SOLUTION BRIEF

Optimize Your Security Analytics

Accelerate threat detection and ensure availability of log data

SIEMs and security analytics are critical for modern cybersecurity, providing real-time threat detection, log correlation, and incident response across an organization's IT environment. They ingest tremendous volumes of data from network, user, system, and application logs to identify anomalous or suspicious activity.

However, SIEMs and security analytics often struggle to keep up with massive data volumes due to scalability limitations, high storage costs, and performance bottlenecks. The influx of logs from diverse sources overwhelms traditional architectures, leading to slow query performance, delayed threat detection, and increased false positives. Additionally, managing and correlating vast amounts of data in real time requires significant computational power, often straining resources and increasing operational complexity.

Storage Challenges for Cyber Security Monitoring and Analytic Systems

Often an afterthought in the world of cybersecurity, storage plays a critical role in the visibility, performance and resilience of modern security monitoring and analytics systems such as SIEM, UEBA, and XDR. Organizations should include storage as part of their security monitoring and analytics strategies, as SIEM and security analytics tools with effective data storage address several key challenges:

1. **Visibility**: Data is the primary target for threat actors, especially mission-critical data that ensures business continuity. Storage systems for critical applications must have seamless integration with security monitoring and analytic tools to identify suspicious access that could indicate ransomware activity or data theft.
2. **Performance:** Real-time threat detection depends on low-latency access to large datasets for rapid querying and analysis. These systems process vast amounts of log and event data, requiring **high-performance, scalable storage** to keep up with demand. Quickly identifying indicators of compromise is key to lowering risk and ensuring fast recovery.
3. **Resilience:** Availability depends on **protection and security** against destructive cyber threats, including ransomware and insider attacks. Threat actors target log data for deletion to cover their actions and to thwart rapid recovery. **And long-term data retention** is essential for compliance, forensics and trending, necessitating cost-effective yet secure storage solutions.

Improve Storage Visibility

Monitor analytics for your critical workloads for data and user anomalies.

Improve Security Analytics Resilience

Ensure your critical log data is available when needed.

Optimize Security Analytics Performance

Speed threat detection and support the scaling requirements of growing log data.

Visibility, Performance and Resilience

Pure Storage® empowers you to detect threats in critical storage and route them to your SIEM and security analytics, remove performance bottlenecks and ensure log repository resilience. And with Pure Storage performance and reliability, you can optimize the performance and reliability of your on-premises security analytics for faster anomaly and threat detection. Should the worst happen, log data is essential. The Pure Storage platform protects security analytics data repositories from malicious deletion from ransomware and cyber threats through layered resilience, robust data security and immutability.

Visibility, performance, and resilience are the foundation for effective security analytics performance and resilience. Visibility ensures you understand your data storage attack surface, get control of your data security safeguards, and monitor your log data repository for threats. Performance means you keep up with the vast quantity of log data that your SIEM, UEBA, XDR, and other solutions must correlate and analyze for rapid threat detection. Layered resilience ensures data availability when threat actors target your security analytics data repository.

For visibility, Pure Storage has integrated into popular SIEM and analytic tools such as Crowdstrike, Varonis, Cisco Splunk, Microsoft Sentinel, Cisco XDR, Exabeam LogRhythm, Palo Alto Networks QRadar, and Elastic. Log data from Pure Storage provides insights into anomalous data changes that could indicate a ransomware encryption event or user activity that could indicate data exfiltration or data theft. Monitoring your critical data improves your cyber resilience readiness and lowers the risk of damaging ransomware or other malicious attacks.

Pure Storage provides the optimal performance for threat detection of on-premises SIEM and security analytic tools. The Pure Storage platform, featuring FlashArray™ and FlashBlade® systems, meets diverse requirements with high-performance unified block and file services running on a single storage pool. It consolidates disparate workloads, scales to petabyte levels in an ultra-dense footprint, and offers advanced data reduction with intelligent deduplication and compression, effectively replacing legacy disk-based storage.

And for the resilience of your on-premises security analytic tools, Pure Storage extensive resilience capabilities provide 99.9999% data availability. Security and recovery innovations such as SafeMode™ Snapshots, zero trust security functions, anomaly detection, and rapid remediation and recovery are integrated into our platform. Combined with stringent service level agreements (SLAs), these features ensure that Pure Storage not only protects data and aids threat detection, but also enables swift, seamless recovery of security analytics data. Pure1® tools further empower organizations through proactive assessments, offering a Data Protection Assessment and Security Assessment to optimize and refine security strategies.

Pure Storage enhances security analytics visibility, performance, and resilience by integrating with leading security tools, optimizing log data analysis, and protecting repositories from cyber threats. With industry-leading performance, security, and recovery capabilities, Pure Storage ensures organizations can detect, respond to, and recover from attacks swiftly and effectively.

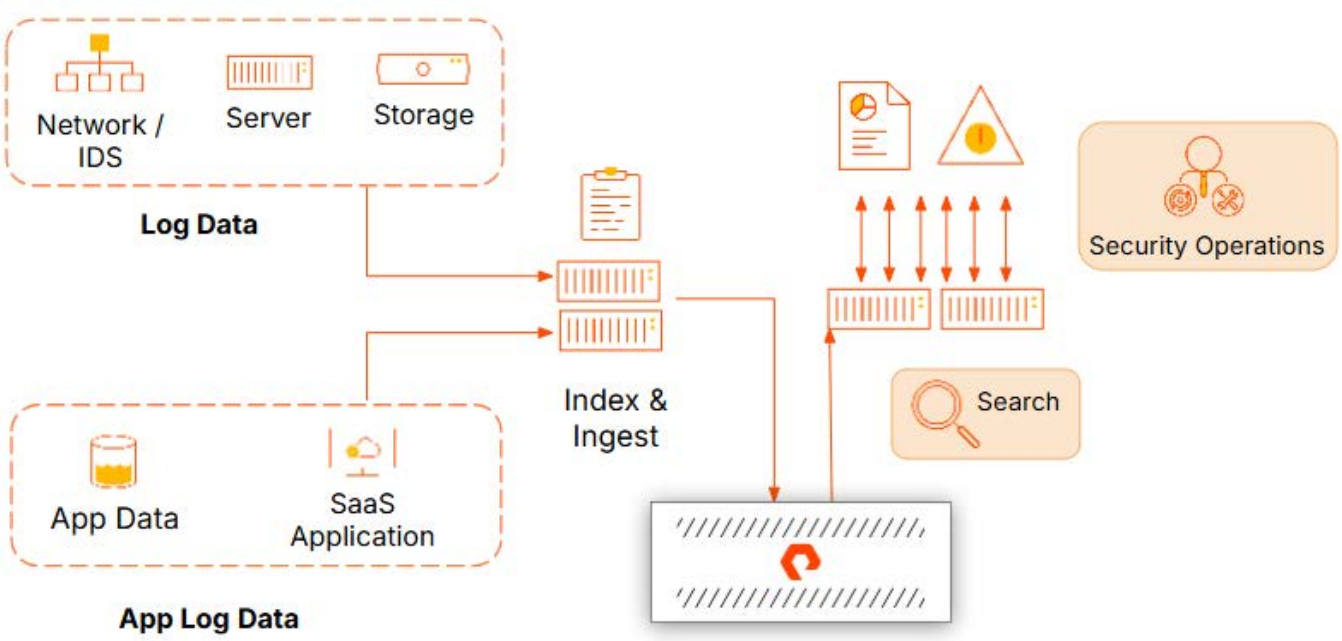

FIGURE 1 Architecture to accelerate SIEM performance

Critical Capabilities

Market-leading capabilities and integrations from Pure Storage help organizations quickly recover from cyber attacks and disasters. The Pure Storage platform supports the detection and response of threats targeting the platform with:

Cyber security integrations:

- Integrate with SIEM, UEBA, and XDR solutions to provide real-time visibility for storage threats
- Enhance threat detection, performance, and scalability when used as on-premises SIEM, UEBA, and XDR storage tier
- Ensure the maximum resilience of on-premises storage for SIEM, UEBA, and XDR solutions

Secure, scalable, and performant platform foundation for a cyber resilience:

- Help prevent ransomware attacks with immutable and indelible SafeMode Snapshots, zero-trust security principles, and anomaly detection
- Consolidate block and file workloads, eliminating data silos by dynamically provisioning recovery workloads
- Gain ultra-low latency performance (150µs to 1ms) for rapid data access with high availability (99.9999%)

Cyber resilience readiness with Pure1:

- Use Data Protection and Security Assessments to evaluate system health, security posture, and performance
- Dashboards and predictive analytics offer real-time monitoring, capacity performance optimization
- Gain actionable insights and seamless integration with recovery and security services

For more information, see our Cyber Resilience Solutions page.

Additional Resources

- Learn about Pure Storage and Varonis
- Learn about Pure Storage and Cisco Splunk
- Learn about Pure Storage and Cisco XDR
- Learn about Pure Storage and LogRhythm
- Learn about Pure Storage and QRadar
- Learn about Pure Storage and Microsoft Sentinel
- Learn more about Pure Storage Technology Alliance Partners

PS2754-01-en 04/25