SECURE CONTENT APPLICATIONS

Voltage Encryption

Overview

Voltage Encryption provides an identity-based solution for inline encryption of email messages and attachments. A one-time identity registration allows users to read encrypted messages by simply supplying a password, with no need to exchange keys. Encryption/decryption takes place on the Sentrion appliance, with no software required on end-user PCs or devices.

Audience

Enterprises that need an easy-to-use, email encryption solution for regulatory compliance, client confidentiality, secure delivery of financial information to clients, and other purposes.

Key Features and Functionality Overview

Voltage Encryption enables Sentrion to perform inline, policy-based encryption of email messages and attachments. Because the system generates encryption keys on the fly based on user identities, there's no need for senders and receivers to exchange encryption keys. You decide what information will be used to identify individual users—such as an email address—and users supply the ID a single time. Once registered in the system, users can read any encrypted email addressed to them simply by supplying their ID and password.

A Voltage-enabled Sentrion appliance can be deployed:

- At the network edge for in-stream decryption of inbound messages
- At the network edge for in-stream encryption of outbound messages
- In the policy layer to perform encryption based on specific email and user policies

In the policy layer, messages can be flagged for encryption based on virtually any aspect of the message, including the envelope, headers, body, and attachments. When an encryption policy is triggered, the original message is encrypted and converted to an attachment on a new message. Once the user supplies the correct password, an embedded JavaScript application verifies the user's identity over the web and decrypts the message.

For applications that don't demand end-to-end encryption, IT administrators greatly prefer Voltage technology because it doesn't require installing and managing encryption software on end-user desktops. Users enjoy the same benefit, because Voltage allows them to receive and read encrypted messages on their Blackberries (with a plug-in), iPhones and other mobile devices that don't have encryption software installed. Even better, users don't have to exchange keys in order to send and receive encrypted messages.

The business as a whole also benefits from the ease of enforcing encryption for communications that may have gone unprotected in the past. Encryption can be applied automatically based on email content and routing policies, without the need to rely on end-users to tag messages for encryption or run a PC-based encryption client. End-user transparency and policy-based automation promote the use of encryption for all kinds of sensitive communications—not just top-secret financial and legal messages.

Increasingly, companies are realizing that something as simple as a clear-text business plan emailed to an employee's home email address can put the company at serious risk. Voltage Encryption closes the security gap with a solution that's easy to use every day, on any message.