Endpoint monitoring and compliance

INNOMINDS: MONITORING REMOTE EMPLOYEES AND ASSURING COMPLIANCE

Company Overview

Considering two top requirements; being able to store data hot over several years as well as having access to significantly more compute for deep analytics on a regular, but infrequent, basis, Ionis Pharmaceuticals realized that legacy platforms such as the ELK Stack would not meet their requirements without significant overprovisioning leading to a high cost and the need to hire additional operational staff to manage and maintain the implementation. The cost of hot data retention became a concern as well as there was no practical way to scale up storage to hundreds of terabytes without going to a tiered hot-warm-cold architecture which would still be costly but, more importantly, not make most of the data available for days when it would have to be re-hydrated from cold storage.

Full Visibility

By ingesting all log data from 1,300 Windows, Linux, and Apple endpoints over 5 global locations, Innominds gained full visibility of their employees' activity. Additionally, log data from their Sophos security gateways was added for additional observability of network activity allowing them to predict threats and facilitate forensic investigations.

Operational Posture

Having gained full observability of all employees and servers across all global locations, Innominds has full real-time visibility of their security posture with out-of-the-box analytics apps for Insider Threat Detection and Advanced Endpoint Analytics.

Faster Disturbances detection

Machine learning-based analytics and alerting reduced meantime to detection by 90%. Full text search across all data and granular contextual 360 views into every user and entity lead to significantly faster detection and remediation. With no practical limit to data retention, all historical data is immediately available making remediation across the network significantly faster.

Observability of remote employees globally

When the Covid-19 pandemic hit, Innominds made the decision to have all their 1,300 global employees work remotely from their homes. Being a software development partner for global corporations in Healthcare, Banking, Finance, Insurance, and Construction, a strong focus on data security and compliance was deemed critical to maintaining a trusted relationship with their clients. As the developers of business-critical platforms and applications, compliance reporting and process transparency are important tools to not only assure integrity of the software but also providing documentation required for solution audits and certification. Additionally, Innominds wanted to be able to retain all log data for several years in hot storage not only to be able to respond quickly should there be a need to access historical data but also to be able to run deep machine learning-based analysis on all historical data on a regular basis, surfacing any potential threats, with the latest algorithms and threat intel.

Platform challenges

Considering two top requirements; being able to store data hot over several years as well as having access to significantly more compute for deep analytics on a regular, but infrequent, basis, Innominds realized that legacy platforms such as the ELK Stack would not meet their requirements without significant overprovisioning leading to a high cost and the need to hire additional operational staff to manage and maintain the implementation. The cost of hot data retention became a concern as well as there was no practical way to scale up storage to hundreds of terabytes without going to a tiered hot-warm-cold architecture which would still be costly but, more importantly, not make most of the data available for days when it would have to be re-hydrated from cold storage.

Cost Challenges

Considering Elasticsearch, Innominds realized they would have to deploy a minimum of 3 master nodes and over 60 data nodes just to ingest 1TB of data per day and retain that data hot for just one year; a far shorter retention time than they wanted to be able to maintain. This configuration would add up to a $500,000 per year just in compute and storage cost, not taking onto consideration any licensing, support, or operational overhead cost. Even when looking at AWS's Ultrawarm solution which stores the data on AWS S3 front-ended by Ultrawarm caching and compute nodes, the cost would still run around $100,000 per year. This led Innominds to look for alternatives.

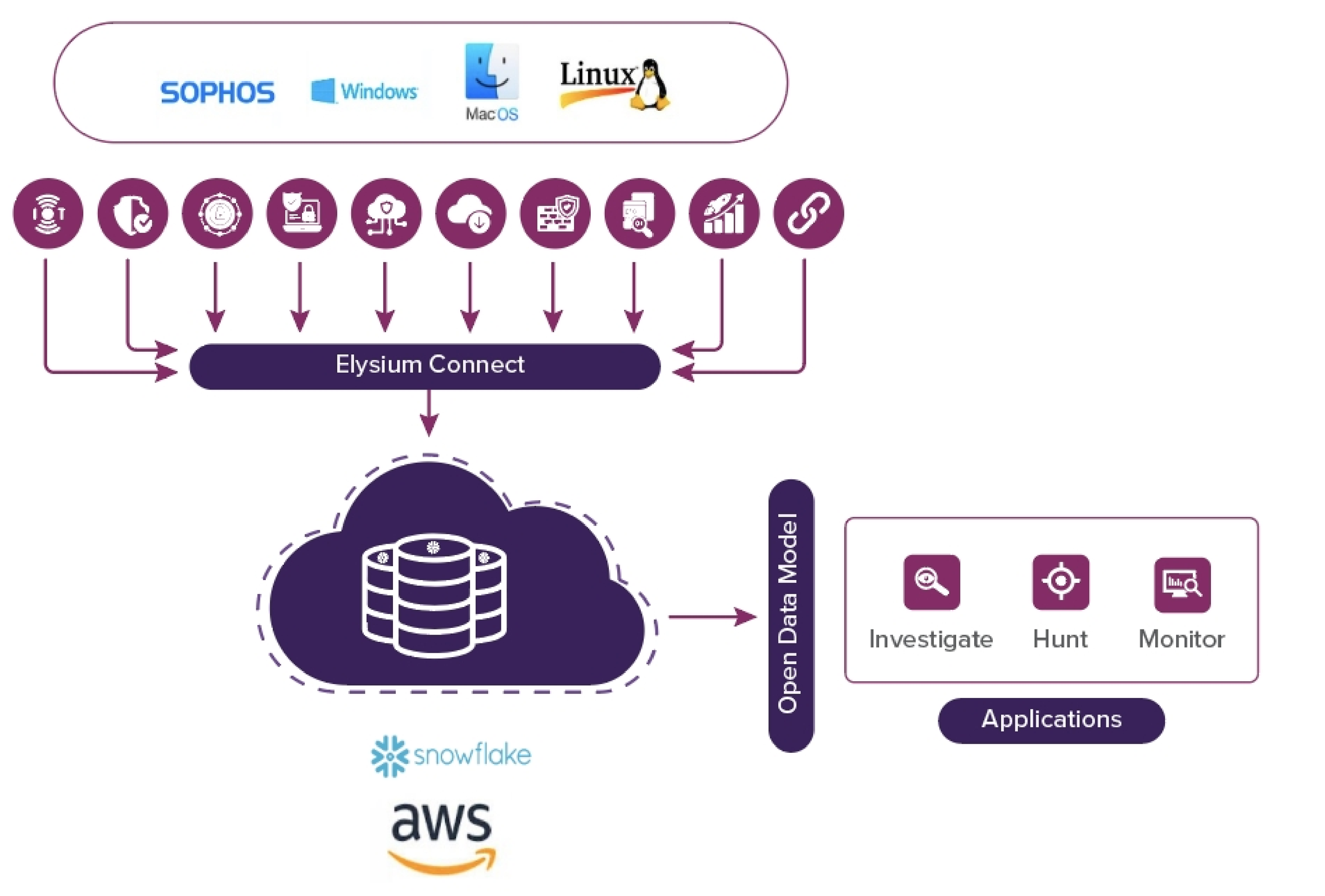
Enter Elysium Analytics and Snowflake

Since Elysium Analytics runs on Snowflake, the solution benefits greatly from a highly efficient cloud native platform where compute and storage are separated and the customer is billed on actual usage, eliminating the cost of infrastructure resources not being utilized as is the case in traditional on-premises or cloud deployments.

Onboarding to the Elysium Analytics solution, a cloud native and cloud scale solution, proved to be simple. First Innominds identified the endpoints and servers they wanted to monitor and determined they would have to be able to collect from Windows clients, Mac clients as well as Linux clients. Additionally, they wanted to collect all logs from their Sophos security gateways that the clients would connect through over VPN for many of their more critical applications for additional visibility.

Data Collection

Near real-time data collection and shipping is facilitated by connecting to the Elysium Analytics collector service…

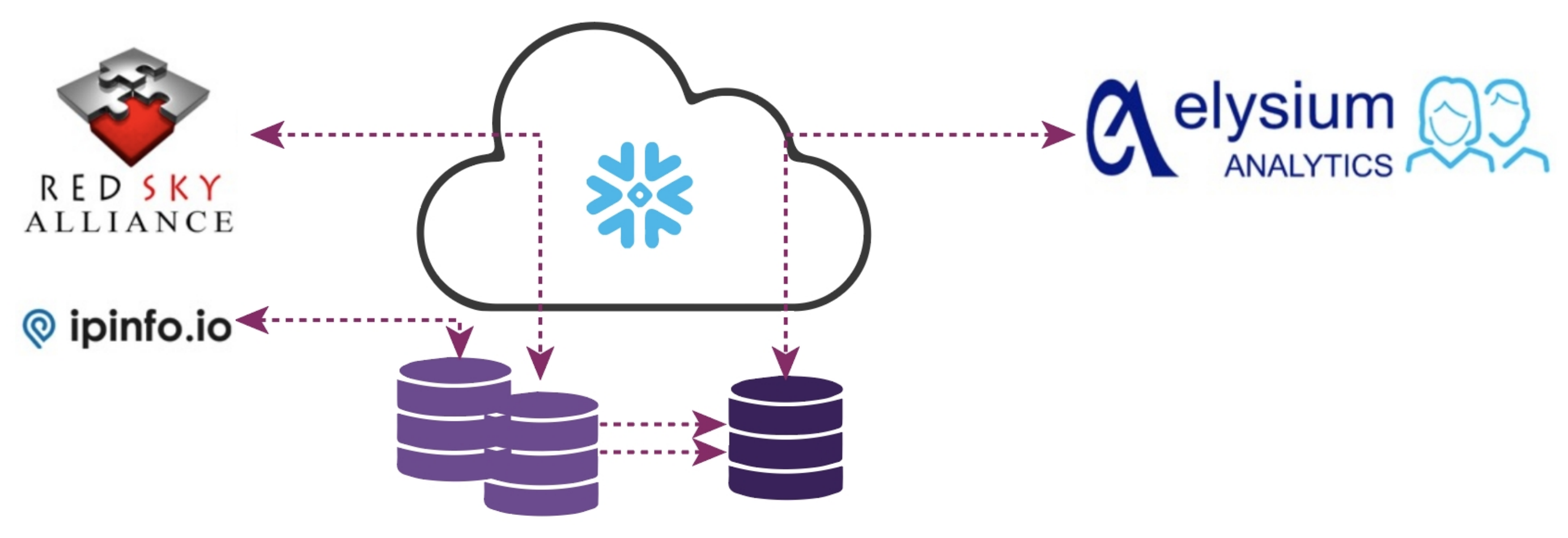


DATA COLLECTION FLOW

File Shippers	Connectors	Parsers	Enrichment
Beats and Minifi compatible for simple integration and leverage of existing enterprise collection frameworks as well as integration with any 3rd party source.	Connect your sources leveraging existing connectors from Logstash and Apache Nifi with our direct output plugin from Logstash to Snowflake. Additionally, we provide Kafka and custom connectors based on Rest API and webhooks.	Parse legacy device data sources in Logstash and modern data sources in JSON and Java.	Enrich data in real-time with Identity, Asset, Geolocation, and Threat Intelligence, as well as data from lookup tables built into the storage platform data pipeline.

DATA SHARING OVER SNOWFLAKE DATA MARKETPLACE

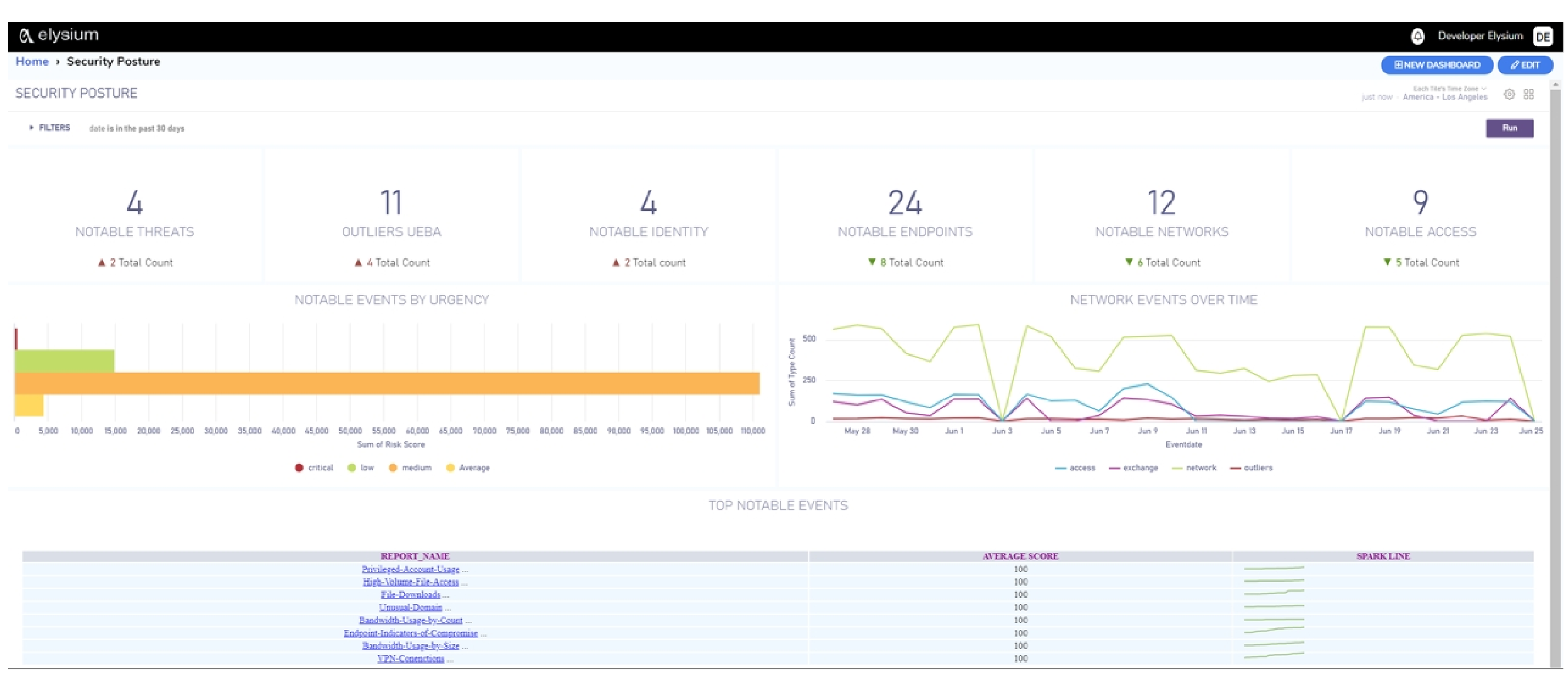
Innominds had a requirement to enrich their data with Threat Intel and IP Location data to improve on their detection and remediation capabilities. Typically, in a legacy application such as Elasticsearch, Enrichment data is provided by 3rd party data vendor who provides regular updates to their data set which, then in turn, the customer can ingest through an ETL service, creating a replica of the data in their own data store used for analytics. For Innominds, having chosen Elysium Analytics, running on Snowflake, the process is significantly simpler and far more cost effective. Accessing enrichment data from two Snowflake Data marketplace vendors, Red Sky Alliance and Ipinfo, is achieved as simply as connecting their data warehouse to the data warehouses of the data vendors, join the data sets, and they have real time access to the 3rd party data with no ETL requirements, no duplication of data, and no maintenance overhead. This not only dramatically lowers the ingestion cost but also relieves Innominds of all operational overhead associated with accessing this data.



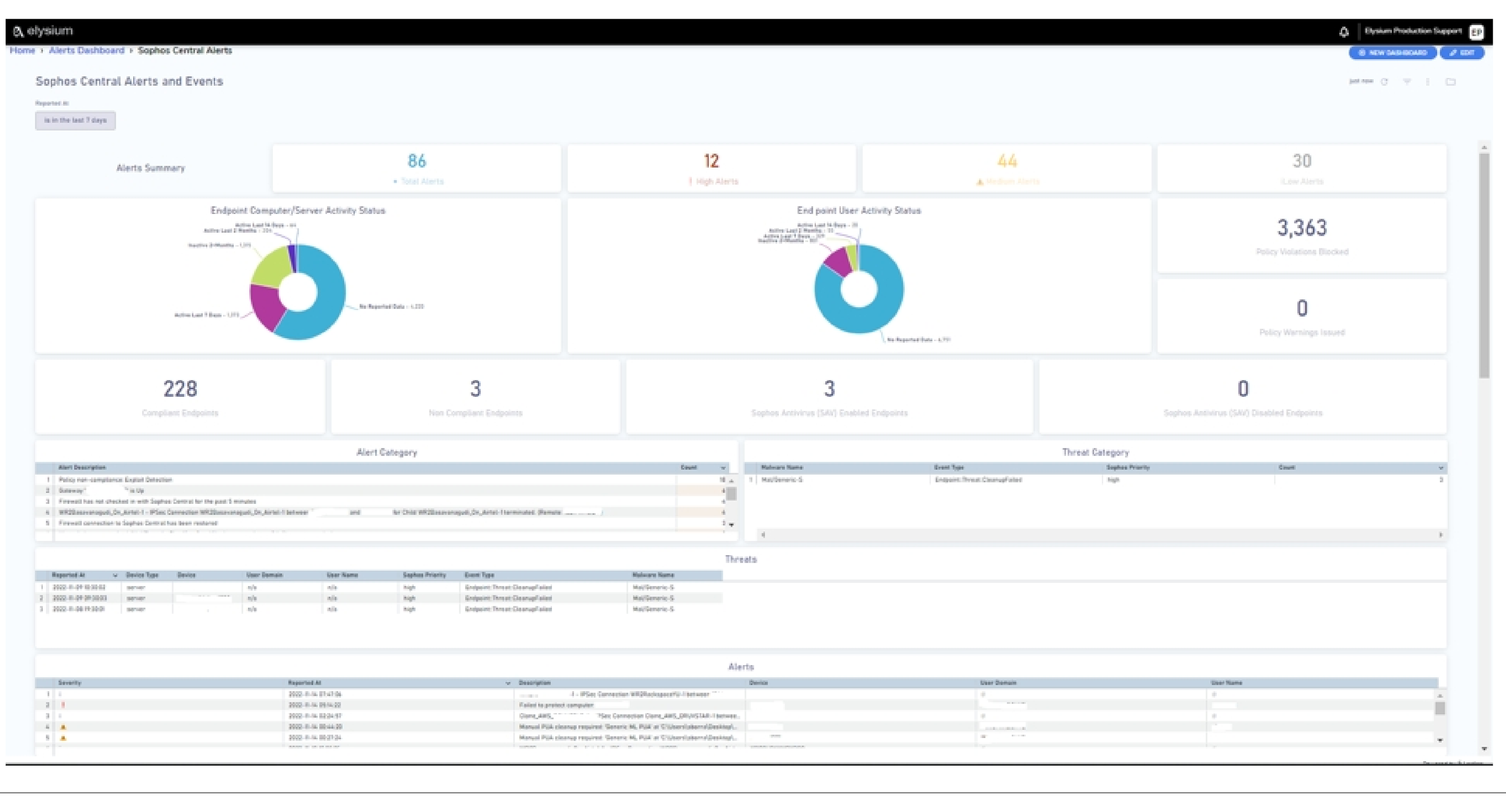
With the data collection configured and the parsing and data mapping verified, data was immediately loading to Snowflake giving Innominds full visibility to activity on the endpoints and network on our included out-of-the-box dashboards. This gave them immediate visibility to possible vulnerabilities and threats on their network as well as the ability to do full text search on any data.

The dashboards of immediate interest were:

Security Posture: Enterprise situational awareness dashboard to view key security indicators that are critical network events to be investigated. It shows outlier events/total volume trend and shows top events and top notable event sources.



Endpoint Analytics: Endpoint protection becomes more complicated as users connect their own devices into the corporate network and as more users work remotely. An organization has to accept that not all traffic on the user's device will go through the corporate security controls, and in many cases the organization may not have device control to enforce a specific endpoint security solution. Elysium's endpoint analytics enable Innominds to collect from all devices and deliver visibility across all endpoints.



Endpoint Analytics

Elysium Analytics bundles both Kibana and Looker, giving Innominds not only access to out-of-the-box dashboards and analytics that are included in the solution but also provides the ability to customize or build their own dashboards at no additional charge. Typically, a BI application license would run well in excess of $100,000 per year and require significant set up efforts before you can run analytics on your data warehouse. With Looker already implemented as a part of the Elysium Analytics solution and with parsing and data mapping in place, Innominds were able to quickly develop custom dashboards specific to their environment and use cases on Looker with minimal effort, no contract negotiations or up-front license expense, billed at the standard usage-based rate.

Machine Learning

Elysium Analytics has several machine learning models implemented providing additional critically important data points for detecting anomalous behavior on end users and entities. This is providing important visibility into behavior

With about 1TB of data loading daily, it became obvious right from the start that the ability to do full text search on their data was invaluable as a tool to quickly be able to do ad-hoc queries on any user or entity in the corporation.