Voltage security

WHITE PAPER

Business Case for Voltage SecureMail Mobile Edition

Introduction

Mobile devices such as smartphones and tablets have become mainstream business productivity tools with email playing a central role in communications. Voltage SecureMail Mobile Edition allows enterprises to leverage this technology trend by delivering secure email communications from mobile devices with a simple user experience that ensures widespread adoption.

Organizations can:

- Meet privacy mandates and regulatory requirements for sensitive email on mobile devices.
- Improve productivity of business users and customers with secure email communication via mobile devices.
- Ensure end-to-end protection of sensitive email across desktops, laptops and mobile devices.
- Extend existing investment in security and compliance solutions such as DLP, archiving, mobile device management (MDM) and e-discovery.

Securing Mobile Email Communications

Reports of data breaches have become a commonplace occurrence as enterprises struggle to protect critical business information. The threat environment is broad in scope, ranging from malware attacks to SQL injections, from insiders to well-funded cybercrime organizations. Yet enterprises need mobile access from anywhere to get business done. As a result of widespread mobile usage and ubiquitous access, the attack surface of enterprise data has increased. The risks associated with these threats must be mitigated while meeting compliance requirements cost effectively through a mobile security solution that enables business – not restricts it.

Business needs for secure mobile email can be summarized as follows:

- Ensuring compliance with internal, government and industry regulations for employee and contractor email communications.
- Enabling exchange of sensitive data with business partners and customers, while providing IT with granular policy control and integration with existing security process such as audit preparation, DLP, archiving, and e-discovery.
- Reaching both employees and customers on their mobile device of choice with a simple and familiar user experience. The experience should build confidence, brand loyalty, and ultimately competitive advantage.

Voltage SecureMail Mobile Edition for Real-World Applications

Many businesses have aggressively adopted mobile devices, yet they face stringent industry and government regulatory requirements. Voltage SecureMail Mobile Edition represents an opportunity to drive further engagement with their customers as well as meet demands for encrypted email for specific business processes. The table below illustrates some sample business use cases for financial services, and some of the capabilities delivered by the Voltage SecureMail Mobile Edition.

SECURE COMMUNICATION - BUSINESS USE CASES	VOLTAGE **SecureMail** MOBILE EDITION CAPABILITIES
Affiliate agents process claims with mobile devices, requiring protection of PII data while maintaining a structured secure email workflow with corporate customer service teams.	Encrypted emails and attachments are delivered to the client's existing inbox in the iOS email client on their iPad or iPhone, and decrypted in the normal email workflow for reading. Pre-set policy enforces secure communications between the parties.
Exchange of sensitive legal documents among acquisition teams, outside counsel and investment banking advisers.	Internal, legal and investment teams depend on their preferred mobile devices to be more productive. Granular policy controls leverage the corporate directory for authentication and ensure compliance with policies.
Delivery of fund transfer authorization and supporting documents to purchasing and accounting teams at commercial business partners.	Voltage SecureMail Mobile Edition encrypts mobile email communications that contain sensitive data between employees and their business partners, following policies defined by IT to meet regulatory requirements.
Executive staff members use secure email to review board packages and financial results with board members.	Email communications with sensitive information originating from a desktop or laptop computer are encrypted by Voltage SecureMail. Voltage SecureMail Mobile Edition extends the same familiar, easy user experience of decrypting and reading emails to mobile devices. Board members can respond to time-sensitive communications and review documents securely while on the road.
Banking customer representatives use secure mail to deliver mortgage documents to customers with mobile devices as well as desktop systems.	Customer service representatives are able to accelerate the mortgage initiation process by sending encrypted emails with attachments generated from their desktops to their clients to decrypt and read on their mobile devices while on the go. Pre-set policies ensure compliance with mandates and regulations.

Unmet Needs for Securing Mobile Emails

Traditional approaches to securing email communications on mobile devices are inadequate and hard to use. Each has forced a trade-off between business productivity and IT control. Each requires complex configuration, administration and provisioning, along with multiple end-user steps to access encrypted email and attachments.

SUMMARY OF UNMET NEEDS FOR SECURING MOBILE EMAILS:

APPROACH	LIMITATIONS	BUSINESS IMPACT
Web mail	• Key and message stores to manage • User experience inhibits productivity • Messages expire, breaking processes such as e-discovery • Enterprise must manage mail-related data • No access to existing contacts on the device • Users don't like it - cumbersome browser experience, clunky and slow	• Lack of adoption by end users • Compromised business productivity • High cost of ownership • Complex and costly compliance process

SUMMARY OF UNMET NEEDS FOR SECURING MOBILE EMAILS (CONTINUED)

APPROACH	LIMITATIONS	BUSINESS IMPACT
Symmetric key systems	• Complex key management • Active code in messages / PDFs • System complexity limits reliability • Time-consuming and expensive backup and replication required • Difficult to manage across multiple data centers and/or geographies	• Lack of adoption by end users • Compromised business productivity • High cost of ownership • Complex and costly compliance process
Application containers	• Does not protect email sent to external recipients • Policy framework and controls are specific to mobile users only, not desktop users • Different user experience for personal and corporate email • Does not protect the data itself – data at risk if container is breached	
PKI-based mobile applications	• Not business friendly (e.g., no ad-hoc usage) • User adoption requires configuration, certificate provisioning • Incompatible with many email clients (e.g., Gmail, Yahoo, Android) • Administrative burden to handle key management and certificate revocation • Poor support for group communications	

To make mobile email both secure and productive, a new approach with the following characteristics is needed.

- No additional layers of containers to protect data, rather protection of the data itself until the moment of use by the authenticated user.
- A solution that meets compliance immediately, provisions policies separately for internal and external users, all without extensive management and customization.
- Non-disruptive encryption that extends from existing email and business workflows without major impact to the systems, processes and people.

Data-centric Security for Mobile Email Communications

Voltage Security has established a track record in data protection for all enterprise data including emails. The Voltage SecureMail platform delivers secure email at scale to organizations such as Wells Fargo, Manulife Financial and AAA, cutting operational costs and meeting compliance requirements efficiently.

Voltage SecureMail Mobile Edition extends the platform to bring email security to the iOS, BlackBerry and Android platforms, with the control that IT operations demand, and with the familiar mobile experience that users expect. The solution allows corporate policies to be extended to mobile devices, assuring compliance, security and privacy of sensitive data with proven encryption technologies. Global scale deployments are simple and less costly to manage and administer with Voltage stateless key management approach. Voltage SecureMail Mobile Edition integrates with major mobile platforms, providing a simple app store install that can be rapidly deployed internally and externally in highly distributed organizations.

Figure 1. Mobile email data protection for the enterprise.

For Users: Familiar Workflow Increased Productivity and Security

Voltage SecureMail Mobile Edition offers uniform security and policy controls across desktop and mobile environments, but with user interfaces that are tuned to each specific mobile platform. The look-and-feel of the process matches the look-and-feel of the native email client on the device.

Email is delivered to the recipient's inbox in the existing email client. Users only need to open an attachment to decrypt a secure message. The reader screen in the Voltage app looks and behaves just like the native email client without replacing it. No forwarding of messages to a proxy email address and waiting for a response email with a link to click and view your message. No "notification email" and "secure pickup center" with separate webmail inbox, which does not include access to your existing contacts, just for encrypted emails.

Sending is equally simple. It's just two taps - tap to open the app, and tap to compose a message. The compose screen in the Voltage app looks and behaves just like the native email client. There's no need to launch a mobile browser and login to a separate web-based "message center" for just the encrypted email.

The setup process is also streamlined. If the user has previously enrolled in Voltage SecureMail, the user installs an app and decrypts a secure message. Doing this will automatically register the user's email account with the app. If the user is decrypting the secure message for the first time, additional enrollment steps are needed. Voltage does not require an administrator to manually enroll new users prior to user activation. Users do not need to worry about how to configure and manage PGP or S/MIME keys or configuration files on the device. They also do not need a physical network connection – the whole process functions "over the air" with any wireless connection.

Compose screen on an Apple iPhone 4

Compose screen on an Apple iPhone 4 ***with Voltage SecureMail***

Figure 2. The Voltage SecureMail interface mimics the native email client.

The first result is improved business productivity. Business users are able to take advantage of familiar workflows and user interfaces to deliver and receive sensitive information and data subject to privacy regulation. Access email addresses for people and groups via integration with contact list and Exchange global address list enhance productivity, while IT can maintain policy control for compliance. The simple user interface will improve the adoption of email encryption, which

will improve overall security and compliance of sensitive data.

The second result is improved customer satisfaction. With an easy-to-use interface, enterprises can confidently drive customer engagement with secure email communications on major mobile platforms. Privacy concerns are reduced while building customer relationships with secure, convenient communications.

For IT: Scalable, Easy-to-Manage Email Security

Voltage SecureMail Mobile Edition offers IT operations a management system that supports consistent policies across all environments, integrating with existing corporate authentication and authorization systems. Figure 3 illustrates a typical deployment of internal and external mobile users.

Unlike legacy key management solutions that require complex replication and scaling architectures, Voltage provides stateless key management that enables on-demand key generation and re-generation without an ever-growing key store. The result is a system that can be infinitely scaled across distributed physical and logical locations with no additional overhead.

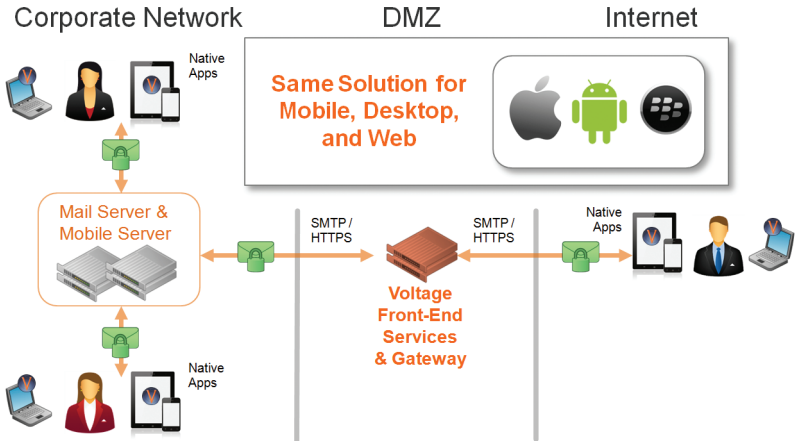

Figure 3. Deployment of Voltage SecureMail Mobile Edition.

To enable reuse of existing infrastructure investments, the Voltage Key Management Server offers a federated authentication model. It integrates with existing identity management or credential stores including Microsoft Active Directory. Voltage can simultaneously support multiple forms of authentication and enrollment for different user populations. Integration with existing messaging flows and processes has also been built in to the architecture. Customer processes such as DLP, archiving, e-discovery, compliance reporting, and audit preparation are fully supported.

Voltage Secure Mail Mobile Edition management system brings the following business value to enterprise IT organizations:

- **Cost reduction through efficient compliance process and operation**
  With end-to-end email data protection, enterprises meet federal, state and industry regulatory requirements with minimum operational costs. Voltage analysis of customer total cost of ownership have shown overall cost savings of up to 70%.
- **Mitigate risk of data breach**
  External attackers, organization insiders and outsourcing partners present continuous threats. Brand damage, litigation, lost business and customer disaffection present significant risk that is mitigated with Voltage SecureMail Mobile Edition. End to end encryption ensures that sensitive data is protected from inadvertent data loss as well as direct attacks – wherever the data travels and resides.
- **Optimized integration with enterprise email infrastructure and processes**
  Email-related business processes, such as e-discovery requests and the retrieval from email archives, must continue to function effectively and efficiently across mobile and desktop infrastructure. With Voltage, IT can manage all data protection policies and processes consistently across the enterprise.
- **Unrestricted ability to scale data protection and grow elastically with the business**
  The stateless key management employed with Voltage SecureMail Mobile Edition has been proven in the most demanding environments. Worldwide customer deployments consisting of hundreds of thousands of internal users, and millions of external users, are routine among Voltage's large enterprise customers. High availability deployment and integration with business continuity and disaster recovery processes are easily achieved.

Conclusion

Mobile email is now a mainstream business productivity tool. Voltage SecureMail Mobile Edition brings a data-centric approach to securing email communications accessed by devices like smartphones and tablets, bringing users the simple and familiar email experience they expect. Organizations can now meet privacy mandates and regulatory requirements, improve user productivity, and build stronger customer relationships, with secure and cost-effective email communications.

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**.

Voltage Security, Inc., Voltage Identity-Based Encryption (IBE), Voltage Format-Preserving Encryption (FPE),Voltage Page-Integrated Encryption (PIE), Voltage Identity-Based Symmetric Encryption, Voltage SecureMail, Voltage SecureMail Mobile Edition, Voltage SecureMail Application Edition, Voltage SecureMail eDiscovery Compliance Tool, Voltage SecureMail Archive Connector, Voltage SecureMail Statement Generator Service, Voltage SecureMail Cloud, Voltage SecureData, Voltage SecureData Enterprise, Voltage SecureData Payments, Voltage Secure Stateless Tokenization (SST), Voltage SecureFile, Voltage SecureData Web, and Voltage Cloud Services are registered trademarks of Voltage Security or are trademarks and service marks of Voltage Security, Inc. All other trademarks are property of their respective owners.

v05062013