DELL Technologies

Dell SafeGuard and Response

CrowdStrike Falcon® Long Term Repository™ (LTR)

Key Benefits

- Advanced threat hunting and threat analytics with extended data retention for a year or longer
- Seamlessly enriched and contextualized Falcon security telemetry across endpoints, workloads and identities for timely and actionable insights
- Low total cost of ownership with long-term retention that requires minimal storage and computing resources
- Index-free, lightning-fast historic searches and sub-second live searches with complex queries to find threats quickly
- Correlated threat intelligence leveraging Falcon IOCs for proactive threat hunting

Redefine threat hunting with enhanced threat context and data management at scale and speed

Ongoing digital transformation in modern businesses is leading to more remote workers, cloud workloads, and devices and assets connected to corporate networks. These factors impede IT and security teams from gaining full visibility and control of their end-to-end environments — and increase their organizations' attack surfaces, which adversaries continue to adapt to and exploit.

Digital transformation also leads to an increase in the amount of available data that these IT and security professionals, faced with minimal budget and resources, often struggle to retain and operationalize to effectively contextualize and prioritize potential threats.

Limited data retention makes it nearly impossible for teams to see the complete history of an attack, limiting threat context and hindering effective threat hunting and remediation. This lack of access to historical and contextual data can lead to slower time-to-detect and potentially cause security teams to miss key threat activities as they fall through visibility gaps, increasing dwell time and putting organizations at risk of a breach. With evolving modern attacks and the heightened risk of a breach, teams must unify and operationalize their IT and security data to gain the threat insights and context needed to effectively safeguard the enterprise.

Enhance Threat Hunting with Data Storage and Management at Scale

An economical way to store, manage and analyze enriched security data is essential to provide your IT and security teams the timely, contextual insights they need from across your environments to effectively detect and respond to threats. CrowdStrike Falcon® Long Term Repository™ (Falcon LTR) combines a wide variety of structured, unstructured and semi-structured data and provides access to extended data retention for a year or longer, enabling your teams to gain visibility and threat context across your growing attack surface.

Falcon LTR offers deep, contextual and faster analytics on massive amounts of log data combined with enriched security data across endpoints, workloads and identities, including the correlation of indicators of compromise (IOCs) from the CrowdStrike Falcon® platform. With powerful search and threat hunting capabilities, you can observe, analyze and act from both real-time and long-term

Learn more at www.Dell.com/endpoint-security

CROWDSTRIKE

historic data and detect potential threats faster and more accurately. Longer data retention, combined with enriched security telemetry from the Falcon platform, enables security teams with enhanced threat insights to gain visibility over attack paths to detect and respond faster. Through longer retention, contextual analytics and lightning-fast search results at any scale, you can meet your unique compliance and security needs.

Falcon LTR is cost-effective with scalable storage and advanced compression techniques that require minimal storage and computing resources, enabling you to reduce your TCO and search a year's worth of data or more. By ingesting, storing and analyzing enriched Falcon telemetry via CrowdStrike Falcon Data Replicator (FDR) alongside Falcon IOCs, security teams can proactively search and uncover hidden threats, remove advanced persistent threats (APTs) by sifting through the data to detect irregularities that might suggest potential malicious behavior, and better prioritize and address vulnerabilities before they can be weaponized. By combining the world's most advanced cloud-native security platform with long-term retention and observability for any logs or data, you get actionable insights and real-time protection.

Key Capabilities

Transform Threat Hunting and Troubleshooting

- **Longer data retention:** Because Falcon LTR keeps data for a year or longer, security teams can access more complete historical and real-time data to gain the threat context they need to more rapidly identify potential threats and conduct searches — enabling threat hunting and troubleshooting at an unprecedented speed and scale.
- **Enriched security telemetry:** By leveraging enriched data from the CrowdStrike Security Cloud — our unified, threat-centric data fabric, correlating trillions of security events per day with indicators of attack (IOAs) — your threat analytics and hunting can benefit from continuously ingested and contextualized security telemetry on more than 400 event types that can be instantly searched and cross-referenced with other data sources.
- **Correlated threat intel:** Improve your understanding of threats and better identify new attacks associated with known adversaries by enriching your existing security data with real-world threat context from the Falcon platform's threat intelligence feed — including Falcon IOCs.

Operationalize Security Data with Scalable Storage and Management

- **Cost-effective scalable storage**: Get all necessary storage and compute resources for fast and efficient interactions, enabling you to scale with zero effort. With scalable storage and advanced compression techniques, you can cost-effectively store and manage Falcon data for a year or more.
- **Fast and custom search**: Access a feature-rich query language and an index-free architecture with lightning-fast historic searches and sub-second live searches, allowing you to get immediate answers about your Falcon security data for actionable insights.
- **Single interface**: Seamlessly collect, analyze and gain immediate access to your distributed data in one place to provide a single comprehensive view of your environment that provides more meaningful context for threat hunting tasks.

Enhance Visibility and Context

- **Real-time and historical data**: Gain a wealth of real-time and historical data that enables complete and accurate threat investigation and analysis, including insights into behavior, helping you achieve compliance and gain complete visibility over any attack path or vulnerability.
- **Unified data types**: Easily combine and search structured, unstructured and semi-structured data across endpoints, workloads and identities for holistic visibility of your attack surface.
- **Custom alerts and dashboards**: Enable custom alerts and dashboards for events that matter most to you based on streaming data in real time, enabling faster detection and investigation of critical threats at scale.

Contact your dedicated Dell Endpoint Security Specialist today at endpointsecurity@dell.com, for more information about the Dell solutions to help improve your security posture

Learn more at www.Dell.com/endpoint-security