sublime

Security at Sublime

ENTERPRISE CLOUD PLATFORM

Single-Tenant SaaS

A high-level overview of the processes, procedures, and other technologies we've put in place to ensure the security of our platform.

https://sublime.security

sublime

Overview

Built by former offensive security professionals, security and privacy are core to everything we do at Sublime. From architectural choices to specific features, Sublime was designed with a defensive mindset and security baked in at multiple layers.

This paper provides an overview of the measures we've taken to architect, evaluate, and provide ongoing security of our products and operations. We're committed to working with security and IT teams, third-party auditors, and security researchers to protect the interests of our customers.

Security at Sublime covers the following key areas:

Topic 1
Deployment Model Overview

Topic 2
Infrastructure Security

Topic 3
AI and Machine Learning

Topic 4
Data Privacy

Topic 5
Data Security

Topic 6
Product Security

Topic 7
Personnel Security

© 2026 Sublime Security, Inc. All rights reserved

sublime

TOPIC 1

Deployment model overview

Single-Tenant SaaS is Sublime's dedicated hosted platform. Sublime provisions, operates, and maintains a fully isolated AWS environment exclusively for each customer. No infrastructure or compute resources are shared with other customers.

This model suits organizations that require dedicated infrastructure and want to manage their own encryption keys. It supports Bring Your Own Key (BYOK) encryption, allowing customers to encrypt all data at rest using their own AWS KMS key. Sublime manages the platform on the customer's behalf, handling patching, updates, scaling, and incident response.

Organizations that need to host data within their own cloud environment and retain full operational control should consider Self-Hosted.

TOPIC 2

Infrastructure security

Sublime provisions and manages each customer's dedicated AWS environment, including all infrastructure operations.

- Sublime is SOC 2 Type 2 certified across all five trust criteria: Security, Availability, Confidentiality, Privacy, and Processing Integrity. Sublime complies with GDPR and HIPAA requirements.
- The platform runs on AWS, whose infrastructure is designed to meet the requirements of GDPR, HIPAA, ISO/IEC 27001, PCI DSS, and other leading security and privacy frameworks.
- Each customer's environment runs in a dedicated AWS account. No compute, storage, or networking is shared with other customers.
- All infrastructure, with the exception of user access to the Management UI and API, runs within a logically isolated Virtual Private Cloud (VPC) not accessible from the public internet.
- Access to the Management UI and API can be further secured using an IP allowlist, security groups, or corporate VPN.
- Sublime staff access to update or maintain infrastructure is highly controlled, fully audited, and requires authentication at multiple service layers using MFA and physical hardware tokens.
- Application updates are managed and applied by Sublime.

© 2026 Sublime Security, Inc. All rights reserved

sublime

TOPIC 3

AI and machine learning

Sublime's platform detects and investigates email threats using purpose-built machine learning models, deterministic detection logic, and artifact-driven analysis. Models analyze observable technical signals — including email headers, links, attachments, sender behavior, authentication signals, and website content — using techniques such as natural language understanding (NLU), computer vision, anomaly detection, and behavioral analysis. Outputs are transparent, explainable, and auditable.

Where generative AI is used, it is scoped to two opt-in analyst-assist workflows: ASA (Autonomous Security Analyst), which accelerates email triage and investigation, and ADÉ (Autonomous Detection Engineer), which assists with detection rule creation. Both run via A WS Bedrock within the customer's dedicated environment. Customer data does not leave that environment, and third-party model providers cannot access or train on it.

Customers control how and where AI features are applied. Consequential actions — such as quarantine or message removal — are always governed by customer-defined policies, never taken autonomously.

TOPIC 4

Data privacy

Sublime maintains that the customer owns their data. In the Single-Tenant SaaS model, each customer's data is held in a fully dedicated environment. Sublime manages that environment on the customer's behalf, with access strictly controlled and limited to what is necessary to maintain the service.

- Email messages and all sensitive customer data are stored exclusively within the customer's dedicated AWS environment and are never co-mingled with another customer's data.
- Customers encrypt all data at rest using their own AWS KMS key (BYOK). Sublime manages the platform but cannot decrypt customer data without the customer's key.
- Sublime staff do not access customer email content during normal platform operation. Access for support or incident response is controlled, logged, and audited.
- Customers control whether email messages are shared with Sublime for threat intelligence and model improvement via the Share with Sublime setting in the admin panel. Customers can change this setting at any time.

© 2026 Sublime Security, Inc. All rights reserved

sublime

TOPIC 4: DATA PRIVACY, CONT.

Operational subprocessors

Sublime uses a limited set of operational subprocessors for platform monitoring, analytics, and support. These subprocessors handle operational metadata — not customer email content. Because customer data at rest is protected by the customer's own KMS key, Sublime's operational tooling operates only on metadata and system-level signals. Sublime has Data Processing Agreements (DPAs) in place with all subprocessors, and Standard Contractual Clauses (SCCs) govern any transfers outside the EEA. A full and current subprocessor list is available at sublime.security.

Data Retention and Portability

Customers control their own data retention periods from within the platform settings. Customers can export their data at any time via the platform UI, REST API, or automated export to S3. Available exports include full emails with attachments, audit logs, and configuration data.

Following contract termination, customer data is securely deleted within 90 days of the termination date or upon written request. Sublime will work with the customer's designated contact to confirm completion of data return or deletion in accordance with contractual obligations.

TOPIC 5

Data security

Physical and logical access to customer data is strictly controlled.

- All customer data, including backups, is encrypted at rest using the customer's own AWS KMS key (AES-256 or stronger).
- All communication between the Sublime platform and the customer is encrypted in transit using TLS/SSL with strong encryption algorithms and keys (2048-bit RSA or higher). Customers can also bring their own certificates.
- The Sublime application employs additional layers of encryption to protect access tokens (AES-256 or stronger).
- Sublime personnel do not have privileged access to customer data unless explicitly granted by the customer for administration and support purposes.
- All access to message data and platform functionality is governed by role-based access controls and strong authentication requirements.

© 2026 Sublime Security, Inc. All rights reserved

sublime

TOPIC 6

Product security

- Sublime supports single sign-on (SSO) through Google Workspace and Microsoft 365 OAuth, as well as through third-party providers like Okta and OneLogin using OIDC.
- Encryption keys are stored outside of the application in Sublime's AWS Secrets Manager, so that in the event of an application layer vulnerability, this data remains protected.
- Sublime adheres to OWASP guidelines to mitigate the risk of application attacks including cross-site scripting (XSS), SQL injection, Insecure Direct Object References (IDOR), and other vulnerabilities.
- The Sublime application supports IP allowlisting to further prevent unauthorized access.
- The Sublime application logs all actions taken by users in an immutable audit log viewable by administrators.

Sublime develops secure code and identifies vulnerabilities through:

- Automated source code analysis to identify common defects.
- Automated dependency analysis scanned for CVE information and remediated through automated pull requests.
- Manual source code analysis on security-sensitive areas of code.
- Mandatory peer review of all code pushed to production.
- Automated unit, integration, and end-to-end tests across isolated test, staging, and production environments. Data is never transferred between environments.
- Regular internal vulnerability scanning.
- Annual third-party penetration tests and application security assessments.

© 2026 Sublime Security, Inc. All rights reserved

sublime

TOPIC 7

Personnel security

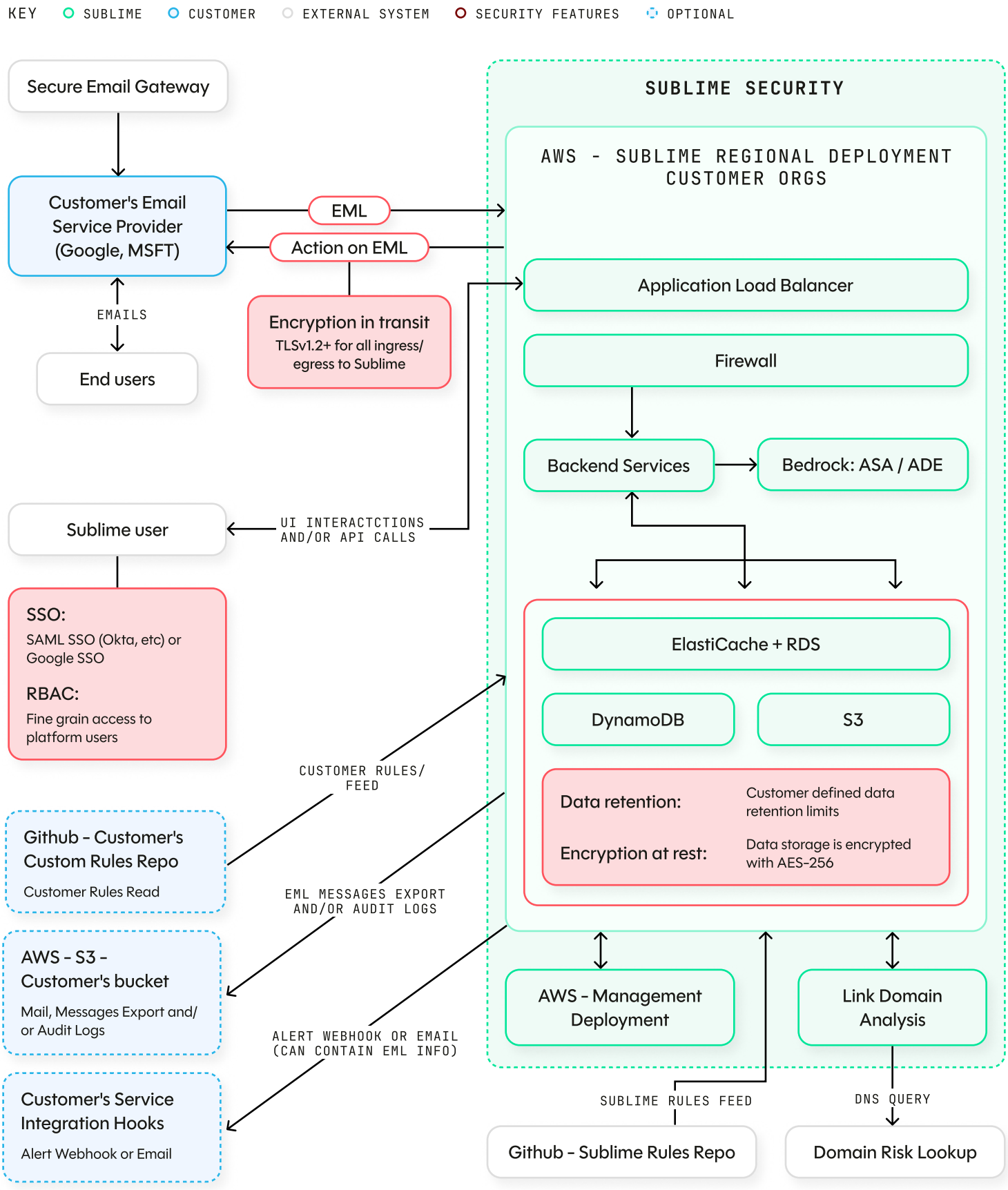
Security at Sublime starts with people and processes. These policies apply to all Sublime personnel (employees and contractors).

- As a condition of employment or engagement, personnel agree to comply with Sublime's information security, privacy, acceptable use, and confidentiality requirements. These obligations continue after separation where required by contract or law.
- Personnel receive the minimum level of access needed to perform their role. Access to production systems or customer data is granted only where required by job function.
- All personnel undergo background checks prior to engagement where permitted by law, including identity verification and employment history checks appropriate to the role.
- Personnel receive security and privacy awareness training as required by their role.
- Sublime maintains a documented Incident Response Policy covering detection, triage, investigation, containment, and recovery. For incidents that affect customer data confidentiality, integrity, or availability, Sublime notifies affected customers and works with them to remediate promptly.
- For sensitive and production systems, phishing-resistant authentication is required, including hardware security keys or device-bound authentication.
- Access is removed promptly upon separation.

© 2026 Sublime Security, Inc. All rights reserved

sublime

Network archictecture



© 2026 Sublime Security, Inc. All rights reserved