SOLUTION BRIEF

Commvault + CROWDSTRIKE

Commvault Cloud integration with CrowdStrike Falcon

Accelerate cyber response and recovery with enhanced threat detection.

CHALLENGE

The modern cyber threat landscape is a dynamic and increasingly treacherous terrain, evolving at an unprecedented pace. Today's cybercriminals are sophisticated, well-resourced, and relentless, employing a diverse range of tactics that are being made increasingly smarter and more widespread due the rise of generative AI. Organizations face a barrage of potential threats daily, each one more ingenious than the last. The proliferation of cloud computing, edge devices, and the shift towards remote work have expanded the attack surface exponentially, providing cybercriminals with more entry points than ever before. Staying resilient in this modern data-everywhere environment requires vigilance, agility, and a comprehensive understanding of the latest threats.

Being cyber resilient means more than just implementing the latest security tools; it's about fostering a culture of cybersecurity awareness, investing in continuous education and training, and maintaining a proactive stance that anticipates and mitigates threats before they can cause significant damage. It requires the intelligence to quickly identify assets affected by a breach, malware, or tampering, and the ability to recover the affected data – and do so as quickly as possible, because your business depends on it. It's a challenge that requires a holistic approach, combining technology, people, and processes to build a robust and adaptable defense against the myriad threats of the modern cyber world.

Key Benefits

- **Identify threats early**
  Uncover evolving threats and suspicious activity faster. Minimize the impact of security breaches and help stop attacks from spreading.
- **Accelerate response times**
  Expedite identification of affected resources and coordinate cross-organizational response and remediation.
- **Recover clean data faster**
  Find affected systems and files, easily identify their last clean version, and recover those instances quickly wherever the business needs them.

SOLUTION

The Commvault® platform approach to cyber resilience integrates multiple layers of protection so organizations are well-equipped to secure and defend data, detect cyber threats early before they spread, and recover (and rebuild) large scale environments quickly. The Commvault Cloud platform goes beyond traditional data protection to help customers minimize risk, improve cyber readiness, and accelerate recovery and rebuild of mission critical data and applications.

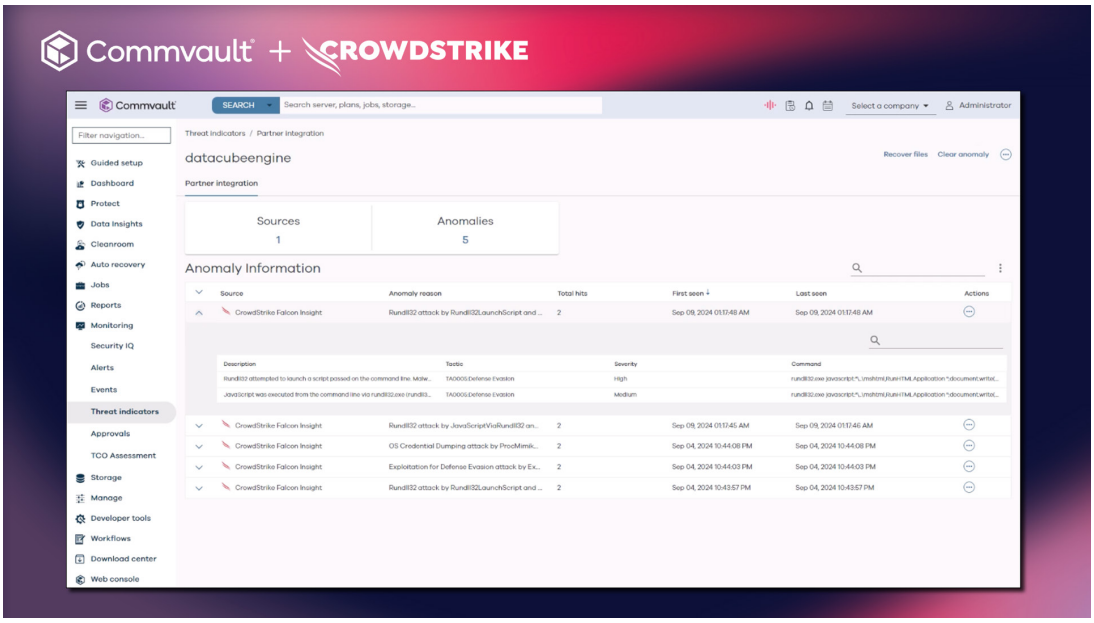
Commvault Cloud's integration with the CrowdStrike Falcon® platform adds another layer of threat intelligence to the Commvault platform, giving administrators the ability to view CrowdStrike's rich indicators of compromise (IOCs) and easily action on affected assets. This integration enables earlier detection of dangerous and evolving threats, allows for better collaboration and response across SecOps and ITOps teams, and ultimately results in faster recovery of affected data. With Commvault and CrowdStrike, IT and security teams can reduce costly downtime, minimize data loss, and enable continuous business, providing uninterrupted services and capabilities their customer base depends on them for.

BUSINESS VALUE

Use Case/Challenge	Solution	Benefits
Uncovering active threats	Add to Commvault Cloud's existing AI-assisted Threat Scan anomaly detection and threat hunting capabilities with the Falcon platform's rich security data to provide another layer of insight and added intelligence.	Threats are detected faster, affected assets are identified earlier, and remediation can begin sooner. The result is reduced risk for your organization.
Improving cyber readiness across the organization	Improve information sharing and collaboration between SecOps and ITOps. Drive better processes responding to threats. Utilize Commvault Cleanroom Recovery capabilities to test cyber recovery plans to further enhance readiness.	Better preparation and organizational response to security incidents, giving security leaders assurance and leading to better outcomes after attacks or breaches
Accelerating recovery of clean data	Through faster threat detection, remediation and recovery are accelerated. Enhanced threat intelligence from CrowdStrike helps Commvault Cloud better determine what data is "clean" (unaffected by the threat) to expedite a clean recovery.	Faster recoveries mean less downtime, less impact on daily services, and reduced financial impact.

TECHNICAL SOLUTION

This connector workflow integrates with CrowdStrike Falcon® Insight XDR to ingest endpoint detections, enriching the Commvault platform with real-time threat intelligence and anomaly detection, and empowering Commvault's backup capabilities to safeguard critical data against evolving cyber threats. You can use it to receive threat intelligence insights and view impacted servers in the Threat Indicators dashboard to drive proactive investigative actions for the clean recovery of data.



KEY CAPABILITIES

This workflow integrates the Falcon platform's detections to enrich Commvault's platform with real-time threat intelligence, empowering Commvault's backup capabilities to safeguard critical data against evolving cyber threats.

- **Monitor for suspicious activity** – gather threat intelligence and view CrowdStrike's indicators of compromise (IOCs) from Commvault's cyber resilience console.
- **Fast, easy remediation** – Protect backup assets by disabling data aging, disabling compromised users and IDP.
- **Detect threats faster** – Uses machine learning, behavioral analysis, and real-time threat updates to detect and alert to unknown cyber threats.
- **Identify clean data for recovery** – recover quickly and with confidence.

ABOUT COMMVAULT

Commvault is the gold standard in cyber resilience, leading the charge to protect the world against ransomware and other cyber threats by helping companies reduce risk, minimize downtime, and control costs. Commvault® Cloud represents decades of innovation, industry leadership, customer trust, and a deep ecosystem of partnerships. It's the only cyber resilience platform built for the modern cloud-first world, offering data security across all workloads, anywhere, combined with the rapid, enterprise-scale recovery. Commvault helps over 25,000 customers worldwide fight ransomware and achieve total resilience in face of tomorrow's threats.

ABOUT CROWDSTRIKE

CrowdStrike has redefined security with the world's most advanced cloud-native platform for protecting critical areas of risk — endpoints and cloud workloads, identity, and data.

The 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.

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