BlueVoyant®

Managed Splunk® Enterprise Service

INTRODUCTION

Managed Splunk® Enterprise from BlueVoyant correlates and analyzes network, user, endpoint asset and other security logs in real time, aggregating disparate data and applying the latest threat intelligence to filter background noise and identifying real security concerns. Powered by best-in-class SIEM technology from our partner Splunk, our Managed Splunk Enterprise solution covers endpoints, network perimeter security, users (directory services and applications) and virtually all others.

Our Managed Splunk Enterprise service enables our SOC analysts to prioritize alerts, and respond to the most suspicious threat behavior faster. Managed Splunk Enterprise allows you to carry out sophisticated queries and use all of your data to defend your enterprise with the same level of protection that large enterprises achieve, at a fraction of the cost. No need to buy expensive add-ins or additional tools, advanced features like UEBA are included natively in our solution.

SERVICE OVERVIEW

Smart Log Management

Managed onboarding, archival, and ingestion of log and event data, tamper-proofing critical logs while ensuring that only the right types and amounts of data needed for investigations are analyzed.

Hosted and Managed Infrastructure

Dedicated high availability and purpose-built secure cloud-hosted infrastructure, provisioning, patching, upgrades, and health monitoring.

Event Enrichment

Augments security data with exclusive threat intelligence from over 40 sources allowing us to get in front of geopolitical threats that are potentially targeting your environment.

Security Monitoring

24/7 real-time monitoring of malicious activity with filtered notifications and alerts supported by a world-class team within BlueVoyant's 100% cloud-based Security Operations Centers (SOCs).

Single-View Security Posture

Security-specific view of all monitored data in real time to get a clear perspective of your organization's security posture through BlueVoyant's Client portal, Wavelength™.

Simplified Compliance

Creation of custom correlation rules and reports that identify threats to sensitive data and demonstrate compliance with regulations like GDPR, HIPAA, PCI, and SOX.

Unified Defense

Analytics, detections, and investigations are shared across BlueVoyant's client base, enabling the ability to identify indicators of compromise that are known to your peer organizations.

Used & Entity Behavior Analytics (UEBA)

Collect additional high-fidelity data sources like endpoint activity and vulnerability insights to drive comprehensive detection of advanced attacks, response, and remediation.

BlueVoyant®

Managed Splunk® Enterprise Service

FEATURES

- Our proprietary, open-source, and dark web intelligence is leveraged to expedite triage and enrich investigations conducted by the SOC. Delivered as intelligence reports with new detections outlined with classifications of threat indicators.
- BlueVoyant SOC monitors your Splunk Enterprise environment and is ready to respond to threats any time, day or night.
- Get on-demand support from our team of expert Splunk operators on how best to optimize your Splunk Enterprise deployment to maximize security detection and response capabilities.
- Leverage BlueVoyant's orchestration, playbook, and automations to accelerate enrichment and response actions in your environment.
- See all of the activity happening within your environment from your BlueVoyant customer portal.
- Simplify compliance reporting through automated and ad hoc reporting capabilities.

BENEFITS

- Improve security outcomes without the burdens of time, effort and expense in buying and installing a SIEM on your own.
- Take advantage of the capabilities offered by a best-in-class SIEM without the time or expense needed to maintain the tool and optimize security operations.
- Quickly scale your security operations within/across your environments without the need to invest in additional hardware/software.
- Expedite SIEM deployments by plugging into the Managed Splunk Enterprise service rather than building from scratch.
- Get more capability out of your SIEM by having it managed by a team of highly skilled and certified experts in our SOC.
- Reduce alert fatigue; only get notified about high priority threats and let the BlueVoyant SOC team filter out the rest.

BlueVoyant offers a broad portfolio of security services designed to meet your needs

Managed Security Services

We combine a global team of experts, comprehensive threat intelligence, extensive automation and best-in-class technologies to provide always-on detection and response solutions to meet your cyber security needs.

Threat Intelligence Services

We provide a cost-effective way for customers to continuously monitor and minimize cyber risk across their entire ecosystem of partners, vendors, supply chains, and more.

Cyber Defense Services

We combine proven front line experience responding to advanced cyber threats with expertise in building world class defensive cybersecurity programs to stop threat actors in their tracks.

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