

When Autonomous Data Protection Was the Only Answer

How the world's leading EDA firm replaced failed legacy DLP with closed-loop autonomous intelligence — and made IP exfiltration **structurally impossible**.

8 of 10

SCENARIOS MISSED

By prior DLP — silently

10 of 10

SCENARIOS CAUGHT

By ISE, automatically

<100ms

ENFORCEMENT

Detect → decide → act

~50%

CAPEX/OPEX SAVINGS

vs. legacy architecture

A Global IP Portfolio Was Already Exposed.

A global EDA firm with sites across 3 continents was operating a DLP system that had already failed — silently, repeatedly, and without detection. The question was not whether to replace it. It was whether a replacement existed that could operate at the speed of the threat.

The problem was not the vendor. It was the architecture class. Any system built on manual data identification, manual classification, and manual sequential policy deployment inherits the same failure modes — regardless of vendor or AI augmentation.

3RD-GEN DLP WITH DATA CLASSIFICATION	ISE AUTONOMOUS PROTECTION
× Manual / semi-automated classification — covers only a fraction of data; unstructured data invisible	✓ Auto identification + auto classification in real time for ALL data — structured and unstructured — no manual input, no preprocessing
× DLP policies written by humans create false positives; cannot detect false negatives; exploitable by insiders with policy knowledge	✓ Granular policies auto-generated for every actor via Automated Policy Generation & Synthesis — no human-error vector
× Detection is rule-triggered: unknown patterns are invisible by design; novel exfiltration paths succeed	✓ 3-Dimensional correlation across Actor + Operation + Data finds what no rule anticipated; GRC-based segmentation of duty access control
× Encrypted traffic and novel vectors bypass all controls	✓ Inline enforcement across all channels — encryption and application-agnostic
× Incident review is retrospective: data gone before alert fires	✓ Enforcement executes in <100ms — exfiltration structurally prevented, not retrospectively logged

Any organization operating manual policy-based governance in an AI-driven environment is operating without effective data control. This is not a risk assessment. It is a structural certainty.

This was not a requirements exercise. It was an impossibility audit. Four capabilities that every legacy and AI-enhanced DLP architecture structurally cannot provide.

01

Classify unstructured IP data without prior definition

No rule-based system can protect what it has not been told to protect. Classification must derive from the data itself — without human pre-labeling. Untagged EDA schematics, source code, and client-confidential documents are invisible to legacy enforcement.

02

Generate enforcement in real time

Any architecture whose enforcement path includes a human decision step is not a control system. It is a notification system with aspirations. Enforcement at <100ms requires a closed-loop autonomous decision — not a workflow ticket.

03

Evaluate intent, not just content

Exfiltration is a behavioral event, not just a content event. Rules cannot see behavioral context. 3-Dimensional Correlation across Actor + Operation + Data detects what no rule anticipated — including novel channels, unusual volumes, and anomalous timing.

04

Scale governance with actor count, not headcount

Enterprise AI agent populations will grow 10x by 2027. Each new agent is an actor that policy-based systems cannot govern. The gap compounds exponentially. ISE governance scales with the environment — with zero marginal analyst cost per new actor.

The Non-Replicability Principle

Closed-loop autonomous protection cannot be replicated by adding AI to a policy-based architecture. The limitation is structural, not technological. Shared state interdependence — the property that makes autonomous decisions possible — is incompatible with modular, sequential architectures by design. This cannot be bridged with an upgrade.

The moment between detection and enforcement is not a performance metric. It is a structural guarantee of loss. The 241-day mean containment window is the product of systems that detect first and act later.

LEGACY DECISION CYCLE		AUTONOMOUS DECISION CYCLE	
Hours → Days → Weeks		Milliseconds	
01 CLASSIFY	Manual identification & classification (weeks or months)	01 CLASSIFY	Real-time auto identification & auto classification of content in motion
02 DETECT	DLP rule matches manual input pattern and/or classification tag	02 DETECT	Machine-generated directive based on corporate business logic
03 DECIDE	Manual policy matching — leads to excessive false positives	03 DECIDE	Auto policy synthesis — cuts false positives and false negatives
04 ACT	Monitor mode only — data actually gets leaked/exfiltrated	04 ACT	Real-time enforcement — exfiltration/leak structurally prevented

What Did NOT Change

No disruption to user workflows. No performance degradation across multiple global sites. No training data or pre-labeled datasets required before day one. ISE operates inline, augmenting existing controls — not replacing them. No rip-and-replace. Each phase independently valuable.

Not ISE's differentiators. The irreducible requirements of autonomous IP protection.

- I** **Auto Identification & Auto Classification** — Identifies and classifies all sensitive data in motion — structured and unstructured, known and previously unknown — without manual tagging. Classification at human speed has a human-speed ceiling. In an agentic environment, that ceiling is the breach window.
- II** **Auto Policy Generation & Synthesis** — Policy synthesized from business logic, not authored by humans. Human-authored policy introduces two failure modes that cannot be engineered out: error and insider exploitation. A system where humans write the rules is a system humans can circumvent.
- III** **Intent-Aware Governance** — Evaluates behavioral context — who, what data, which channel, what time, what volume — not merely standing permission. GRC-based data access control extends to the word level within documents. Rules that operate at the file level cannot govern at the data level.
- IV** **Real-Time Interdiction** — Enforcement executes at the moment of transmission. Detection without immediate action is forensics preparation, not protection. The 241-day mean containment window is the product of systems that detect first and act later.
- V** **Immutable Forensics** — Every decision produces a complete, tamper-proof causal chain. Compliance must be a continuous system property — not an audit-preparation activity. A system that requires humans to reconstruct evidence has already failed the governance standard.

Detection: 20% → 100%. The difference is architecture.

Scenario A — Sensitive IP Design Documents Emailed to Unauthorized External Recipients

LEGACY DLP

IP Design Documents freshly created with no classification tagging. DLP doesn't understand unstructured data within the documents. No DLP rule is in place to trigger. Days later, analyst reviews anomaly report. Data already gone.

DATA LOST — UNDETECTED

ISE AUTONOMOUS

Actor Intelligence IDs agent. Data Intelligence classifies payload Financial/Highly Confidential. Access Intelligence flags anomalous volume. Blocking directive generated. Enforcement <100ms. Immutable forensic chain logged.

CLASSIFIED · BLOCKED · REPORTED · LEARNED

Scenario B — Proprietary Source Code Upload to GenAI Platform

LEGACY DLP

No detection covers unclassified uploads to GenAI channels. Proprietary source code exits. Surfaces in a competitor product six months later.

IP LOST — UNDETECTED

ISE AUTONOMOUS

Data Intelligence classifies Proprietary Source Code/Highly Critical. Access Intelligence flags GenAI platform as unauthorized for this data class. Enforcement <100ms. Full causal chain logged.

CLASSIFIED · BLOCKED · REPORTED · LEARNED

Scenario C — Malicious Insider Exfiltration of IP Documents via Encrypted FTP

LEGACY DLP

Legacy DLP/CASB cannot process encrypted traffic. Sensitive data exits, surfaces on dark web. Regulatory violations, material fines.

DATA LOST — REGULATORY EVENT

ISE AUTONOMOUS

Access Intelligence flags anomalous encrypted content. Transfer quarantined and escalated to supervisor in real time. Supervisor denies. Complete causal chain logged immutably.

QUARANTINED · ESCALATED · REPORTED

The Board Trigger

If this is true, continuing with a policy-based model is not a risk decision. It is the absence of one.

Choosing a legacy manual policy-based system in an autonomous data environment introduces a known and unresolvable control gap. The CISO who selects a manual policy-based architecture in 2026 is not making a conservative choice — they are accepting structural liability for the class of breaches that architecture cannot detect.

Visit gccybersecurity.ai to discuss a technical demonstration and proof-of-value assessment.