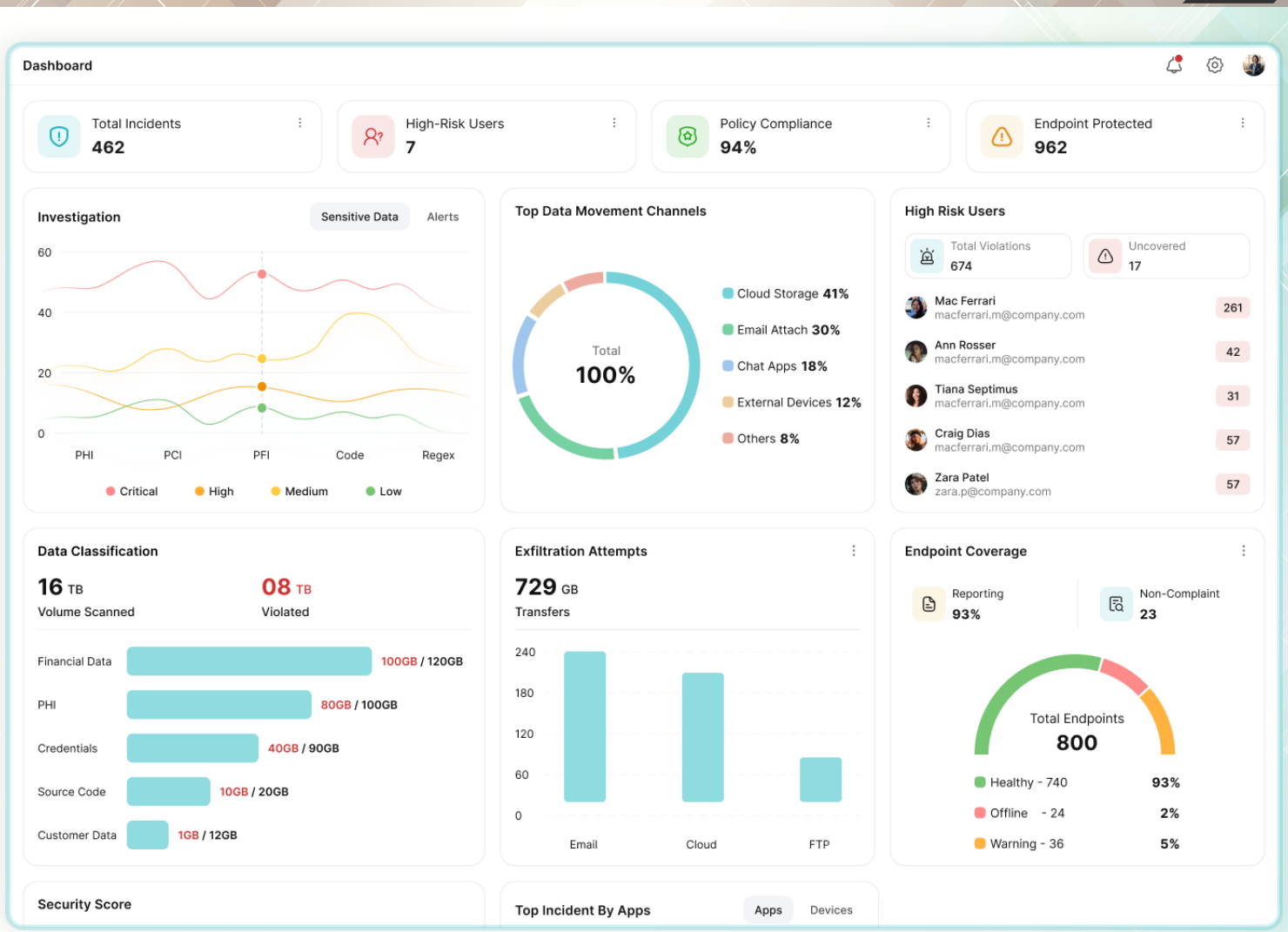
Defensely

“COMPLETE VISIBILITY. TOTAL CONTROL. ZERO DATA LOSS.”

AI powered DLP Solution that protects sensitive data across every channel, every device, every user.

Scan | Detect | Protect | Response

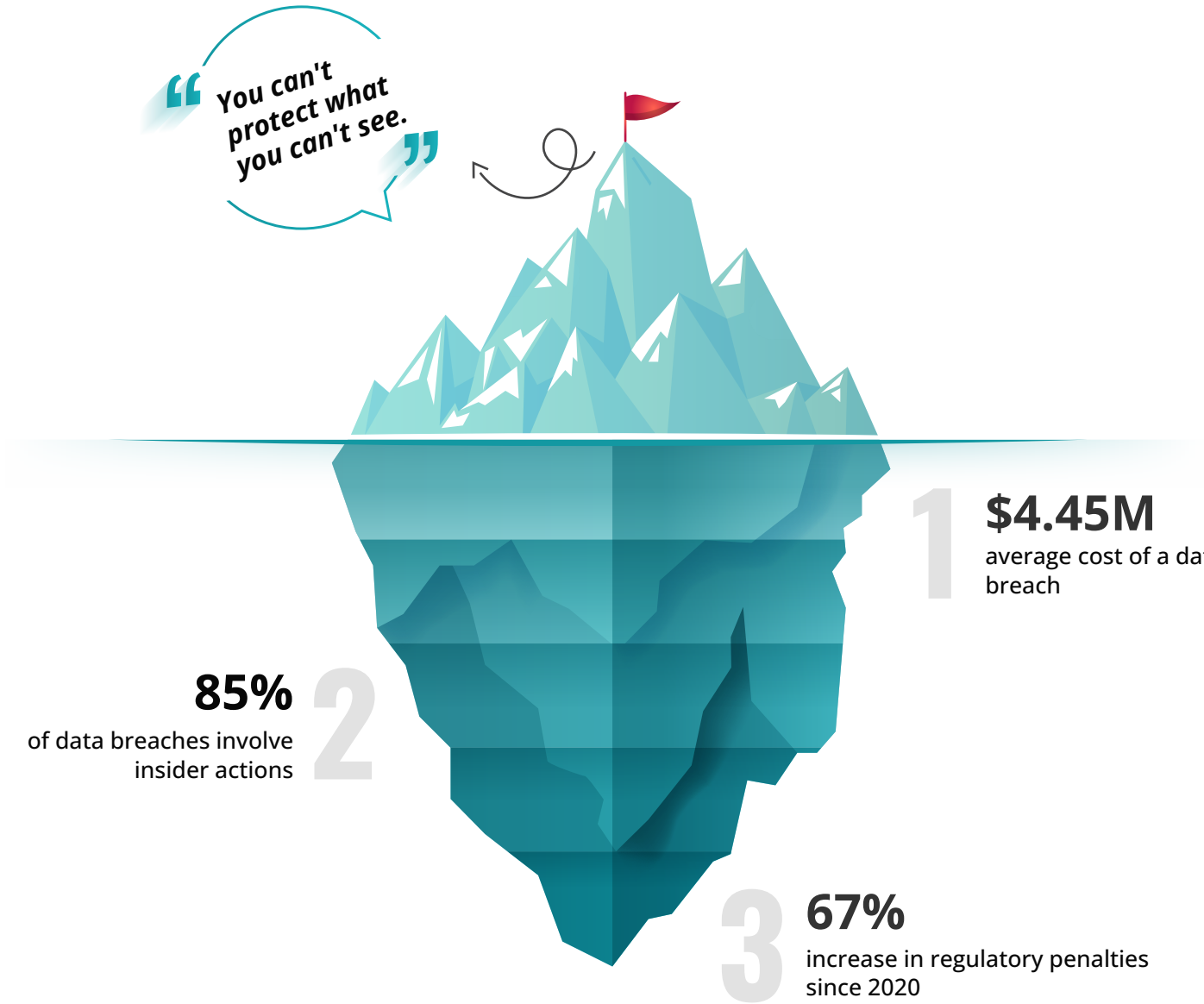


The Challenge

“Your Data Is Leaving. Do You Know Where?”

Every day, sensitive data moves through your organization across emails, cloud apps, USB drives, AI platforms, and messaging apps. A single misconfigured policy, one careless upload to ChatGPT, or an insider threat can expose customer PII, financial records, source code, and compliance-critical information.

Traditional DLP solutions are reactive, complex, and create alert fatigue. Security teams need real-time visibility, intelligent detection, and actionable insights not more noise.



1 **$4.45M**
average cost of a data breach

2 **85%**
of data breaches involve insider actions

3 **67%**
increase in regulatory penalties since 2020

The Shadow AI Problem

Every AI prompt is a potential data leak. Employees paste confidential data into ChatGPT, Claude, DeepSeek, and other AI tools daily often without realizing the security implications. Traditional DLP wasn't built for this.

The Solution

Introducing Defensely

Defensely is a AI powered DLP Solution platform that gives security teams complete control over sensitive data movement without disrupting business operations.

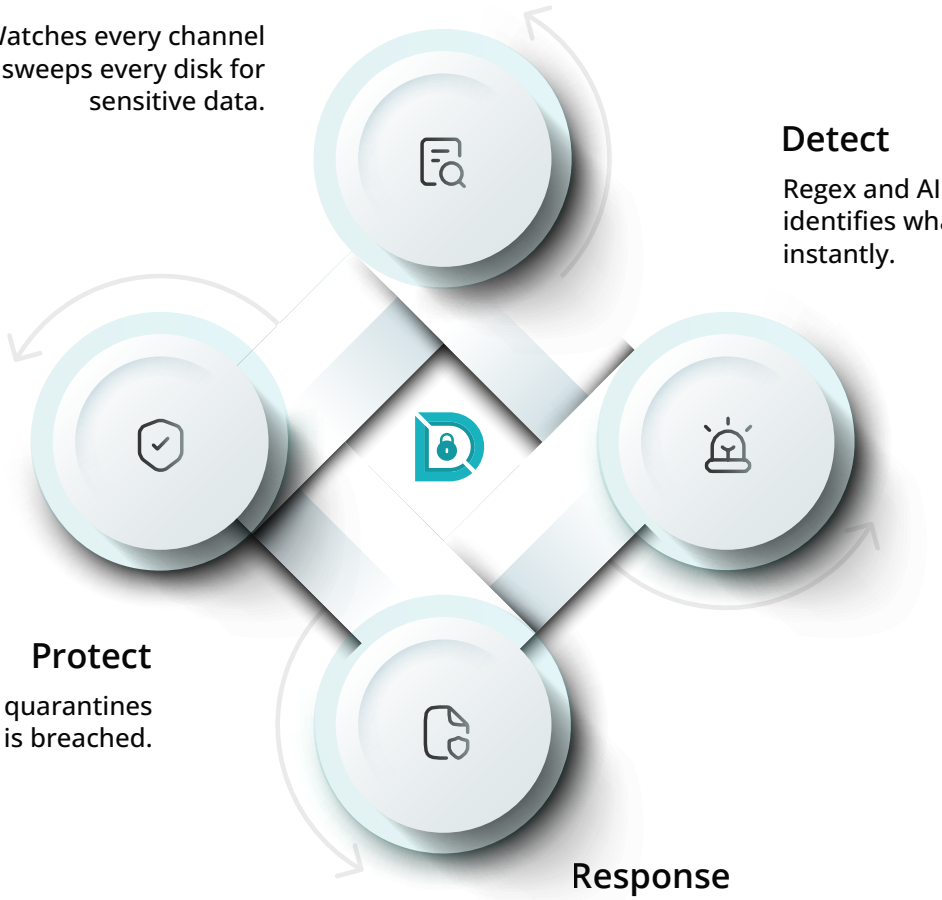
Purpose-built for enterprise environments, Defensely combines intelligent content inspection, behavioral analytics, and granular policy enforcement into a single, unified console

Scan

Watches every channel and sweeps every disk for sensitive data.

Detect

Regex and AI classification identifies what's sensitive, instantly.



Protect

Blocks, warns or quarantines the moment policy is breached.

Response

Video evidence, file lineage and approval workflows close the loop.

500+
Agents

95%
Policy Compliance

50+
Channels Monitored

24/7
Real-time Protection

FEATURES OF DEFENSELY

Core Platform

- Endpoint DLP via installed agent (.exe)
- Policy-driven content control per user
- Dual detection mode regex-based and AI-based
- Cloud DLP for cloud DLP for all cloud storage platform

Policy Management

- Create unlimited custom policies
- Configure permissible and blocked applications
- Configure allowed and blocked content types
- Assign policies to individual users or groups

Self Override & Approval

- Monthly self-override quota, admin configured
- Approval request raised once the quota is exhausted
- Admin approval workflow for upload requests
- Employee overrides a block with written business justification

File Trace History

- Traces a file across multiple hops from its origin
- Identifies the people involved at each hop
- Per-file trace view of the complete movement chain
- Records every destination application or service reached

Data Discovery & Classification

- On-demand scan launch from the dashboard
- Live progress, background run and stop mid-run
- Estimated duration shown before launch
- Scan status shown in the page header while running
- Live progress, background run and stop mid-run
- Last scan and next scan visibility

Cloud DLP & Gen AI DLP

- Cloud coverage, connected services, scan and enforcement behaviour in development.
- ChatGPT and Claude prevent data leakage

Logs

- Shadow file copies are stored in the client environment
- Forensic video evidence
- Full upload activity log across all endpoints

AI Agents

01

Incident Investigator

Generates a detailed per-user incident report

02

Behaviour Intelligence

Tracks and analyses user behaviour over time

03

Shadow AI Goverance

Auto-blocks unrecognised AI tools on detection

04

Autonomous Response

Identifies new applications, websites accessed by users

KEY CAPABILITIES OF DEFENSELY

Visibility & Detection

Unified Dashboard

Single-pane view of your entire data security posture. Monitor total incidents, high-risk users, policy compliance, and agent health at a glance.

Multi-Channel Coverage

Monitor data movement across all critical channels:

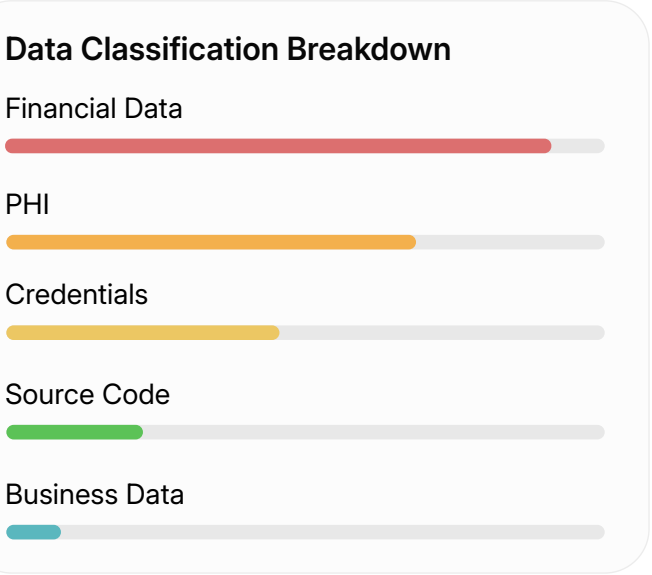
- ✓ Email
- ✓ Browser
- ✓ AI Platforms
- ✓ Chat Apps
- ✓ USB/Devices
- ✓ Cloud Storage

Intelligent Classification

Automatically identify and classify sensitive data types:

PHI | PFI | PCI | PII | Source Code | Credentials | Custom Regex

Data Classification Breakdown



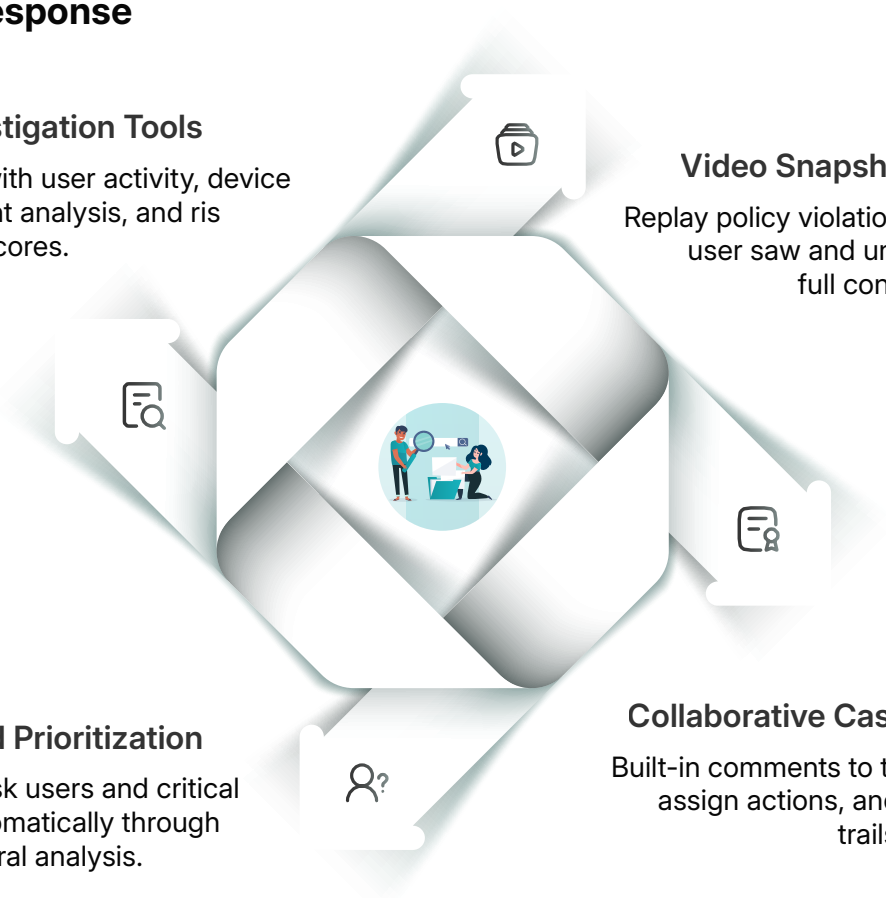
Investigation & Response

Deep Investigation Tools

Drill into incidents with user activity, device details, content analysis, and ris scores.

Video Snapshot Playback

Replay policy violations to see what the user saw and understand the full context.



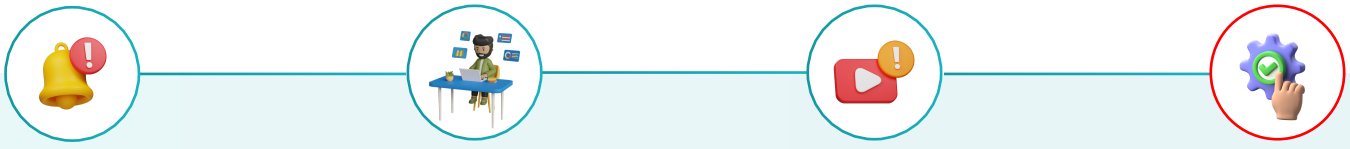
Risk-Based Prioritization

Surface high-risk users and critical violations automatically through behavioral analysis.

Collaborative Case Management

Built-in comments to track investigations, assign actions, and maintain audit trails.

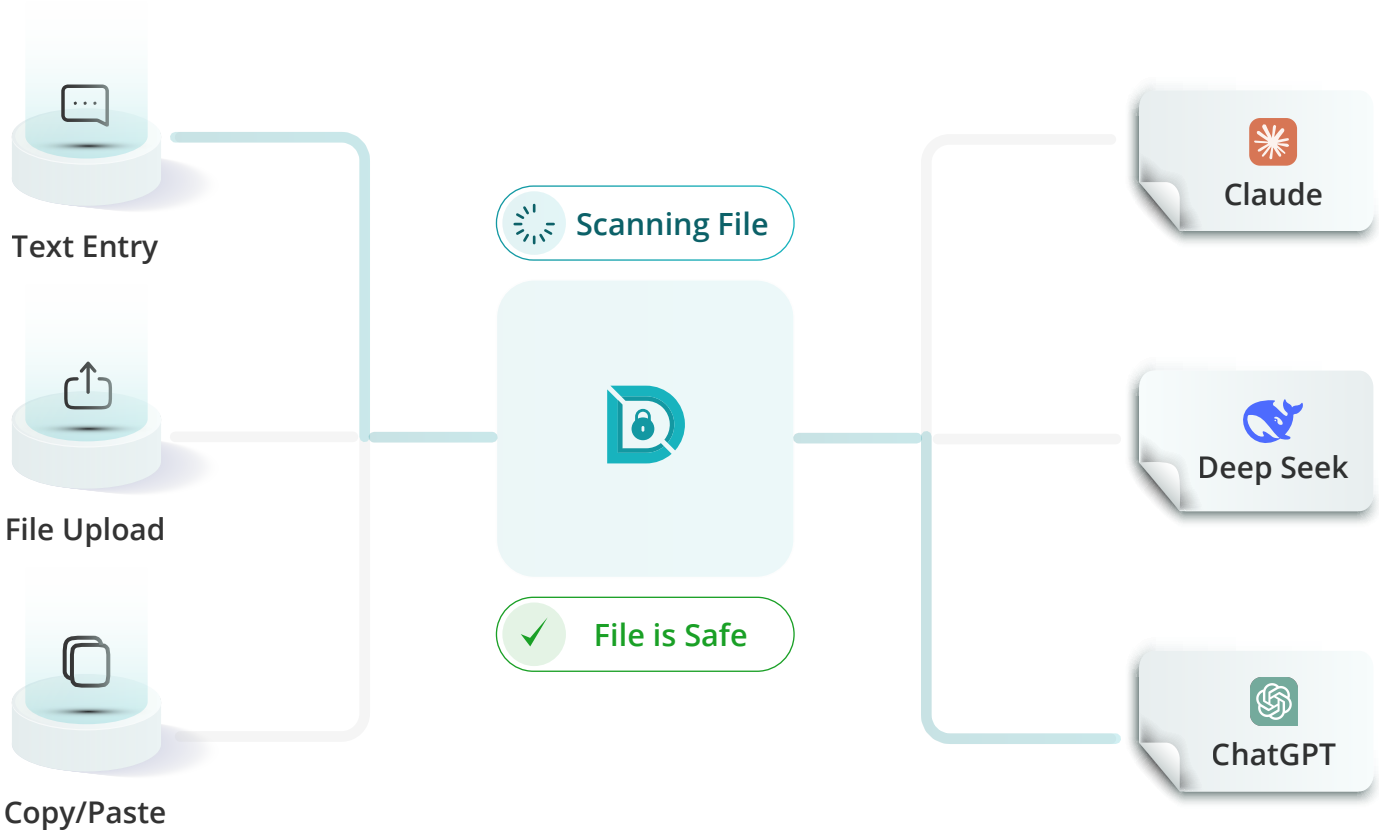
Investigation Workflow



AI Data Security

Prevent Data Leakage to Shadow AI

Every AI prompt is a potential data leak. Protect intellectual property from entering unauthorized AI applications.



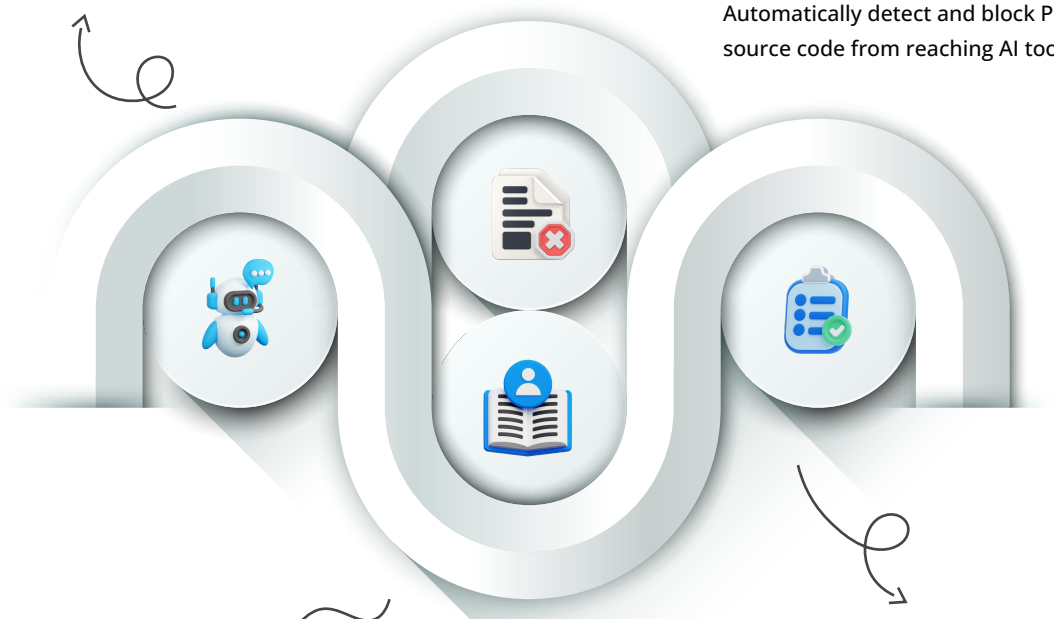
AI Data Protection Features

Monitor AI Prompts

Track text entry, file uploads, and copy/paste actions to AI platforms in real-time.

Block Sensitive Data

Automatically detect and block PHI, PCI, PII, and source code from reaching AI tools.



User Education

Show contextual warnings to coach safer behavior when sensitive data is detected.

Audit & Compliance

Full audit trail of all AI interactions for compliance reporting.

File Lineage & Data Discovery

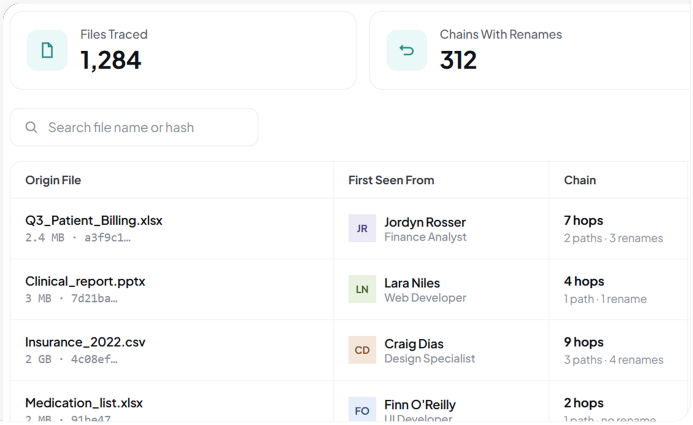
Follow sensitive data after it moves and find where it already sits at rest on every endpoint.

Lineage & Discovery Intelligence

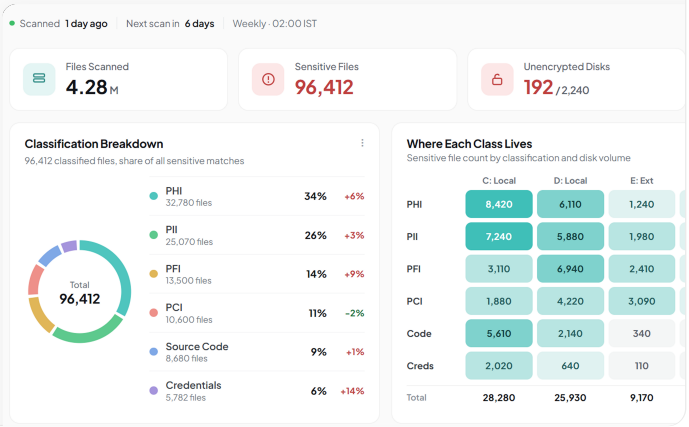
- ✓ Full movement chain for every sensitive file, hop by hop
- ✓ Renames detected in transit and linked back to the origin file
- ✓ Agent-driven discovery of sensitive data at rest across local and mapped drives
- ✓ Unencrypted disks, hotspot folders, and top data holders surfaced automatically

Visual Screens

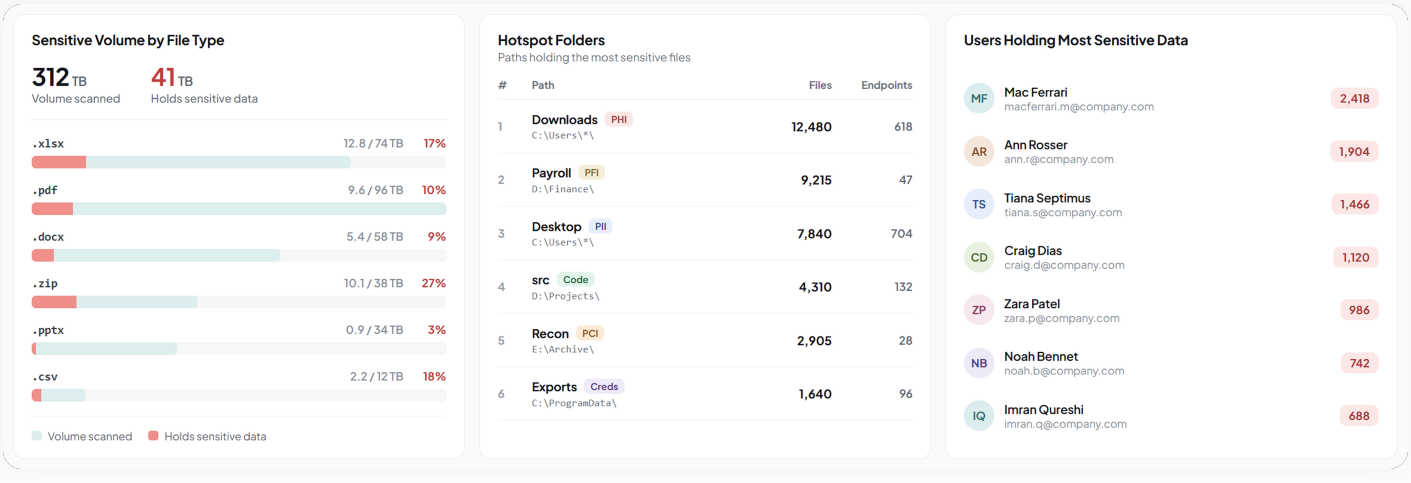
File Trace History



Data Discovery Dashboard



Discovery Insights



Key Capabilities

- ✓ End-to-end file trace with hop, path and rename counts
- ✓ Classification at rest across PHI, PII, PFI, PCI, source code and credentials
- ✓ Worst-verdict scoring and blocked exfiltration points per chain

Real-Time Visibility & Analytics

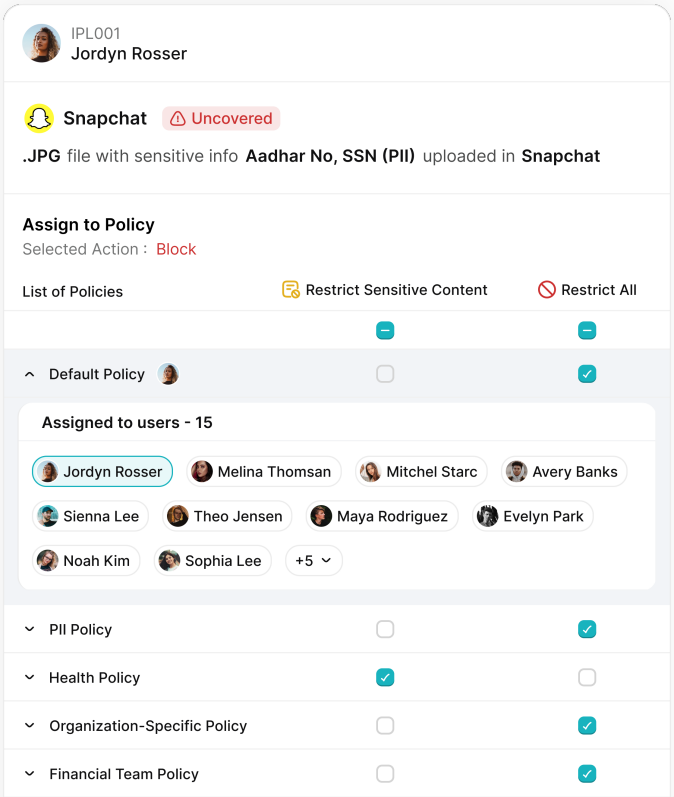
Watch data movement as it happens, with a video snapshot of every violation for instant context.

Real-Time Analytics & Monitoring

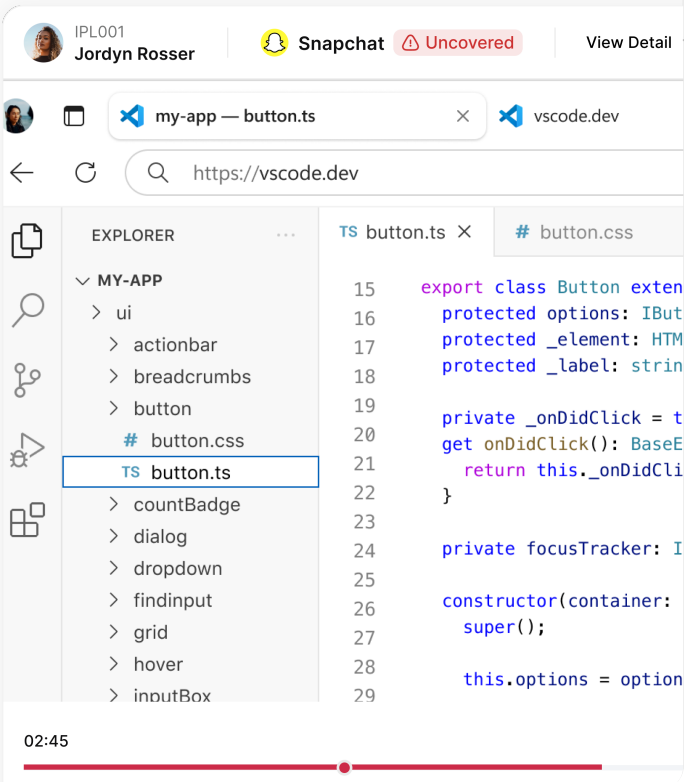
- ✓ Live endpoint activity tracking
- ✓ Comprehensive log summary of data movement
- ✓ Visibility across files, applications, devices, and users
- ✓ Video snapshot of policy violations for instant context

Visual Screens

Log Summary



Violation Snapshot Video



Key Capabilities

- ✓ Real-time activity monitoring
- ✓ Real-time activity monitoring
- ✓ Video snapshot of DLP violations

Investigation & Incident Response

Drill into any incident for the full user, device and file story behind it then act.

Faster Investigation. Smarter Response.

Defensely enables security teams to:

- ✓ Investigate incidents with full activity context
- ✓ Review user behavior timelines
- ✓ Analyze file movement, application usage, and device access
- ✓ Take immediate corrective action

Visual Screens

Investigation List

Medical_recoders.Pdf 2 MB	IPL001 Jordyn Rosser	Allowed
Dummyfile.Pdf 601.11 KB	IPL002 Ann Rosser	Blocked
Treatment.Docx 10 MB	IPL003 Chance Rosser	Blocked
Clinical_report.Pptx 3 MB	IPL004 Tiana Septimus	Blocked
Insurance_2022.Csv 2 MB	IPL005 Craig Dias	Blocked
Contact_list.Pdf 2 MB	IPL006 Abram Herwitz	Blocked
Medical_research.Docx 2 MB	IPL007 Martin Geidt	Blocked
Medication_list.Xlsx 2 MB	IPL010 Zara Vang	Blocked
Lab_results.Pdf 2 MB	IPL008 Kaiya Rhiel Madsen	Uncovered
Patient_feedback.Docx 2 MB	IPL009 Makenna Press	Warned
Telehealth_schedule.Xlsx 2 MB	IPL011 Eliot Packer	Blocked
Staff_training.Pdf 2 MB	IPL012 Sofia Tandon	Warned
Surgery_checklist.Docx 2 MB	IPL013 Rafael Choi	Uncovered
Healthcare_policy.Pdf	IPL014	

Investigation Details View

dummyfile.pdf
Under Review

View File

User Information

Name	Anna Rosser
Employee ID	#IPL002
Department	UI Team
Machine	Hp Pavilon 14inch intel 7

File Information

File Type	.TXT
File Size	603.11 KB
Source	file path / rosser / : desktop/ file1 /
Destination	MS Teams
Created On	12/02/26 04:52pm
Last Modified	14/02/26 11:43am

Key Capabilities

- ✓ Centralized incident investigation
- ✓ User and agent behavior correlation
- ✓ Evidence-backed decision making

Policy Engine

Granular Control. Maximum Flexibility.

Create, customize, and deploy policies that match your organization's unique requirements—without writing code.

Content Restriction

PHI (Protected Health Info), PFI (Financial Information), PCI (Payment Card Data), PII (Personal Identifiers), Source Code, Custom Regex Patterns.

PHI	PFI	PII	Code	File Type
Name	Bank account	Aadhaar	.js	.PDF
Date Of Birth	Credit card	Driver's License	.java	.SVG
Policy Number	CVV	Passport	.py	.PPTX
Prescription	IFSC codes	Home address	.php	.XLSX
Hospital Name	Debit card	Phone number	.html	.MP3

Target Applications

Browsers	Instant Message	Cloud	Device
MS Edge	Telegram	Adobe Cloud	Bluetooth
Safari	WhatsApp	Dropbox	Card Reader
Firefox	Teams	One Drive	Wifi
Opera	Messenger	We Transfer	Floppy Disk
Google Chrome	Hangout	Google Drive	Printer

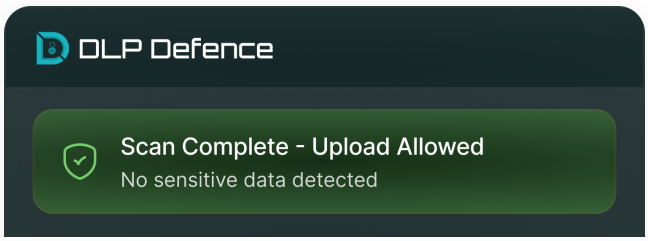
Response Actions

Action

- **Block** - Prevent entirely
- **Warn** - Alert before action
- **Notify** - Real-time alerts
- **Video Record** - Capture screen
- **Quarantine** - Isolate file

Custom Workflows

Safe Upload | Warned Upload



Self-Service Override with Admin Approval

Allow users to request policy overrides with business justification. Admins can approve or reject from the centralized Approvals dashboard.

1. User triggers policy
2. Shows justification form
3. Admin reviews request
4. Approve or Reject

Policy Management

Automatically detect and control sensitive data based on defined policies.

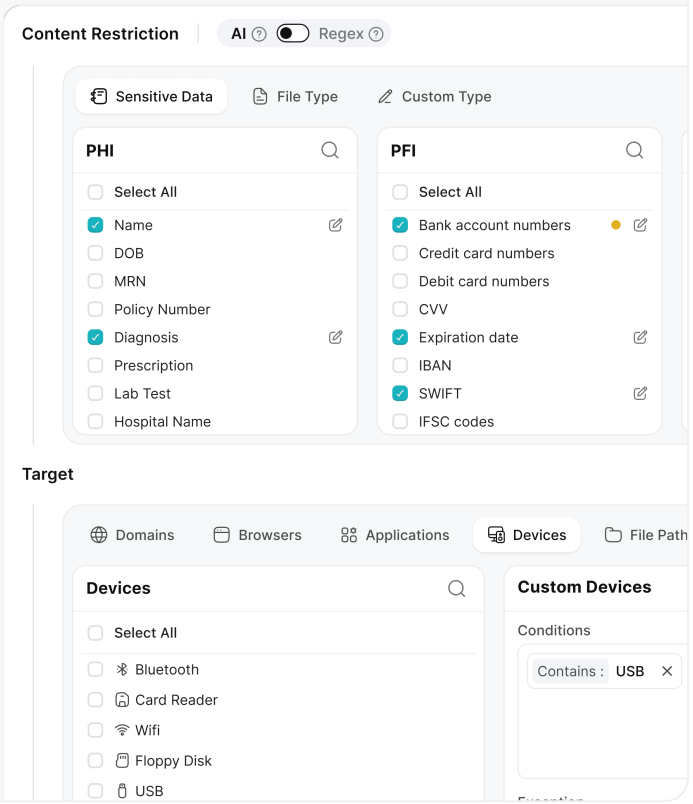
Advanced Controls

Create powerful DLP policies based on:

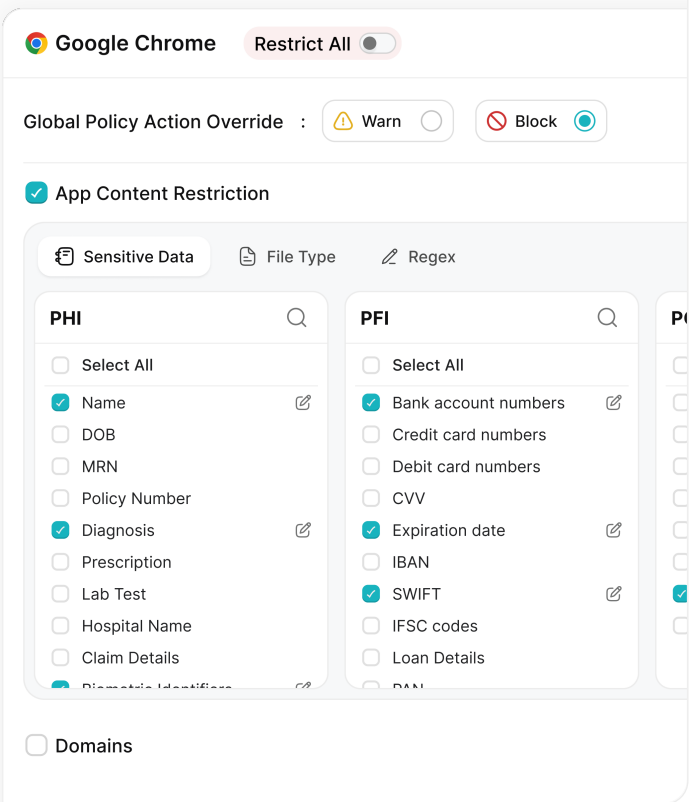
- ✓ Regex-based data detection
- ✓ Target-based policy application
- ✓ Context-aware enforcement
- ✓ Applications & channels

Visual Screens

Policy List



Policy Details View



Key Capabilities

- ✓ Sensitive data & application-based policies
- ✓ File type and device-level restrictions
- ✓ Regex-based detection

Override

Defensely allows secure file upload overrides with business justification, enabling users to continue work with administrators retain fully policy control and visibility.

Admin Override Control

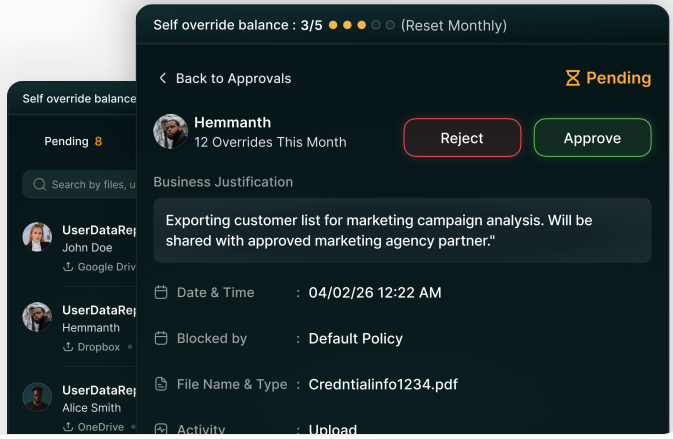
- ✓ Configure override count limits and renewal timelines
- ✓ Detect abnormal or excessive override behavior
- ✓ Approve upload requests from a single dashboard.

User Self Override Experience

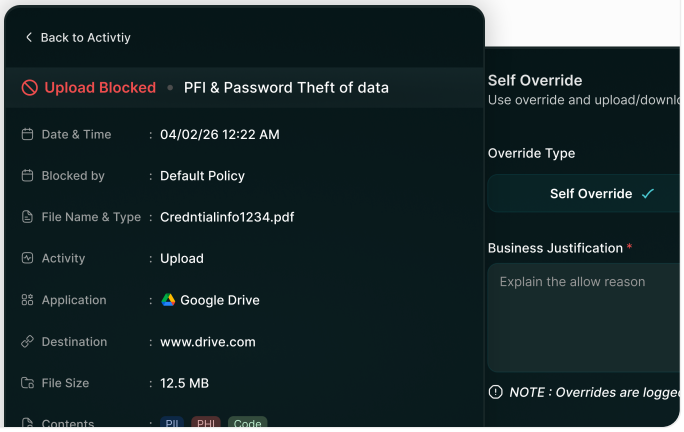
- ✓ Request temporary access with business justification
- ✓ Receive alerts when limits are reached
- ✓ Submit approval requests after override limits are reached.

Visual Screens

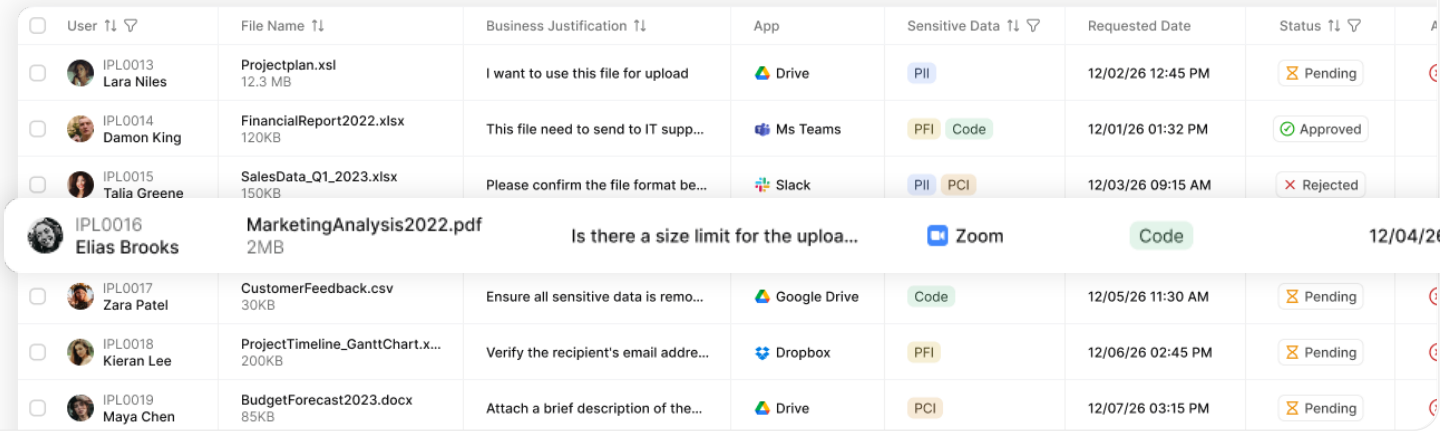
Tray App - Admin



Tray App - User



Override Approvals



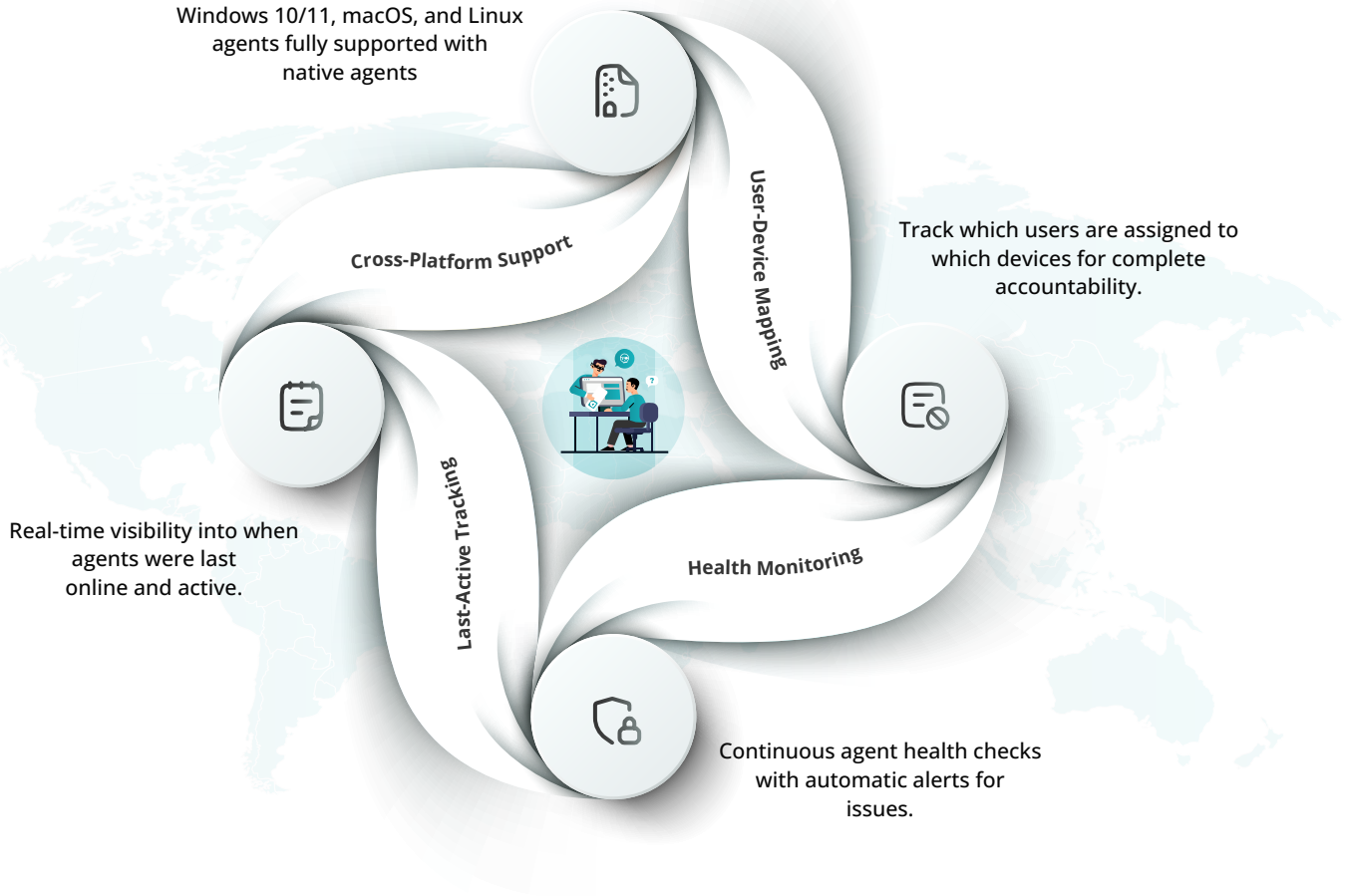
Key Capabilities

- ✓ Override Limits & Thresholds
- ✓ Role-based access control (RBAC)
- ✓ User groups for targeted enforcement

Agent Management

Complete Agent Visibility

Know the status of every deployed agent in your organization from rollout to daily health monitoring.



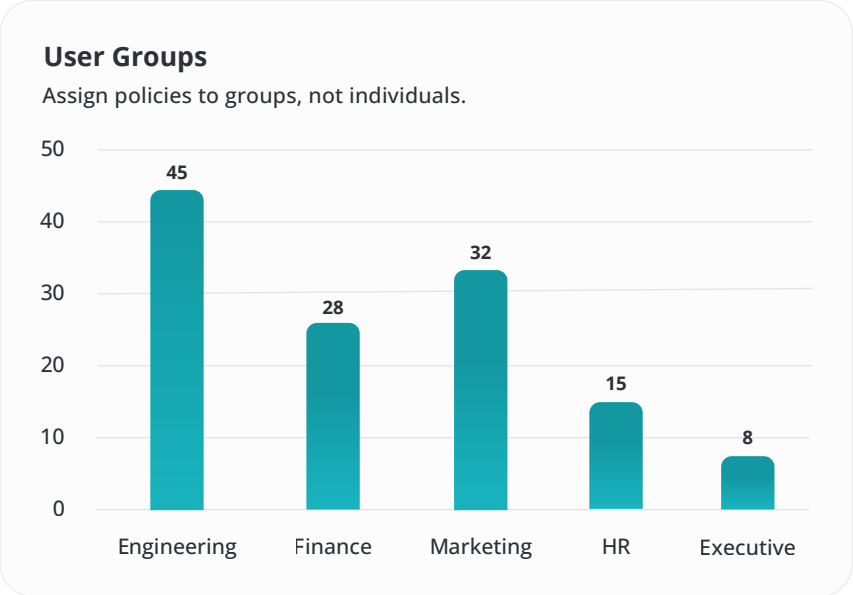
ACCESS CONTROL

Right Access. Right People.

Align DLP policies with your organizational structure through flexible role-based access control.

User Management

- ✓ Centralized user directory with 100+ users
- ✓ Status tracking (Active/Inactive)
- ✓ Activity log history per user
- ✓ Designation-based grouping
- ✓ Bulk user import and export



Role-Based Access Control

1 **Admin** – *Full system access* , 2 **Network Admin** – *Network configuration* , 3 **User** – *Basic access*

4 **Department Lead** – *Team management* , 5 **Group Lead** – *Group policies*

Agent & User Management

Manage agents, policies, and actions from one place.

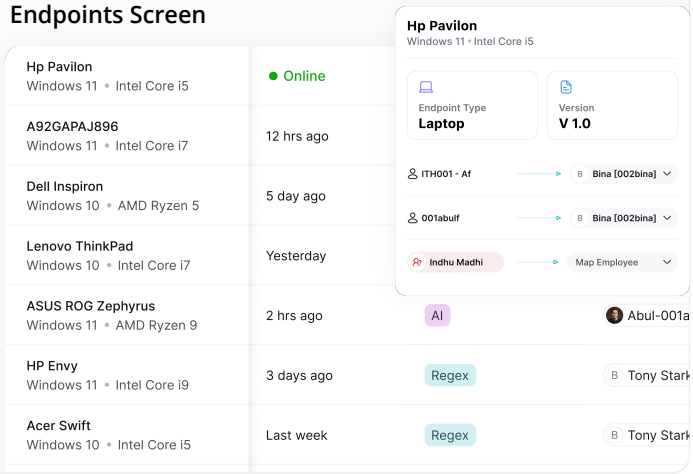
Centralized Agent Control

Agent Management

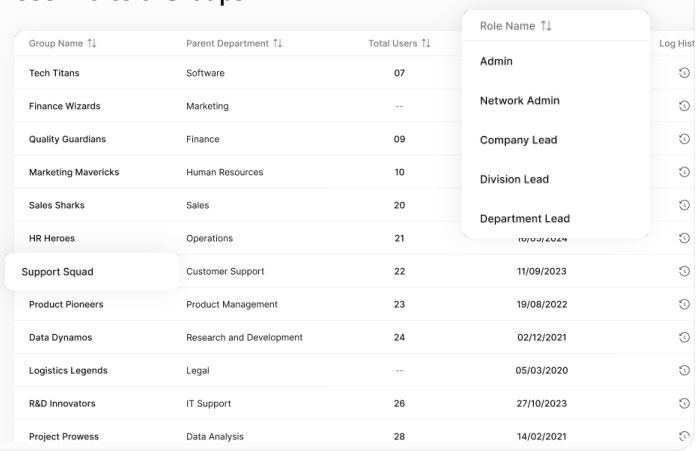
- ✓ View all connected endpoints
- ✓ Monitor agent health and status
- ✓ Configure agent-specific settings
- ✓ Secure agent download & deployment

Visual Screens

Endpoints Screen



User Roles & Groups



Agent Download

Installing the Agent

Command Path copy / paste

Specifies the system path where command executions for the DLP Agent are initiated.

msiexec.exe /i "https://qadlpinstaller.blob.core.... Copy

DLP Desktop Agent (.exe version)

Use this version to install the DLP agent on Windows computers for data protection and activity tracking.

Download for Windows Or Download for Mac

Key Capabilities

- ✓ Agent visibility & health status
- ✓ Role-based access control (RBAC)
- ✓ User groups for targeted enforcement

Platform Features

Everything You Need. One Platform.

Video Snapshot

Industry-first forensic capability—replay the exact moment of policy violations

Unified Dashboard

Single-pane view of your entire data security posture with real-time incident monitoring.



User Risk Scoring

Behavioral analytics to identify high-risk users with detailed risk breakdowns

Investigation Tools

Deep drill-down into incidents with timeline, comments, and collaborative case management

Approval Workflows

Self-service override requests with admin approval for legitimate business needs.

Policy Engine

No-code policy builder with 20+ templates for PHI, PCI, PII, and custom rules

Deployment Options

On-Premises

Captured and maintained entirely on the client.

Where It runs

Deployed inside your own environment, on client-managed infrastructure

Where data is stored

Data, audit, logs, files and video evidence all stored client-side.

Suits

Teams that need every artifact to stay within their own estate.

Cloud

Maintained by **Defensely**, with evidence kept on client.

Where It runs

Deployed inside your own environment, on client-managed infrastructure

Where data is stored

Data, audit, logs, files and video evidence all stored client-side.

Suits

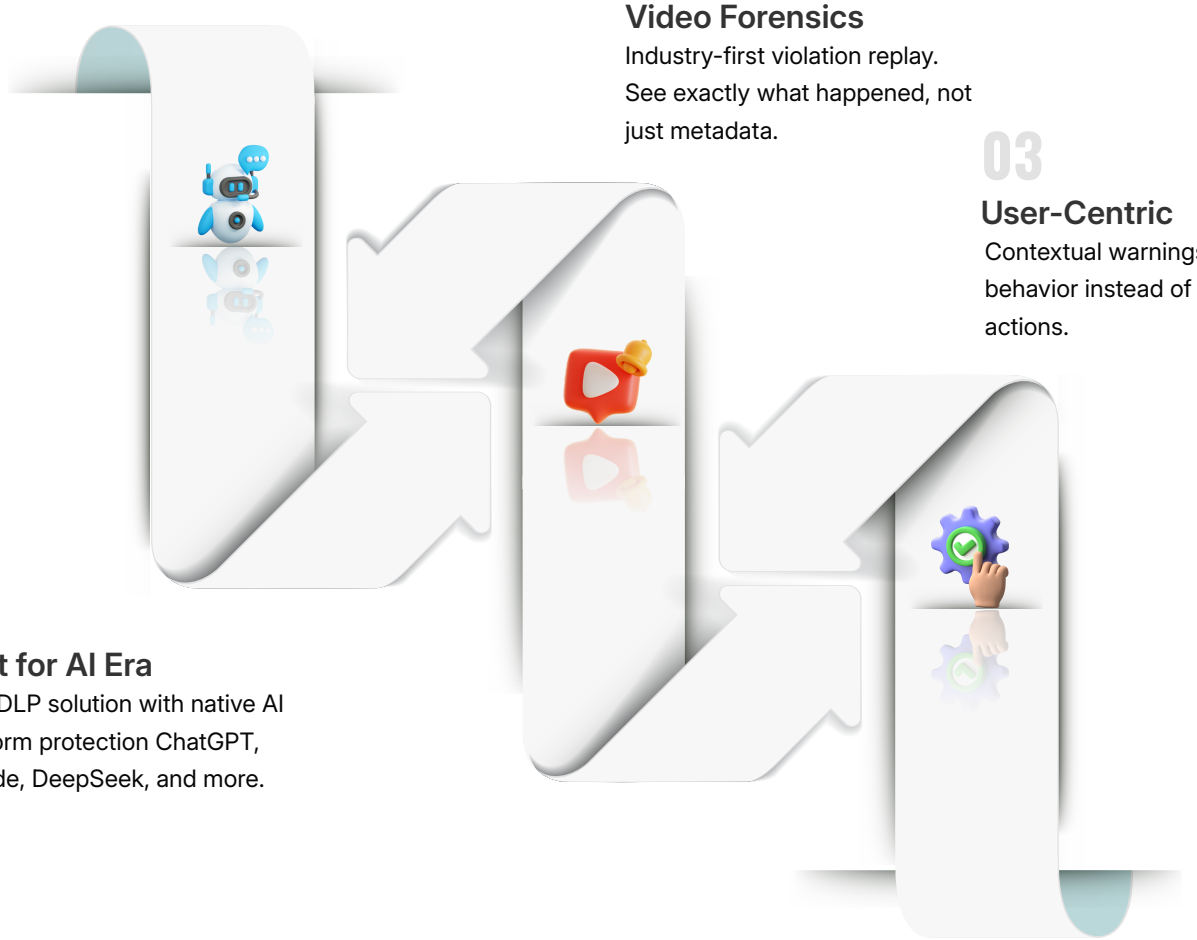
Teams that want a faster rollout without hosting the platform.

The Advantage

Why Defensely?

Capability	Legacy DLP	Defensely
Deployment Time	Weeks/Months	Hours/Days
Policy Config	Complex scripting	Visual, no-code
Investigation	Log files only	Full video playback
Channel Coverage	Limited	50+ channels
Alert Quality	High false positives	Context-aware
Collaboration	Siloed	Built-in case mgmt

Key Differentiators



01

Built for AI Era

First DLP solution with native AI platform protection ChatGPT, Claude, DeepSeek, and more.

02

Video Forensics

Industry-first violation replay. See exactly what happened, not just metadata.

03

User-Centric

Contextual warnings that coach behavior instead of just blocking actions.



USE CASES

Real-World Security Challenges



Healthcare

How do you monitor and prevent sensitive data loss in your organization?

The Challenge:

Organizations struggle to track where sensitive data moves—across cloud apps, emails, USB drives, and messaging platforms. Without visibility, preventing data breaches becomes nearly impossible.

Defensely Solution:

Defensely provides unified monitoring across 50+ channels with intelligent content classification. Our dashboard gives you real-time visibility into data movement, policy compliance, and high-risk activities—all from a single console.

> *"Defensely gave us visibility into sensitive data movement, helping prevent leaks and strengthen compliance."*
>
> — Head of IT Security, Healthcare Network

Cybersecurity and R&D

How do you protect intellectual property from being shared on AI platforms (ChatGPT, Claude, etc.)?

The Challenge:

Employees regularly paste source code, customer data, and proprietary information into AI tools for assistance—often unaware of the data security implications. Traditional DLP wasn't designed for this threat vector.

Defensely Solution:

Defensely monitors all AI platform interactions including ChatGPT, Claude, DeepSeek, and more. We detect and block sensitive data in text prompts, file uploads, and copy/paste actions—with options to warn users or require admin approval.

> *"AI boosts productivity but brings risks—Defensely protects intellectual property without limiting innovation."*
>
> — Director of Security, Technology Company

Solving Complex Security Challenges



IT and BPO

How do you prevent accidental data leakage by your employees?

The Challenge:

Most data breaches aren't malicious—they're accidents. Employees email the wrong attachment, upload files to personal cloud storage, or share sensitive docs in Slack without realizing the risk.

Defensely Solution:

Defensely uses intelligent content inspection to detect sensitive data in real-time. When risky behavior is detected, users see contextual warnings explaining why the action was blocked coaching safer behavior over time.

> *"Accidental data sharing used to be a constant risk. With Defensely, our teams now understand when data should not leave the organization."*
>
> — IT Operations Manager, BPO Company



Finance and Banking

How do you secure remote and hybrid workforce?

The Challenge:

With employees working from home, coffee shops, and co-working spaces, data can leave your organization from anywhere. Traditional perimeter security doesn't protect data on agent devices.

Defensely Solution:

Defensely lightweight agent protects data regardless of network or location. Policies are enforced locally, even when devices are offline, ensuring consistent protection for your distributed workforce.

> *"Our biggest concern was protecting financial data beyond the office network. Defensely gave us consistent protection across all employee devices."*
>
> — CISO, Financial Services Firm



Sales and Marketing

How do you detect and mitigate insider threats?

The Challenge:

Insider threats—whether malicious or negligent—account for 85% of data breaches. Detecting unusual behavior patterns and preventing data exfiltration before it happens is critical but challenging.

Defensely Solution:

Defensely combines behavioral analytics with risk scoring to identify high-risk users. Our investigation tools provide full user timelines, video snapshots, and anomaly detection to spot threats early and gather evidence for response.

> *"We can now detect unusual behavior before it turns into a serious data breach. Defensely gives us the visibility we needed."*
>
> — Security Lead, Global Marketing Firm



“Stop Data Leaks Before They Even Begin”

Every file. Every channel. Every user.

Connect with us

Phone
+91 88700 04553

Website
www.defensely.ai

Email
sales@defensely.ai

Defensely