CUSTOMER SUCCESS STORY: Voltage SecureData Enterprise

Voltage security

US Government Organization

Advancing Medical Research by Sharing Big Data

Sharing with Security

A United States government organization faced an interesting problem. It had joined an initiative of the U.S. Surgeon General to encourage collaboration on medical treatments by sharing data with medical researchers. They wanted to utilize the history of medical information from their staff members to improve medical research and ultimately improve healthcare for all Americans. But while sharing this data, all personal information had to be masked so that privacy could be maintained.

Voltage Security® was selected to provide the data protection solution for the government organization. The healthcare enterprise data warehouse is a database of up to 100 terabytes, holding healthcare information on hundreds of thousands of personnel. The data is de-identified and shared with other federal agencies, and with researchers and insurance entities outside the government for analytic research. The system is set for expansion to include data from other government branches in the future.

Voltage Format-Preserving Encryption™ (FPE), a mode of AES called FFX, was chosen to de-identify the data in this giant database. It provided three important and unique benefits:

- **Simplicity:** Voltage Security provides tools to allow integration with existing workflows without modifying them. A web services API, and easy-to-use APIs including mainframe and Teradata, allow for choices with minimal impact upon existing processes and programs. As a result, this implementation did not modify existing workflows and plugged into their existing Informatica® ETL system.
- **Efficiency:** Traditional solutions require large lookup tables, estimated at up to three times the size of the original database. FPE works without lookup tables. Transformation from the original data to the masked data is performed on-the-fly as data is loaded, without having to build a large and vulnerable lookup system. Performance of existing applications is not impacted.
- **Reversibility:** It was possible that researchers might need to return to the source of the data if they found a case that was particularly important or meaningful. For example, if they discovered that certain patients might have an elevated medical risk of some kind, they would want to be able to contact those patients and act upon that newly discovered risk. So they would need to take the de-identified data and, with proper administrative controls and audits, securely reverse masked data under strict controls to determine the affected patient record.

"BY 2017, BIG DATA TECHNOLOGY WILL BE THE NORM FOR DATA MANAGEMENT…"

- Forrester, The Top Emerging Technologies To Watch: Now Through 2018, by Brian Hopkins and Frank E. Gillett, February 7, 2013

Highlights

- Data masked using a provably secure data de-identification algorithm.
- Massive 40-terabyte database, growing to 100 terabytes in the near future.
- Masking Social Security numbers, names, and dates in medical records.
- Integrated into existing workflow with minimal program changes.
- Lowers operational costs, employing stateless data-masking for highly automated key management.
- Not just locking down data – enabling sharing of data.

How It Works

The Informatica ETL software was employed during a proof of concept to build a patient datamart with the identified data. The Voltage Security secured data appliance was invoked using the high performance Voltage Security web services API which can process several reports in parallel. This meant that no Voltage Security software needed to be loaded onto the ETL system. The ETL system made web services calls using an Informatica capability called a "Java transformation." This allowed for a technically simple and quickly demonstrable integration. It also left open the alternative of using the Voltage SecureData ™ Simple API to perform the encryption locally on the Informatica servers or in a private cloud if that was desired at any point in the future. The customer could demonstrate the value using the web services API, and know there were additional alternatives if they were required in the future.

The US government organization's patient datamart application is an example of how Voltage FPE can do more than lock down data to make it less available. It can also transform data to enable it to be shared securely in compliance with HIPAA rules and made available to more people without risk of breach. Voltage was uniquely able to provide this with software that was simple to integrate without changing existing workflows, and reversible under formal security procedures to retrieve the data when needed.

ABOUT VOLTAGE SECURITY

Voltage Security®, Inc. is the leading data protection provider, delivering secure, scalable, and proven data-centric encryption and key management solutions, enabling our customers to effectively combat new and emerging security threats. Leveraging breakthrough encryption technologies, our powerful data protection solutions allow any company to seamlessly secure all types of sensitive corporate and customer information, wherever it resides, while efficiently meeting regulatory compliance and privacy requirements.

For more information, please visit **www.voltage.com**.

v02-22-2013