Data Security as a Service Breakdown: **Observability**

Gain intelligence through powerful visibility into data consumption across your organization

ALTR's Data Security as a Service platform brings enhanced data security to enterprises across their modern data architectures. With ALTR, organizations can implement a data consumption governance model, benefitting from ALTR's ability to observe, detect, and automatically respond to threats. Further, leveraging ALTR's protection service secures data from direct access threats while ensuring all requests flow through the organization's data consumption governance model. In this brief, we'll discuss ALTR's observability capabilities.

Why Observability is Critical

Enterprises invest heavily in security, but still lack observability into how data is consumed in their organization. This limitation makes it hard for companies to understand how data is being used across the enterprise and puts their security teams into a more reactive stance in the face of constantly growing threats. Without observability, companies are also unable to determine their level of operational risk, which is a growing requirement in today's rapidly evolving regulatory landscape.

With the accelerated move to remote work and subsequent adoption of even more cloud technologies, this lack of knowledge into data consumption has become a critical problem that enterprises need to address.

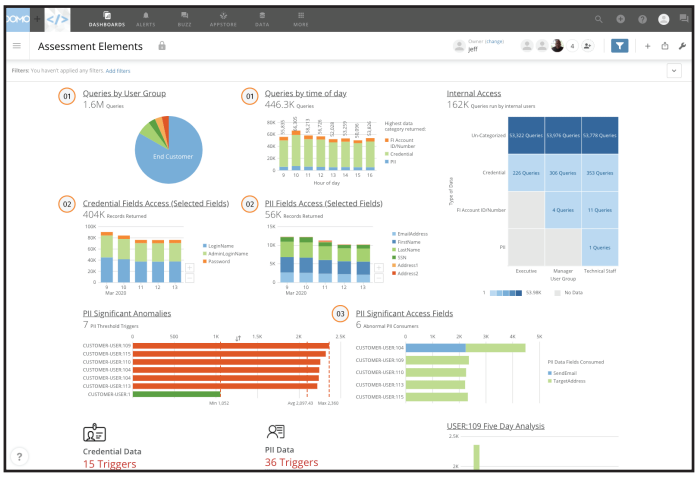
ALTR's DSaaS platform offers a complete solution for observability, delivering highly granular insights and rich context so enterprises can analyze, understand, and ultimately control data consumption.

The three main components of data security as a service: Observability; Detection and Response; Protection

How ALTR Delivers Observability

While applications request data directly from data sources, ALTR records each request in real-time without impacting query processing time. By seeing and recording the query, result set, and the application's usage of the result set, along with additional metadata around the request (time, IP address, and more), ALTR provides unparalleled intelligence around data consumption from a single application to the entire enterprise.

ALTR's record keeping is extensible as well, allowing for the tracking of custom metadata like identity information, the reason for a data request, and any additional current or future compliance requirements. All of this information is stored as tamper-resistant records using ALTR's proprietary distributed ledger technology. Storing records this way benefits forensics and compliance reporting as information viewed from ALTR can be trusted as actually having happened. Records can be viewed within ALTR's console and sent to your chosen SIEM, security cloud, or visualization platform.



Visualizing observed queries within Domo

01. Which groups of users are issuing queries, and what time of day is the sensitive data being consumed the most?

02. Which types of data are being requested?

03. Who are my top users consuming sensitive data like PII or PHI?

The Benefits

- **Analyze risk** - Understand where sensitive data is viewed most often through ALTR's easy-to-use dashboards
- **Reduce costs** - View captured SQL queries (and responses) to improve poorly performing or data-hungry applications
- **Simplify compliance reporting** - View and export timeboxed query history to easily prove governance policies are working