Better Together: Splunk and Veritas

Detect user threats in the Veritas data protection platform.

Leverage Veritas and Splunk to provide insights on user behavior in the Veritas NetBackup data protection. With Splunk User Behavior Analytics (UBA), security operations can monitor NetBackup user activity logs to detect actions or patterns that indicate account compromise, malicious insiders, or privileged account abuse. With the continuous monitoring of user activity, organizations can improve security and reliability of disaster and cyber recovery.

Data protection provides the foundation for cyber and disaster recovery. User and administrators are trusted to maintain data protection policies and retentions to ensure the organization can recovery effectively and quickly when a destructive data attack (such as ransomware) occurs. Key to lowering the risk of disruption is the availability of reliable recovery data. By continually monitoring user actions and patterns on NetBackup, organizations can ensure they will detect changes to settings and policies that would jeopardize a trusted and reliable data for recovery.

Many organizations utilize Splunk UBA to monitor the behavior of users and administrators. With Splunk UBA, the data protection platform is continually monitored for malicious user actions that could emanate from rogue insiders or via compromised credentials.

The Veritas and Splunk UBA Solution

Together, Veritas and Splunk UBA UEBA work together to help organizations improve the security and reliability of their Veritas environment. This collaboration allows for the quick identification of potential user and administrator actions that could disrupt backup policies and data availability. Through continuous automated monitoring and prompt handling of user activity logs, organizations can ensure effective and reliable oversight of the appropriate and approved use of their Veritas platform. This proactive approach enables analysts, IT and security teams to quickly address risk to cyber resiliency and operations.

Veritas NetBackup is the only enterprise backup solution that combines data management, automation, artificial intelligence, and elastic architecture to improve agility and data security across the integrated hybrid cloud. With 500 exabytes of information currently under management, no other solution comes close.

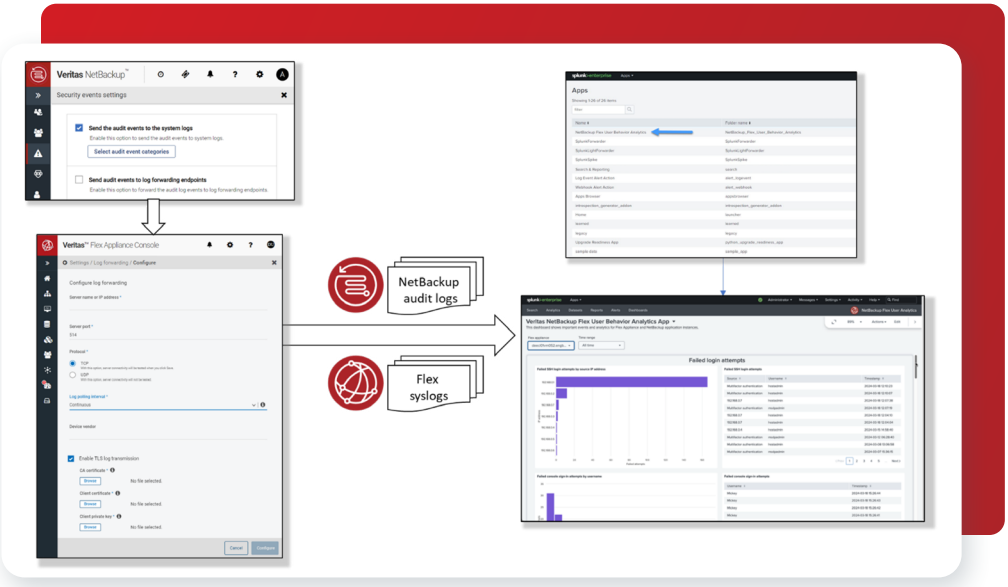

Figure 1: Need a caption for this

Splunk User Behavior Analytics (UBA) helps organizations find known, unknown and hidden threats using multidimensional behavior baselines, dynamic peer group analysis, and unsupervised machine learning. This allows Splunk UBA to rapidly detect anomalous behavior — such as compromised or misused accounts or devices, IP theft or data exfiltration — and eliminate it. Using machine learning, Splunk UBA derives sequences and patterns across all anomalies, in addition to other indicators, to filter down and identify the top threats that are critical and actionable. Amidst all the noise, these threats represent the most likely risk to your business. Splunk User Behavior Analytics addresses security analyst and hunter workflows, requires minimal administration and integrates with existing infrastructure to locate hidden threats.

> *Organizations can lower the risk cyber resilience management and response with Splunk UBA and Veritas. With powerful analytics, organizations can monitor user and administrator activity in their cyber security and cyber recovery platforms."*

Veritas

- **Zero-trust data protection platform:** Tightly controlled access to platform with continuous service authentication
- **Data immutability:** Tamper-proof backup data
- **Threat detection:** Early identification of ransomware threats and malicious activity
- **Isolated recovery environment:** Reliable data recovery through limiting risk of re-contamination

Splunk UBA

Splunk User Behavior Analytics uses unsupervised machine learning algorithms to establish baseline behaviors of users, devices and applications, then searches for deviations to detect unknown and insider threats.

- **Detect advanced threats** and anomalous behavior using machine learning.
- **Enhance visibility** and generate rich contextual insights to rapidly assess risk and take action.
- **Simplify and streamline** incident investigations and workflows to increase SOC efficiency

About Veritas

Veritas Technologies is the leader in secure multi-cloud data management. Over 80,000 customers—including 91% of the Fortune 100—rely on Veritas to help ensure the protection, recoverability and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems and 1,400+ storage targets through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. Learn more at www.veritas.com. Follow us on X at @veritastechllc.

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact

V2103 04/24