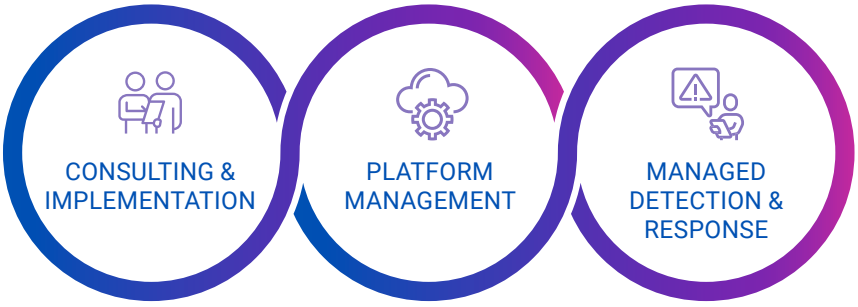
SOLUTION BRIEF

BlueVoyant Modern SOC

Uniting Managed Detection and Response (MDR) with Microsoft® Azure Sentinel and Microsoft® Defender XDR



INTRODUCTION

New approaches to cyber security are needed more than ever!

The exponential growth in remote employees and the acceleration of digital transformation initiatives have expanded the attack surface for companies big and small. Security teams that are already stretched struggle to cobble together integrated solutions consisting of technologies from multiple vendors, many of which were only designed to operate in legacy environments. Integration complexities, a lack of security resources that can force painful compromises, and unrelenting attacks from cyber criminals have made securing the organization a seemingly unattainable goal.

Today's sophisticated cyber attacks are no longer exclusive to endpoints. They are multi-faceted and target identities, email, infrastructure, cloud platforms, servers, databases and more. Endpoint-centric detection and response solutions alone do not provide the visibility and response capabilities required to identify and neutralize broader attacks.

We believe a cloud-native, fully integrated security solution is what makes the most sense to companies trying to operate safely in today's dangerous, highly interconnected world. To bring our vision to life and to help our customers get the business and security outcomes they want, we have partnered closely with Microsoft and also made significant investments in people, processes and technology. We can now offer customers an end-to-end portfolio of consulting, implementation and managed security services, enabled and powered by Microsoft's security technologies and designed to expand on your existing investments in Microsoft security tools. We call this portfolio of automation and 24x7 human security analysts the BlueVoyant Modern SOC.

The BlueVoyant Modern SOC is designed to come to you, to where your data is, and to assist your team with the monitoring and protection of your assets and resources in your Microsoft Azure and your Microsoft 365 environment and any connected appliances, servers, VMs, clients, and on-premises networks. We are ready to assist you wherever you are in your Microsoft-powered security journey.

Your data is the lifeblood of your business. With data privacy now front and center globally and the costs of cloud consumption rapidly increasing, customers are asking their data stay within their environment. While other MSSP require data to be sent to their infrastructure and data centers for analysis, BlueVoyant's service allows you to keep your data in your own environment, reducing cost and ensuring stronger compliance.

BlueVoyant's Modern SOC provides a complete portfolio of Microsoft security-focused services, including a customized deployment of Microsoft security tools, ongoing platform care & maintenance and 24/7 security operations as a service.

Consulting and Implementation

Do you feel that you are maximizing your use of Microsoft's security capabilities? If not, we can help. With our Modern SOC consulting and deployment services, honed and perfected across many Azure Sentinel deployment, you don't need to be an expert to take your security and compliance posture to the next level. Our "Accelerator" services are focused consulting engagements designed to get you up and running quickly and to maximize your investment in Microsoft Azure Sentinel, Microsoft 365 Defender, and Azure Defender security technologies.

We 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. What's included: A detailed assessment of your risks, guidance on how best to leverage Microsoft-powered solutions and/or deployment & configuration assistance to best meet the requirements of your unique situation.

SOLUTION FEATURES

Azure Sentinel Accelerator

- Infrastructure setup
- Log source ingestion
- Alert and SOAR configuration
- Knowledge transfer
- Initial alert tuning and optimization
- Integration with MDR monitoring
- Incident response playbook creation
- Security controls deployment

Microsoft 365 Defender Accelerator

Defender for Endpoint; Defender for Identity; Defender for Office 365; Cloud App Security (MCAS)

- Infrastructure setup
- Configuration
- Integration with SIEM
- Policy tuning
- Integration with MDR monitoring
- Security controls deployment

Platform Management

Not looking for a full MDR service, but still want help with keeping your Microsoft security tools up to date and running smoothly? Our Modern SOC Platform Management for Azure Sentinel solution can help. This service provides complete health monitoring for your Microsoft security environment(s), assists with onboarding of new log sources, and ensures continuous delivery and optimization of security alert and correlation rules.

You will get access to our 500+ customized alert rules, 80+ data connectors, playbook automations, and related log optimization services apart from those offered by Microsoft out of the box. Our on-demand Azure Sentinel experts will be accessible to you and ready to assist you when you need them.

SOLUTION FEATURES

Azure Sentinel

- Alert tuning
- New log source ingestion
- Custom data connectors
- Continuous cloud consumption optimization
- Threat Intelligence
- Support during incidents
- Monthly reviews

Managed Detection and Response (MDR)

The BlueVoyant Modern SOC MDR adds 24x7 monitoring, detection, investigation, and response capabilities to our Platform Management services. Depending on which Microsoft security tools you decide to use, we offer optimized services to match:

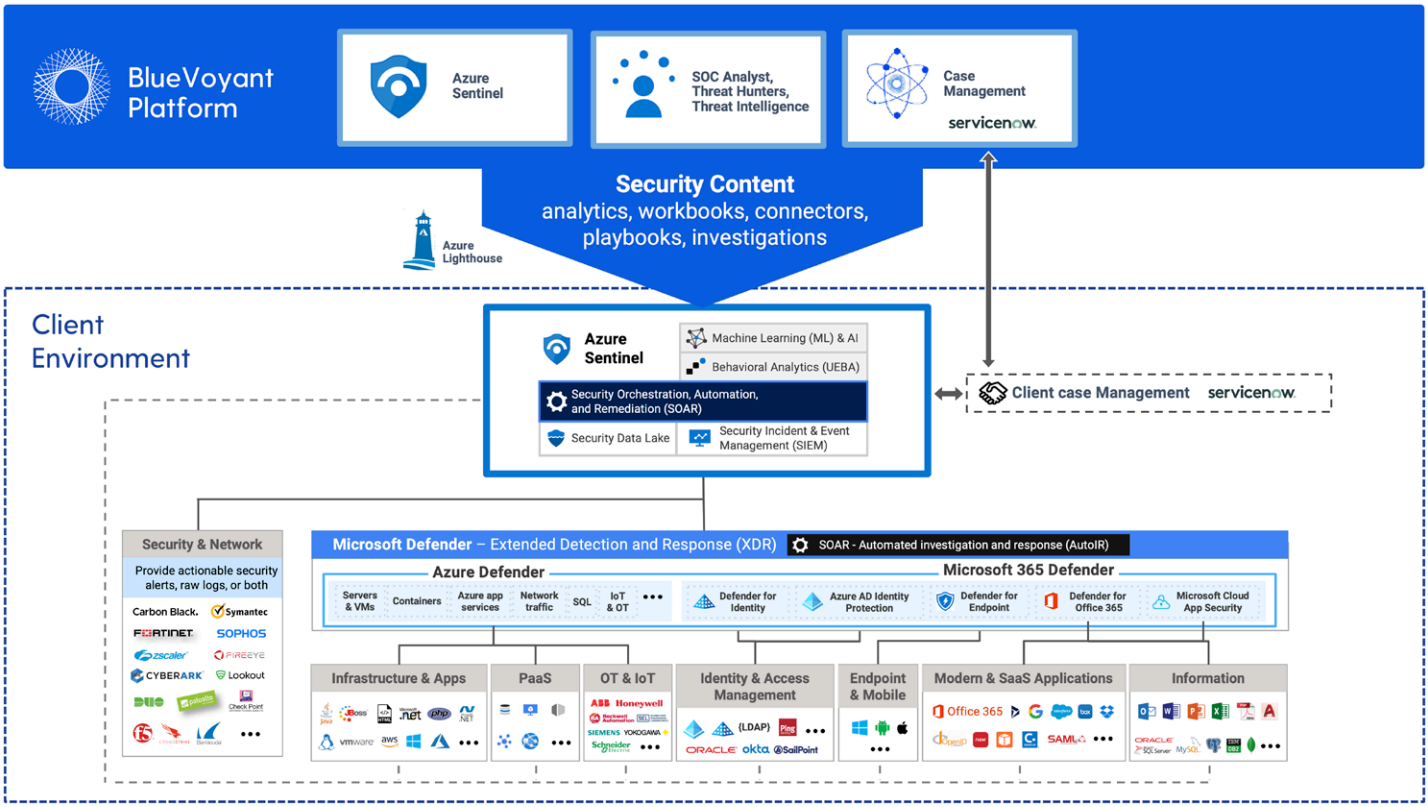
- **Azure Sentinel:** Monitoring and investigations of Sentinel alerts.
- **MDR for Microsoft 365 Defender:** Monitoring, investigations and remediation across the Microsoft 365 Defender suite of products.
- **MDR for Azure Defender:** Monitoring, investigations and remediation across Azure Defender suite of products.

SOLUTION FEATURES

24/7 SOC with MDR

- Alert triaging and Investigations
- Unlimited Remote Incident Response
- Threat Eradication
- Threat Intelligence
- Escalations and notifications as appropriate
- Monthly account reviews
- Threat Hunting

Proactive threat hunting by BlueVoyant security analysts can be purchased as an optional add-on with all Modern SOC MDR services.



The BlueVoyant Modern SOC is is a powerful solution that can incorporate security logs from the entire Microsoft security toolset as well as many third-party technologies.

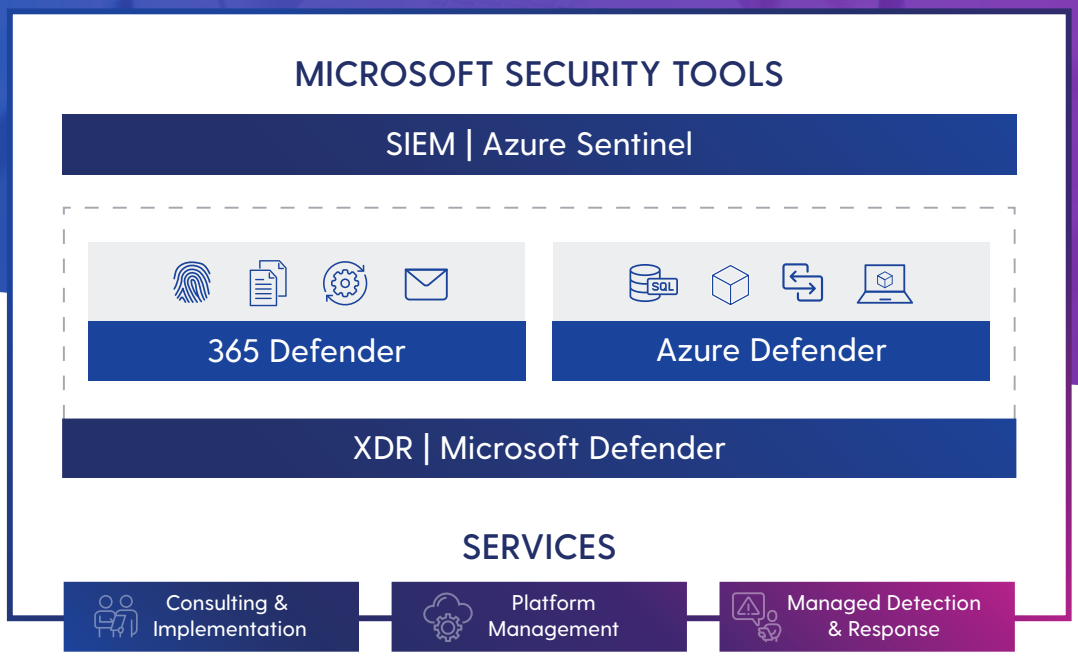
Rather than you sending us your logs and us sending you alerts back, our security experts will operate inside your environment, enriching incidents, raising alerts, and closing incidents, etc., directly within your Azure Sentinel environment, where you can watch in real-time as we work to protect your company from threats.

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.



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®

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