

# Better Together: Veritas and Securonix

## Detect user threats in the Veritas data protection platform.

Leverage Veritas and Securonix to provide insight on user behavior in NetBackup™ data protection. With Securonix, security operations can monitor NetBackup user activity logs to detect actions or patterns that indicate account compromise, malicious insiders, or privileged account abuse. With 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. Users 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 Securonix to monitor the behavior of users and administrators. With Securonix, the data protection platform is continually monitored for malicious user actions that could emanate from rogue insiders or via compromised credentials.

### The Veritas and Securonix Solution

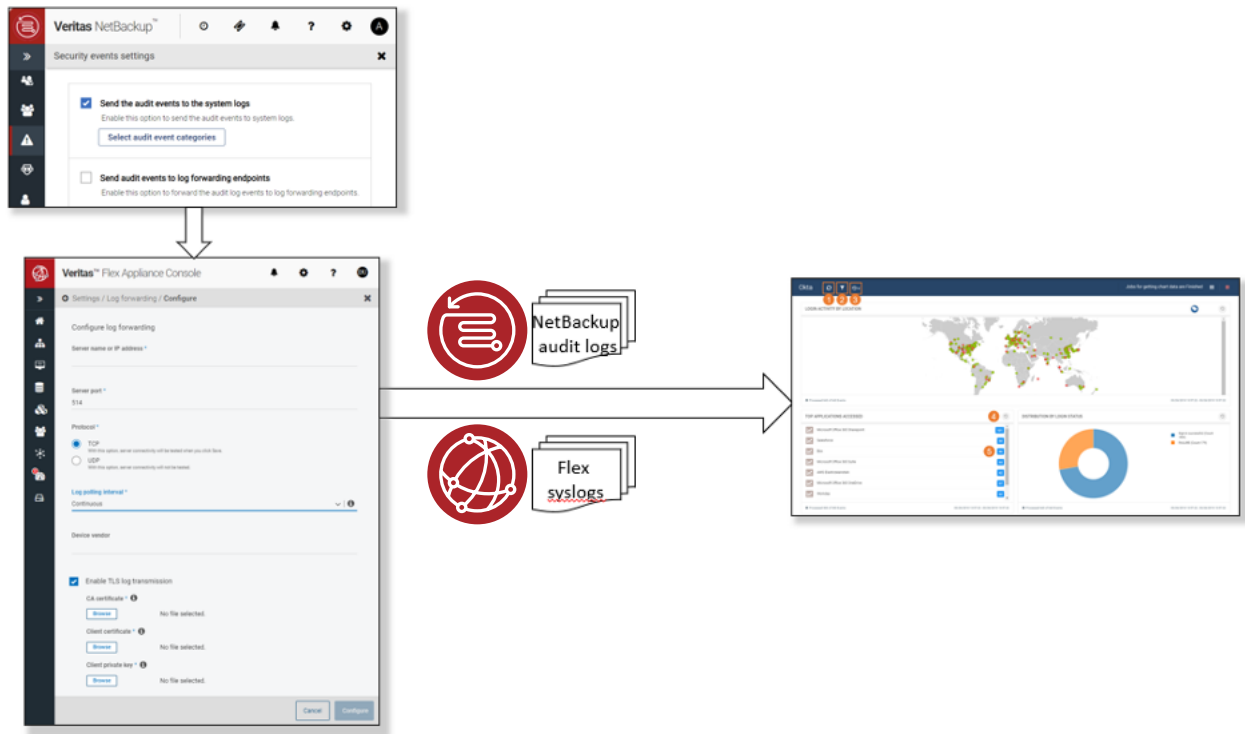
Together, Veritas and Securonix UEBA work to help organizations improve the security and reliability of their Veritas environment. This collaboration allows for the quick identification of potential user and administrator actions that could disrupt backup policies and data availability. Through continuous 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.

Securonix UEBA helps organizations detect unknown and insider threats. As cyberattacks become more complex, these threats are harder to detect. Traditional rule-based approaches are ineffective against advanced threats because rule-based solutions generate thousands of false alerts. Securonix UEBA tracks anomalous user behavior, suspicious lateral movements, and insider threats within your organization — whether in the cloud or on-premises. Your team will gain cloud monitoring with built-in APIs for all major cloud infrastructures as well as many security and business applications. Additionally, our UEBA solution reduces noise by leveraging machine learning capabilities and out-of-the-box use case content, so your team can focus on the highest-risk alerts.



*Organizations can lower cyber resilience risk with Securonix and Veritas. With powerful analytics, organizations can monitor user and administrator activity in their cybersecurity and cyber recovery platforms."*



Veritas	Securonix UEBA:
<p><b>Zero-trust data protection platform:</b> Tightly controlled access to platform with continuous service authentication</p> <p><b>Data immutability:</b> Tamperproof backup data</p> <p><b>Threat detection:</b> Early identification of ransomware threats and malicious activity</p> <p><b>Isolated recovery environment:</b> Reliable data recovery through limiting risk of re-contamination</p>	<p><b>Leverages advanced machine learning and behavior analytics:</b> Reduces false positives and give you a complete understanding of user and entity threats</p> <p><b>Behavior analytics:</b> Understand behavior patterns with pre-built analytics that help you uncover complex threats with minimal noise</p> <p><b>Threat chains:</b> Identify low and slow attacks with threat models that map to the MITRE ATT&amp;CK and US-CERT frameworks</p> <p><b>Peer group analysis:</b> Automate anomaly detection with the ability to baseline user activities against their peers</p>

**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](http://www.veritas.com). Follow us on X at [@veritastechllc](https://twitter.com/veritastechllc).

**VERITAS™**

2625 Augustine Drive  
 Santa Clara, CA 95054  
 +1 (866) 837 4827  
[veritas.com](http://veritas.com)

For global contact information visit:  
[veritas.com/company/contact](http://veritas.com/company/contact)