Technology Brief

FOR IT PROFESSIONALS

Orion Labs

Research & Development

February 2014

Email Encryption Made Easy

Based on the growing volumes of confidential and sensitive information traversing networks on a daily basis, regulatory bodies and firm executives have become concerned with ensuring that messaging is protected from unauthorized viewing. Regulations such as Sarbanes-Oxley (SOX), PCI, HIPAA, GLBA and others have been introduced to mandate that email messages containing sensitive or confidential data are handled securely. Email encryption has emerged as a vital aspect of an overall email security solution, to secure confidential data while continuing to allow the free flow of communications between colleagues, customers and partners.

Follow Orion on LinkedIn:

http://www.linkedin.com/company/1681643

The Solution: Seamless Email Encryption from WatchGuard®

WatchGuard XCS SecureMail Email Encryption (XCS SecureMail) technology, powered by Voltage, provides easy-to-use, business-class encryption to enable organizations to securely transmit and receive private/sensitive data. This encryption solutions, available as an add-on subscription for all WatchGuard XCS appliances, provides transparent, policy-driven email encryption, supporting the encryption of large messages up to 100 MB.

The transparent nature of XCS SecureMail adds to its ease of use. The WatchGuard XCS data loss prevention engine identifies outgoing messages that meet pre-defined polices for confidentiality and automatically encrypts messages with no additional action required by the sender. Encrypted messages are sent as HTML attachments and are delivered directly to the recipient who can then decode and view the encrypted messages using any web browser (including mobile devices).

How XCS SecureMail Encryption Works

1. A sender from within the organization triggers an email.
2. The email is processed within the organization's email environment and is then routed to the WatchGuard XCS appliance for scanning.
3. The email passes through the XCS data loss prevention engine's pattern and content filters, which scans the data and matches it against pre-defined company and regulatory policies. Each message is checked to determine if it needs to be encrypted, quarantined, bounced or handled in other ways as established by the defined policies.
4. If the message meets the requirements of a specific encryption policy, the XCS SecureMail engine communicates with the Voltage SecureMail Cloud to generate encryption keys, branding data and then creates the notification message. XCS SecureMail uses Identity-Based Encryption (IBE) technology which generates encryption keys based on the sender and recipient email addresses. The message is signed with the sender's

public key and is securely pushed by the WatchGuard XCS appliance to the intended recipient.
6. The recipient opens the attachment, and if it is their first time receiving an encrypted email via XCS SecureMail, they then complete a one-time registration which authenticates their email address.
7. Once the recipient has authenticated their email address with this service, a private session key is issued based on the recipient's identity.
8. The entire email, including attachments, is decrypted and the recipient can now view the message securely.

Secure Reply and Forwards

Once an encrypted message is received and opened by the recipient, reply, replay all or forward actions of an encrypted email are also encrypted in order to ensure on-going secure communication.

Conclusion

No other solution on the market provides greater flexibility and ease-of-use. With its transparent application and universal reach, messages encrypted with WatchGuard XCS Securemail Email Encryption can be sent to any email inbox without cumbersome and costly administration or infrastructure requirements (or extra steps by the recipient including installing client software). Thus, confidential communications with business partners and customers is simplified and scalable.

XCS SecureMail provides maximum security to organizations with its transparent encryption capabilities using custom or pre-defined policies, data loss prevention and compliance dictionaries. Also, since messages are never stored on the same server as their keys, XCS SecureMail ensures that only those with permission to view the encrypted message have access to its content.

It has never been easier to deploy encryption as part of an overall email security solution. WatchGuard XCS SecureMail Email Encryption provides the necessary infrastructure so that all compliance rules and your outgoing emails/data will be protected from unintended viewers.

If you still have questions, we can help. Feel free to contact Orion Support today.