Solution Brief

MXDR for Splunk®

Extend protection from endpoint to cloud using Splunk technology

If you take a best-of-breed approach to your security technology stack, then how do you handle the challenges of such as systems such as:

- Have you accounted for the blind spots in data silos?
- How quickly do you update your security content and is it uniform across your tech stack (e.g., EDR, SIEM)?
- Can you detect attacks that use oft-benign actions across security tools?
- How well integrated is your security team/SOC with third-party systems?

Adversaries thrive on blind spots, slowly updated security content, lack of uniformity in content updates, oft-benign actions to help them evade your cybersecurity.

BlueVoyant's MXDR for Splunk provides a cloud-native, fully integrated security solution that utilizes a single dashboard to enable data collection visibility across multiple platform (such as endpoint, IoT, cloud workloads, networks) to avoid crossstack blind spots. Our Risk Based Alerting thwarts attackers who try to use oft-benign actions to evade detection. To help breakdown the data silos and provide a centralized repository of best of breed technologies, we have partnered EDR providers to provide you the best risk remediation possible.

Key Differentiators

- Integrated Splunk technology with multiple Endpoint Detection and Response (EDR) tools with cross-stack visibility
- Rapid and comprehensive Splunk platform implementation to provide visibility to your suite of security tools from experts who have completed over 3,000 Splunk engagements with 200 active Splunk Certifications.
- Two-time Splunk Professional Services Partner of the Year validates our Splunk expertise.
- Triage 100% of threats and eliminate more than 90% of them with advanced automation to reduce risk and required resources.
- BlueVoyant's Next Generation Content cuts time to upgrade security content in half, and includes Risk Based Alerting (RBA) alerts you about threat actors who use often benign activities that may lead to malicious actions.
- Deployment services provide you with proper onboarding and log collection. We start with a CIS-Based Security Maturity Engagement that helps you understand the strengths and vulnerabilities in your overall security plan.

BlueVoyant's team of world-class cybersecurity experts, elite proprietary data, and process automation, to serve as an extension of a company's security team, delivering a level of protection that helps businesses sustainably protect themselves in a changing threat landscape. MXDR for Splunk identifies and mitigates threats as they emerge and ensures that businesses and wider ecosystems are always prepared for rapid, effective response, and threat neutralization. Clients benefit from our Splunk and cybersecurity expertise, and our consultative approach to solving their security problems.

splunk> Partnerverse Cloud Migration

splunk> Partnerverse Manage ELITE

splunk> Partnerverse Cloud Migration: Co-Delivery

Providing fast, effective, and intelligent detection-based content to address the growing threat landscape of your business, MXDR for Splunk correlates and analyzes network, user, endpoint, and other security logs in real time, aggregating disparate data and applying the latest threat intelligence to filter background noise, prioritize alerts, and respond to the most suspicious threat behaviors.

BlueVoyant's human security expertise, proven processes, and security operations leadership empower you to accelerate your Splunk and EDR investment to quickly mitigate business risk, enable security at scale, and support you wherever your Splunk lives.

BlueVoyant

Features

Splunk Deployment Service
Professional services engagement focused on onboarding customers to the MDR For Splunk service for either Splunk Enterprise or Splunk Cloud Platform. BlueVoyant implementation experts provide data onboarding to enable go-live activities with the Security Operations Center (SOC) through a defined and repeatable program.

CIS-Based Security Maturity Engagement
Includes four phases: a brief overview of where we have been and where we are headed in cybersecurity; illustrations of how various factors influence risk; a review of our expert approach to identifying key cyber strengths and vulnerabilities; and an exercise to clarify your strengths and vulnerabilities, resulting in a findings and recommendations report.

24/7 Security Monitoring
Real-time alerting, triage, threat indicator enrichment, and investigation of malicious activity with filtered notifications and alerts supported by a world-class team within BlueVoyant's 100% cloud-based SOC.

Security Orchestration and Automation
Supports the BlueVoyant SOC in accelerating event triage, reducing false positives, and improving mean time to resolution.

Splunk Professional Services
Splunk experts customize and extend the capabilities of Splunk maximizing the MDR for Splunk investment.

Investigation and Notification
Triage and investigation of alerted events by expert security analysts to confirm true-positive, benign, or false-positive, alerting the client as appropriate.

Indicator Enrichment
Automatic extraction, scoring, and enrichment of Indicators of Compromise (IoCs), leveraging BlueVoyant automation with open source and BlueVoyant proprietary threat intelligence.

Unlimited Live Remote Response
Includes unlimited remote investigations and response services for all activities consistent with remote SOC capabilities and visibility and response capabilities of your EDR tool.

Wavelength™ Client Portal
A web-based portal that provides real-time visibility / dashboards to detected alerts, confirmed incidents, and enables approved client employees to interact with our SOC analysts and view all detected assets.

ITSM Integration
BlueVoyant provides a fully documented, bi-directional API that can be used to synchronize security incidents and service management cases with a client ITSM tool. Pre-built integration for ServiceNow via the ServiceNow Store is available at an additional cost.

Risk Behavior Analytics (RBA)
RBA content provides an extra layer of detections by applying risk scoring to activity and enriching case severity.

Next-Generation Content
Cuts time to upgrade security content in half using our proprietary BlueVoyant Information Model and leveraging Continuous Integration and Continuous Delivery (CI/CD) pipelines to deliver the most accurate and update to date content to our customers' environments. We operate on data parallel from customer content to ensure best service time and uptime while allowing client security team and BlueVoyant to focus on different SIEM use cases, such as security and observability, within the same Splunk environment.

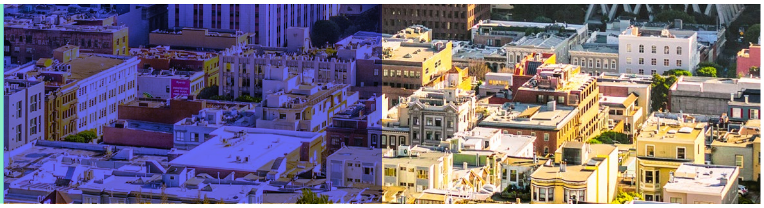
Single-View Security Posture
Get a clear perspective of your organization's security posture through BlueVoyant's Client Portal, Wavelength™ with a security-specific view of all monitored data in real time.

Health Monitoring
Notification and assistance with troubleshooting if agents and/or log collection appliances become uncommunicative or unreachable, or output has not been received from log sources within the scope of service.

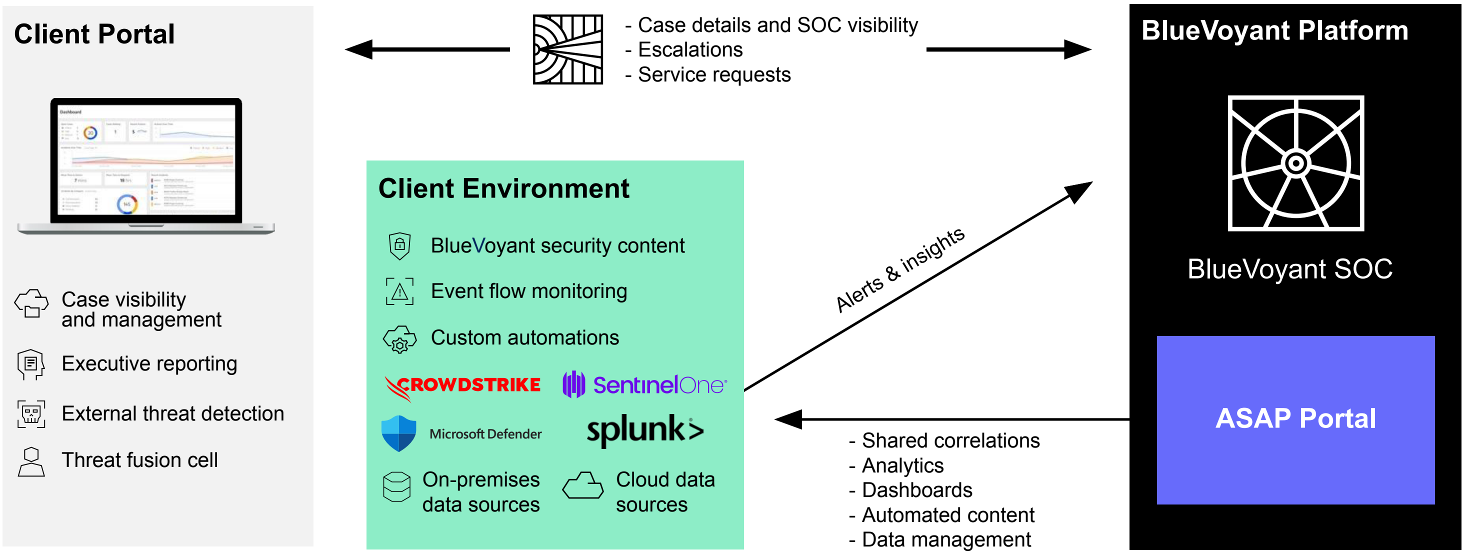
Endpoint Response
BlueVoyant will take a specific set of actions at the completion of an investigation: quarantine, delete, whitelist, monitor, or blacklist. Depending on your services if an advanced investigation with live/real-time response is needed. BlueVoyant may perform remote intrusion response activities.

Threat Detection
Advanced endpoint software will be used to expand enrichment and enhance behavioral correlations. Depending on your services, BlueVoyant will proactively and iteratively search through events to detect and isolate advanced threats that evade existing security solutions.

Malware Prevention
Deployed endpoint software will automatically prevent the execution of suspicious or known malicious software, often preventing the outbreak, or spread of malware. Through blacklist policy management, delivery of unique signatures and threat intelligence indicator matching, BlueVoyant can deny, terminate, and block operations remotely.



How It Works



Client Portal

- Case visibility and management
- Executive reporting
- External threat detection
- Threat fusion cell

- Case details and SOC visibility
- Escalations
- Service requests

Client Environment

- BlueVoyant security content
- Event flow monitoring
- Custom automations

- On-premises data sources
- Cloud data sources

Alerts & insights

BlueVoyant Platform

BlueVoyant SOC

ASAP Portal

- Shared correlations
- Analytics
- Dashboards
- Automated content
- Data management

Ready to get started? Learn more here.

SOC - V1 - 478.45.900.854 - 3570.56893
ROC - 484/98293 - 025.35702
CN - MS - 6739 - 7394
BLUEVOYANT
CYBER DEFENSE
10010
BlueVoyant