# Health Information Technology Provider

## HEALTH IT PROVIDER PARTNERS WITH PRESIDIO AND AWS TO TRANSFORM ITS ENTERPRISE DATA HUB WITH CLOUD-BASED SECURITY AND CENTRALIZED LOGGING

### The Challenge

This customer is a leading provider of health information technology products, specifically electronic health records (EHR), practice management and lifecycle services. One of its flagship offerings is a cloud-based EHR and practice management solution used by a competitive share of the ambulatory/urgent care practices market.

As the install base for this product grew in scope and complexity, executive leadership realized they needed to quickly modernize their platform. This would require a modern Enterprise Data Hub (EDH) that could be a centralized source of all downstream data to ensure quality, consistency, and transparency from their clients' EHR systems.

With highly confidential client and patient information on the line, the customer sought trusted partners who could maintain the utmost security standards to meet strict regulatory and legal compliance mandates while delivering a new data hub on time and on budget.

### The Solution

As a part of this endeavor, the health IT provider would need to implement two new foundational components: Security Services and the Operations Console, a centralized logging platform with a customizable monitoring dashboard.

The customer engaged Presidio and AWS to tackle this essential initiative. The primary focus of these solutions was the development of the EDH to centralize the management of all incoming and outgoing patient/provider data within the enterprise.

### Security Services

Security Services is a centralized authentication and authorization suite for all current and future applications and services within the customer's ecosystem. Primarily, Security Services is intended as an enterprise mechanism to identify and protect users and resources. Additionally, it helps detect and respond to upfront threats while providing mechanisms for recovering from attacks, with an auditable path to compliance.

Presidio built:

- An Authentication API for creating and managing client tokens
- A Management API for managing clients, users, and groups, among other administrative functions
- A Login Application for end-user authentication and self-service functions

To lay the foundation for these services, the Presidio DevOps team deployed several cloud infrastructure components. PingFederate, an OAuth-compliant authentication and authorization service, and PingDirectory, a performant enterprise datastore for customer client and user identity data, were deployed as an Amazon EKS cluster within the customer's cloud infrastructure. This deployment scheme allows them to abstract upstream access to the core functionality of applications to simplify the internal client interface, reduce the attack surface and prevent vendor lock-in.

For the Authentication API, the Presidio team leveraged AWS Lambda, fronted by an API Gateway, to provide proxy functions to the underlying Ping Identity EKS cluster. NestJS, a flexible and progressive Node.js framework for building services, was used to build out the functions that provide token creation, validation and management for OAuth clients and end users.

The Presidio team used the same approach to implement the Management API. This API provides:

- Endpoints for new client registration
- User management functions such as identity creation, modification, and deletion
- Identity grants
- Legacy application user migration
- Client secret management tasks

Certain endpoints, such as those that provide end-user management actions, were built using Amazon SNS for routing messages to outbound mail services. Others, such as the client secret management functions, use AWS Glue to disable clients with expired secrets, in addition to SNS for messaging.

The Security Services suite of services and applications ultimately includes a custom Angular web application. The Login App interacts with the Authentication API for all user actions, such as communicating auth codes and retrieving tokens.

**Operations Console**

The Operations Console is a unified platform logging dashboard and centralized repository for application and service event data that allows an operations support team to manage and view logs, view data ingestion metrics, and monitor the quality of the incoming data. Additionally, the Operations Console dashboards provide insights into infrastructure performance, as well as jobs and alerting capabilities.

So that the customer could meet its application observability needs, the Operations Console contains:

- An end-user dashboard application providing insights and operational intelligence on key KPIs informed by log and metric events
- A centralized log and event data lake for long-term storage
- Ingestion endpoints for pulling in heterogenous application log and metric data packets
- An endpoint for third-party tools to pull specific, indexed data for external alerting and messaging.

Central to the Operations Console architecture is the implementation of AWS OpenSearch, in which Logstash handles event data coming from various ingestion streams and writes the data to S3 while simultaneously pushing the events into an Elastic-search cluster. Kibana is then used as the dashboard for viewing the various customer-defined KPIs.

Presidio leveraged a variety of AWS offerings to allow the customer to pull in event data as needed, on-demand. Third-party applications can now access the Elasticsearch indices using a proxy API Gateway whose endpoint is managed by Security Services via a Lambda authorizer. Security Services also allow team members to access the Kibana dashboards to track user and client activity metrics.

**Services / Technologies Used:**
**AWS Services:** Amazon VPC, AWS VPN, Amazon CloudWatch, Amazon S3 (including Glacier), AWS Lambda, Amazon API Gateway, Amazon EKS, AWS WAF, Amazon Kinesis, Amazon OpenSearch Service, Elastic Load Balancing, AWS Network Firewall, Amazon CloudFront

**Other Services/Frameworks/ Technologies:** PingFederate, PingDirectory, Terraform, NodeJS, NestJS, Angular, Typescript

### Results/Benefits

The Security Services and Operations Console solutions are intended to be more than just prerequisites for the Data Insight program overhaul. Both solutions provide upfront value to any integrated service or application. Security Services is based on the widely adopted OAuth 2.0 specification, which translates into smoother and less costly integrations with new application development, as well as third-party services and products. Similarly, the Operations Console is a configurable centralized logging and metric event service that allows for more efficient application/service observability for newly developed endeavors within the enterprise.

### Partners

aws

The customer selected AWS primarily to build out a centralized, cloud infrastructure for EHR and revenue lifecycle services. The primary goal being to manage large streams of data coming from its practice-oriented customer base and avail the data to operational and application intelligence solutions. This progressive move to the cloud enables the client to take advantage of the whole AWS ecosystem, providing scale to meet their end customers' needs. The new EHR is also designed to enable Regulatory Reporting to be an automated byproduct of their day-to-day activity instead of an after-hour burden for clinicians and staff, enabling more time and attention to patient care.

### About Presidio

Presidio is a global digital services and solutions provider accelerating business transformation through secured technology modernization. Highly skilled teams of engineers and solutions architects with deep expertise across cloud, security, networking, and modern data center infrastructure help customers acquire, deploy, and operate technology that delivers impactful business outcomes. Presidio is a trusted strategic advisor with a flexible full life cycle model of professional, managed, and support and staffing services to help execute, secure, operationalize and maintain technology solutions.

**For more information on how we connect IT of today to IT of tomorrow, visit presidio.com**