BlueVoyant®

Vulnerability Management Service

INTRODUCTION

BlueVoyant's Vulnerability Management Service (VMS) delivers vulnerability assessments of your environment to let you know where there are weaknesses that threat actors could potentially exploit. From missing updates and patches to software bugs and operating design flaws, weaknesses in your system leave you open to possible risk. Our VMS solution offers automated, recurring vulnerability scanning utilizing the BlueVoyant technology platform in conjunction with a team of elite, highly-certified security analysts to help you catalogue and prioritize vulnerabilities within your system.

SERVICE TIERS

VMS combines the power of best-of-breed VMS technologies with a world class managed service provider.

Option 1: Vulnerability Import works with you to enable the automatic import of vulnerabilities into the BlueVoyant platform utilizing support third-party vendor assessment software. Vulnerabilities will be visible to the expert analysts in the Security Operations Center.

Option 2: Internal Scanning includes the functionality in option1 and also adds the deployment of BlueVoyant Virtual Appliances into your environment in order to conduct vulnerability assessments and internal asset discovery.

Option 3: Full VMS combines all the features from options 1 and 2, and also adds external scanning capabilities.

FEATURES

Tailored Solution:
Configures and runs vulnerability scans at a predetermined frequency based on your environment and requirements.

Expert Support:
VMS is supported by expert analysts who operate 24x7x365 from our security operations centers.

Triaged Findings:
VMS offers prioritized remediation and patching guidance to customer technology teams in order to reduce identified risks.

Self-Service Reporting:
Access vulnerability reports containing content such as new and resolved vulnerabilities and high-risk vulnerabilities on critical assets through our portal.

Meaningful Data:
Renders insights into vulnerability scans conducted by our technology partner Tenable.

Comprehensive Scope:
VMS looks at customer password policies, authentication, network configurations and more.

Validated Approach:
VMS uses the same threat model that we use to protect our own environment in order to protect our customer environments.

By 2025, 70% of MSEs [Mid-Sized Enterprises] that take a traditional, volume approach to vulnerability management will have been breached through a known vulnerability. - Gartner
Midsize Enterprises Must Prioritize to Achieve Effective Vulnerability Management (Nov 2019)

BlueVoyant®

Vulnerability Management Service

BENEFITS

- Better understand the inventory of assets throughout your organization through regular scanning activities.
- Quickly identify previously unknown assets so that you can either remove them or secure them per your requirements.
- Reduce your overall cyber risk by better understanding the types and criticality of vulnerabilities faced by your organization and by receiving guidance on remediation prioritization.
- Streamline and simplify your vulnerability scanning requirements without the investment of time, resources and money that would otherwise be needed.
- Reduce time, cost and effort required to meet your compliance mandates.
- Scan all of your environments (cloud, on-prem, hybrid) from a single service and see scan results in a single view.

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.

Research from Cybersecurity Industry Leaders

Only 40% of MSEs [Mid-Sized Enterprises] have a formal vulnerability management program in place. - Gartner

Security and Risk Infrastructure and Protection Survey (2019)

Only 50% of identified vulnerabilities are patched within 3 months of discovery. - Verizon

Verizon Data Breach Investigations Report (2020)

60% of breaches were linked to a vulnerability where a patch was available but not applied. - Ponemon

Ponemon Institute: *Cost and Consequences of Gaps in Vulnerability Response* sponsored by ServiceNow (2019)

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