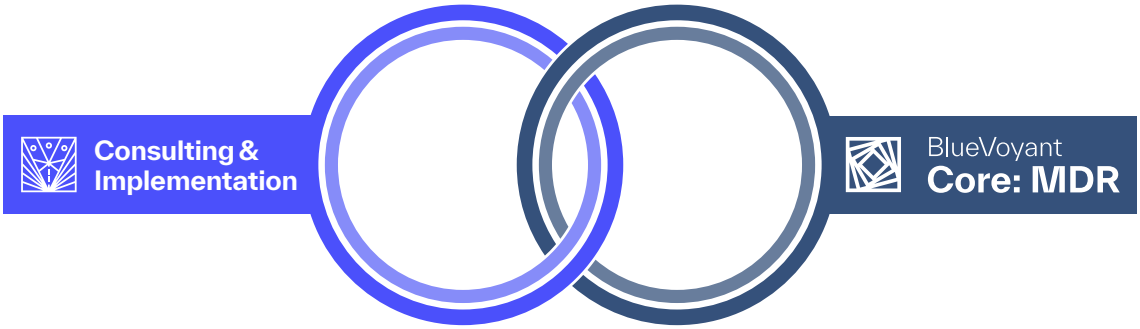
Spirity
TOMORROW:TODAY

Solution Spotlight

BlueVoyant Core: MDR for Microsoft (Managed Detection and Response)

Microsoft SIEM plus XDR Implementation and Management



New approaches to cybersecurity are needed more than ever.

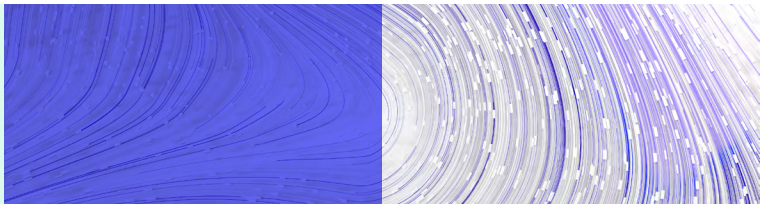
The exponential growth in remote employees and the acceleration of digital transformation initiatives have expanded the attack surface for companies big and small. Security teams that are already stretched struggle to connect and construct integrated technology solutions from multiple vendors, many of 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 multifaceted 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.

A cloud-native, fully-integrated security solution helps companies operate safely in today's interconnected world. To bring this vision to life and help our clients achieve their business and security outcomes, BlueVoyant has partnered with Microsoft. In addition to making a significant investment in people, process, and technology, BlueVoyant offers clients an end-to-end portfolio of consulting, implementation, and managed security services, all powered by Microsoft's security technologies and designed to expand on your existing Microsoft security tools investment. We call this automation portfolio and 24×7 human security services BlueVoyant Core: MDR for Microsoft SIEM plus XDR.

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 want their data to stay within their environment. While other Managed Security Service Providers (MSSPs) require security data to be sent to their infrastructure and data centers for analysis, BlueVoyant's service allows you to keep your security data in your own environment, reducing cost and ensuring stronger compliance.

BlueVoyant



MDR for Microsoft SIEM plus XDR provides a complete portfolio of Microsoft security-focused services, including a customized deployment of Microsoft security tools, ongoing management and maintenance, as well as 24×7 MDR, protecting you from cyber threats and providing continuous security posture improvement.

Consulting and Implementation

Are you maximizing your Microsoft security tools' capabilities? If not, we can help. With MDR for Microsoft, 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 maximize your investment in Microsoft Sentinel, Microsoft 365 Defender, and Microsoft Defender for Cloud security technologies. BlueVoyant performs a detailed analysis of your environment(s) and provides actionable security insights, leveraging the BlueVoyant catalog of prebuilt playbooks and alert rules.

What's included:

- A detailed assessment of your risks
- Guidance on how to best use Microsoft-powered solutions and deployments
- Configuration assistance to meet your unique requirements

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

BlueVoyant

BlueVoyant Core: MDR for Microsoft SIEM plus XDR

MDR for Microsoft activates 24×7 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.

Microsoft 365 Defender: Monitoring, investigations, and remediation for Microsoft 365 content, with the Microsoft 365 security signals.

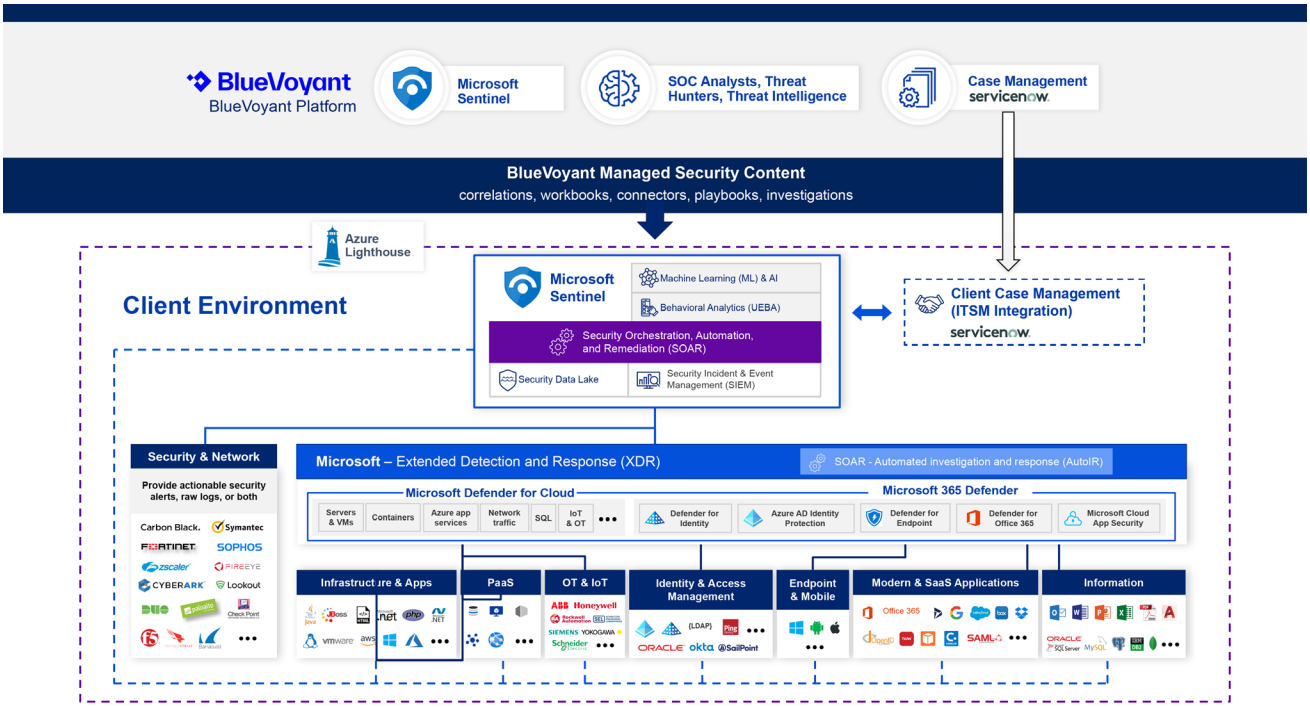
Defender for Cloud: Monitoring with investigation support for cloud workloads.

Solution Features

24×7 MDR for Microsoft

- Alert triaging and investigation
- Unlimited remote incident response
- Threat eradication within Microsoft 365 Defender
- Threat intelligence
- Environment security health monitoring
- Log source collection, optimization
- Threat hunting
- Access to BlueVoyant library of 900-plus customized alert rules, hundreds of 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 MDR for Microsoft services



BlueVoyant Core: MDR for Microsoft is a powerful solution that can incorporate security logs from the entire Microsoft SIEM plus XDR security toolset as well as many third-party technologies.

Rather than sending BlueVoyant your logs and receiving alerts back, our security experts operate inside your environment. Watch in real time as they enrich investigations, raise alerts and close incidents, directly within your Microsoft Sentinel environment.

BlueVoyant

MDR for Microsoft 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 Cloud

A platform that provides XDR capabilities for infrastructure and cloud workloads including virtual machines, databases, and containers.

BlueVoyant

Benefits

Reduce the level of risk faced by your organization

- 24×7 monitoring by our cybersecurity 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.

Fast time to value

- BlueVoyant has helped many clients 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, A5, G5, 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 your deployment, we will review all of your security log sources and recommend which ones you need and which ones you don't. BlueVoyant clients 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 laserfocused on ensuring that you are getting the most value out of your service at all times.
- As part of the MDR for Microsoft service, you will also have access to the BlueVoyant Security Operations Center 24×7. 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

Spirity TOMORROW:TODAY

Contact us to learn more.

Éva Szunomár | hello@spirity.hu |

BlueVoyant