

Your security telemetry, retained and searchable.

Most security teams need searchable historical telemetry. Not every team needs the full capabilities of a SIEM. Daylight delivers retention, searchability, and self-service investigation as a fully managed layer on top of your MDR.

THE Daylight Service

A fully managed security data layer for Daylight MDR customers. Telemetry from Daylight integrations is retained, and accessible through a conversational AI agent. Ask questions in plain English and get results, without building pipelines, writing parsers, or operating a SIEM.

THE Daylight Difference

01

Zero operational burden

No ingestion pipelines, parsers, schemas, dashboards, or SIEM administration for your team to own. Daylight manages the data layer end to end.

02

Raw telemetry, retained as-is

Telemetry stored in its original format. Schema-on-read at query time means nothing is out of reach because it was not prepared in advance.

03

No data pipeline to build

Coverage is defined by your MDR integration footprint. No ingestion pipelines, no infrastructure to manage, no retention policies to tune, and no new platform to operate.

04

Long-term retention without SIEM economics

The most recent 90 days stay hot and immediately searchable. Older telemetry can move to lower-cost archival storage and be rehydrated when historical investigation is needed.

From retained telemetry to investigation-ready answers

Daylight integrates with your security and business systems

- 1 Daylight integrates with endpoint, identity, cloud, email, SaaS, and other relevant systems to collect the telemetry and context needed for managed security operations.

Data flows into the managed data lake

- 2 Security alerts and logs from Daylight integrations are automatically ingested into the Agentic Security Data Lake, with no separate pipeline project for your team to manage.

Raw telemetry is stored as-is

- 3 Data is retained in its original format, without requiring upfront normalization, parser work, or schema mapping. Nothing is excluded because it was not prepared in advance.

Recent data stays hot and searchable

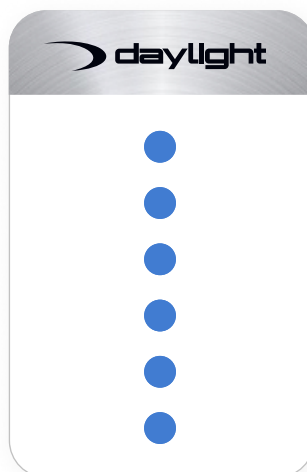
- 4 The most recent 90 days of telemetry remain in hot storage for fast investigation. Ask questions conversationally or use KQL for direct control. The AI agent helps query the data, return results, and explain what it searched and why.

Older data moves to cold storage

- 5 After the hot-retention window, data can move to lower-cost cold storage and be rehydrated when historical investigation is needed.

Three approaches. One clear leader.

Long-term data retention
Self-service investigation
Plain-English AI query UI
Zero operational overhead
Integrated with MDR
No pipelines, parsers, or schemas to manage



SIEM



MDR's
data lake

