

ENDPOINT · EMAIL · NETWORK · GENAI

Data Loss Prevention

Your data. Intact.

One agent. Every exit ramp. Real time.

Modern workplaces expose sensitive data across an expanding range of channels — browsers, cloud applications, AI tools, email, removable devices, screenshots, clipboard operations and collaboration platforms. iSquare Tech Labs Data Loss Prevention uses a lightweight endpoint agent to provide real-time visibility and protection across these channels, helping organisations detect, monitor and prevent sensitive data leakage **before information leaves the endpoint.**

32+

Built-in detectors

25

Countries covered

3

Operating systems, one agent

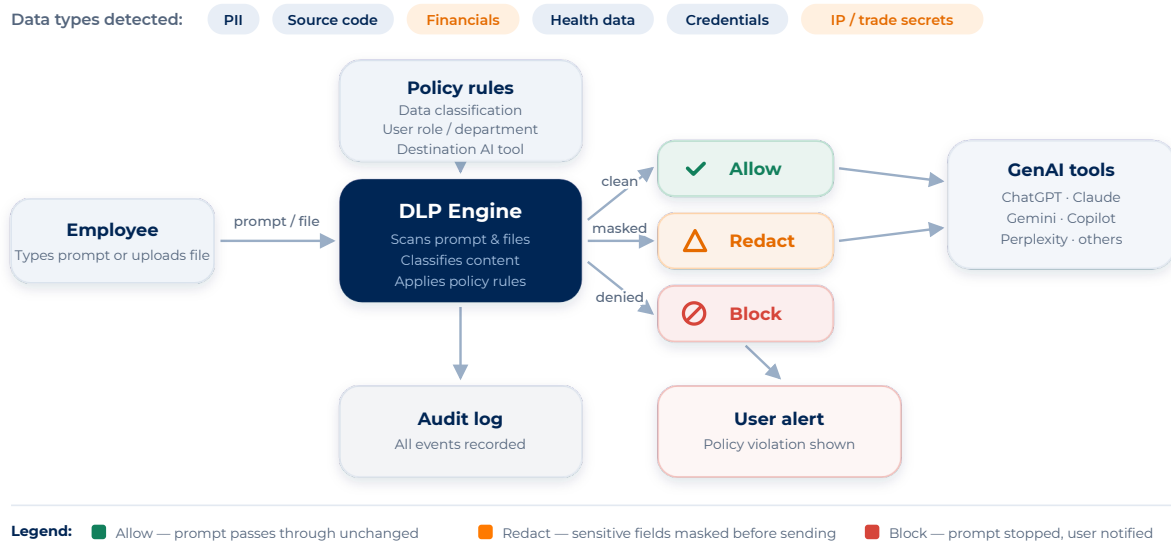
3

Enforcement modes

Product features

GenAI Data Loss Prevention

- Protect sensitive organisational data from being shared with public and enterprise GenAI platforms including ChatGPT, Claude, Gemini, Copilot, Perplexity, Poe, Hugging Face, Grok and other AI assistants.
- Inspect and control AI prompts in real time to prevent users from submitting confidential, regulated or policy-violating information to GenAI applications.
- Monitor and scan streamed AI-generated responses dynamically to detect and mask sensitive or restricted information before it becomes visible to end users.
- Enforce centralised AI usage policies across browser-based and desktop-accessed AI platforms to support enterprise governance and compliance requirements.
- Provide visibility, monitoring and audit reporting for GenAI interactions, helping organisations manage AI adoption securely while reducing the risk of sensitive data exposure.



GenAI DLP — every prompt is inspected on the device before it reaches the AI provider.

01 Removable device security & monitoring

Enforce security controls for removable and peripheral devices including USB drives, external HDD/SSD storage, printers and network-connected devices.

- › Identification and restriction of unauthorised or non-compliant devices through centralised, policy-based device control.
- › Hot-plug detection to control and manage access to external storage, preventing unauthorised data transfer while letting administrators define approved device access policies.
- › Monitor, audit and generate detailed reports on removable media usage and data transfer activities.

02 Securing outbound email communications

Define intelligent email security policies based on content, attachments, recipient domains and sensitivity classifications.

- › Inspect outbound emails and attachments across platforms such as Gmail, Outlook and Microsoft 365 to prevent unauthorised sharing of sensitive data.
- › Apply automated policy-driven actions including blocking, quarantine, administrator approval workflows, warning notifications and sensitive data redaction.
- › Control email communication through domain-based whitelisting and restriction policies for trusted and high-risk recipients.
- › Provide centralised monitoring, audit logs and reporting for visibility into email-based data movement.

03 File upload & secure content sharing control

Restrict unauthorised file uploads based on file type, content classification, application or organisational security policies.

- › Prevent sensitive files, images and clipboard-based content from being shared through browsers, cloud applications and web-based messaging platforms such as WhatsApp Web.
- › Block potentially harmful, non-compliant or unauthorised content uploads to reduce the risk of malware, ransomware and sensitive data leakage.
- › Scan PDF, DOCX, XLSX, PPTX, TXT, CSV, ZIP, RAR and 7z files for sensitive information.
- › Detect and flag password-protected or encrypted archives for policy-based control and review.

04 Endpoint channel control

Kernel-level enforcement on the device itself, so protection applies before any application can read or move the data.

- › Instant clipboard wipe when sensitive content is copied, leaving no window in which to paste it.
- › Print guard that closes the print dialog on every path — keyboard shortcut and menu alike.
- › Screenshot and screen-share control on protected content.
- › Image-open and file-save blocking, with on-device OCR that reads tilted, low-contrast camera shots of cards and identity documents.
- › Enforcement continues when the device is offline, with no network dependency.

Forensics, audit & live telemetry

- › Centralised forensic dashboard with detailed visibility into endpoint activities, including sensitive data detections, clipboard events, web uploads, OCR findings and removable media usage.
- › Perform initial endpoint discovery scans to identify and map sensitive data stored across enterprise devices, helping organisations uncover potential regulatory and security exposures early.
- › Maintain tamper-aware audit records with contextual information such as endpoint, user, timestamp, policy action and masked sensitive data references for secure investigation and compliance reporting.
- › Provide real-time endpoint telemetry and geo-location awareness to support location-based policies, adaptive enforcement and protection for devices operating outside approved regions.
- › Deliver comprehensive monitoring, search and drill-down capabilities for faster incident investigation, operational visibility and compliance management.

Why iSquare TechLabs Data Loss Prevention?

Detection that doesn't need a specialist	Detect sensitive information using built-in data protection policies covering identities, payment cards and banking information across multiple global regions, with support for custom detection rules configurable directly from the management console.
Audit evidence regulators accept	Provide detailed forensic and compliance-ready audit records including user, endpoint, file path, timestamp, policy action and masked sensitive data references. Raw personal data never leaves your own database.
One console, three operating systems	A single cross-platform agent covers Windows, Linux and macOS, managed from one web console with live findings, a fleet map and exportable per-policy reports.
Three operating postures	Support flexible enforcement modes including monitoring, selective content blocking and strict policy enforcement, with real-time policy updates delivered directly to endpoints by heartbeat — no re-install and no user logout.
Day-one visibility into existing exposure	Perform automated endpoint discovery scans to identify and map sensitive data already stored across enterprise devices, helping organisations quickly uncover hidden compliance and security risks.

Compliance coverage

Detectors and evidence map out of the box to **GDPR, PCI-DSS, HIPAA, PDPA, India DPDP, SOX** and **ISO 27001**. Card and identity numbers are checksum-validated, so random digit strings never raise a false alarm.



+91 86670 69354

sales@isquaretechlabs.com

www.isquaretechlabs.com



Scan to visit