CrowdStrike White Paper

CROWDSTRIKE

LOG EVERYTHING TO ANSWER ANYTHING IN REAL TIME

How streaming observability from Falcon LogScale empowers organizations to drive performance and stop breaches

INTRODUCTION

Every minute of the day, the systems within your IT infrastructure generate event-based data that is critical to understanding the performance and health of your systems. When you can aggregate, manage and explore all of that information, you can optimize system performance, identify technical issues, improve resource management, strengthen security and improve compliance.

Today's organizations need a modern log management technology that collects and aggregates streaming log data from a variety of different sources in real time. Falcon LogScale (formerly known as Humio) gives DevOps, ITOps and SecOps professionals the complete observability they need to prevent, detect and resolve their most complex security and infrastructure incidents. And Falcon LogScale does this faster and at a fraction of the cost compared to traditional log management solutions.

Falcon LogScale gives users:

- Complete system observability across distributed systems that eliminates the need to make cost-based concessions on which log files to include in the system
- Streaming ingestion at any scale, with a benchmark of 1+PB per day with live queries
- Index-free architecture that handles massive data volumes and powers blazing fast search
- Industry-leading data compression and cloud-storage options to manage more data in your log management processes
- Flexible and scalable deployment for any configuration — on premises, cloud or hybrid
- Faster implementation, extension and maintenance than legacy solutions
- Technology that augments and extends existing enterprise investments in IT monitoring and observability
- Industry-leading TCO through OpEx and CapEx reduction
- Operational cost is one-fourth of the cost of legacy log management vendors

WHY MODERN LOG MANAGEMENT?

Today's IT leaders are responsible for delivering business results. They need to stop system outages, protect their organization from attacks and ensure optimal performance across all workloads in their infrastructure. DevOps, ITOps and SecOps teams need multifaceted data — event data, logs, erroneous calls, traces, telemetry data, pipeline feedback and more — to understand and manage their environment. On top of that, they need to accomplish these feats while balancing OpEx and CapEx.

What organizations often lack is true observability. Logs, a critical component of a modern data fabric, are fundamental for diagnosing system health and launching investigations. But IT teams experienced with traditional log management solutions know the challenges of managing logs from distributed and legacy systems. These can include:

- Exorbitant costs associated with logging high data volumes
- Slow search speeds that hamper investigations

Data is growing exponentially, and traditional log management solutions lack the technology or accessibility required to meet the needs of modern IT. Legacy solutions treat logging like a general-purpose database by organizing and searching datasets using outdated indexing techniques. This consumes excessive CPU and memory resources, which adds hardware expenses. It also introduces delays in both ingestion and search, slowing the time it takes to get results, inhibiting investigations and creating additional risk and cost.

Most organizations can't afford to gather and retain log data from all their networking gear, security products and other IT systems to give them a holistic view. Consequently, they must limit the types of log records collected or periodically age-out log data. These decisions can leave IT teams in the dark. By not logging everything, data gaps make it difficult to troubleshoot system performance problems, conduct thorough investigations and pinpoint application issues.

IS IT TIME TO MODERNIZE YOUR LOG MANAGEMENT STRATEGY?

If you experience any of the following pain points with your current log management system, then it's time to consider a modern solution.

- The amount of data retention is limited by license restrictions or excessive hardware requirements
- Deployment options are limited to on-premises or cloud deployments
- Indexing requirements bloat storage
- Data storage costs exceed your budget
- There's a delay between data compilation and the ability to search the data
- Data is only available after it's indexed and written to disk
- You can't run searches on both streaming live-tail data and retained historical data

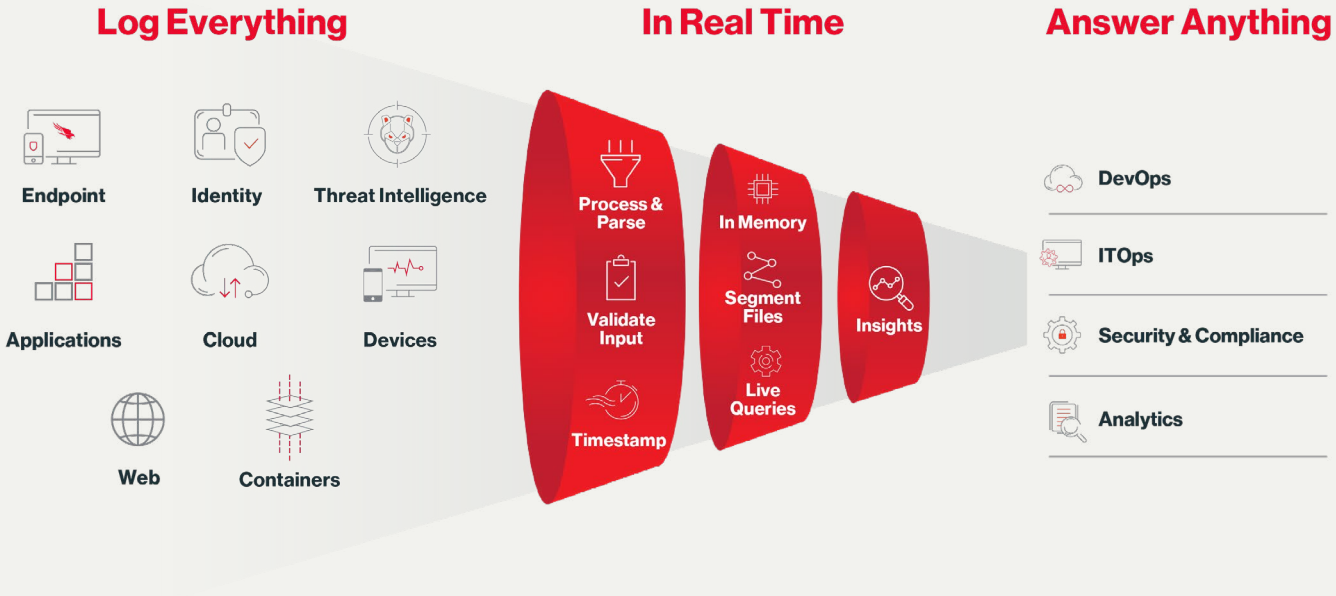
LOG EVERYTHING TO ANSWER ANYTHING

Without logs, IT teams are blind. That's why it's important for organizations to have access to all their log data in a solution that supports instant search and scalability. With Falcon LogScale, businesses aren't forced to make difficult decisions about which data to log and how long to retain it.

Falcon LogScale provides live observability with sub-second latency, index-free search for unmatched speed and advanced data compression for more cost-effective storage and management of log data. By ingesting all log data available, then making it available to search in near real time, Falcon LogScale gives IT organizations an advantage. Now, DevOps, ITOps and SecOps teams get the insight they need to truly understand their IT environment and make better decisions from that data. And through the Falcon LogScale architecture, you can accomplish all of this — 1+PB of data storage per day and 30 million events per second — at 20-30% of the total cost of a traditional log management system.

WHAT MAKES FALCON LOGSCALE UNIQUE?

- Powerful, intuitive technology and an index-free architecture
- Modern architecture to optimize storage and search capabilities
- Industry-leading total cost of ownership (TCO)
- Real-time streaming and instant search



POWERFUL, INTUITIVE TECHNOLOGY AND AN INDEX-FREE ARCHITECTURE

Modern infrastructures generate large amounts of structured, semi-structured and unstructured log data. Many enterprises already collect, aggregate and correlate tens of gigabytes to hundreds of terabytes of logs daily. Due to the sheer amount of this data, IT teams face constant challenges around effectively using this data.

Falcon LogScale helps you gain valuable insights with a powerful, flexible and intuitive technology that delivers live observability across distributed systems. The technology aggregates streaming data in real time, with hybrid options that allow you to choose where the ingested data resides. Falcon LogScale's innovative index-free architecture resolves data storage challenges by compressing data by 6-80x.

With Falcon LogScale, you can:

- Aggregate, ingest and analyze massive volumes of streaming log data from a wide array of sources
- Increase data fidelity and cardinality by storing data in a central location, which enables system-wide analysis to identify correlated events
- Efficiently query log data with sub-second latency, making it easier and more cost effective to manage data at scale
- Achieve industry-leading data compression rates with minimal strain on computation resources
- Perform full-fidelity investigations and confidently uncover the full extent of cyberattacks
- Create configurable, shared dashboards that make it easy for IT teams to visualize and analyze complex systems
- Examine both application-layer data and infrastructure-level information for complete observability across all microservices
- Collate events both upstream and downstream to gain insights and prevent issues

By logging everything, Falcon LogScale gives you the complete visibility needed to detect and respond to any issue in real time — all at a fraction of the cost of traditional log management solutions.

MODERN ARCHITECTURE TO OPTIMIZE STORAGE AND SEARCH CAPABILITIES

With Falcon LogScale, you don't have to choose which data to log. Falcon LogScale logs everything — unstructured, semi-structured and structured data — in real time to give IT teams everything they need to resolve incidents. Through a flexible and intuitive technology that delivers live observability, Falcon LogScale aggregates and visualize streaming data with hybrid options to enable users to choose where ingested data resides.

To meet these challenges, Falcon LogScale engineers delivered high-performance ingest capabilities that incorporate both high-velocity and low-velocity data sources. The goal was to make it simple to look at logs, begin to ask questions and dig deeper by searching for errors or filtering by certain parameters.

To make this possible, Falcon LogScale used these principles:

- Create an easy way to ingest and manage massive amounts of logs and troubleshoot with an easy-to-use query language
- Build a system that makes it cost effective to retain log data for future reference and allow users to absorb large spikes in incoming data
- Provide configurable, shared dashboards that make it easy for teams to visualize data, carry out investigations and collaborate
- Deliver interactive ways for users to discover and explore their data.
- Keep everything simple yet powerful

A composite organization who invested in LogScale's centralized log management solution can potentially achieve a **210% return** on investment (ROI) and **generate $9.88 million** in total benefits across a three-year period.

SOURCE: Forrester Consulting, **The Total Economic Impact™ Of CrowdStrike Falcon LogScale** commissioned by CrowdStrike.

INDUSTRY-LEADING TOTAL COST OF OWNERSHIP (TCO)

At Falcon LogScale, the focus goes beyond delivering a fast and efficient log management technology. Falcon LogScale also offers the lowest TCO in the industry. As a modern log management technology, Falcon LogScale is purpose-built in a way that makes it cost effective and highly efficient to collect and search all log data and do so at scale, in real time.

Falcon LogScale's Unlimited Plans deliver predictable log management costs. No matter how much data you collect and store, the cost of the license remains the same. There is no penalty for collecting more data in the system. Organizations have the freedom to collect all the data they want to collect — even if they want to log everything. With Falcon LogScale, your log management strategy can be based on your business objectives and service-level agreements, not on the licensing constraints of your log management technology.

REAL-TIME STREAMING AND INSTANT SEARCH

Because users rely on Falcon LogScale to run searches and explore data quickly, Falcon LogScale optimizes data ingestion, retention, compression and storage to take advantage of today's modern hardware.

Streaming data queries happen almost instantly by removing the complex indexes that often slow investigations. To search streaming and historical data quickly, Falcon LogScale uses optimized brute-force searching.

Here's how it works:

- Instead of searching your entire database, Falcon LogScale uses time and metadata selection to reduce the problem space.
- Falcon LogScale further speeds up searches by using principles of mechanical sympathy to decrease processing times, compress data and pull it from cached memory whenever possible.
- An optimized search with Falcon LogScale can run at 30-40x the speed of a regular search, enabling IT teams to find insights, resolve incidents and boost performance.

Furthermore, two areas that traditionally hinder large-scale data processing are storage and processing. By leveraging Kafka, Falcon LogScale addresses both of these drawbacks by processing data in a compressed form. This allows you to keep data in memory longer, reduce data transfer loads, protect against crashes and facilitate high-speed data processing.

"We were able to maintain the same cost structure as our ELK stack and improve retention from 7 days to 90 days. Ingestion went from 15 minutes to near real time."

Steven Gall, *VP of Engineering M1 Finance*

ECOSYSTEM AND MARKETPLACE

To increase interoperability and value for customers, Falcon LogScale continues to expand its ecosystem through technology partners and integrations.

Highlights include:

STEP 1: Ingest integrations, including AWS, Corelight, Google, Mimecast, ServiceNow, Proofpoint, Windows Logs and ZScaler. Use case: Provide an easy method to ingest data from these partners into Falcon LogScale and a package of pre-built parsers, dashboards and queries available through the Falcon LogScale Marketplace.

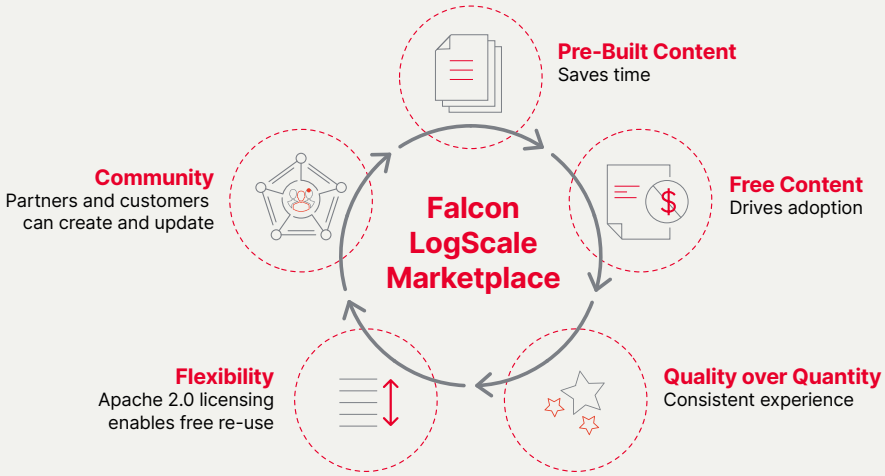
STEP 2: Platform partners, including Grafana, Instana, Kafka, Cribl and SOC Prime. Use case: Enables customers to use Falcon LogScale in conjunction with other key technology investments to deliver new possibilities and ease of management.

STEP 3: Alert and action integrations, including Tines, PagerDuty, Slack, OpsGenie and Splunk OnCall (formerly Victofkar Ops). Use case: enable customers to integrate LogScale with their chosen ticketing, SOAR and response technologies. These integrations allow for detections and alerts from Falcon LogScale to be integrated into existing workflows and processes to deliver efficient response and remediation operations.

As a result of these partnerships, you can access unique capabilities for your specific use case. These integrations are made available through platforms, software applications and open-source products that can enhance your unique scenario.

Falcon LogScale Marketplace also provides a variety of packages that give convenient ways to get more from your data. Falcon LogScale Marketplace provides a central location of packages directly available for installation within your Falcon LogScale instance. Marketplace packages can be contributed by Falcon LogScale, external companies or the community.

Since each customer has unique requirements, Falcon LogScale Marketplace gives you access to content that is ready to be recycled and freely adapted. To do so, all content is provided under an Apache 2.0 license, ensuring users don't infringe upon patents by using the packages.



WHY FALCON LOGSCALE COMMUNITY EDITION?

- Ingest up to 16GB per day
- 7-day retention
- No credit card required
- Ongoing access with no trial period
- Index-free logging, real-time alerts and live dashboards
- Access Falcon LogScale's marketplace and packages, including guides to build new packages
- Learn and collaborate with an active community
- Sample data included so users can explore improved threat hunting capabilities at speed

FALCON LOGSCALE COMMUNITY EDITION

Falcon LogScale Community Edition is a free offering that delivers the power of Falcon LogScale's streaming observability with 16GB of data ingestion per day for up to seven days of retention. With Falcon LogScale Community Edition, Falcon LogScale provides the most powerful capabilities needed for modern observability in a format that allows you to test the technology within your infrastructure. This is the largest no-cost data ingestion offering of any log management offering.

With Falcon LogScale Community Edition, users can access Falcon LogScale's modern architecture, including data streaming, index-free search and advanced compression technology. With this offering, users can understand how Falcon LogScale helps DevOps, ITOps and SecOps professionals break free from the constraints of traditional log management solutions.

The entire observability community can now use Falcon LogScale Community Edition at no cost to empower streaming observability, improve the quality and reliability of systems in real time, and proactively prepare for the unknown. This helps teams prevent, recover from and quickly understand the root cause of incidents. With Falcon LogScale Community Edition, users have the real-time insights needed to enable enhanced performance as well as increased speed to delivery.

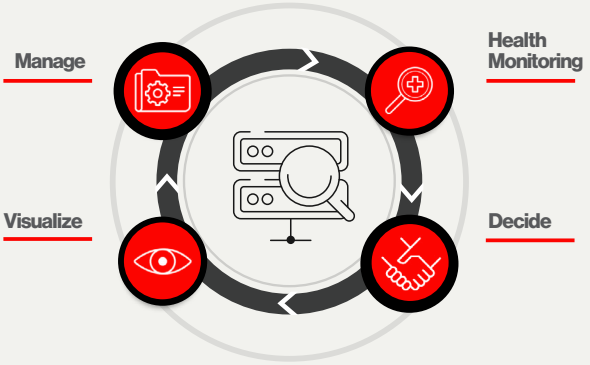
THE FALCON LOGSCALE ECOSYSTEM

CrowdStrike is driving the convergence of security and observability with a centralized log management strategy that focuses on deriving insights from log data — and helping organizations easily access, ingest, store and analyze this critical and always-growing amount of information.

Falcon LogScale is available as a standalone module to ingest, search, transform and retain all of your log data. Built using a unique index-free architecture and advanced compression technology that minimizes hardware requirements, Falcon LogScale allows DevOps, ITOps and SecOps teams to aggregate, correlate and search live log data with sub-second latency.

For companies that want to outsource their log management and observability functions, **Falcon Complete LogScale** is a fully managed service offering that combines the effectiveness of Falcon LogScale with CrowdStrike's dedicated team of service professionals. Falcon Complete LogScale delivers highly personalized log management expertise to help you answer any query and gain valuable insights from your logs in real time.

CrowdStrike's elite team of observability experts provides deep and coninuous analysis for key business outcomes via Falcon Complete LogScale.



Business Value

- Achieve critical data visibility
- Enhance observability at scale
- Gain expertise
- Reduce cost
- Improve decision making
- Compliance

Through scalable storage that minimizes the size and cost of retention, **Falcon Long Term Repository** allows all Falcon customers to store their endpoint detection and response (EDR) data for as long as they want. Alone, this capability helps companies meet compliance requirements and perform historical investigations on Falcon telemetry. When combined with Falcon LogScale, Falcon EDR data can be correlated with other data sources to become a force multiplier for real-time and historic threat hunts.

Finally, the CrowdStrike Data Fabric provides an underlying set of capabilities across the Falcon platform. Rather than a module licensed separately, CrowdStrike Data Fabric underpins Falcon platform technology to enhance observability of your IT assets. The innovative data fabric works by ingesting distributed, third-party log data into the CrowdStrike Security Cloud and enriching it to enhance your threat hunting abilities.

WANT TO LEARN MORE?

Learn more about Falcon LogScale: **www.crowdstrike.com/products/observability/falcon-logscale**

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.**

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/**