INDUSTRY
Healthcare

CHALLENGES
- Disparate and siloed systems and data sources
- Higher risk from slow security investigations
- Lack of enrichment data from third-party sources
- Inaccurate or incomplete analysis from poor data quality
- Limited use cases with existing SIEM architecture
- Limited retention and historic analysis
- Lack of advanced machine learning functionality

SOLUTION
- In-depth Secure Data Lake Assessment
- Orchestrated deployment of services
- Integration of data sources
- Deployment of enterprise data lake with low-latency search capability
- Deployment of hundreds of nodes, fully configured, in minutes
- Support of actual data volumes exceeded original estimates—by double
- Mitigated the lack of customer development environment by leveraging Optiv’s private cloud environment
- Automated incident response

RESULTS
- Decreased incident response time from 2-4 hours to 12 minutes
- Expanded use cases from incident response (SOC) to fraud, compliance, IT and more
- Average monthly savings of $100-400k by enabling fraud detection analysis
- Creation of new capabilities in machine learning and advanced analytics
- Detection and resolution of complex or unknown issues

CASE STUDY
Large Healthcare Organization Leverages Optiv to Increase Visibility, Accelerate Response and Enable Advanced Analysis

OVERVIEW
A large healthcare IT services provider helps clients with population health, care management and other data-driven initiatives to improve quality and reduce costs. Maintaining a secure environment for customers is critical in this industry which is compelled to adhere to strict privacy regulations. The company’s cyber defense director began to question whether the company’s security information and event management (SIEM) was up to the task of quickly analyzing log data for risk.

The system was buckling under the load of 140 million customers, 250,000 endpoints and eight terabytes of raw logs daily. Analysts running queries to research an incident often didn’t get results for hours, delaying the identification of problems before damage was done. This presented problems in complying with healthcare rules for timely public breach notification. Data quality was another issue. The SIEM couldn’t make sense of the disparity in data formats, which resulted in limitations on the usefulness of the system for broader investigation research and resolution.

HOW OPTIV HELPED
Optiv Security partnered with the health IT company to design and deploy an enterprise-scale data lake comprised of petabytes of customer data. This new system supports more than 110 disparate data sources and processes peaks of up to one million events per second (EPS). Analysts can perform basic searches and run more advanced analytics at a much faster rate. Correlation and enrichment of logs prior to data ingestion speeds up investigations. The company’s cyber defense organization is using the data lake to perform new queries and tasks which weren’t possible with the SIEM. This includes automated incident response, which immediately triggers action based on rules. The data lake is improving vulnerability scanning by aggregating and analyzing data to pinpoint the location of attacks.