Predatar and Veeam Backup & Replication.

Ready
Security

Predatar's Recovery Assurance platform has been developed to deliver unprecedented levels of data validation, and gives storage and security teams confidence in the ability to execute a fast, effective recovery in the event of a cyber attack.

The Challenge

Cyber criminals have recognised that the existence of backups undermines their attempts to disrupt and extort organisations. They are actively targeting these repositories to infect, encrypt and even delete data. If your backups or snapshots have been compromised — your recovery is at risk.

Predatar Recovery Assurance

Predatar Recovery Assurance uses AI, automation, and built-in End Point Detection & Response (EDR) to hunt down and remove malware from your backups, and proactively validates the data — to make sure it's fully recoverable and infection free.

Predatar has found hidden malware in the backups of more than 70% of deployments within the first month.

Predatar and Veeam

Predatar is compatible with Veeam Backup & Replication, meaning that Veeam users can benefit from Predatar's AI-powered threat hunting, automated recovery testing, deep malware scanning and malware removal on the workloads they backup with Veeam.

Predatar also utilises the Veeam Incident API to alert Veeam users when Malware has been found in a Veeam backup. By raising an alert directly inside the Veeam Backup and Replication GUI, users can react quickly and take any follow-up steps that might be required — for example notifying the security team and checking production workloads.

Veeam Ready

Predatar's integration with Veeam has undergone a rigorous review process and has been awarded Veeam Ready status in the security category.

Benefits at a glance

01 | Prove recoverability before a crisis hits.
Don't wait for a crisis to put your recovery to the test. Predatar provides proactive validation so you'll always know your data is good.

02 | Big advantage. Small human effort.
Automation means that Predatar is 'always on' working 24/7 to deliver unparalleled recovery assurance without additional burden on busy IT and Security teams.

03 | Supports mixed storage environments.
Deploy Predatar across Veeam, Rubrik, Cohesity, IBM Storage Protect, IBM FlashSystems, Pure Storage and more.

New infection signature detected
2 minutes ago

Recover to CleanRoom

SIEM alert recieved from QRadar
Just now

VM_WORKLOAD
VE_SPTA
125.3 GB
Safe

PREDATAR

Solution componants
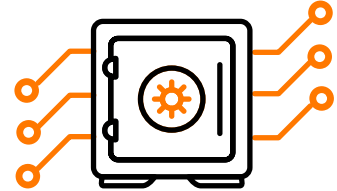There are two components to Predatar's Recovery Assurance solution:

01. Predatar Cyber Recovery Orchestration Software
A cloud-based SaaS application, Predatar CRO provides a single portal where users can manage all aspects of Predatar's Recovery Assurance capabilities. The portal includes all of the real-time reporting and alerts you expect from a modern SaaS application.
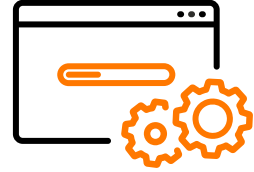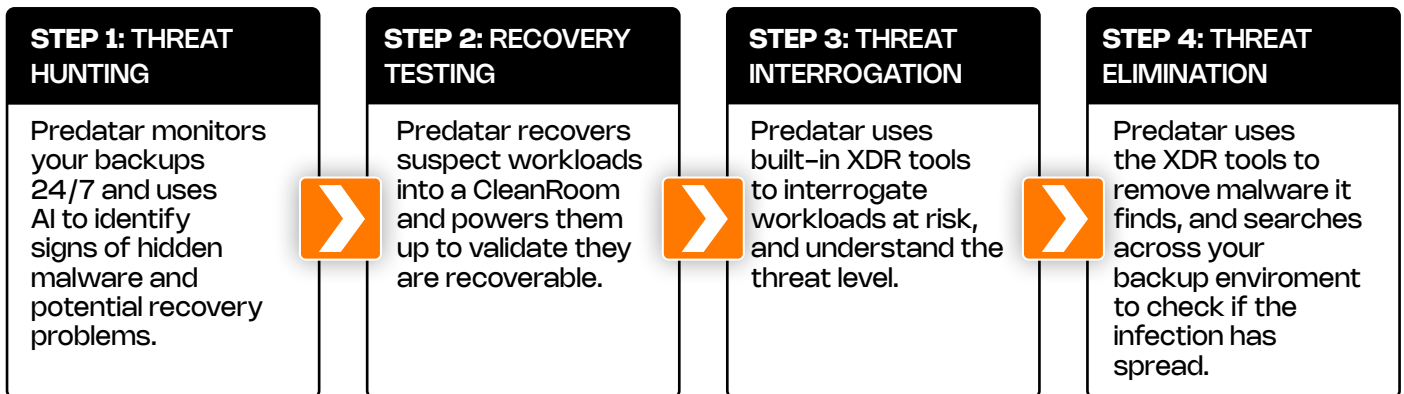
02. Predatar CleanRoom
On-premise or in the cloud, Predatar Recovery Assurance requires an isolated recovery environment to act as a target to perform automated recovery testing, malware scanning, and infection removal.

Recovery Orchestration process

STEP 1: THREAT HUNTING

Predatar monitors your backups 24/7 and uses AI to identify signs of hidden malware and potential recovery problems.

STEP 2: RECOVERY TESTING

Predatar recovers suspect workloads into a CleanRoom and powers them up to validate they are recoverable.

STEP 3: THREAT INTERROGATION

Predatar uses built-in XDR tools to interrogate workloads at risk, and understand the threat level.

STEP 4: THREAT ELIMINATION

Predatar uses the XDR tools to remove malware it finds, and searches across your backup enviroment to check if the infection has spread.

Example Predatar deployment for Veeam

Predatar CRO Platform

Threat detection powered by Aurora AI

Recovery prioritisation powered by Aurora AI

Governanance reporting and insights powered by Aurora AI

Metdata (Collection & commands)

Metdata (Collection & commands)

Customer site   or

veeam
Backup software

Predatar agent

Firewall controlled access

Predatar CleanRoom   or

Predatar agent

Test & Scan

Bitdefender

ClamAV

EDR/XDR tools

PREDATAR