HORNETSECURITY

FACT SHEET

AI RECIPIENT VALIDATION

AI-POWERED, AUTOMATED MISDIRECTED EMAIL PROTECTION FOR MICROSOFT 365

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.

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

What is affected?

M365 Email Communication

How does AI Recipient Validation help you?

Pattern Analysis

AI-based self-learning engine analyses email communication.

Recipient Validation

Emails are checked for potentially unintended recipients.

Sensitive Data Check

Avoid accidentally leaking sensitive and PII data.

What improves?

Minimized risk of sensitive data leaking within and outside an organization

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

REAL-TIME ANALYSIS AND INSTANT FEEDBACK AND CHANCE FOR CORRECTION

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

Recipient Validation

- Sending an email to a 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.

Supplementary Checks

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

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.

CUSTOMIZATION TO FIT YOUR COMPANY NEEDS

Admins can configure AI Recipient Validation to fit their company's needs, ensuring warning instances are triggered efficiently and productively by:

- Disabling specific warning scenarios from triggering warnings.
- Excluding users from specific warning scenarios.
- Enabling trusted domains for external domains to be treated as internal ones.

QUICK AND EASY SETUP WITH A USER-FRIENDLY 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.

SMART ALERTS

Thanks to Smart Alerts, AI Recipient Validation delivers intuitive, side-panel warnings and unlocks seamless offline functionality. Smart Alerts ensure uninterrupted access to AI Recipient Validation features, empowering users to work efficiently anytime. The streamlined and user-friendly experience prioritizes reliability and ease of use, making AI Recipient Validation an indispensable tool for productivity and performance.
Powered By AI Cyber Assistant.