

Streamline Business Resilience:

Ensure the Availability and Integrity of your Backups with the Veeam App for Splunk

Business Challenge

Today's IT and security leaders are living in a world of increasing cyberthreats. Recent studies show that 76% of organizations suffered a ransomware attack in the last year. The data also tells us that 93% of those attacks explicitly targeted an organization's backups.

Building a strategy for ultimate business resilience is no longer a conversation reserved for security leaders but should be considered by IT and security team members alike. These teams must come together and build end-to-end solutions for their organization's cyber resiliency across its entire environment — including everything from endpoints, to networks, to backups. To reduce organizational risk and ensure business continuity when a cyberattack occurs, it's important to ensure that your Security Information & Event Management (SIEM) solution alerts you to cyberthreats in any and every part of your system, including your backups.

Benefits

- **Customize alerts for stronger threat detection:** Customize both operational and security alerts to notify you of a potential cyberthreat. From malware, to changes in your security settings, to network connection issues, Veeam can detect hundreds of events that could impact the integrity of your backups.
- **Define locations to accelerate response time:** Improve visibility into Veeam servers in different data centers by segmenting your servers based on location. This level of visibility can help your security teams locate and respond to potential threats faster.
- **Implement role-based access for increased control:** Assign appropriate access levels to different users depending on their role and location. By controlling what individual users can see in your Veeam environment, you can improve the security of your backups.

Streamline Business Resilience with the Veeam App for Splunk

Splunk, an industry leader in Security Information & Event Management (SIEM), provides organizations with a comprehensive view of their operational data, insight into security activities, and response capabilities to help them stay ahead of cyberthreats. Now, with the Veeam App for Splunk, security leaders can leverage Splunk to closely monitor their Veeam backup environments through detailed dashboards, reports, and alerts.

The Veeam App for Splunk brings your Veeam event data into Splunk and monitors it for security events like ransomware, accidental deletion, malware, and other cyberthreats. With this application, organizations can quickly and easily process vital monitoring and event data on their backup environments in the same single pane-of-glass as the other source environments they may be monitoring.

With the Veeam App for Splunk, organizations can expand their view into their security posture and extend daily monitoring to their backup environment, thus ensuring that their backups remain clean, reliable, and resilient against cyberthreats.

Environment Configurations

The Veeam App for Splunk is only available to Veeam Data Platform Advanced and Premium users that leverage version 12.1 or later. The application leverages the event data in the latest security features in version 12.1, including new in-line malware detection via the AI-powered Threat Detection Engine and Four-eyes Authorization via syslog event forwarding functionalities. Syslog event forwarding enables Veeam events to be streamed to compatible SIEM solutions that support syslog ingestion. With the Malware Detection Engine, Veeam detects threats earlier by performing low-impact, real-time data and file extension analysis during backup. If malware is detected, the details are then sent to Splunk via syslog, where security teams can be alerted. This expedites response times.

The Veeam App for Splunk can be implemented at no additional Veeam cost via Splunkbase and is compatible with the latest releases of Splunk Enterprise and Splunk Cloud.



Use Cases

Keep a constant pulse on your backup environment

Access real-time insights on your backup environment in the same single pane-of-glass as the other source environments you may be monitoring in your Splunk SIEM.

Detect cybersecurity threats in real-time

Receive immediate notifications and alerts for potential security incidents, suspicious activities, or operational issues in your environment so you can respond quickly and proactively.

Minimize downtime and recover quickly

Identify and address cyberthreats before they lead to prolonged downtime. Quickly identify the data you want to recover in the event of loss with the power of Veeam Data Platform.

Maintain recovery compliance

Easily meet recovery time objectives (RTO), recovery point objectives (RPO), and other industry compliance regulations with rapid detection and recovery capabilities.



Conclusion

We know that backups are often the target of cyberattacks like ransomware. To minimize downtime and ensure business can continue when an attack occurs, it's crucial to consider a holistic strategy for cyber resiliency across your organization's entire environment — including your backups.

The Veeam App for Splunk combines the cyber resiliency of Veeam Data Platform with the power of Splunk. With the Veeam App for Splunk, security leaders can now leverage Splunk to closely monitor their Veeam backup environment, making it easier to ensure the integrity of this data remains uncompromised.

About Veeam Software

Veeam, the #1 global market leader in data protection and ransomware recovery, is on a mission to empower every organization to achieve radical resilience through data security, data recovery, and data freedom for their hybrid cloud. The Veeam Data Platform gives IT and security leaders peace of mind that their apps and data are protected and always available. Headquartered in Seattle, with offices in more than 30 countries, Veeam protects over 450,000 customers worldwide, who trust Veeam to keep their businesses running. Radical resilience starts with Veeam. Learn more at www.veeam.com or follow Veeam on LinkedIn [@veeam-software](https://www.linkedin.com/company/veeam) and X [@veeam](https://twitter.com/veeam).

➔ Learn more: veeam.com