HORNETSECURITY

FACT SHEET

AI RECIPIENT VALIDATION

AUTOMATED MISDIRECTED EMAIL PROTECTION FOR MICROSOFT 365

Key Facts:

- **ALWAYS SELECT THE RIGHT RECIPIENTS**
- **AVOID EMAIL SECURITY BREACHES**
- **PREVENT DATA LOSS**

Why do I need AI Recipient Validation?

In some critical industries like finance, healthcare, and utilities, human error such as misdirected emails fall under the most common causes of security breaches.*

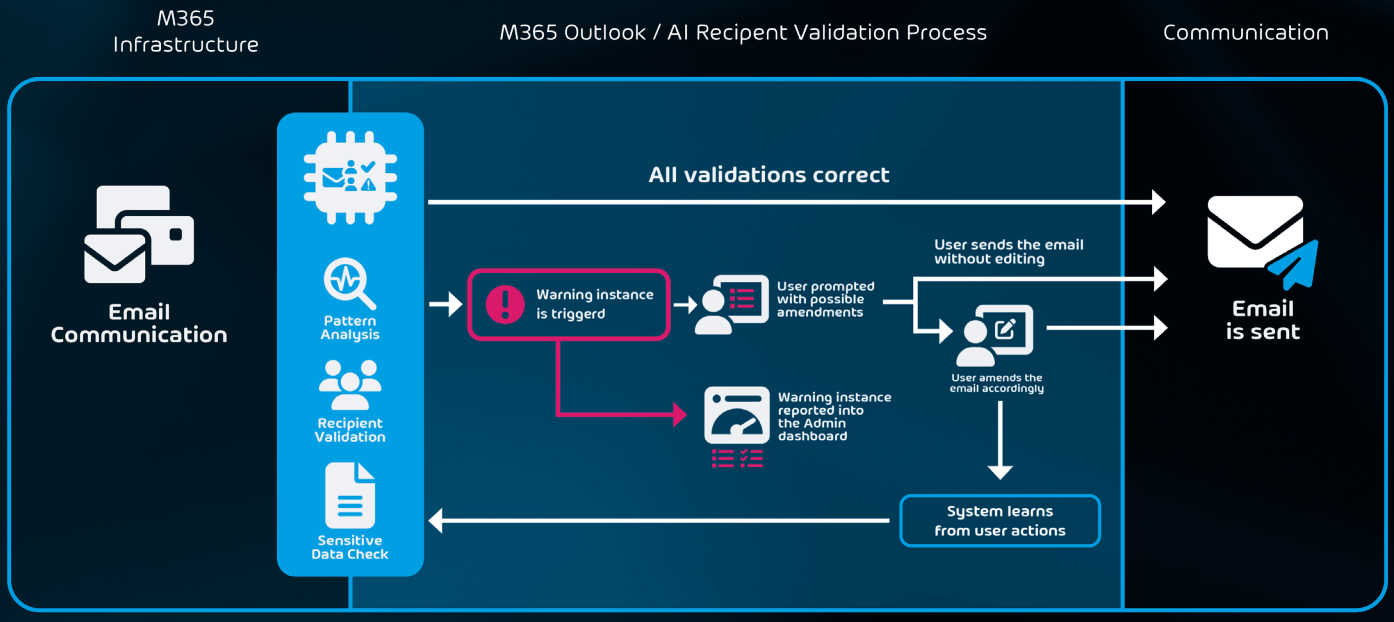
Data breaches caused by misdirected emails can be costly to businesses in financial terms and also result in loss of reputation and trust.

Regulations, including GDPR in Europe, have shown their strict side when it comes to protecting sensitive data. As a result, businesses not only need a reliable solution that reduces email threats caused by human error but also ensures that an organization can comply with regulatory requirements.

Hornetsecurity's AI Recipient Validation safeguards email users by assisting them to always select the right recipients. It gives security and compliance leaders true visibility over how their employees are handling and responding to preventing misdirected emails.

*2023 Data Breach Investigations Report, An analysis of 16,312 incidents and 5,199 confirmed data breaches
https://www.verizon.com/business/resources/reports/dbir/

AI Recipient Validation is an AI-based, self-learning service that continuously analyzes a user's email communication patterns in the background. It automatically detects potentially unintended recipients, warns about emails containing sensitive data like Personal Identifiable Information or inappropriate wording, and factors in user behavior and responses to automatically adjust warnings and suggestions issued in upcoming communications.



HORNETSECURITY

FACT SHEET

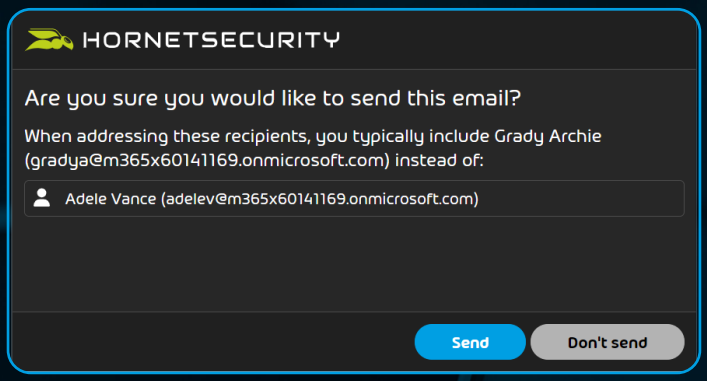
AI Recipient Validation warns users when attempting to send emails in the following instances:

Recipient Validation

- Sending an email to an potentially unintended recipient.
- An otherwise common recipient from a cohort is missing.
- A user is added or replaced in an existing cohort.
- Sending emails to users from different organizations or personal email addresses for the first time.
- Replying to a large distribution list.
- Sending an email to a recipient whom the user has no previous relationship with.
- Suggesting a user based on the context of the email.

Supplementary Checks

- Sending an email with sensitive information, such as PII or PCI data.
- Sending an email with inappropriate wording.

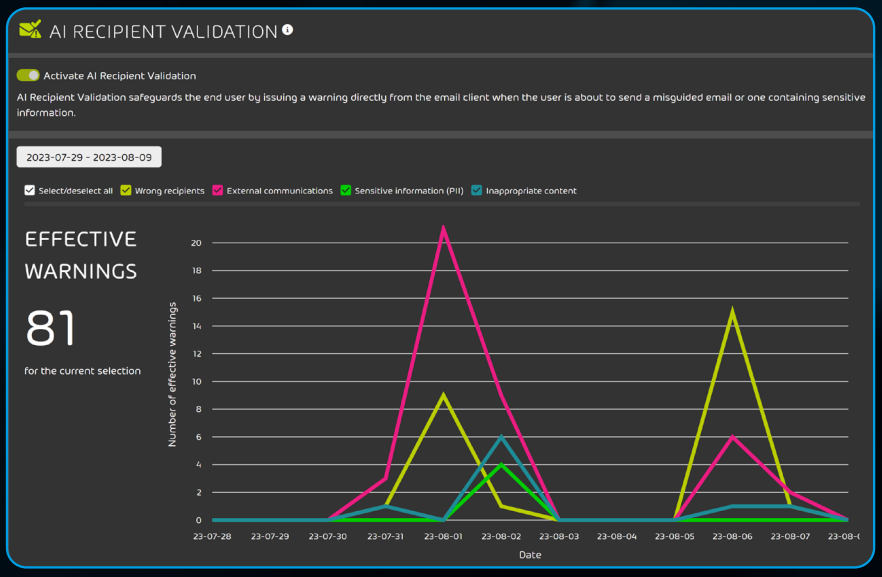


The self-learning AI engine adjusts the warning instances according to user behavior.

GET A CLEAR OVERVIEW OF USER VIOLATIONS

The AI Recipient Validation dashboard provides administrators with an overview of the various warning instances that users are exposed to.

This empowers them to take further action such as raising employee awareness of data privacy in email communications.



QUICK AND EASY SETUP WITH A FRIENDLY USER EXPERIENCE

Our onboarding wizard will set you up in no time. Benefit instantly from an extra pair of eyes that autonomously notify you upon the possibility of misdirected communication and safeguards against potential data leaks.

AI Recipient Validation integrates seamlessly with your Microsoft 365 infrastructure, with no change of existing configurations settings and MX Records required! AI Recipient Validation is available for Microsoft 365 users on the latest versions of their Outlook Mail Client for Windows, Mac and Web.