Solution Brief

BlueVoyant Microsoft Security Deployment Services

Expert configuration and deployment services for Microsoft Security

Are you prepared to fully leverage Microsoft Security to protect your organization?

Many teams can swiftly deploy Microsoft Sentinel workload with native connectors, a Microsoft Defender XDR instance, Microsoft Security Copilot, or other innovative Microsoft Security tools. However, your organization may have more complex requirements that require deployment from Microsoft experts. Some complexities include creating MITRE ATT&CK aligned analytic rules, integrating third-party data sources, managing a multi-tenant architecture, optimally deploying multiple Microsoft tools, or migrating from another SIEM or XDR platform. These challenges require a deep level of Microsoft platform expertise to maximum security value that can significantly enhance your security operations, and help you stay within budget. Let BlueVoyant help your network defenders accelerate your path to success.

BlueVoyant Microsoft Security Deployment Services will efficiently help meet your organization's complex needs. Our process begins with comprehensive analysis of your security environment, delivering actionable insights through BlueVoyant's proven methodology, extensive connector catalog, automated playbooks, and curated detection rules. We provide specialized guidance for maximizing your Microsoft security investments, alongside expert deployment and configuration services tailored to your organization's unique security landscape and compliance needs. We deploy single or multiple Microsoft Security tools based on your organization's needs.

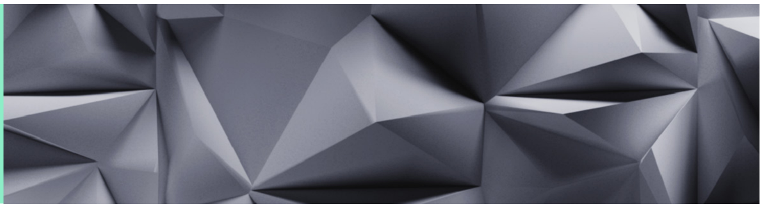
Delivered Outcomes

- Rapid and comprehensive Microsoft Security tech stack implementation to provide visibility to your security data from experts who have completed over 1,000 deployments.
- Seasoned experience in complex architecture (multi-tenant, multi-workspace), as well as migration from competitive SIEM, EDR, and XDR solutions.
- We offer over 350 pre-built data connectors and 1,000 analytic rules, with the ability to create custom data connectors and/or analytic rules tailored to your specific SIEM requirements.
- 2024 Worldwide Security Partner of the Year, three-time US Security Partner of the Year and 2024 Canada Security Partner of the Year validates our Microsoft expertise.
- Increased security and visibility powered by our team of security experts, massive library of proprietary alert rules, Threat Intelligence, Automation, and AI capabilities.
- Complimentary Microsoft Security assessments such as Threat Gap Analysis and Cost of Adoption.
- BlueVoyant Defender Assessment app continually minimizes risk, improves your security posture, and optimizes your Microsoft Security investment.

Microsoft
2024 Partner of the Year

Winner
Security Award

BlueVoyant



Features

Microsoft Sentinel

We assess your current SIEM, Azure tenancy, and security controls, identify key log sources, and establish a project timeline. Following this, we customize and tune data connectors, tailor analytic rules, and develop data visualizations with BlueVoyant Workbooks, complemented by response automation using BlueVoyant playbooks.

Microsoft Defender XDR

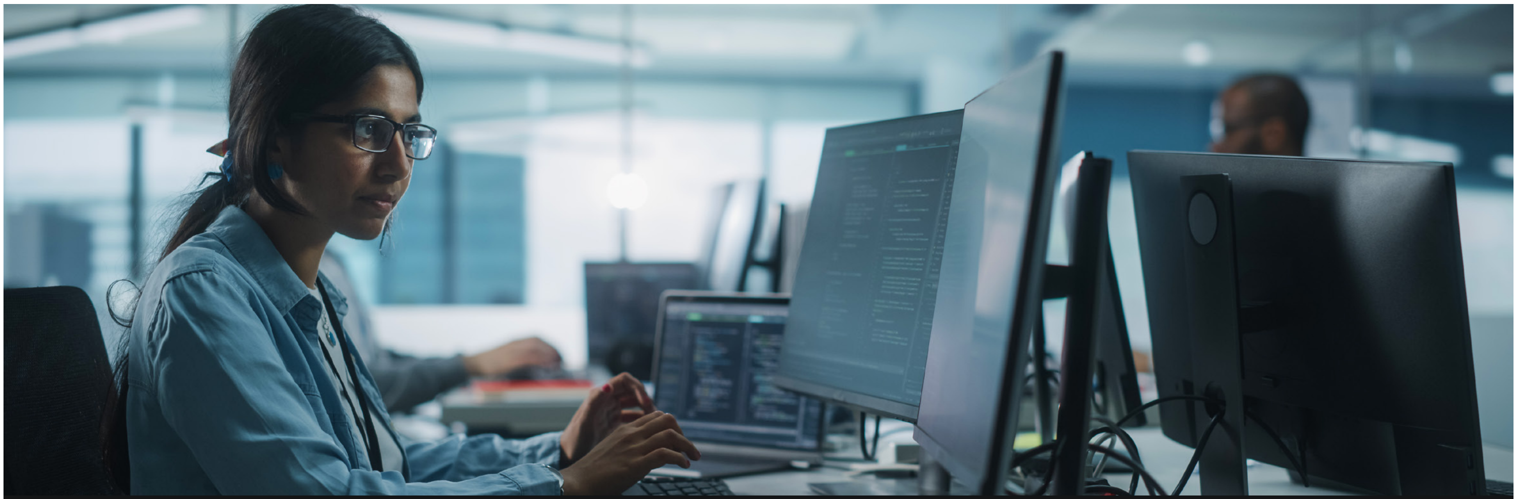
Deployment and implementation of security features within the Microsoft Defender XDR product suite included in the Microsoft 365 E5/A5 & G5 Security licenses. This includes Defender for Endpoint; Defender for Identity; Defender for Office 365; Defender for Cloud Apps; Microsoft Entra ID Identity Protection; Microsoft Entra ID Password Protection.

Microsoft Defender for Cloud

Streamlining the activation and optimization of Microsoft Defender for Cloud Workload Protection solutions, this fixed-price engagement offers a robust suite of deployment activities led by BlueVoyant's expert team. This service includes the enablement of the following Defender for Cloud Workload Protection services: Defender for Servers; Defender for Databases; Defender for App Services; Defender for Storage; Defender for KeyVault; Defender for Resource Manager; Defender for APIs.

Microsoft Azure Data Explorer

Implements Azure Data Explorer as a cost-effective alternative to Microsoft Sentinel for log storage, enabling fast analysis of big data streams and reducing time to insights.



Don't let missing logs translate to missed security events.

Start here.

BlueVoyant delivers a comprehensive cloud-native security operations platform that provides real-time threat monitoring for networks, endpoints, and supply chains, extending to the clear, deep, and dark web. The platform integrates advanced AI technology with expert human insight to offer extensive protection and swift threat mitigation, ensuring enterprise cybersecurity. Trusted by more than 1,000 clients globally, and the 2024 Microsoft Worldwide Security Partner of the Year, BlueVoyant sets the standard for modern cyber defense solutions.

BlueVoyant