Recovery. Assured.

Built to boost your resiliency, Predatar helps enterprises find, remove, and stay ahead of threats in their storage environment – including hidden ransomware and unrecoverable workloads.

PREDATAR WORKS WITH:

IBM

IBM FlashSystems
IBM Storage Protect
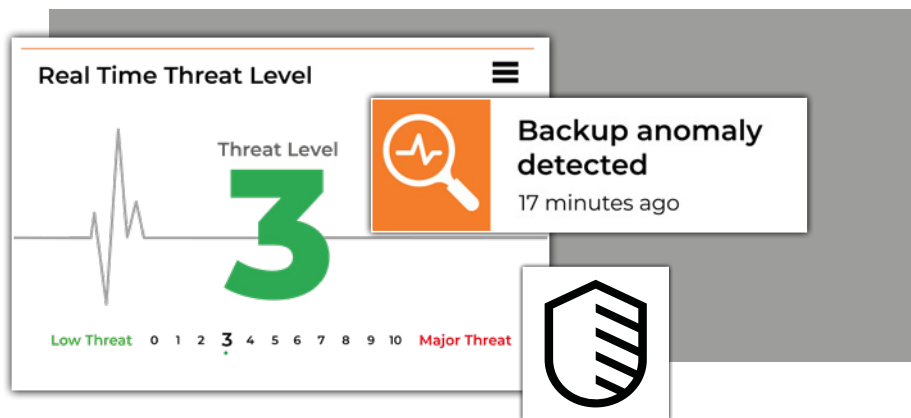IBM Storage Protect Plus
IBM Data Protect

veeam

Veeam Backup & Recovery

COHESITY

Cohesity DataProtect

Hunt down hidden threats with Predatar Signal

Predatar Cyber Recovery Orchestration™ includes Predatar Signal™, a state-of-the-art machine learning engine designed to find the signals of danger amongst the noise of busy storage environments.

By analysing multiple data inputs Predatar Signal can understand threats, assign threat-ratings and prioritise automated recovery testing and antivirus scanning of the workloads that pose the greatest risk.

Signal inputs include:

Priority node groups:
By understanding which workloads are most critical, Predatar can prioritise these for immediate interrogation if signals are found.

Backup Anomaly detection:
Predatar Signal monitors storage activity data across all users to find and understand anomalies in behaviour. If a suspect behaviour pattern is validated as a real threat Predatar will search across all the environments it monitors around the world for the same pattern.

SIEM Events:
SIEM integrations allow Predatar to prioritise workloads based on security events in wider IT environment.

PREDATAR SIGNAL

Learn more at
www.predatar.com

PREDATAR

Interrogate and eliminate problems with automation
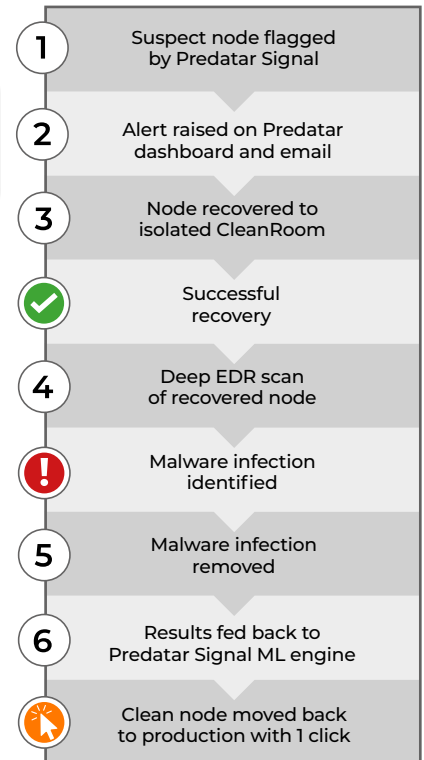
When Predatar finds signals of potential danger, automated workflows are triggered to interrogate the suspect workloads, this includes the ability to initiate automated recovery testing in an isolated CleanRoom™, and antivirus scanning using integrated best-in-class End Point Detection and Response (EDR) tools.

User can easily customise the workflows using toggle-based controls to select the specific actions for different types of alert and threat-level.

1	Suspect node flagged by Predatar Signal
2	Alert raised on Predatar dashboard and email
3	Node recovered to isolated CleanRoom
✓	Successful recovery
4	Deep EDR scan of recovered node
!	Malware infection identified
5	Malware infection removed
6	Results fed back to Predatar Signal ML engine
⊙	Clean node moved back to production with 1 click

Stay ahead of threats with cyber analytics and benchmarking

Predatar Cyber Recovery Orchestration includes unique cyber analytics capabilities.

Real-time cyber benchmark scores show users the overall cyber-health of their estate at any moment in time and lets them easily see the health of individual nodes and fix problem with a few clicks.