

# Singularity Skylight

Unify Enterprise Security Data for Autonomous Context and Action

Many organizations have too much data in too many places. With data feeding from several tools to multiple consoles and data lakes, enterprise security teams have to look in too many places, take too much time, and spend too much money to figure out what is happening and respond to it. The struggle to normalize data leaves these teams with a fragmented data store that can only be utilized with immensely complex queries.

**Singularity Skylight** delivers on SentinelOne's commitment to a holistic approach to cybersecurity, arming your team with the power of machine-speed technology and the flexibility of open & native data ingestion to make better decisions, automate workflows, and derive more value from existing technology and security tools. By unifying your security and enterprise data in a singular view, you can take autonomous action on a more complete picture of your environment. Skylight provides complete data visibility, ingestion, and storage capabilities, integrating SentinelOne and third-party data within our patented Storyline™ technology.



## One Home for All of Your Security Data

Unlike traditional SIEMs, which require manual scripting and continuous schema adjustments, Skylight makes all data classification and ingestion simple. Singularity XDR seamlessly ingests data from any source, including third-party endpoints, clouds, containers, IoT devices, and more. Analysts no longer need to understand how data is structured or queried to action and respond in real time.



## Threat Hunting & Visualization, Simplified

Skylight enables security teams to observe and hunt across all security events for increased efficiency. It also helps you visualize and analyze threats before they cause impact, enabling the SOC to move from reactionary playbooks into anticipation of possible attacks or breaches.



## Automated Context & Correlation Across All Your Security Data

Skylight allows you to intuitively correlate SentinelOne-native endpoint, cloud, identity data with third party data from across your security & IT stack. This enables you to cross-analyze and potentially find new threats in your ecosystem that can be addressed quicker, reducing MTTI and MTTR.

## Key Benefits

### Unified Ingestion

Ingest all of your data at scale, efficiently, and cost-effectively — all available through a single platform.

### Affordable Data Retention

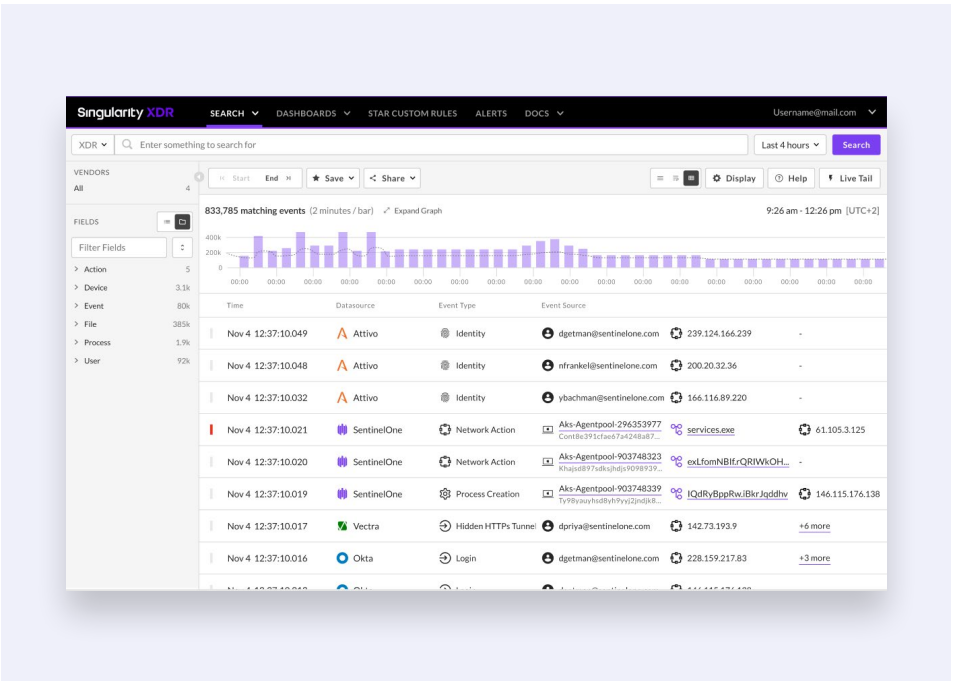
Retain large quantities of data for multiple years, without compromising on query speed, power, or flexibility.

### Intuitive Visualization

Understand the complete picture with dashboards and visualization trends to identify anomalies then respond to & remediate security issues through a single, unified workflow.

### Power Analysis

Filter, compute, extract new fields in real-time, create groupings and statistical summaries and more to get contextualized data that empowers analysts to triage, investigate swiftly, and respond to suspicious and malicious activity.



## Key Benefits

- + Meet the needs of every analyst, from entry-level admin to sophisticated threat hunter
- + Reduce Mean Time to Investigate (MTTI) with data structure, flexibility, and scale
- + Improve actionability, including native platform EDR, cloud, and identity events, to third party security data
- + Ingest data from third party sources such as identity, email, cloud, and more with out of the box integrations and APIs
- + Visualize queries and other activities with built-in dashboards and graphs

## Unlock the True Potential of Security Events & Forensic Data Through a Holistic, Unified Workflow.



Unified data platform for SentinelOne and third party security data



Out-of-the-box Visualization tools and dashboards to identify trends, see suspicious data, hunt for threats, and quickly respond to malicious events.



Contextualization and correlation of data from across your environment



Great customer service, even better product.



**SENIOR DIRECTOR, IT**  
Healthcare

## Innovative. Trusted. Recognized.

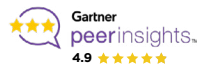


A Leader in the 2021 Magic Quadrant for Endpoint Protection Platforms



### Record Breaking ATT&CK Evaluation

- 100% Protection. 100% Detection.
- Top Analytic Coverage 3 Years Running
- 100% Real-time with Zero Delays



### 99% of Gartner Peer Insights™

EDR Reviewers Recommend SentinelOne Singularity



### About SentinelOne

SentinelOne is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks at faster speed, greater scale and higher accuracy than human-powered technology alone. The Singularity XDR platform offers real-time visibility and intelligent AI-powered response. Achieve more capability with less complexity.

### sentinelone.com

sales@sentinelone.com  
+ 1 855 868 3733