Security and Architecture Overview

Material is designed with the most security-conscious Security and IT teams in mind. We've also taken deep care to ensure our internal policies are secure from the get-go.

This paper provides a current overview of the state of Material's security. Our approach takes advantage of modern cloud computing practices while adhering to strict policies and controls that ensure the security and integrity of the data we touch.

Material is committed to working with security and IT teams, third-party auditors, security researchers, and other professionals to continually strengthen our investments across all aspects of our company and product.

Overview

Security on Material consists of five critical components. These enable us to maintain security and integrity on multiple levels for data ingestion, transfer, storage, and access:

- Corporate Governance
- Data Security
- Security Architecture
- Product Security
- Data Privacy

Corporate Governance

Our commitment to the security and privacy of customers starts with information security policies that guide the how we run business, product, and operations. Some of these are outlined below.

- Employees and contractors sign agreements that require them to preserve and protect the confidentiality of sensitive information they may access while doing their jobs.
- We conduct mandatory background checks for all employees.
- Employees are required to enable two-factor authentication in every internal and external service that is in the critical path of the customer data.
- Employees receive security awareness training monthly.
- We have a well-documented Incident Response Plan, which requires the prompt disclosure of customer data confidentiality, integrity and availability issues to a customer's security organization and working with them for prompt remediation.

Data Security

Physical access to customer information is strictly controlled.

- The Material application does not store any customer data, including any personally identifiable information, anywhere outside of the customer's deployment.
- All systems that store or transmit customer data, including backup, are encrypted at rest (AES-256 or stronger).
- Material employees do not automatically have privileged access to the application, unless granted by customer.
- Only customer-designated operators can access the deployment for the purposes of administration and support.

Security Architecture

Material's deployment model side steps many of the traditional sources of third-party risk while keeping Material easy to use and setup.

Every Material customer gets their own Google Cloud Platform (GCP) project that is single-tenant and fully isolated from other customers. The customer's GCP project wholly contains the Material application and data. As a result, no customer data is ever stored or processed outside the project.

All customer projects have GCP Security APIs enabled and monitored by Material's Security Team.

GCP is an industry-leading cloud service platform that provides Material with professional security staff, nondescript facilities, controlled access, video surveillance, intrusion detection, and other security features. All data is separated from outside connections, and access is limited to select system administrators approved by the customer.

- Material is a SOC 2 Type 2 certified provider.
- All Material clients use TLS/SSL when communicating with deployments for data transfers and API calls.
- We can configure Material to meet customer's requirements for data retention.
- Every Material deployment includes immutable audit logs stored within the customer GCP project and are available for use by the customer. Every user and administration action is logged and can be audited at any time by the customer.
- The GCP infrastructure has been designed and managed in compliance with regulations, standards, and best-practices, including HIPPA, SOC 1, SOC 2, SOC 3, PCI DSS, ISO 27001, FedRAMP, FIPS 140-2, CSA and GDPR.
- More on Google Cloud's security policies and compliance certifications.

Product Security

Material is built with industry-tested technology and security practices.

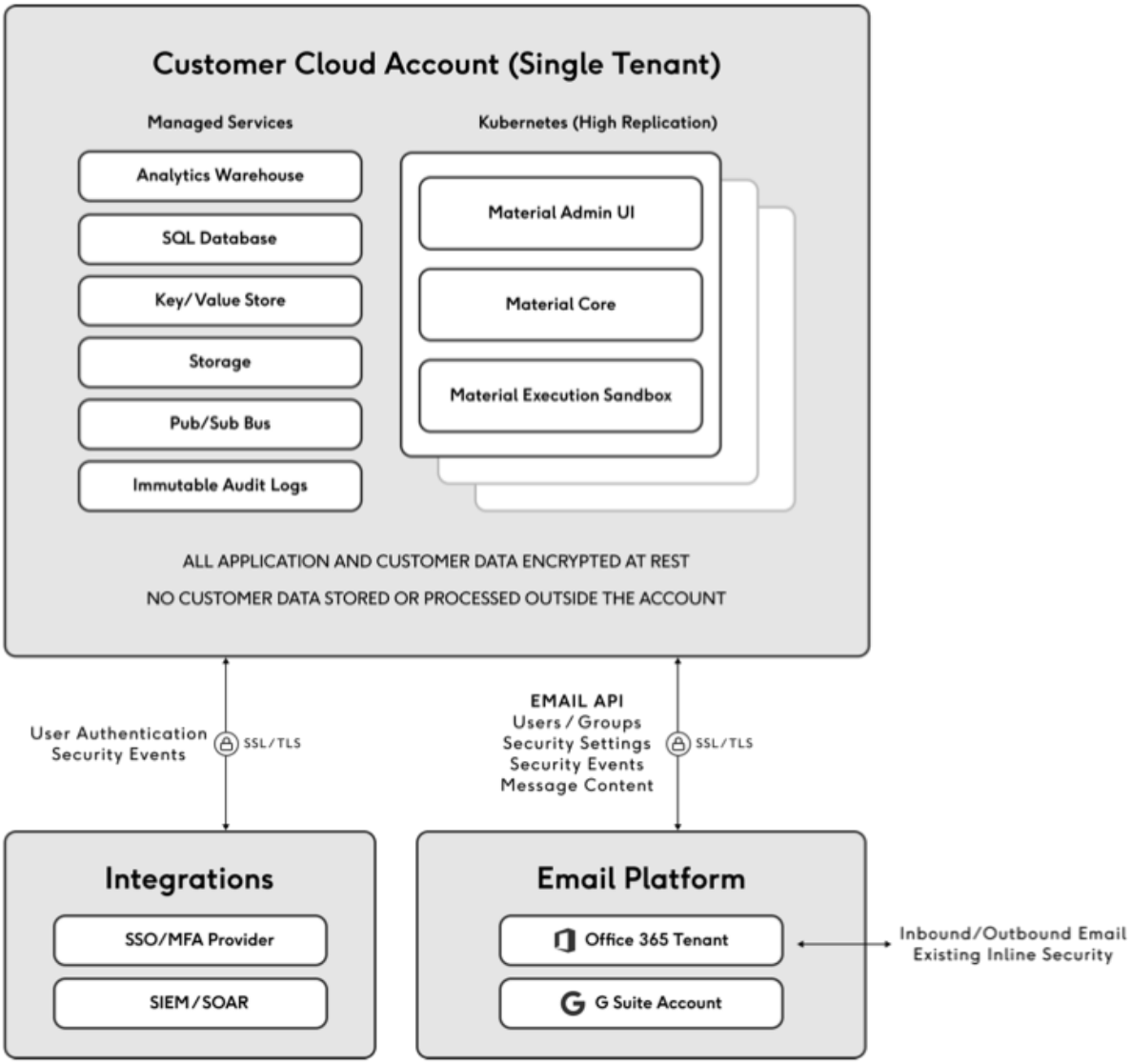
- Material supports single sign-on (SSO) through G Suite and Office 365 OAuth for authentication.

- There are no Material-specific application usernames, passwords or hashes created or stored. All access tokens are encrypted and securely stored in the customer's project.
- Material adheres to OWASP guidelines for security best practice.
- Material uses a combination of methods to verify application correctness and security including mandatory peer review, suites of automated unit and integration tests, end-to-end diagnostics running on live systems as well as pre-release and post-release validation tests.
- Material runs a whitebox pen-test assessment at least once a year with reputable security firms. We also run a private bug bounty program through HackerOne.

Data Privacy

- Material maintains that the customer's data is wholly owned by the customer and due to the way our GCP project is designed, we're able to manage, co-manage or relinquish control of the GCP project to the customer at any point during or after the engagement.
- We adhere to all restrictions and limitations defined by your email service provider.
- For more information: Privacy Policy and Subprocessors.

Architecture and Data Flow



Isolation and Control

Customer deployments operate as fully isolated instances in the public cloud. Only customer-designated administrators can access them.

Encryption at Rest and Transit

Application and customer data is encrypted at rest with AES-256 and all data transfers and API calls happen over SSL/TLS.

Immutable Audit Logs

Every admin action in Material is logged to an immutable audit log inside the customer's public cloud instance.