HITACHI

White Paper

Intelligent Storage Operations With Hitachi Virtual Storage Platform 360

Hitachi Vantara

AI-Powered Anomaly Detection, Correlation and Insights

HITACHI

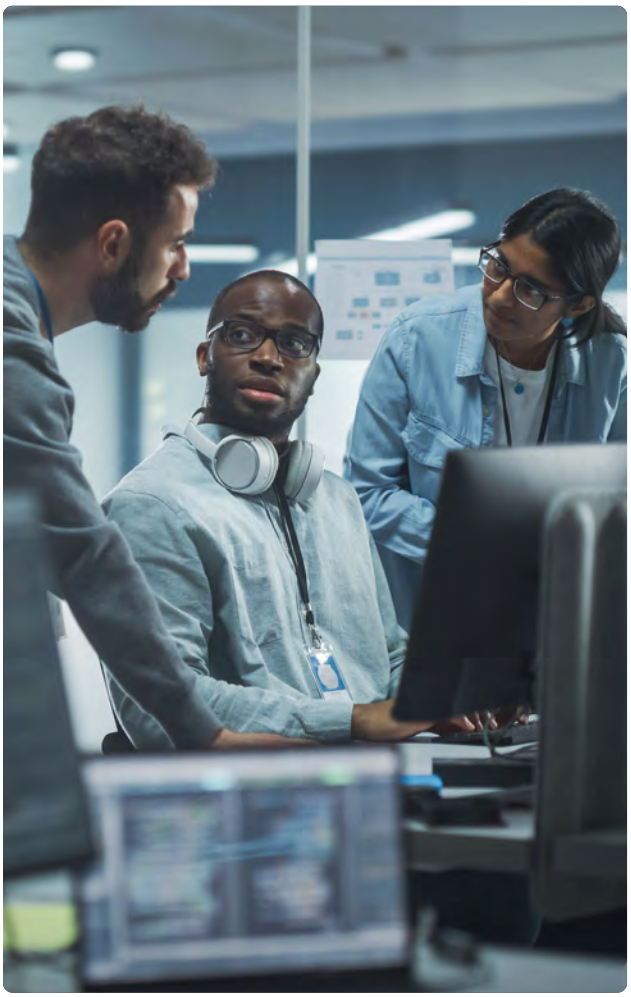
White Paper

Table of Contents

Executive Summary

Hitachi Virtual Storage Platform 360 (VSP 360) advanced analytics features an AIOps-powered anomaly detection engine that continuously learns each application's normal storage behaviors — helping to automatically spot abnormal patterns, performance bottlenecks and prevent outages.

This white paper details the advantages of VSP 360 anomaly detection capabilities, explains its detection model, and shows how IT and storage teams can utilize it daily. Aligned with industry analysts' AIOps frameworks, VSP 360 provides the essential AIOps recognition layer and self-learning anomaly detection with resource-context correlation, forming part of a broader AIOps strategy that includes event correlation, causality analysis and automated remediation.



The Challenge: Reactive Storage Operations

VSP 360 advanced analytics collects and reports on a wide range of performance metrics from Hitachi block storage systems. In real-world customer environments, telemetry data inevitably includes abnormal values, workload spikes, unpredictable system responses and contention over shared resources. Up to this point, there has been no built-in mechanism to detect such outliers. Anomalous data points go unnoticed, and by the time a problem surfaces as a slow application or a support ticket, users are already affected.

The operational cost of that gap is familiar to every storage team:

- Detection happens after the fact; an application is already slow before anyone investigates.
- Tracing an issue from the application down to the responsible storage resource means manually correlating spreadsheets and charts, often for hours.
- Static thresholds require constant hand-tuning, and they may still miss context-dependent anomalies.
- Knowing whether a spike is a one-time event or a recurring pattern depends on tribal knowledge rather than evidence.

Anomaly detection closes this gap by moving storage operations from reactive firefighting to proactive, data-driven monitoring.

Solution Overview

The goal is clear: Proactively identify and highlight unusual activity in applications and related storage-system resources to IT operations. The engine constantly monitors performance metrics such as IOPS, response time, transfer rate and the storage resources used by each application workload. Any anomalies are promptly reported in the VSP 360 analytics user interface (UI), enabling quick detection, monitoring and analysis.

These capabilities are organized as a four-stage pipeline:

- **Baselining —** Compute the mean and standard deviation for each metric from historical data.
- **Incremental updates —** Continuously refresh those statistics as new data arrives, using Welford's algorithm.
- **Detect and validate —** Identify candidate anomalies with a Z-score test, then confirm them against a dynamically maintained operating range.
- **Store and report —** Continue to detect anomalies and display them on the VSP 360 analytics dashboards.

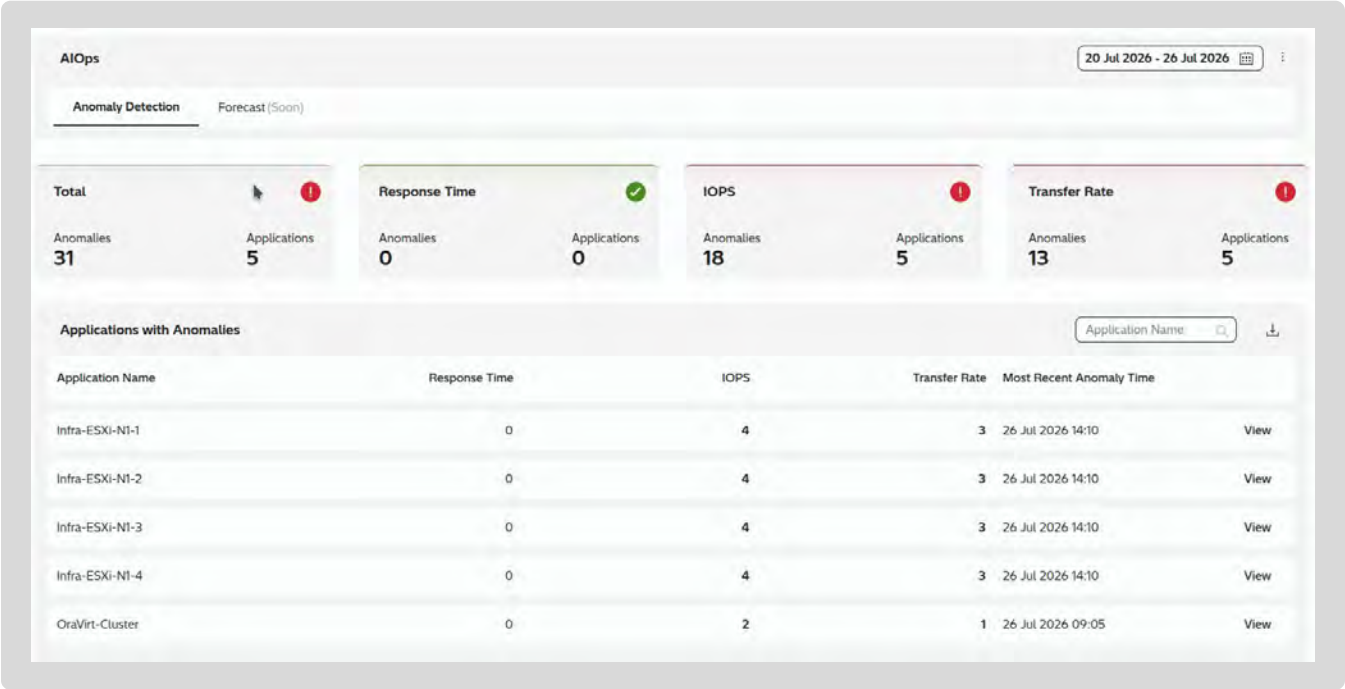


Figure 1. The VSP 360 AIOps anomaly detection dashboard: Data estate-wide anomaly counts by metric with an "applications with anomalies" table for drill-down.

Detection occurs at the application level and across all resources accessed by each application. The metrics tracked at each layer include:

Resource	Metrics Monitored
Application	IOPS, Response Time, Transfer Rate
Volume	IOPS, Response Time, Transfer Rate
Port	IOPS, Response Time, Transfer Rate, Utilization
Cache	Write Pending Rate
Processor	Utilization

Operational Use Cases

Anomaly detection can impact the daily tasks of teams responsible for storage health and IT risk management. The following scenarios mainly address storage and IT operations personnel challenges, with extra benefits for architects and application owners highlighted at the end.

Storage Administrator — Day-to-Day Health and Performance

Problem or Pain Point	How VSP 360 Solves It	Business Outcome
I get alerted only after an application is already slow, so users are impacted before I can investigate.	The anomaly detection dashboard's applications with anomalies table shows IOPS, response time and transfer rate deviations as they occur, ranked by severity so the most critical issues surface first.	Reduced mean time to detect; the administrator acts before end-user impact.
Tracing a performance issue from the application down to the root-cause resource takes hours.	Drill down from an anomalous application directly to correlated volume, port, processor and cache charts; timing correlation makes the root cause visible in minutes.	Mean time to resolve cut from hours to minutes, with no manual correlation.
I can't tell whether a spike is a one-time event or a recurring pattern.	A date range of up to seven days shows point-in-time anomaly history, revealing when anomalies started and how often they recur.	Evidence-based escalation and capacity decisions instead of guesswork.

IT Administrator or Manager — Risk, Security and Compliance

Problem or Pain Point	How VSP 360 Solves It	Business Outcome
I have no visibility into ports with LUN security disabled, so any host on a shared port can reach any volume.	The port LUN security insight flags every port where LUN security is disabled, with drill-down to the exposed ports and affected host groups.	Closes an unauthorized-access exposure and supports audit requirements.
Idle applications consume allocated capacity, but I can't identify reclamation candidates without a manual review.	The idle applications insight surfaces applications with no recent I/O including capacity details, so IT can reclaim or archive.	Direct storage cost recovery and reduced wasted capacity.
When an application slows down, storage and application teams spend hours arguing over where the problem originated.	The anomaly timeline correlates application and storage metrics, giving every team a shared view of whether storage is the cause.	Shorter bridge calls, faster cross-team alignment, quicker remediation.

Valuable for Architects and Application Owners

Storage architects review a seven-day anomaly history and resource correlation to distinguish real workload growth from temporary misconfigurations. This aids in making informed decisions about cache sizing, workload placement and hardware updates. Application owners receive a shared time series with anomaly tags that they can view alongside the storage team. If VSP 360 shows no anomaly for an application, the storage layer is considered clear, leading to investigations in other areas, such as the application or network. The seven-day view also acts as a supportive tool, a timeline of incidents, which is useful for post-incident reports and SLA discussions.

How It Works: The Detection Model

Anomaly detection mimics the approach of a seasoned operator, but it does so continuously and at a larger scale. It learns the normal patterns for each metric and then compares every new reading to this learned baseline. Two checks operate in tandem: One assesses how far a reading deviates from usual behavior, while the other verifies if it lies outside the realistic operating range of the metric. Using both checks helps achieve high accuracy and reduces false positives.

Learning What's Normal. The engine creates a baseline for each metric based on its historical data, representing the typical value and its usual variation. This baseline updates automatically with new data, ensuring it always captures current behavior without needing to reprocess all past data. It also adapts seamlessly to new or changing workloads as they develop recognizable patterns.

Flagging What's Unusual. Each new reading is assessed based on its deviation from the normal baseline. Readings within the expected range pass, while those deviating significantly are flagged as candidates. Sensitivity settings can be adjusted in VSP 360 › Administration › Settings › Report Parameters, allowing teams to control how reactive the monitoring system is.

- Stable production environments — Lower sensitivity to minimize alert noise.
- General production — The balanced default.
- Test or dynamic environments — Higher sensitivity for earlier detection.

Two safeguards prevent the engine from over-reacting to subtle metrics: Tiny changes are disregarded even if they seem statistically significant, and stable metrics are protected from false alarms caused by minor fluctuations.

Confirming it matters. A flagged reading undergoes a second validation against the metric's actual operating limits before being reported. Only readings that fail both checks are identified as anomalies, ensuring that a harmless unusual blip never alerts the operator. These boundaries adjust over time, reflecting recent behavior while allowing past isolated spikes to fade, preventing a single historical event from affecting future detection.

The system maintains up-to-date detection that adapts to the environment and highlights what truly matters, all without requiring manual thresholds or data-science skills.

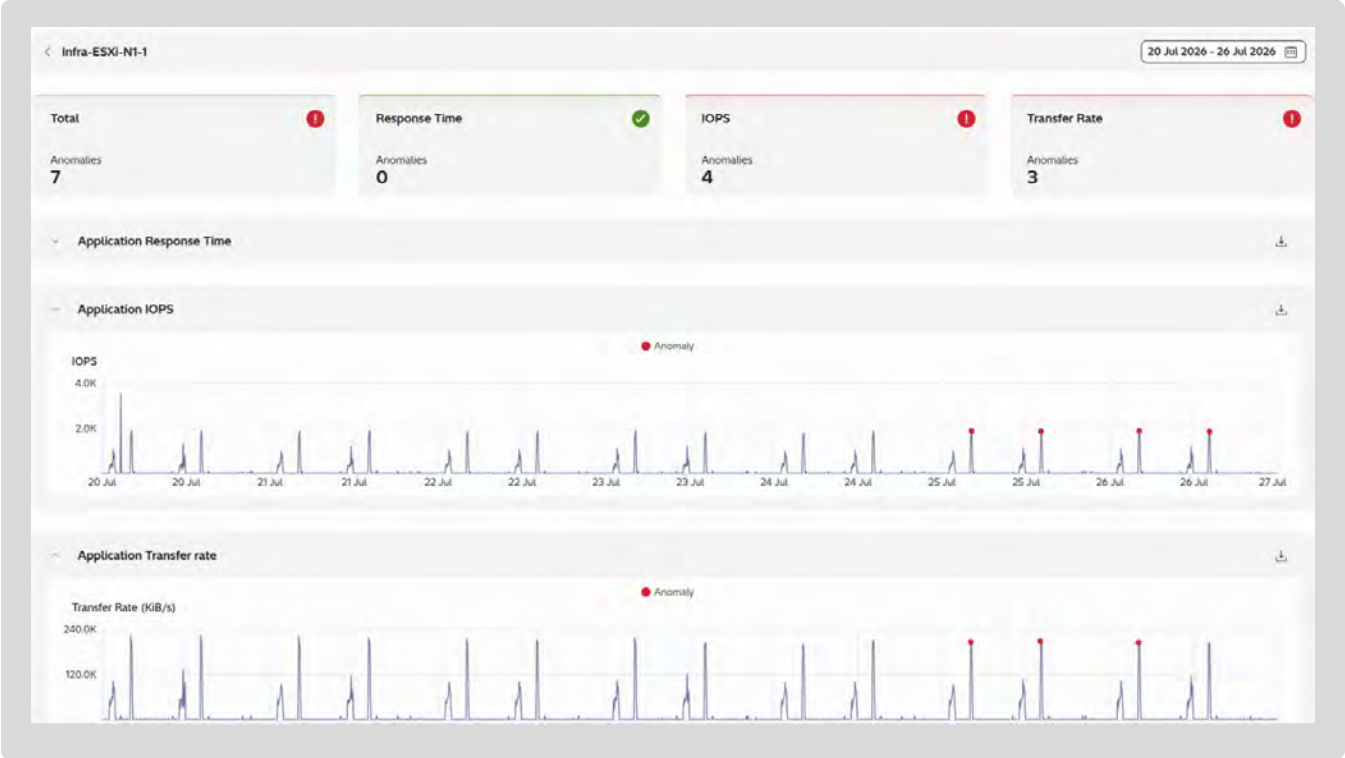


Figure 2. Application deep-dive view showing total and per-metric anomaly counts, with detected anomalies highlighted across each performance chart.

Working With Anomalies in the UI

Detection works best when operators can respond quickly. Anomalies are shown through three interconnected views, moving from a broad estate overview to a detailed root-cause analysis for a particular application.

Dashboard Widget

The anomalous applications widget on the VSP 360 main dashboard displays the total affected applications and shows how anomalies are distributed across IOPS, response time and transfer rate. Clicking on it takes you directly to the AIOps anomaly detection dashboard for more detailed analysis.

AIOps Anomaly Detection Dashboard

A new "AIOps" feature located under the VSP 360 analytics menu offers a centralized view of anomalies across all applications and metrics. It defaults to displaying data from the last 24 hours, but users can select a historical range of up to seven days. KPI cards at the top provide a summary of total anomalies and affected applications, with detailed breakdowns by metric, anomaly count and application. The applications with anomalies table lists each application with at least one anomaly, organized by total anomaly count to highlight the most impacted applications first. Clicking "View" opens a detailed analysis for the selected application.

The seven-day limit is intentional. Anomalies are specific events at a point in time that need detailed data for accurate display, and such data is only accessible within that period. Extending the duration involves using summarized aggregates, which cannot precisely reflect the timestamps of each anomaly.

Application-Specific View

The application view offers detailed analysis for a selected app over a specified time range (Default: last 24 hours). KPI widgets provide summaries of total and per-metric anomalies related to response time, IOPS and transfer rate, assisting operators in pinpointing key contributing metrics. Performance charts display each metric over time, with anomalies marked in red; charts with anomalies are expanded by default, while others remain collapsed to highlight important issues.

Importantly, related-resource charts for volumes, ports, processors and caches connected to the application are displayed alongside. By default, the top five resources ranked by anomaly count are shown, with options for operators to modify this selection. These combined views enable teams to quickly verify whether an application issue is caused by an underlying resource — such as cache write-pending pressure, port contention or processor saturation — reducing a multiple-hour troubleshooting process to just a few minutes.

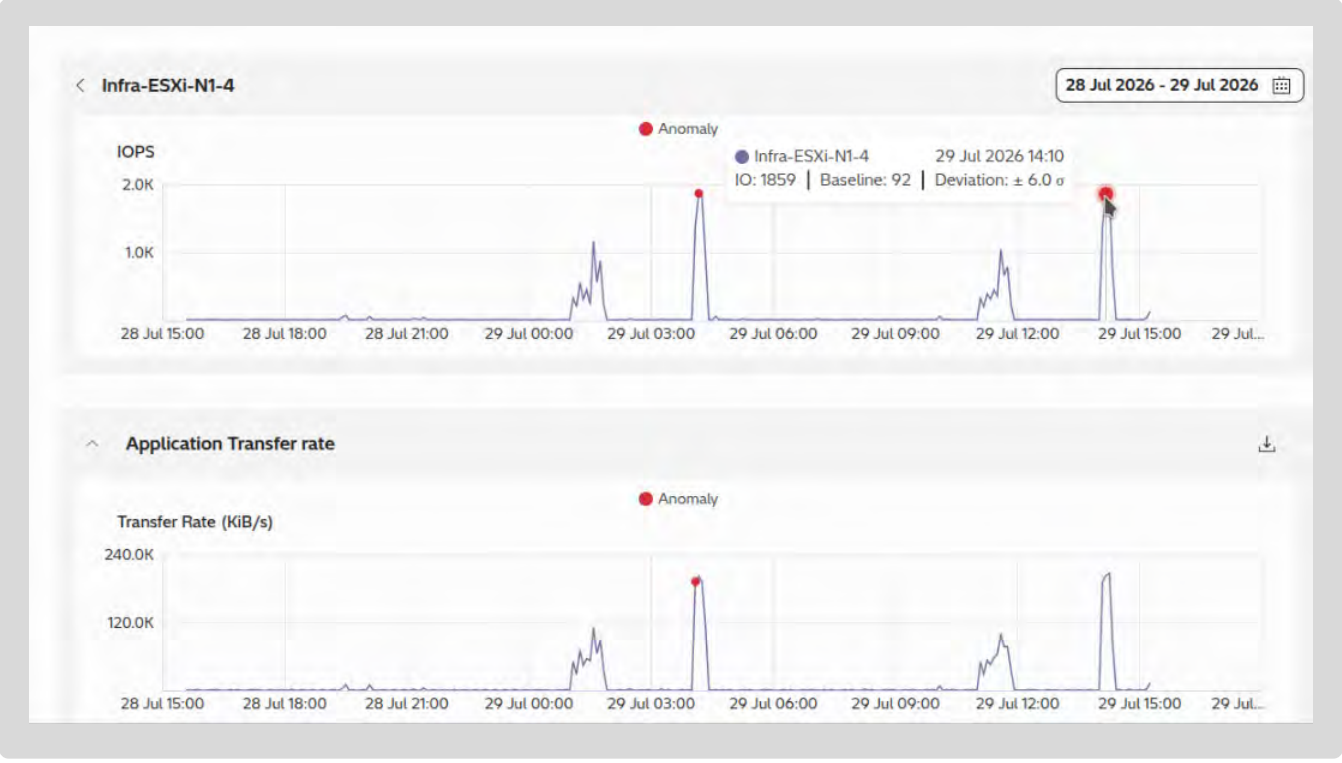


Figure 3. Drill-down into a single application's anomalies, correlating IOPS and transfer-rate spikes over a selected time range.

Beyond Detection: Actionable Insights

Alongside anomaly detection, VSP 360 surfaces a set of actionable insights that translate storage hygiene into concrete, prioritized work items:

- **Port LUN security —** Flags ports where LUN security is disabled.
- **Unused host groups —** Identifies host groups with no associated hosts, no volumes or both.
- **LUN single path —** Highlights volumes exposed on a single path, a high-availability risk.
- **Port and processor imbalance —** Reveals uneven load distribution across front-end ports and processors. The processor load-balance range defaults to 30–70% utilization measured over the last seven days, and it is configurable under VSP 360 › Administration › Settings › Report Parameters.
- **Idle applications —** Surfaces applications with zero recent I/O as reclamation candidates. The idle threshold defaults to 30 days without IOPS activity and it is configurable under VSP 360 › Administration › Settings › Report Parameters.
- **Workload Placement —** Recommends the best system or pool for a new workload based on capacity, utilization and performance headroom.

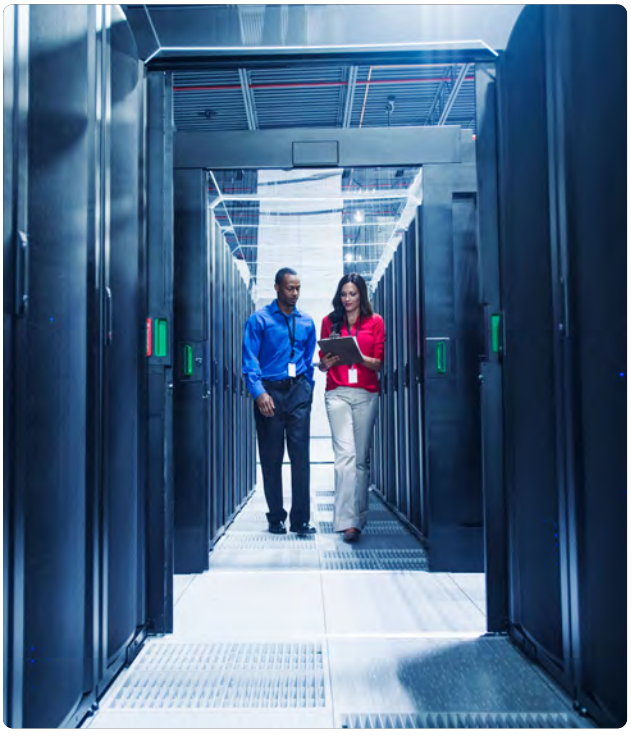
Behaviour Considerations

- Since detection relies on deviations from learned behavior instead of fixed thresholds, understanding a few key characteristics can help when interpreting results.
- Metrics usually having low or near-zero values can trigger an anomaly with even a small increase, due to the significant relative change.
- Recent workloads with limited historical data might yield fewer stable results until sufficient baseline data is collected.
- Temporary events like workload spikes, maintenance or scheduled operations may be flagged if they noticeably differ from typical historical patterns.

Configuration and Administration

VSP 360 analytics allows operators to control the engine's learning process and reaction sensitivity, and it is accessible via VSP 360 › Administration › Settings › Report Parameters. Anomaly detection is enabled by default; disabling it halts calculations and hides the AIOps card from the dashboard. Re-enabling it triggers a recalculation of the baseline over the specified learning period.

- **Configurable learning period —** Minimum and maximum historical duration used for baselining (Default minimum 14 days, maximum 365 days). Until the minimum is met, the dashboard shows "Insufficient data for anomaly detection."
- **Configurable deviation range —** The Z-score threshold that defines an anomaly (Default ±3). Higher values reduce sensitivity and alert noise; excessively high values can delay detection of emerging issues.
- **Configurable monitored window —** The days and times over which data is evaluated (Default "All"). Changing the window discards the previous baseline and recomputes a new one.
- **Expanded resource selection —** Related-resource charts default to five selected resources and support up to 10 aligned with existing performance-chart behavior.
- **Anomaly tool tips —** Selection of an anomaly marker shows the exact metric value at that moment, along with relevant baseline and deviation context, giving operators a clearer view of the anomaly without leaving the chart.



What's Coming Next

Expanding Anomaly Detection Capabilities

VSP 360 anomaly detection starts by identifying point-in-time deviations in performance. The direction from here follows three threads.

Sharper signal, less noise. Detection widens to a richer set of operational signals and finer-grained data, so short-lived and localized anomalies become visible rather than averaged away. Baselines become time-aware: Comparing a reading against the behavior that period normally shows, instead of a flat historical mean, surfaces gradual drift alongside sudden spikes. Confidence scoring separates the familiar and harmless from the deviations that actually warrant attention.

From detection to direction. The near-term work moves the platform past surfacing what happened and toward explaining why it matters and what to do about it. That includes classifying anomalies by severity, routing them to the team that owns the problem through the channels team already uses, and letting operators scope closer monitoring to the applications the business cares most about. Over time, the outcome of each action feeds back into the model.

Recognition layer that extends past performance. The same detection engine is not limited to performance metrics. As the range of signals it observes broadens the value of a single recognition layer across an environment compound, the ability to act against what it surfaces becomes the natural next step.

Overall, these directions steer VSP 360 analytics toward a well-defined objective. Instead of just highlighting anomalies, VSP 360 focuses on explaining what is significant and why it is important. Then, it recommends actions. This approach aligns with the expectations of a contemporary, AIOps-powered VSP One data storage platform.

Summary

AIOps anomaly detection provides self-learning, proactive monitoring within VSP 360 analytics. It uses a statistically robust engine featuring online baselining with Welford's algorithm, Z-score screening with practical safeguards, and range verification on an EWMA (exponentially weighted moving average) adjusted operating spectrum — identifying abnormal application behaviours without manual thresholds or machine learning expertise. Anomalies are highlighted where operators already work, in a comprehensive dashboard and linked resource charts for individual applications.

With this approach, IT and storage teams can shift from reactive firefighting to evidence-based decision-making. It enables faster detection, pinpointing root causes within minutes rather than hours, and provides a unified view that aligns storage, applications and IT personnel. Built on a self-learning foundation tailored to each environment's normal patterns and with a clear direction toward pattern-based intelligence, VSP 360 analytics provides a simple, scalable solution that evolves with the enterprise.

About Hitachi Vantara

Hitachi Vantara is transforming the way data fuels innovation. A wholly owned subsidiary of Hitachi, Ltd., we're the data foundation the world's leading innovators rely on. Through data storage, infrastructure systems, cloud management and digital expertise, we build the foundation for sustainable business growth.

Get more information about VSP 360

Learn More

Hitachi Vantara

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA
hitachivantara.com | community.hitachivantara.com

Contact Information
USA: 1-800-446-0744
Global: 1-858-547-4526
hitachivantara.com/contact

© Hitachi Vantara LLC 2026. All Rights Reserved. All other trademarks, service marks and company names are properties of their respective owners.

HV-BTD-WP-Intelligent-Storage-Operations-1Aug26-A