CROWDSTRIKE

CROWDSTRIKE FALCON DATA REPLICATOR (FDR)

Collect events in near real time from your endpoints and cloud workloads, identities and data, enriched by the AI-powered CrowdStrike Security Cloud

CHALLENGES

A seemingly insurmountable volume of data has become a norm in security today, and not all data is good data. Far too often, organizations ingest and retain large amounts of data across their distributed environment, overwhelming their systems and staff and decreasing efficiency. Although data volume fuels enrichment and context for effective and efficient detection and response, large amounts of irrelevant and non-contextual data or logs can slow down security efforts and create immense amounts of noise for security and IT teams to cut through. They need the right contextually rich data at the right time to derive valuable, actionable insights to help accelerate threat detection, response and prevention — all without straining their infrastructure and teams.

SOLUTION

CrowdStrike Falcon Data Replicator (FDR) delivers and enriches endpoint, cloud workload and identity data with the CrowdStrike Security Cloud and world-class artificial intelligence (AI), enabling your team to derive actionable insights to improve security operations center (SOC) performance. FDR contains near real-time data collected by the CrowdStrike Falcon® platform via its single, lightweight Falcon agent across all of your cloud workloads, identities and managed endpoints, including laptops, servers, workstations and mobile devices. The data is ingested, transformed and analyzed to address your organization's unique needs, using cloud delivery and storage mechanisms such as AWS S3 buckets and Google Cloud buckets.

FDR data is enriched with Falcon agent-collected detection and audit events, allowing your team to gain unique and detailed insights, build customizable dashboards for reporting, and enable advanced threat hunting capabilities. In addition, the data feed can be leveraged by CrowdStrike's technology partner ecosystem, allowing partners to build advanced applications and analytics that deliver greater context and extended capabilities to solve your security or compliance challenges. With enriched data delivered seamlessly by the Falcon platform, your team will have the best data, empowered by the best tools, to ensure end-to-end coverage and stop breaches.

BUSINESS VALUE

Use Case/Challenge	Solution	Benefits
Long-term retention: Gain data for long-term retention to address slow-moving attacks and compliance use cases, and easily filter data to cut through the noise.	The FDR feed is enriched by the CrowdStrike Security Cloud and world-class AI to deliver actionable and unique insights in near real time, delivering the right context for the threats in your environment. You can also customize filter options to drill down on relevant business-critical data, while cutting through the noise to aid with advanced analytics and compliance use cases.	Seamlessly draw actionable insights from the Falcon platform's rich telemetry and focus on critical data to improve the efficiency and effectiveness of your detection and response to get ahead of adversaries.
Forensic analysis and threat hunting: Empower security teams with enriched data and actionable insights to more effectively hunt for and analyze threats for faster detection and response.	FDR data can be easily filtered, consumed and leveraged by CrowdStrike's ecosystem via the CrowdStrike Store, allowing your team to address your use cases with data correlation and powerful search capabilities.	Address advanced security use cases with enhanced hunting and analysis capabilities enabled by CrowdStrike's best-of-breed ecosystem. Empower your team with interoperable tools that leverage CrowdStrike's enriched single pool of data.
Simplified implementation and deployment: Simplify operations with rapid and scalable cloud-enabled deployment that is not resource-intensive.	Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment. You gain rich security telemetry — without friction — from trillions of endpoints, workloads, identities and data for superior protection and performance, delivering immediate time-to-value.	Save time and resources in implementing and using FDR data via the Falcon platform. Leverage rich security telemetry from across your enterprise and extend it to partner solutions without any hassle or operational friction.

KEY BENEFITS

Access rich data feeds: Draw key insights with trillions of endpoint, workload, identity and data telemetry including detection and audit events

Enable advanced threat hunting: Speed up investigations with advanced security and threat hunting enriched by Falcon platform data

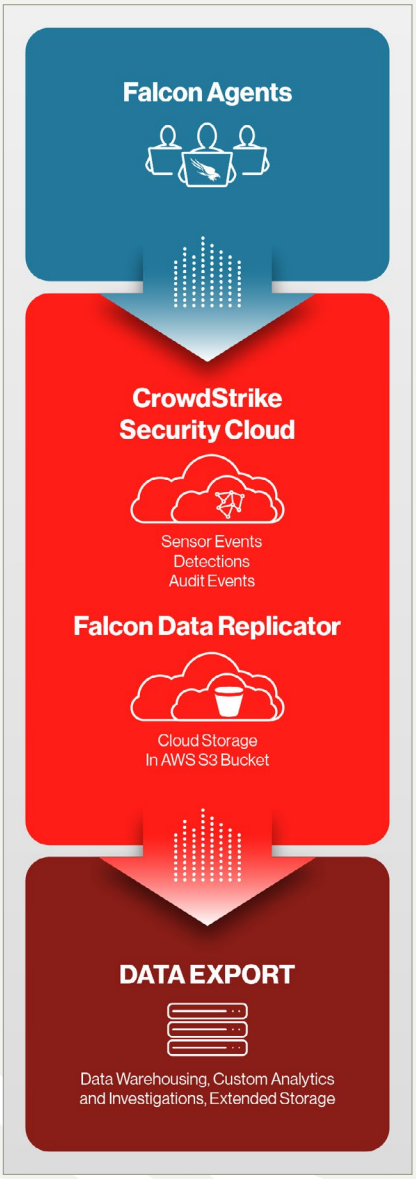
Export insights: Extract near real-time data for offline analytics and build custom dashboards for in-depth reporting

Filter data: Customize and filter the data you want to receive to meet your advanced analytics and compliance needs

Leverage the ecosystem: Enable filtered FDR data for partner integrations in the CrowdStrike Store to meet additional security and IT use cases

TECHNICAL SOLUTION

Using world-class AI, the CrowdStrike Security Cloud creates actionable data, identifies shifts in adversarial tactics and maps tradecraft in the patented CrowdStrike Threat Graph® to automatically prevent threats in real time. FDR data is available through real-time interactive searches and a robust set of open APIs that can be made available for offline analysis. CrowdStrike maintains a full, unfiltered record of data received from every endpoint for a minimum of seven days, which can be adjusted based on your organization's needs. For users who want to maintain their own archive or incorporate their security telemetry into data lakes or warehouses, FDR allows you to implement potentially unlimited storage to meet those unique data retention needs. FDR's turnkey, cloud-delivered solution enables better insights, with the highest levels of availability, with nothing to maintain, upgrade, patch or tune.



KEY CAPABILITIES

Gain rich security telemetry from trillions of endpoints, workloads, identities and data

Allow filtered FDR for partner applications and additional advanced use cases across the technology stack

Benefit from subscription flexibility to meet your unique business and security needs

Build custom dashboards and visualizations for reporting needs

ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

Start Free Trial
of Next-Gen AV

CrowdStrike: **We stop breaches.**
Learn more: **https://www.crowdstrike.com/**
Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**
Start a free trial today: **https://www.crowdstrike.com/free-trial-guide/**