CROWDSTRIKE

WHY FALCON LONG TERM REPOSITORY?

Cost-effectively store your CrowdStrike Falcon® platform data for months or years to support security and compliance requirements

As a CrowdStrike customer, Falcon® Long Term Repository (Falcon LTR) is the ideal way to store your Falcon platform data, offering unbeatable scale, convenience and affordability. Supporting blazing-fast search, real-time alerting and a broad set of dashboards, Falcon LTR lets you retain your data as long as you need for compliance, threat hunting, investigations and more.

LONG-TERM DATA RETENTION HAS NEVER BEEN MORE IMPORTANT

Adversaries use a variety of underhanded techniques to infiltrate organizations, blend in with legitimate users and elude detection, resulting in a mean-time-to-identify (MTTI) breaches of 207 days[1] in 2022. Because threat actors can operate under the radar and dwell in networks for months, your security team must be able to search for signs of intrusions in past data.

On top of this danger, thousands of new vulnerabilities are disclosed every year, sometimes weeks after they have been exploited in the wild. When the next Log4Shell attack strikes, your IT and security teams will need to locate vulnerable software in your environment and hunt for signs of compromise — not just in current data, but logs dating back to when the attacks were first observed.

Whether you're facing malicious insider activity, supply chain attacks, zero-day exploits or low and slow threats, you should store security data, including endpoint events, long term to identify the impact and origin of attacks. Without this information, your incident responders will struggle to fully eradicate threats or prevent similar attacks in the future.

Unfortunately, the cost of logging endpoint events using legacy log management and SIEM platforms can quickly escalate. Many of these platforms are index-based, meaning as data volumes rise, the size of the indexes grow and search queries stall — making it harder to track down an adversary during a breach or alert on threats in real time.

What Customers Say

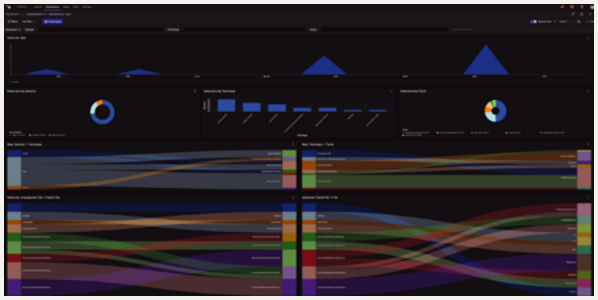
"With Falcon LTR, we saved $150,000 in the first year. And the ability to save our Falcon data for an extended time period is critical. When we detect an IOC, we can go back in time and analyze the entire attack chain to accelerate investigations and pinpoint issues more quickly."

Tom Sipes
Director of IT Security and Compliance, Tuesday Morning

1 Cost of a Data Breach Report, Ponemon and IBM, 2022

GET SCALABLE, POWERFUL LOGGING AND BLAZING-FAST SEARCH WITH FALCON LTR

Built on the powerful CrowdStrike Falcon® LogScale technology, Falcon LTR lets you cost-effectively store Falcon data long term, so you can easily explore critical log information, eliminate blind spots and find the root cause of any incident. With Falcon LTR, you can store, analyze and retain your Falcon platform data at petabyte scale and search across your data at exceptionally fast speed to uncover threats faster.

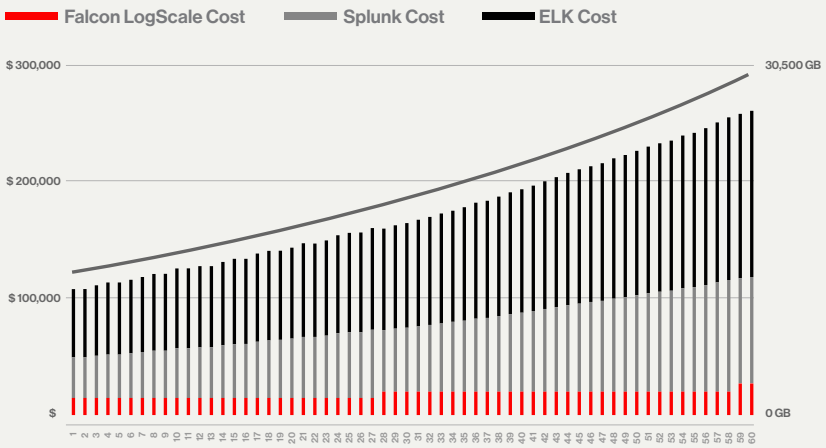


EXTEND STORAGE TO THIRD-PARTY DATA

After you've experienced the power and speed of Falcon LTR, you might be eager to expand data collection to additional sources. Falcon LogScale makes it a snap to centralize, analyze and access all your log data in one place without worrying about scale or performance. You can let hundreds of users simultaneously access custom dashboards, empower analysts to execute as many queries as they need while getting instant results, and detect threats when they occur with real-time alerting.

With Falcon LTR and Falcon LogScale, you can drastically reduce your logging expenses and avoid the exorbitant licensing and hardware fees of legacy vendors. The Falcon LogScale infrastructure savings estimator shows that switching to Falcon LTR and Falcon LogScale can cut your log management costs by up to 80% compared to alternative solutions.

Total Cost of Ownership of Falcon LogScale vs. Splunk and ELK



Savings over time with 10TB/day ingestion and 25% growth rate

COMPLIANCE

Government and industry regulations require many organizations to store their security data for 365 days or longer. Falcon LTR provides an affordable, high-scale logging platform to store data for compliance. Falcon LTR lets you retain data for as long as you need without overloading your SIEM with endpoint telemetry. And when it comes to audits, Falcon LTR's flexible query language, sub-second searches and customizable dashboards make it easy to demonstrate compliance.

THREAT HUNTING

Falcon telemetry is a rich data source to hunt for threats that might have occurred months ago. Threat hunting helps your team proactively investigate potential breaches and figure out how to prevent future threats. And since no single data source can tell the full story of a possible breach, you can easily bring in third-party data with Falcon LogScale, providing even more context and visibility for threat hunts — all from one user interface.

HISTORICAL INVESTIGATIONS

From software vulnerabilities and supply chain attacks to persistent espionage-related threats and insider abuse, today's threat landscape may force your security analysts to conduct historical investigations. Whether you use the Falcon platform to protect endpoints, workloads, identities, or all three, Falcon LTR extends visibility into those areas for faster and more complete investigations into long-term threats.

Ready for the double-click?

This whitepaper elaborates on the technical details and business value of Falcon LTR.