

Managing Security & AI in Local Government

Webinar
30 May 2024

1pm (AEST)
3pm (NZST)

Presenters



Martin Buckland
Microsoft Solution Specialist



Andrew Bentley
Generation-e Client Manager



Kash Sharma
BlueVoyant Regional Director



Monish Ramani
BlueVoyant Sales Engineer



Copilot



Copilot



Microsoft



Describe what a perfect day would be for a walrus and give them a name



Give some life advice that an astronomer would find inspiring and delightful



Compose a song about the ups and downs of life in a folk rock style

Ask me anything...

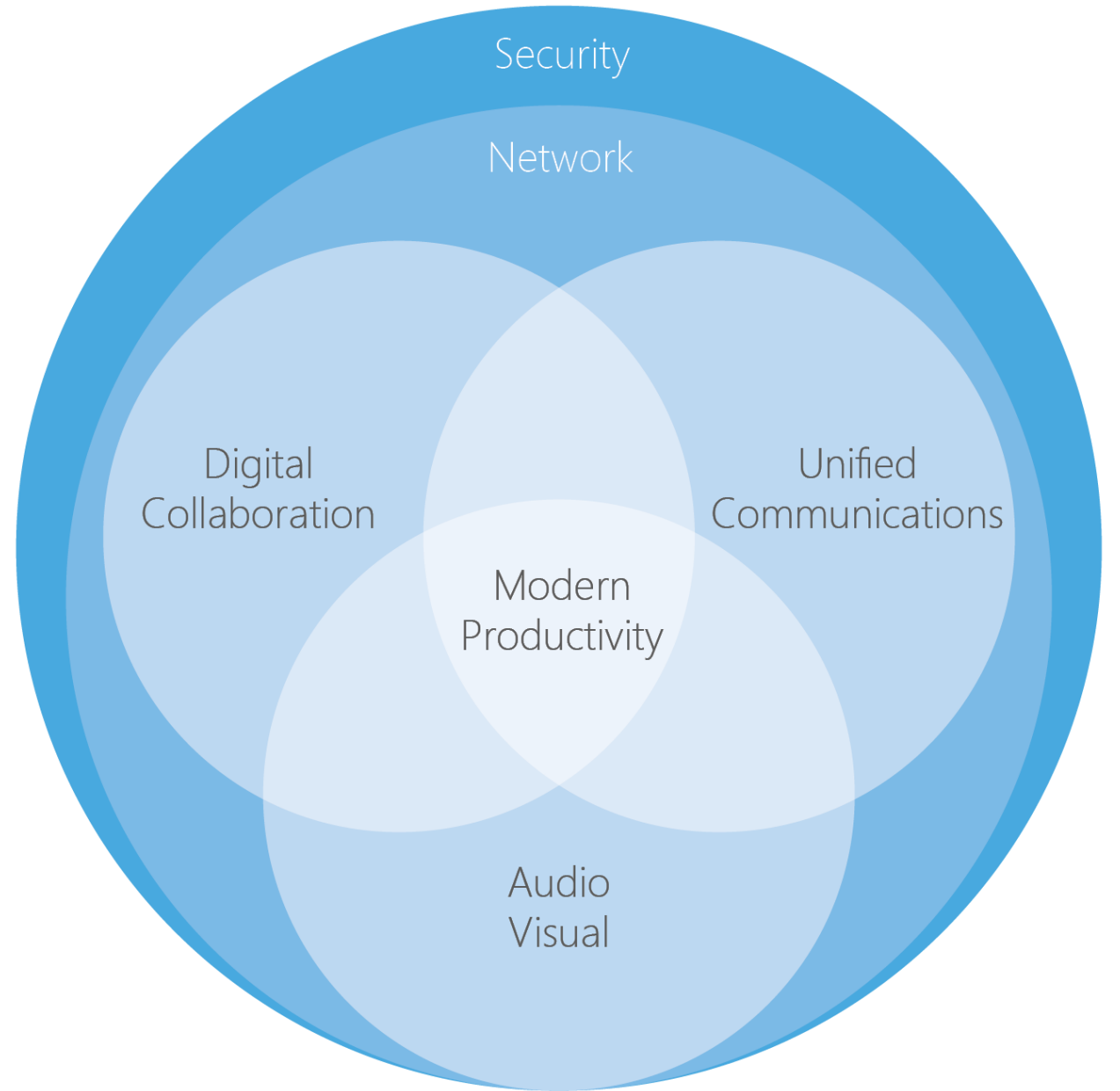


0/2000



We deliver this through our core capabilities.

Five areas of technology expertise in which we are the proven industry leaders.



Our professional services are delivered via a customer-centric model that delivers flexible project engagements through to fully managed service & as-a-service offerings.



Consulting

Change
Management

Managed Services

Our Story

Highly Confidential

6

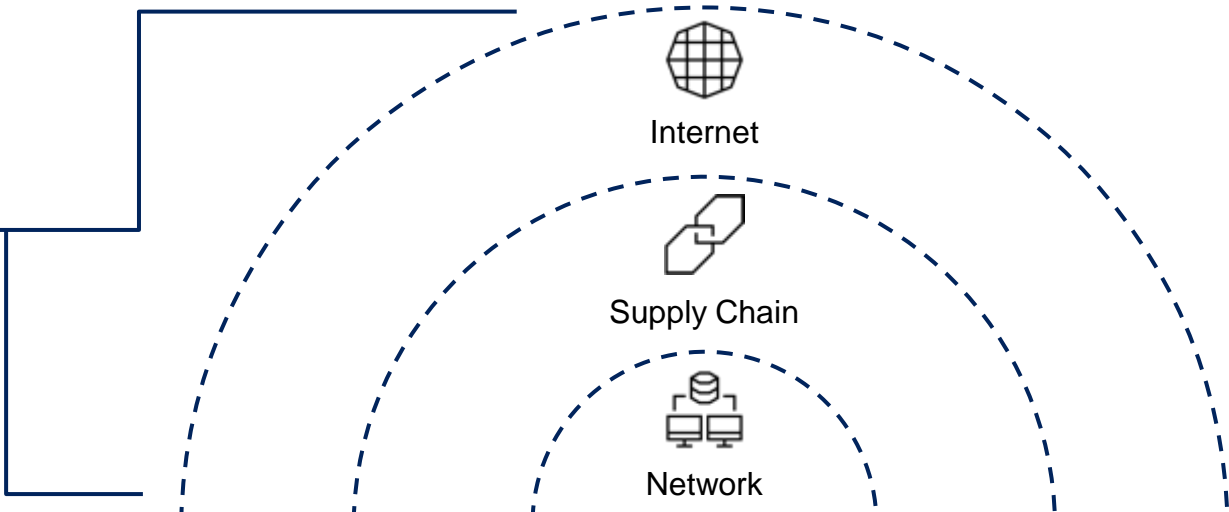
BlueVoyant was founded in 2017 by Jim Rosenthal (former COO of Morgan Stanley) and Thomas Glocer (former CEO of Thomson Reuters).

With decades of experience in high-stakes industries and having navigated market challenges including 9/11, the financial crisis and more, they foresaw the next big challenge: defending against rapidly evolving cyber threats.

With the founding of BlueVoyant, Jim and Thomas brought together leading experts from private industry and government in order to ensure that all organizations have access to best-in-class cyber defense, no matter their industry or geographic location.

Today, BlueVoyant offers an end-to-end platform that combines internal and external cybersecurity to help clients across the globe defend against the most sophisticated attacks.

Threat Landscape



BlueVoyant Platform



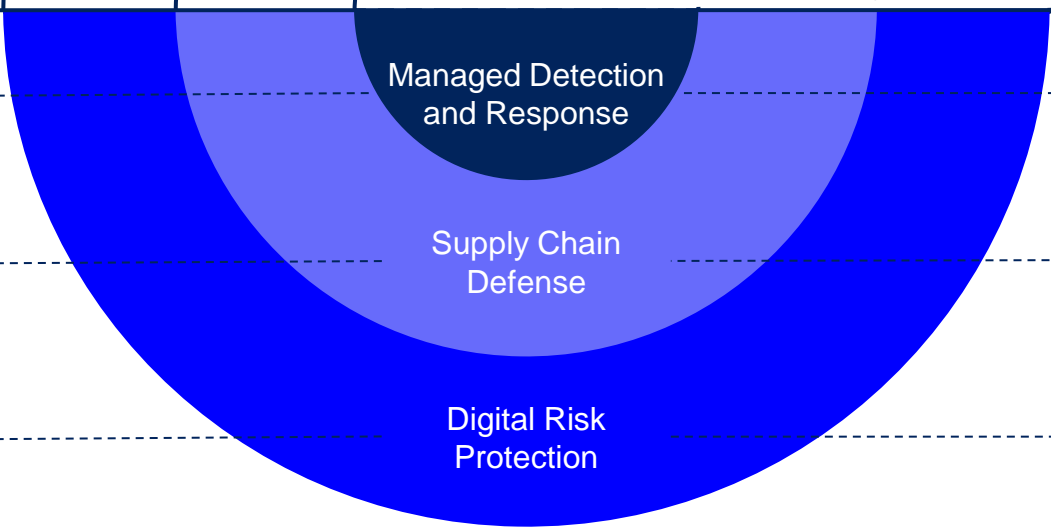
BlueVoyant MDR™



BlueVoyant SCD™



BlueVoyant DRP™



BlueVoyant PS™

What We Do | BlueVoyant Platform

Internal Security Services



BlueVoyant
MDR™

Managed Detection
and Response

- Microsoft Security and Splunk
- CrowdStrike, Carbon Black, Sentinel One
- 24x7 Monitoring, Management, and Threat Eradication
- Log Management - Threat Intelligence
- Detection Content - Automation

External Security Services



BlueVoyant
DRP™

Digital Risk Protection

- Digital Brand Protection
- Fraud Campaigns Discovery
- Account Takeover Monitoring
- Data Leakage Detection
- Executive Cyber Guard
- External Attack Surface Analysis



BlueVoyant
SCD™

Supply Chain Defense

- Supply Chain Monitoring
- Identity Cyber Defense Issues
- SOC-style Third-Party Cyber Alerting and Remediation



BlueVoyant
PS™

Professional
Services

- Digital Forensics
- Incident Response, Forensics and Incident Response Retainer
- Litigation Support
- IR Plan, Tabletop Exercises, Incident Prep
- Governance, Risk, and Compliance
- Security Maturity & Readiness Programs (CIS, HIPAA)
- Penetration Testing, Red Team/Purple Team
- Social Engineering & User Awareness
- VISIBL Vulnerability Identification Services



Microsoft Security Specialists

Microsoft Security Solutions

Microsoft Services:

- Microsoft Sentinel Deployment Service
- M365 Defender Deployment Service
- Defender for Servers Deployment Service
- MXDR for Sentinel
- MXDR for M365 Defender
- Digital Forensics and Incident Response (DFIR)
- Scan and Protect – External Digital Risk Protection
- VISIBL- Vulnerability Scanning

Complementary Solutions:

- Microsoft Solution Assessment Engagements
- Cyber-insurance consulting
- Azure data ingestion optimization
- 3rd Party Cyber Risk Mgt.

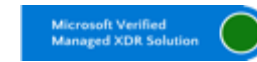
Sentinel Content Engineering

- Content library of over **1,000** analytic rules mapped to MITRE ATT&CK framework.
- **350+** custom validated Data Connectors for ingest and parsing of Microsoft and 3rd Party data sources.
- Scalable “as-code” Sentinel content deployment technology with weekly/daily detection updates.
- Specialized Workbooks and Playbooks for key SecOps and data/cost management use cases.
- ITSM integration via REST API and dedicated apps

Enterprise Experience

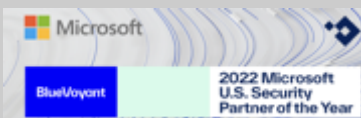
700+ production deployments of Microsoft Sentinel in enterprise environments in 30+ countries, including:

- **US Hospital network** with 42,000 employees; presence in 11 states; \$8B revenue. MXDR Sentinel+M365D solution.
- **Top North American research university** with 62k students; deployment of M365 Defender and Sentinel; SecOps training program
- **Large State Government with 100K+ endpoints** and dozens of independent agencies with unique security requirements.



Recent Accolades:

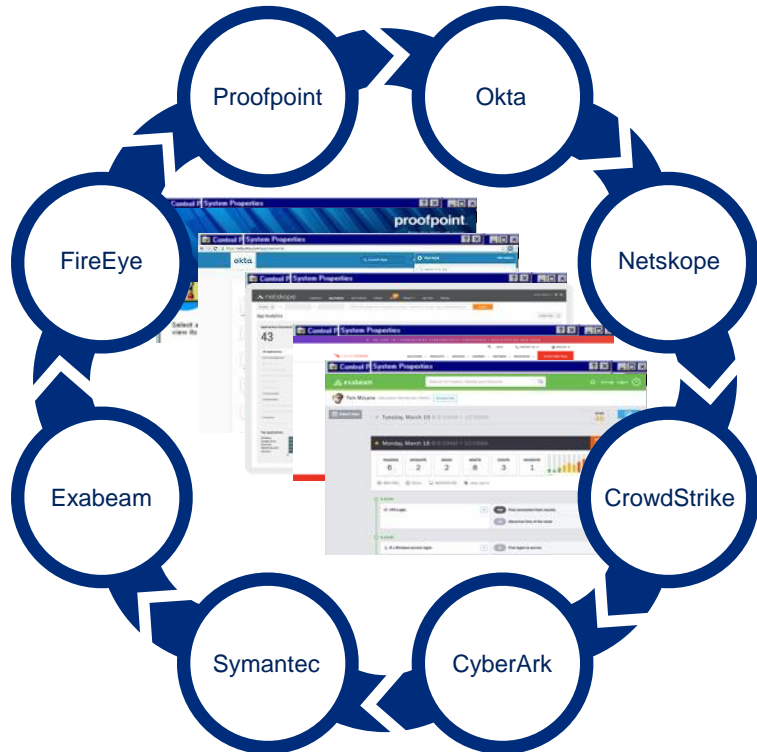
- **Winner - Back-to-Back 2023 / 2022 Microsoft US Security Partner of the Year**
- **Winner - 2023 Microsoft Security Excellence Awards for Security MSSP of the Year**
- **Winner - 2021 Microsoft Security 20/20 Partner Awards for “Top MXDR Team”**
- **Microsoft MXDR Verified Partner**
- Finalist – 2022 Microsoft Security Excellence Awards for Security MSSP of the Year
- Finalist – 2022 Microsoft Impact Awards (CA) for Top Security Partner and Top Healthcare Partner
- Advanced Security Specialization, Cloud Security Advanced Specialization
- Microsoft Security Experts design partner
- Authors of Microsoft Sentinel Deployment Best Practices field guide (2021/2023)



MXDR for Microsoft

Enhance and Simplify Your Security Operations with the BlueVoyant MXDR and Microsoft Technologies

Security at some companies looks like...



Highly Confidential

 **BlueVoyant**

Security for BlueVoyant MXDR customers looks like...



 **BlueVoyant**



BlueVoyant MXDR for Microsoft

What we do

Deploy	Design, build, and operationalize Microsoft Sentinel & M365 Defender in your environment
Manage	Expert maintenance, management, and strategic advice for your Sentinel SIEM deployment, including continuous content updates and log tuning
Monitor & Respond	24x7x365 cloud-based security monitoring and threat eradication from trained SOC Analysts and Threat Hunters, aligned to MITRE ATT&CK framework



Our shared outcomes

Control Costs	Data source advisory, vendor consolidation, and automation of response actions to optimize costs and manage resource requirements
Increase Visibility	Scalability and standardization of SIEM content for all enterprise security products, infrastructure, and applications
Defend Faster	Current Mean Time To Acknowledge (MTTA) security incidents in <15 minutes , with integration to your ITSM tools

Manage, Monitor, and Respond

Do More with Less - BlueVoyant for Microsoft


BlueVoyant Microsoft Security Technology Expertise

- Sentinel Content Engineering team for custom content on demand
- Security & Automation co-managed within your Microsoft Sentinel
- Log onboarding and optimization of new data sources
- Continuous access to Microsoft Security technology experts


BlueVoyant Security Operations Expertise

- 24x7x365 SOC Analysts with live response
- Weekly SIEM content updates; Rapid zero-day detections
- Proactive Threat Hunting and Response
- Integrated global threat intelligence

Platform Leadership




700-plus
Sentinel
Engagements



950-plus
Developed
Alert Rules



Fast Reporting
Workbooks
Deployed



**Bespoke
Automation
Playbooks**



350-plus
Data
Connectors




**Aligned to
MITRE ATT&CK
Framework**



Extending Security Capabilities



40-plus
Threat Intelligence
Sources



100%
Automated
Enrichment




< 15 min.
MTTA



9.8
Avg Years of
SOC Experience



> 145
Certifications
Held

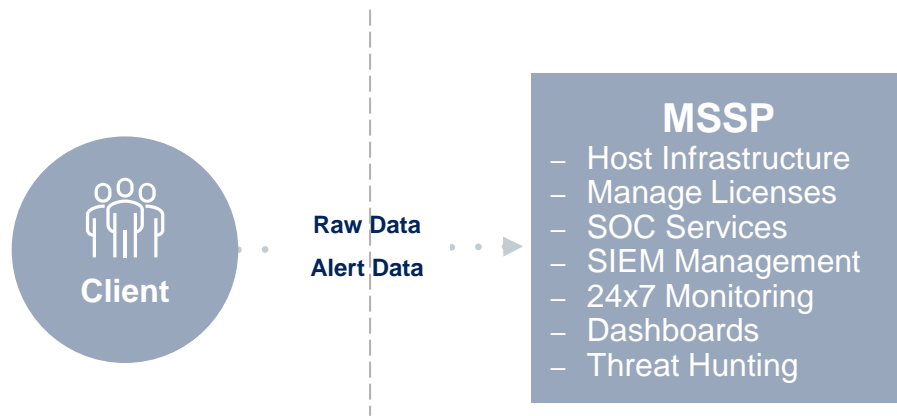


90%
Automated
Triage

Unique to BlueVoyant is Our Co-Managed Approach

Other MSSPs Approach

- Log and alert data sent to MSSP infrastructure for analysis
- 'Black-box' analytics designed to accommodate wide variety of security technologies
- Alerting and reporting as outputs via the MSSP's portal



BlueVoyant's Co-Managed Approach

- We work within our client's environment, optimizing Microsoft security tools with BlueVoyant analytics, automation, and expertise
- Detection content deployed in our client's environment - stays in their environment
- Complete visibility to all BlueVoyant operations in the Azure environment, auditable and access controlled



The BlueVoyant approach enables our customers to:



Maximize your investments in Microsoft technologies



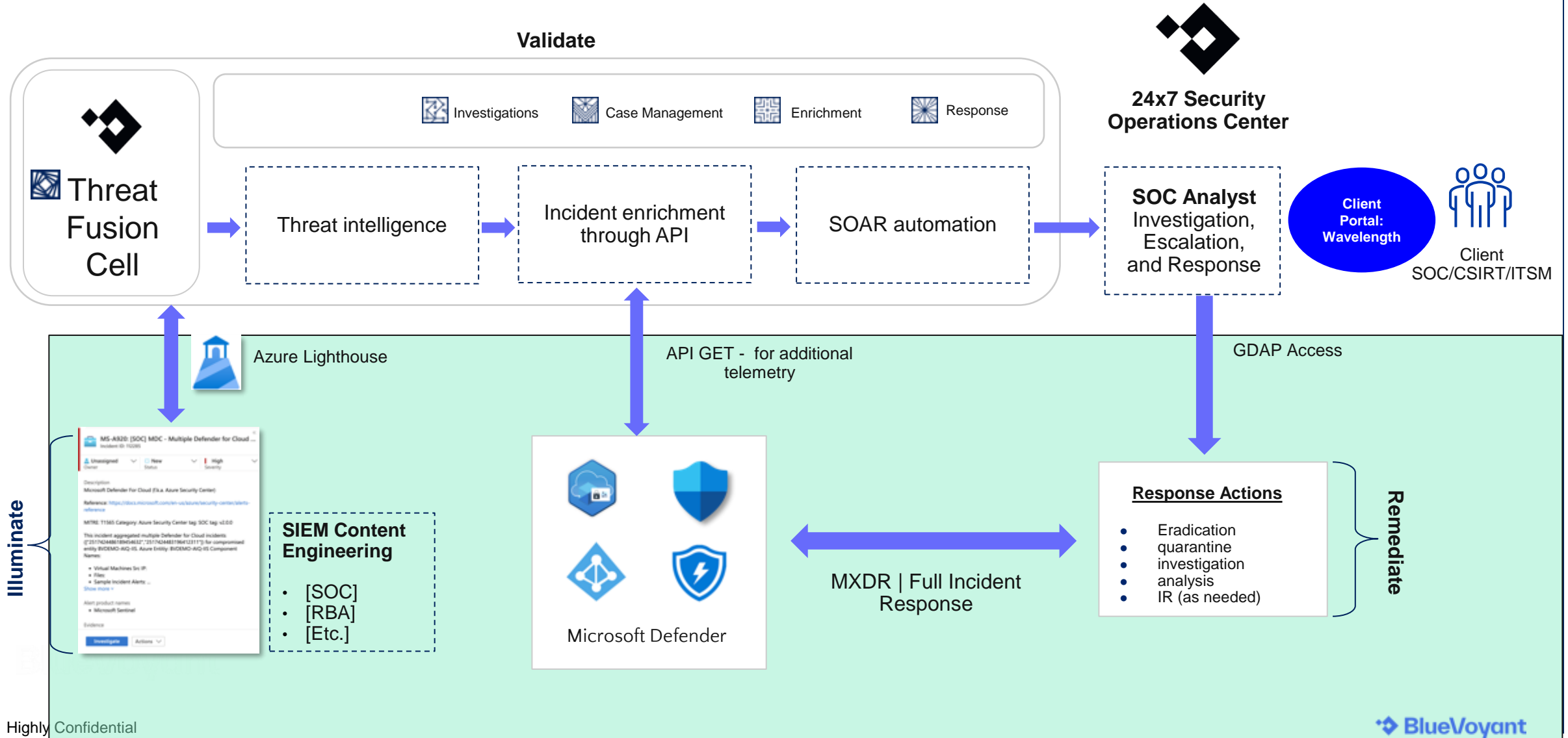
Minimize data egressing your environment



BlueVoyant Platform Approach | Microsoft MXDR

BlueVoyant

Customer Environment

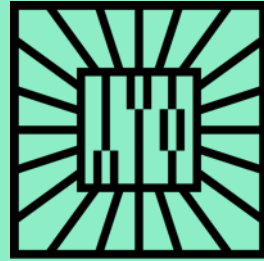


BlueVoyant: MXDR for Microsoft in State & Local Government



Protect Infrastructures

Combine Microsoft 365 Defender with BlueVoyant's elite 24x7 security team to identify, investigate and eradicate today's most sophisticated cyber threats. Whether you have one or multiple departments and Sentinel tenants, BlueVoyant provides the same level of protection for them all - 24x7.



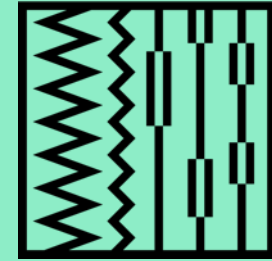
Secure risky public data

Our active and proactive threat hunting uses advanced machine learning and is designed to identify adversary activity, risky users and sign-ins., cyber-attacks, and advanced persistent threats and eliminate them quickly.



Protect government cloud apps

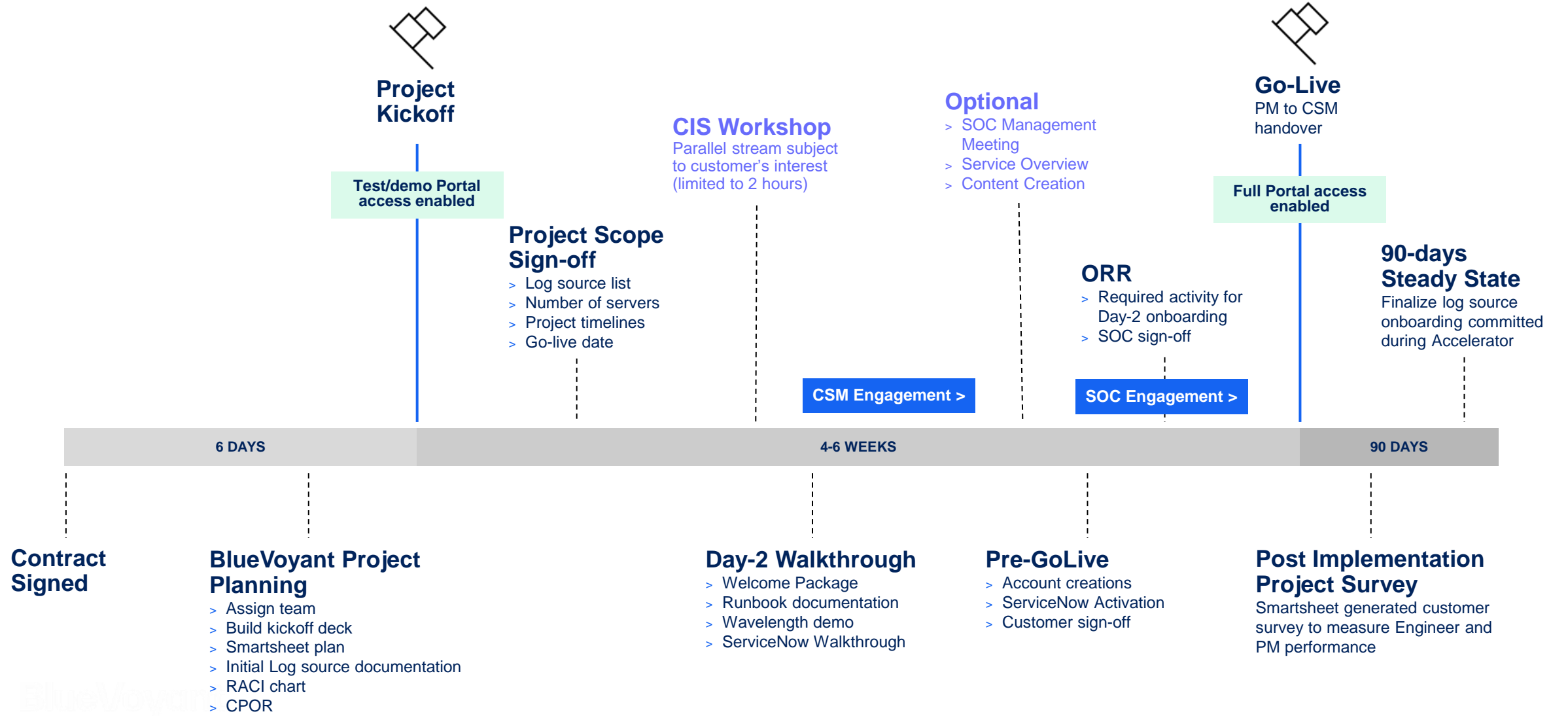
Microsoft Defender for Cloud Apps with our MXDR provides visibility, control over data travel, and sophisticated analytics to quickly find and combat threats across all cloud services.



Meet regulatory compliance

Our array of regulatory compliance reporting capabilities, well-defined SLAs, with fast incident response, and eradication ensure you stay secure and compliant. Rely on our SOC metrics to track KPIs that help you ensure operational excellence.

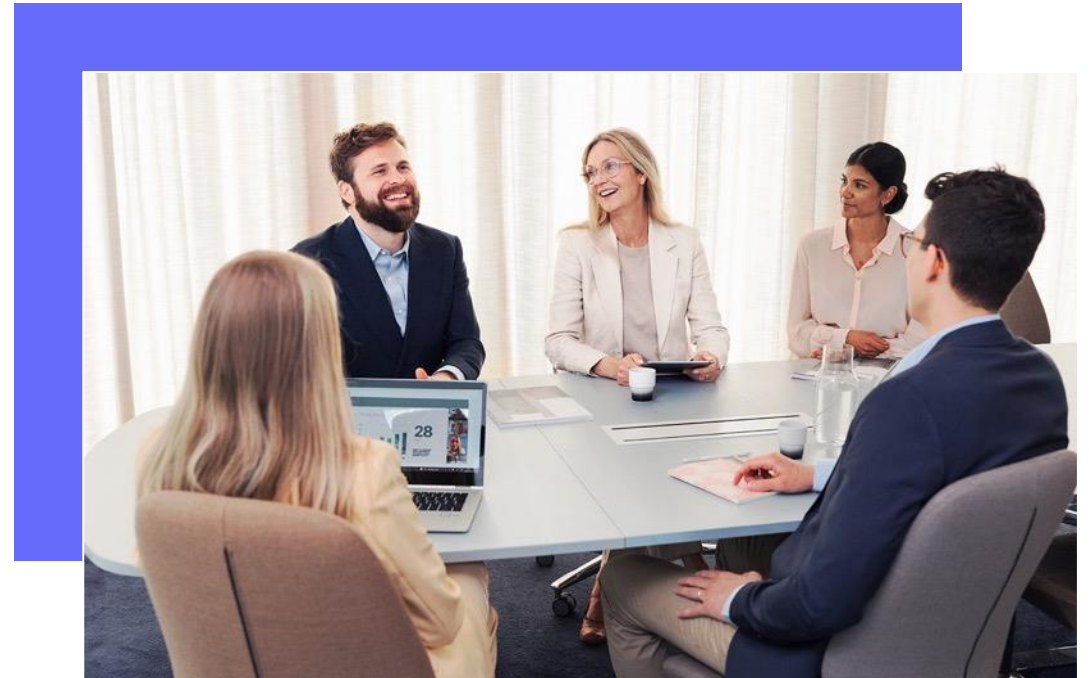
BlueVoyant Typical Deployment Lifecycle - MXDR



BlueVoyant Security Diagnostics and Assessments – Zero cost to You

Assessments, insights, and data to help you move forward

- Sessions between you and our experts
- Gain insights and actionable data about Microsoft's security products - tailored to your environment
- Provides the information you need to move forward with BlueVoyant Deployment and MXDR 24/7 Managed Security Services



Security Diagnostics and Assessments to Support You

Exploring the Cost of Adopting Microsoft 365 E5

Realising the full value of Microsoft 365 E5 requires knowing the real-world operational and security benefits vs. costs.

Microsoft 365 Threat Gap Analysis

Analysis of M365 platform security posture evaluates vulnerabilities and risks with recommendations to mitigate

Exploring the Cost of Adopting Sentinel

The major factor in realising the full value of Microsoft Sentinel is understanding how to manage and predict costs.

Microsoft Copilot for Security Readiness

Understand what's possible, how and where to start first, and what you need to be successful

[Click HERE to request an assessment](#)

Thank-you

