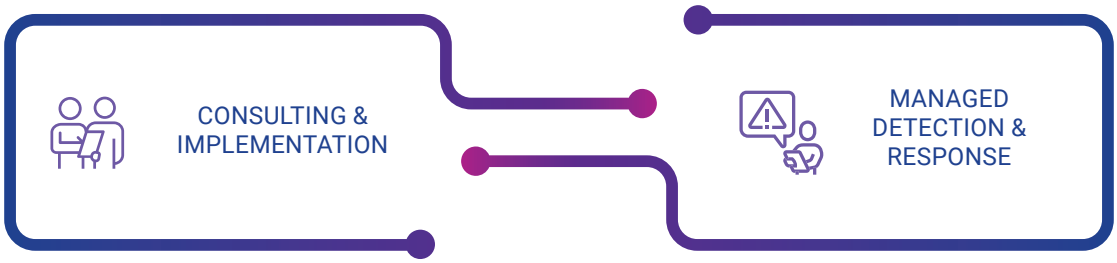
SOLUTION BRIEF

BlueVoyant Modern SOC

Uniting Managed Detection and Response (MDR) with Microsoft® 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 connect and construct integrated technology solutions from multiple vendors, many of which were only designed to operate in legacy environments. These integration complexities, combined with a lack of security resources and training, can force painful compromises, and the unrelenting attacks from cyber criminals make 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 offer customers an end-to-end portfolio of consulting, implementation and managed detection and response services, enabled and powered by Microsoft's security technologies and designed to expand on your existing investments in Microsoft security tools and to augment your in-house expertise. 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 assets and resources in your Microsoft Azure and Microsoft 365 environment with all connected appliances, servers, VMs, clients, other clouds, 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 management & maintenance and 24/7 Managed Detection and Response (MDR), protecting you from cyber threats and providing continuous improvement of your security posture.

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 Microsoft 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 Sentinel, Microsoft 365 Defender, and Microsoft Defender for Endpoint 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

Microsoft 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

Managed Detection and Response (MDR)

The BlueVoyant Modern SOC MDR service activates 24x7 monitoring, detection, investigation, hunting, and response capabilities to augment Microsoft security tools and to work alongside customer security tools and personnel.

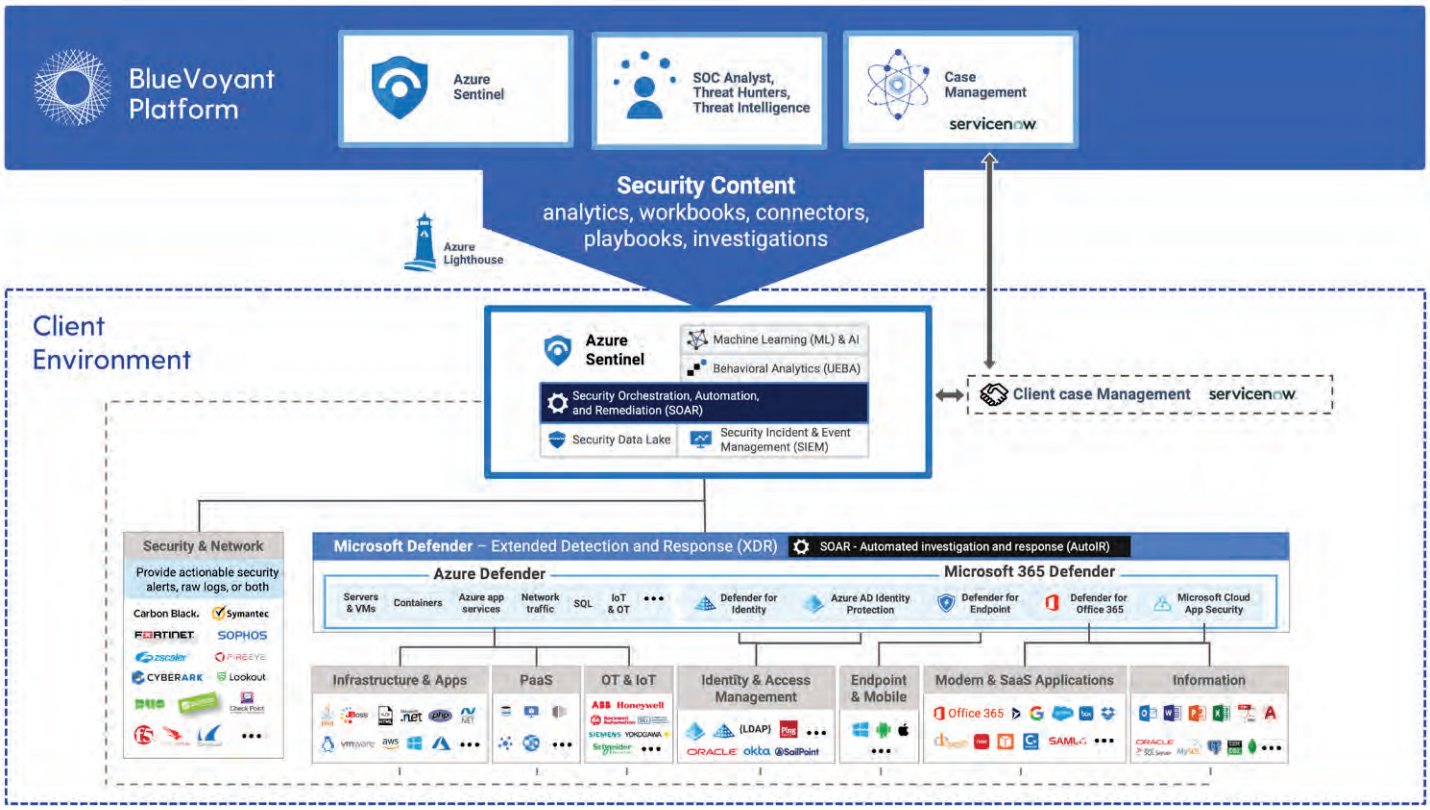
- **Microsoft Sentinel:** Monitoring and investigations of infrastructure and log alerts surfaced via Microsoft Sentinel.
- **MDR for Microsoft 365 Defender:** Monitoring, investigations, and remediation for Microsoft 365 content, with the Microsoft 365 security signals.
- **MDR for Microsoft Defender for Endpoint:** Monitoring, investigations and remediation for Azure PaaS and IaaS services, with the Microsoft Defender for Endpoint security signals.

SOLUTION FEATURES

24/7 SOC with MDR

- Alert triaging and investigation
- Unlimited remote incident response
- Threat Eradication
- Threat Intelligence
- Environment security health monitoring
- Log source collection, optimization
- Threat Hunting
- Access to BlueVoyant library of 500+ customized alert rules, 80+ data connectors, and playbook automations
- Concierge Support included
- Escalations and notification as appropriate

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 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 Microsoft 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 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 Microsoft Sentinel. (This includes all Microsoft 365 Defender services - for Endpoint, Office 365, Identity, and Cloud App Security).

Microsoft Defender for Endpoint
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 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

At BlueVoyant, we recognize that effective cyber security requires active prevention and defense across both your organization and supply chain. Our proprietary data, analytics and technology, coupled with deep expertise, works as a force multiplier to secure your full ecosystem.

Accuracy. Actionability. Timeliness. Scalability.

Founded in 2017 by former Fortune 500 executives and former government cyber officials, BlueVoyant is headquartered in New York City and has offices in Maryland, Tel Aviv, San Francisco, Manila, Toronto, London, Latin America and Budapest. Visit www.bluevoyant.com

BlueVoyant®

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