

When the Mission Cannot Tolerate a Data Exfiltration Event

How a National Cyber Coordination and Command Center Achieved Centralized, Automated Sensitive-Data Enforcement

5th Gen ISE ARCHITECTURE Generation of enforcement platform	Multi- AGENCY COVERAGE Centralized across org boundaries	Real-Time APT DETECTION Advanced persistent threat response	Zero-Touch POLICY SYNTHESIS From operational guidelines to rules
--	---	--	---

A national-security agency in Southeast Asia faced a challenge that defines modern government data protection: how to apply consistent, automated enforcement across heterogeneous systems, multiple agencies, and mixed populations of cleared personnel, contractors, and partners — **without a human in every decision loop.**

The Operational Problem

The agency commissioned a National Cyber Coordination and Command Center to monitor sensitive communications, information exchanges, and critical cyber infrastructure across a multi-agency environment.

The challenge was not detecting threats in isolation — it was enforcing protection at scale, in real time, across structured and unstructured data, for an organization where unauthorized disclosure carries mission-level consequences.

Threat Landscape

Insider Threats

Personnel with legitimate access and elevated trust create the hardest enforcement problem — standard perimeter controls cannot distinguish intent.

Advanced Persistent Threats (APT)

State-sponsored and sophisticated external actors target high-value government repositories through long-dwell, low-signal exfiltration patterns.

Multi-Agency Complexity

Different agencies, contractors, and partners operate under different classification rules — a single unified enforcement layer must account for all of them simultaneously.

Six Requirements the Agency Could Not Compromise On

Centralized monitoring & control · Automated classification of structured & unstructured data · **Policy synthesis from operational guidelines** · Identity- & role-based access controls · **Real-time transfer enforcement** · Forensic investigation support

The deployment used GC Cybersecurity's Information Security Enforcer (ISE) to connect four capabilities that legacy DLP treated as separate problems: identification, authorization, enforcement, and investigation — unified under centralized command and control.

01

CENTRALIZED
OVERSIGHT

A command-and-control capability provided a consolidated view of data-protection incidents and system status across all agencies and repositories — with analytics and forensic investigation tools for security operations.

02

AUTOMATED DATA
IDENTIFICATION

ISE identified and classified structured and unstructured sensitive information without relying on manual tagging or preprocessing. Classification ran continuously against active data flows — not point-in-time scans.

03

POLICY SYNTHESIS &
ROLE CONTROLS

The platform generated enforcement policies directly from operational guidelines and information classification, with access-control decisions informed by organizational roles and personnel clearances — no manual rule translation required.

04

REAL-TIME TRANSFER
ENFORCEMENT

ISE correlated actors, operations, and data in real time to distinguish permissible communications from unauthorized transfers — applying configured controls at the enforcement point before exfiltration completed.

Why ISE Was Selected Over Third-Generation DLP

The agency evaluated multiple third-generation DLP solutions. ISE was selected because those platforms could not simultaneously address insider threats, external APT exfiltration, automated unstructured-data classification, policy synthesis from guidelines, and centralized enforcement across a multi-agency environment.

BEFORE ISE	AFTER ISE
✗ Sensitive-data classification required manual tagging and preprocessing across every repository	✓ Automated identification of structured and unstructured sensitive data — continuously, without manual intervention
✗ Policy rules written by hand from classification guidelines — updated manually when guidelines changed	✓ Policy synthesis directly from operational guidelines — enforcement rules generated automatically
✗ No unified view: each agency or system maintained separate security operations and incident data	✓ Centralized command-and-control: consolidated incident visibility, analytics, and forensic investigation across all entities
✗ Role and clearance context ignored at enforcement — data type alone drove permit/block decisions	✓ Identity- and role-based controls: the same data transfer produces different outcomes based on personnel authorization
✗ Forensic investigation required manual log correlation across multiple agency systems	✓ Structured forensic records generated at enforcement time — supporting rapid incident investigation and attribution

Phase 1 · Proof-of-Value Framework for Government Environments	
What to Measure □ Automated classification accuracy on representative data sample □ Policy synthesis accuracy from operational guidelines □ Role-context enforcement accuracy across personnel tiers □ Insider-threat and APT scenario detection rate □ Forensic record completeness for a defined incident set	Success Conditions □ No unauthorized transfer of classified data in test scenarios □ Policy rules accurately reflect operational classification □ Authorized personnel operations uninterrupted □ Forensic records produced for 100% of test events □ Centralized C2 view validated across simulated agencies

The agency evaluated and rejected multiple third-generation DLP platforms. The gaps were not configuration issues — they were **architectural limitations** that no amount of tuning could close.

Unstructured data blindness

Legacy: Third-gen DLP relied on manual tags, metadata, and structured data types. Sensitive information in documents, communications, and repositories without preprocessing was invisible to enforcement.

ISE: ISE automated classification of structured and unstructured content — enforcement applied to actual information, not labels applied in advance.

Static policy authoring

Legacy: Rules were written by analysts, one by one, from classification guidelines. When guidelines changed or new threats emerged, the policy lag created an enforcement gap.

ISE: ISE generated enforcement policies directly from operational guidelines — policy changes propagated automatically without analyst intervention.

Siloed agency visibility

Legacy: Each agency or system maintained its own security operations. Coordinated exfiltration attempts that crossed agency boundaries were invisible to any single operator.

ISE: Centralized command-and-control provided a unified incident view across all agencies — enabling correlation and response that isolated tools cannot support.

Context-free enforcement

Legacy: Third-gen DLP evaluated data type alone. A colonel and a contractor attempting the same transfer received the same decision — regardless of clearance level or operational role.

ISE: ISE incorporated identity and role context: the same data, the same transfer direction, but different enforcement decisions based on the actor's authorized access.

Forensic reconstruction burden

Legacy: Investigating a potential exfiltration event required manual log correlation across multiple systems — a process that took days and produced incomplete attribution.

ISE: ISE generated structured forensic records at enforcement time — enabling rapid incident reconstruction, attribution, and investigation support.

In a national-security environment, a data protection failure is not an IT incident — it is a mission-level event. Unauthorized disclosure of classified information, compromise of operational communications, or exfiltration by an advanced persistent threat each carry consequences that no breach notification process can remediate. The question is not whether to protect sensitive data. It is whether your current architecture can do it automatically, at scale, and with the evidence to prove it.

Can our enforcement keep pace with automated exfiltration attempts?

ISE operates in real time — correlating actor, data, and operation before any transfer completes. Manual review processes cannot compete with automated APT exfiltration at machine speed.

Do our policy controls reflect our actual classification system?

ISE synthesizes enforcement rules directly from operational guidelines and classification information — policies are not authored by analysts, they are generated from the authoritative source. When classification changes, enforcement changes.

If a breach occurred today, could we reconstruct what happened?

ISE generates structured forensic records at every enforcement event. Incident reconstruction does not require multi-system log correlation — the evidence is already organized, timestamped, and attributed.

Discuss Data Protection for Sensitive and Mission-Critical Environments

GC Cybersecurity's ISE platform brings automated classification, policy synthesis, role-aware enforcement, and centralized forensic records to organizations where a data protection failure is not recoverable. We offer a structured technical assessment scoped to your environment's classification system, personnel structure, and operational requirements.

[Visit gccybersecurity.ai](https://gccybersecurity.ai) to arrange a technical discussion.