

SECURITY IS HARD. SECURING YOUR INFRASTRUCTURE WITH MULTIPLE POINT SECURITY SOLUTIONS ACROSS DIFFERENT OPERATING SYSTEMS AND A HYBRID CLOUD ENVIRONMENT IS EXPENSIVE, INEFFICIENT AND INEFFECTIVE.

The sheer volume and variety of alerts, events, and tickets across these solutions and across different environments makes it extremely hard for any analyst to find and fix issues; and even harder for a CISO and Security Director to effectively understand and manage the security risks to their infrastructure. For example, servers go through many changes over their lifetime. These changes can include the addition of new services, modification of user permissions, installation of new software, and allowance of egress internet access. All of these chang-

es increase the attack surface in your environment, regardless of whether it is on-premise, in a colocation facility, or in the public cloud. The high rate of these changes, especially in today's environment, pose a huge challenge for the organizations because, if these changes are tracked then they are tracked in multiple places such as firewalls, SIEM, configuration management systems, and in the public cloud provider's user interface or API. This is a fragmented, broken, and ineffective security architecture.

VantagePoint

VANTAGEPOINT IS A SECURITY PRODUCT BUILT TO SOLVE THESE PROBLEMS. WITH ITS CLOUD-FIRST APPROACH, IT ENABLES YOU TO MEASURE AND MONITOR YOUR SECURITY POSTURE AND DETECT THREATS ACROSS CLOUDS AND OPERATING SYSTEMS.

It does so across five security verticals: file integrity monitoring, log analysis, vulnerability management, threat detection, and security configuration baseline analysis. VantagePoint aggregates data across these verticals and normalizes it into one security score to help you identify your current holistic security posture

along with providing guidance on remediation steps. It does this using the "batteries included but swappable" motto, shipping with default policies that will cover 80% of cases with zero additional action required.

CHALLENGES

KEY FEATURES

 **FILE INTEGRITY MONITORING:** Continuously monitor important configuration files for unauthorized or malicious changes to protect the integrity of your servers. VantagePoint will, by default, monitor and track the important configuration files in your infrastructure. It also enables you to easily specify additional files to monitor and allows you to set up alerts for unauthorized changes.

 **LOGS ANALYSIS:** Aggregate, automatically analyze, index, and archive important log files in a centralized location. Our search interface allows you to perform advanced searching across all log files that are monitored across your infrastructure. VantagePoint ships out of the box with default analysis and saved search rules that allow you to detect and view suspicious events across your entire infrastructure. Saved search capabilities and custom alerting allow you to be notified for any event in your infrastructure.

 **THREAT DETECTION:** We've built a threat intelligence repository so you don't have to. Our feed contains over 100 proprietary and open source (OSINT) feeds with over 1.5 million indicators. VantagePoint leverages that threat intel to automatically and continuously inspects files and network payloads for suspicious or malicious activity, automatically alerting you to threats in your environment.

 **VULNERABILITY MANAGEMENT:** VantagePoint performs daily vulnerability scans across all hosts to detect security risks. We assign our own criticality based on real security factors, like whether one or many public exploits are available, whether defensive techniques are available, CVSS score, and vulnerability type. These factors allow you to quick detect, triage, prioritize, and track vulnerabilities and remediation efforts.

 **SECURITY CONFIGURATION BASELINING:** VantagePoint continuously assesses the security posture of each server against best practices and custom security baseline configuration policies. These policies leverage human readable Boolean-style queries to test all of your infrastructure to help you enforce security best practices and to report on and detect security risk and configuration drift. VantagePoint ships with a default best practices policy, but custom queries and policies can easily be developed using our policy writing user interface.

 **UNIFIED RISK SCORING AND REMEDIATION PLANNING:** Get one, single, trackable score of your security posture based on our proprietary scoring algorithm that takes into account all factors and functionality provided by VantagePoint. Along with the security score, receive prioritize guidance on remediation for security risks in your environment.

Benefits

-  **REDUCE COST AND IMPROVE EFFICIENCY**
-  **MULTIPLE POINT PRODUCTS UNDER ONE ROOF**
-  **EASY INSTALLATION**
-  **SCALE ON DEMAND**
-  **FOCUS ON REMEDIATION**