AI-Powered Ransomware Detection and Protection with Affordable Cloud Storage for Your Veeam Backups from Wasabi and Opti9

What is Opti9 Observr

Hackers are targeting backup & replication infrastructure when they breach an organization to destroy all means of recovery, thus increasing their chances of being paid the ransom. To combat this emerging threat, Opti9 launched Observr to detect anomalies using artificial intelligence and machine learning within customers' Veeam backup environments.

Observr is a SaaS-based platform that can be utilized by anyone using Veeam & Wasabi. Observr requires no special software or network configurations, and utilizes Veeam's proprietary and encrypted CloudConnect protocol to transfer metadata securely. Customers can add Observr to their Veeam install with a few simple clicks and immediately start benefiting from its security assurances.

Observr works by detecting anomalous activity within the environment they may indicate the presence of an attacker, such as suspicious changes to: RPOs, job settings, retention, immutability, encryption, deletions, incremental change rates, and many other factors. When threats are detected, Observr can send alerts via email, APIs, and integrations with 3rd party security platforms. Additionally, users have the option to configure Observr to automatically airgap Wasabi storage buckets to ensure they're protected and can be utilized as a means for recovery.

Why Wasabi and Opti9 Are Better Together

Wasabi Hot Cloud Storage and Opti9 Observr provide a comprehensive protection solution available for your Veeam backup strategy. It combines resilient and immutable storage with a platform to detect suspicious or malicious activities that typically precede an attack. Since Observr is external to Veeam and Wasabi, it provides monitoring, alerting, and remediation capabilities which insider threats cannot tamper with or disable.

Observr features native air-gap support for Wasabi that detects suspicious activity occurring within Veeam, to automatically disconnect the related Wasabi bucket from Veeam ensuring attackers have no ability to read, write, delete, or modify any of the backups stored within Wasabi.

Seamless integration of the technologies allows for a quick set-up to start mitigating risk. With just a few clicks, your data is protected without any special software or network configurations required. Combine that with a cloud storage solution that allows you to lower your data recovery costs with no egress fess or API costs, you have the most cost effective and secure solution available in the market today.

Features

- Machine learning algorithms to detect suspicious activity and mitigate against ransomware attacks
- Automated remediation when threats are detected
- Centralized and intuitive reporting for Veeam and Wasabi

Benefits

- Mitigate suspicious activity occurring within your backup environment
- Automatically air-gap & protect your Wasabi data in response to threats
- Monitor & alert backup RPOs and other metrics independent from the backup software
- Reduced data recovery costs with no egress fess or API costs