



## Making Encryption Work

Protecting customer and employee data across systems, supply chains, and business partners

**CxO Information Series**

Copyright © 2008 Voltage Security, Inc. All rights reserved.

All companies need customer information – the more they know, the better their ability to deliver the right products and services and build stronger customer relationships. Yet this desire for information introduces risks, especially when customer or employee data falls into the wrong hands – either by mistake as in the case of Bank of New York Mellon, which managed to lose 12.5 million customer records, or by criminals intent on stealing identities, as in the case of Hannaford where 4.2 million credit card numbers were stolen from internal systems.

Encryption is an approach to combat the risk of exposure of sensitive data. However, encryption technology has historically been very difficult to use and manage, particularly for non-technical end users. Typically security approaches that are difficult to use fall into disuse, increasing the risk of data breaches.

Another factor that has made encryption difficult to deploy in commercial implementations is the need for scalability – information is now shared not just within organizations but also with business partners, consultants, supply chains, and other service providers. Existing solutions have required massive administration in order to manage all the keys necessary to protect content inside and outside the organization.

A different encryption approach is needed: one that focuses on the data itself, ensuring protection of that data no matter where it goes, without requiring administrators, end users, or architects to learn and manage complex cryptographic systems.

Voltage Security provides innovative solutions to protect customer, employee and corporate information, wherever it lives: in databases, business applications, email, documents, and portals. Voltage has helped insurance, retail, banking and healthcare companies protect their most sensitive data.

## New Standards for Security

Voltage Security has developed new cryptographic approaches that can be used to protect data inside and outside an organization. These unique technologies overcome the limitations of scale, usability and ongoing operational costs associated with earlier approaches.

[Identity-Based Encryption](#) (IBE) dramatically simplifies the ability to encrypt emails, files and documents, providing ease-of-use for non-technical users, huge scalability (e.g., one implementation has over 600,000 internal users sending messages to their business partner network) and, on average, up to five times lower operational costs than other encryption approaches such as PKI.

### *Customer Example*

*ING Canada recently chose the Identity-Based Encryption approach to secure its email communication with 16,000 broker/dealers. The system is deployed for use across all of its business units and has been architected to support over 7,000 ING Canada employees communicating with outside recipients. According to Minaz Sarangi, VP of Architecture, “The technology is the easiest to maintain. The total cost of ownership in our case over five years was the lowest.”*

[Format-Preserving Encryption](#) (FPE) enables the persistent encryption of credit card numbers, Social Security Numbers, and other PII data while maintaining the underlying format of the data. Through FPE, data can be encrypted in databases and applications without changing schemas

or formats, enabling remediation in record time. With FPE, it is now possible to protect information rapidly and cost effectively—without changing your business processes.

### *Customer Example*

*A large national retailer with over 4,000 retail locations, processing over 10 million credit cards a day, faced an upcoming PCI audit deadline. Working with a leading system integrator, this organization was able to implement Voltage SecureData in under two months, five times faster than conventional approaches to data protection. Another company, a top ten US insurance provider working with Accenture, will use FPE to protect 180 applications, including business applications such as PeopleSoft, with little or no modification to underlying databases or applications.*

## Solutions for Data Protection

Voltage solutions incorporate multiple products which integrate with an organizations disparate environment to provide comprehensive data protection:

- Voltage SecureData – Protects structured data such as credit card numbers and social security numbers inside databases and applications
- Voltage SecureMail – Protects email communication inside and outside an organization, including mobile email.
- Voltage SecureFile – Protects files and documents on desktops, network shares and portals such as Lotus Quickr.
- Voltage Security Network – An on-demand SaaS system that can protect email, files and documents without the need to deploy infrastructure.
- Voltage Key Management – All Voltage solutions are built on the unique Voltage Key Management architecture, which enables secure administration of encryption keys across users, groups, systems, and applications.

## About Voltage Security

Voltage Security, Inc., is an enterprise security company, providing innovative solutions that protect employee and customer data wherever it goes—via email, documents, or stored in databases and accessed by business applications. Voltage's solutions stop identity theft, enable fast compliance with PCI regulations for protecting sensitive data, reduce risks associated with developer, outsourced and off-shore environments, and protect the privacy of communications with employees, business partners and consumers.

Voltage solutions are in use at more than 580 enterprise customers, including some of the world's [leading brand-name companies](#) in banking, insurance, retail and healthcare such as ING, Kodak and Kaiser Permanente.

For more information please visit [www.voltage.com](http://www.voltage.com).