SOLUTION BRIEF

Detect and Remediate Critical Threats

Pure Storage® and Crowdstrike accelerate threat detection in mission-critical workloads to detect and remediate malicious activity.

Organizations need a high-performance, scalable solution to protect their mission-critical workloads. Accurate threat detection depends on rich telemetry from storage systems—such as access logs, I/O behavior, and snapshot activity—combined with real-time analytics, advanced correlation, and automated response. Together, these capabilities enable faster detection, clearer visibility, and effective remediation of threats targeting storage infrastructure.

Threat Detection Challenges

Detecting threats in mission-critical storage environments poses a growing challenge for security teams. While SIEM platforms are essential, they often struggle with accuracy—generating false positives from broad correlation rules or incomplete context. This wastes analyst time, erodes trust in alerts, and delays response to real threats. Compounding the issue, modern infrastructure produces a flood of logs and telemetry that can overwhelm traditional SIEMs, leading to alert fatigue and missed signals.

A core challenge is limited visibility into storage-layer activity. Many storage systems can't generate the rich, high-fidelity telemetry—such as access logs, snapshot activity, and I/O behavior—that SIEM tools need to detect threats accurately. As a result, attacks like unauthorized access or ransomware encryption may go undetected until damage is done.

When malicious activity reaches critical storage, the stakes are even higher. Without real-time visibility, organizations can't respond fast enough and business-critical processes and services grind to a halt. Worse, during recovery, identifying clean, uncompromised data is difficult, risking reinfection or data loss. True cyber resilience requires a solution that connects storage-layer anomalies with broader security analytics, enabling faster detection, real-time alerts, automated response, and confident recovery.

Accelerated Threat Detection

Real-time telemetry from Pure Storage is enriched by CrowdStrike intelligence for rapid anomaly detection.

Automated Response and Streamlined Remediation

Automated CrowdStrike Fusion workflows accelerate investigation and containment with SOAR-driven actions.

Confident Recovery

Immutable snapshots and integrated analytics enable fast, reliable recovery to clean restore points without reinfection risk.

Identify Threats Faster and More Accurately

CrowdStrike and Pure Storage work in tandem to significantly improve the speed, accuracy, and effectiveness of detecting threats in mission-critical storage environments. Together, Pure Storage and CrowdStrike transform storage-layer telemetry into actionable security intelligence.

Pure Storage FlashArray™ and FlashBlade® stream detailed activity logs such as user behavior, I/O patterns, and snapshot events through a secure pipeline to CrowdStrike's Next-Gen SIEM. There, the data is parsed, enriched, and correlated in real time, enabling rapid threat detection and automated incident response.

CrowdStrike Falcon NG SIEM combined with Crowdstrike Fusion SOAR delivers real-time threat detection by ingesting and analyzing large volumes of security telemetry, enabling rapid identification of malicious patterns and anomalies with minimal latency. Its built-in automation engine triggers response workflows, while behavioral analytics and integrated threat intelligence enrich alerts with context—reducing false positives and accelerating investigations.

Pure Storage FlashArray and FlashBlade enhance this joint solution by contributing high-fidelity storage-layer telemetry—such as user access patterns, snapshot operations, audit trails, and I/O behavior. These data points are ingested by CrowdStrike NG SIEM to extend visibility into storage environments, helping detect threats like unauthorized access, lateral movement, or ransomware encryption attempts.

Together, the integration of CrowdStrike NG SIEM and Fusion SOAR with Pure Storage FlashArray and FlashBlade enables faster detection, greater context, and automated remediation of threats targeting critical storage infrastructure, ensuring that security teams can respond proactively before damage occurs.

Together, they provide a high-fidelity, real-time view of storage-layer threats, enabling organizations to detect and respond to attacks before data is lost or compromised.

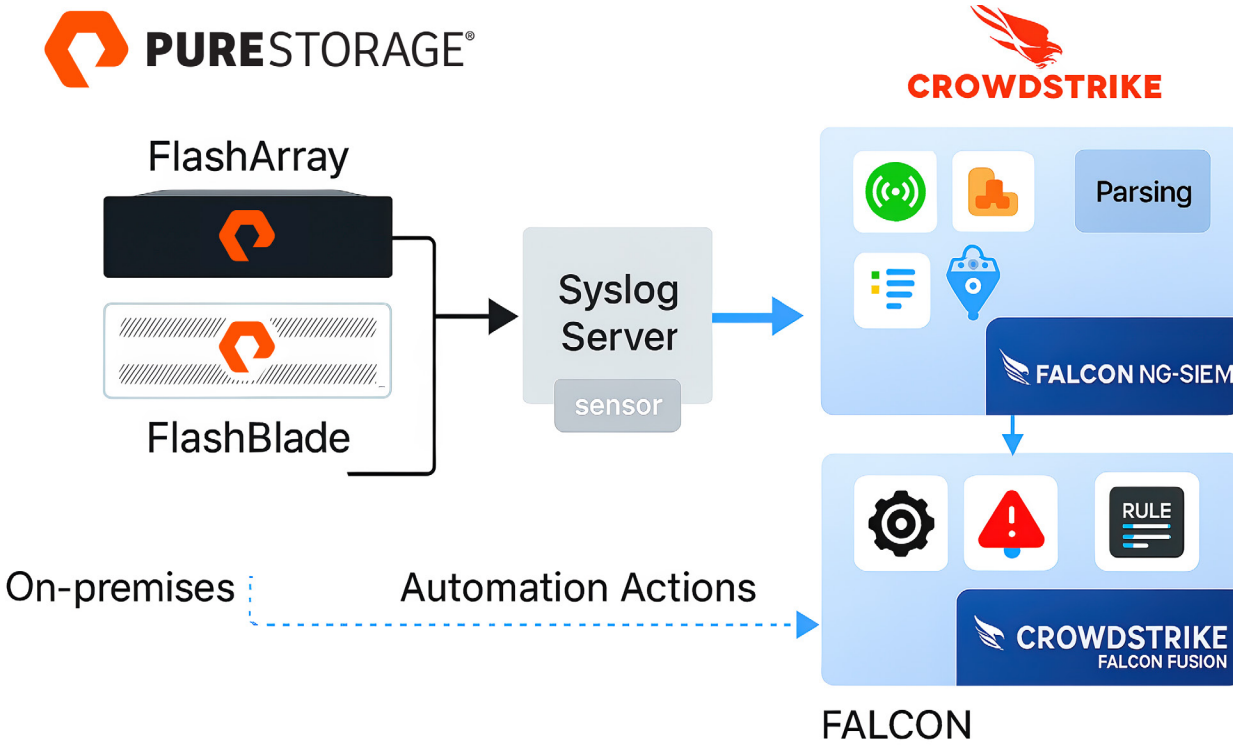

FIGURE 1 Pure Storage and Crowdstrike Falcon NG-SIEM-SOAR Solution Architecture

Solution Benefits

The integration of CrowdStrike NG SIEM and Fusion SOAR with Pure Storage FlashArray and FlashBlade offers organizations:

- **Real-time threat detection**: This enables immediate, automated responses to unusual storage access or anomalous behavior.
- **Proactive approach to security:** This proactive approach transforms storage signals into active security measures, triggering orchestrated remediation and preserving forensic data.
- **Increased security**: Ultimately, this capability significantly enhances security operations and analyst efficiency through improved incident investigation.

Additional Resources

- Explore Pure Storage cyber resilience.
- Learn more about Pure Storage technology alliance partners.
- Read the ESG report "How Organizations Are Defending Against Evolving Ransomware Threats."

ID5817-01-en-08/25