Europe's first digital general contractor

One DIGITAL company

econocom
equipment | services | financing

# Econocom & BlueVoyant

## Winning together


Steve Dierckens

Dylan Crokaert

Vincent Turner


BlueVoyant

# Introduction | **Who are we?**

BlueVoyant is a global **expert-driven** end-to-end cybersecurity services company whose mission is to proactively **defend** organizations of **all sizes** against today's constant, sophisticated attackers and advanced threats.

**Leadership, Experience, Global Presence**

**700+ employees, 900+ Customers**

## Exemplary Leadership

Co-Founded in 2017 by F500 Executives and Former government officials, together with private sector experts

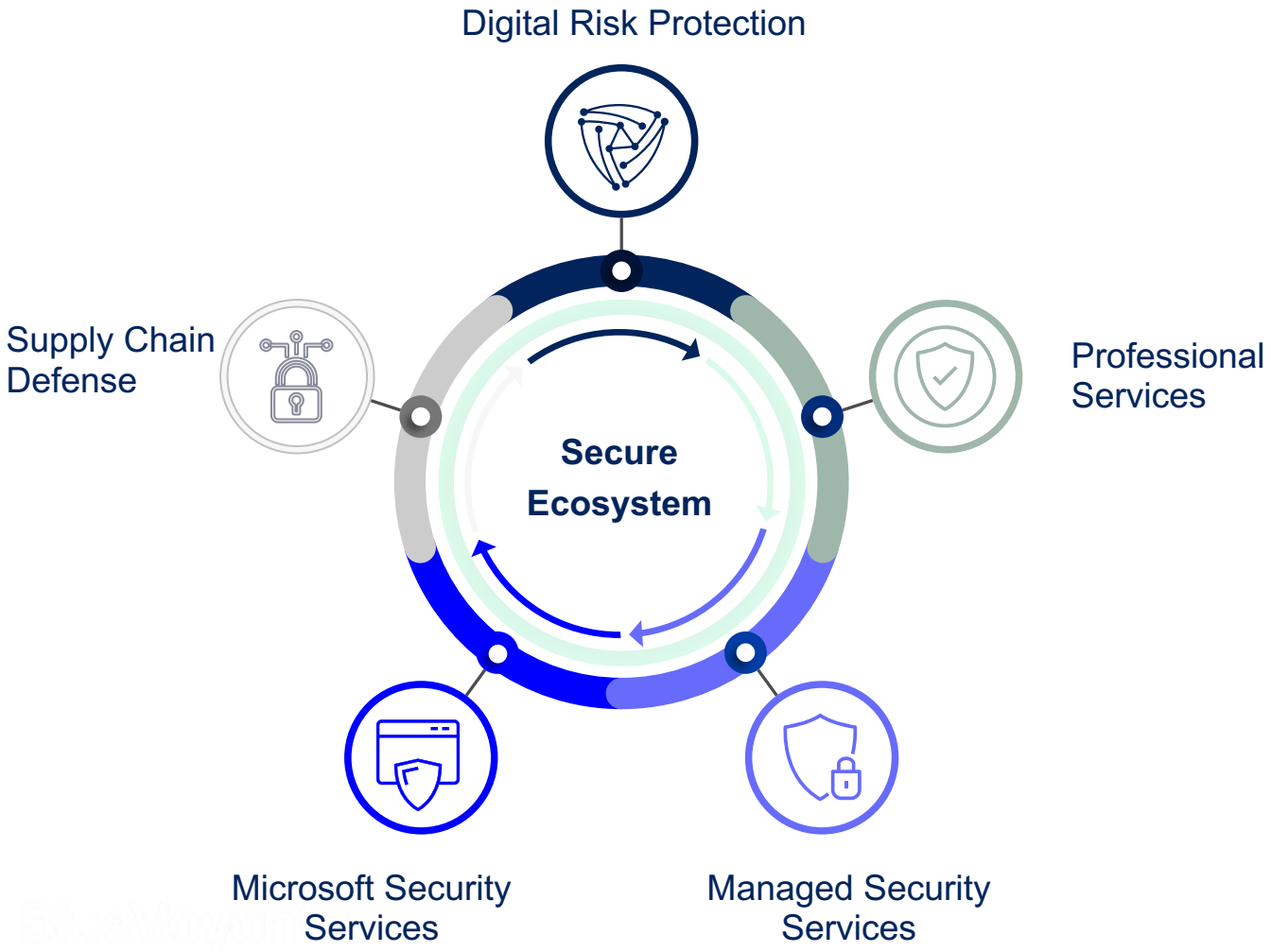
## Global Footprint

New York City (Headquarters), Amsterdam, Maryland, Tel Aviv, San Francisco, London, Manila, Toronto and Bogota

## Global BlueVoyant SOC

Budapest, Geneva, London, Maryland, Singapore + local delivery

# Introduction | **Our Solution Portfolio**




### Supply Chain Defense

Effectively manages supply chain risk, with BlueVoyant becoming an extension of your risk operations team.

### Digital Risk Protection

Proactive search and takedown of fraudulent use of digital assets, and discovery of leaked digital assets and credentials

### Professional Services

Reduce attack surface with Vulnerability Management, Penetration Testing and tabletop exercises. Put expert Incident Response services in place to be prepared.

### Managed Security Services

Effective Managed Detection and Response solutions provide 24x7x365 monitoring, investigation and response from our Security Operations Center.

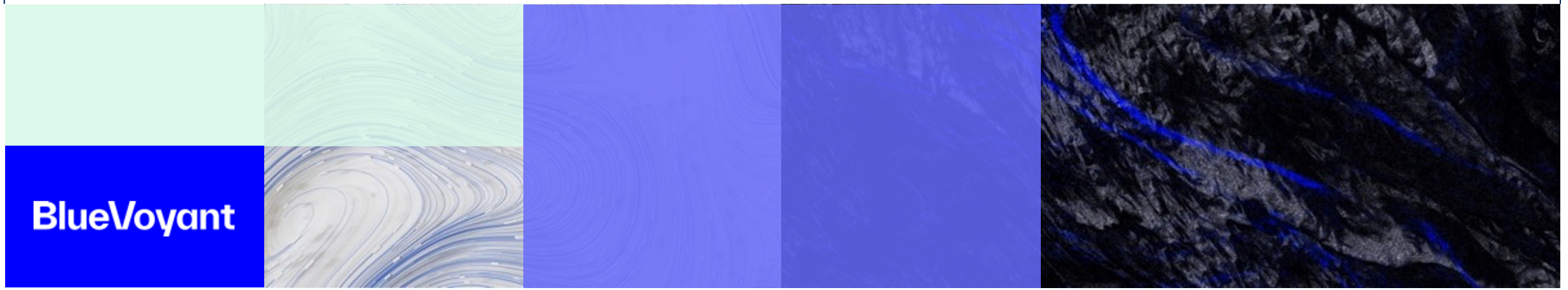
### Microsoft Security Services

For organizations investing in Microsoft Cloud and Security technology, Bluevoyant brings specialized expertise in Microsoft XDR solutions including Azure Sentinel and Defender.

BlueVoyant

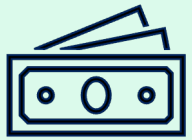

Europe's first
digital general
contractor
One
DIGITAL
company
econocom
equipment | services | financing

# Our Value


BlueVoyant

# Our Value | **Financial Value**

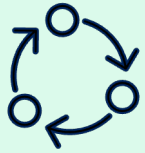
## Margin



### Margins apply on all BlueVoyant deals

- Default margin on BlueVoyant deals is 15%.
- When registered on the partner portal, margin can go up to 25%.

## Approach



### Guidelines on the approach

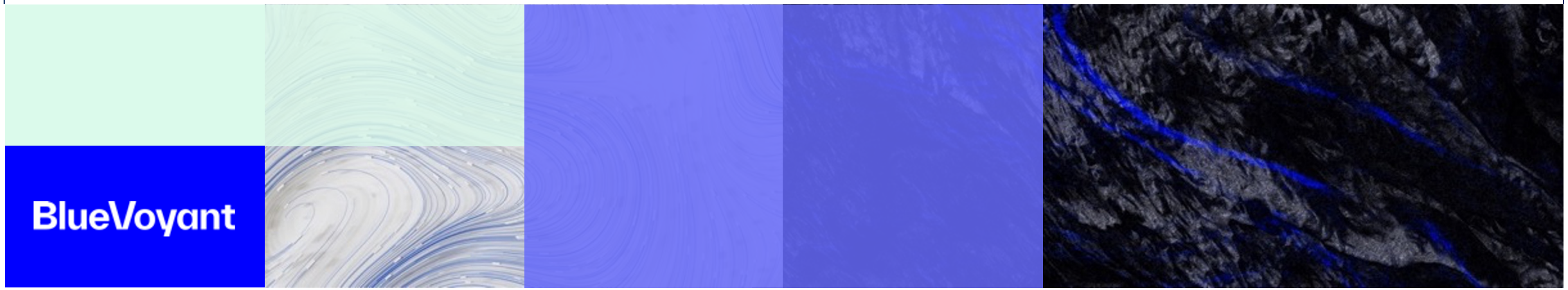
- Cyber Security is a hot topic, and can act as a door opener
- We are available (*Steve Dierckens & Dylan Crokaert*) to support on every deal to co-sell.
- Koen Matthijs or Frank Reymenants are your SPoC for every BlueVoyant deal registration.
- Once the service is in place, many up-sell opportunities ( CIS, MITRE, … )

## Qualification

### Our target customers

- Upsell for all current managed services contracts of Econocom
- Starting from 600+ endpoints.
- Actively using Microsoft Azure services
- Looking to mature their SOC, EDR, XDR and/or SIEM approach
- Microsoft E3/E5 license in place


# Our Solutions



# Our Solution | **Demystifying the SOC**

***What is a SOC?***

**Key Functions:**

- 24/7 continuous human monitoring
- Monitoring on network, infrastructure and applicative level
- Detection, Triage & Response of your Security Incidents

**Why do you need it:**

- Proactive threat detection & prevention
- Efficient incident response & remediation
- Improved risk management

# Our Solution | **Demystifying the SOC**

> ***How about Pricing?***

**Cost Approach:**

- Pricing is a mix between the following elements:

1. Tools to manage (EDR/XDR/SIEM)
2. Number of endpoints
3. Build + Run + Extra Services

**Ballpark Costs Examples:**

- 6000 Endpoints SIEM + EDR project

1. Set-Up Cost = **60,000 EUR**
2. Run Cost = **290,000 EUR** Yearly

- 2000 Endpoint SIEM project

1. Set-Up Cost = **20,000** EUR
2. Run Cost = **67,000** EUR Yearly

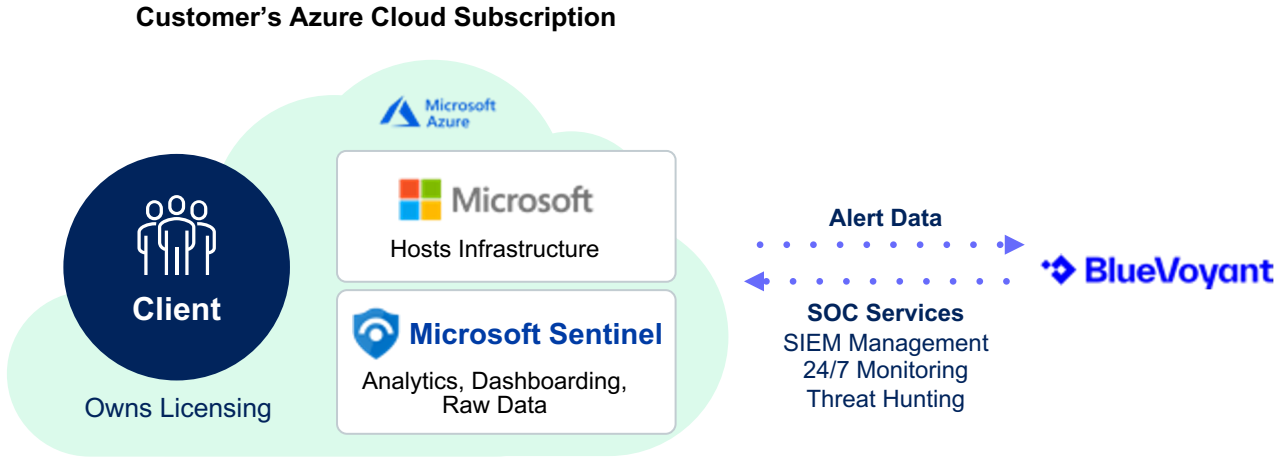
# Our Solution | **SOC Methodology**

## Other MSSP Approach

Client has to come to MSSP and send their data to MSSP platform.


## BlueVoyant's Approach

We go to your Cloud-native platform; 100% transparent metrics.



# Our Solution | **Metrics**




Microsoft retained BlueVoyant to author the 2021 Azure Sentinel Deployment Guide

**430+** Sentinel Engagements

**15-17** net new Sentinel deployments/month

**4-6 weeks** average deployment

**Dedicated:**

- EU Engineer
- EU Architect
- EU Project Manager

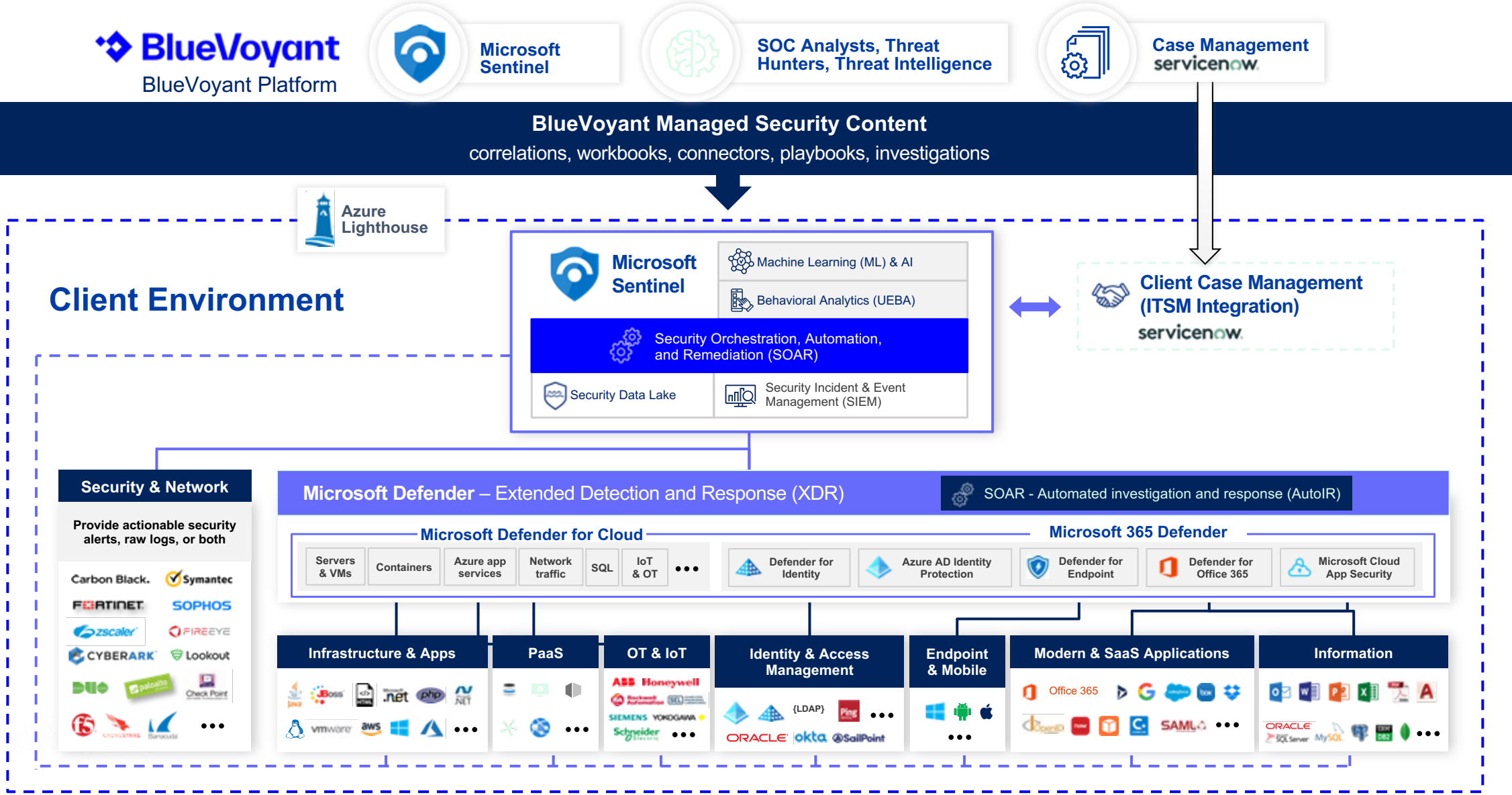
**The Standard Microsoft Sentinel Deployment Best practices**

Microsoft Partner
Microsoft
Gold Security
Gold Data Platform
Gold Cloud Platform

Member of Microsoft Intelligent Security Association
Microsoft

AICPA SOC
SOC 2 TYPE II CERTIFIED

# Our Solution | **Architecture**



# Our Solution | **Differentiators**

01

## Our Focus

Enabled by our **Portfolio**

02

## Our Transparency

Enabled by our **Architecture**

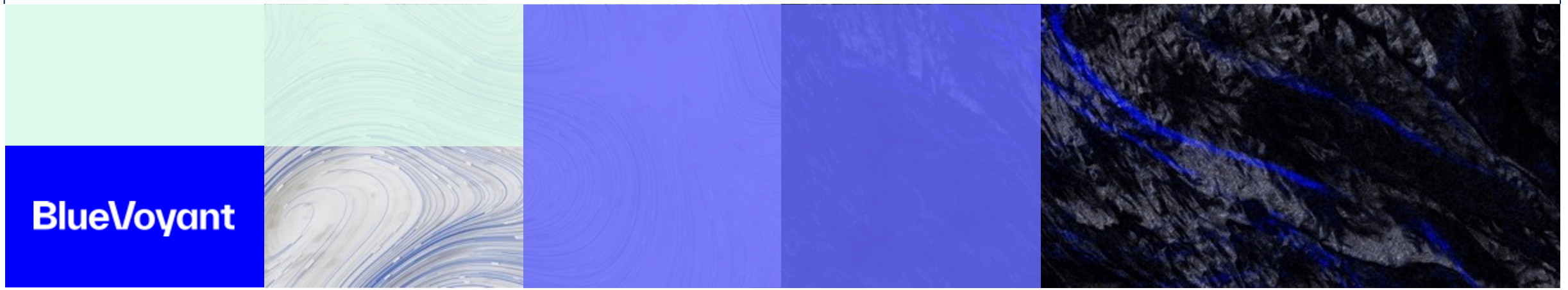
03

## Our Speed

Enabled by our **Experience**


# Econocom & BlueVoyant

Backup

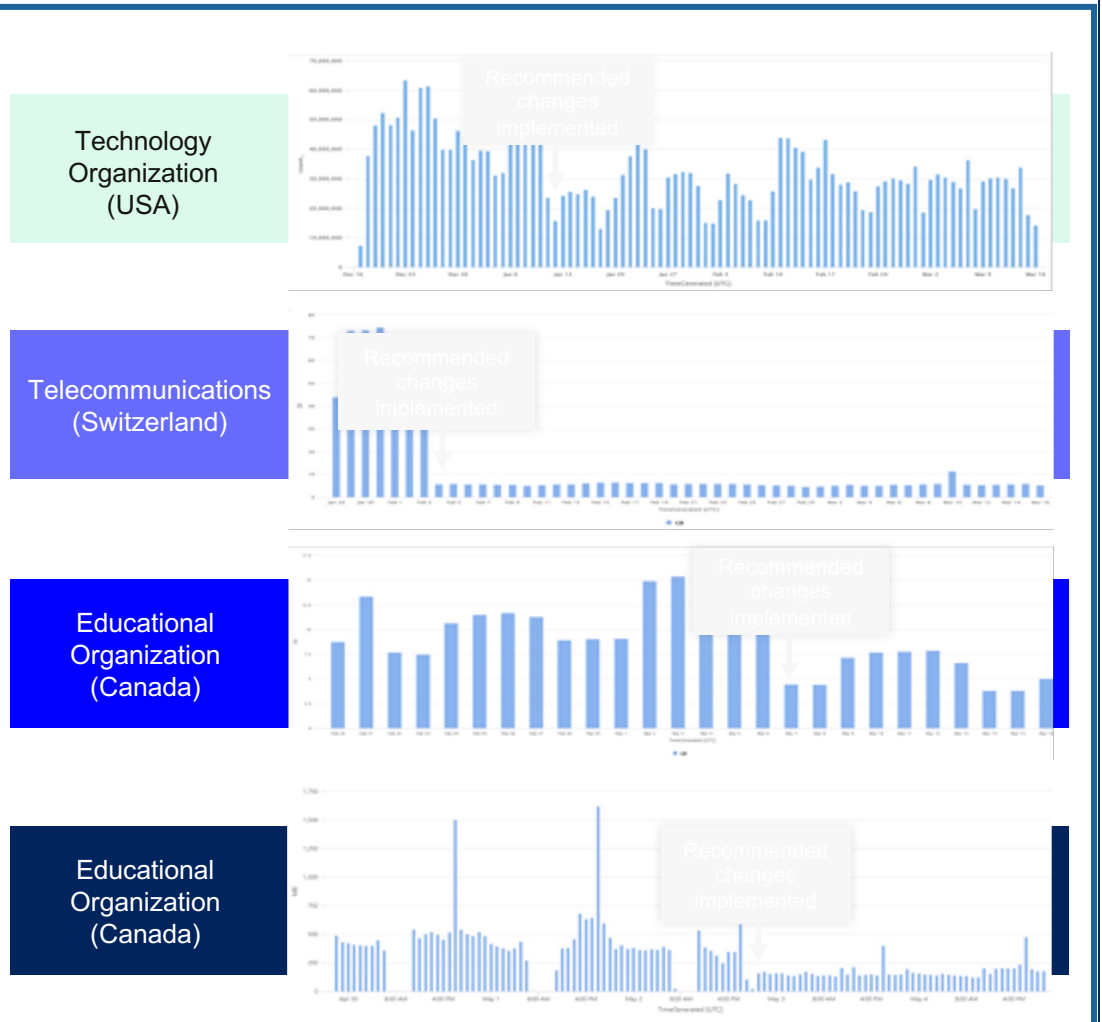


# Our Solution | **Cost Optimization**

## Strategies and Techniques

- Custom CEF templates
- Firewall logging analysis and strategy
- Windows event IDs analysis / GP settings
- Deployment and configuration of Log Collectors using a variety of technologies
- Analysis of log data cost vs. actionable intelligence


Average Cost Reduction



# Our Solution | **SOC Collaboration**

- Client Management & Project management
- SOC Governance & Customer Service Manager
- SOC Compliance
- SOC Advisory (Optimisation & Advisory)
- Threat Hunting
- Threat Intelligence
- SOC Tier 3 – In depth analysis, Mitigation & implementation
- On-site Incident Response
- SOC Tier 2 – Revalidation & Proactive TH
- SOC Tier 1 – Initial Triage & Mitigation
- SOC Engineers
- Advisory (Assessment & Design)
- Implementation / Onboarding
- SOC Platform & Tools (SIEM, Lighthouse, Threat Intel, Ticketing, Wavelength)

**Econocom**

**BlueVoyant**

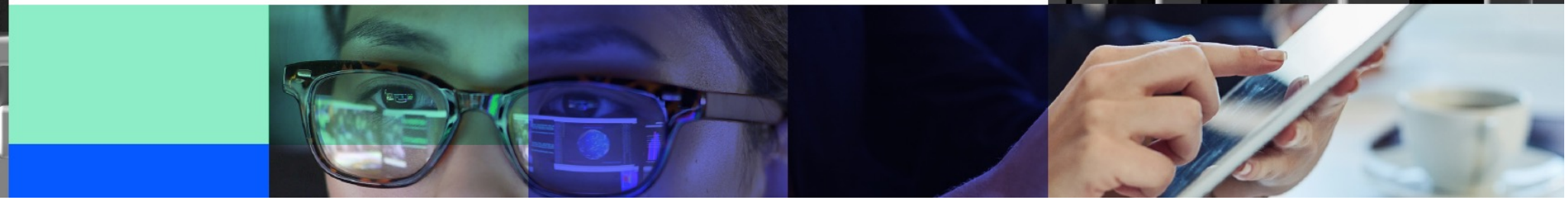
**Econocom + BlueVoyant**

# Introduction | **Trusted Partners**

econocom + Microsoft + BlueVoyant

# BlueVoyant MXDR for Microsoft

## Playbook for Sellers, Resellers, and Partners



BlueVoyant

# BlueVoyant MXDR for Microsoft SIEM (Sentinel) Plus XDR

## Problems Microsoft SIEM (Sentinel) Plus XDR Solves

Microsoft's strategy for securing the enterprise is Microsoft SIEM Plus XDR, which combines all its security products into one.

When security analysts need to wade through logs and alerts from dozens of tools without metrics, intelligence, contextual data, or correlation, it's challenging to identify threat patterns, routes, infiltration, and damage across an organization's entire digital estate. Extracting security insights from disparate data sets from a patchwork of poorly integrated third-party security systems creates an overwhelming number of false-positive alerts and alert chatter. Too much time, effort, tools, and resources are required to identify and contain a threat— and might still not be enough to detect and eradicate a highly sophisticated threat, especially one designed by a hostile nation-state. These sophisticated threats move quickly across different domains within the customer's digital estate and can hide for weeks or months without detection.

## Microsoft SIEM (Sentinel) Plus XDR Solution Overview

By consolidating security tools and operations with Microsoft and then combining Microsoft Sentinel with Microsoft 365 Defender and Microsoft Defender for Cloud for a SIEM Plus XDR strategy, clients gain centralized insights across their entire digital estate. They can use a single platform with integrated intelligence and automation to detect threats quickly and protect endpoints, infrastructures, and clouds.

When threat intelligence and security data are correlated, and response is orchestrated across tools and domains, SOC (Security Operations Center) experts have the visibility and insights needed to hunt and eradicate a threat more quickly. Even if a threat attempts to mutate, multiply, move, and hide, a central Microsoft SIEM Plus XDR security infrastructure will identify it, track it as it moves, and contain and eradicate it before it does serious harm. SIEM Plus XDR leverages historical data from the organization, other clients, and threat intelligence feeds to detect unknown and new variations of known threats. It can expand its portfolio of attack stories and, with the aid of Microsoft Sentinel machine learning and continuous security self-assessment, will become more efficient, faster, and secure over time.

## BlueVoyant MXDR for Microsoft

BlueVoyant MXDR (Managed Extended Detection and Response) for Microsoft delivers a combined solution of assessment, implementation, automation, analytics, intelligence, and technology. Add to that a 24×7×365 security team of Microsoft security experts that provide end-to-end monitoring and management of the client's Microsoft SIEM Plus XDR strategy. We enhance Microsoft SIEM Plus XDR with data, automation, and intelligence previously available to the Fortune 100. Regardless of the maturity of the client's SOC (Security Operations Center), we can drive scale and standardization while helping to monitor and defend the client's organization 24×7 from sophisticated threats.

## Types of Threats and Vulnerabilities Managed by BlueVoyant

- Ransomware
- Cloud app vulnerabilities
- Compromised banking credentials and synthetic identities
- Multi-vector attacks
- Shortage of security resources
- Compromised endpoints
- Email and social-engineered threats (phishing)
- Persistent, insider, and highly evasive threats
- Third-party and supply chain risks (BlueVoyant SCD)
- Brand damage and data leakage (BlueVoyant DRP)

Screenshot

# BlueVoyant Services for Microsoft

| Workshops | Accelerators | Managed Extxended Detection and Response |
|---|---|---|
| **Assess** | **Deploy** | **Manage and Monitor** |
| – Assess Your Security Posture<br>– Understand Microsoft Security<br>– Roadmap Your Next Steps<br>– High Value - Low or No Cost | – Project Management<br>– Deployment and Integration services<br>– Customization Available<br>– Project-based fees | – 24×7×365 managed detection, response and threat eradication<br>– Platform concierge services<br>– Subscription based fees |
| Microsoft Sentinel Workshop | Microsoft Sentinel Accelerator + CIS Evaluation | MXDR For Microsoft Sentinel |
| Defend Against Threats with SIEM plus XDR Workshop | Microsoft XDR Accelator | MXDR For Microsoft XDR |
| MXDR Workshop | Defender for Endpoint Accelerator | MXDR For Defender for Endpoint |
| Secure Multi Cloud Environments Workshop | Defender for Serves Accelerator | |
| Microsoft Security Assessments | Office 365 Accelerator | |

Screenshot

# Our Ideal Customer Profile (ICP)

## Customer Size and Industry

BlueVoyant MXDR for Microsoft is sold to any Microsoft enterprise customer in any industry, including government. Due to the nature of our services, typical customer requirements, budget limitations, and BlueVoyant resources required to onboard a new customer, it is preferred that customers have a minimum of 500-600 seats/endpoints. Ideal customers have multiple thousands of seats/endpoints. BlueVoyant is becoming more successful with large and complex accounts that include multiple larger departments, agencies, or sites that require their own security controls yet be part of a larger underlying Microsoft security infrastructure. These types of customers have tens of thousands of seats/endpoints and can be as large as 100,000 or more endpoints. These large accounts typically have dozens of distributed entities (sites, business units, agencies, departments) and can be found in any industry, including government, healthcare, education, and finance.

## Reasons Customers are Looking for a New Supplier

- They are changing from their old SIEM supplier to Microsoft Sentinel
- They are migrating more applications to the cloud and don't have enough security expertise
- They just had a breach or fear one and need better security
- They have the Microsoft security suite, but it's not optimized and delivering full value
- They don't have enough staff or expertise to implement and manage their security and Microsoft security products
- Their existing MSSP is underperforming
- They need better security to meet regulatory requirements or reduce their cyber insurance risk

## Common Titles of MDR Buyers

CISO, CIO, CTO, Director or VP of Cyber Security Services, Director or VP of IT, Cyber Security Manager, VP or Director of Security Operations. SOC Director, InfoSec Manager or Director, Central Security Director

# What are key differentiators for BlueVoyant MXDR for Microsoft

**BlueVoyant Microsoft Awards**

- New Elite Microsoft Verified Managed XDR Solution Status
- 2022 Microsoft US (MSUS) Security Partner of the Year Award
- Microsoft - Top MDR Team MISA awards 20/20 2021
- Microsoft Security Design Partners for:
  - Microsoft Security Experts for XDR
  - Microsoft Security Experts for Hunting
  - Microsoft Security Service Expert for Enterprise
- First Microsoft Intelligent Security Association (MISA) MSSP Member

## Technical and Service Advantages

There are many reasons BlueVoyant is Microsoft's 2022 US Security Partner of the Year and a leader in implementing and managing Microsoft Sentinel, 365 Defender and, Defender for Cloud

**Industry-Leading Content Engineering**
BlueVoyant's alert rule automation considers all available data sources, including third parties. Our content teams develop deep and unique data parsers that uncover intelligence and potential threats that others may miss. BlueVoyant has an ever-growing library of 900+ threat detection rules.

**Risk-Based Analytics**
BlueVoyant Risk-based Analytics (RBA) looks at all seemingly innocent incidents. RBA assesses and adds risk factors to each incident to determine if it's an early indicator of a more sophisticated threat.

**Threat Fusion Cell (TFC)**
BlueVoyant's TFC collects and curates feeds from more than 40 diverse data sources. SOC engineers analyze open sources, use partners, and include added intelligence to operationalize and contextualize malicious activities that could pose a risk.

**Active and Proactive Threat Hunting**
BlueVoyant active and proactive threat hunting is designed to identify adversary activity, cyber attacks, or advanced persistent threats and eliminate them quickly. SOC engineers also execute queries against raw data from endpoints, network devices, and other sources to reduce risk and stop threats.

**Fast and Efficient Content Distribution**
BlueVoyant pushes cybersecurity content updates, critical exploit detections, and relevant dashboards to all our clients at once. We do that weekly and for critical threats, like zero-day, on the same day.

**Greater Visibility, Insights, and Control**
Unique to BlueVoyant, client security data remains private and is analyzed within the client's Sentinel environment and Defender workspaces. This method is simple, secure, and allows for a quicker response. Moreover, clients have a unique 360-degree view of what is occurring in their environ

Screenshot

**More Responsive, More Productive**
BlueVoyant fosters a DevOps approach and leads with custom automation, which includes hundreds of unique rules and dozens of custom out-of-the-box playbooks for Microsoft clients. Today, all threats are automatically triaged, and the vast majority are resolved using BlueVoyant automation.

**Access to Microsoft Experts**
Unlike other providers, BlueVoyant's elite SOC engineers average nearly 10 years of experience and include dozens of valuable Microsoft-certified experts, including Microsoft security instructors. When clients call, they speak to an expert.

**Meet Regulatory Requirements**
BlueVoyant includes a full array of regulatory compliance reporting capabilities, well-defined SLAs, fast incident response, and eradication to ensure clients remain secure. Compliance begins by accessing client vulnerabilities, finding gaps, and closing them. It ends with visibility, reporting, compliance assessments, and KPI monitoring.

**Secure More with Unique Connectors**
BlueVoyant connectors allow clients to monitor more of their extended environment than before. MXDR consumes a broader range of security data from more sources inside and outside client networks and centralizes everything on Microsoft Sentinel. That provides a comprehensive "real-world, real-time" view of what is happening beyond the network's horizon.

**Developed IP stays with the Client**
Unlike other providers, when BlueVoyant develops IP, the work is completed inside the client's tenant, and that's where it remains. With BlueVoyant, clients have complete real-time visibility as we work and deploy new technology to protect our clients from threats both inside and out.

# Handling Objections

Salespeople may get skepticism or negative responses from prospects when selling any product. The following are common objections we hear when presenting our Microsoft MXDR solution to the client, with some recommendations for countering those objections.

| Objection | Counter |
|---|---|
| **There are many MXDR suppliers for Microsoft, why BlueVoyant?** | Microsoft has rated BlueVoyant as one of their top MXDR suppliers worldwide. For example, BlueVoyant wrote the book on optimizing Sentinel for Microsoft. They don't come in with a boilerplate solution like others but look at where you are and where you want to go and then work with you on a plan. They are also end-to-end and can handle everything where other MXDR suppliers fall short or ignore critical disciplines, which can be dangerous when you're dealing with the rising tide of sophisticated threats. |
| **I've thought about MXDR, but I don't think I can afford it with the budget I have today.** | BlueVoyant knows that costs and budget optimization are key considerations and concerns. BlueVoyant is different from other MXDR suppliers because they view cost management as being nearly as important as their services. What makes them different is their experience. They know how to optimize security tools and logs to cut out waste. In some cases, the money clients save pays for the security services. |
| **I like the idea of using a MXDR security service provider but need to retain control of what is happening.** | Clients won't get much control, security data may need to be exported, and work will be done outside your environment with most other MXDR suppliers. BlueVoyant is a leader because they work inside your environment. Your security data stays where it is, and you see and can control everything they are doing. The BlueVoyant portal provides full visibility and has a full array of reports and dashboards so you can have the insights you need and know you are secure. |

Screenshot

# Case Studies

BlueVoyant MXDR is usually sold as a complete services package. The sales journey starts with workshops and assessments, advances to implementation, and ends with an ongoing MXDR annual renewable contract. Depending on the customer size, urgency, and deal complexity, sales cycles can be from 30 days to several months. Three months is typical to close and start onboarding. Very large customers may take a few quarters. In some cases, the customer has already invested in and implemented Microsoft security products, but they are not optimized, or their existing MDR supplier is not performing.

## Large Healthcare Provider

**What was sold:** Consulting & Implementation + MXDR for Microsoft Sentinel and Microsoft Defender for Endpoint by BlueVoyant

**Deal Size:** $3.7m

**Employees:** 42,000

**Win Strategy:**

- Demonstrated significant savings in partnering with BlueVoyant vs. building a SOC internally.
- Demonstrated ability to fully optimize and expand use-cases through E5
- Demonstrated how BlueVoyant can neutralize sophisticated attacks with automation and security experts.

## Mutual Insurance Holding Company

**What was sold:** Implementation and MXDR for Microsoft

**Deal Size:** $175k

**Employees:** 500

**Win Strategy:**

- Showcased credibility, demonstrated value, and articulated BlueVoyant's approach to Microsoft's security strategy.
- Stayed one step ahead of legal/procurement processes to ensure project deadlines were met.

## Technology Company

**What was sold:** BlueVoyant MDR for Sentinel + MXDR for Microsoft 365 Defender

**Deal Size:** $1.5m

**Employees:** 6000

**Win Strategy:**

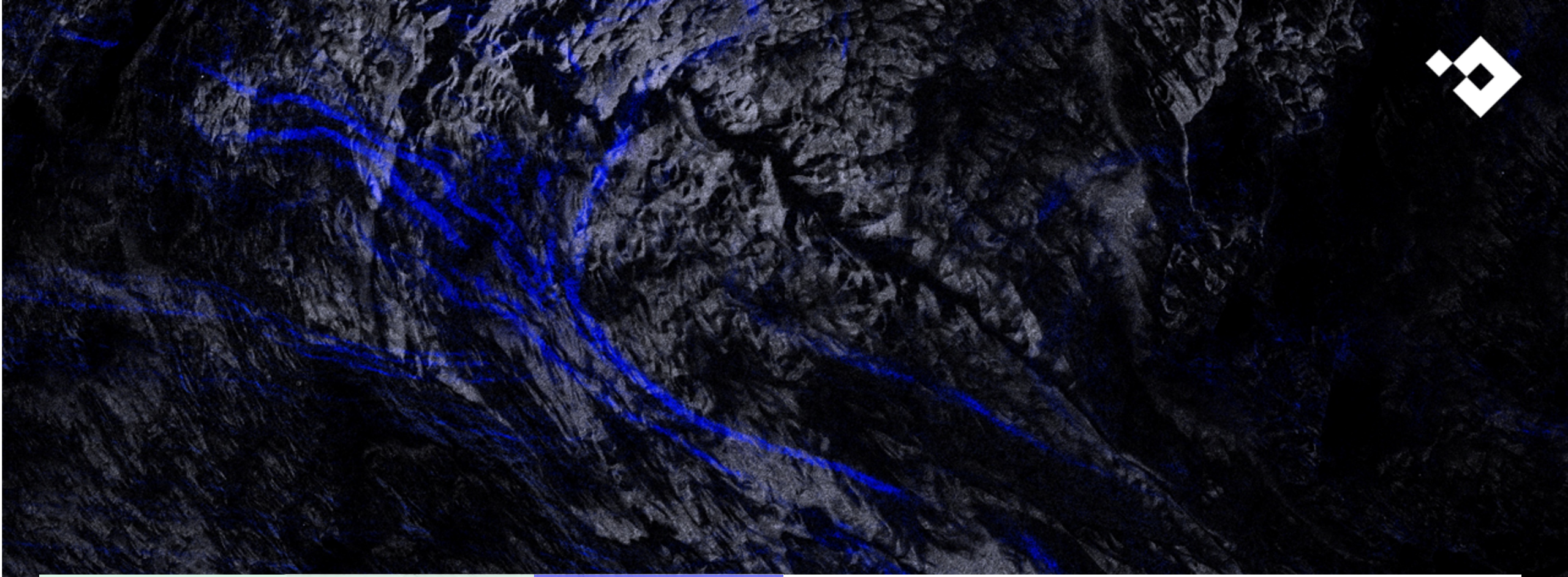
- BlueVoyant completed a technical deep dive on Splunk and Azure Sentinel and laid out the value of native integrations and automation that are not available in Splunk.
- BlueVoyant also completed a detailed analysis of TCO between both SIEMs.
-

BlueVoyant combines internal and external cyber defense capabilities into an outcomes-based cloud-native platform 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 platform 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.

Screenshot

yant, please visit our website at **www.bluevoyant.com** or email us at **contact@bluevoyant.com**

BlueVoyant



BlueVoyant

**New York HQ**

**335 Madison Ave, Suite 5G**
**New York, NY 10017**
**+1 646-558-0052**