Datasheet

BlueVoyant SecOps Diagnostics

Microsoft 365 Threat Gap Analysis - Client Sessions

75% of Microsoft customers not using the Microsoft 365 and Azure security capabilities in their licenses

Our Microsoft experts have performed hundreds of Microsoft deployments, workshops, and assessments. We have deep knowledge of the security stack and even teamed with Microsoft to publish the ultimate guide to deploying Sentinel correctly the first time.

Microsoft's XDR + SIEM capability provides a quick win for security simplification throughout the Microsoft Security platform strategy.

- Defender for Endpoint: Endpoint Detection & Response
- Defender for Cloud Apps: Cloud Application Security Broker
- Defender for Office: Email and Productivity Protection
- Entra ID: Identity Protection & Defender for Identity
- Sentinel: Security Analytics & Event Management

Business Challenges Solved

1. **Technology Rationalization:** Adopt Microsoft Security capabilities included in existing licensing and depreciate point solutions
2. **Operationalize Security:** Use Microsoft Security solutions to increase security operations effectiveness while standardizing and scaling
3. **Cloud Cost Optimization:** Optimize cloud costs by leveraging BlueVoyant's ingestion and alert strategies
4. **Microsoft Security Expertise:** Rely on BlueVoyant's team of Microsoft Security experts to guide your team through the intricacies of Microsoft products

BlueVoyant SecOp Diagnostics

Microsoft 365 Threat Gap Analysis
Our two 1-hour each sprint sessions help security professionals

- Uncover vulnerabilities in Identities and Devices
- Discover where and how to seal gaps in M365 defenses
- Learn how to tune threat detection and streamline response actions

In addition to valuable insights, the session produces a data-driven analysis and recommendations on how to move forward.

Microsoft 365 Threat Gap Analysis Sessions

Session One: Strategy

- Identify your security priorities
- Review M365 and Azure to collect operational/security data

Session Two: Findings

- Review data-driven insights together
- Verify remediation/services strategy for strengthening posture maturity across Devices and Users
- Discuss configuration adjustments for the Unified Defender portal and Entra ID

BlueVoyant

Microsoft 365 Threat Gap Analysis - Overview

BlueVoyant M365 E5 Threat Gap Analysis focuses on three critical areas: Identities, Devices, and Incidents. Our expert team thoroughly reviews your organization's M365 Defender Security Portal to identify potential vulnerabilities and provide actionable recommendations.

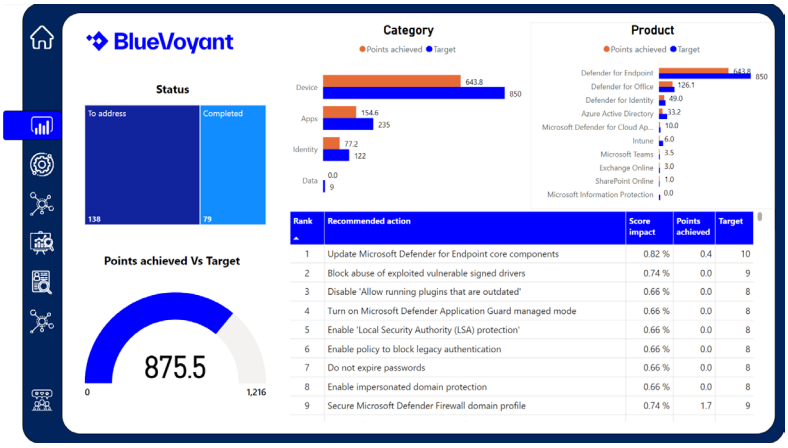
The analysis begins with an in-depth examination of your Identities, ensuring that user accounts are properly configured, access controls are in place, and any potential security gaps are addressed. By scrutinizing your identity infrastructure, we will help you minimize the risk of unauthorized access and enhance your overall security posture.

In the Devices phase of the analysis, we delve into the security of your organization's devices within the M365 ecosystem. That includes meticulously evaluating device configurations, patch management, and compliance with security policies. Our team examines the M365 Defender Security Portal to identify any misconfigurations or vulnerabilities that attackers could exploit. Uncovering these gaps enables you to proactively mitigate risks, enhance device security, and strengthen your organization's overall defenses against potential threats.

Finally, our M365 E5 Threat Gap Analysis extends to the Incidents aspect, where we focus on your organization's incident response capabilities and the effectiveness of threat detection and response within the M365 environment. Our experts evaluate the incident management process, review security logs, and assess the efficiency of threat-hunting techniques employed by your organization. By identifying any weaknesses or areas for improvement, we empower you to refine your incident response procedures, minimize the impact of security incidents, and enhance your organization's resilience against emerging threats.

Why BlueVoyant

- 2023 MISA Security MSSP of the Year
- 2023 & 2022 Microsoft US Security Partner of the Year
- **Sentinel Expertise:** 500+ deployments & authors of the Sentinel Deployment Best Practices Guide.
- **Time to Value:** 42 day deployments.
- **Delivery Architecture:** BlueVoyant content delivered and maintained in customers environment.
- **Simplified MS Security Experience:** Frictionless experience - alerts and events are actioned using Microsoft portals.



Ready to get started? Learn more.

About BlueVoyant
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.

BlueVoyant