Sensitive data is classified where it is produced, and stopped there.

Verifyi recognises personal data, financial data and source code in place: on Windows, macOS and Linux endpoints, inside TLS traffic and in cloud stores. Policy is enforced on the endpoint; only the verdict reaches the console. Everything runs in your own data centre, installed from two ISOs.

3 endpoint platforms · Windows, Linux, macOS	2 appliances · management and Network DLP proxy, separate ISOs	< 2 % agent CPU target · under 150 MB memory, 10 ms policy decision	0 raw content to the cloud · verdicts and masked samples only

Modules

Three licensed modules and the extensions that feed them

DLP Endpoint agents, policy engine, incident management, cases, review queue, reports and SIEM/webhook integration.	**Proxy** The Network DLP appliance: TLS inspection, destination policies, web categories, flow log, block-with-override.	**Discovery** Data-at-rest discovery: endpoints, databases, SharePoint/OneDrive, S3/GCS/Azure; scan profiles and labelling.
CASB connectors GitHub repository scanning is available today; M365, Google Workspace and Salesforce connectors are on the roadmap.	**Browser extension** User-input DLP in forms and generative-AI prompts on Chromium browsers; deployed by enterprise policy.	**Office add-in** Apply sensitivity labels in Word, Excel and PowerPoint; labels are written into OOXML and read by the agent.

Detection technologies

The right method for each data type

Patterns with validation TCKN, IBAN, card numbers (Luhn), passport, phone, e-mail; context dictionary, proximity and distinct-value thresholds.	**Exact data matching (EDM)** Hashed columns of your customer or HR table; real-record matching with no raw data stored.	**Document fingerprinting** Partial copies and reformatted versions of contracts, designs and source code.	**Trainable classifiers** Models running inside the agent for your organisation's own document types; training data never leaves the endpoint.
OCR Text inside screenshots, scanned documents and photos; embedded, no extra installation.	**File type and encrypted files** True-type detection regardless of extension; encrypted Office/PDF and archives are never treated as clean and are reported as their own event type.	**Sensitivity labels** MIP labels are read from OOXML and become rule conditions; the Office add-in applies them.	**Decoding and structure** Base64/URL encoding is decoded; bare numeric IDs inside JSON are not treated as TCKN; proximity rules.

Coverage

Channel and platform matrix

Channel	Windows	Linux	macOS	Actions
Clipboard	Yes	Yes	Yes	monitor · warn · block
File movement and at-rest quarantine	Yes	Yes	Yes	monitor · shadow copy · quarantine
USB storage	Yes	Yes	Yes	monitor · block
Mobile devices (MTP/PTP)	Detect	Detect	Detect	alert
Printing	Yes	Yes	—	monitor · block

Channel	Windows	Linux	macOS	Actions
HTTP/HTTPS egress	Yes	Yes	Yes	monitor · block · override with justification
File integrity (FIM)	Yes	Yes	Yes	monitor
Browser input	Extension	Extension	Extension	warn · block

Use cases

The seven scenarios we start with most often

Data leaking into generative AI
Source code, customer data and contracts pasted into ChatGPT, Copilot and similar tools. The proxy with AI platform packs, the browser extension on typed text; override with justification available.

Leavers and insider risk
Bulk copies to USB, uploads to personal cloud storage, attachments to personal e-mail. User-risk view, shadow copy and the Incident Analyzer timeline as evidence.

KVKK: personal data leaving the organisation
TCKN, health and contact data leaving by e-mail, web form, file sharing and clipboard; inventory with a discovery profile, control with egress blocking.

PCI-DSS: card data spilling out of scope
Card numbers on call-centre and accounting endpoints; quarantine for files at rest, blocking on the network, evidence in reports.

Source code and intellectual property
Code copied out of the repository, pushes to GitHub under the wrong account, secret leaks. Document fingerprinting, GitHub CASB scanning and the browser extension together.

Multi-user servers (RDS, Citrix)
Dozens of sessions on one machine; the incident must name the right user. Per-session identity, proven in agent and Kerberos modes.

Systems where no agent can run
Production servers, guest networks, contractor devices. Agentless proxy mode: the same policy and the same console with PAC/WPAD and Kerberos.

Rollout

From monitoring to blocking in four weeks

1 · Discovery and inventory
Endpoint and repository scans with the chosen framework profile (KVKK, PCI, HIPAA); a what-is-where report.

2 · Monitor mode
Policies only raise incidents in the pilot group; the false-positive rate is measured in the review queue with justifications.

3 · Warn and justify
Users are warned in their own language; override with justification is on; behaviour and justifications are reported.

4 · Block and expand
Measured rules move to blocking; rollout proceeds group by group; SIEM and notification rules are connected.

Licensing

An offline, per-module, time-limited licence

Three modules
dlp (endpoint agents and console), proxy (Network DLP appliance), discovery (discovery and classification). Buy what you need; adding a module means uploading a new file.

Signed file
The licence body is signed as canonical JSON; the product carries only the public key. Changing the expiry or the modules breaks the signature.

Expiry and agent cap
Every licence has an expiry date and an optional maximum agent count. An expired licence makes the console warn, not silently downgrade; renewal is uploading a file.

Trial
The 30-day trial licence uses the same mechanism; when the PoC ends, the production licence is uploaded to the same installation.

See it in your own environment
With the installation guide, port matrix and AV/EDR exclusion list you can stand up a PoC in an afternoon. The 30-day trial licence works offline. · info@verifyi.tech · https://verifyi.tech/en/