SOLUTION BRIEF

IT Operations Analytics without Compromise

Get more information in less time with Pure Storage®.

Data is the most important tool IT operation teams have for ensuring a business runs effectively and is safe from cyberattacks. Data from systems and applications help predict and prevent performance issues, system outages, security events, and more. Unfortunately, many teams struggle to provide the breadth of analysis needed. Digital environments generate tremendous amounts of log data and running concurrent queries on it can quickly overwhelm log-analytics storage. The result? Teams can't be as effective as they want and may miss events that create risk.

IT Operations and the Need for Massive Scale

Finding potential security and stability issues in modern IT environments requires operation teams to monitor IT systems, software-as-a-service (SaaS) applications, cloud, endpoints, and more. It also requires correlating system data with details from internal databases (e.g., HR) for advanced insights. All of this requires capturing hundreds of GBs to TBs of log data every day. It also requires event teams to run a large number of concurrent queries on log data for:

- Security monitoring and threat detection
- Performance and availability monitoring (VMs, Kubernetes, applications, etc.)
- Outage incident response and forensics

Running these concurrently, or even in batches, places tremendous I/O stress and capacity requirements on legacy storage, so much so that many teams can run only a fraction of the analysis possible. Even then, constant tuning of storage may be necessary for timely insights.

What IT operation teams need—and leaders expect—is to be able to run every desired query without worrying about storage bottlenecks that can slow down analysis.

Gather Real-Time Insights

- Ingest data at low latency for real time insights.
- Eliminate compromise on the number of queries before slowdowns occur.

Enable Innovation

- Provide teams with the agility to build new queries and dashboards, improving business efficiency.

Eliminate Downtime

- Non-disruptive upgrades and integrated business continuity software prevent exposure risks during upgrades or outages.

FlashArray™: A Scalable, All-Flash Infrastructure

With latency as low as 250µs, the architecture of FlashArray provides superior performance for powering IT operation analytic processes including security information and event management, application performance monitoring, and more. Pure engineered the flash architecture specifically to process numerous concurrent queries at high-speed. This ensures that as the breadth of analysis and correlation searches increases, teams will get insights on potential issues without delay.

As your environment grows, FlashArray easily scales capacity while continuing to deliver high performance. Data reduction controls capacity needs and Evergreen™ capacity consolidation enables you to move up to the newest flash technology. Pure1® further simplifies growth by predicting workload needs over time and modeling how you can optimize loads.

To eliminate risks of downtime, FlashArray//X offers a wide range of data-protection technologies plus industry-leading non-disruptive upgrades. Add in Pure1 predictive support, and Pure gives you the peace of mind critical for IT operations.

IT Operation Analytics at Pure Storage: No Compromises While Expanding Analytics

At Pure Storage, our IT Operations team faced similar challenges. To deliver the highest level of support for our business, the team needed to implement a robust set of security and performance management queries to monitor every aspect of the business—inside and out. (Figure 1).

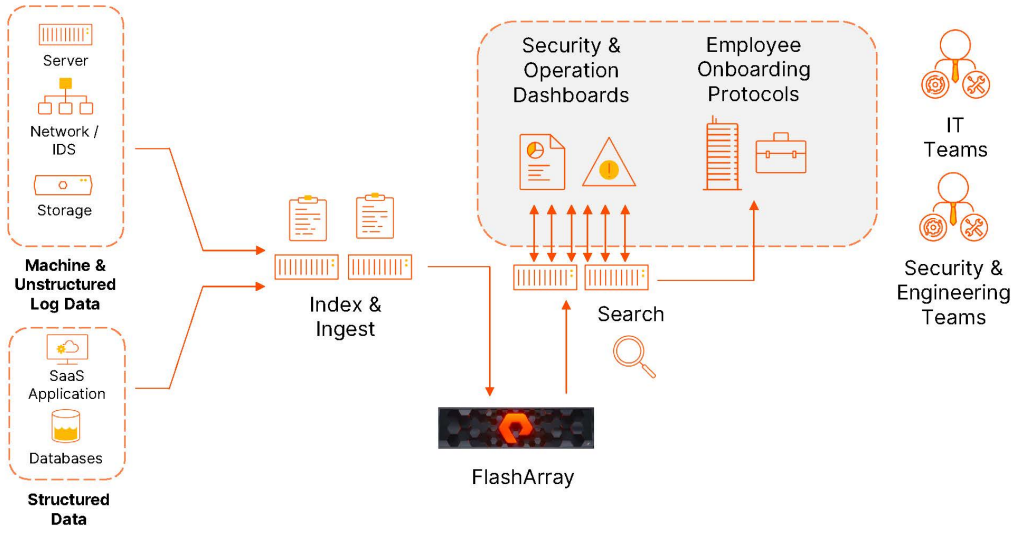

Figure 1: Pure IT operations security and performance management monitoring.

Our operations team ingests hundreds of GBs of data every day across IT systems as well as internal, cloud-based, and SaaS applications. Information is correlated and analyzed for a range of use cases including vulnerabilities, potential intrusions, user behavior and application stability.

All of this data is then delivered to the operations team in real-time for analysis, investigation, and triage. Ad hoc queries are also processed by help desk staff based on concerns about performance or availability of resources.

"It's a lot," says Lucas Sweany, a Pure Storage security architect. "Initially, the goal was to monitor the security of IT systems, applications, and corporate data. As the company expanded though, we saw an opportunity to monitor the health of our environment and manage business processes too. That added a whole new set of queries to manage and users to serve."

This expansion in the number of users and systems dramatically increased the amount of log data and more than doubled the number of concurrent queries. "With my previous implementation, this would have crippled the legacy SAN we had in place," says Lucas. "I was constantly monitoring Splunk's ingest queues to make sure the storage wasn't hampering Splunk performance."

With FlashArray, the security and operation teams haven't had to worry about this. In fact, the teams have been able to do more than their IT operations software provider thought possible. "They told us to run only sub-set of queries because too many would have killed the storage. We decided to run an experiment and see how much the FlashArray could handle. We turned on a massive number of ES correlation searches, just to see if it would kill the FlashArray." It had no impact on the storage. The team did ultimately have to increase the number of compute nodes, but the storage continued to deliver high-speed access with index queues—a measure of the amount of wait time on the array—staying at zero.

Enabling Innovative Thinking

Now that the Pure team isn't hindered by limits on what they can monitor or the need to constantly monitor their analytics infrastructure to make sure it is delivering on SLAs for queries, they are free to try new things. The first thing they did was to develop and implement new queries. "Latency kills the creative process," said Jason Brewer, Pure senior security engineer. "With FlashArray, I can model an analysis I think would help the company and iterate quickly. If it doesn't work as I'd like, I can pivot and try something else."

Similarly, the team saw an opportunity to simplify and accelerate new employee onboarding with the tools at their disposal. They designed a new dashboard, implemented on the same FlashArray, that managed all of the tasks HR and IT teams needed to complete new employee onboarding like adding them to internal systems, assigning them a laptop, and more. This cut the time required by HR and help desk staff to onboard a new employee significantly, freeing them to focus on critical issues and creative thinking.

Additional Resources

- Find out more about FlashArray//X.
- Learn how Evergreen Storage improves uptime and ROI.
- Find out more about Pure solutions for analytics.
- Use Pure as-a-Service™ consumption to lower acquisition risks.

PS1945-01 11/2020