SOLUTION BRIEF

Fortinet and Seclore Email Security Solution

Seclore and FortiMail Best-of-Breed Email Security, Encryption, and Rights Management for Enterprises

Executive Summary

As email remains the primary communication channel for sharing information, organizations must have control over who accesses and shares sensitive data. Often referred to as the "last-mile" problem, the challenge is heightened by growing privacy regulations. Granular and automated security of emails sent within and outside the enterprise continues to be a challenge.

With the addition of Seclore Email Encryption Plus, Fortinet customers can automatically attach persistent, granular usage controls to protect email content and attachments flowing in and out of the business, ensuring sensitive information remains under the organization's control no matter where it is sent. The automated nature of the solution eliminates the need for end-users to take action to protect emails, as the action is based on the content and policy. For email recipients, the innovative browser-based solution eliminates the need to download and install agents in order to access the information.

Joint Solution Description

The combination of Fortinet FortiMail's scanning and discovery, along with Seclore's Email Encryption Plus, ensures information that leaves (or enters) the enterprise is always protected, trackable, and revocable. Leveraging FortiMail's configurable business logic, sensitive emails can be rerouted through Seclore's Mail Transfer Agent (MTA) to automate granular Rights Management.

Delivered both on-premises and in the cloud, extend your FortiMail solution with granular policy rights so that content is protected anywhere it travels: "who" can access it (identity access framework that leverages existing identities), "what" can they do with it (view, edit, copy/paste, print, screen capture, etc.), "when" can they access it (time bombing), and from "where" or which device (deny mobile access, IP or IP addresses, GEO fencing, etc.).

The functionality of the joint solution is summarized in the illustration below.

1. **User sends a document unprotected**
2. **Email server or cloud service receives email**
3. **FortiMail detects sensitive information, and then usage rights are automatically applied**
4. **Recipients receive protected email that is revocable and trackable**

Figure 1: Flow diagram: Fortinet FortiMail and Seclore Email Encryption Plus.

Joint Solution Benefits

Benefits of Seclore Email Encryption Plus and the Fortinet FortiMail solution include:

- Combining best-of-breed technologies—Innovative threat protection, data loss prevention, and rights management available as one integrated solution will enable enterprises to get best-of-breed technologies under one umbrella.
- Persistent, granular usage controls—Enable enterprises to control WHO (people, groups) can access emails and attachments, WHAT (view, edit, print, cut/paste) each person can do, WHEN (dates, time span), and from WHERE (devices, networks).
- Remote usage control—Access to the email and attachments can be modified or revoked by the sender even after the email has been sent and is no longer within the organization.
- Ease of use—The ability to automatically protect an email based on business policy ensures confidential information is always safeguarded from accidental or malicious activities. Recipients can access protected files from any device and any browser, making it easy for any recipient to engage in secure collaboration.
- Ability to protect incoming emails—Organizations who receive sensitive information from customers and business partners can automatically protect the incoming email and attachments, ensuring they keep shared information secure.
- Usage tracking for compliance—Organizations can track and report on all activities performed on an email and attachments to facilitate compliance with data privacy regulations, including unauthorized attempts to open the email or attachments.

FORTINET Fabric-Ready

Seclore Product Name and Description

Seclore's "Data-Centric Platform" brings together best-of-breed Data-Centric Security solutions with existing Enterprise systems to streamline the discovery, identification, protection, and tracking processes. The Seclore Data-Centric Platform enables organizations to increase agility, automate processes, and extend the value of individual point solutions for the highest degree of document security and tracking.

Fortinet Product Name and Description

The FortiMail secure email gateway utilizes the latest technologies and security services from FortiGuard Labs to deliver consistently top-rated protection from common and advanced threats while integrating robust data protection capabilities to avoid data loss. Organizations select FortiMail email security to shield users from a wide range of cyber threats. These include ever-growing volumes of unwanted spam, socially engineered phishing and business email compromise, accelerating variants of ransomware and other malware, increasingly targeted attacks from adversaries of all kinds, and more.

Use Cases

1. **Protecting End-user's Outbound Emails**
   - An end-user shares confidential information via email (contract, PII, PHI, IP, etc.).
   - Email sent to wrong email address—data breach.
   - Email recipient shares document with unauthorized parties—data breach.
2. **Protecting External Inbound Emails**
   - An inbound email is received from a third party (legal counsel, outsourcer, subcontractor, healthcare provider, etc.) which contains confidential information (contract, PII, PHI, IP, etc.).
   - Internal employee shares this information with other unauthorized internal employees—data breach.
   - Internal employee shares this information with other unauthorized external parties—data breach.
3. **Protecting Auto-generated Outbound Emails**
   - An Enterprise Application auto-generates content for distribution purposes which contains sensitive information (financials, statements, PII, PHI, IP, etc.).
   - Information leaves the enterprise unprotected—data breach.

About Seclore

Seclore offers the market's first open, browser-based Data-Centric Security Platform, which gives organizations the agility to utilize best-of-breed solutions to discover, identify, protect, and track the usage of data wherever it goes, both within and outside of the organization's boundaries. The ability to automate the data-centric security process enables organizations to fully protect information with minimal friction and cost. Over 2,000 companies in 29 countries are using Seclore to achieve their data security, governance, and compliance objectives. www.seclore.com

March 20, 2020 1:11 AM

D:\Fortinet\Solution Briefs\grey solution briefs\Seclore\sb-fortinet-and-seclore-email-security-solution-V1-3192020-1108PM

622670-0-0-EN