DATA SHEET

DataSet as a Data Lake

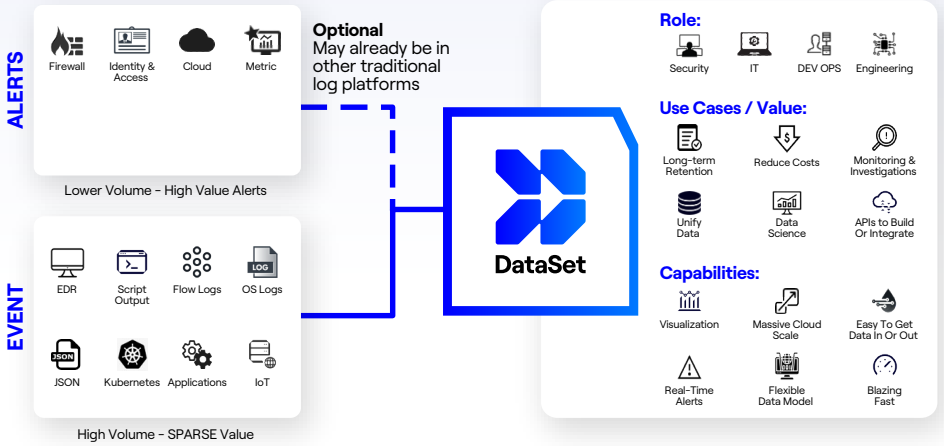
Modern cloud data platform built to maximize the value of data. Gain increased visibility, real-time alerting, and keep your data for as long as needed for investigations and compliance.

Data is used in many ways across an organization. Security teams need visibility into many different sources and types of data in order to detect or investigate threats, including IT, DevOps and Engineering data. Many organizations struggle to have all the data they need to detect and see all threats and security teams and solutions often become isolated. A visibility gap occurs when an incident happens and administrators lack the contextual data or must go to other places to try and find the answers.

Security Information and Event Management (SIEM) technologies are designed to handle specific security incidents, not high-volume data. To control costs, and not overwhelm SIEM with high-scale data, security organizations only capture critical security alerts in the SIEM and often lose important visibility. DataSet is the same platform used to deliver the Singularity XDR product and is built to scale to handle petabytes of data, with blazing fast search and instant visibility with an industry leading low total cost of ownership. Unify your EDR data with your other security telemetry into DataSet.

Stop Throwing Away Valuable Data

Many organizations have to make tough decisions regarding the data they are capturing in their SIEM, Log Management, or other data stores. Usually, these decisions are being driven by cost, scalability, or limits on supported data types and sources versus business value. DataSet leverages a modern cloud architecture that allows you to keep all of your data, for as long as you need it, without breaking the bank. Use DataSet as a critical foundation of your security stack or to augment your SIEM by sending only high-volume data, while keeping your SIEM clean with high-value security alerts. DataSet takes a scalable approach to data management, which reduces the total cost of ownership and delivers positive ROI for most customers in just weeks—even when compared to open source technologies.



DataSet as data lake to instantly get value from all your data.

Key Benefits

- Collect, parse, search all of your organization's event data
- Powerful search interface for quickly digging through data to get answers quickly
- 96% of Queries return in under a second - up to 60x faster than the competition
- Index-less, columnar data store scales to any size environment
- Fully managed SaaS offering with 99.99% uptime - no need to patch or scale data stores or indexes
- Real-Time alerts instantly notify you when there is an issue
- Parsers built on-demand as part of the service
- Leverage our cloud or keep the data in your own S3 bucket
- Hindsight Pay-per-query models that enable affordable, long-term retention for security or compliance
- Real-time ingest and live streaming views of event data
- Rich set of APIs for seamless integration and access to your data
- Build dashboards and graphs for any data
- Trust a security company to secure your data

Instant Answers to Your Questions

Data is a critical part of your monitoring, troubleshooting, and security program. When an incident occurs, answers are needed quickly. With DataSet, you get your answers almost instantly. Taking advantage of an elastic cloud-based query engine, most queries return in a second or less. Data is ingested and available in near-real-time with an index-less architecture. Users can even view and search their events with a live view of data as it flows into the platform.

Easy Analytics

DataSet also offers a strong PowerQuery interface that allows customers to analyze their data to answer difficult questions across a large data set easily.PowerQueries provide a rich set of commands for transforming and manipulating data. You can filter, perform computations, extract new fields from your events, and create groupings and statistical summaries on the fly. You can freely mix and match commands, to create sophisticated analyses and find the answers you need.

It also provides additional analytics tools for graphing data and calculating mathematical functions (Mean, median, 95th percentile, etc.). Easily turn these queries into dashboards to gain instant insights into your event data.

Easily generate Analytics off any query

Maximum Scalability

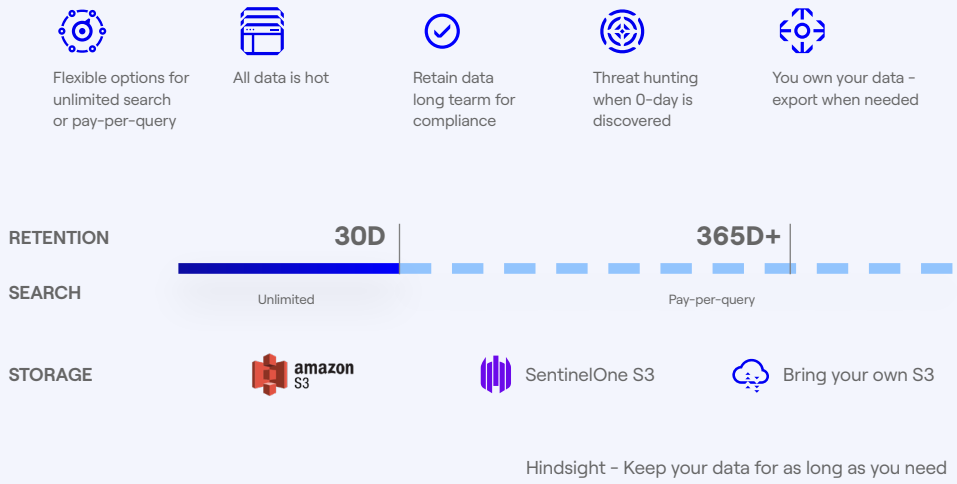
DataSet is designed to seamlessly scale to any amount of data, even hundreds of terabytes per day. Delivered as a SaaS solution with true multi-tenancy it automatically scales to ensure all of your data is captured and available in real-time or for a long time. Leverage the same data platform used by SentinelOne to handle petabytes of data and trillions of events per day. Never worry about having to scale your data platform - SentinelOne has you covered. Combine dynamic ingestion, compute elasticity, and the scalability of cloud storage to maximize performance and minimize cost without rebalancing nodes, managing storage, or re-allocating resources.

Hindsight: Cost-Effective Retention for Compliance and Historical Investigations

Retention of log data is a key driver for compliance and security use cases. Many legacy solutions struggle to keep data for long periods of time because of the cost and performance impacts of building large indexes and the compute power needed to query them. Keep your data for as long as you want: simple as that. Whether you need it for one month or ten years, DataSet maintains hot, searchable data at production speed. Retain event data indefinitely using SentinelOne-hosted or customer-managed, low-cost S3 storage, and simply pay when you need to query it.

"With DataSet, our engineering, infrastructure and security teams have one single source of truth to make data-driven decisions.
We no longer have to stitch context across teams and use cases.

Josh Danielson
Chief Information Security Officer, Copart



Hindsight - Keep your data for as long as you need

Customer Goals

Goal	DataSet
Capture high volume log sources for security investigations and hunting	Collects any type of event data including high volume sources such as EDR, NDR, DNS, DHCP, Flow Logs, Firewall Traffic logs, and more into a single data platform
Automatically Scale your data collection and retention capabilities	Delivered as a SaaS platform with no need to scale, upgrade or deal with indexes.
Integrate with other tools in your security or IT stack	Built on an open API framework that allows for easy integrations built for data ingestion or notifications
Share data across your organization	Logically separates data across teams (IT, Security, DevOps, Engineering), but supports cross-team search for easy sharing of data to support various use cases from security to IT, DevOps and Engineering. Supports access to data in various ways including via Singularity XDR, Log Analytics, or 3rd party tools such as Grafana, Google Data Studio, or Kibana.
Store Data for 12+ months for security and compliance use cases	Provides flexible and cost-effective storage with flexible query models (unlimited or pay -per-query) to meet the needs of any organization

Used and loved by innovative companies around the world

TOMTOM DOORDASH zalando
asana STITCH FIX Shipt

The data platform with security at its core

PCI AICPA SOC HIPAA

DataSet is built using security best practices and technologies. DataSet is certified for SOC2 Type2, HIPAA and PCI DSS3 to meet your compliance needs.