VARONIS + SPLUNK

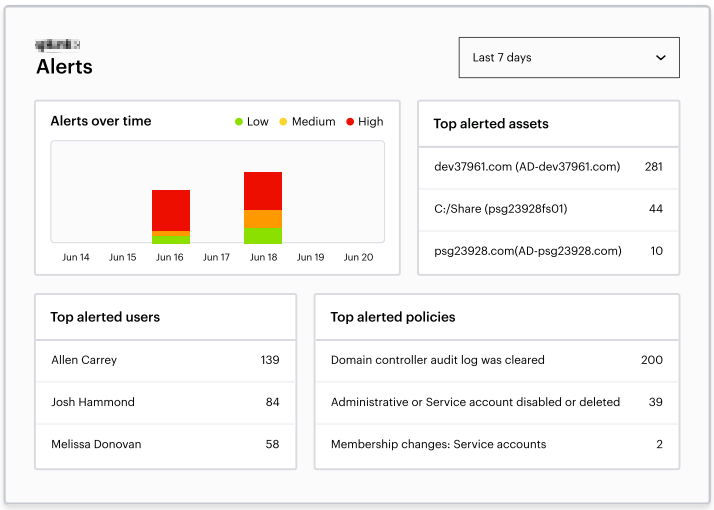
Gain a unified picture of data risk, enhance investigations, and streamline incident response.

CHALLENGE

As security tech stacks grow and become too costly for security teams to manage, they turn to solutions like Splunk to consolidate monitoring efforts and streamline security operations. However, a SIEM is only as good as the logs it receives. Teams often struggle with an overwhelming volume of raw security logs that lack insights into critical, at-risk data, making it difficult to cut through the noise and respond effectively to threats targeting data.

SOLUTION

Varonis' integration with Splunk enables security teams to access and manage Varonis' data-centric and context-rich alerts directly within Splunk for faster triage, investigation, and remediation. Unlike many other tools, Varonis surfaces only meaningful alerts that provide valuable insights into critical, at-risk data. When put into context with your broader security stack, Varonis provides a unified picture of data risk that will help you quickly catch and respond to threats.



KEY BENEFITS

- Meaningful and actionable insights, not just logs.
- Reduce false positives and enhance investigations.
- Streamline monitoring and security operations.

"With Varonis, we're not getting overloaded with alerts and not spending time chasing after false positives. That's been a huge time-saver and a stress reliever."

Ken Christman
Director of IT,
Mackenzie

Read the full case study here:
varonis.com/case-study

Data-centric alerts

Varonis monitors data activity, authentication activity, directory service activity, and perimeter telemetry using behavior-based threat models to detect suspicious activity that could indicate an active threat. From billions of events, Varonis only surfaces a handful of meaningful alerts that can be easily integrated into Splunk, allowing security teams to focus on genuine threats.

Meaningful and actionable security insights

Varonis goes beyond simply sending raw logs; it delivers meaningful and actionable alerts enriched with additional context, including user details, data sensitivity, permissions, and device information. These alerts can be seamlessly integrated into your Splunk security workflows to create a unified picture of data risk, enabling faster triage, investigation, and remediation.

Effortless integration

Varonis offers multiple easy-to-configure integration methods with Splunk. Using a pre-built API integration, Syslog forwarding, or webhooks, you can easily send Varonis' enriched, data-centric alerts to Splunk with minimal configuration.

TRY VARONIS FOR FREE.

See how our cloud-native solution covers all your data security needs.
Get started today at **varonis.com/trial.**