CONFIDENTIAL

Sensitive Data Risk Report

Customer Data Universe | Data Security Posture Assessment | June 2026

4.56 TB	42.7M	HIGH	14	90%
Sensitive Data Scanned	Corporate Objects	Overall Risk Rating	Unsanctioned AI Services	Data Estate Unmonitored

Executive Summary

HIGH

Overall Risk Rating

Regulated data actively exposed

PII · PHI · PCI

Regulated Data Types Exposed

Across M365, shadow cloud & AI

14 Services

Unsanctioned AI Platforms

Processing sensitive data without governance

CRITICAL: PHI and PCI/DSS data is actively flowing to 14 unsanctioned AI services and multiple shadow cloud platforms with no governance controls, no audit trail, and no deletion rights — constituting a notifiable breach condition under the Privacy Act 1988 and NDB Scheme.

Top Risk Findings

CRITICAL PHI and PII detected in Shadow Cloud services including Adobe Experience Cloud and Kiteworks → direct Privacy Act & APRA CPS 234 exposure

CRITICAL 14 unsanctioned AI services processing sensitive member data with zero governance controls or data residency visibility

HIGH Over 150 GB of sensitive data concentrated in 4 user accounts → elevated insider risk and access sprawl requiring immediate review

HIGH PCI/DSS and credential data identified in outbound flows to non-approved shadow platforms

CISO Priority Actions

1. Enforce controls immediately on 14 shadow AI platforms and shadow cloud services transmitting regulated data via Skyhigh Web DLP & Application Control
2. Conduct access review for the 4 high-volume user accounts → validate business justification, data ownership, and least-privilege status
3. Enable CASB inline controls for sanctioned M365 apps holding the highest sensitive data volumes
4. Expand DSPM capacity to 300 TB to gain full-estate visibility → 90% of your data is currently unmonitored

Three Critical Areas Requiring Board Attention:

Material Business Exposure | **Audit & Board Defensibility** | **Prioritised Remediation**

Slides 3–7 address each area in detail

Thank You