Nightfall AI™

Nightfall Data Encryption

Secure data by applying context-aware automatic encryption

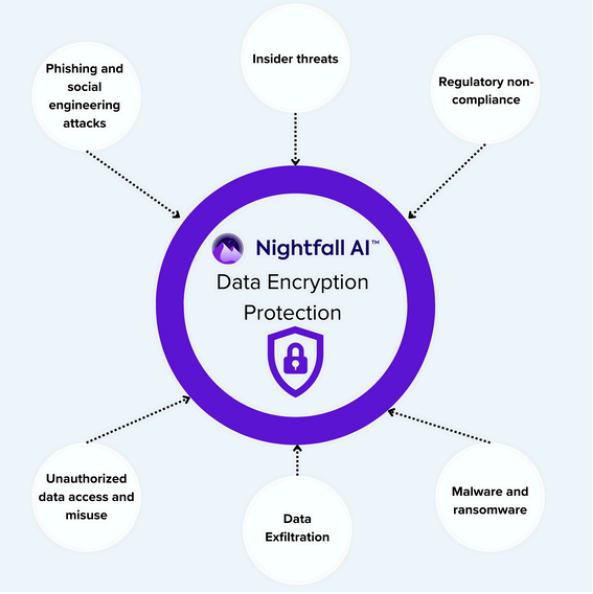
Cloud productivity suites have become the backbone of modern organizations, revolutionizing the way we collaborate and communicate. At the forefront of this transformation is Google Workspace, a powerful suite of cloud-based tools that has gained widespread adoption across industry verticals. At its core, Gmail has emerged as the predominant email solution, boasting a staggering 30% of the global email market share.

This rapid migration to the cloud has undoubtedly brought numerous benefits, streamlining workflows and fostering seamless information sharing. However, it has also introduced new security and compliance challenges. Email has become a primary vector for cyber threats, with a staggering increase in cyber attacks originating from email as per Verizon's 2024 data breach investigations report. Additionally, many organizations handle and store a significant amount of sensitive personal information, such as protected health information, customer data, financial records, secrets and credentials and employee details. This type of information is often subject to strict privacy regulations like HIPAA, PCI DSS and CCPA, GDPR, which mandate robust security controls to protect against unauthorized access and misuse.

Failure to comply with these regulations can result in severe financial penalties and reputational damage. As security regulations evolve and organizations grapple with safeguarding sensitive data in email, the need for comprehensive safeguards to protect sensitive information shared through Gmail and other email platforms has become increasingly paramount.

Introducing Nightfall: Industry's first AI-native, context-aware data encryption solution for emails

Nightfall's Data Encryption solution leverages artificial intelligence (AI) to automatically detect and secure sensitive information within your emails and attachments. This context-aware intelligence allows us to apply robust, military-grade encryption tailored to the specific data being shared - no manual intervention is required. Utilize the power of cutting-edge AI-trained detectors to achieve unprecedented accuracy in identifying sensitive data like PII, PCI, PHI, secrets and credentials or intellectual property to lighten the security team's workload.

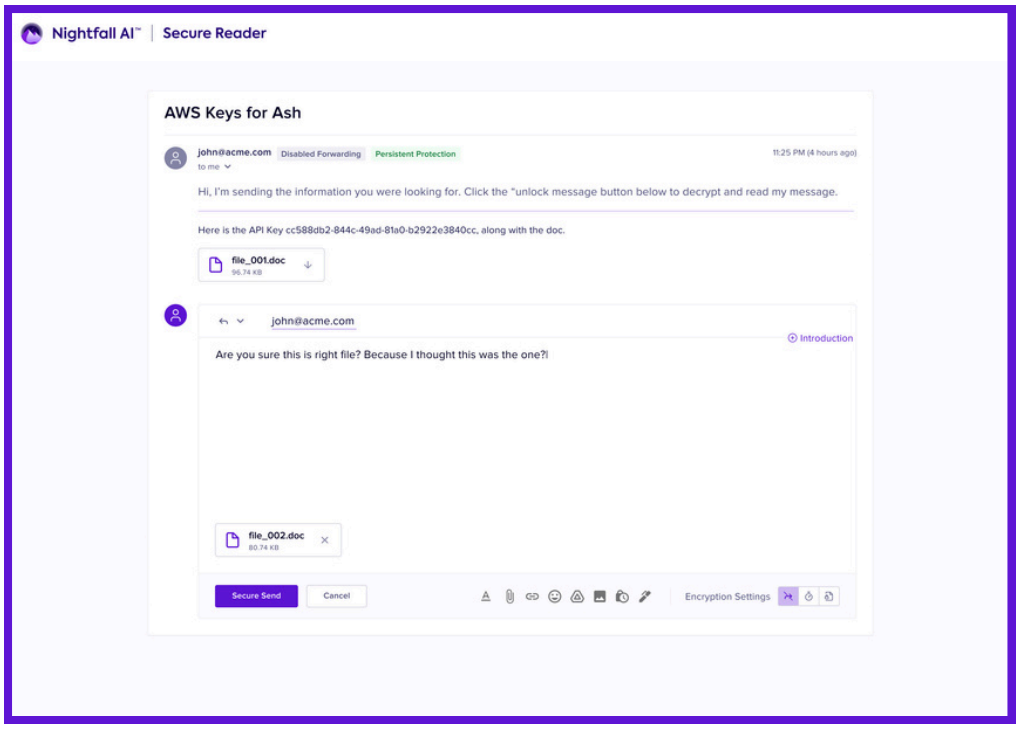


DATA SHEET

You have the flexibility to automate encryption as per sensitive information in emails or provide control to end-users to enable encryption when they are composing emails - all while utilizing the native experience in Gmail.

Industry's first AI-native, context-aware encryption

Nightfall's Data Encryption solution leverages artificial intelligence (AI) to automatically detect and secure sensitive information within your emails and attachments. This context-aware intelligence allows us to apply robust, military-grade encryption tailored to the specific data being shared - no manual intervention is required. Utilize the power of cutting-edge AI-trained detectors to achieve unprecedented accuracy in identifying sensitive data like PII, PCI, PHI, secrets and credentials or intellectual property to lighten the security team's workload. You have the flexibility to automate encryption as per sensitive information in emails or provide control to end-users to enable encryption when they are composing emails - all while utilizing the native experience in Gmail.



Effortless compliance, iron-clad control

Struggling to keep up with evolving compliance regulations and security requirements like HIPAA, PCI DSS, CCPA, GDPR and others? Nightfall Data Encryption has you covered. Our AI-native approach ensures continuous compliance, giving you the power to granularly control access to encrypted emails, revoke permissions, set expiration dates, disable forwarding and more - all without disrupting your team's productivity. Persistent file protection ensures attachments remain encrypted at all times and can only be accessed via Nightfall's secure reader. Nightfall uses AES with Galois/Counter Mode (AES-GCM) 256-bit encryption to encrypt data - email body and attachments. Data is encrypted using a dynamic, randomly generated cipher key.

The encrypted content is then stored in a cloud object storage protected with IAM policies ensuring the principle of least privileges with AES 256 bit encryption enabled at rest. This ensures all emails are double encrypted by Nightfall enabling continuous compliance and guaranteeing peace of mind.

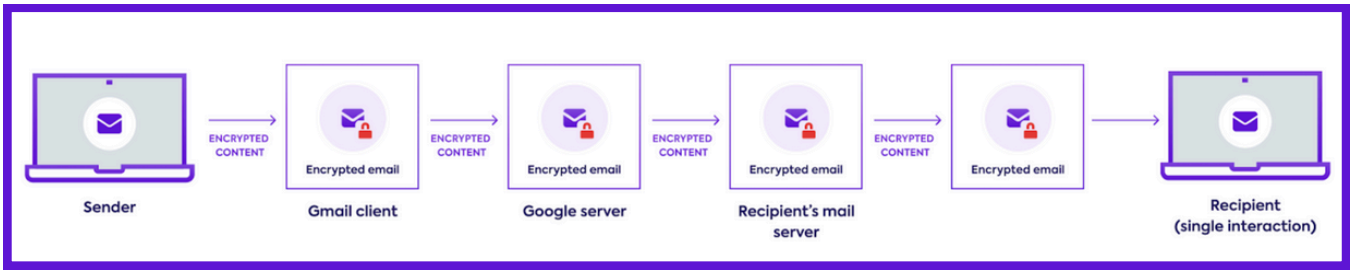
"I recently had the opportunity to use Nightfall, and I must say, it has transformed our data protection strategies! Nightfall offers a comprehensive and seamless solution that not only identifies and classifies sensitive data but also actively prevents data leaks and breaches. It is very user-friendly. The user-friendly interface made the setup process a breeze, and the configuration was straightforward, even for someone with limited technical expertise (me). The customer service team went above and beyond to help us in every aspect. The accuracy of Nightfall's data discovery capabilities AMAZING! It successfully detected sensitive information across various data sources.One standout feature of Nightfall is its real-time data loss prevention (DLP) capabilities. The system immediately flagged any attempts to share sensitive data, giving us peace of mind knowing that confidential information remains protected at all times."
- G2 Customer Review

Unparalleled Visibility and Automation

Gain unprecedented insight into how your sensitive information is being accessed and shared via email. Nightfall centralized admin console and reporting provides complete visibility of all encryption activity, including encrypted emails read by recipients, attachments downloaded, and sender actions like disabling forwarding or revocation of access. This enables you to swiftly investigate any potential breaches and demonstrate compliance to regulators. With robust policy controls like per policy alerting to Slack, Email, Jira or Webhooks, you can automate incident triage and response via SIEM/SOAR tools and significantly reduce the manual workload on security teams. With end-user notifications and a human firewall, you can coach users after the fact on acceptable usage of sensitive data. Nightfall reduces costs for overburdened IT and security teams.

DATA SHEET

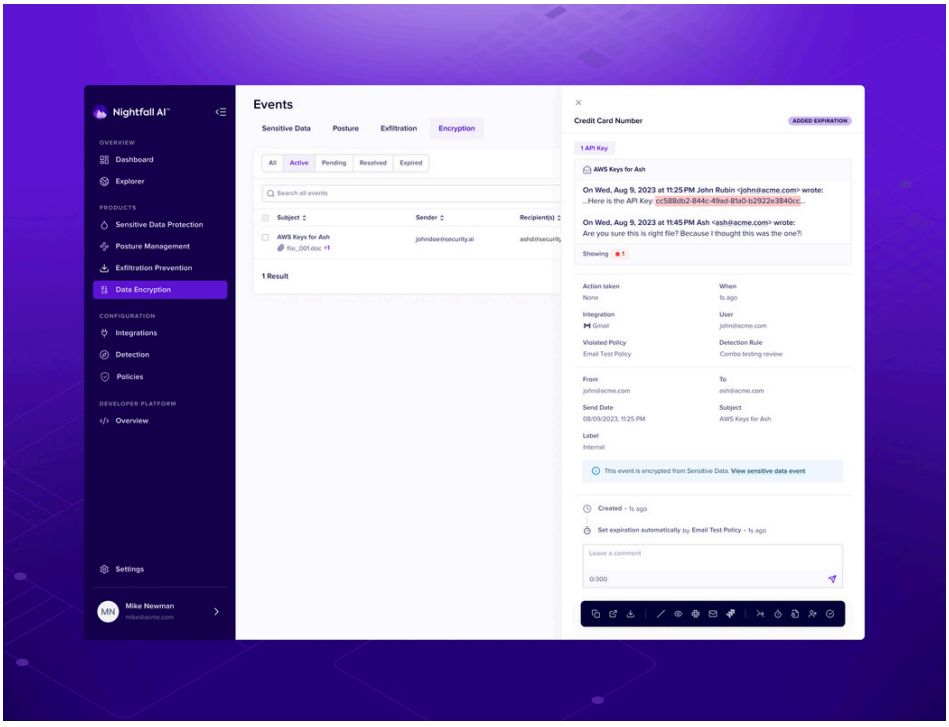
How it works



Keeping email communications secure is a top priority for modern organizations. Nightfall's AI-native, context-aware data protection solution for Gmail is considered a security best practice, enabling organizations to leverage Gmail's productivity features while ensuring encryption of messages and attachments, wherever they're shared.

Nightfall provides best-in-class AI-driven data loss prevention (DLP) and automatic, context-aware email encryption, keeping Gmail messages and attachments private and compliant throughout collaboration workflows. Embedded directly within the native Gmail interface via a Chrome extension, Nightfall enables encryption before emails reach Google's servers, preventing unauthorized access by Google or other parties.

With a simple toggle, senders can encrypt message bodies and attachments, set expiration dates, disable forwarding, and revoke access at any time. Persistent file protection ensures attachments remain secure even when shared beyond email, allowing recipients to download and collaborate on files across desktops, network drives, Google Drive, and other cloud platforms, while the sender maintains control.



Nightfall's seamless integration into Gmail reduces support costs for IT and security teams. Automated, context-aware encryption based on detection of sensitive data empowers security teams and eliminate reliance on end-users to do the right thing. IT and security teams can also provide end-users the control by allowing flexible, end-user self-management of outgoing emails via protection options in the Chrome plugin. 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. Admins and senders retain persistent visibility and control over protected messages and attachments, with encryption and sharing activity available natively in Gmail and within the Nightfall console. The sharing activity is available in logs which can be ingested in SIEM tools for enhanced threat response.

Nightfall's AI-native, context-aware approach to data encryption provides organizations using Gmail with the highest assurances that email data will remain private and compliant throughout its entire lifecycle.

To learn more about how Nightfall can support your organization's compliance and privacy programs, visit www.nightfall.ai to speak with a DLP expert.

DATA SHEET