Solution Brief

BlueVoyant Microsoft Azure for IoT Hub Health Check

Helping you optimize your Microsoft Azure for IoT Hub to secure your telemetry data

Have you optimized your IoT platform investment?

Azure IoT Hub uses device-to-cloud telemetry data to understand the state of your devices and define message routes to other Azure services—without writing any code. To reduce the security risk of these added devices, Azure has features such as Defender for IoT that provide security posture management and threat monitoring and remediation for the IoT environment.

To maximize your investment, how aligned is your Azure architecture to Azure best practices? When was your last technical Azure platform assessment tied to Azure frameworks, such as data integrity, performance, and Azure usage and adoption?

BlueVoyant's Azure IoT Hub Health Check provides a technical assessment of your Azure IoT Hub platform designed to identify your system's security, performance, configuration, and system reliability problems before they affect your critical operations.

Key differentiators

- BlueVoyant is the Microsoft Security US Partner of the Year, and a design partner for Microsoft new security services.
- Our consultants have extensive experience in developing and implementing cyber security programs for Fortune 10 manufacturing firms.
- We incorporate lessons learned from our entire Professional Service team who have extensive expertise supporting global enterprises across Digital Forensics, Incident Response, and traditional Cybersecurity Consulting.
- Follow-on product security assessment can be synchronized with other Microsoft Security tools such as Microsoft Sentinel, Active Directory, etc.

Azure IoT Hub Health Check Features:

Understand the strategic vision for the Azure IoT Hub platform
Find the baseline of the current state of implementation and understand near-term operational goals

Benchmark your current state using the key frameworks
Evaluate your Azure IoT security implementation against best practices in Azure such as the CIS cloud benchmark and layers in industry expertise

Develop a high-level future state for IoT
BlueVoyant will work with your team to develop a future state that blends operational goals that accounts for the risk appetite of the organization

Prioritized improvements roadmap
Prepare and present a deliverable that features a roadmap and resource requirements

BlueVoyant converges internal and external cyber defense capabilities into an outcomes-based, cloud-native platform called BlueVoyant Elements™. Elements continuously monitors your network, endpoints, attack surface, and supply chain as well as the open, deep, and dark web for vulnerabilities, risks, and threats; and takes action to protect your business, leveraging both machine learning-driven automation and human-led expertise. Elements can be deployed as independent solutions or together as a full-spectrum, cyber defense platform. BlueVoyant's approach to cyber defense revolves around three key pillars — technology, telemetry, and talent — that deliver rock-solid cyber defense capabilities to more than 700 customers across the globe.

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

BlueVoyant

Ready to get started?
Get in touch