Predatar and Veeam (Recovery Testing):

Frequently Asked Questions.

Q: What do Predatar and Veeam offer?

Both provide solutions for recovery assurance, securing data, automating workflows, and integrating with SIEM platforms.

Q: How does Predatar handle automated workflows?

Predatar offers robust automated workflows for backup testing and recovery across many leading backup platforms. It can automate recovery tests if a high threat score is detected, works for both virtual and physical workloads, and supports backup and primary storage. It is designed for SME to Enterprise clients.

Q: How does Veeam handle automated workflows?

Veeam provides comprehensive features but requires more manual effort for setting up recovery job tests and integrating threat data. It only supports virtual workloads and is designed for the SME space.

Q: What insights does Predatar's dashboard offer?

Predatar's dashboard provides insights and drives automated testing and recovery based on those insights. It can act on information from SIEM platforms, triggering automated responses to threats.

Q: What insights does Veeam's Threat Centre offer?

Veeam One's Threat Centre offers valuable backup security insights but requires a separate licence in some cases and lacks automation for triggering recovery tests directly from threat insights.

Q: How easy is the setup process with Predatar?

Predatar simplifies setup with automated workflows handling testing and recovery, using anomaly detection to trigger necessary activities automatically.

PREDATAR

North America
4208 Six Forks Road, Suite 1000,
Raleigh, North Carolina 27609

+1 919-827-4516

Europe
Bloxham Mill, Bloxham,
Oxfordshire. OX15 4FF

+44 (0)1295 500081

Q: How easy is the setup process with Veeam?

Veeam requires significant manual setup for testing recovery jobs via SureBackup, including manually selecting and downloading Yara rules for specific threats.

Q: How does Predatar manage performance during file scanning and backup testing?

Predatar manages file scanning and backup testing efficiently without significant performance degradation.

Q: How does Veeam manage performance during file scanning?

Veeam users with large environments report concerns about file scanning impacting the VBR database performance due to additional data storage requirements.

Q: How does Predatar integrate with SIEM platforms?

Predatar integrates seamlessly with SIEM platforms, triggering automatic recovery and scanning processes based on threat data.

Q: How does Veeam integrate with SIEM platforms?

Veeam can feed information back to SIEM platforms but lacks the capability for automatic actions within Veeam triggered by those platforms.

Q: Does Predatar use AI techniques?

Yes, Predatar uses machine learning to spot anomalies and threats and has a custom-trained Large Language Model for providing backup environment information and answering questions.

Q: Does Veeam use AI techniques?

No, Veeam does not use AI techniques as part of its recovery solution.

Q: What malware detection does Predatar support?

Predatar supports malware scanning and cleaning for both Windows and Linux VMs, as well as physical file systems. It plans to include AIX systems soon.

PREDATAR

North America
4208 Six Forks Road, Suite 1000,
Raleigh, North Carolina 27609

+1 919-827-4516

Europe
Bloxham Mill, Bloxham,
Oxfordshire. OX15 4FF

+44 (0)1295 500081

Q: What malware detection does Veeam support?

Veeam's Malware Detection Engine requires advanced or premium licensing and its Secure Restore feature is limited to Windows environments only.

Q: How does Predatar handle anomaly detection?

Predatar uses anomaly detection within backups to automatically trigger relevant actions for proactive threat management.

Q: How does Veeam handle anomaly detection?

Veeam offers anomaly detection based on file scanning, which requires manual review within the Veeam GUI.

Q: What does Predatar offer for isolated recovery environments?

Predatar provides a virtual appliance as part of the subscription, allowing clients to deploy as many as required at no extra cost.

Q: What does Veeam offer for isolated recovery environments?

Veeam requires the environment to be built manually and supports only one Isolated Recovery Environment target, which can be problematic for environments with more than 50 virtual machines.

Q: Which solution is better, Predatar or Veeam?

Predatar stands out for its automation, SIEM integration, and broader environment support. Veeam offers rich features but needs more manual effort and higher-tier licensing for full capabilities. It's easier to procure Veeam's SureBackup if already a Veeam customer, while Predatar will require a new agreement.

PREDATAR

North America
4208 Six Forks Road, Suite 1000,
Raleigh, North Carolina 27609

+1 919-827-4516

Europe
Bloxham Mill, Bloxham,
Oxfordshire. OX15 4FF

+44 (0)1295 500081