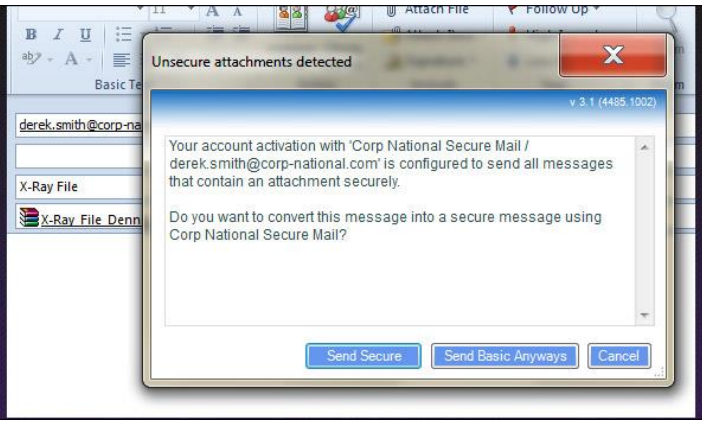


DATA LEAK PREVENTION

CATCH MISTAKES BEFORE THEY HAPPEN

A flexible light weight DLP feature which can help stop mistakes before they happen. Helps prevent data leaks, privacy breaches and protect sensitive information.

Overview

Business information is the most valuable asset; exchange confidential information knowing that data is protected with additional content, data leak and IP protection.

Pre-emptive Data Leakage Prevention allows keyword filtering of messages and enforces secure delivery based on policies as centrally set by the group administrator. Two deployment scenarios offer the most flexibility: a) in an employee Opt-in model, only a plug-in in Microsoft Outlook is required and b) to cast a wider net and offer better control, a Secure Messaging Gateway can be deployed at the organization's perimeter or in the Cloud. In an Opt-in model, p**olicy control takes place dynamically – on 'SEND' before the message is transferred to the server**. This is significantly different (and more effective) than solutions which rely on ad-hoc parsing or outgoing message filters. Prevent SNN and credit card numbers, or any other 'keyword', 'algorithm', email addresses or email domains based rules from ever leaving the organization, or enforcing encryption. Messages that do not meet the organization's customized criteria are automatically sent securely using the unique 'Enforce Secure' feature.

For smaller or departmental deployments, **only Microsoft Outlook is required** (Opt-in model) to benefit from the DLP feature:

- Force all messages that contain specific keywords, regular expressions, email addresses, email domains or messages with a file attachment to be sent secure.

In contrast, with the Secure Messaging Gateway model, all inbound and outbound traffic is monitored. The Gateway offers a more advanced Compliance Policy Engine that includes file attachment scanning and custom lexicons. Encryption occurs at the perimeter and does not require installation of a plug-in in Outlook.

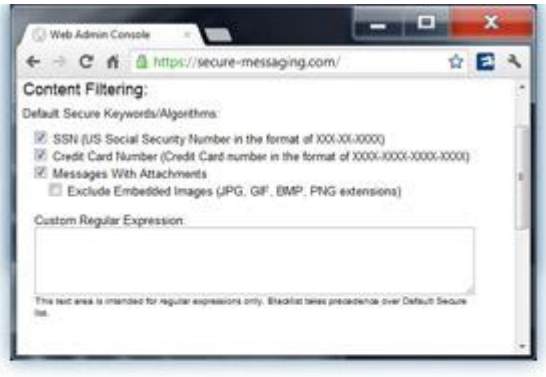
The Secure Messaging Gateway & API connectivity to the Secure Messaging platform allows for integration with existing DLP rules engine already deployed within the organization. When a basic unsecure message or file attachment is detected by the organization's existing DLP engine as requiring encryption, it can be re-routed instantly. The secure message is then prepared and sent on behalf of the user, in a completely transparent manner. Recipients respond in the same secure manner back to the original sender ensuring that the entire thread is secure.

SYSTEM REQUIREMENTS

- Microsoft Office Outlook® 2003, 2007 & 2010, 2013 all Editions.
- Optional Gateway for perimeter or Cloud deployment.

Quick Facts

- Avoid brand damage and financial liabilities caused by improper data leaks such as Personal Identifiable Information (PII).
- Pre-emptive customizable data leak prevention (DLP) feature with an admin function to make global rule changes for all staff.
- Users can be prompted pre-emptively 'on SEND' in Microsoft Outlook® to make appropriate corrections.
- Provides enhanced email security for extra protection that sensitive information won't fall into the wrong hands.
- Prevents data from being sent unsecured if certain words, patterns or attachments are included in the email message.
- Prevents data leaks and mitigates the risk of a breach of privacy of client or sensitive information.
- Reduce financial liability by 'catching' errors prior to data leaving the organization or being caught in quarantine.
- Opt-in model only requires Microsoft Outlook® to function, optional Gateway for perimeter protection.
- API integration with existing DLP rules engine.
- Helps address compliance with Privacy and National and State Technical Security Safeguard Standards (**HIPAA, SOX, GLBA, PCI**).
- Provides additional tools for group administrators to manage corporate IT security and privacy policies.



Administrator manage global corporate policies from a single interface that applies to all users.