February 23, 2022 Case Study

CapStorm

Enterprise Salesforce Security Breach Detection

Multi-National Manufacturing Enterprise

An organization supporting the construction, building, and manufacturing industries.

This global enterprise is headquartered in Switzerland with subsidiaries around the globe. The complex network of 250+ factories, suppliers, and distributors is bolstered by a multi-org Salesforce implementation leveraging multiple Salesforce clouds including Service, Sales, and Pardot. These geographically segmented Salesforce organizations effectively create data silos with limited ability to monitor user activity across each environment. CapStorm enables data driven automated thread detection with aggregation across all Salesforce environments.

Industry
- Manufacturing

Company Size
- 25,000+

Specialities
- Production at Scale
- Research & Development
- Supply Chain

Tech Stack
- Salesforce
- On-Premise Hosting

Problem

A multi-org Salesforce environment created a security gap as there was no way to proactively monitor for potential security breaches across all systems of record.

Salesforce is used with multiple divisions to support Sales, Support, & Marketing with each SF Production organization designed to meet the needs of a different geographic region. This regional segmentation has inadvertently created data silos and limited the ability of the security team to efficiently monitor for potential threats. As a further complication, the business struggled with Salesforce's limits related to two key data points. Retention periods for login history are too short to provide meaningful trends. Query timeouts are frequent when attempting to access event history.

Solution

1. Secure Data Extraction

Data is replicated incrementally from Salesforce into the enterprises' on-premises relational databases. This replication retrieves key login and history data which is critical for threat detection analysis.

2. Data Consolidation

Each Salesforce organization maintains a unique SQL database which ensures the fidelity of the data and allows for individual org analysis.

3. Security Analysis

The single source of Salesforce activity is connected to an analytics tool, enabling visualization of trend data across all Salesforce production organizations.

Outcome

Automated threat detection reduced enterprise risk with near real-time precision alerting.

A one-source privilege comparison ensured that the business enforced a global standardization for Salesforce data access.

Forecast accuracy increased as trend data for all Salesforce objects can now be monitored over a long period of time, impacting Sales, Service, and the companies' overall revenue.