Solution Brief

BlueVoyant MXDR for Microsoft SIEM Plus XDR: Security Service Offerings

Consulting, implementation, and 24×7 security management with BlueVoyant Deployment Services and BlueVoyant MXDR (Managed Extended Detection and Response).

Properly implementing and optimizing a SIEM plus XDR strategy while operating a 24×7 Security Operations Center (SOC) is challenging. It requires converging and streamlining several security tools so they act as one. Data from multiple sources needs to be correlated to identify sophisticated multi-vector threats before they mutate, move laterally, and hide. To implement and operationalize SIEM plus XDR, and to do it well, experience is required to avoid wasting resources and creating new or hidden vulnerabilities.

Managing a security-hardened SOC with all the required tools, monitors, software, systems, network appliances, and sensors is also expensive, as organizations need to acquire, integrate, and manage all the third-party services and licenses. The SOC must have the additional resources required to evaluate and integrate new technologies, and continue to evolve to keep pace with the ever-increasing volume and complexity of threats.

The most difficult aspect of developing and maintaining a SOC is hiring and clearing a security team that has the experience and training needed to properly maintain the security infrastructure and protect your digital estate end-to-end around the clock.

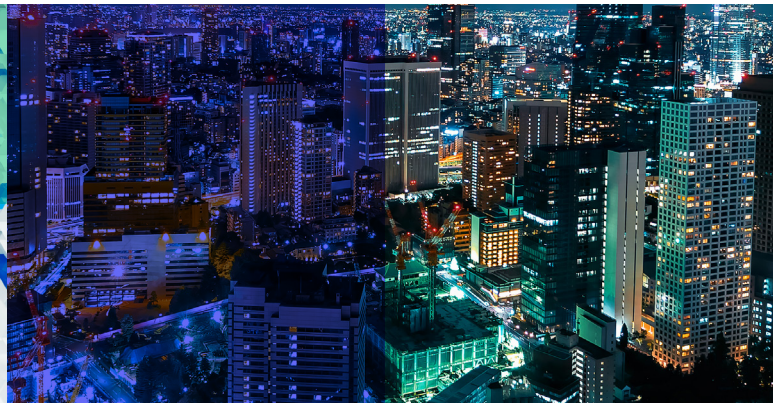
In many cases, using a cloud-native MXDR (managed extended detection and response) service is a prudent and cost-effective solution for properly implementing a SIEM plus XDR strategy and managing daily operations 24×7.

Microsoft SIEM Plus XDR security products combined with BlueVoyant's MXDR and our unique capabilities reduce cyber risk and provide the highest security posture possible.

Key Differentiators

- Implement and operationalize Microsoft SIEM Plus XDR to achieve the highest security posture possible and optimize your E5 Microsoft investments.
- Converge Microsoft 365 Defender, Microsoft Defender for Cloud, and Microsoft Sentinel into a unified solution that works as one.
- Gain 360 degree visibility into everything we do, including threat identification, actions, and outcomes.
- With more than 40 unique and proprietary data feeds and BlueVoyant's risk-based analytics, we find threats that others may miss.
- Elite content engineers unify and correlate seemingly innocent alerts to uncover complex multi-vector threats and halt them before they start.
- Proactive and reactive SOC engineers and threat hunters with nearly 10 years experience each contain and eradicate the most sophisticated threats before they spread.

BlueVoyant



BlueVoyant One-Time Deployment Services

Implementing, operationalizing, and optimizing your Microsoft SIEM Plus XDR strategy.

With BlueVoyant's Microsoft Security Deployment Services, you don't need to be an expert to take your security posture to the next level. Our hands-on BlueVoyant Deployment Services can have you up and running quickly.

BlueVoyant will perform a detailed analysis of your environment(s) and provide hands-on-keyboard baselining and hardening services, leveraging the BlueVoyant catalog of pre-built playbooks and alert rules.

Our Deployment Services include a detailed assessment of your risks, guidance on how to best leverage Microsoft Sentinel, Microsoft 365 Defender, Defender for Cloud, with E3, E5, A5, F5, and G5. That can include implementation and configuration assistance to best meet the requirements of your unique environment. All our services are delivered by BlueVoyant Microsoft-certified experts who specialize in SIEM plus XDR.

BlueVoyant Ongoing MXDR Service

Around-the-clock security monitoring and management using our SOC, unique technologies, intelligence, AI, and expert threat team.

BlueVoyant MXDR™ for Microsoft SIEM Plus XDR is our cyber defense offering that leverages cutting-edge technology and world-class experts who operate a fully co-managed SOC for our Microsoft clients.

Our Microsoft MXDR experts are an extension of your team and remain vigilant 24×7 — detecting, investigating, and hunting threats. We use our 900+ detection rules, a library of custom automation, and hands-on keyboard responses to detect, halt, and eradicate threats. We leverage Microsoft and your other security investments, working alongside you, inside your environment and leveraging your tools to keep infrastructures, operations, and assets secure.

Cybersecurity is a Team Sport

Cybersecurity involves working with our clients to halt threats and keep operations, assets, and people secure.

Whether our clients are transitioning from on-premises to the cloud, are between SIEM providers, or starting over from scratch, they can rely on BlueVoyant to be there every step of the way.

BlueVoyant partners closely with Microsoft and is an expert at implementing Microsoft's SIEM Plus XDR strategy uniquely for your organization.

Our Deployment Services and MXDR services will have you up and running quickly, optimize your investments, and keep you secure 24×7 while preparing you for the future.

BlueVoyant

BlueVoyant MXDR for Microsoft

Halt Ransomware
We combine the power of Microsoft's security products with our elite 24×7 security operations, content engineering, correlations, and threat intelligence to identify and halt today's most sophisticated ransomware threats before they start.

Outpace Multi-Vector Attacks
BlueVoyant analyzes real-time network, user, endpoint IT security logs, as well as others. We correlate disparate data, and apply threat intelligence and automated playbooks to find and halt related threats across multiple systems, networks, and clouds.

Secure Cloud Apps, Data, and Workloads
BlueVoyant MXDR optimizes Microsoft Sentinel for Microsoft Defender for Cloud and provides visibility, control over data travel, and risk-based analytics to find and quickly combat threats across cloud services.

Block Email and Social Engineering Threats
BlueVoyant's MXDR investigates malicious threats in email messages, external links in files, collaboration apps, and other communication tools. Proactive and active threat hunting drastically reduces detection bypass risk.

Detect Compromised Credentials and Synthetic Identities
MXDR for Microsoft Defender for Identity with Microsoft Sentinel detects compromised credentials and malicious insider actions by correlating events, including those that appear innocent but are not.

Contain Persistent, Insider, and Highly Evasive Threats
We leverage cross-system attribution capabilities within Microsoft security products combined with our correlation and risk-based analytics to identify adversary activity, including malware-less attacks, advanced persistent threat actors, and historical compromises.

Secure Endpoints
BlueVoyant MXDR for Microsoft Defender for Endpoint protects data, assets, and business operations by inspecting IOCs and identifying malware, including ransomware variants, zero-days, and non-malware attacks.

Certified and Experienced Teams
At BlueVoyant, when it comes to security we don't believe in generalists. Your BlueVoyant expert teams focus on doing their job right — every time. They include Implementation, Client Success, SOC Threat, Content Engineering, Advanced Threat Detection, Threat Fusion Cell, Incident Response and Forensics teams.

BlueVoyant

More capabilities included with BlueVoyant MXDR for Microsoft

BlueVoyant DFIR (Digital Forensics and Incident Response)

DFIR includes incident forensics, root cause investigation, analysis, and reporting to stakeholders. Evidence processing is performed in Azure with a proper chain of custody and includes legal support with expert witness testimony. Meet cyber insurance and regulatory requirements with experienced crisis commanders and complete threat lifecycle management.

BlueVoyant Scan and Protect

Scan and Protect provides proactive threat detection across the clear, deep, and dark web with unlimited takedowns of phishing sites, social media impersonations, and rogue apps. Automated threat validation virtually eliminates false positives and delivers high-fidelity threat data. Expert cyber threat analysts provide context and track threat actor behavior and campaigns.

BlueVoyant VISIBL for Microsoft MDVM

VISIBL for MDVM (Microsoft Defender Vulnerability Management) enables organizations to conduct automated, recurring scans to help identify and investigate vulnerabilities in their IT environments in near real-time and includes our cloud-based dashboard. Senior vulnerability assessors will help implement and validate tests and provide actionable guidance on remediation next steps.

Assessments and Engagements

In addition to our deployment, MXDR, and other security services, our expert-lead assessments and engagements help you:

- Examine Identities, Devices, Incidents, and your organization's M365 Defender Security Portal to identify vulnerabilities and provide recommendations.
- Assist with utilizing Microsoft 365, Defender for Cloud, and Sentinel to their fullest potential.
- Review your Secure Scores and provide insights to improve security while managing costs.
- Leverage our CIS-based maturity engagements to illuminate the key elements of a holistic security program and help identify your strengths and vulnerabilities.

Ready to get started? Schedule a demo.

BlueVoyant combines internal and external cyber defense capabilities into an outcomes-based cloud-native solution by continuously monitoring your network, endpoints, attack surface, and supply chain, as well as the clear, deep, and dark web for threats. The full-spectrum cyber defense solution illuminates, validates, and quickly remediates threats to protect your enterprise. BlueVoyant leverages both machine-learning-driven automation and human-led expertise to deliver industry-leading cybersecurity to more than 900 clients across the globe.

BlueVoyant

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