DATA & AI SECURITY PLATFORM

Find your data. Understand what it is. Protect it the moment it moves.

A customer list can be uploaded to an AI tool. Source code can be copied to a personal account. A contract can be shared through the browser, a critical file moved to a USB drive. Sensitive data no longer moves only through e-mail or the file server.

GuardStance is a Data & AI Security platform that helps organizations discover sensitive data, classify it, and apply the right security policy the moment it moves. Endpoint, e-mail, web, cloud and AI usage are handled with the same data-security approach, running on a single agent.

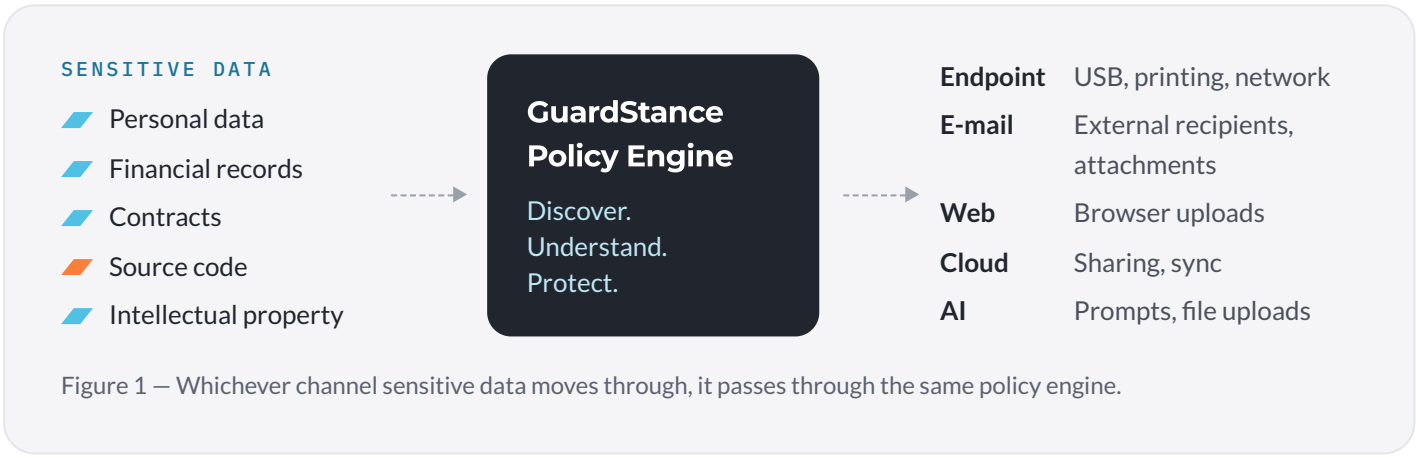


Figure 1 — Whichever channel sensitive data moves through, it passes through the same policy engine.

DATA DISCOVERY
Find the data

CLASSIFICATION
Determine its meaning

DLP
Control its movement

AI DATA SECURITY
Govern AI usage

INVESTIGATION
Examine the context

The real problem in data security is no longer a single channel.

You may be controlling USB usage.

But do you know what your employees are sending to AI tools?

You may be labeling a document “Confidential”.

But when the file leaves, does that label actually turn into a security policy?

GuardStance closes the gap between discovering data and protecting it.

02 — ARCHITECTURE & CAPABILITIES

From where the data lives to the security decision.

01 DISCOVER

Find sensitive data.

The first problem with data you cannot protect is usually not knowing where it is. GuardStance discovers sensitive data across connected environments and makes it visible.

02 UNDERSTAND

Understand what the data is.

Determine what the data means to the organization based on content, location and existing policies.

- Personal data
- Financial
- Contracts
- Source code
- IP

03 PROTECT

Make the right decision when data moves.

When a file is copied, uploaded or shared, policy is enforced through a single lightweight agent. The decision follows the risk level:

MONITOR	Visibility
WARN	Notify the user
RECORD	Create evidence
BLOCK	Stop the movement

04 INVESTIGATE

See why the incident happened.

The goal is not more alerts, but clearer decisions. Review every incident in context:

- Which data?
- By whom?
- Where was it going?
- Which policy fired?

CAPABILITY MATRIX

Platform capabilities

Data Discovery & Classification

Discover sensitive data and classify it into categories that are meaningful for your organization.

Single Lightweight Agent

Classification and DLP run on one optimized agent that does not affect end-user performance.

AI Data Security

Bring AI usage within the scope of your existing data-security policies.

Endpoint & Network Protection

Manage data movement across USB, browser upload, printing, network and e-mail channels.

Cloud Data Protection

Include supported cloud and collaboration environments in your data-security scope.

Insider Risk & Investigation

Evaluate file movement and user behavior in incident context, and report on it.

Multi-Tenant, MSSP Ready

Multi-tenant architecture for service providers: customer environments isolated, management centralized.

03 — USE CASES

Modern data risk requires modern protection.

SOURCE	EVALUATION	DESTINATION	EXAMPLE DATA	POLICY DECISION
Employee endpoint SINGLE AGENT Copy · Upload Share · Send	GUARDSTANCE Data type + Destination + Policy = Decision	**Corporate AI** Approved tool	Internal report summary	ALLOW WARN
		Personal AI Unapproved account	Customer list	BLOCK REVIEW
		E-mail External recipient	Draft contract	WARN RECORD
		Personal cloud Unapproved storage	Project files	RECORD REVIEW
		USB drive External device	Source code	BLOCK

Figure 2 — Example policy evaluation. In every flow, data type, destination and policy are evaluated together; your organization's policy determines the decision.

01 AI DATA SECURITY

Turning AI off is easy. Governing its safe use is far more valuable.

The real question is not which AI tool is used, but what data is sent to it. GuardStance makes AI usage visible, identifies sensitive content, and separates approved use from unapproved use.

Shadow AI is not just an application problem. It is a data-security problem.

02 INTELLECTUAL PROPERTY

Your most valuable data is not always personal data.

Source code, CAD files, formulas, strategic plans. GuardStance goes beyond classic data patterns and also protects content that is critical and specific to your organization.

03 INSIDER RISK

Not every data breach starts with bad intent.

An employee who drops a file into a personal cloud to work from home. A user who downloads the project before leaving. Review data movement and security incidents in their context.

04 COMPLIANCE & AUDIT EVIDENCE

Being able to show the control matters as much as applying it.

Provide technical evidence for your regulatory compliance processes with data discovery, classification, policy and incident records.

GDPR HIPAA PCI DSS ISO 27001

04 — DEPLOYMENT & NEXT STEP

Flexible deployment that fits your security architecture.

Not every organization has the same data-security requirements. Some do not want data to leave their own infrastructure; others prefer to consume the operation as a service. GuardStance adapts to your architecture.

A · CORPORATE INFRASTRUCTURE



On-premises

Place the management components in infrastructure the organization controls. For regulatory and full data-sovereignty requirements.

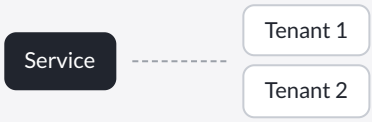
B · THE ORGANIZATION'S CLOUD



Private cloud

Deploy GuardStance in your own cloud environment and let it integrate with your existing architecture.

C · MSSP · CENTRAL MANAGEMENT



Managed

Set up a structure where GuardStance operations are run under a service model.

Service provider / MSSP

Build managed data-security (SECaaS) services for your partners on a dedicated multi-tenant architecture.

01
Choose one type of data you need to protect.

02
Identify your real usage scenarios.

03
Let's look together, in your own environment, at what GuardStance sees and how the policy behaves.

04
Then you decide.

TEST IT WITH YOUR OWN DATA.

We prefer to talk about your real workflow rather than ready-made demo files.

Request a demo | Plan a PoC | Contact us

www.guardstance.com
sales@guardstance.com