Solution Brief

Managed Detection and Response (MDR)

Extend protection from endpoint to cloud with BlueVoyant

Whether you take a single-stack or a best-of-breed approach to your security technology stack, then how do you handle the challenges of such as systems such as:

- Have you accounted for the blind spots in data silos?
- How quickly do you update your security content and is it uniform across your tech stack (e.g., EDR/XDR, SIEM)?
- Can you detect attacks that use low-and-slow actions across security tools?
- How well integrated is your security team/SOC with third-party systems?

Adversaries thrive on blind spots, slowly updated security content, lack of uniformity in content updates, living off the land actions to help them evade your cybersecurity posture.

BlueVoyant's Managed Detection & Response (MDR) provides a cloud-native, fully integrated security solution that utilizes a single dashboard to enable data collection visibility across multiple platform (such as endpoint, IoT, cloud workloads, networks) to avoid cross stack blind spots. Our Risk Based Analytics thwarts attackers who try to use low-and-slow actions to evade detection.

To help breakdown the data silos and provide a centralized repository of best of breed technologies, we have partnered EDR/XDR providers to provide you the best risk remediation possible.

BlueVoyant's team of world-class cybersecurity experts, elite proprietary data, and process automation, to serve as an extension of a company's security team, delivering a level of protection that helps businesses sustainably protect themselves in a changing threat landscape.

MDR identifies and mitigates threats as they emerge and ensures that businesses and wider ecosystems are always prepared for rapid, effective response, and threat neutralization. Clients benefit from our technology and cybersecurity expertise, and our consultative approach to solving their security problems.

Key Differentiators

- 40% SIEM log cost savings without sacrificing coverage
- Utilizing best practices from 4,500+ deployments across Microsoft and Splunk
- 100+ SOC personnel (Tier 2/3 analysts, Threat Hunters, Content Engineers) across 4 global SOC locations that can support local data residency requirements
- Our detection engineering rules find 40% more true positive risks compared to native tools
- Curated Threat Intelligence and Emerging Vulnerability alerts
- Centralized MDR view for multi-tenant organizations
- Supports compliance needs for SLED, DIB, and many others

Microsoft 2024 Partner of the Year Winner Security Award

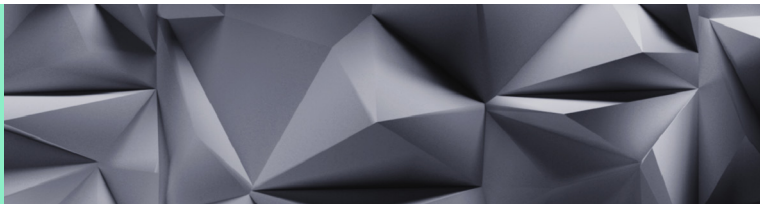
Cisco Partner Select Developer

splunk> Partnerverse Manage PREMIER

SentinelOne

CROWDSTRIKE

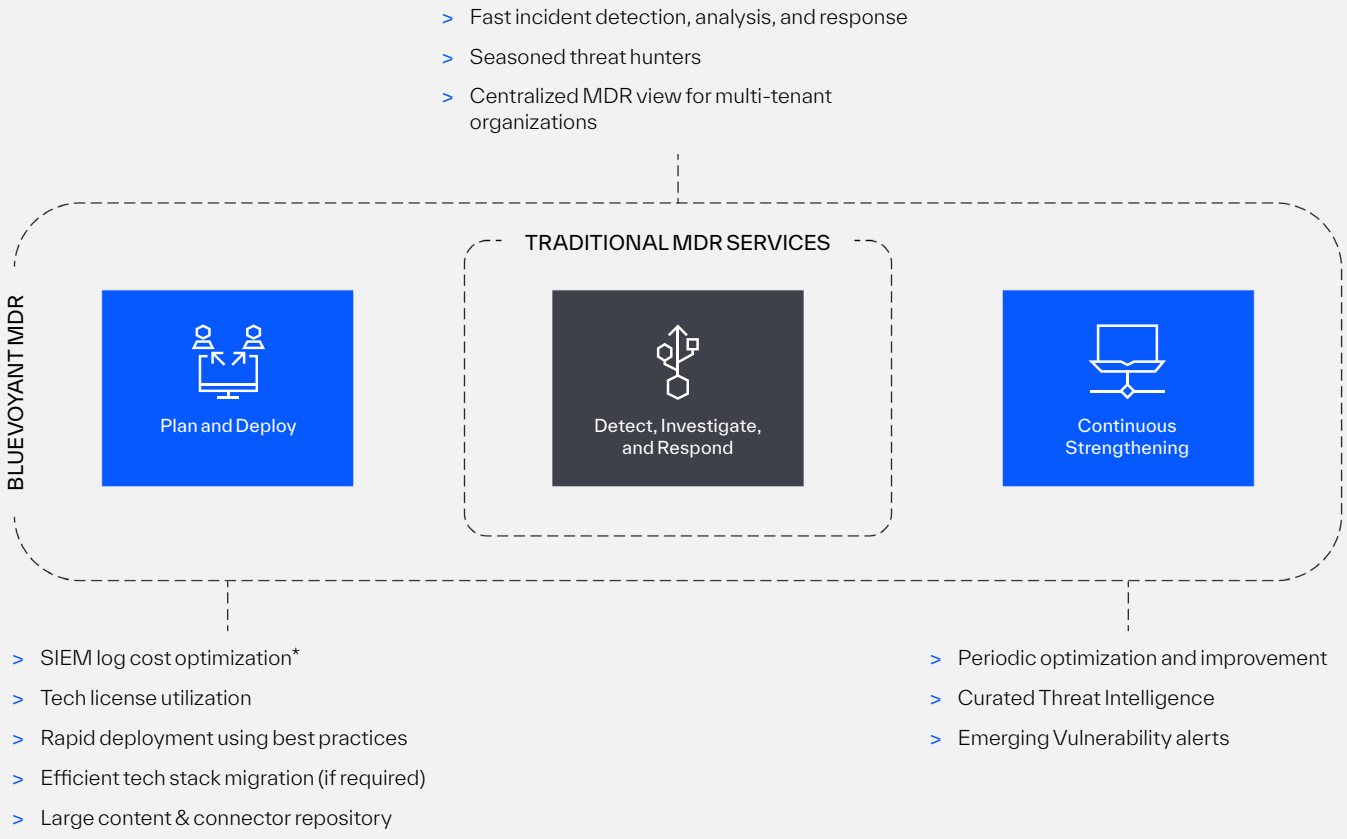
BlueVoyant



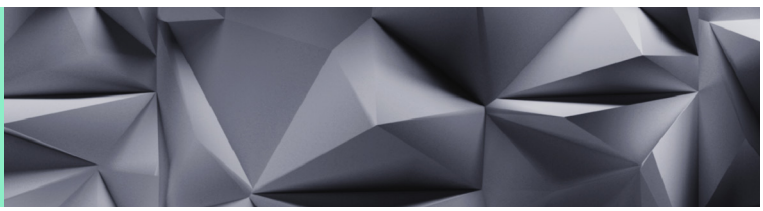
MDR Challenges BlueVoyant Solves

Planning	Deployment	Operation
> SIEM log cost optimization*	> Slow deployment without using best practices	> Slow incident detection, analysis, and response
> Tech license utilization	> Limited content and connector repository	> Inexperienced threat hunters
	> Painful tech stack migrations	> Lack of curated Threat Intelligence and Emerging Vulnerabilities
		> Decentralized MDR view for multi-tenant organizations
		> Lack of ongoing platform optimization and improvement

BlueVoyant MDR Provides Lifecycle Support



BlueVoyant



How BlueVoyant Solves MDR Challenges

SIEM log cost optimization*

Our SIEM deployment focus on ingesting logs with relevant security data which saves clients' money post-deployment. Additionally, as an MDR client we perform periodic SIEM log analysis to determine additional cost savings.

Tech license utilization

Clients want to use more of their Microsoft/Cisco licenses, but don't know the best approach to do it. We offer security diagnostics to help plan a good path forward to get more out of client licenses which we execute as part of our deployment.

Rapid deployment using best practices

We have performed over 3,300 Splunk and 1,200 Microsoft deployments, and we apply best practices from those engagements to effectively and efficiently deploy for you.

Large content and connector repository

BV has a pre-built repository with 350+ connectors & integrations to help you reduce deployment time. And as an MDR client, you can use this repository to add additional data sources.

Efficient tech stack migration

We have done a lot of technology migrations, and we can apply our best practices to help you avoid common migration pitfalls.

Fast incident detection, analysis, and response

We have 100+ SOC personnel across 4 global SOC locations staffed by Tier 2 and Tier 3 analysts, Threat Researchers, Threat Hunters, and Content Engineers. Thus, we are very seasoned in incident detection, analysis, and response.

Seasoned threat hunters

MDR clients have access to a seasoned threat hunting team that identifies and neutralizes threats designed to slip past conventional security defenses, ensuring no loose threads can damage the cyber landscape. We find the threat actor, create a detection alert/query that can be used by our SOC to keep you safe against future attacks using this attack vector.

Curated Threat Intelligence

Our MDR clients get a weekly curated Threat Intelligence email, bi-monthly Threat Landscape report, and an annual Sector Threat Landscape report as well.

Emerging Vulnerability alerts

BlueVoyant MDR clients will get alerted to relevant Emerging Vulnerabilities via email with details on the vulnerability, a list of products that affected, BlueVoyant's recommendations and client specific details (IP's / Ports running affected software).

Centralized MDR view for multi-tenant organizations

Our MDR has a Parent Portal setup to enable multi-tenancy so that parent cybersecurity teams can view all incidents, while child security teams can focus on the ones in their division/entity.

Periodic optimization and improvement

Our functional app conducts weekly controls assessment and provides remediation recommendations. Periodic SIEM log optimization recommendations*. Platform management, health monitoring, troubleshoot collectors, repair offline log sources.

Clients must utilize SIEM.

BlueVoyant MDR Supported Technologies

EDR	XDR	SIEM
> Microsoft Defender for Endpoint	> Microsoft Defender XDR	> Microsoft Sentinel
> CrowdStrike Endpoint Security	> Cisco XDR	> Splunk Enterprise Security
> SentinelOne Singularity		

BlueVoyant SOC provides 24×7 global security monitoring and support

Unlock the seasoned expertise needed to maximize your technology investment.

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