SOLUTION BRIEF

Integrated Cyber Defense with Commvault and CrowdStrike Next-Gen SIEM

Part of the Commvault and CrowdStrike integration series:

Falcon Insight XDR (threat visibility)

Falcon Next-Gen SIEM (detection)

Charlotte Agentic SOAR (agentic response and recovery)

EXECUTIVE SUMMARY

Cyber resilience depends on more than detecting threats. Security and IT teams also need to understand how an incident affects protected data and coordinate response and recovery. Integrations between the CrowdStrike Falcon® platform and Commvault® help bring these workflows together for faster detection, response, and recovery.

THE CHALLENGE

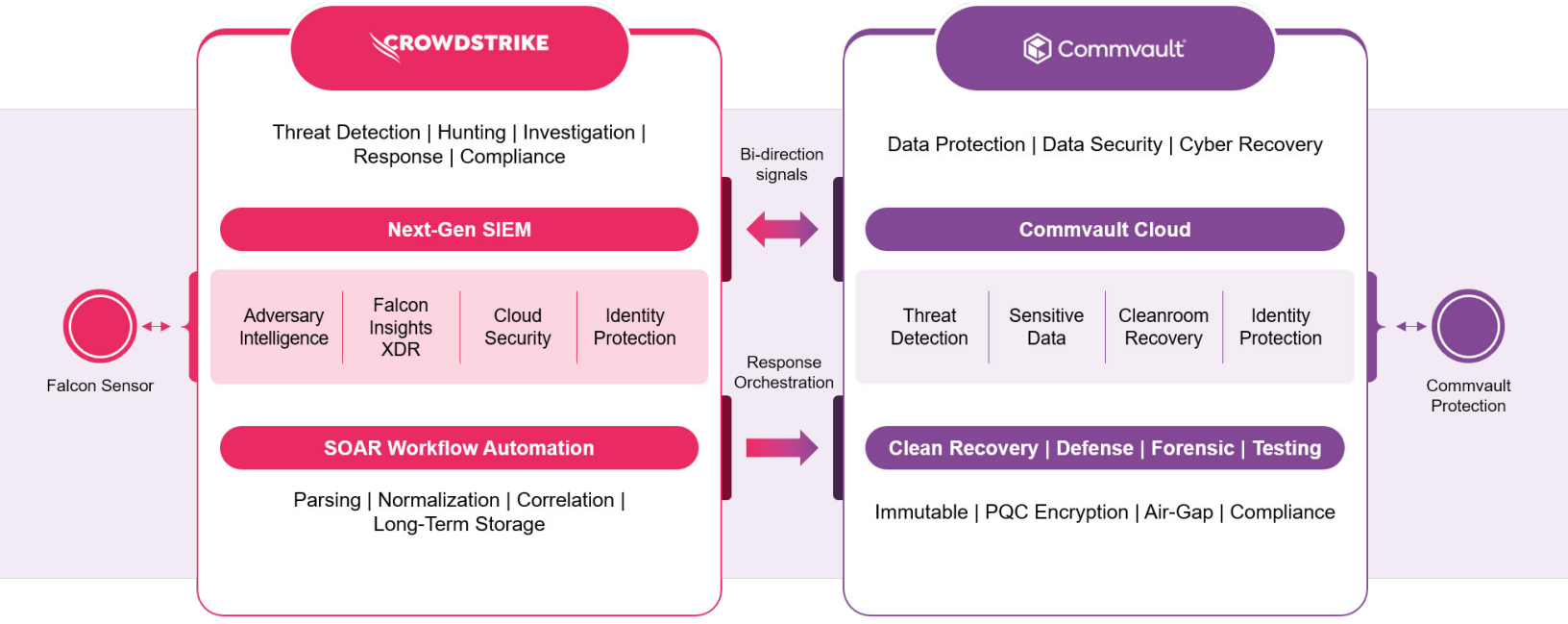
In today's volatile cyber threat landscape, every second counts. Attacks are designed to disrupt business and endanger data. To combat these threats, organizations need a coordinated defense that spans teams. That defense depends on three critical capabilities:

Detect Compromises Earlier	Identify threats before they escalate.
Clearly Understand Risks	Gain deeper insight into your data's security posture.
Recover with Confidence	Enable rapid, clean recovery from an incident.

SOLUTION OVERVIEW

The integration's value comes from the bi-directional flow of intelligence between the two platforms. CrowdStrike Falcon enriches the Commvault platform by identifying threats that could compromise data, while Commvault provides critical telemetry to CrowdStrike to enhance investigations and enrich Security Operations Center (SOC) intelligence.

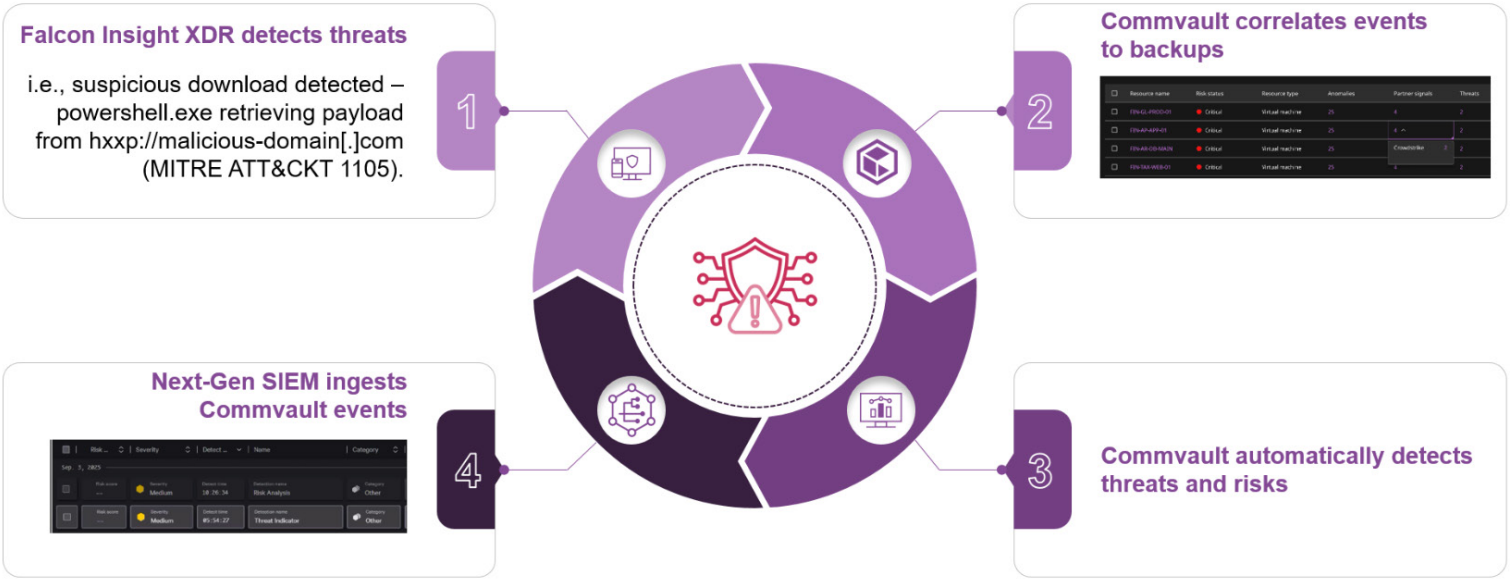
This creates a unified security ecosystem. SecOps is integrated with the cyber resilience platform, which in turn enhances SecOps with vital data context. The result is a closed loop across detection, response, and recovery that strengthens cyber defense.



SOLUTION BENEFITS

Joint CrowdStrike + Commvault customers can benefit from bi-directional signal sharing through:

- **SOC Team Upskilling:** Greater visibility and AI-enabled intelligence for faster, more informed decision-making.
- **Orchestrated Incident Response:** Powerful automation to help contain threats and accelerate remediation.
- **Accelerated, Verifiable Recovery:** Restore to a clean, isolated environment with Commvault Cleanroom and use Threat Scan capabilities to recover with confidence.



HOW IT WORKS

The integration and bi-directional signal sharing between CrowdStrike and Commvault unify detection, correlation, and response. Organizations can detect threats, understand their impact on backup data, and recover quickly and confidently.

Step 1 – Threat Detection with CrowdStrike Falcon

- The CrowdStrike Falcon platform continuously monitors production systems and detects threats in real time with its Falcon Insight XDR capabilities.

Step 2 – Correlation with Commvault Backup Assets

- Commvault extends this visibility to backup data by linking threat detections to backup resources. This provides crucial context by identifying which backup sets might be at risk and what data may be impacted.

Step 3 – Threat Scan and Risk Analysis

- Commvault performs advanced Threat Scanning and Risk Analysis on the correlated assets. This includes searching for ransomware signatures, identifying data anomalies, and flagging sensitive or high-value data at risk. This step helps verify not only that an attack occurred, but also whether the last line of defense, the backups, has been impacted.

Step 4 – Event Sharing with CrowdStrike Falcon® Next-Gen SIEM

- Commvault security events are ingested into CrowdStrike Falcon Next-Gen SIEM for incident response and forensics. This gives the SOC team a unified view, from endpoint detection with CrowdStrike to backup integrity with Commvault, enabling coordinated and effective incident response.

ABOUT COMMVAULT

Commvault (NASDAQ: CVLT) is a leader in unified resilience at enterprise scale. In a constantly evolving threat landscape, Commvault keeps customers ready by unifying data security, identity resilience, and cyber recovery, on one cloud-native, AI-enabled platform. Customers trust Commvault to conduct the fastest, most complete recoveries – not just their data, but their entire business. Purpose-built for the agentic enterprise, Commvault also enables organizations to safely embrace AI while protecting against AI-driven threats.

ABOUT CROWDSTRIKE

CrowdStrike has redefined security with an advanced cloud-native platform for protecting critical areas of risk: endpoints and cloud workloads, identity, and data. The CrowdStrike Falcon platform harnesses real-time threat intelligence and enterprise telemetry to automate threat prevention, detection, remediation, hunting, and vulnerability observability through a single, intelligent, lightweight agent.

Experience the benefits today: Request a demo **here**.

To learn more, visit **commvault.com**

commvault.com | 888.746.3849