



THE PROBLEM

Most organisations cannot say where their data went today.

Data no longer leaves through the network perimeter. It leaves through a browser tab, a chat window, a personal drive, a file picker pasted by someone doing their job. Ask yourself four questions.

- 01 Do you know which applications your staff uploaded company data to this week?
- 02 How is personal data protected once it leaves an approved system?
- 03 AI is essential today - So how are you proving nothing sensitive gets pasted into it?
- 04 If a breach happened last month, could you produce the record of it?



Watch the video

Scan the code to see a
live Defensely walkthrough.

THE LAW

The DPDP Act now has a schedule, a Board, and a date.

India's Digital Personal Data Protection Act, 2023 was operationalised by the DPDP Rules, notified on 13 November 2025. Penalties are fixed rupee ceilings in the Schedule to the Act, assessed per instance, and they stack.

Statutory Max Ceiling = ₹250 cr

Segment	Records Held	Realistic Penalty Range (Illustrative)
SMB	Under ~5 lakh	₹25 lakh - ₹5cr
Mid-market	~5 lakh - 50 lakh	₹5cr - 40cr
Enterprise / SDF	50 lakh+	₹40cr - 250cr

**Illustrative purpose only*

13 Nov 2025

Board constituted.
Complaints can be filed.

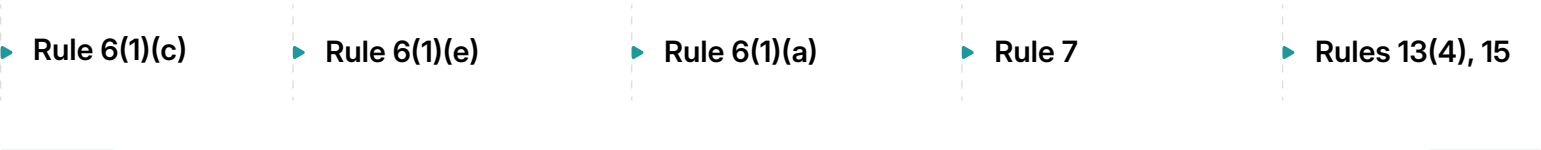
13 Nov 2026

The Board can inquire
and levy penalties.

13 Nov 2027

Full compliance. No
grace period expected.

Defensely provides direct coverage for these rules



Beyond the DPDP Act, DO it for yourself.

- ✓ Protect your proprietary information

✓ Know every movement of your data

✓ Discover the AI tools your staff already use

✓ Control USB, clipboard and cloud in one policy
- ✓ Spot the insider before the damage is done

✓ Stay protected even when devices go offline

✓ Replay any incident exactly as it happened

✓ Prove compliance instead of claiming it

PRODUCT FEATURES

One agent on the endpoint. Four modules in the console.

Logs Summary

Log every data, every channel, every user with forensic evidence.

Who moved data, and the proof

By user

MF Mac Ferrari · 12 activities · PCI

Uncovered

JR Jordyn Rosser · 9 activities · Code

▶ Playing

Uncovered

LN Lara Niles · 2 activities · PII

Covered

1.cpp · pasted into Snapchat web

Credential in clear text

```
31 {
32 cout<<"account "<<acct_no;
33 cout<<"key "<<api_secret;
34 }
35 int main() {
36     Record r1;
37     r1.ShowData();
38 }
```

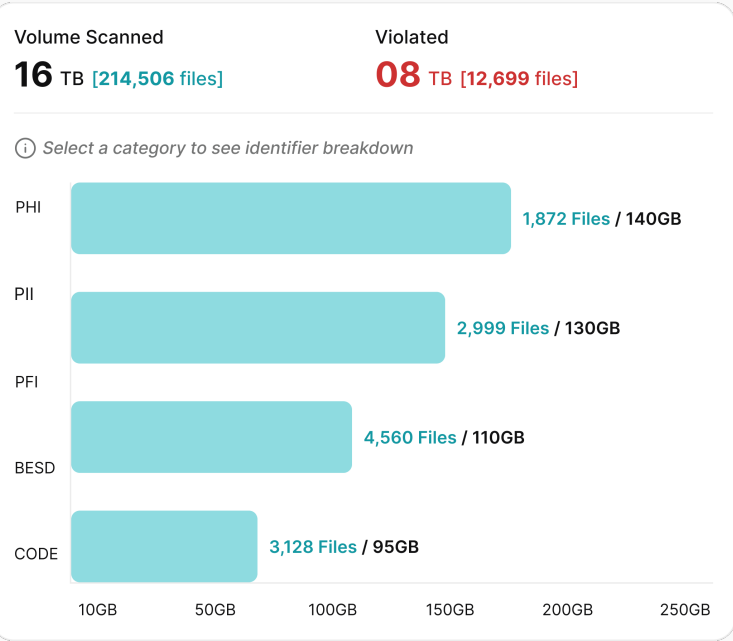
02:45 / 15:00

⏮ ⏪ ⏩ ⏭

Recording attached

Data Classification

Sorts data in motion into PHI, PII, PFI, BESD and code, and flags what broke policy.



High Risk Users Analytics

Ranks people by violation volume, so repeat offenders surface before they become the breach.

🔔 Total Violations

674

⚠️ Uncovered

17

Mac Ferrari

macferrari.m@company.com

261

Ann Rosser

macferrari.m@company.com

42

Tiana Septimus

macferrari.m@company.com

31

Craig Dias

macferrari.m@company.com

57

Maya Singh

maya.s@company.com

57

Liam Chen

liam.c@company.com

57

Data Loss Prevention for Endpoints

One policy across domains, browsers, apps, devices and file paths. Anything else stays untouched.

Where this policy applies

Target

Healthcare · PHI and PII · block on unsanctioned

🌐 Domains

9

4 restricted 5 allowed

📄 Browsers

3

Chrome Safari Firefox

📱 Applications

3

Telegram Drive Outlook

📱 Devices

3

USB Bluetooth Printer

📁 File paths

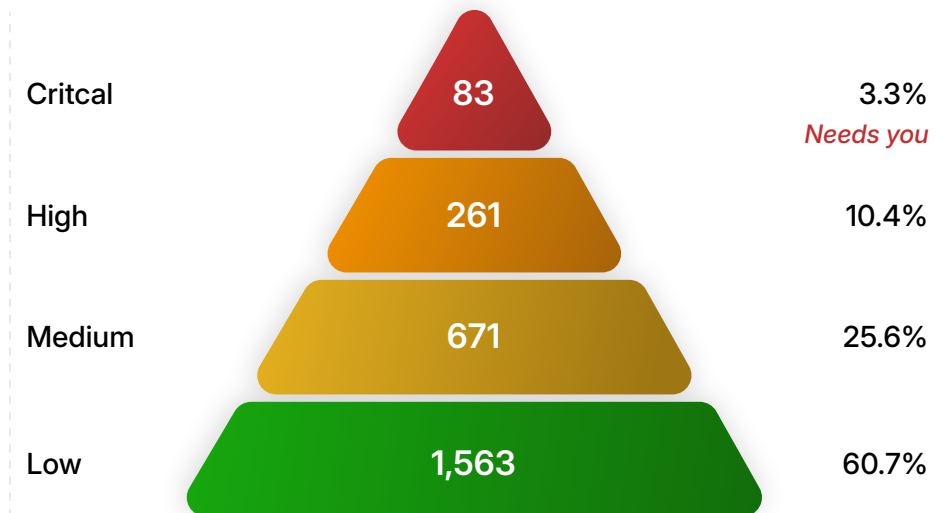
2

/Desktop /Downloads

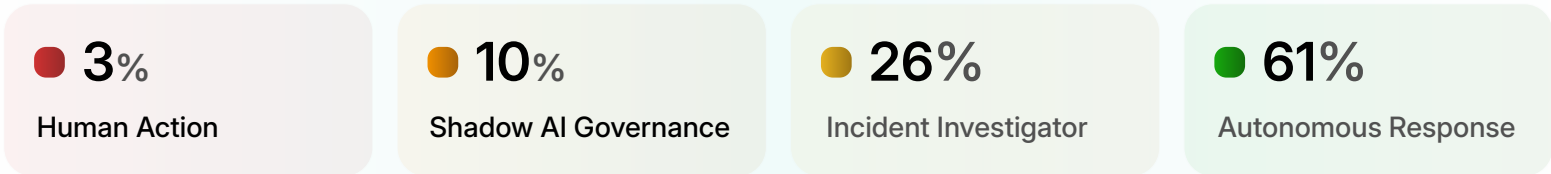
One policy, five surfaces. Anything not listed stays untouched.

AI AGENTS

Four agents that investigate, not just block.



Files handled by agent

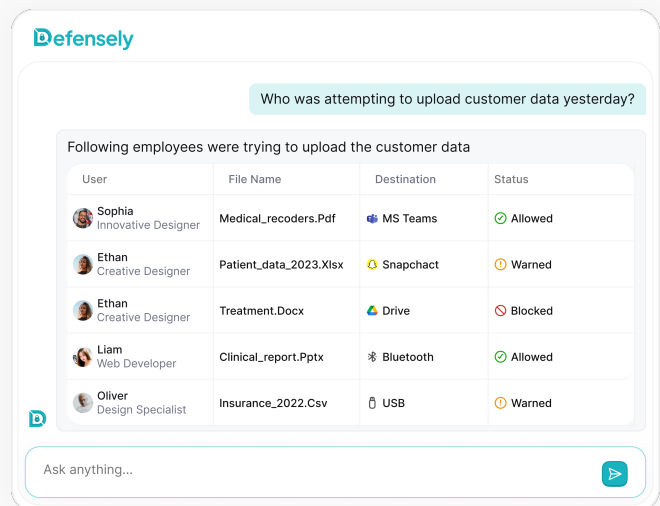


“ Stop Data Leaks Before They Even Begin ”

AI Chatbot

A conversational layer over the DLP console. Ask why a file was blocked, which policy triggered, or what a data type means in plain language.

Suggested prompts and investigation history help users quickly explore and revisit past queries.



Your data doesn't leave. Four agents make sure of it.

OS Support:

Windows | MacOS | Linux

Reach Out:

www.defensely.ai | +91 88700 07553 | sales@innovly.io

Admin / User Access:

Web Console | Android | iOS