TrustLayer

CLOUD ACCESS SECURITY BROKER | AI GOVERNANCE PLATFORM

SAMPLE REPORT

Executive Security Assessment

AI Usage & Data Exposure Review

Reporting Period: Last 30 Days | Prepared by TrustLayer Security Intelligence

14,083	13,342	5	30 days
Upload Events	AI App Events	AI Platforms	Reporting Period

Audience: CISO | IT Leadership | Risk & Compliance | Executive Management

01 Executive Summary

The TrustLayer CASB analysis confirms that the organisation has already entered widespread, operational AI adoption. This is no longer an emerging or experimental phase. Within a single 30 day assessment window, the platform identified 14,083 file upload events and 13,342 AI related application events spanning five distinct external AI ecosystems.

The primary finding of this assessment is not simply that AI is being used at scale. The critical governance challenge is the uncontrolled movement of organisational data into external AI platforms, with limited visibility, no application governance framework, and no sanctioned versus unsanctioned application separation in place prior to this assessment.

TrustLayer CASB is already delivering the foundational visibility required to understand and govern this rapidly evolving environment. The newly introduced Sanctioned Applications capability provides the operational mechanism to transition from reactive awareness to proactive, enterprise grade AI governance, without disrupting legitimate productivity.

STRATEGIC CONTEXT

- → AI adoption is operational, not experimental. User behaviour confirms daily AI engagement across all major platforms.
- → 14,083 upload events in 30 days signals active data movement into external AI ecosystems at enterprise scale.
- → Shadow AI is the norm, not the exception. Users are naturally adopting whichever AI tool best meets their immediate needs.
- → Without governance controls, the organisation faces potential uncontrolled data exposure and compliance exposure.
- → TrustLayer CASB provides the visibility infrastructure required to implement meaningful, low disruption AI governance.

02 Key Findings

The assessment produced multiple categories of critical findings, each with direct implications for the organisation's security posture, data governance framework, and regulatory compliance obligations.

FINDING 1 Large-Scale Operational AI Adoption

The environment demonstrated extensive, daily interaction with multiple external AI platforms. This is not incidental usage; the event volumes confirm that AI tools have become embedded in core operational workflows. With 13,342 AI related events recorded across five platforms in a single month, AI is functioning as an operational utility rather than an experimental tool.

AI Platform	Event Count	% of Total	Risk Classification
ChatGPT	6,020	45.0%	PUBLIC, HIGH VOLUME
Copilot Business	3,791	28.4%	ENTERPRISE, SANCTIONED
Claude	1,801	13.5%	PUBLIC, MONITORED
Gemini	334	2.5%	PUBLIC, EMERGING

FINDING 2 Significant File Upload Activity at Enterprise Scale

The most operationally significant finding is the volume of file upload events: 14,083 uploads recorded across the 30 day assessment period. This represents an average of approximately 469 upload events per day, each event representing organisational data being transferred into an external AI ecosystem. Upload activity is the primary data exposure vector in AI governance.

- Organisational documents uploaded to external AI processing environments
- Internal business content transmitted beyond the organisation's security perimeter
- Sensitive data potentially retained by third party AI platforms
- Compliance implications under data protection and industry specific regulatory frameworks
- Limited prior visibility into which content was being uploaded or to which platforms

FINDING 3 Widespread Shadow AI Behaviour

The simultaneous usage of multiple AI platforms, including both enterprise and public consumer services, confirms a classic Shadow AI pattern. Users are independently adopting whichever AI tool best meets their immediate operational requirement, without centralised oversight, policy guidance, or governance controls.

Fragmented AI Adoption	Multiple uncoordinated AI ecosystems in active use simultaneously.
Uncontrolled Data Flows	Uploads occurring to platforms with varying data governance standards.
Inconsistent Handling	No uniform data classification or handling protocol applied pre upload.

Governance Gaps	No application level policy enforcement in place at point of upload.
Visibility Deficit	Without TrustLayer CASB, this activity would have remained undetected.

03 Shadow AI & Data Exposure Analysis

Shadow AI represents the most operationally complex dimension of this assessment. Unlike traditional shadow IT, where the primary concern is software licensing and vendor risk, Shadow AI introduces a data exposure vector that is continuous, high volume, and largely invisible without purpose built CASB tooling.

AI Platform	Data Exposure Consideration
ChatGPT (OpenAI)	Consumer tier may use submitted content for model training depending on account settings.
Claude (Anthropic)	Content handling governed by Anthropic's privacy policy; requires per user API review.
Gemini (Google)	Data subject to Google's privacy framework; enterprise controls vary by account type.
Google AI Studio	Developer oriented platform requiring governance review before organisational use.
Unknown / Other Apps	Usage of additional AI tools cannot be excluded; further discovery may reveal additional platforms.

04 Business Value Delivered by TrustLayer CASB

The TrustLayer CASB deployment is already delivering measurable, operational security value. This section quantifies the specific capabilities that have been activated and the direct security outcomes they produce.

Capability Delivered	Measurement	Security Outcome
AI Application Discovery	5 platforms, 13,342 events	Broad visibility into AI ecosystem usage across the organisation
Shadow AI Visibility	Concurrent multi-platform	Significant Shadow AI and unsanctioned AI usage surfaced through CASB visibility
Upload Monitoring	14,083 events captured	Upload events are logged, timestamped, and attributable within current CASB policy scope
User-Level Behavioural Analysis	Per-user event attribution	Identify high risk users and behavioural anomalies
Unsanctioned App Identification	Full app inventory	Complete catalogue of AI platforms in active use
Governance Intelligence	Assessment-ready reporting	Evidence base for audit, compliance, and board reporting
Executive Reporting	CISO-ready dashboards	Structured security intelligence for leadership briefings

05 Strategic Recommendations

The following recommendations are structured around TrustLayer CASB's phased governance approach, designed to deliver immediate risk reduction whilst preserving operational flexibility and avoiding blanket AI blocking strategies that would negatively impact productivity.

Phase 1: Define Sanctioned Applications Immediate, 0 to 30 days

- Activate TrustLayer CASB Sanctioned Applications capability within the existing deployment.
- Identify and formally designate approved AI platforms for organisational use, commencing with Microsoft Copilot Business.
- Maintain comprehensive visibility across all AI usage to inform Phase 2 policy decisions.
- Separate sanctioned versus unsanctioned application classifications within the platform.
- Communicate the sanctioned AI framework to users to set clear expectations.

Phase 2: Control Upload Activity Short-term, 30 to 90 days

- Allow productive, unrestricted uploads to formally sanctioned AI platforms.
- Block file uploads to unsanctioned AI applications, reducing the primary data exposure vector.
- Monitor upload volumes and patterns to confirm risk reduction and identify remaining gaps.
- Review user feedback and adjust the sanctioned application list as legitimate business requirements emerge.
- Produce updated upload metrics to demonstrate measurable risk reduction to executive stakeholders.

Phase 3: Progressive Enforcement Medium-term, 90+ days

- Gradually tighten controls to restrict access to unknown and unclassified AI ecosystems.
- Apply application governance policies based on risk classification and verified business need.
- Extend upload control policies to cover document type, sensitivity classification, and user group.
- Establish quarterly governance reviews to assess maturity progression and update the sanctioned application register.
- Develop an executive reporting framework to demonstrate ongoing AI governance effectiveness to board and regulators.

This report was generated from TrustLayer CASB telemetry. Figures shown are illustrative, sample data for partner and prospect demonstration purposes.