SOLUTION BRIEF

Enhance Security Analytics

Responsive security analytics starts with performant, scalable, and simple data storage.

Investments in security analytics are essential to risk management in our modern digital world. The scale of data volume and movement means that security operations teams need automated and intelligent applications to maximize productivity. Capturing vast volumes of data in real-time can introduce unwanted challenges in the form of low performance or complexity. A scalable, simple foundation optimizes applications that are protecting your critical digital assets.

A Data Delivery Foundation for Security Analytics

Security operations need to monitor, analyze, and respond to security threats including phishing, denial of service attacks, ransomware, and advanced persistent threats. The need for effective applications to enhance the capabilities and productivity of security operations is well-understood. What can be overlooked, however, is how a foundation for data storage and delivery can impact common operational challenges. Specifically, the insights from security information and event management (SIEM) platforms can be optimized by combining performant access to real-time data with scalable, reliable access to historical data.

The massive growth of big data requires solutions that can keep pace with security analytics capacity requirements. Ensuring sufficient data capacity is just the beginning. Data storage and delivery performance can affect time to insight and the operational experience for modern applications. Inefficient scaling adversely impacts stretched IT budgets, and non-disruptive scalability is required to minimize application downtime. Easy to manage infrastructure ensures that IT teams aren't bogged down by repetitive tasks and that they can focus on delivering needed insights for action by security operations.

Performance

- Support more users and data sources with highly concurrent speed
- Fast data ingest and low latency for MTTR and MTTD needs

Efficient Scalability

- Disaggregated architecture real-time and historical data
- Grow from TB to PB, without disruption

Simplicity

- Easy to use systems help you focus on delivering more insights
- Efficient architecture reduces systems to manage and TCO

Enhance Security Analytics with a Modern Data Foundation

Security analytics often presents challenging requirements for collecting, delivering, and analyzing log and event data. The growing need to respond to threats as they occur mandates real-time data processing. Effective correlation and threat analysis require a thorough data capture from across the digital environment and the ability to maintain a rich historical data set. Data systems must also be resilient in the face of increasing data and a constantly changing landscape of data-forwarding systems and ever-present risks and threats.

Pure Storage® helps IT organizations by providing a performant, efficiently scalable, and simple data storage platform. Diagnosing and analyzing more threats become possible through high-speed ingest that captures more high-volume, rapidly growing log, packet, flow, and event data. Reliable all-flash performance helps security operations teams keep up with demanding, complex queries and the real-time processing needed for rapid mean time to detect (MTTD) and the mean time to remediate (MTTR) security threats. Adding blades enables you to scale for historical data analysis with consistent, linear performance. Complex search and forensic analysis are simplified with quicker access to high volumes of historical data to address a broader range of APT and legal discovery requirements. Finally, the disaggregated architecture from Pure separates storage and compute resources for efficient, agile resource deployment. This approach maximizes application uptime with nondisruptive scale and replacement, diminishing costly rebalancing, data re-hydration, and rebuild operations. Additionally, Pure1® offers AI-driven forecasting of capacity needs, simplifying essential workload planning. Pure systems have built-in ease of use that makes them easy to deploy, easy to upgrade, and easy to operate—helping more IT organizations focus on delivering insights by simplifying repetitive operational tasks.

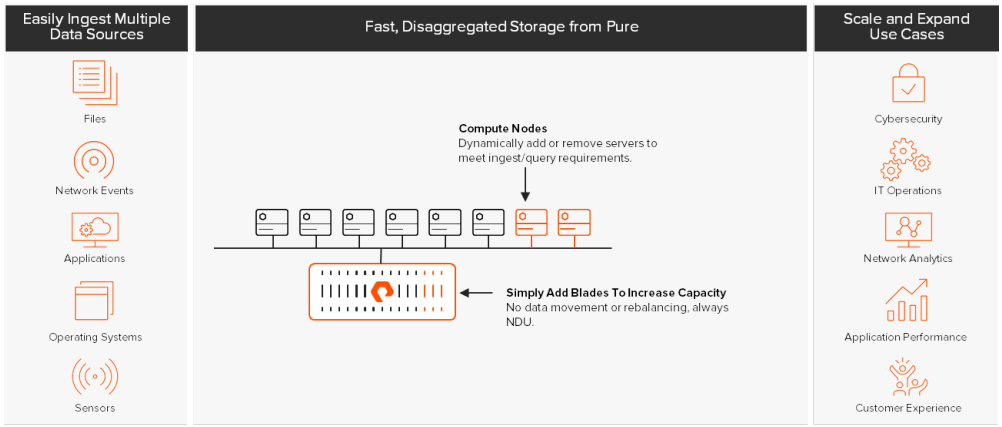

Figure 1: Pure Storage easily ingests log and event data and non-disruptively scales for multiple use cases. Pure offers performant, efficient, and simple data storage for security analytics.

Pure Storage Powers Security Analytics with Uncomplicated Data Storage

At Pure, we understand data is the most valuable asset modern enterprises have. We accelerate the time to insight from data analytics by turning bottlenecks into breakthroughs. Pure uncomplicates data storage for security analytics by building intuitive experiences, evergreen platforms, and architectures that launch innovation into everything we do. This enables IT organizations to transform data into powerful outcomes by keeping these priorities in mind:

An intuitive experience: With an emphasis on simplicity, Pure products disaggregate compute from storage to provide an efficient platform for hosting multiple analytics applications, concurrently supporting large user populations, easily scaling with data growth, and allowing you to eliminate the complexity of siloed approaches. This emphasis ensures that we build products

that are easy to install, easy to upgrade, and easy to use. We infuse our solutions with cloud-like models with the agility and flexible services to keep delivering as data needs change. Additionally, our disaggregated architecture enables administrators to scale and maintain infrastructure resources without causing expensive rebuild and rehydration operations for leading SIEM applications.

Evergreen by nature: The Pure Evergreen™ subscription model simplifies purchasing and upgrades, freeing budget for areas critical for analytics (such as compute) locally or in the cloud. With Evergreen, you get data infrastructure solutions that keep evolving, stay always-leading, and never go obsolete with upgrades handled on your behalf. Additionally, pay-as-you-go billing options provide you with the flexibility to scale up and down so that you can consume IT resources to fit your business needs. All of this helps ensure that you have sustainable and ESG-ready solutions to save space, consume less power, and ensure hardware never reaches end-of-life.

Architected for innovators: Pure wants to equip IT organizations with tools that will keep their applications and services on the leading edge of innovation to ensure a business advantage by making advanced insights possible with more of their modern data. Pure offers all-flash, high-performance platforms that can support every analytics tool on a data pipeline from ingest to visualization to help you gain real-time results at any scale, for both structured and unstructured data. Fast-object capabilities from Pure FlashBlade® allow you to run modern cloud applications with the control and efficiency of on-premises solutions and cloud-like economics of Evergreen with a single, scalable storage resource. Pure helps to keep your storage container-ready so that you can support modern app development with evolution, growth, and ambition in mind. We keep Infrastructure-as-Code as a guiding principle so that innovators can rapidly manage and provision data storage and create robust data services.

Additional Resources

- Learn more about how Pure can optimize IT and Security Operations Analytics.
- Learn more about our high throughput FlashBlade systems, low latency FlashArray™ systems, and professional service offerings.

PS2149-02 5/2022