

HEALTHCARE Use Case

Where Patient Data Walks Out.

Six ways clinical data leaves a hospital endpoint. What DLP Defense does about each, and what it stops.

01

Patient records uploaded to personal cloud

The endpoint agent inspects every upload across every application, using regex and AI detection on content, and stops the transfer at the device.

RESULT- Records stop at the laptop, on any network.

02

Risk that builds quietly in one user

Behaviour intelligence analyses activity over time and maintains a dynamic risk score per user, so a pattern is visible while it is still a pattern.

RESULT- The at-risk user surfaces early, not in a post mortem.

03

Legitimate work blocked at the wrong time

A monthly self-override quota lets clinicians release blocked uploads with written reasoning; beyond the quota, requests go to admin approval.

RESULT- Care is not delayed, and every exception has a reason on file.

04

No way to prove who did what

Upload activity is logged across all endpoints and applications, and Incident Investigator compiles a per-user report covering all of their incidents.

RESULT- A defensible record when breach notification is on the table.

05

One policy cannot fit every department

Unlimited custom policies, with permissible and blocked applications and content types, assigned to individual users or to whole groups.

RESULT- Radiology, billing and HR governed on their own terms.

06

Clinical notes pasted into public AI tools

Shadow AI governance detects unrecognised AI tools, blocks first use, and routes them for admin verification and whitelisting.

RESULT- No patient text in a model you never approved.

REPORTED AS

Incidents by policy and user, dynamic risk scores, override and approval history, and Shadow AI tools pending verification on one dashboard.



Call for more details...

+91 88700 07553

www.effortly.ai

MANUFACTURING Use Case

Where designs and Pricing walk out.

Six ways engineering and commercial data leaves a plant endpoint and how DLP Defense detects and stops each.

01

CAD files leaving a departing engineer's laptop

The endpoint agent inspects uploads across every app, using regex and AI detection to block transfers at source.

RESULT- Drawings do not leave with the notice period.

02

Supplier pricing pasted into public AI tools

Shadow AI governance detects unrecognised AI tools, blocks first use, and routes them for admin approval before whitelisting.

RESULT- Costings and tender data stay out of unapproved models.

03

Production held up by a blocked file

A monthly self-override quota lets an engineer release a blocked upload with written reasoning. Beyond it, an admin approval request is raised.

RESULT- The line keeps moving, with the exception on record.

REPORTED AS

Incidents by policy, plant and user, dynamic risk scores, override history, and Shadow AI tools awaiting approval on one dashboard.



04

No trail after an IP leak

A full upload log across every endpoint, with Incident Investigator producing a per-user report and the investigation workflow that produced it.

RESULT- Evidence ready for legal, insurance or a customer audit.

05

Contractors working on your devices

Policies assigned per user or group, with permissible apps and content types, plus a dynamic risk score for each.

RESULT- Visiting engineers bounded without separate hardware.

06

Unknown software on plant machines

Autonomous response identifies new apps and websites, flags unrecognised activity, and shows agent status per endpoint.

RESULT- Shop-floor endpoints stop being a blind spot.



Call for more details...

+91 88700 07553

www.defensely.ai

AUTOMOBILE Use Case

Where a platform programme leaks.

Six ways design, sourcing, and pre-launch data leaves an endpoint and how DLP Defense detects and stops each.



01

Design files heading somewhere unapproved

Policies define which applications users may upload through and which content types are restricted, ensuring only approved routes remain available.

RESULT- One sanctioned path for drawings, and no other.

02

A file-transfer site nobody knew was in use

Autonomous response builds a view of the applications and websites people use, and flags unrecognised activity for review and action.

RESULT- The channel is named before sourcing data uses it.

03

A joint programme with a Tier-1 partner

Partner groups are assigned programme-specific policies, so collaboration access can be added or removed without rebuilding rules.

RESULT- Programme boundaries survive the next collaboration.

04

A leak that surfaces after the reveal

Investigations run as tracked cases, with incidents collected against users, findings recorded, and ownership maintained throughout.

RESULT- Something legal and the partner contract can rest on.

05

Machines that quietly stop being covered

Agent status is monitored for every endpoint, making coverage gaps visible when a device stops checking in.

RESULT- No unmonitored machine inside the design centre.

06

A build release stopped at a gateway

Override requests enter an approval queue with the file and business justification attached, and every decision is fully logged.

RESULT- A named person owns every release, not a quota.

REPORTED AS

Incidents by policy, programme, and user, risk scores, override history, approval logs, and Shadow AI tools awaiting verification on one dashboard.



Call for more details...

+91 88700 07553

www.defensely.ai

IT & BPO Use Case

Where client data walks out.

Six ways your clients' data leaves a delivery endpoint.
What DLP Defense does about each, and what it stops.

01

Remote agents on client work

Inspection runs on the device rather than the network, so the same content rules hold on home broadband, a client VPN or the delivery floor.

RESULT- Hybrid delivery without a hybrid security posture.

02

Different AI rules by client

Each account becomes its own group with its own whitelist, so a tool cleared for one engagement stays blocked on every other.

RESULT- Contractual AI terms enforced account by account.

03

Escalations outside shift hours

A team lead spends one of the month's overrides to release the file, with the reason typed in. Anything past the quota queues for an admin decision.

RESULT- Night-shift SLAs met without a standing exemption.

04

The agent who is already halfway out

Each person carries a risk score that moves with their own activity, so the shift before a resignation reads differently from the fifty before it.

RESULT- High attrition stops being an unmeasured exposure.

05

Subcontractors in the delivery chain

Agent status per endpoint shows which of their machines are actually reporting, and which have gone quiet on an account you are accountable for.

RESULT- Coverage you can state to the client, per device.

06

A client audit asks for the last quarter

The dashboard already holds incidents by policy and user, override and approval history, and the AI tools still awaiting verification.

RESULT- The evidence pack is a report, not a project.

REPORTED AS

Incidents by policy, programme, and user, risk scores, override history, approval logs, and Shadow AI tools awaiting verification on one dashboard.



Call for more details...

+91 88700 07553

www.defensely.ai

RETAIL Use Case

Where customer data walks out.

Four ways customer and commercial data leaves an endpoint and how DLP Defense stops each.

01

A loyalty list attached to an outbound email

Rules detect sensitive data patterns such as card numbers, phone numbers, and addresses, and block them at the device regardless of the application used.

RESULT- Customer records cannot be mailed out of the business.

02

Festive hires who start on a Monday

Policies follow user groups rather than devices, so seasonal staff inherit access rules at login and lose the when removed from the roster.

RESULT- Peak-season headcount governed from day one.

03

A merchandiser tries a new AI assistant

Unrecognised tools are blocked on first use, with users informed before supplier, pricing, or margin data can be exposed.

RESULT- Curiosity costs nothing, and teaches the estate.

04

A promotion file needed before opening

Overrides allow authorised users to release blocked content with a reason; additional requests require admin approval.

RESULT- Tomorrow's promotion ships without a standing exemption.

05

Franchise stores outside your payroll

Agent status is monitored per endpoint, making tills and back-office PCs that stop reporting visible as coverage gaps.

RESULT- Franchise coverage stated store by store, not assumed.

06

Loss prevention asks about last week

Incidents filter by policy, user and site, so the review opens on which stores generate exceptions and which people are behind them.

RESULT- A weekly review with the estate already ranked.

REPORTED AS

Incidents by store, region, and policy, risk scores, override history, approval logs, and Shadow AI tools awaiting verification on one dashboard.



Call for more details...

+91 88700 07553

www.defensely.ai



EDUCATION Use Case

Where academic data walks out.

Six ways student, exam, and research data leaves an endpoint and how DLP Defense stops each.

01

An unpublished question paper

Exam office staff operate under dedicated policies, ensuring papers and marking schemes cannot leave the device through any application.

RESULT- A paper cannot leave before the exam does.

02

Marks pulled from the student system

Authorised exports are still logged, with activity recorded and risk scores adjusted when behaviour falls outside normal patterns.

RESULT- An unusual export reads as unusual, not as outline.

03

A researcher pastes data into a public AI model

Unrecognised AI models are blocked on first use, with approval requests routed to a designated administrator.

RESULT- Consent terms survive the deadline pressure.

04

A results leak before publication

Investigations run as tracked cases, with incidents, findings, and ownership maintained from start to closure.

RESULT- An answer the examination board can act on.

05

Shared terminals across teaching labs

Estate visibility shows which applications and websites lab machines access, making unrecognised destinations easy to identify.

RESULT- Open labs stay open, and stay known.

06

Departments that run their own machines

Agent status per endpoint distinguishes a device that reports nothing from a device with nothing to report, department by department.

RESULT- Coverage stated as fact, not as assumption.

REPORTED AS

Incidents by store, region, and policy, risk scores, override history, approval logs, and Shadow AI tools awaiting verification on one dashboard.



Call for more details...

+91 88700 07553

www.defensely.ai