Managed Detection & Response (MDR)

Azure Sentinel + Microsoft Threat Protection

INTEGRATED CLOUD-NATIVE SIEM WITH CROSS-DOMAIN RESPONSE AND THREAT ERADICATION

Learn more at www.bluevoyant.com
THE STATE OF CYBERSECURITY

The digital economy is in full swing. Organizations are evolving faster than ever, adopting new technologies such as cloud services that are transforming how they operate and creating new gaps in security. Cybercriminal activity is in full swing too!

Today, more than ever, adversaries are creating new techniques to launch attacks across an organization’s on-premises and cloud infrastructure to evade detection and ensure they continue to stay one step ahead of their victims.

Security teams and service providers not only have to collect, triage, and investigate alerts, they have to be able to respond in real-time to stop sophisticated fast-moving malicious activities across an expanded ecosystem of distributed networks and cloud-based services.

BlueVoyant is revolutionizing Managed Detection and Response by increasing threat visibility and expanding response actions beyond endpoints.

Managed Detection and Response (MDR) services by BlueVoyant unify Microsoft’s cloud-native Security Information and Event Manager (SIEM), Azure Sentinel, and Microsoft Threat Protection to allow a 360-degree view of your attack surface across endpoints, on-premises infrastructure, identities, email, and cloud apps and enable cross-domain threat prevention and proactive threat hunting.
WHY BLUEVOYANT

Exemplary Leadership:
Co-Founded in 2017 by F500 Executives and Former officials NSA, FBI, Unit 8200, and GCHQ, together with private sector experts.

Microsoft Expertise:
Member of the Microsoft Partner Network (MPN), Microsoft Cloud Solution Provider (CSP), Member of Microsoft Intelligent Security Association (MISA), Microsoft MSSP Partner, and targeting attainment of Microsoft Gold Security Competency by July 2020.

Global Footprint:
New York City (HQ), Maryland, Tel Aviv, San Francisco, London, Manila, and Latin America.

Cloud-Native SOC-as-a-Service:
BlueVoyant Security Operations Center is 100% cloud-native allowing limitless flexibility and scale.

Rapid Incident Response:
Same day incident response support available for ALL Microsoft Defender ATP clients, whether or not you’re part of BlueVoyant’s customer base.
HOW IT WORKS

Deployment and Implementation

Maximize your investment in Microsoft security solutions with BlueVoyant to:

• Design and configure Azure Sentinel cloud instance
• Configure and onboard log data using Azure Sentinel built-in connectors across cloud and on-premises sources
• Create client-specific dashboard design and customization
• Create proactive threat hunting playbook
• Construct alerting scenarios to trigger case generation and investigations
• Integrate playbooks to enable automation

MANAGED SECURITY OPERATIONS

BlueVoyant’s Managed Detection and Response provides real-time, customized threat response and remediation - terminating malicious processes, isolating devices, and manually preventing persistence and lateral movement associated with sophisticated attacks.

BlueVoyant incorporates client-driven rules of engagement (ROE) to enable immediate, decisive action, utilizing analyst driven expertise to stop threats that could cripple a network versus non-critical events where a lower-tiered response may be appropriate.

MDR services integrate proven frontline expertise, comprehensive threat data analytics, and advanced technology solutions to deliver remote monitoring and incident remediation utilizing Azure Sentinel, Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP), Office 365 Advanced Threat Protection (Office 365 ATP), Azure Advanced Threat Protection (Azure ATP), and Microsoft Cloud App Security.
Your Security Stack

**Email**

**Endpoints**

**Apps**

**On-Prem**

**Users**

---

**BlueVoyant MDR**

**MICROSOFT THREAT PROTECTION**

- **Microsoft Defender ATP**
- **Azure ATP**
- **Microsoft Cloud App Security**
- **Office 365 ATP**
- **BLUEVOYANT SECURITY OPERATIONS**

---

**Outcome**

- Transparency and Accountability
- Unified Visibility
- Hunt and Stop New Threats

---

**Azure Sentinel**

A scalable, cloud-native, security information event management (SIEM) platform providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.

**Microsoft Defender Advanced Threat Protection**

Unified endpoint platform for preventative protection, post-breach detection, automated investigation, and response.

**Office 365 Advanced Threat Protection**

Safeguards your organization against malicious threats posed by email messages, links (URLs) and collaboration tools.

**Azure Advanced Threat Protection**

Uses Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

**Microsoft Cloud App Security**

A comprehensive cross-SaaS solution bringing deep visibility, strong data controls, and enhanced threat protection to your cloud apps.
BlueVoyant MDR powered by Microsoft Security includes:

24 x 7 Managed Detection and Response
Real-time monitoring of Azure Sentinel alerts with full-scale investigations and response to security events supported by expert Cyber threat analysts who operate 24/7, across multiple locations within Security Operations Centers (SOC).

Increased Visibility to Resolve Every Alert
Collects and analyzes data from multiple data sources, including endpoint, email, user activity, and other third-party security solutions, providing visibility into risks and threats across multi-cloud and hybrid environments.

Cloud-Native MDR Protection with Speed and Scale
Near-limitless connectivity speed to security logs and scale delivered in the cloud without the time and cost of appliance-based SIEM.

Integrated Automation Enhanced with Expertise
Integrated cross-product automation layer that ingests all alerts generated to automate and coordinate prevention, defensive responses, and remediation across all platforms.

Ongoing Building and Tuning of Azure Sentinel Alerts
Simplified implementation tailored to your unique environment, providing custom configurations and ensuring limited operational interruption.

Custom Correlations
Analyst developed unique searches, custom correlations, and tracking integrated with BlueVoyant threat intelligence providing contextual insights unique to your enterprise.

Built-in Automation and Orchestration
Integrated, proprietary playbooks designed to automate responses, enabling the ability to fully automate routine operations to recurring types of alerts and/or automated responses to specific alerts.

Collaboration
Customers leverage Wavelength™, BlueVoyant’s client portal, to access real-time information about alerts and investigations.

Threat Intelligence Integration
BlueVoyant threat intelligence amplifies and enriches correlations to create custom insights.

Hunting
BlueVoyant’s dedicated hunting team proactively investigates activity that standard detections can miss.
Cloud-Native MDR with Azure Sentinel and Microsoft Threat Protection Architecture and Operations Model

Client Environment

Client’s Azure

- Azure Sentinel
- Microsoft Threat Protection
  - Microsoft Defender ATP
  - Microsoft Cloud App Security
  - Office 365 ATP
  - Azure ATP
- Azure Active Directory
- Office 365
- Microsoft 365 Security
- Google Cloud
- Amazon Web Services

Other Clouds

Logs

Client Experience

Wavelength Portal

- Cases
- Reports
- Assets
- Threat Intelligence

24/7 Security Operations

- Customized Case Management
- Threat Response and Eradication
- Custom Rules of Engagement

Policy Management & Tuning, Granular Response, Alert Status Updates

Cross Solution Investigation, Response, Remediation