sublime

Security at Sublime

ENTERPRISE PLATFORM

Self-Hosted

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

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

Self-Hosted is Sublime's customer-operated deployment model. Customers deploy and run Sublime within their own AWS or Azure cloud account, retaining full ownership and operational control of all infrastructure, data, and configuration. Sublime delivers the platform as versioned software; the customer's team manages installation, updates, and ongoing operations.

This model suits organizations that must control the environment in which their data is hosted and processed — including those in highly regulated industries such as healthcare, financial services, and government. Sublime staff have no access to the customer's cloud environment, databases, or email content.

Organizations that want Sublime to manage infrastructure on their behalf while maintaining dedicated, isolated environments should consider Single-Tenant SaaS.

TOPIC 2

Infrastructure security

The customer's team provisions, operates, and maintains all infrastructure. Sublime has no access to the customer's cloud environment.

- Sublime's internal development, software delivery, and operational processes are SOC 2 Type 2 certified across all five trust criteria: Security, Availability, Confidentiality, Privacy, and Processing Integrity.
- The platform runs as a containerized workload on ECS/Fargate within the customer's AWS account, or via ARM deployment in Azure. The customer provisions and manages all underlying infrastructure.
- Sublime delivers software updates, container images, and ML models via Amazon Elastic Container Registry (ECR) and CI/CD pipelines managed by Sublime. This software delivery channel does not give Sublime access to the customer's environment or data.
- 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.
- Customers control the update cadence. Deployments can be configured to apply updates automatically as Sublime publishes new images, or updates can be reviewed and applied manually on the customer's own schedule.
- Traffic can be routed through a transparent SSL terminating proxy for inspection and audit at any time.

© 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 AWS Bedrock within the customer's own cloud 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 Self-Hosted model, the customer controls the environment entirely. Sublime has no default access to customer infrastructure, databases, or email content.

- Email messages and all sensitive customer data remain within the customer's own cloud environment at all times.
- Sublime staff cannot access the customer's environment unless the customer explicitly grants access for a specific support or remediation purpose.
- Customers manage their own encryption keys within their cloud environment.
- Customers can disable product analytics (PostHog) within their deployment.

© 2026 Sublime Security, Inc. All rights reserved

sublime

TOPIC 4: DATA PRIVACY, CONT.

Operational subprocessors

In Self-Hosted deployments, the platform runs in the customer's cloud account, which reduces routine sharing of customer content with Sublime-operated systems. Depending on configuration and enabled features, limited operational data (e.g. service and usage telemetry) may be sent to Sublime systems and subprocessors. Customer content is shared with Sublime-operated systems only when customer-enabled features require it — specifically Share with Sublime and Link Analysis where applicable. 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

In the Self-Hosted model, customers retain direct control over all data within their own environment. For any data held by Sublime — such as data shared via Share with Sublime or Link Analysis — customers may request deletion at any time. Following contract termination, any Sublime-held 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.

TOPIC 5

Data security

Physical and logical access to customer data is strictly controlled.

- All systems that store or transmit customer data, including backups, are encrypted at rest (AES-256 or stronger). Customers manage their own encryption keys within their cloud environment.
- 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 bring their own certificates.
- The Sublime application employs additional layers of encryption to protect access tokens (AES-256 or stronger). Keys are stored in the customer's own cloud secrets manager.
- Sublime personnel cannot access customer-managed infrastructure 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 the customer's own cloud 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

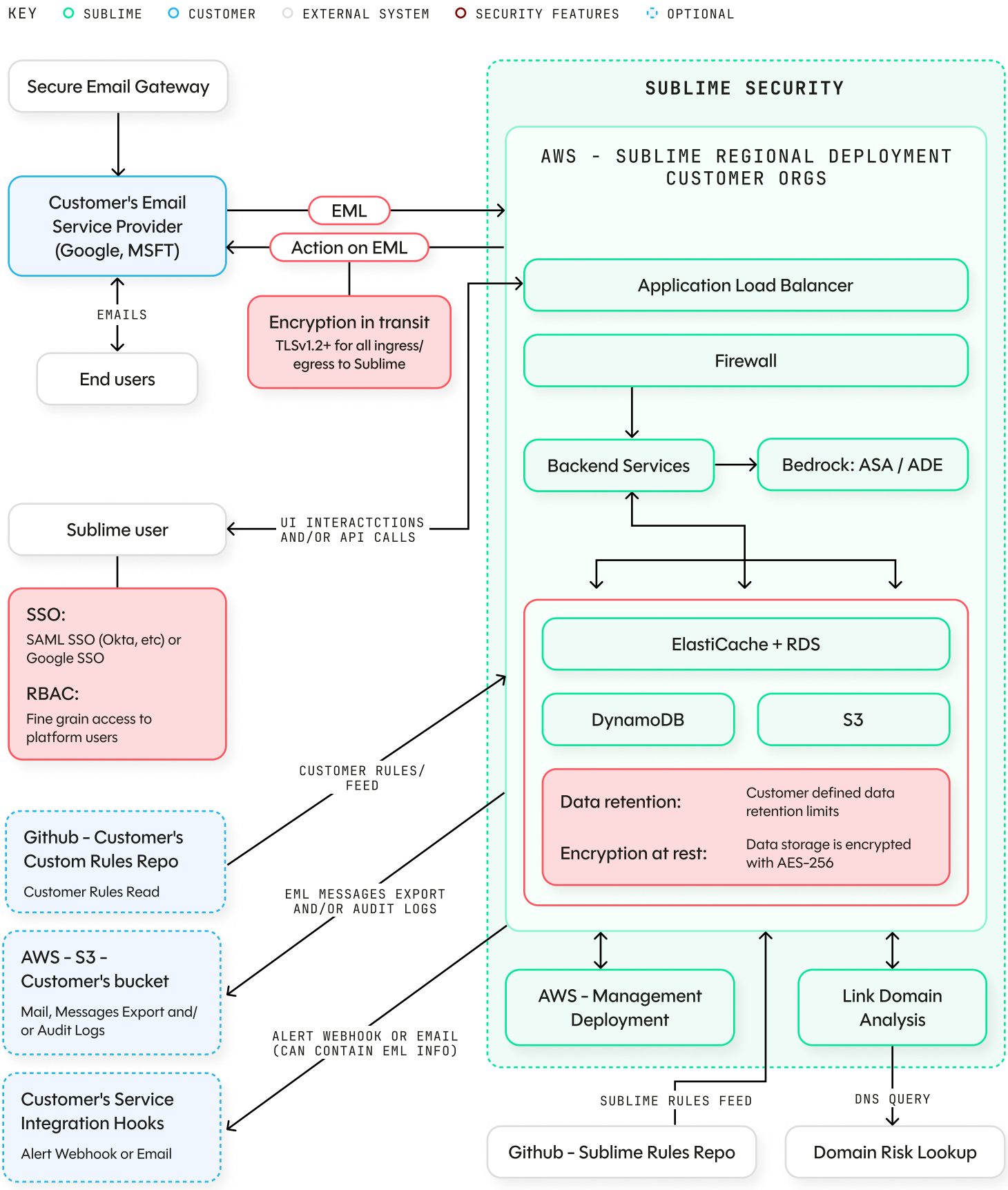
Security at Sublime starts with people and processes. These policies apply to all Sublime personnel (employees and contractors).

- 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