Solution Brief

Accelerate Threat Detection and Response

One partnership with four integrated solutions for full-lifecycle cyber resilience across mission-critical workloads

Attacks now move at machine speed, and defending mission-critical data requires comprehensive security and recovery solutions. Storage can no longer be a passive target sitting outside the security stack. It has to be an active defender in detection, investigation, and recovery.

Everpure™ and CrowdStrike are one of the first storage and endpoint security vendors to bring this level of integration to market, giving thousands of joint customers a single, connected path from detection to recovery. This is a platform-level partnership, not a point integration: four distinct capabilities, each covering a different phase of the security life cycle, all connected to the same storage layer telemetry.

Four cyber resilience solutions to reduce cyber risk

Threat detection in mission-critical storage is difficult. Security information and event management (SIEM) platforms struggle with accuracy: correlation rules and incomplete context cause false positives, while log volume overwhelms them. Storage lacks the telemetry SIEM needs, letting attacks like unauthorized access or ransomware go undetected. Once compromised, recovery suffers: stalled processes and hard-to-verify clean data compound the damage.

Everpure and CrowdStrike close this gap end to end, spanning visibility, intelligence, investigation, and response:

- **Visibility: Real-time detection with Falcon Next-Gen SIEM**. Everpure FlashArray™ and FlashBlade® stream detailed activity logs, including user behavior, I/O patterns, and snapshot events, through a secure pipeline to CrowdStrike Falcon NG-SIEM. There, the data is parsed, enriched, and correlated in real time, extending visibility into the storage layer to help detect threats like unauthorized access, lateral movement, and ransomware encryption attempts that endpoint tools alone would miss.
- **Response: Closed-loop remediation with Falcon Fusion SOAR**. Fusion SOAR automates response workflows triggered directly by Everpure detecting destructive events or configuration changes in real time on FlashArray and FlashBlade, accelerating containment and remediation on the array within seconds. Built-in automation, behavioral analytics, and integrated threat intelligence enrich alerts with context, reducing false positives and accelerating investigation and containment with security orchestration, automation, and response (SOAR)-driven actions.
- **Intelligence: Automated threat identification with Enterprise Threat Graph**. CrowdStrike's AI-powered Threat Graph identifies malicious activity in Everpure storage workloads using CrowdStrike's global threat intelligence and adversary tactics, techniques, and procedures, and it then remediates directly with actions on the Everpure Platform such as taking or isolating snapshots. This automates cyber defense so systems can be isolated and policies updated in real time, empowering SecOps to act with speed and confidence instead of waiting on a manual escalation.



Real-time detection

Storage layer telemetry from FlashArray and FlashBlade extends CrowdStrike's visibility to where your most critical data lives.



Automated remediation

Enterprise Threat Graph and Falcon Fusion SOAR isolate systems, update policies, and trigger snapshot actions within seconds of detection.



Petabyte-scale investigation

Falcon LogScale on FlashBlade keeps months or years of log data hot and searchable for forensics, audits, and compliance.



Confident recovery

Immutable, tamper-proof snapshots ensure you always have a clean restore point, with no reinfection risk.

- **Investigation: Petabyte-scale forensics with Falcon LogScale**. FlashBlade delivers scalable, high-performance, immutable storage, while Falcon LogScale complements it with index-free, real-time log management that supports long-term retention without compromising speed. Together they give security teams instant, high-performance access to months or years of log data for threat hunting, audits, compliance, and long-term investigations, with SafeMode™ and Object Lock ensuring that data can't be modified or deleted, even if credentials are compromised.

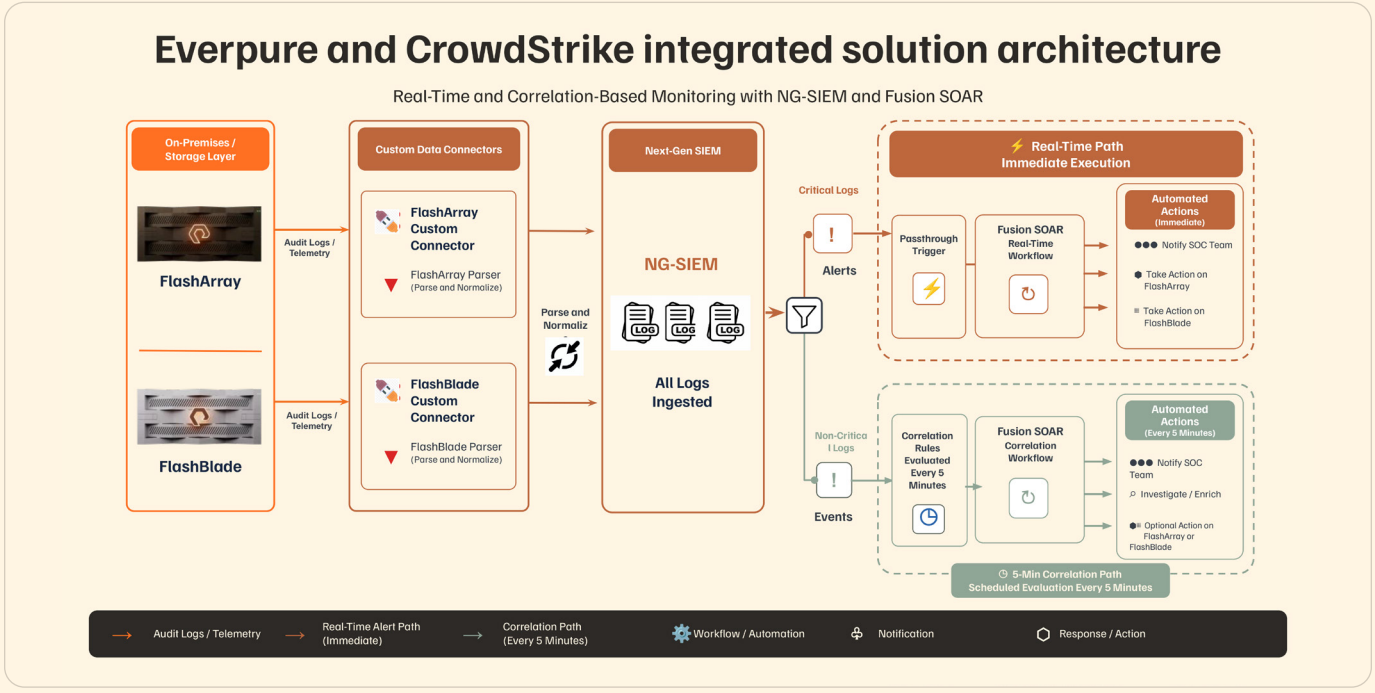
A closed-loop architecture

These four capabilities operate as a single, closed-loop pipeline rather than four disconnected integrations. Real-time storage telemetry feeds CrowdStrike security operations; dedicated FlashArray and FlashBlade connectors normalize that storage log data; Falcon NG-SIEM centralizes correlation and severity triage; and Falcon Fusion SOAR enables closed-loop action on storage, with real-time critical and non-critical classifications. All four phases of the life cycle—detect, hunt, investigate, and respond—are fully connected.

Solution overview

This integrated platform from Everpure and CrowdStrike is purpose-built for full-lifecycle cyber resilience, combining real-time detection, intelligent correlation, automated remediation, and long-term investigation into a single connected pipeline. It offers:

- **Real-time storage telemetry**: FlashArray and FlashBlade continuously stream access, I/O, and snapshot telemetry into the CrowdStrike Falcon platform for immediate correlation and analysis.
- **AI-driven threat correlation**: Enterprise Threat Graph applies CrowdStrike's global threat intelligence to storage layer signals, identifying malicious activity that endpoint-only tools miss.
- **Automated, closed-loop remediation**: Falcon Fusion SOAR triggers response actions directly on FlashArray and FlashBlade within seconds, with no manual escalation required.
- **Petabyte-scale log performance and retention**: Falcon LogScale on FlashBlade keeps years of immutable log data hot and searchable for forensics, audits, and compliance.
- **Clean, confident recovery**: Immutable snapshots ensure every recovery point is verified and reinfection-free, closing the loop from detection to restoration.



Critical capabilities

Everpure and CrowdStrike together provide:

- Real-time threat detection across storage and endpoints, enabling immediate, automated responses to unusual storage access or anomalous behavior.
- AI-powered Threat Graph correlation that identifies malicious activity in storage workloads and remediates directly with actions like snapshot isolation.
- Automated, closed-loop remediation triggered directly on FlashArray and FlashBlade within seconds of detection.
- Petabyte-scale, tamper-proof log retention for long-term threat hunting, audits, compliance, and forensic investigation.
- Reduced false positives and faster investigations through enriched, contextual alerts.
- Confident recovery to clean, immutable snapshots without reinfection risk.

Together, Everpure and CrowdStrike deliver an intelligent, full-lifecycle cyber resilience solution that detects and remediates threats in real time while ensuring your data is always recoverable to a clean, trusted state.

For more information, see our cyber resilience solutions.

Additional resources

- Learn more about the Everpure and CrowdStrike technology alliance.
- Learn about CrowdStrike Falcon.

Explore Everpure Cyber Resilience Solutions

Visit Our Website | **800.379.PURE**

©2026 Everpure, the Everpure P Logo, Pure Storage, FlashArray, FlashBlade, SafeMode, and the marks in the Everpure Trademark List are trademarks or registered trademarks of Everpure, Inc. or its licensed subsidiaries in the U.S. and/or other countries. The Trademark List can be found at everpuredata.com/trademarks. Other names may be trademarks of their respective owners.

ID55987-01-en-09/26