Voltage security

Business Value Solution Brief

Solving data residency and privacy compliance challenges
Delivering business agility, regulatory compliance and risk reduction

Introduction

In today's dynamic business environment, corporation's intangible assets such as customers, systems and business process information form the foundation of competitive advantage. Concern for data privacy has resulted in a growing array of guidance and regulation that address issues such as what information can be collected, how the data should be stored, how and where information can be transmitted, what security practices must be followed and the actions required in the event of a data breach. Financial institutions in particular require a comprehensive solution for security, privacy and compliance that deliver the flexibility for soon to be implemented regulations such as the European Data Protection law and the Dodd-Frank act as well as meet country specific requirements in jurisdictions such as Switzerland, the Channel Islands, Luxembourg and Singapore.

This business value solution brief examines information privacy and data residency solutions in the context of multinational business with a particular focus on European Union requirements as they apply both in the EU itself, and across other jurisdictions with potentially conflicting regulations such as the US Patriot II mandate. The case studies of Voltage Security customer's explore not only using data-centric security to meet compliance requirements cost effectively, but also using existing applications, infrastructure, processes and administrative staff to grow new business in regulated markets.

Data-centric security has emerged as the most effective method to protect data as it is used, stored or moved across data centers, cloud services or mobile devices. We will review the case of a financial services customer with headquarters in the European Union that is using Voltage SecureData Enterprise to ensure privacy compliance, reduce data breach liability and use banking applications efficiently to improve business results. We will also cover another multinational institution solving data residency compliance challenges and achieving increased security and privacy compliance across their lines of business while taking advantage of their private cloud infrastructure.

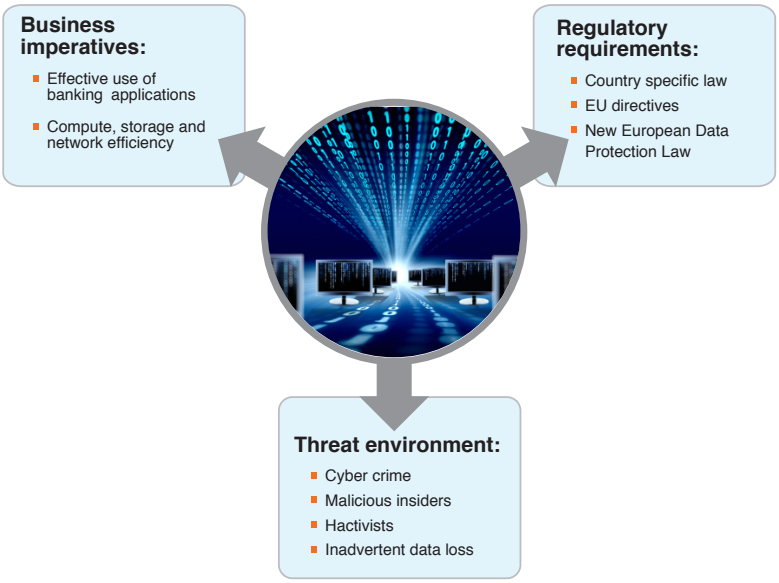

Figure 1. Business drivers for data-centric security

The multinational bank standardized on the Alnova banking application working with a global systems integrator. The business drivers for adoption of data-centric security are illustrated in figure 1. Similar to most financial services organizations, the customer faced an increasingly hostile threat environment as well as costly regulatory processes to comply with EU Data Protection Directives. In this case, urgency to deploy an effective encryption and key management solution was driven by business expansion into Luxembourg with stringent laws enforced by the Commission de Surveillance du Secteur Financier (CSSF)[1] governing use of personally identifiable information requiring data to be accessed and controlled within the jurisdictional boundaries of the country.

Voltage SecureData Enterprise was deployed rapidly with the Alnova banking application enabling the customer to make use of existing IBM mainframes, data warehouses and general purpose Linux servers within their primary data centers while enforcing strict and auditable policies on information access. The company achieved significant return on their investment from streamlined compliance and more importantly the adoption of data-centric security enabled the company to enter previously unserved markets and grow new business. The primary driver of return on the data-centric security spend was the ability to take advantage of the production application environment, the associated infrastructure and administrative processes. Without the Voltage solution the customer estimated the cost to replicate the application environment at more than ten million Euros.

Challenges

Regulatory environment

The customer faced immediate requirements in terms of compliance with the data residency laws within Luxembourg to which they were deploying new business services with the Alnova application suite. The financial regulator CCSF prohibits transmission and storage of personally identifiable information of nationals outside the country. Compliance with this regulation (Law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data implemented Directive 95/46/EC) and approval of sanctioned controls to ensure compliance were necessary to do business in Luxembourg.

In addition, the organization required a data-centric security solution that would be suitable for the forthcoming European Data Protection law. This unification of the current European Privacy Directive has received a great deal of attention for many reasons including fines up to 5% of annual revenue similar to existing anti-trust fines currently in place. Under the European Commission's current proposal data security breach notification is also more rigorous, requiring notification of affected customers within 24 hours[2]. In relation to this requirement, data-centric security is particularly attractive because an exemption is granted provided that data is encrypted and supported with a formalized information security program.

Compliance requirements most certainly will place a greater burden on organizations, particular multinational companies, with additional focus on formal information access policies, privacy by design, clearly articulated governance structure and appointment of a data protection officer.

Threat environment

The threat environment is growing increasingly hostile. Financial data and the associated PII present an attractive target. Attacks must be defended against a broad class of threat actors, most significant of which are organized cybercrime, malicious insiders and hackers. Cybercrime organizations are well funded, financially motivated groups with advanced attack methodologies, monetization networks and constantly evolving tactics. In the 2012 Verizon Data Breach Investigation Report; data collected from actual data breach investigations found that 83% of breaches were aimed at financial gain from threat agents affiliated with organized crime.

Malicious insiders are also often financially motivated, understand business processes, weaknesses in the infrastructure and have created increasing liability for the financial services ecosystem. Hackers with varied motivation present continuous challenges primarily for weak links in the overall system. Hacktivism from politically motivated groups was also a significant concern for this customer given the dynamic social landscape and diverse political landscape in which the financial services company operates. The Verizon Data Breach Investigation Report also highlighted the rapid growth of hacktivism in the past year, with attackers stealing data at a rapidly growing rate amounting to 58% of records breached.

Application and compute environment

The customer had made a major investment in infrastructure, application development and ongoing operations. The security approach needed to fit in with the Microsoft .net application environment and support a user experience that facilitated an improved workflow. Once sensitive data was captured by the front-end user facing application, subsequent back-end processing in mainframe and data warehouse systems needed to take place without changes to data format or negatively impact overall throughput and latency.

Solution Adoption

The customer adopted the Alnova banking application centralizing the operations in data centers associated with headquarters. In order to expand banking services to countries with legal requirements to protect PII data the IT and security team investigated several alternatives to protect data. Transport encryption using SSL as well as data at rest encryption were proposed and rejected as insufficient through internal review and verification with national regulatory bodies. These methods are sufficient to protect from network sniffing or stolen hard drives, but data is not protect from attackers at the application layer and exposed through security gaps in the overall system.

Voltage SecureData presented unique capability in that data format could be preserved, the key servers controlling data access could be run in the regulated country with minimal administrative overhead such that authorized users could use their applications without any modifications to their workflow or changes to the associated databases. The system was deployed rapidly and presented business benefit in four major areas as outlined in the table below.

Drive Business Growth	Increase Business Efficiency
The company entered the Luxembourg market with a systematic method to address data residency regulations imposed by CCSF	Streamlined audit processes demonstrating compliance to internal policies and country specific laws
Increase Productivity	**Deliver IT Efficiency and Continuity**
Expanded the deployment and business processes associated with the Accenture Alnova banking platform while reducing data breach liability	Leveraged existing data center infrastructure and IT processes while ensuring compliance and supporting consistent business processes

The IT initiatives that delivered business value by this leading international bank were a result of rapid roll out and application of the Voltage SecureData Enterprise solution. The product provides a complete solution for protecting data across a broad set of business processes and is used by the customer to ensure security, privacy and compliance for personally identifiable information (PII) and financial account information associated with the Alnova banking system. Through the use of Voltage's unique Format-Preserving Encryption and Identity-Based Encryption technologies, Voltage SecureData Enterprise eliminates the traditional complexities associated with key management, and application modification. This results in an architecture that can be rapidly deployed in even the most complex environments.

Deployment considerations

The customer had considered several alternatives from data at rest solutions using symmetric key encryption to transport encryption. Until Voltage was considered none of these alternatives were able to meet the requirements of preserving data format, providing end-to-end security against directed threats and requiring minimal operational expertise within the regulated country.

Data protection approach	Strengths	Considerations
Encrypt data in transit; SSL	Familiar; well understood implementation	Protects only data in transit
Encrypt data at rest; storage encryption	Minimal application and process impact	Protects only data at rest
Application encryption; internal project with cryptography toolkit	Addresses risk factors;	Significant time, cost and implementation risk
Application encryption; Voltage data-centric security	Addresses risk factors; minimal application and process impact	Chosen alternative; low risk and low cost of ownership

The customer validated that the Voltage solution could meet these requirements with a proof of concept across lasting less than a week across three business processes. The Voltage Key Server and Management Console was deployed to work in conjunction with the Alnova application running in two data centers within the country with data residency laws. With minor changes to the application to add function calls to encrypt and decrypt data the customer was able to support the existing business processes. Importantly, data format was preserved such that application components running in the headquarters data center on an IBM mainframe and data warehouse environments continued to operate with no performance impact using encrypted data. A simplified view of the customer deployment is shown in figure 3.

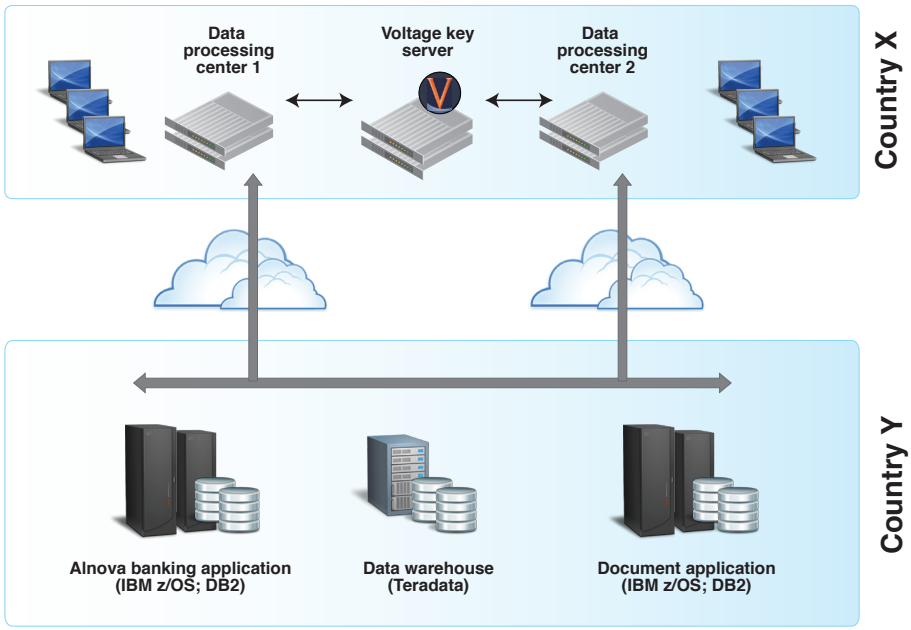

Figure 3. Deployment within headquarters and branch offices

The customer was able to move from proof of concept into production and now has adopted data-centric security as the mainstream method to protect sensitive data and meet compliance requirements. The policies, information security processes and data governance methods associated with this deployment have been adopted across the corporation and assured the customer that they will be prepared for the expected data privacy requirements associated with new European Data Protection law.

Extending the data residency solution across private cloud services

This innovative approach to applying key management and encryption to solve data residency conflicts and leverage shared infrastructure has become common with many customers, particular in the financial services industry segment. For multi-national corporations, the ability to address conflicting regulatory requirements provides increased business agility and offers control to the responsible business units while leveraging a common data-centric security architecture and uniformly enforced policy.

One international bank employed Voltage SecureData Enterprise in their private cloud environment. The information security and IT team adopted the Votlage Simple API to integrate format-preserving encryption across a broad range of applications and business units running on shared infrastructure in the company's private cloud. A simplified representation of the deployment is shown in figure 4.

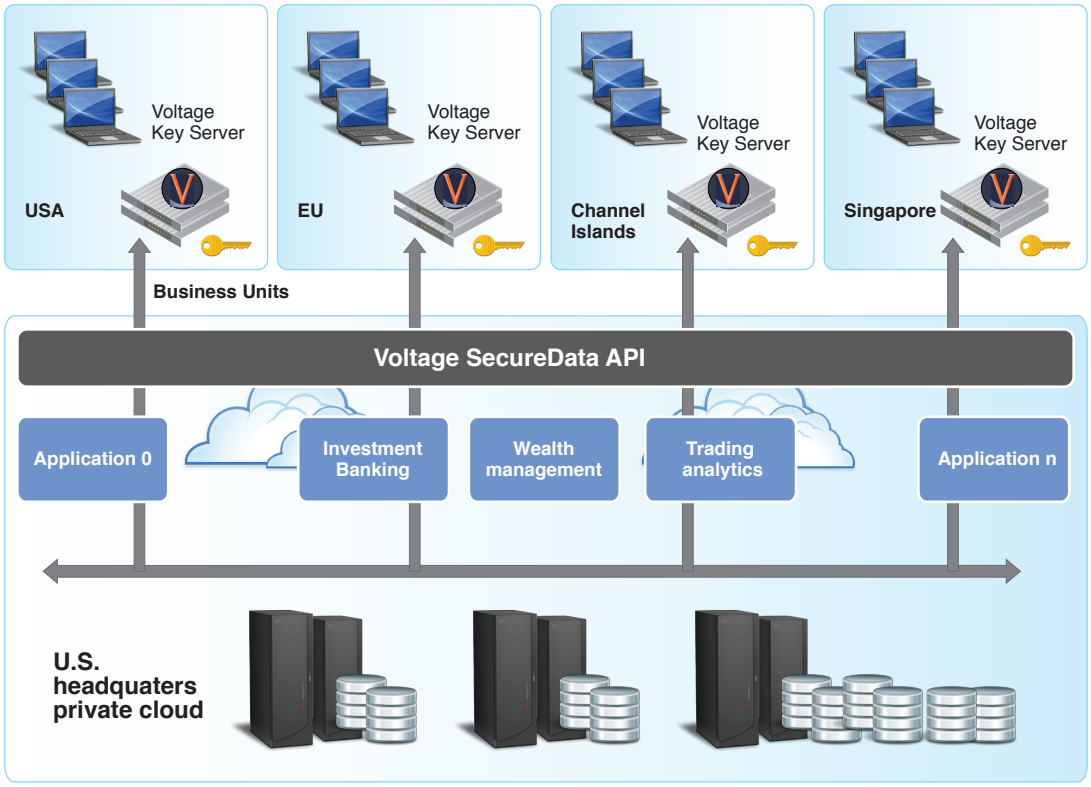

Figure 4. Voltage SecureData Enterprise offers business units control over data residency while enforcing consistent policy and streamlining compliance while leveraging shared private cloud services.

Deployment of the key servers in particular jurisdictions enables the business units to demonstrate compliance with data residency regulations without facing the cost and overhead required to replicate infrastructure and operational staff. The information security and IT organizations gain significant benefit as well, in that they focus their efforts on working with the development teams using a consistent API, allowing data-centric security to be deployed with minimal effort. Beyond the integration with the company's private cloud the company applied the Voltage solution to additional areas such as masking of production data for test and development processes as well as protecting information transferred to business partners and contractors. The same data-centric security architecture was applied across the entire solution set.

Summary

Voltage SecureData Enterprise provided the customer with the capability to grow new business while leveraging existing applications, infrastructure and business processes. The Voltage Data Security platform is a production ready solution that has been proven throughout the financial services ecosystem. The benefits include creating new business, increasing compliance efficiency and mitigating risk. The business outcome is increased business agility and competitive advantage.

Business Requirement	Result
Risk reduction	The IT organization and information security team dealt successfully with a diverse and hostile threat environment
Increased compliance efficiency	Streamlined audit process and business unit enablement
Increased business agility	Demonstrated the ability to enter new markets while meeting country specific laws
Cost effectiveness	Used existing banking application suite and shared infrastructure making the project feasible

About Voltage Security

Voltage Security®, Inc., is the world leader in providing data-centric encryption and key management solutions for combating new and emerging security threats. Voltage customers represent a wide variety of industries including payments, financial, insurance, medical, e-commerce. Offerings include Voltage SecureMail™, Voltage SecureData™, Voltage SecureData Payments™, Voltage SecureData Web™, Voltage SecureFile™ and Voltage Cloud Services™. The company has been issued several patents based upon breakthrough research in mathematics and cryptographic systems. To learn more about Voltage customers please visit voltage.com/customers.

References and further reading

1. Commission de Surveillance du Secteur Financier (CSSF); http://www.cssf.lu/en/laws-and-regulations/legislation/

2. New European Data Protection Law – A First Look; SNR Denton; http://www.snrdenton.com/news__insights/alerts/2011-12-09-data-protection-law.aspx

3. Voltage product portfolio; http://www.voltage.com/products

Copyright © 2012 Voltage Security, Inc. All rights reserved. All information in this document is subject to change without notice. This document is provided for informational purposes only and Voltage Security, Inc. makes no warranties, either express or implied, in this document.

Voltage Identity-Based Encryption, Voltage SecureMail, Voltage SecureFile, Voltage SecureData, Voltage Data Protection System and the Voltage Security Network (VSN), are trademarks of Voltage Security, Inc. All other company and product names may be trademarks of their respective owners.