CASE STUDY

DEVELOPMENT OF REAL-TIME DATA DASHBOARD FOR NETWORK THREAT PROTECTION

An intuitive & easy to use dashboard to improve network threat analysis

Client Background

The client is a deep learning innovator specialized in safeguarding enterprises from cyber threats with its real-time network threat protection platform. The AI-based platform comprised of network threat appliances and deep learning cloud for generating threat prediction messages and performing threat detection, respectively. The client faced challenges in network data representation and reporting as it was available only in the backend. Additionally, the client wanted quick and easy provisioning of new tenants with a scalable data pipeline capable of handling a large amount of data every day.

Xoriant Solution | Key Contributions

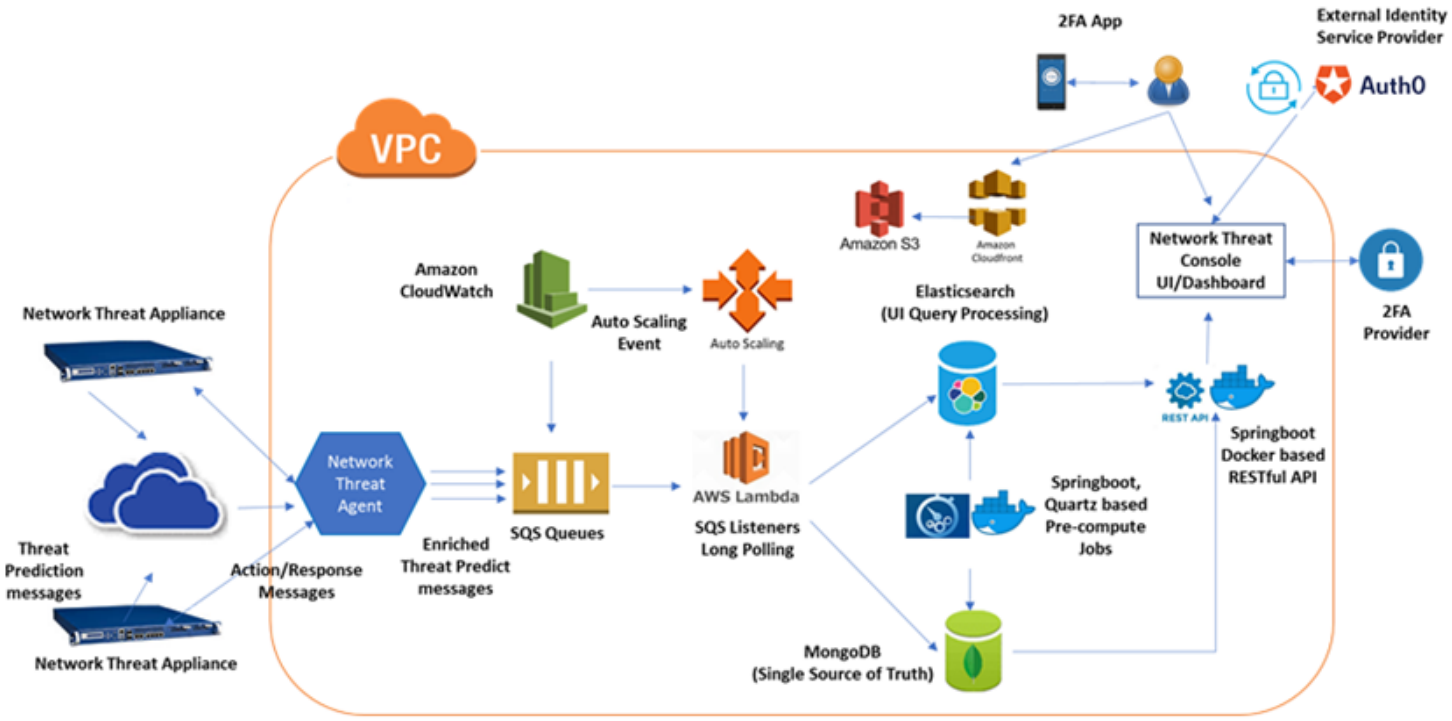
- Development of an end-to-end functionality of the GUI and server-side
- Configuration of O365 and multi-tenancy support for real-time analysis of emails ensuring better visualization and analytical capabilities of network threats
- MongoDB Shards (EC2 based across AZ) as a single source of truth and Managed Elasticsearch for aggregated data storage for querying
- Creation of real-time dashboards with ReactJS and report generation with AWS Managed Elasticsearch Services
- Provision for both shared and dedicated deployments leveraging Terraform and Ansible

KEY BENEFITS

- Creation of this dashboard being a fresh development, we achieved a query latency of 5 seconds, which covers data ingestion, data visualization and remediation
- Growth in the customer base with quick adoption of the user-friendly UI system on both shared and dedicated deployments
- Quick and easy onboarding of new tenants with a simple interface
- Reduced infrastructure costs to 70% using the multi-tenant provision with isolation at both logical and physical level using shared MongoDB and Elasticsearch cluster

- Lambda-based server-less implementation for robust and scalable message handling of network threat data
- Scalable infrastructure and storage for data ingestion and dashboard
- Data interface creation for reporting with REST APIs over Elasticsearch and hosting them on AWS EC2 instance
- Implementation of user authentication using Auth0, which worked seamlessly with multi-tenancy

High Level Architecture



Technology Stack

Elastic Search | MongoDB | EC2 | Lambda | AWS | ReactJS

Xoriant is a product engineering, software development and technology services company, serving technology startups as well as mid-size to large corporations. We offer a flexible blend of onsite, offsite and offshore services from our eight global delivery centers with over 3600 software professionals. Xoriant has deep client relationships spanning over 30 years with various clients ranging from startups to Fortune 100 companies.