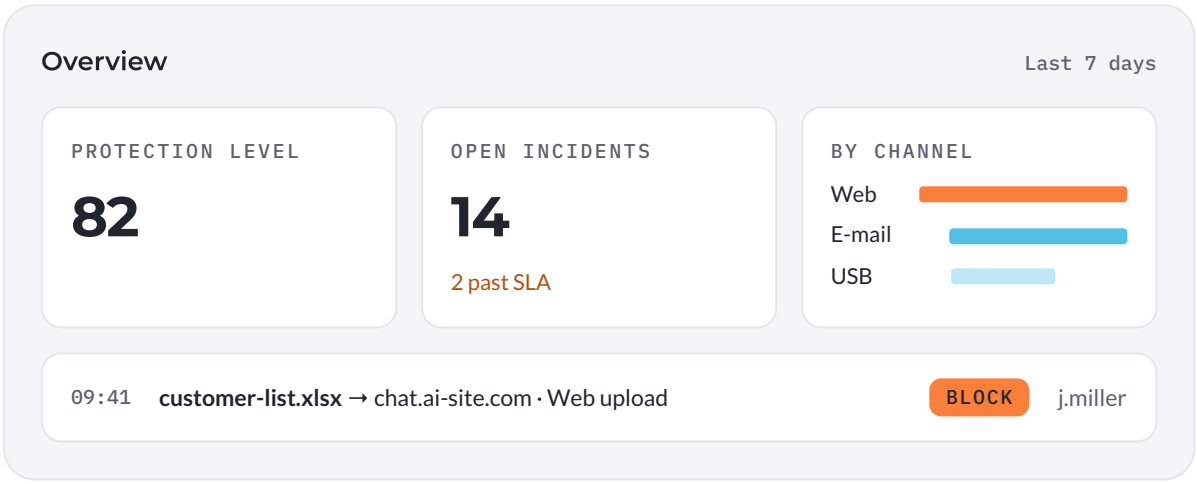
INTERNAL DATA LEAK PREVENTION

Sensitive data is caught before it leaves the organization.

Before a customer list goes to a USB drive, a payroll file to a personal e-mail, or source code to an AI website, GuardStance steps in. Incidents and evidence stay in your infrastructure.



your protection level in one number

SLA breaches visible at once

the riskiest channel

here the moment it happens

See first

Start with the Log action; tighten the rule as you see the risk.

Then stop

Warn, ask for a reason, or block: the risk decides the action.

Data stays with you

Incidents and evidence are stored encrypted on an appliance inside the organization.

Audit-ready

GDPR executive summaries come with a ready template.

day one: publish the first rule, see the first incident

CHANNELS AND RULES

Eight channels. One ordered rule table.

Every path data can take out of the organization is managed from the same window. Pick the scope, say what you are looking for, set the action.

USB
Content and access rules; read-only mode

Clipboard
Copied content is scanned before it is allowed

Printing
Documents are scanned before they print

Web upload
HTTP and HTTPS; cloud storage, webmail

E-mail
Outlook add-in and SMTP, one rule

Network DLP
Web, SMTP, remote sessions; GenAI and messaging

Network share
Content, monitoring and write-limit modes

Cloud sync
OneDrive, Google Drive, Dropbox, Box

Rule 3 · Customer data / AI sharing — Priority 3 of 12

SCOPE	Sales group · Web upload, Network DLP · destination: GenAI services
CONTENT	Personal data (national ID, phone) ≥ 5 matches · dictionary: customer terms
ACTION	ASK AND JUSTIFY · notify user · mask captured values

who, where to

what we look for

what to do; user informed, data masked

SEVEN ACTIONS

Allow | Log | Shadow copy | Ask and justify | Block | Silent block | Read-only

DETECTION AND INCIDENTS

Every alert tells you why.

A policy is written like a sentence and goes to all agents at once in a signed package. An incident arrives with why it matched, who did it, and the evidence.

- Built-in GDPR policy pack
- National ID, IBAN, phone and card validators
- Dictionary and regex library
- OCR on images
- True file type and sensitivity label

built-in GDPR pack

reads like a sentence

channel action

POLICY

GDPR · Personal data is detected in Web upload going to unapproved GenAI services → **Block** and **Shadow copy**

Incident #4821 · customer-list.xlsx BLOCKED

why it matched: validator, confidence

behavior signals

evidence with SHA-256

captured values masked and highlighted

WHY IT MATCHED

Detector	National ID validator · 37 valid hits
Confidence	High
Dictionary	customer terms · 12 hits

BEHAVIOR SIGNALS

First upload to this destination · outside working hours · 3 files in 10 min

EVIDENCE

User	j.miller · Sales · WS-0412
Destination	chat.ai-site.com
SHA-256	`9f2a…c41e`

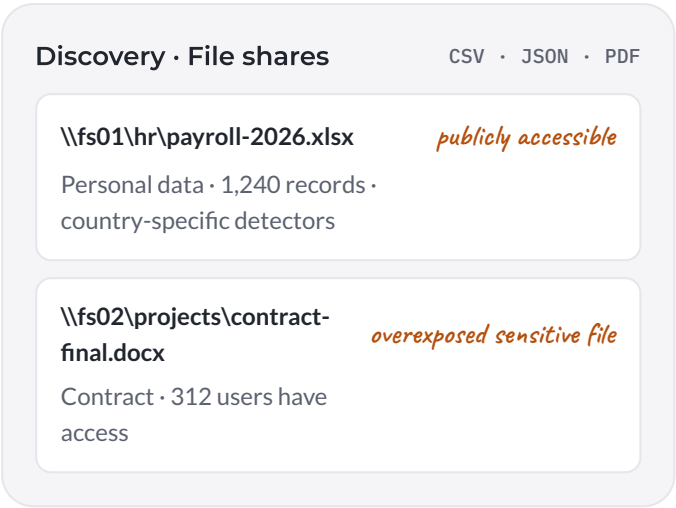
CAPTURED VALUES

`AB 12 ** ** C` `+44 7*** *** 407` `DE89 **** **** 3000`

DISCOVERY AND REPORTS

Know where data sits. Prove it in the audit.

SMB and NFS shares and endpoint disks are scanned. Reports: GDPR executive summary, data inventory, period comparison; can be scheduled by e-mail.



TRUST AND GOVERNANCE

No fixed default password

The temporary password is shown only on the appliance screen.

Encrypted disk and evidence

The system disk is encrypted at installation.

Signed packages

Policy, agent and appliance updates are signed.

Immutable records

The audit log cannot be deleted; it is chain-protected.

Roles and reviewer

A review role that cannot see the content.

Directory and 2FA

LDAP / Active Directory, Entra ID, two-step verification.

Windows: single signed MSI, GPO deployment **Linux:** .deb and .rpm Staged agent updates, automatic rollback

Signed appliance updates, also offline

clear limits

In Teams, Slack and Discord, file uploads are scanned, not message text. WhatsApp content arrives encrypted and cannot be scanned; the decision follows the rule's action. Telegram, Git command line and FTP/SFTP are blocked at the network level only.

You don't have to take our word for it. Test it with your own data.

Choose the data you want to protect and your real user flows. Let's see together what the PoC catches, then you decide.

Plan a PoC sales@guardstance.com