DealLayer Security Overview

The secure transaction layer for SharePoint, OneDrive, Box, Google Drive and Dropbox.

Architecture

DealLayer is an overlay control plane. Source documents remain in the customer's existing tenant. Access is brokered just-in-time through scoped tokens, and overlay controls (watermarks, expiry, redactions) are applied at the moment of delivery. DealLayer never takes custody of customer documents.

Identity & access

Authentication	SAML 2.0, OpenID Connect (OIDC), Microsoft Entra ID, Okta, Ping, Google Workspace
Provisioning	SCIM 2.0 for user lifecycle and group sync
MFA	Enforced for external users; inherited from IdP for internal users
Access model	Role-based access with time-bound, IP-restricted external sessions
Revocation	One-click global revocation across sessions, devices and cached previews

Data protection

• Encryption in transit: TLS 1.3 across all connections.

• Encryption at rest: AES-256 for audit, metadata and configuration stores.

• Data minimization: only metadata required for access control and audit is processed.

• No model training on customer content. No third-party data sharing.

• Data residency: US, EU and UK regions available; customer-selectable at workspace creation.

Audit & monitoring

Every user action — views, searches, downloads, Q&A and admin changes — is recorded in a tamper-evident audit log. Logs are exportable to Splunk, Microsoft Sentinel, Datadog and other SIEMs via syndicated stream or API.

Watermarking

Dynamic per-session watermarks are rendered on previews and downloads with user identity, IP, timestamp and session fingerprint — enabling forensic tracing of any leaked artifact back to the originating session.

Compliance

SOC 2 Type II	Audited annually
ISO/IEC 27001	Certified
GDPR / UK GDPR	Compliant; EU SCCs available
HIPAA	BAA available on Enterprise plan
FINRA / SEC 17a-4	Supported via WORM-mode audit export

Shared responsibility

DealLayer provides the overlay control plane, audit pipeline and external access perimeter. Customers retain control of their source repository, identity provider configuration, retention policies and data classification. Workspace administrators are responsible for permission assignment and external-user lifecycle.

This document is maintained by DealLayer to summarize platform capabilities. It is not an independent attestation. Request the full security pack (SOC 2 report, penetration test summary, DPA) at security@deallayer.io.