



Client: A large US based company was facing continuous DDOS attacks days after days, impacting their core business.

Challenges:

- Massive amount of semi-structured data
- Massive volume of real-time data
- Weekly new event's types and schema updates
- Hardware footprint
- Data privacy & security
- Scale as needed

Solution:

CaliStream's team worked jointly with the customer's security team to collect, store and analyze a massive amount of network related data.

Benefits:

With all the data in one place, the data-science team and the development team came up with a new set of business rules able to keep most of the DDOS data out of their data-centers reducing their hardware footprint by 40%.

The key benefits were:

- Ability to take a large diversity of data without fixed schema
- Ability to collect and analyze Billions of events in real-time
- Self-Service data collection pipeline
- Data-centers friendly solution
- Reduce DDOS traffic by 90%
- Reduce hardware footprint by 40%

A large US based company was facing continuous DDOS attacks days after days, impacting their core business serving over 100 Million online users.

CaliStream's team worked jointly with the customer's security team to first instrument various network probes, then bring this massive amount of new data to the main customer data-warehouse using CaliStream data pipeline and SDKs.

Then based on newly acquired knowledge, the network infrastructure team upgrades the backbone infrastructure to support dynamic filtering rules triggered by CaliStream real-time data pipeline.

Not only this project allowed to reduce DDOS traffic by more than 90% but also to reduce hardware footprint by 40% thanks to DDOS network traffic being stopped outside of the customer backbone.

