agency, Federal Bureau of Investigation, Unit 8200 and GCHQ, together with private sector experts. BlueVoyant services utilize large real-time datasets with industry-leading analytics and technologies.

Founded in 2017 by Fortune 500 executives and former Government cyber officials and headquartered in New York City, BlueVoyant has offices in Maryland, Tel Aviv, San Francisco, London, and Latin America.

BlueVoyant®

cadre
information security