SOLUTION BRIEF

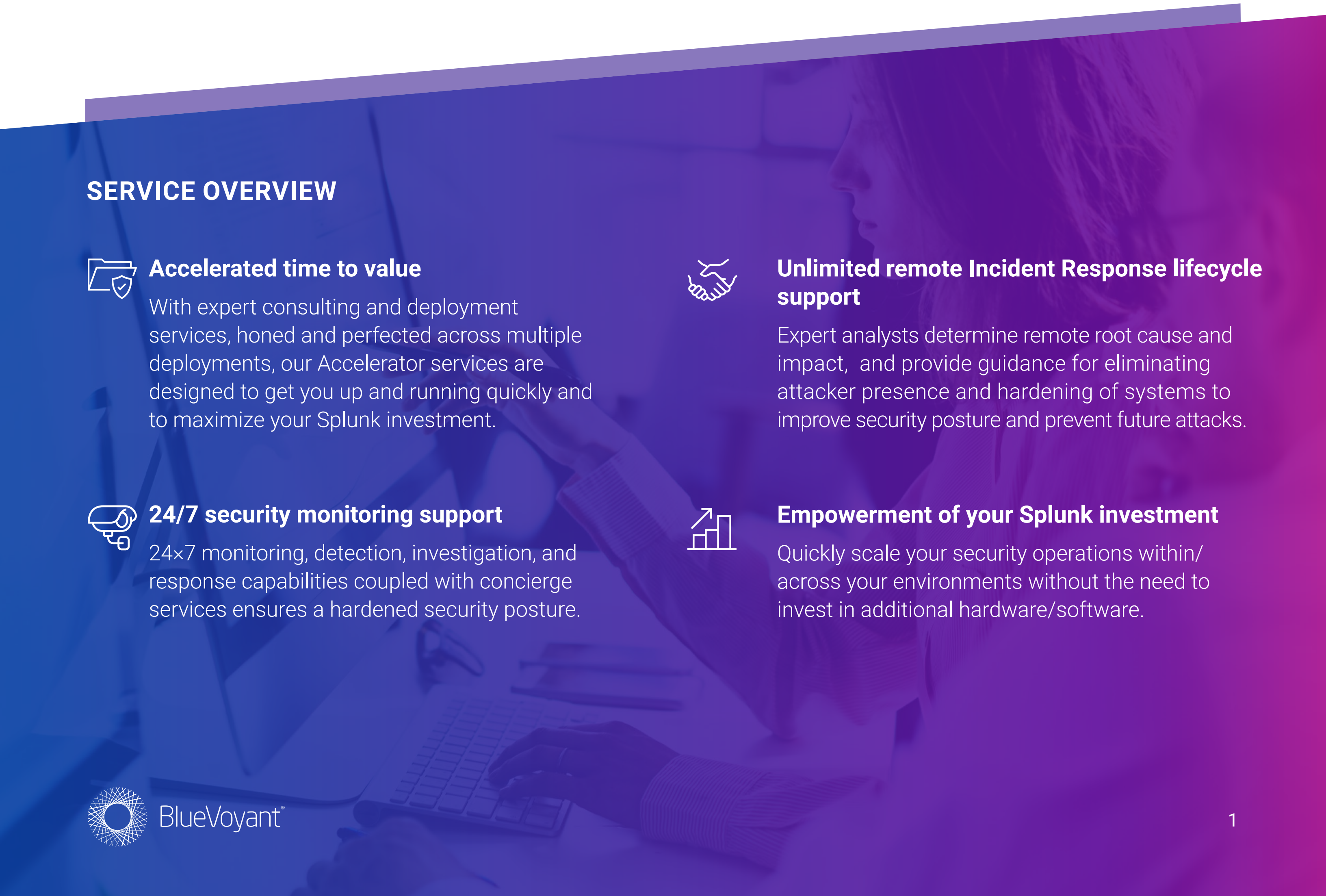
Modern SOC for Splunk® Cloud Platform

INTRODUCTION

BlueVoyant Modern SOC for Splunk® Cloud Platform is designed to assist your team with the monitoring and protection of your assets and resources in your Splunk environment, maximizing your investment in Splunk technology and providing a complete portfolio of security services, ongoing platform care and maintenance, and 24/7 security operations as a service. BlueVoyant's human security expertise, proven processes, and security operations leadership empower you to accelerate your Splunk deployment in order to quickly mitigate business risk, enable security at scale and support you wherever you are in your Splunk journey.

BlueVoyant Modern SOC for Splunk Cloud Platform 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, prioritize alerts, and respond to the most suspicious threat behavior faster.

Get on-demand support from our team of expert Splunk operators on how best to optimize your Splunk Cloud Platform deployment to maximize security detection and response capabilities.



SERVICE OVERVIEW

Accelerated time to value

With expert consulting and deployment services, honed and perfected across multiple deployments, our Accelerator services are designed to get you up and running quickly and to maximize your Splunk investment.

24/7 security monitoring support

24×7 monitoring, detection, investigation, and response capabilities coupled with concierge services ensures a hardened security posture.

Unlimited remote Incident Response lifecycle support

Expert analysts determine remote root cause and impact, and provide guidance for eliminating attacker presence and hardening of systems to improve security posture and prevent future attacks.

Empowerment of your Splunk investment

Quickly scale your security operations within/across your environments without the need to invest in additional hardware/software.

FEATURES

Splunk Cloud Platform Accelerator

Expert consulting to accelerate implementation and onboarding with honed and perfected processes that build use cases, dashboarding, and migrate your data to get you up and running quickly.

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 Security Operations Center (SOC)

Splunk Cloud Concierge

Ongoing maintenance and customization to maximize Splunk Cloud Platform

Smart Log Management

Logs are aggregated and stored on the client's instance of Splunk Cloud Platform, tamperproofing critical logs while ensuring that only the right types and amounts of data needed for investigations are analyzed.

Investigation & 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.

Advanced Threat Hunting

Detects potential threats based on reputation by correlating inbound and outbound network traffic to suspicious and/or malicious domains or IP addresses utilizing proprietary and open source threat intelligence.

User and 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.

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™.

Health Monitoring

If BlueVoyant detects that agents and/or log collection appliances become uncommunicative or unreachable or output has not been received from log sources that are within the scope of service, BlueVoyant will notify the Client and assist with troubleshooting.

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.

Customer Outcomes

- Faster time to value through rapid deployment
- Maximized value from your investment in Splunk
- Automated blocking of known threats
- Detection of advanced threats and zero-day threats
- Containment of compromised assets, preventing further spread
- Mitigation of potential business disruption
- Reduced alert fatigue
- Satisfaction of compliance requirements
- Improvement in overall security posture
- Reduction in overall costs and fewer resource demands

BlueVoyant Offers a Broad Portfolio of Services Designed to Meet Your Needs

Professional Services

- Full-Service Incident Response
- Consulting Services
  - Cyber Maturity Assessment
  - Cyber Consulting Retainers
  - Incident Response Planning
  - Penetration Testing

Threat Intelligence Services

- Global Cyber Threat Detection
- Predictive Analysis
- BIN Watcher™
- Brand Watcher™
- Credential Watcher™
- Executive Cyber Guard

3rd Party Cyber-Risk Management

- Comprehensive Assessments and Monitoring
- Risk Improvement
- Third-Party Risk Management

About BlueVoyant

At BlueVoyant, we recognize that effective cybersecurity requires active prevention and defense across both your organization and supply chain. Our proprietary data, analytics and technology, coupled with deep expertise, works as a force multiplier to secure your full ecosystem.

Accuracy. Actionability. Timeliness. Scalability.

Founded in 2017 by former Fortune 500 and former government cyber officials, BlueVoyant is headquartered in New York City and has offices in Maryland, Tel Aviv, San Francisco, Manila, Toronto, London, Latin America and Budapest. Visit www.bluevoyant.com.

BlueVoyant®

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