Data Sheet

Falcon LogScale

All log data. Real-time insights. All in one place.

Challenges:
Traditional logging can't keep pace with data growth

Log management platforms provide the visibility you need to uncover and investigate attacks, avoid outages and optimize application performance. But to realize these benefits, your log management platform must deliver real-time alerting, high-speed search and the sheer scale to ingest all of your logs.

Unfortunately, as log volumes increase, you may be struggling to collect and quickly search across your data. Legacy log management platforms simply make it cost-prohibitive to log high-volume telemetry. Furthermore, these platforms are index-based, meaning as data volumes rise, the size of the indexes grows, and search queries stall — making it harder to track down an adversary during a breach or discover the source of an outage.

DevOps, SecOps and ITOps teams faced with limited budgets and resources are forced to make tradeoffs on which logs to collect and for how long. As a result, some logs are inevitably left out, creating blind spots into the health and security posture of digital assets. The consequences? Slower investigations and increased risk of attack.

Solution:
Log everything in real time at petabyte scale

Falcon LogScale is a modern log management platform that lets you collect logs at petabyte scale and rapidly access live data with sub-second latency. Its blazing-fast search, real-time alerting and customizable dashboards allow you to retain data as long as you need for compliance, threat hunting and historical investigations.

Through a unique index-free architecture and advanced compression technology, Falcon LogScale minimizes the computing and storage resources required to ingest and manage data while delivering the power and speed your team needs to stop threats.

With Falcon LogScale, you can log everything to answer anything, while cutting log management costs by **up to 80%** compared to alternative solutions. Its vast scale and affordable price let you avoid making tough trade-offs between cost, how much data you can collect and how long you can store it — because with Falcon LogScale, you can retain petabytes of data for months or years.

Key Benefits

Full visibility across distributed systems to eliminate the need to make cost-based concessions on which logs to ingest and retain

Streaming ingestion at any scale, with a benchmark of 1+ PB per day with live queries

Index-free architecture that supports blazing-fast search and sudden bursts in data ingestion

Industry-leading data compression rate and cloud-storage options to ingest and manage more data with ease

Flexible and scalable deployment for any configuration: on-premises, cloud or hybrid

Key Capabilities

Modern Log Management for All of Your Data

- **Log everything:** With Falcon LogScale, you can store, analyze and retain massive volumes of streaming log data from a wide array of sources at petabyte scale.

- **Centralize all of your data:** Through a unique index-free architecture and advanced compression technology designed to minimize hardware requirements, you can break down silos and consolidate all high-volume telemetry — including security, IT and DevOps data — in one place.

- **Retain data for months or years:** Because Falcon LogScale offers cost-effective long-term storage, you can access comprehensive historical and real-time telemetry for threat hunting and troubleshooting while maintaining unprecedented speed and scale.

Instant Search Results

- **Quickly search all of your data:** Falcon LogScale provides real-time streaming and index-free searching to help your DevOps, ITOps and SecOps teams receive immediate answers to their most complex queries.

- **Drive continuous improvement:** Understand the root cause of issues and recover more quickly from incidents by searching across as many as 3 billion records in under a second.

- **Aggregate, search and visualize live data:** Alert on attacks in real time and query data with sub-second latency to quickly uncover security threats and performance issues.

Low Total Cost of Ownership

- **Reduce infrastructure and licensing expenses:** Falcon LogScale offers affordable cloud, self-hosted and hybrid licensing options, as well as decreases infrastructure costs because it compresses data by 6x to 80x and does not store ever-increasing database indexes.

- **Simplify deployment and reduce time-to-value with CrowdStream:** You can quickly onboard, enrich, normalize and filter data with CrowdStream powered by Cribl observability pipelining technology. CrowdStream, available at no additional cost for the first 10GB of streaming data, provides an elegant and cost-effective way to get data into Falcon LogScale to greatly accelerate the adoption of log management.

- **Maximize return on investment:** According to a Forrester Consulting Total Economic Impact™ study, Falcon LogScale provides a 210% ROI after three years.

[1]Outcomes based on real Business Value Assessments for individual customers.

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.**

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Start a Free Trial