Look Out for Anomalous Drops in Data Reduction Ratios on Your Appliances

Any time there's a deviation from normal steady state operational patterns, it's a situation worthy of note. It does not always imply a malicious attack or breach in security, but cautious IT administrators prefer to be aware of these deviations.

Customer environments are unique to each customer given the applications/workload mix, multi-vendor hardware, and usage patterns that vary with the time of the day, day of the week, and month of the year. It's extremely important to establish what is "normal" for that environment for a given customer and surface the anomalous deviations so that further analysis can take place. It's painstaking to constantly monitor these metrics and spot significant deviations.

At Pure, we understand this acute need for proactively discovering anomalies and have started surfacing them in Pure1®.

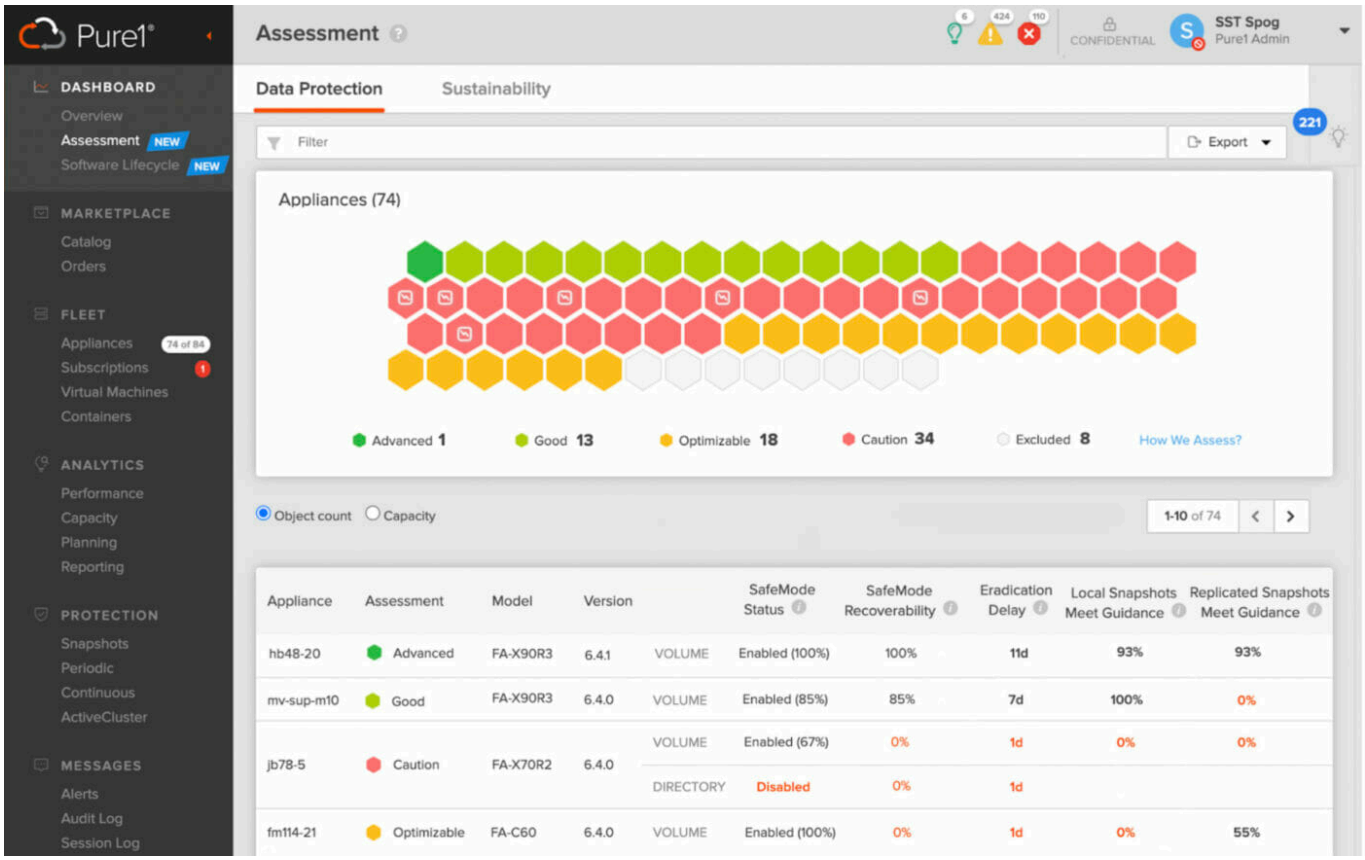

Figure 1: Pure1 Data Protection Assessment dashboard.

Storage is the last line of defense and the anomalous patterns noted in data storage need qualification by external markers before they can be associated with an unintended action by unsuspecting insiders or an intentional attack. In either case, it's important to review the anomalous alert raised and clear it.

Data Reduction Ratio (DRR) represents the level of compression and deduplication that a Pure Storage array provides to the customer. This is a highly desired feature of all Pure Storage appliances. For a given application and usage pattern, the DRR tends to stay within a normal operating range.

Sharp drops in DRR are usually the result of drastic operations on the data—such as a large-scale encryption followed by deletion of data, as is common in many malicious attacks. By surfacing anomalous drops—sharp drops, typically over 30%—in volume level DRR for multiple volumes on your array, we aim to get your attention to analyze them.

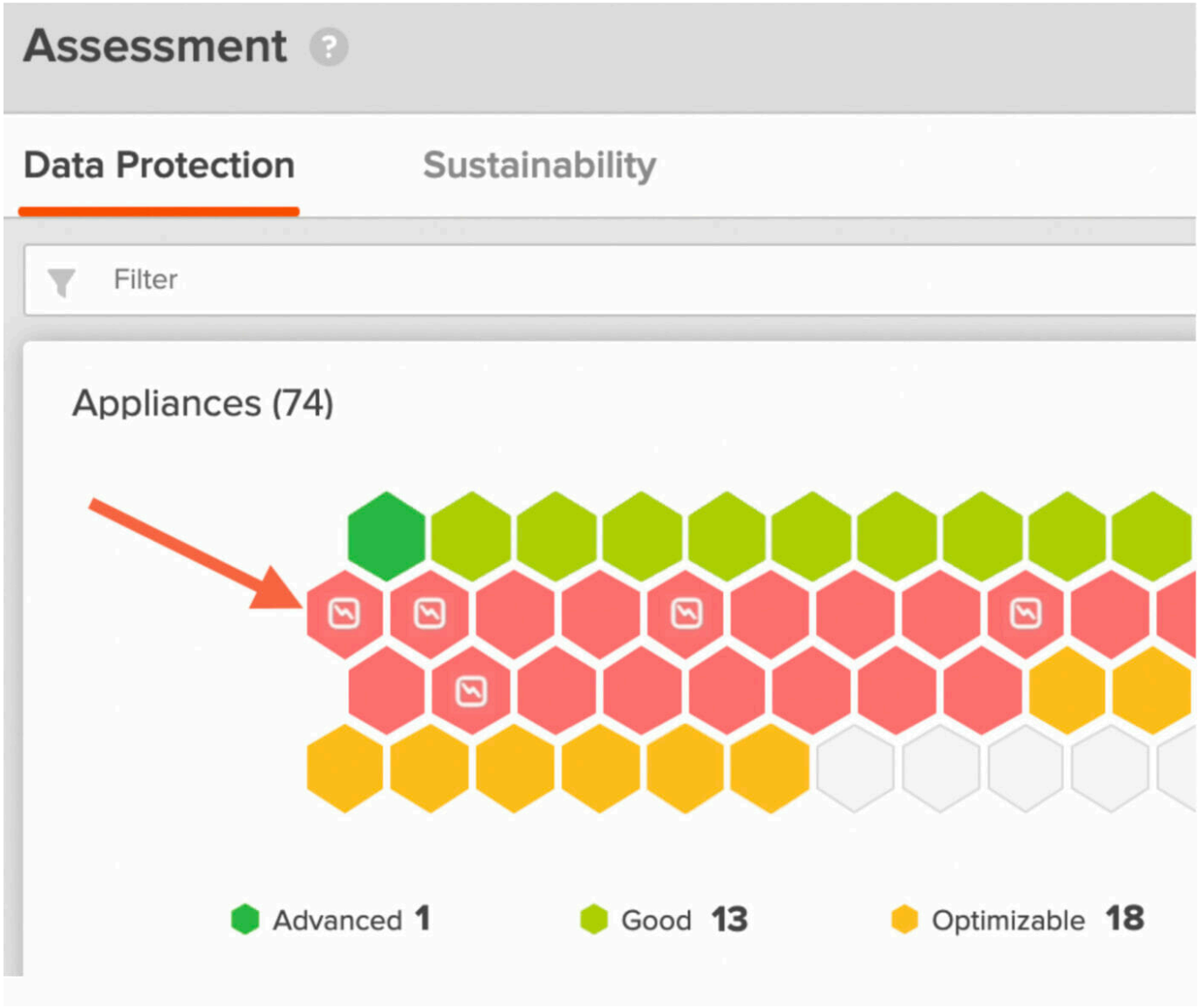

Figure 2: Pure1 Data Protection Assessment showing arrays with DRR drop anomalies.

To see if any arrays have such anomalies, go to the Data Protection Assessment in Pure1 and look for cells that have a lightning bolt (as pictured in the screenshot above). Clicking on the cell will bring up the insights sidebar where you can get more detail on what was detected.

To see the DRR anomaly detection feature in action, check out this Digital Bytes episode.

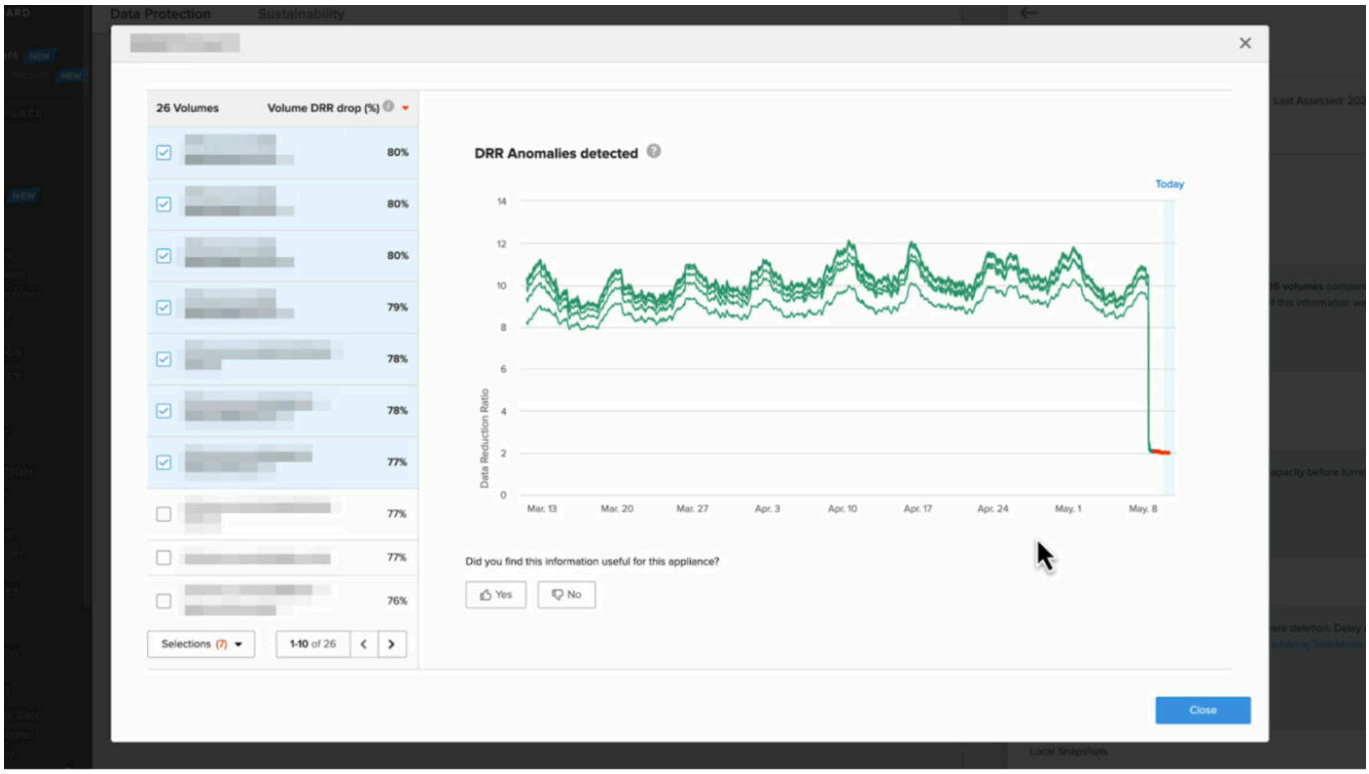

Figure 3: DRR past behavior for an array with an anomaly detected.

This is not intended to replace your SIEM or other security systems. By the time DRR falls, it's usually too late as your data has already begun to encrypt. However, this is a great tool for identifying the spread of an attack and can greatly reduce recovery times by identifying the ideal recovery time point. This also helps reduce data loss by recovering from older backups.

Pure uses a data science-driven approach to detecting these DRR drop anomalies based on past behavior (90 days) and filters out common noisy triggers.

This is just the first step, and Pure Storage is committed to expanding anomaly detection to multiple other metrics and correlating them to provide the highest-quality signal needed to protect your data.

For more information, check out the Pure1 product page. If you're an existing customer, log in to Pure1 and start taking advantage of this great tool provided to our customers at no additional cost.