CROWDSTRIKE

CrowdStrike Products
Data Sheet

Falcon Search Retention

Cost-effectively store your data for months or years to uncover hidden threats

A lack of long-term storage creates dangerous blind spots

Rising data volumes and exorbitant logging costs are forcing security teams to make tough trade-offs to stay on budget. Faced with painfully slow SIEM tools and complex data export and import processes, many teams simply forgo long-term storage of essential data, such as endpoint, identity and cloud telemetry.

To uncover threats, teams need a vast amount of historical, context-rich data as well as a scalable, intelligent logging platform to quickly search for indicators of attack. Unfortunately, insufficient data retention makes it nearly impossible for teams to identify the root cause and scope of an attack, hindering effective analysis and remediation. As adversaries become stealthier, your team needs a cost-effective and scalable way to store your security data long term to fuel AI-led investigation and response.

Hunt down and stop threats with full visibility and context

CrowdStrike Falcon® Search Retention lets you amplify the power of the AI-native CrowdStrike Falcon® platform by retaining critical endpoint, identity and cloud data for months or years. Your analysts and threat hunters can go back in time and discover hidden threats lurking in data from long ago to root out adversaries and safeguard your enterprise. Your team can take advantage of the Falcon platform's blazing-fast search, workflow automation and AI-powered analyst-assist features to accelerate investigations.

Harnessing the rich, contextual data gathered by the Falcon agent, Falcon Search Retention provides deep insights into user and device activity, including process information, registry updates, network communications, threat detections and much more. Encompassing over 600 event types, Falcon platform data provides extensive details for threat hunting and investigations. Your team can run complex queries using regular expressions, aggregations and joins to uncover advanced threats and risky behavior.

Falcon Search Retention not only offers an affordable, turnkey way to extend the storage of your Falcon platform data, it lays the foundation for next-gen SIEM. Once you've started retaining Falcon endpoint, identity and cloud data long term, you can easily bring in additional data sources to achieve 360-degree visibility across your entire digital estate.

Key benefits

Find threats faster with ultra high-speed search that's up to 150x faster than legacy SIEMs

Store petabytes of Falcon platform data for months or years while avoiding the cumbersome setup and ingestion bottlenecks of siloed legacy SIEM tools

Uplevel SOC analysts by enriching data with world-class threat intelligence

Reduce response times, improve productivity and say goodbye to tedious tasks with workflow automation powered by native SOAR capabilities

Slash security and compliance costs by simply extending the retention of your Falcon platform data

Key capabilities

Turbocharge threat hunting with speed and intelligence

- **Flexible, blazing-fast search:** Uncover threats instantly with an index-free architecture for exceptionally fast search performance. A feature-rich query language lets you scan all events swiftly and easily with free text search or construct complex queries with regular expressions.
- **Correlated threat intelligence:** Quickly assess threats and better identify new attacks associated with known adversaries by enriching your existing security data with real-world threat context, including indicators of compromise (IOCs) from the industry-leading CrowdStrike Falcon Adversary Intelligence module.
- **Native security orchestration automation and response (SOAR) capabilities to unearth threats and enrich data:** Speed up threat hunting and investigations with workflow automation on your side. More than 125 workflow actions let you fully eradicate threats and free up your team to focus on higher-order operations.

Achieve boundless visibility to accelerate incident response

- **Real-time and historical data in one place:** Get a complete view of endpoint, user and cloud activity by searching live and historical data for accurate threat investigations. Your analysts can dig deeper to track adversaries' every move and reveal hidden threats.
- **Rich, contextualized data:** Simplify threat analysis with comprehensive endpoint telemetry that includes user IDs, processes, hashes and more. Longer data retention, combined with enriched telemetry, gives your team the context and attribution details it needs to quickly investigate attacks.
- **Predefined and customizable dashboards:** Monitor security status in real time and document your security posture with graphical dashboards that display the events that matter most to you. Falcon Search Retention allows you to identify trends over time and visualize past activity for investigations and forensics analysis.

Easily scale your SOC for security and compliance

- **Petabyte-scale data storage:** Analyze and retain massive volumes of log data for threat analysis and compliance. Falcon Search Retention lets you scale your security operations with zero effort and cost-effectively store Falcon platform data for as long as you need it.
- **Affordable, long-term data retention:** Simply extend the storage of Falcon platform data for months or years with a license upgrade and avoid costly third-party data lakes and legacy SIEMs. A cloud-native architecture eliminates the hassle of on-premises infrastructure, while hot storage access ensures your data is always at your fingertips for swift triage and analysis.
- **The foundation for next-gen SIEM:** Maximize security outcomes by breaking down silos and consolidating all of your data — including alerts and high-volume telemetry — in one unified platform with CrowdStrike Falcon® Next-Gen SIEM.

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.

CrowdStrike: We stop breaches.

Request a Free Demo →