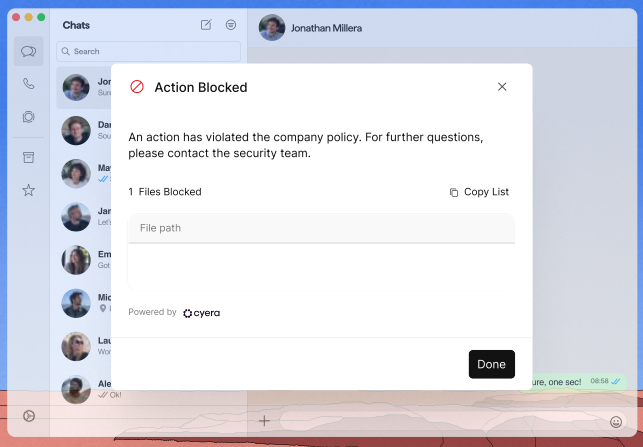
cyera

Cyera Endpoint for Data Loss Prevention

Stop risky data actions on the device.
Keep legitimate work moving.



Christine works in Business Operations and is preparing an acquisition review for Monday's leadership meeting. The report holds unannounced deal terms and an internal negotiation ceiling. It's Friday afternoon, and she copies the report into the Dropbox folder on her laptop so she can keep working from home. The folder syncs to her personal account.

Your gateway sees sync traffic to a domain you already approve. Your browser extension sees nothing, because Christine never opened a browser. Your DLP policy was probably written for email attachments and USB drives.

The same report is fine on the USB drive she carries to the meeting, because moving acquisition files is part of her job, and off-limits in her personal Dropbox. Block every file transfer and Christine finds a workaround by Monday. Allow them all and the acquisition report leaves with her personal account. Imprecision costs the business twice: work stops when it shouldn't, and sensitive data moves when it shouldn't.

Cyera Endpoint is built for that decision. It brings data loss prevention to the device. A sensor on the laptop classifies the content involved in an action, applies the policy you wrote in Omni DLP before the action completes, and reports the result to the same console as your alerts from email, cloud, and browser.

Challenges for security teams

Every control sees a fragment

A proxy sees the traffic routed through it, and a browser extension sees the browser. Neither sees what a user does inside a native AI app, and USB drives, printers, and file shares sit outside both.

A pattern match leaves the real decision open

Static patterns and labels can find a match without knowing whether the data matters, who is acting on it, or where it is going. At fleet scale that becomes alert noise and policy tuning, until teams narrow enforcement to keep the program manageable.

Alerts arrive without a story

An endpoint alert that says a file moved doesn't say what was in it, who owns it, or whether the destination was approved. Analysts rebuild context that should have arrived with the alert.

Another sensor adds tension between security and desktop teams

Each extra endpoint agent adds an install, an update cycle, a policy model, and another thing for desktop teams to support and troubleshoot. When that cost rises, rollout slows and coverage narrows.

The solution

One sensor covers people and agents

Cyera Endpoint is one sensor with one console for policy, events, and agent health, versions, and upgrades. This brief covers what people do on the device, and its companion, Cyera Endpoint for Agent Security, covers what local AI agents do there. The same endpoint sensor supports both, so adding agent security to a DLP deployment doesn't mean another install.

Discover: see how people and agents use and move data

Cyera Endpoint observes supported actions on the device and ties each one to the person, device, application, and data involved. That covers prompts and attachments in native AI apps, clipboard actions, and transfers to USB drives, printers, file shares, and AirDrop, which proxies and browser extensions can't see. Cyera Browser Shield covers the browser. Teams see where guardrails are needed before they turn on enforcement.

Classify: know what the data is before deciding how to protect it

Cyera Endpoint evaluates the content involved in an action, not its filename, extension, or existing label. Renaming a file doesn't get it past inspection.

- On-device AI classification works alongside deterministic detection, so unstructured content such as source code and product plans is evaluated by meaning as well as by pattern.
- A separate inspection process reads inside documents, spreadsheets, archives, and PDFs, so content is evaluated even when it is compressed or embedded.

Protect: stop risky actions before they complete

Cyera Endpoint applies policy before the action completes. With Real-Time Validation, the endpoint sensor holds the action while the Cyera Platform adds data sensitivity, identity, destination, and business context. Cy Triage supports the blocking decision, and the endpoint sensor enforces it locally, allowing, warning, or blocking.

- Each policy sets its own mode: alert only, notify, block with override, or block. Available modes vary by channel.
- The employee sees an on-device notification when an action is blocked or needs a justification, and approved work can proceed through the override.
- Policy and classification already on the device keep enforcing offline, and events queue until the device reconnects.

Triage: know what happened and why

Endpoint events land in Omni DLP alongside alerts from your other connected channels. Cy Triage analyzes, prioritizes, and explains them.

- Cy Triage orders the queue so analysts start with the events that carry meaningful risk.
- Each explanation comes with the data and context behind the alert, so the analyst doesn't rebuild it from logs.

Use cases

Native AI data protection. An employee pastes customer data or attaches source code in a desktop AI app such as Claude or ChatGPT, including from a personal account. Cyera Endpoint inspects prompts and attachments and applies policy before they are sent.

Insider and IP exfiltration. An employee who is about to leave, or a developer with access to source code, secrets, and product designs, copies them to a USB drive, a file share, or an unapproved app. Cyera Endpoint classifies the content and monitors, notifies, or blocks the transfer, with a justification path for approved work.

Regulated data on everyday channels. PII, PHI, PCI, and financial records move through clipboard copy and paste, USB drives, file shares, AirDrop, printers, and desktop messaging apps such as Discord and WhatsApp, which email and cloud controls never see. Cyera Endpoint applies the policy defined in Omni DLP across these channels.

Graduate from visibility to enforcement. Customers roll out gradually. They begin in alert-only mode on a few channels, add user notifications and justified overrides, and expand to more channels and blocking as each policy proves out.

How to deploy

Cyera Endpoint is a lightweight sensor for macOS and Windows that is easy to deploy and manage, with minimal impact on endpoint performance. It works at the application and operating-system level, so it doesn't proxy traffic, decrypt TLS, or inspect packets. Your IT team installs it with the device-management tools you already run, such as Intune, Jamf, or SCCM, using a signed MSI package on Windows and a signed package on macOS. Once installed, each device registers with the Cyera Platform and pulls the DLP policies you define in Omni DLP. From the platform, you then monitor sensor health, connectivity, and versions.

Why Cyera

Enforcement by your data and identity context

Cyera Endpoint applies what the platform already knows about your data and identities. With Real-Time Validation, each decision rests on what the content is, who is acting, and where it is going.

On-device AI that understands meaning

Cyera Endpoint classifies content locally by meaning as well as by pattern, so it recognizes sensitive information that matches no known format, and classification keeps working when the device is offline.

One sensor and one control plane

One endpoint sensor covers employee data movement and local AI agent workflows. Its policies, events, and investigations live in the same platform as your connected browser, email, cloud, and SaaS channels, so the device doesn't become another silo.

Cyera Endpoint is available as an add-on to Cyera Omni DLP or Cyera Agent Guardian.

Explore how Cyera Endpoint fits your data loss prevention program. Book a demo →