Nylas

Nylas Security White Paper

Learn how Nylas employs security procedures and processes to keep your data safe.

Nylas

Enterprise-grade security and privacy controls are at the heart of the Nylas infrastructure and cloud communications platform. Nylas strives to earn customer trust by enforcing world-class security practices and standards. We keep customer data private and secure through a multilayered physical and network-level security hierarchy. This document details all of these platform security procedures and processes.

For direct inquiries, please contact security@nylas.com.

CONTENTS

TRANSPARENCY

Nylas adheres to a high level of operational excellence. Nylas has multiple interlocking policies for incident response, audits, and privacy. We believe security practices should be transparent to customers, and these measures are outlined below.

Incident Response Policy: As part of our basic service to all customers, all service impacting and business-critical incidents are closely monitored and responded to 24/7, 365 days a year. Our Engineering team is constantly monitoring both our infrastructure and alerts from upstream vendors. We use notification and alert systems to immediately identify and manage risks and threats. Nylas network status and incident reports are hosted by a third party and available publicly in realtime at https://status.nylas.com/.

Privacy Policy: The Nylas Privacy policy is publicly accessible at https://nylas.com/privacy-policy and strictly adhered to by all Nylas agents and employees. Only those Nylas employees who require customer data access as a necessary part of their job function are permitted access to encrypted customer data. These groups include our customer support, development, and infrastructure security teams.

Audit Policy: All access to production clusters is logged and audited regularly. The production cluster is accessible only to Nylas operational staff and engineers, whose primary responsibility is the construction and maintenance of the Nylas API and services. We also perform regular security audits of our own code, third-party libraries, and our infrastructure automation. Before code is deployed to production, it must pass a rigorous series of security tests that ensure data is secure and our systems are safe.

COMPLIANCE

Nylas fully complies with key government and industry regulations and policies, including US-EU as well as US-Swiss Safe Harbor and PCI DSS as a merchant. Nylas also supports a variety of use cases employed by companies engaged in PCI- and HIPAA-covered activities.

Privacy Shield Compliance: On July 16, 2020, the Court of Justice of the European Union invalidated the Privacy Shield Framework; however, because Nylas offers an EU datacenter, Nylas customers are not affected by this issue.

PCI DSS Compliance: Nylas is a PCI DSS 3.1-compliant merchant and can securely accept credit card payments for its services. But apps built on top of Nylas are not covered under Nylas' compliant status. Nylas strongly recommends that customers familiarize themselves with the PCI DSS requirements and security assessment procedures. Use of a PCI-DSS-compliant application does not by itself make an entity PCI-DSS-compliant, as the application must be implemented in conformity with the overall Payment Application Data Security Standard (PA-DSS) Implementation Guide.

Many businesses have architected their applications in a PCI-compliant manner while still using Nylas for parts of their workflow. The key is to avoid processing, storing, and transmitting cardholder data on Nylas.

HIPAA Compliance: By law, the HIPAA Privacy Rule applies only to covered entities: health plans, healthcare clearinghouses, and certain healthcare providers. Nylas is HIPAA Type 1 and HITECH compliant, and it is possible to architect your application to be compliant with the HIPAA Privacy and Security Rules, while using Nylas for part(s) of your workflow. HIPAA Type 1 confirms that Nylas passed the HIPAA regulations at the time of our SOC 2 audit. Additionally, HITECH strengthens the regulations laid out by HIPAA and requires any significant breach to be reported to the affected individuals and government.

GDPR

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy, and to reshape the way organizations across the region approach data privacy. Under the GDPR, Nylas is considered a data processor. Our customers are considered data controllers. Our customers' end users are considered data subjects.

For example, let's say Nylas had a customer called "The World's Best CRM." "The World's Best CRM" would be considered a data controller. Jeremy, a small-business owner, uses "The World's Best CRM" to send awesome emails and engage his customers. Jeremy is considered a data subject. The Nylas API, which powers "The World's Best CRM," is considered the data processor. We define these roles in more detail below.

Data controllers: In regards to GDPR, Nylas customers are considered "Data controllers." Any data controller working with Nylas must sign a data processor agreement prior to using our API.

A controller is a person, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data. All compliance requests from data subjects are first vetted by data controllers. Any compliance requests to Nylas will be forwarded to the relevant data controller for approval.

Data processors: In regards to GDPR, Nylas is considered a data processor. A data processor is a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller.

Data subjects: In regards to GDPR, the customers of the data controller are considered the data subjects. A data subject is a natural person whose personal data is processed by a controller or processor.

Data processor agreement: Legally binding agreement between Nylas and the data controller guaranteeing provisions of GDPR.

Right to be forgotten: In compliance with GDPR, Nylas guarantees that the data controller is able to request deletion of all stored data (inbox, calendar, contacts) for their data subjects and that Nylas will fulfill that request in 30 days or less.

Data portability: In compliance with GDPR, data controllers can request to download a copy of their data subjects' data (inbox, calendar, contacts) in a machine-readable format. This export will be available for a one-week period.

Personal Data Breach: In compliance with GDPR, Nylas guarantees that all data controllers affected by a data breach will be contacted within 72 hours using their registered email address.

SOC 2 TYPE II

The SOC 2 Type II certification is the most comprehensive security certification in the SaaS industry. To achieve SOC 2 Type II certification, Nylas underwent independent audit and penetration tests of existing security protocols, processes, and systems. The SOC 2 Type II certification demonstrates our data management systems, and processes are designed to keep users' sensitive information secure while ensuring a high degree of performance and reliability.

Our comprehensive SOC 2 Type 2 report is available at: www.nylas.com/soc2-security-report

SOC 2 Standards of Excellence Used at Nylas:

Security: Nylas API architecture is protected against unauthorized access, both physical and logical.

Availability: The Nylas API supports high-availability operations as committed to in SLA contract.

Processing Integrity: System processing is demonstrably complete, accurate, timely, and authorized.

Confidentiality: All email information is handled as confidential and is protected as committed or agreed.

Privacy: Personal information is collected, used, retained, disclosed, and destroyed in conformity with our commitments in the Nylas Privacy Policy and with the criteria set forth in Generally Accepted Privacy Principles (GAPP).

ENCRYPTION AND ACCESS CONTROL

Nylas uses multiple application-level security mechanisms and features to ensure customer data safety. All customer API calls require proprietary OAuth2 authentication tokens granted only by Nylas, and user data is encrypted using military-grade encryption standards.

OAuth2: Nylas ensures user information and identity protection through our adherence to the OAuth2 protocol. User Authentication to email back-ends (e.g., Gmail, Microsoft Exchange) is completed via OAuth2 where possible, and encrypted password-based Auth otherwise. OAuth2 is the top industry-standard secure authentication protocol that provides developers with individual revocable tokens per email account.

SSL: Nylas uses TLS 1.3 to encrypt bidirectional session traffic between the customer application and Nylas. We update and renew the encryption methods when they expire. This includes (and is not limited to) email synchronization, Nylas API endpoints, and user authentication. Our API is exclusively accessed via authenticated SSL connections. We use private key authenticated encryption via the Libsodium Secretbox Module to secure user credentials and authentication tokens. Nylas runs a comprehensive test suite and holds industry best-practice code reviews to ensure security safeguards are upheld prior to launching new features.

Customer Data Backups: Encrypted email message bodies are cached using Amazon's S3 service. S3 is secured with strict authentication and authorization rules. All raw message bodies are automatically deleted after 7 days. Email metadata is cached in a combination of Amazon's RDS service and dedicated MySQL databases. This data is regularly backed up to guard against data loss scenarios. All backups are encrypted both in transit and at rest using strong industry encryption techniques. Hot data backups ensure no data is lost in the handoff process and the archival backup process ensures full recovery in the unlikely event that data centers are lost. Backup files are stored redundantly across multiple availability zones and are secured by Amazon.

Role-Based Access: Nylas has procedures and controls in place to appropriately limit access to customer data and mitigate the risk of insider threats. Customer data may be accessed in case a customer account enters a failure state that requires accessing email data for debugging purposes. This data is not accessed for debugging unless an error cannot be resolved without doing so; all private data is excluded from system logs.

NETWORK TRANSPORT AND STORAGE

Nylas implements best practices for maintaining service-wide network security. We deploy the latest technology to provide uninterrupted service and guard against attack. Internal sync infrastructure is isolated from the public Internet within separate VPCs, blocking all inbound connections and persistence, and storage layers are encrypted and secured behind VPN and firewalls.

Network Firewalls: Nylas adheres to industry-standard practices for securing and maintaining our infrastructure, with additional protection being afforded by our firewalls. Each system uses firewalls to restrict access from external networks and between systems internally. To mitigate both internal and external risk, access is restricted to only the ports and protocols required for specific business needs.

Denial-of-Service (DOS) Prevention: Nylas implements best practices for preventing DoS attacks, including maintaining redundant DNS servers and following DoS prevention and mitigation practices. As an example, Nylas DoS security controls protect against a runaway account or malicious user who swamps the Nylas API with traffic. As a result, no one customer's bad application code can take down the Nylas API.

Distributed Denial-of-Service (DDOS) Prevention: Nylas data centers are hosted at AWS, and AWS uses a variety of proprietary DDoS mitigation techniques to guard against the risk of attacks. In addition, AWS's networks are multi-homed across a number of providers to achieve Internet access diversity and to ensure network availability.

Clustered Infrastructure: Automated systems deploy new code to Nylas clusters in real time, to ensure smooth transitions between software updates with no downtime.

TLS 1.3 Encryption: All web traffic between your application and Nylas is encrypted using TLS 1.3 (Transport Layer Security) to protect customer data. Our systems enforce TLS communication channels over public networks, and support only certificates signed by well-known CAs. The TLS protocol provides data encryption and authentication between customer applications and Nylas servers, and prevents third parties from gaining illegitimate access to information. Nylas upgrades to newer versions of TLS as needed to ensure the safety of our communications.

INFRASTRUCTURE AND PHYSICAL SECURITY

All Nylas physical infrastructure and data centers are housed in state-of-the-art secure facilities with industry, standard access controls and physical security measures. Nylas development machines run on unprivileged networks secured by VPN.

Nylas is hosted at Amazon Web Services (AWS) data centers, which are highly scalable, secure, and reliable. AWS complies with leading security policies and frameworks, including SSAE 16, SOC framework, ISO 27001, and PCI DSS Level 1.

SSAE 16, or more formally, Statement on Standards for Attestation Engagements No.16, is key guidance for reporting on internal controls for service organizations. SSAE 16 is used for reporting on the Service Organization Control (SOC) framework, which consists of SOC 1, SOC 2, and SOC 3. SOC 1 is focused toward an organization's internal controls over financial reporting, while SOC 2 and SOC 3 cover reporting for the security, availability, processing integrity, confidentiality, and privacy for service organizations, including cloud and data center providers.

AWS is certified to ISO 27001, which describes a systematic approach to managing sensitive information so that it remains secure. ISO 27001 covers a risk management process that encompasses people, processes, and IT systems. AWS is also Level 1 compliant under the Payment Card Industry (PCI) Data Security Standard (DSS), enabling customers to run applications on AWS's PCI-compliant infrastructure for storing, processing, and transmitting credit card information in the cloud.

Additional AWS physical security measures include:

At each AWS hosting site, Nylas servers are secured at all times by trained security guards, and access is authorized strictly on a least-privileged basis. The data centers use state-of-the-art electronic surveillance to monitor any suspicious activity.

Security Logs: AWS CloudTrail provides logs of all user activity to the Nylas servers. Nylas employees can monitor and track which actions were performed on each of the Nylas resources, and by whom.

Multi-Factor Authentication: AWS provides built-in support for Multi-Factor Authentication (MFA) to access Nylas servers. This requires the user to input her credentials, a password, and a two-factor PIN to protect against unauthorized use.

Multiple Redundancy Zones: AWS spans multiple geographic regions and Availability Zones, which allow Nylas servers to remain resilient in case of most failure modes, including natural disasters or system failures. In addition, each AWS data center has independent power grids, as well as redundant power, HVAC, and fire suppression systems. The AWS data centers use state-of-the-art practices for fault tolerance at each level of the system infrastructure, including Internet connectivity, power, and cooling.

RELIABILITY & SLAS

SLAs: At Nylas, our goal is to ensure you are able to successfully integrate and scale your business on our platform. To that end, all Nylas customers have free access to our Basic support plan. For additional assistance, we offer Business and Enterprise SLAs. You can learn more about our SLA plans here.

Status reports: Nylas maintains a live systems status report at https://status.nylas.com.

Communications: If a data breach occurs, Nylas notifies all impacted customers within 72 business hours of the data breach via email.

Nylas

Nylas.com

Github.com/Nylas

@Nylas