What is Strac?

Strac is a DLP solution that offers No-Code and APIs for detecting & redacting (masking) sensitive PII data and credentials like API keys across all communication channels. Strac supports Email (Office 365, Gmail), Slack, MS Teams, Intercom, Confluence, SharePoint, OneDrive, Web Applications (FrontEnd & BackEnd), etc. All of those integrations are powered by Strac's APIs

Problems with Sensitive Data over Email

Businesses face the following challenges when receiving sensitive customer information from popular communication channels like email.

1. Compliance

Regulatory compliance such as SOC, HIPAA and GDPR require security controls such as data retention, audit trails and auto logout to fulfill. These capabilities may not be available in the SaaS providers or are work intensive to set up. For example, a financial services company operating in New York requires compliance with Cybersecurity law NY-CRR to operate. In order to comply with requirement 500.7, businesses must restrict its employees from accessing sensitive customer data and here to limit employee access to sensitive data but it is hard to implement for email. Setting a general policy to delete all emails after 90 days would cause critical emails to be deleted. Even worse, it is an issue of business discontinuity if one can't securely access past emails. A more fine-grain policy might enforce data retention only on customer-facing email addresses. Even this would cause valuable customer exchanges to be lost after the data retention period.

2. Account Compromise

In 2021, FBI reported $2.4 billion worth of damages due to email account compromise. Account compromises are not unique to email and can happen due to a variety of reasons including using weak passwords, not enabling 2FA and phishing.

Secure account settings are not enforced by default because SaaS providers need to appeal to all types of users including those that do not handle sensitive information. It is easy for IT admins to make a configuration mistake when onboarding to SaaS providers, increasing the likelihood of account compromise. This is especially true in today's world where small businesses use an average of 16 SaaS applications which increase to 177 for enterprises.

3. Accidental Data Leakage

Today's fast paced business environment requires customer support agents to handle an average of 36 tickets on a daily basis while continuously making the best decisions

to improve customer satisfaction. There's little room to squeeze in security processes that slows down businesses and that's when accidents happen.

For example, U.S. Marine Corp made an accident in 2018 when an attachment containing personal information of 21,426 people including bank accounts was sent to the wrong email distribution list.

Today, existing providers do not protect against accidental data leaks.

4. Data Liability

With open communications like email, customers are free to send unsolicited sensitive data and a business is liable even if they did not ask for it. This issue adds additional complexity to a company's security plan because all communication channels now require a high level of security bar to clear. One customer testimony summarizes this issue well:

"The huge problem with email is that anyone can send sensitive data to a business and a business is liable even if they did not ask for it. Strac solves that huge problem by automatically redacting sensitive data that is shared by our customers over email with their unique technology. It dramatically reduces security and SOC compliance risks for us while improving security posture for us."

5. Lack of Visibility

Knowing is half the battle. When a company's Information Security team (InfoSec) reviews security risks, they need a holistic view of not just where the sensitive data might be but also the severity if a breach were to happen. This type of data is usually obtainable for internally developed applications but not for SaaS applications handling email, tickets and instant messaging.

This visibility gap prevents InfoSec from making the best decisions when prioritizing security risks for the company.

Strac Email DLP

Strac's Email DLP solution works by applying Strac's Machine Learning (ML) model on email messages (body and attachments). It detects & redacts sensitive PII data from email messages.

Strac's Email DLP works with Office 365 & Gmail inboxes of users in an organization & scans the message body and attachment contents of inbound and outbound email messages in real time. Inbound applies when an employee receives an email. Outbound applies when an employee sends an email.

Strac Detector

When the Strac's Email DLP detects content with sensitive personal information, it alerts/notifies the configured admins on sensitive messages being detected. All findings can be accessed in Strac's UI Vault or via email.

Strac Redactor

When the Strac's Email DLP detects content with sensitive personal information, it quarantines the information to a secure data vault and updates the email message to replace the sensitive personal information with links to the secure data vault where contents can be read and/or downloaded.

A business can configure the individual PII/PHI data elements based on the compliance rules in your organization.

Sensitive Data Elements Catalog

Following sensitive Data Elements can be configured by the business to redact from email messages:

- Identification: SSN (Social Security Number), Drivers License, Passport, etc.
- Payments: Credit/Debit Card Number, Bank Account/Routing Number, etc.
- PII: Name, Address, Email, Phone, Date of Birth, Age, etc.
- Credentials: API Keys, Passwords, Passphrases, etc.
- Crypto Secrets: Bitcoin, Ethereum, Litecoin Addresses, etc.
- PHI: PII data, Medical Record Number (MRN), Medical Notes, etc.
- Physical Network: IP Addresses, Mac Address, etc.
- Custom: Create your own rules

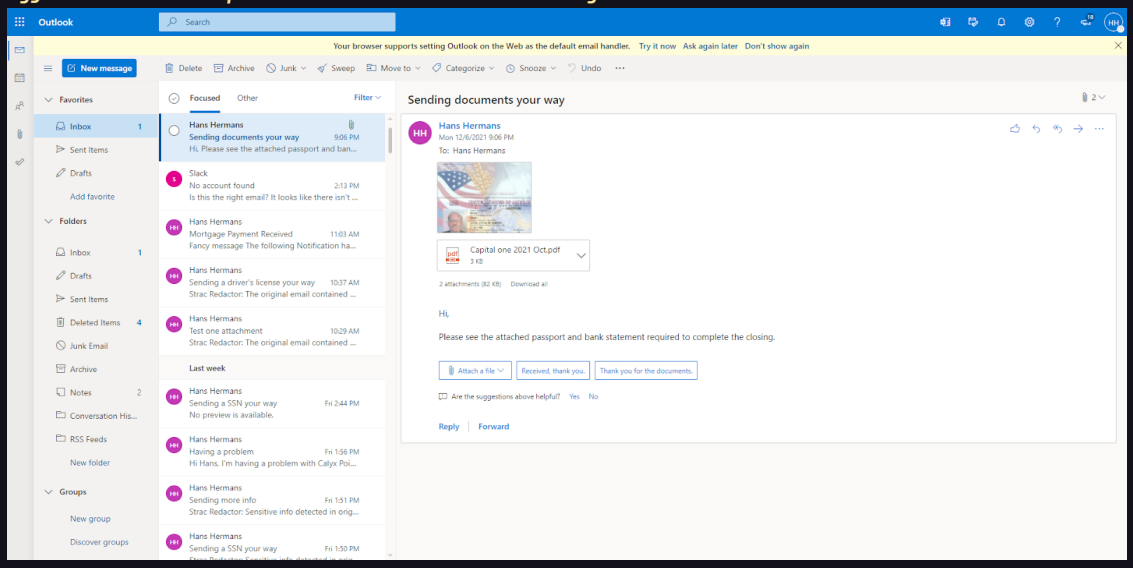
Integration Time

Businesses launch with Strac Email Redactor in *less than 15 minutes*

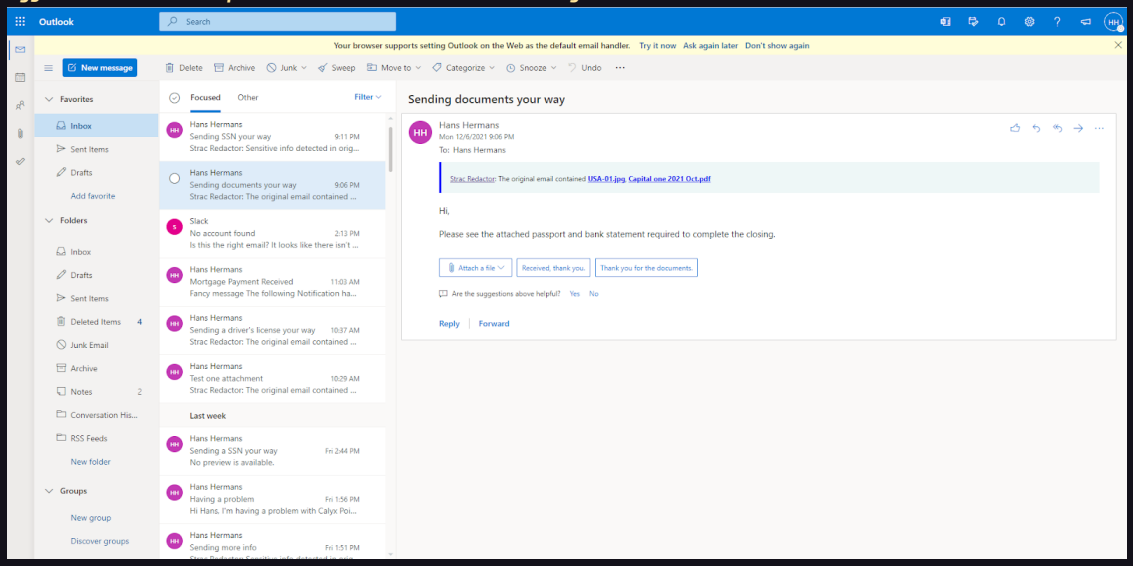
Below are screenshots of Office 365. Gmail screenshots are in the Appendix.

Strac

Office365 Example with Attachments: Before Redaction

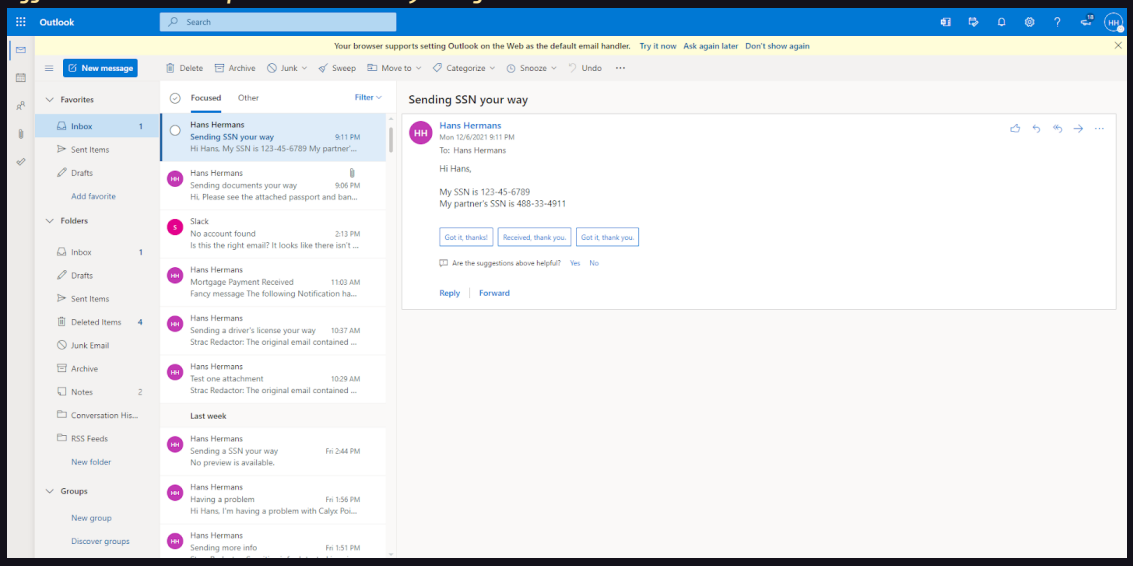


Office365 Example with Attachments: After Redaction



Strac

Office365 Example with Body: Before Redaction



Office365 Example with Body: After Redaction