Nightfall AI
Email DLP with Encryption

Protect your data *everywhere* employees work.

Cloud productivity suites have become the backbone of modern organizations. While this has undoubtedly helped streamline workflows and information sharing, it's also made email a top threat vector for data breaches.

Enforce compliance with ease.

Organizations handling and storing a lot of sensitive data, including protected health information (PHI), customer data, financial records, secrets and credentials, and employee data, need stronger data handling compliance enforcement.

Stay off the "breached" list.

The need for comprehensive safeguards to protect sensitive information shared via email has never been greater.

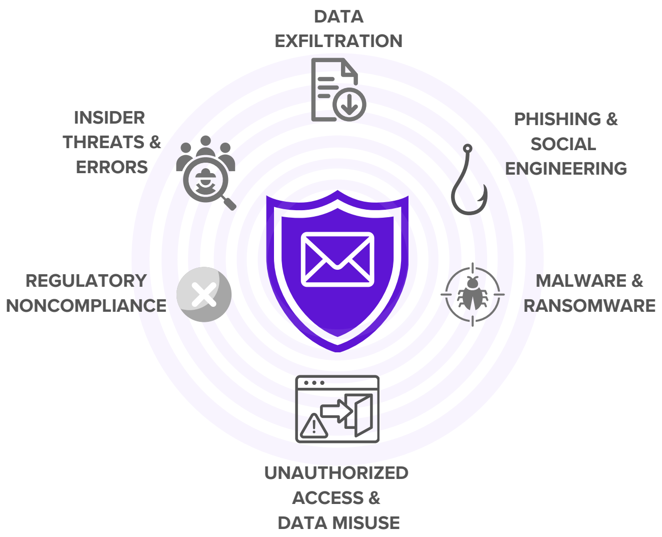
*Meet the first **AI-native, context-aware** email encryption solution.*

- AI-powered ***smart*** detection
- Automated remediation actions
- Market-leading detection accuracy
- Robust, military-grade encryption
- Email compliance enforcement

- Encrypt emails *and* attachments
- Tailored to specific data being shared
- No manual intervention needed
- Excels with data types other solutions miss
- Lightens security team's workload

Nightfall AI™

Protect your data from leaks & loss via email–



DATA EXFILTRATION

INSIDER THREATS & ERRORS

PHISHING & SOCIAL ENGINEERING

REGULATORY NONCOMPLIANCE

MALWARE & RANSOMWARE

UNAUTHORIZED ACCESS & DATA MISUSE

no matter what comes your way.

Mitigate Insider Risk

Admins and senders retain persistent visibility and control over protected messages and attachments both natively in Gmail and within the Nightfall console. Sharing activity is available in logs which can be ingested in SIEM tools for enhanced threat response.

Automated, context-aware encryption eliminates reliance on end-users to do the right thing, but involves them in the process.

No Advanced Skills Needed

DLP scans are *inline*. As users type or add attachments, Nightfall AI analyzes text on users' behalf with our award-winning detection engine to identify sensitive data.

End-user encryption controls are embedded within the Gmail UI–**easy to find, easy to use.** We even made a **plugin for Google Chrome** to keep it simple for you!

External recipients can access secure emails without creating new accounts or managing additional passwords, simply authenticating with their existing accounts using a one-time login code.

Granular Control Over Your Data

- Automated scans for all outgoing mail
- Encrypt with a simple toggle
- Apply to message body & attachments
- Quarantine for review or automate blocking
- Specify which user accounts to monitor
- Set expiration dates
- Disable forwarding
- Revoke access at any time
- Configure custom policies

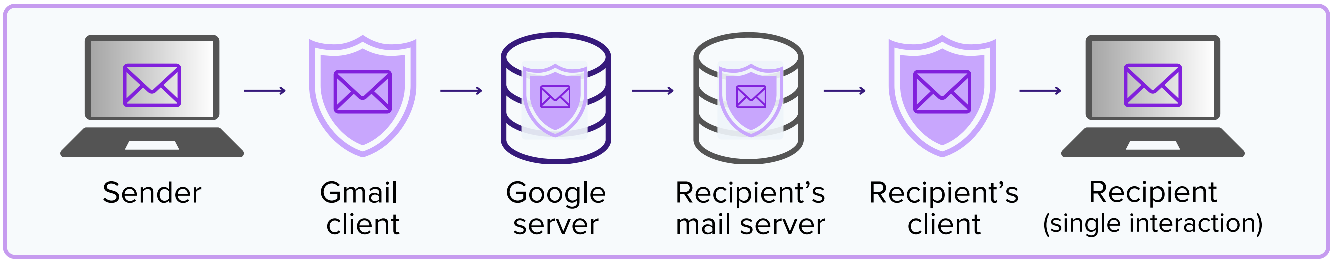
Nightfall AI™

Details & Technical Specifications

A Solution Designed to *Work*

- Persistent file protection
- Attachments remain encrypted 24/7
- Encrypted attachments accessed **only** via Nightfall's secure reader
- Outlook encryption is forthcoming
- Tight integration with Gmail / Google
- Uses AES with Galois/Counter Mode (AES-GCM) 256-bit encryption
- Leverages dynamic, randomly generated cipher keys

How Nightfall Email Encryption Works



Protection You Can Trust

Not only does our encryption tool provide reliable data security, but Nightfall gives you response flexibility. Automate encryption upon discovery of sensitive information within emails, or provide control to end-users–all without leaving the native email app experience.

Using the most robust detection engine on the market, Nightfall's email encryption tool gives you the compliance assurance you need, especially for complex, highly regulated data types like HIPAA and PII (personally identifiable information).

Nightfall AI™