SOLUTION BRIEF

Response Doesn't Stop at Containment:

Extend Automated SecOps Into Cyber Recovery

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)

THE CHALLENGE

Security operations have become highly automated. Detection now happens in seconds, incidents open automatically, telemetry is enriched, and containment actions can run from the same Falcon workflows security teams already use every day.

But recovery is often still the manual step. When ransomware, identity compromise, or a destructive attack hit, teams still leave the security workflow, coordinate handoffs, preserve evidence, identify trustworthy recovery points, and restore without reintroducing the threat.

That gap creates friction at the moment where speed and confidence matter most. Detection and response may be orchestrated, but the step that determines when the business comes back is still too often handled outside the flow of incident response. Security teams are left pivoting between consoles, coordinating across teams, and manually connecting investigation to recovery at precisely the moment they need the greatest speed and precision.

THE SOLUTION

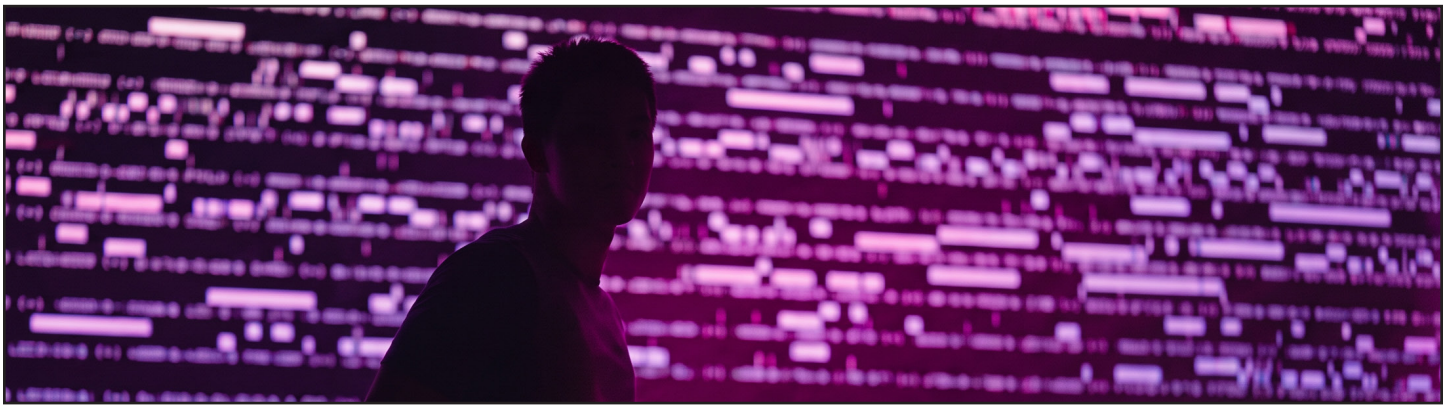
Commvault's integration with CrowdStrike Charlotte Agentic SOAR brings recovery-aware actions into the Falcon workflows security teams already use. Analysts can move from detection and containment into preservation, clean investigation, and trusted recovery without waiting on disconnected processes or manual handoffs.

The integration builds on the broader Commvault and CrowdStrike partnership:

- Falcon Insight XDR brought CrowdStrike threat intelligence into Commvault
- Falcon Next-Gen SIEM extended visibility
- Charlotte Agentic SOAR turns that shared visibility into machine-speed action across the full incident lifecycle.

WHY IT MATTERS

- **Faster incident response** – Contain threats and kick off recovery actions from the Falcon workflow, reducing tickets, delays, and coordination overhead.
- **Preserve clean recovery points** – Automatically suspend backup data-aging policies so clean recovery options remain available while the incident is still active.
- **Investigate safely in isolation** – Restore potentially compromised assets into Commvault Cleanroom™ so teams can analyze suspect systems without touching production.
- **Cleanly recover with confidence** – Use Threat Scan and recovery-aware orchestration to help validate a known-good state before business operations resume.
- **One coordinated loop** – Connect SecOps, incident response, and recovery teams so detection, investigation, response, and recovery operate together.



HOW IT WORKS

Response orchestration

1 Falcon detects a threat and triggers orchestration within Charlotte Agentic SOAR.

2 The resulting workflow can disable compromised user accounts and identity providers to help stop attackers from extending access.

3 Recovery-aware actions are launched from the same SOAR motion security teams already use for detection and response.

Recovery orchestration

1 Backup data-aging is automatically suspended to preserve clean, viable recovery points during the incident.

2 Potentially compromised assets can be restored into Commvault Cleanroom for isolated forensic analysis.

3 Teams orchestrate agentic response and recovery together, moving from detection to trusted recovery through Charlotte Agentic SOAR.

Recovery stays connected to the investigation, rather than becoming a separate handoff after containment.

AT A GLANCE

What it does	Extends CrowdStrike Charlotte Agentic SOAR machine-speed automation with cyber recovery actions during active security incidents
How it works	Falcon detects and triggers a Charlotte Agentic SOAR workflow that contains compromised identities, preserves recovery points, and orchestrates trusted recovery
How it differs from Falcon Insight XDR	XDR brought CrowdStrike threat intelligence into Commvault for visibility; Charlotte Agentic SOAR turns that visibility into machine speed action
Where investigation happens	Potentially compromised assets are restored into Commvault Cleanroom for isolated forensic analysis
Who it's for	Joint Commvault and CrowdStrike customers looking to extend security automation into cyber recovery

BUILT FOR REAL CYBER RESILIENCE WORKFLOWS

- **Ransomware or destructive attack** – contain the threat and preserve viable recovery points while the investigation is still underway
- **Identity or insider compromise** – disable affected accounts and identity providers before attackers extend access
- **Suspected breach of unknown scope** – safely analyze suspect assets in an isolated Cleanroom without disrupting production
- **Post-incident recovery** – close the delay between SOC containment and recovery-team execution as one workflow

GET STARTED

The integration between Commvault and CrowdStrike Charlotte Agentic SOAR is generally available worldwide at no additional cost for joint Commvault and CrowdStrike customers and is also available through the CrowdStrike Marketplace.

BRING RECOVERY INTO THE SECURITY WORKFLOW

Detect, contain, investigate, and recover through a coordinated Commvault and CrowdStrike workflow, so cyber recovery becomes part of response, not the step that waits after it.

Talk to your CrowdStrike or Commvault representative to get started.

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

commvault.com | 888.746.3849