



**Insurance Solution Series**  
**Protecting Customer Data**  
**Moving Beyond Compliance**

## Contents – Insurance Solutions Series

<b>Introduction.....</b>	<b>1</b>
<b>Securing Sensitive Customer Data.....</b>	<b>2</b>
<b>Business-Specific Security Concerns.....</b>	<b>4</b>
<b>Architecting Your Data Protection Plan .....</b>	<b>6</b>
<b>Balancing Conflicting Needs – Security vs. Usability.....</b>	<b>8</b>
<b>Key Take Aways .....</b>	<b>9</b>
<b>Customer References .....</b>	<b>9</b>
<b>Footnotes &amp; Links .....</b>	<b>12</b>
<b>Learn More/Contact Us .....</b>	<b>12</b>

## Introduction

Over the past few years, the insurance industry has experienced unprecedented levels of change that have made the requirement to secure customer and corporate information a regulatory necessity rather than an option. Today, the complex array of privacy regulations mandate that new protection strategies are implemented that go well beyond the requirement for NAIC and GLBA compliance. New regulations such as the Payment Card Industry Data Security Standard (PCI DSS), State laws such as Massachusetts CMR 217, US Federal privacy regulations such as HITECH, and emerging international regulations are explicit in their compliance objectives: *private data must be protected to permit safe harbor in the event of a breach*. While regulatory changes produce many opportunities, they also demand that insurance carriers contend with new levels of security risks, thereby increasing compliance costs. Of course, maintaining high levels of customer service requires that personally identifiable information (PII) and other sensitive data that drives insurance business process to be accessible by employees of the company, its brokers, and its partners.

Meanwhile, the protections required for privacy compliance are not the only driver to improve the control and protection of personal data. Well-funded criminal organizations have learned that institutions with significant databases of personal information are lucrative targets for motivated hackers. The Verizon Data Breach Report<sup>1</sup> illustrates how easy it is to attack systems, steal data, and monetize the information bounty through identity theft, fraud, and abuse of payment and banking data. Compared to other financial institutions, insurance companies often hold the *most* personal information. The exchange and accumulation of claims data, investigations, and collaboration with other firms result in enormous data warehouses – which, in turn, means more information is at risk of disclosure.

Because the corporate database must be continuously available for employees, partners, and other “controlled” sources of data access to do their jobs and to generate revenue for the business, simply locking the data away is not the answer. In addition, due to the unique structure of the insurance industry, insurance carriers must make corporate data available to users at remote locations over which the carrier has no visibility or formal control. These independent agents include staff who are not employees, many of whom also represent competitors. Data must also be available for continuous analysis, to establish risk positions and future product strategies that are critical to the company, its revenues, its ratings, and ultimately to its shareholders. Of course, with increasing pressure to reduce costs, insurance companies often outsource operations and services. Offshore IT management, software development, and the use of external analytical services are attractive options to bring new products to market more quickly and at a significantly reduced cost. This creates another dimension to the risk management challenge – to secure data that is distributed outside the business and into jurisdictions where controls and privacy laws may be less mature or nonexistent.

Insurance providers entrusted with sensitive customer information must find a way to protect its information assets *persistently*. This means as data is first collected, stored, processed, used in databases and applications, as well as when it moves within or outside the organization through its extended enterprise. All the while, the firm must keep pace with a continuously evolving business environment, where potential attacks on information are the norm, rather than the exception. Suffering a security breach can devastate a company's reputation, brand image, and destroy customer trust. Additionally, such a breach can negatively impact the company's stock price and require the firm to pay millions in reparations.<sup>2, 3, 4</sup>

*"We reviewed our data protection requirements for PCI compliance with our analyst contact at Forrester Research. They quickly encouraged us to look at a short list of vendors, which included Voltage Security. We selected Voltage Security, because they met our broad set of data protection requirements for both structured and unstructured data, and were able to address our cross-platform architectures with one common infrastructure. We implemented Voltage SecureData, Voltage SecureMail and Voltage SecureFile in about four months – enabling us to meet our PCI deadline."*

**Tim Masey**  
Infrastructure Security Consultant  
AAA The Auto Club Group

## Securing Sensitive Customer Data

Databases and applications play an essential role in the smooth operation of the business. The storage of, and access to, sensitive information such as policy and claims history, driver's license data, social security numbers, business risk information, medical records, accident case history, family status information, age and health statistics, smoking status, and other pertinent claim or risk profile data are an everyday necessity, and therefore must be readily available to ensure a high level of customer service. However, it must be recognized that the "pertinent customer data" is also sensitive personal information, and that databases are subject to the risk of security breaches – by both internal and external sources. In 2009, 64 percent of system breaches were performed by external hackers.<sup>1</sup> External attacks on databases have also become commonplace, with hackers employing sophisticated attacks to infiltrate enterprise networks and break traditional defenses such as intrusion detection systems and firewalls.

For this reason, many organizations may first react to the compliance mandates by considering encryption of the entire database or server. These approaches suffer from two major shortcomings:

- 1) Database-level encryption only protects the data while it is at rest, and data does not remain at rest for very long in dynamic organizations. The data is *unprotected* during database access, as well as when it exits the database on its way to the application. It is in the clear “on the wire”, leaving sensitive information open to insider compromise and external hacker abuse.
- 2) Server-level encryption does not permit separation of duties between database administrators and data owners – an aspect of nearly all current privacy regulations and a security best practice. Administrators need to manage systems, but do not require access to sensitive data.

With whole or “native” database encryption, as data is used by customer service employees, claims adjusters, billing agents, and other critical personnel as part of their daily activities, they essentially have full access to unprotected information. Moreover, as has been reported many times, the largest data breaches have occurred when the data was “on the wire” – while in motion and as a result of techniques like SQL injection attacks, which cause databases to deliver data to attackers or “sniffers”. Data that is only protected while at rest does nothing to thwart this common form of system compromise. Thus, only protecting the database at rest leaves significant data protection gaps that are easily exploited. A sound data security plan requires that sensitive data be protected in such a way that it remains usable.

Security professionals know that with each incremental person who is granted access, the data becomes inherently less secure. As illustrated in Figure 1, the multi-tiered network common to most insurance carriers makes data protection particularly difficult. When those outside the firm’s immediate control are added to the equation, the potential for data breach potential becomes more significant. For insurance industry security professionals, the standard business model creates difficult risk and compliance challenges.

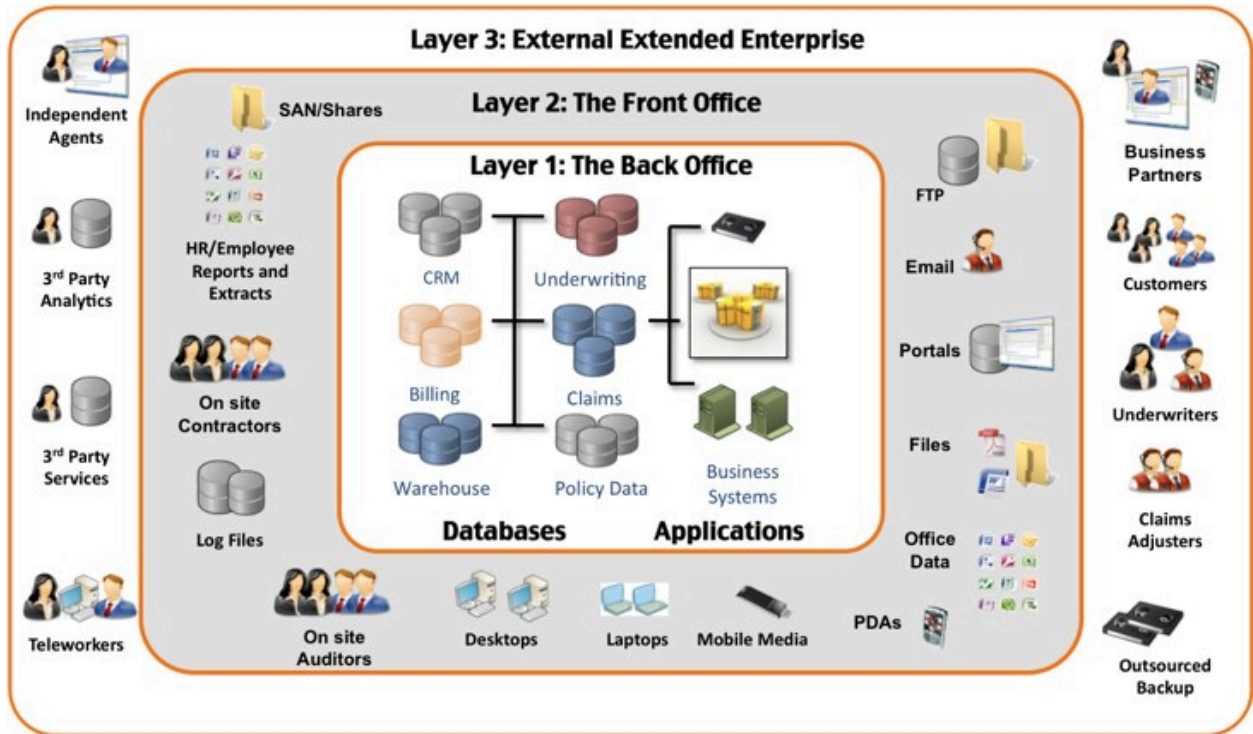


Figure 1: Data Protection in a Multi-Tiered Insurance Carrier Network

## Business-Specific Security Concerns

In addition to the database challenges discussed above, insurance carriers routinely use email as a preferred least-cost method of interaction with agents and customers. However, methods to protect email, whether to manage the risk of compromise, or to adhere to specific compliance regulations, must also minimize change and be easy to use. Independent agents will do business with carriers with whom it is easiest to work. The most money will be made by the quickest business interactions. Therefore, securing business communications must be simple, low impact, and above all, easy.

**Email Communications.** Email provides enormous business advantages, including the capability to communicate rapidly and efficiently with customers. Information on premiums, details about additional or alternate plans, claims/adjustments, billing details, and a host of other essential daily communications can be conducted instantaneously and with ease, using email. However, the communications between employees and the company's agent or broker dealer network often contain social security numbers, policy information, medical diagnoses, and other forms of sensitive customer information. Email sent between the company and external partners passes through an average of four intermediate servers between the sender and the receiver – exposure points and “air gaps” which can be compromised by hackers to intercept the communication. Despite its many benefits, email is

an inherently insecure medium which presents an unacceptable level of risk for the transmission of sensitive customer information. Email is also classified as discoverable content from a legal perspective. It is therefore imperative that when email is secured, e-discovery processes are not impacted. With e-discovery involving many legal parties, delays in the discovery processes or the inability to recover insurance firm correspondences can lead to the unnecessary escalation of costs and legal complexities.

**Partnerships and Alliances.** Developing partnerships and alliances help firms survive these difficult times. However, these same partnerships also increase the number of sensitive communications that are sent outside the organization, and therefore the number of places where data is at risk from accidental loss or malicious attack. Many partnerships mandate the sharing databases, or provide access to sensitive information by external participants in a business process. Granting database access to partner organizations requires that sensitive data leave the direct control of the organization that "owns" that data. It is therefore essential to determine how to protect that data while in the hands of external staff – perhaps by limiting access to a need-to-know basis, or by controlling the process under central policy when data is required in full live form.

**Direct and Internet-Based Sales.** While the Internet enables the company to directly interact with the end user, foregoing the traditional agent, this new channel also presents extraordinary security challenges, as sensitive customer data flows directly through the company's web portal. An essential component to the company's end-to-end data security plan must include this channel, which is highly vulnerable to hackers and a wide range of other Internet-based threats.

**Automating Payments to Simplify Customer Relationships.** To retain customers and simplify collections, a growing number of insurance firms are using automated credit card processing to accept direct payments and offer flexible payment methods. Along with the many benefits of this come associated risks and compliance requirements. Credit card details are a lucrative target for hackers, and data breaches of this type are on the rise. PCI DSS is a mandatory compliance requirement for any merchant – including insurance carriers – that accepts credit card payments. Carriers must ensure that investment in data protection for other privacy regulations does not incur substantial re-investment costs to meet PCI DSS. Given the rigor of PCI audits, audit costs must be kept at a minimum to ensure a positive return on investment for the new payment acceptance processes.

**Expansion into Foreign Markets.** Foreign expansion holds tremendous opportunity for growth and is therefore an important component of the company's strategy. However, each country has its own standards for data security – and many lesser-developed countries are severely lacking in formal security standards. These present an additional layer of risk for data theft. Moreover, many countries, including the United States, have dramatically increased the regulations for private information that crosses country borders, as well as the associated fines when a breach occurs.

**Direct Customer Interaction and Support.** Once a customer has been enrolled into a business service or under an insurance policy, providing a high level of customer service is essential to maximize customer satisfaction and minimize customer churn. It also creates an intimate customer relationship, from which new products and services can be sold. Of course, such a relationship relies on personal data. Whether this is handled through agent communications or via direct interactions with customers – through e-statements, email-based claims processes, interactive e-forms, or social media – the security of customer information is an absolute necessity, and the management of data breach risk must be a top priority.

## Architecting Your Data Protection Plan

When designing your organization's data protection strategy, it is essential to consider all aspects of the data, including who can access it. The following questions will help determine the extent to which the organization's data must be protected:

**Where is the sensitive data?** A simple survey to determine which lines of business have which kinds of regulated data, versus the data items covered by specific regulations, is a good first step to determine the risk and exposure – by system, process, and business unit.

**How sensitive is the data?** For the vast majority of insurance organizations, most of the data is extremely sensitive – due to regulatory compliance issues and potential legislative action, as well as the enormity of the ramifications, should that data be breached. Prioritizing the systems that have the largest amount of regulated data, the most frequently accessed data, or the largest amount of shared sensitive data will often be the top targets to address with a data protection plan. However, sometimes organizations forget that the vast majority of data may not be in live production systems – it may be live data that is utilized by development, QA, or an outsourcer to build and test applications. The data that is most vulnerable to compromise is frequently in systems that are afforded the least thought.

**Who will require access to the database?** Regardless of company size, many different people – from an array of departments – require access to information stored in corporate databases to conduct their normal job responsibilities. Security best practices dictate that access should be dependent upon the person's role – but this is often not the case. Sometimes people will be categorized into large groups which reflect broad permissions. Some of these groups may be located both locally and remotely, and may include independent agents. When this is the case, other questions come into play, including the physical security of the office where the agent is located, as well as the security capabilities of the computer that is used to access the data. Is the computer updated with the latest operating system patches? Does it have current, top-rated security software? Another important consideration is whether or not the data from other carriers is accessed using the same computer.

**Will different people require different levels of database access?** The answer to this question is “yes” for nearly 100 percent of all companies, regardless of their size and industry in which they do business. Firms often add access to information over time, but fail to remove it when employees move to new roles or change jobs. The ability to control access under these conditions is an excellent way to manage risk.

**What and how much data do they require?** Data access naturally varies greatly by job responsibility. Front office personnel may require only minimal access, while those involved in policy underwriting may require close to complete access. Claims adjustment agents and others may require access that is somewhere between these two extremes. Moreover, claims adjustment agents will likely require access to sensitive data fields such as social security and policy information that are not required by others in the organization.

**How will appropriate access levels of database be monitored and managed?**

Absolutely essential to the security of the company’s data is the ability to provide appropriate levels of database access to each person and organization, based on their needs. Providing more access than is truly necessary – even to one person – degrades the overall level of security of the data.

**Will data be shared with partners or other external organizations?** Data sharing in the insurance industry is a business requirement. Sharing customer data with external organizations, including partners and brokers, as well as with internal and external agents, is essential to the day-to-day operations of the business. Furthermore, sharing information with government auditors is critical for regulatory purposes.

**How will data be shared outside the organization?** Are whole files or just select data elements shared? Will it be emailed to partners or external adjusters? Do agents require the flexibility of email communications with their customers?

**Will all development, QA, and other database work be performed by employees, or will some activities be outsourced?** The outsourcing of functions such as database development and QA activities are an essential part of the business strategy for many companies, in an effort to decrease costs. Oftentimes, outsourced work is performed off-shore, where technical expertise is in abundance and rates are low. However, outsourcing of any type requires that sensitive data leave the direct control of the organization. Determining how to protect that data while in the hands of others is a critical issue for many companies.

*“Data encryption was an integral part of our overall enterprise data protection strategy. We were looking at encrypting outgoing e-mail with sensitive content, as well as encrypting sensitive data elements in structured data stores. We also wanted to be sure that the data remained encrypted end-to-end, and that deployment did not cause unreasonable performance drag. Voltage SecureData and Voltage SecureMail had exactly the features and functions we were looking for. Selecting Voltage Security quickly became a no-brainer.”*

**Director of IT Security Strategy & Planning**  
Fortune 1000 Insurance Provider

## Balancing Conflicting Needs – Security vs. Usability

When it comes to sensitive data, security and usability are typically considered to be opposing ideals, thereby forcing companies to choose one or the other. Security inherently weakens with every person who is provided database access, and email transmission of data carries the extraordinary risk that the transmission will be intercepted, therefore compromising the data. Furthermore, trusting external individuals and companies with sensitive data is inherently at odds with sound security practices. However, business reality dictates that internal and external users *must* have access to the data to maintain smooth, efficient operations, and email communications are a fact of modern business.

Voltage SecureData™ delivers a comprehensive solution for data encryption, tokenization, de-identification, and masking – at run-time, as well as for test and QA data generation – that does not require costly and time-consuming data schema and data format changes in existing systems, including legacy mainframes. Voltage SecureData ensures that sensitive data is protected persistently – as it is collected, used, stored, and distributed to less controlled environments – regardless of infrastructure or application format requirements. Voltage SecureData ensures that customer data, claims information, and payment transaction data will remain safe, regardless of where it resides – including backups – on an end-to-end basis over the information lifecycle. With fine grained control over which user and application can view each portion the data, Voltage SecureData can remove the risk of accidental access, while minimizing the scope of compliance audits. Most importantly, Voltage SecureData protects data end-to-end – while it is “in motion”, as well as when it is at rest in the database. With Voltage SecureData, entire systems can be protected within weeks of purchase, rather than months for competing solutions. Even if a claims processing or payment infrastructure is a complex arrangement of legacy mainframe, contemporary java, or a mix of modern systems like Oracle databases, third-party processes, or complex

CRM systems such as PeopleSoft, Voltage SecureData can quickly provide the protection necessary for compliance, and control access on a fine-grained basis.

Likewise, Voltage SecureMail™ employs proven encryption technologies for sensitive email communications. Voltage SecureMail helps achieve and maintain regulatory compliance and enforce best-practice email protection, without disrupting normal business operations, or conflict with e-discovery or email sanitation and monitoring processes. Voltage SecureMail effectively mitigates the risk of email security breaches by providing end-to-end security for email and mobile messaging. Whether embedded in the email, or included in attachments of any size, policy details, health and medical information, and other essential customer data can all be transmitted securely, just as easily as sending standard email. Voltage SecureMail works inside and outside the company, so adjusters, customers, and agents can communicate with one another, with confidence that their sensitive communications will remain secure. Voltage SecureMail is easy to use, whether it is employed for secure two-way communications, or multi-party correspondence.

## **Key Take Aways**

The rapid changes occurring in the insurance industry present enormous opportunities for companies to develop new partnerships, expand to new markets, and achieve a more direct relationship with their customer base. However, these opportunities come with unprecedented risks to the security of their company and customer data, and are subject to a variety of international regulations. Suffering a security breach can be devastating to the company's reputation and brand image, and lead to regulatory or legislative action, due to industry regulations and emerging encryption laws.

Insurance providers entrusted with sensitive customer information must ensure its protection, regardless of where it resides. The organization must first consider where and how the data will be used, then implement the technology that blends the need to maintain proper data security with the business need to maintain usability of the data. This approach enables companies to protect sensitive customer data while continuing to meet the business needs of the organization.

## **Customer References**

Providing robust security solutions for more than 80 major insurance carriers throughout the world – securing their databases, as well as the communications of their approximately two million brokers, agents, and customers – Voltage Security understands the unique and often complex security issues you face. As a global leader in information encryption, Voltage Security possesses the expertise to help you maximize the efficiency of your business

operations, while ensuring that your sensitive customer data and business information maintains the highest level of security. With our knowledge and expertise in providing security solutions for businesses like yours, Voltage Security understands the specific complexities of your dynamic business and can help you navigate through them, to maintain the level of security you require – even in your rapidly changing business environment.

Customer	Data Protection Needs	Voltage Security Solution
<p><b>AAA The Auto Club Group</b> <i>Detroit, MI</i> USA</p>	<p>PCI Compliance – Protection of Credit Card numbers in 30 applications. Needed a common solution across Windows, Open Systems, and Mainframe z/OS</p>	<p>"We reviewed our data protection requirements for PCI compliance with our analyst contact at Forrester Research. They quickly encouraged us to look at a short list of vendors, which included Voltage Security. We selected Voltage Security, because they met our broad set of data protection requirements for both structured and unstructured data, and were able to address our cross-platform architectures with one common infrastructure. We implemented Voltage SecureData, Voltage SecureMail and Voltage SecureFile in about four months – enabling us to meet our PCI deadline."</p>
<p><b>Fortune 1000 Insurance</b> <i>Chicago IL</i> USA</p>	<p>Protection of PII data at rest and in use for 180 applications and the privacy of email communications with outside business partners, including broker dealer communications.</p>	<p>"Data encryption was an integral part of our overall enterprise data protection strategy. We were looking at encrypting outgoing e-mail with sensitive content, as well as encrypting sensitive data elements in structured data stores. We also wanted to be sure that the data remained encrypted end-to-end, and that deployment did not cause unreasonable performance drag. Voltage SecureData and Voltage SecureMail had exactly the features and functions we were looking for. Selecting Voltage Security quickly became a no-brainer."</p>
<p><b>RLI</b> <i>Peoria, IL</i> USA</p>	<p>Protection of PII at rest and in use, including from business partner organizations</p>	<p>"We needed a solution that protects information securely and can be deployed rapidly – with as little impact as possible to the existing environment. We started talking to Voltage Security, did a competitive evaluation and were up and running within six weeks."</p>
<p><b>National Life Insurance Company</b> <i>Montpelier, VT</i> USA</p>	<p>Provide secure email communication with its network of over 11,000 agents throughout the United States</p>	<p>"We looked at traditional PKI solutions but there was no way we wanted to deal with that nightmare of key management. Then we looked at web mail solutions but we did not want to create the management issues associated with working with a third-party data center for archived email. When we found Voltage Security we recognized immediately the benefits of their innovative approach to encryption."</p>

<p><b>Intact Insurance Company of Canada</b> <i>Toronto, ON Canada</i></p>	<p>To protect the privacy of communications with outside business partners, including broker dealer communications</p>	<p>“Although we looked at the legacy secure email solutions before selecting Voltage Security, they won our business based on simplicity and ease of use for the end user. The low impact on our IT operations and ability to satisfy our complex requirements were also determining factors.”</p>
<p><b>Integro Insurance Brokers</b> <i>New York, NY USA</i></p>	<p>To provide strong policy-based data protection for the trusted transmission and storage of email communications</p>	<p>“We required a solution that could accommodate a diverse user base, address the dynamic nature of our business, and provide strong security while keeping costs low. Voltage SecureMail was the only choice.”</p>

## Footnotes & Links

<sup>1</sup> [2009 Data Breach Investigation Report. Verizon Wireless, Incorporated. 2009.](#)

<sup>2</sup> [Press Release. Information Commissioner's Office \(ICO\). 2010.](#)

<sup>3</sup> [Statement of Breach. 2010.](#)

<sup>4</sup> [Security Report. Datalosdb.org. 2010.](#)

## Learn More/Contact Us

[Learn more about protecting sensitive communications](#) across your organization and business partner network. Alternatively, for a direct response, please [email us](#) and we will contact you the next business day. We also invite you to visit [www.voltage.com](http://www.voltage.com)