BlueVoyant

MANAGED DETECTION AND RESPONSE (MDR+)
MICROSOFT DEFENDER ADVANCED THREAT PROTECTION

THE CHALLENGE

With the ever-growing number of access points, it is becoming harder for organizations to stop incidents from becoming breaches. Microsoft Defender Advanced Threat Protection (ATP) detects attacks and data breaches, and gives businesses insights and tools to prevent, detect, investigate, and respond to incidents. However, some businesses might not have the capacity or expertise to manage the security of their endpoints on their own.

THE SOLUTION

BlueVoyant provides Managed Detection and Response (MDR+) for Microsoft Defender ATP to help Microsoft customers detect, prevent, respond to and mitigate advanced attacks.

Utilizing the breadth of threat protection capabilities built into Microsoft Defender ATP, BlueVoyant provides organizations with a fully-managed, end-to-end advanced threat management service, that includes:

- Ongoing policy management and tuning
- 24/7 security operations
- Endpoint monitoring
- Triage and investigation
- Real-time incident response
- Threat containment and mitigation
- Robust detection with advanced hunting

FEATURES

ONGOING POLICY CONSULTATION AND DEVELOPMENT

Whether you are already using Microsoft Defender ATP or just getting started, we help you to quickly realize it's value by applying our deep operational knowledge and expertise in Microsoft Defender ATP deployments. Beyond initial set up, we continuously review and update your policies to whitelist applications, assets, and processes as your business changes over time.

AUTOMATED ALERT ANALYSIS

Microsoft Defender ATP integrates into our cloud-native platform that utilizes security orchestration, automation, and response to triage, enrich, and integrate automation of alerts received from Microsoft Defender ATP. We use playbooks to simultaneously run dozens of queries and processes at machine speed and utilize intelligence from more than forty sources to identify indicators of compromise.

MANAGED PREVENTION ENHANCED WITH HUMAN ANALYSIS

BlueVoyant's security operations center analyzes alerts received from Microsoft Defender ATP. The combination of expert-level analysis coupled with Microsoft technology makes protection against new and unknown threats even more effective by eliminating the black magic typically associated with machine learning and minimizing misses and false positives.

BlueVoyant

MANAGED DETECTION AND RESPONSE (MDR+)
MICROSOFT DEFENDER ADVANCED THREAT PROTECTION

CUSTOMIZED DETECTIONS AND PREVENTION

Cyber threats are always evolving, so your detections should do the same. We provide ongoing refinement of your detection policies based on real-time threat intelligence. Equipped with this intelligence, we proactively protect your organization from modern day threats by writing customized policies to neutralize sophisticated malware and stop lateral movement that could potentially evade standard detections.

REAL-TIME RESPONSE, CONTAINMENT, AND MITIGATION OF THREATS

It is fast, real-time action that helps minimize the damage done by adversaries. We rapidly isolate affected assets, including hardware, to prevent lateral spread and manually remove malicious files. As new threats are detected and neutralized across our client base, they are added to the platform, enabling crowd-sourced protection that acts as a force-multiplier for enhancing detection and mitigation of threats.

THREAT HUNTING

Advanced adversaries can evade standard detection techniques and tools. We will proactively and iteratively search through events to detect and isolate advanced threats that evade existing security solutions. We will also conduct remote hunt missions on a regular basis that will perform manual and semi-automated activities for targeted data analysis to search for signs of advanced attacks and malicious behavior.

ROOT CAUSE ANALYSIS

Remote root cause analysis is performed on all positively identified malicious activity. Identifying the nature of the attack, timeline, attack chain, and the attack's underlying persistence to help you understand how adversaries are trying to exploit your infrastructure.

WHY CHOOSE BLUEVOYANT MDR+ FOR MICROSOFT DEFENDER ATP

- Most Experienced MDR Provider for Microsoft Defender ATP
- MDR platform built by cyber experts from the private sector, FBI, and NSA

COMPLIMENTARY SERVICES
BY BLUEVOYANT

- Managed SIEM powered by Splunk® Enterprise
- Detection as a Service powered by Splunk® Enterprise

KEY FEATURES

- Integrated global threat intelligence from over forty open, closed, and proprietary sources
- SOAR integration that automates Microsoft Defender ATP alerts
- Rapid response to contain malicious attacks
- Real-time incident mitigation
- 24/7 support from a team of security experts
- Customized policy management, tuning, refinements

Learn more at www.bluevoyant.com