SCCAI FUSION™ FABRIC

# Your security has boundaries.
# Your data does not.

**Executive overview** on maintaining Zero Trust control, resilience and accountability over sensitive information inside your environments and beyond the boundaries you govern.

SCCAI GUARD™
Controls data access

SCCAI VAULT™
Secures data lifecycle

SCCAI DATA™
Enables active data defense



INTUFO

EXECUTIVE SUMMARY

# Your data leaves every day. Your control doesn't have to.

Intufo SCCAI FUSION™ extends governed protection to sensitive files wherever business takes them.

## THE SITUATION

Sensitive data moves to customers, partners, suppliers and cloud platforms because the business requires it. That movement is part of normal operations.

## THE CONTROL GAP

Your security protects the environments you operate. Beyond them, protection depends increasingly on systems and people you do not control. Exposure can persist after the incident is contained.

**Recovering infrastructure does not automatically restore control of exposed data.**

## Protection becomes part of the data.

Protected data participates in its own defense.

Policy, access controls and accountability operate at the data-object level, evaluating context and executing approved protective responses to extend enterprise control beyond your infrastructure.

1. **PROTECT** — Apply policy
2. **EVALUATE** — Check interaction
3. **RESPOND** — Enforce action

### CONTROL

Retain authority as data moves.

Apply enterprise policy to supported sensitive files shared beyond your infrastructure.

### RESILIENCE

Reduce the value of stolen data.

Disrupt unauthorized access and limit the downstream consequences of compromise.

### ACCOUNTABILITY

Answer with evidence.

Preserve an immutable record of interactions and enterprise-approved responses.

**EXTENDS YOUR EXISTING SECURITY**

Network / Endpoint / Identity / Cloud / Zero Trust / Response

**SEE IT ON YOUR OWN DATA** Request a demonstration at info@intufo.com ›

THE RISK SHIFT

# The incident ends. Exposure does not.

Cut off one head, two grow back. Once sensitive data is compromised, containing the incident does not contain the exposure. Stolen information can be copied, combined, resold and reused—creating risk long after systems are restored.

### ONE COMPROMISE, MANY CONSEQUENCES

Compromised data can fuel extortion, fraud, credential abuse, social engineering and follow-on intrusion. Each reuse extends the impact of a single breach across the enterprise and over time.

### EXPLOITATION HAS INDUSTRIALIZED

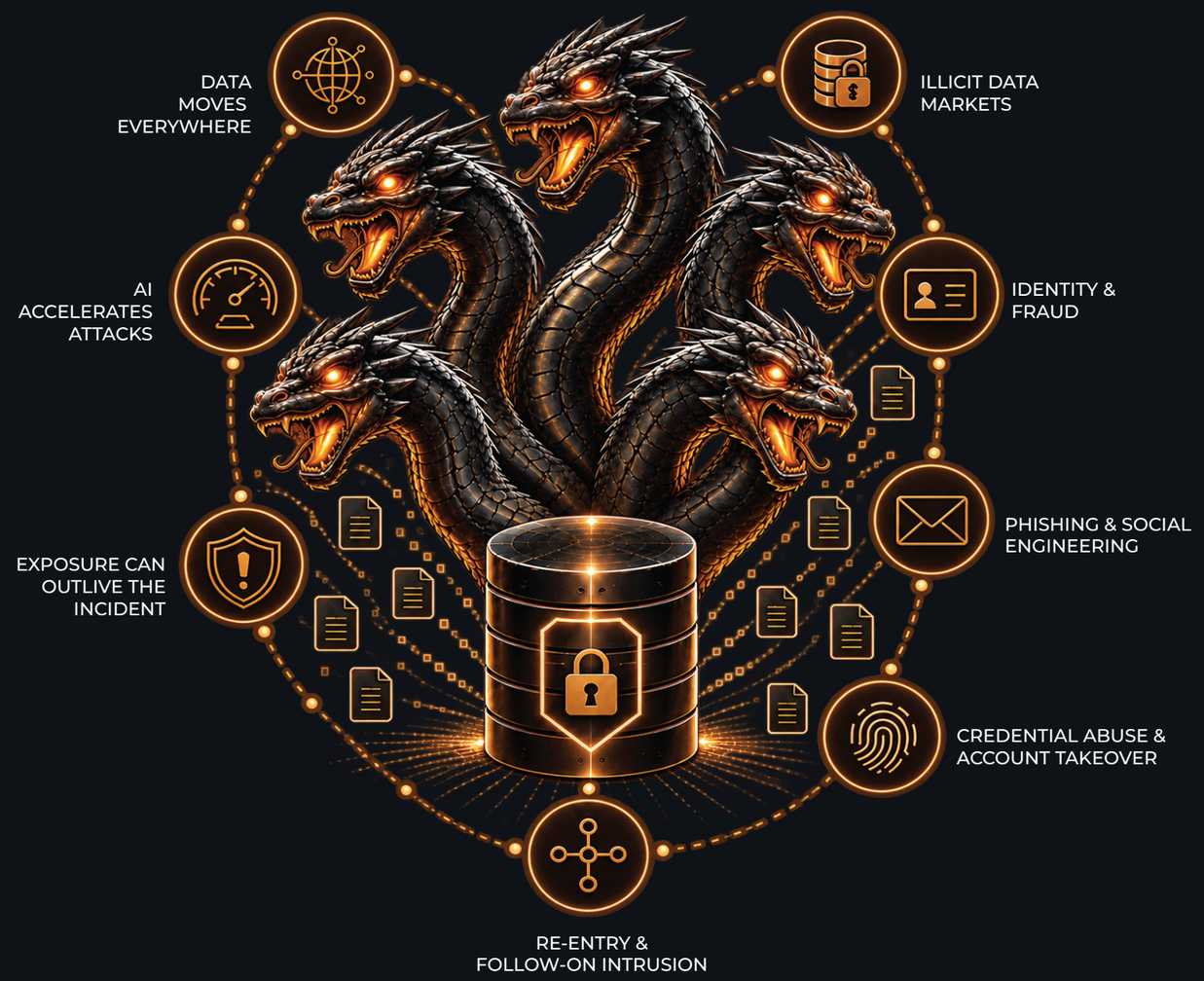
Stolen data becomes reusable inventory—traded, combined and exploited at scale. AI and automation are accelerating how quickly adversaries analyze and act on compromised information, increasing the speed and scale of exploitation.

### AND IT OFTEN STARTS OUTSIDE YOUR CONTROL

Increasingly, compromise begins in vendor-operated platforms where sensitive information accumulates through ordinary business activity. In 2025, one compromised chatbot integration exposed data at more than 700 organizations.[1]

## THE HYDRA EFFECT

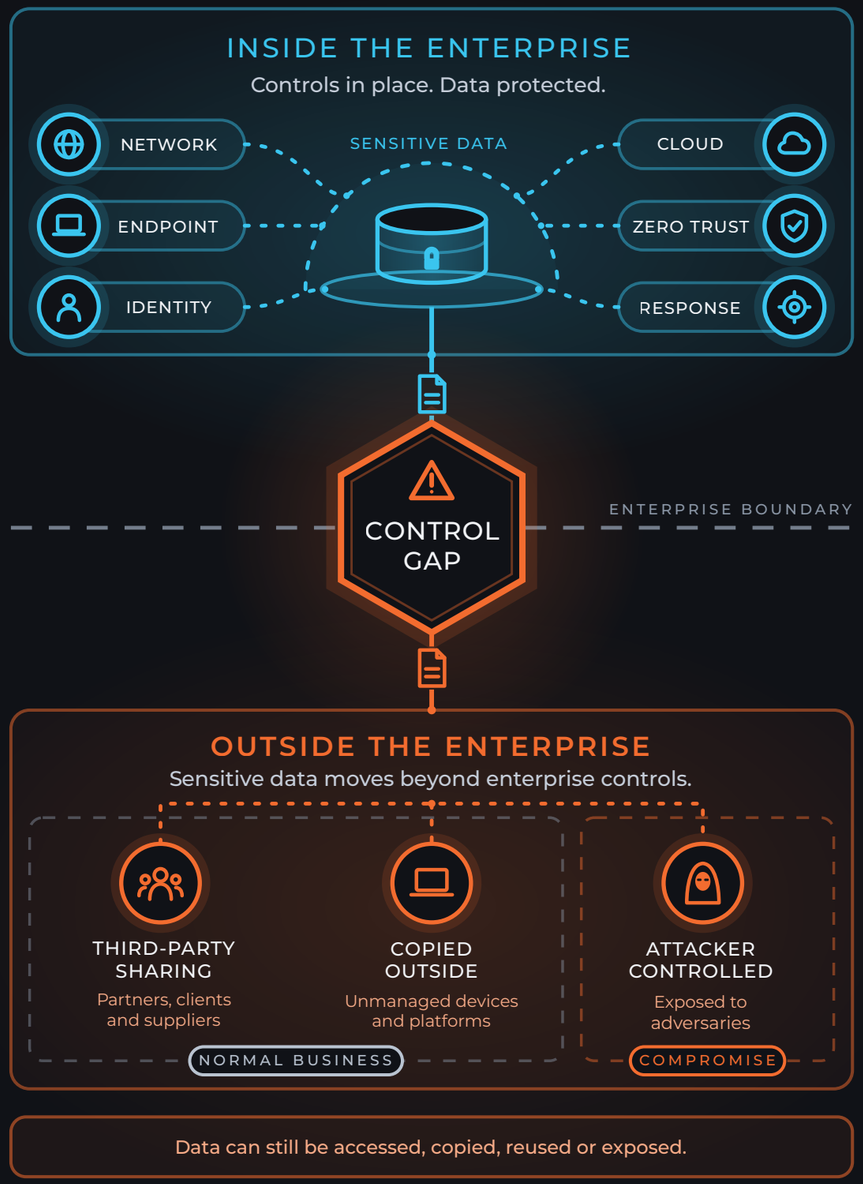
**ONE BREACH. MANY CONSEQUENCES.**




## A breach is no longer a point-in-time event.

[1] *https://www.obsidiansecurity.com/blog/unc6395-salesloft*

## THE CONTROL GAP




# Sensitive data must be shared. Retaining control is essential.

Protection requirements don't change when the environment does. Control must persist wherever protected data goes — across your infrastructure, through partner and supplier environments, and even after exfiltration.

### NOT AN INVESTMENT PROBLEM

Mature, well-funded security programs face the same gap. Your controls protect the environments you operate. Once data leaves them, enforcement depends on systems and people you don't control.

### DEPENDENCY INCREASES. RESPONSIBILITY REMAINS

As sensitive data operates beyond enterprise-governed infrastructure, its protection increasingly depends on the environments and controls of others.

### AND THE ANSWERS ARRIVE LATE

When sensitive data is compromised in a vendor-operated platform, the enterprise may learn what happened after control has already been lost.

**An enterprise can recover its infrastructure without recovering control of its data.**

When data moves, control can be lost.

**Unless the data participates in its own defense.**

FROM PASSIVE ASSET TO ACTIVE PARTICIPANT

# Protection becomes something the data does.

Traditional data is passive. Remove the controls around it, and it cannot protect itself. SCCAI FUSION™ changes that. The data becomes part of the defense.

### A NEW KIND OF FILE

A conventional file is content and metadata. Self-defending data combines identity, policy and trusted behavior as part of the object.

### PROTECTED THE MOMENT IT EXISTS

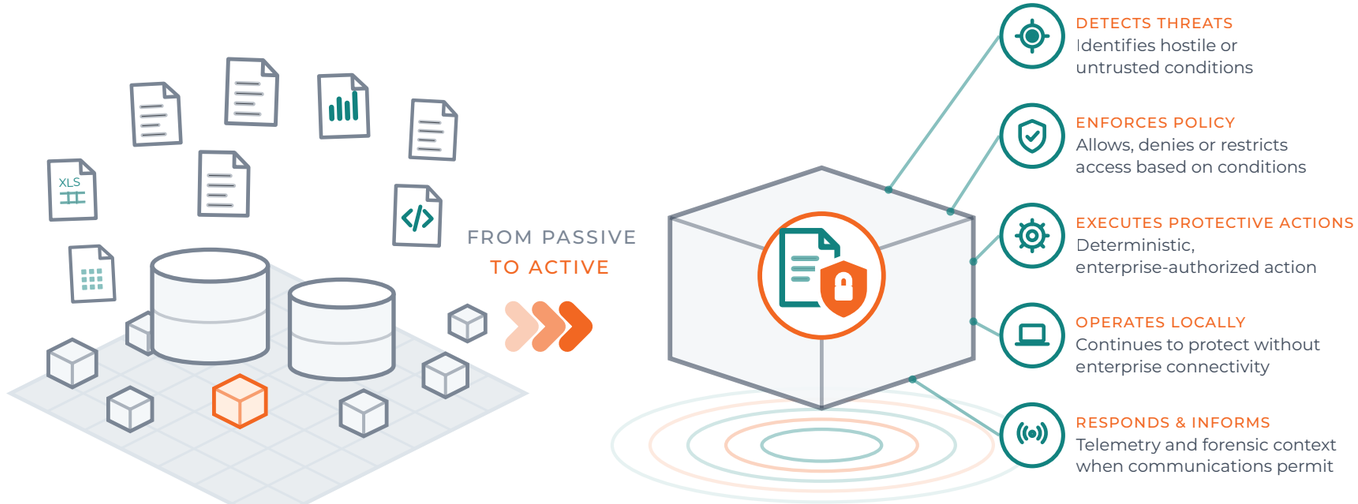
Instead of relying on discovery to secure sensitive data, SCCAI FUSION™ applies protection the moment a file is stored.

### THE ENTERPRISE DEFINES. THE DATA EXECUTES.

Every action available to protected data is authorized by your organization before it is ever needed. The data responds to changing conditions within defined enterprise constraints, enabling automated, proactive self-protection.

**PASSIVE DATA**
Dependent. Passive. Silent.

**ACTIVE SELF-DEFENDING DATA**
Detects. Defends. Responds.




No awareness. No response. Dependent on the controls around it.

## SCCAI™ — SMART CYBER CELL™ AI

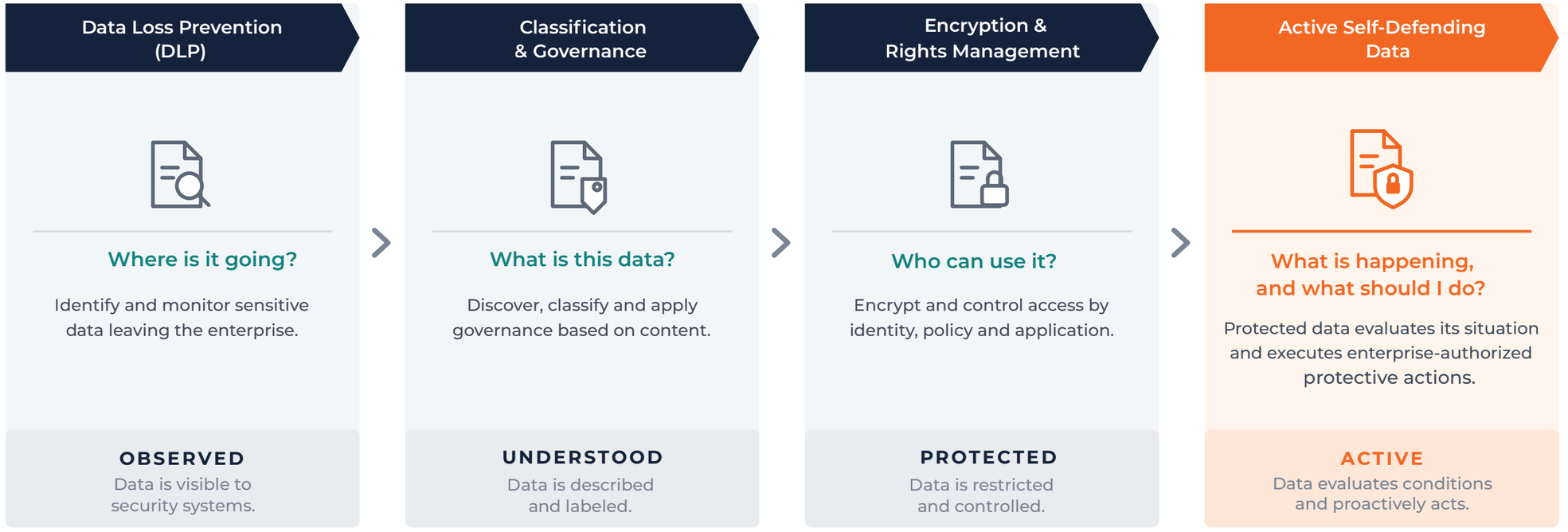
Intufo's patented and patent-pending technology for transforming protected data from a passive asset into an active participant in its own protection and enterprise defense.

THE DATA PROTECTION SPECTRUM

# Data has remained passive. Until now.

Enterprise data protection spans several capabilities. Each solves a real problem — preventing loss, understanding content, controlling access. Most organizations run all three.

Across every one of them, the data itself stays passive. It is watched, labeled and restricted by the systems around it, but it cannot evaluate its own situation or act on what it finds.




**Security systems have become increasingly intelligent about data.**
**SCCAI FUSION makes data smarter about security.**

## THE FUSION ADVANTAGE

What extending protection to the data means for business.




# Extend what you've built. Don't replace it.

SCCAI FUSION™ extends this protection and empowers the data with self-protection wherever it goes.

**Control.**
Your policies travel with the data, and your organization holds the keys. So a contract shared with a supplier can stay under enterprise control even after it's downloaded.

**Resilience.**
Protected data executes enterprise-authorized protective actions when hostile or untrusted conditions are detected, helping contain the consequences of compromise.

**Accountability.**
Access is recorded in an immutable chain of custody. When a partner is breached, you can explicitly show which files were exposed, and which weren't.

**Empower your enterprise defense.**
**Extend protection to the data itself.**

THE SCCAI FUSION FABRIC

# Three coordinated Zero Trust layers. One protection fabric.

CONTROL INSIDE

## SCCAI GUARD™

Verifies every interaction before protected data is accessed.

**VERIFY THE INTERACTION**
Evaluates user, device and context before any access.

**ENFORCE POLICY IN REAL TIME**
Least-privilege access; risky or unauthorized activity is blocked.

**ESTABLISH A TRUSTED FOUNDATION**
Kernel-level enforcement and tamper-resistant controls.

Kernel-level enforcement · Real-time monitoring · Policy-driven access

Trust the interaction, not simply the endpoint.

ACCOUNTABILITY THROUGHOUT

## SCCAI VAULT™

Enterprise-held keys and policy, from creation through every use.

**PROTECT BY POLICY**
Applied at creation or export, by policy rather than user decision.

**RETAIN AUTHORITY**
You own the keys and the policy. We enable protection.

**CONTROL ACCESS AND USE**
Govern who can use data, and how, across people, devices and systems.

**PRESERVE ACCOUNTABILITY**
Immutable records: evidence for security, compliance and audit.

Customer-managed keys · Automated key rotation · Immutable chain of custody · Protection in use

Your data. Your keys. Your control.

CONTROL BEYOND

## SCCAI DATA™

Protection that stays with the data, beyond enterprise infrastructure.

**DETECT**
Recognizes defined threats and untrusted conditions.

**DEFEND**
Executes authorized, pre-defined countermeasures.

**OPERATE LOCALLY**
Protective actions continue without connectivity.

**INFORM THE ENTERPRISE**
Telemetry and alerts when communications permit.

Policy-defined actions · Zero Trust in the data · Deterministic countermeasures

When infrastructure control ends, protection doesn't.

---

**SCCAI GUARD™**
Controls the interaction — enforcing enterprise policy before protected data is accessed.

**SCCAI VAULT™**
Controls the lifecycle — enterprise-held keys and policy from creation through access, use and sharing, with immutable chain of custody.

**SCCAI DATA™**
Extends defense beyond enterprise control — detecting defined conditions and executing authorized countermeasures.

SCCAI FUSION FABRIC IN ACTION

# From data-level intelligence to business resilience.

**Protect. Respond. Limit Impact.**
SCCAI operates at the data-object level—evaluating changing conditions and executing enterprise-authorized protective actions where the data operates.

The three layers operate as one system, continuously evaluating changing conditions and enforcing enterprise-defined responses. Protection adapts as conditions change, response accelerates, and the consequences of compromise are contained.



### DISCOVER SOONER
Detect changing security conditions and capture relevant telemetry.

### EVALUATE IN CONTEXT
Evaluate context and determine whether conditions remain trusted.

### RESPOND FASTER
Enforce enterprise-defined policy and execute authorized protective actions.

### LIMIT THE IMPACT
Reduce exploitation while preserving evidence and accountability.



**DETECT**
Conditions at the data object.



**TELEMETRY**
Signal with context.



**EVALUATE**
Context against your policy.



**DETERMINE**
Trusted or not.



**ENFORCE**
Checked at every interaction.



**CONTAIN INSTANTLY**
Revoke a device — all files, at once.



**MAKE UNUSABLE**
Unreadable outside your policy.



**EVIDENCE KEPT**
Immutable record.

**Intelligence evaluates. Policy decides. Enforcement acts.**
**Fast because the response was authorized in advance.**

THE EXECUTIVE STANDARD

# What the board is actually asking

Three questions every board should be able to answer — with evidence, not assurance.

1 Where does our data go, and do we still control it?

Yes. Control travels with the data into every environment.

ANSWERED ON PAGE 12 →

2 Can we limit the consequences if our data is exfiltrated?

Yes. What an adversary takes can be rendered unusable when unauthorized access is attempted.

ANSWERED ON PAGE 13 →

3 If something happens, can we prove what occurred?

Yes. *Immutable records preserve what happened, rather than requiring reconstruction*.

ANSWERED ON PAGE 14 →

QUESTION 1 OF 3

Where does our data go, and do we still control it?

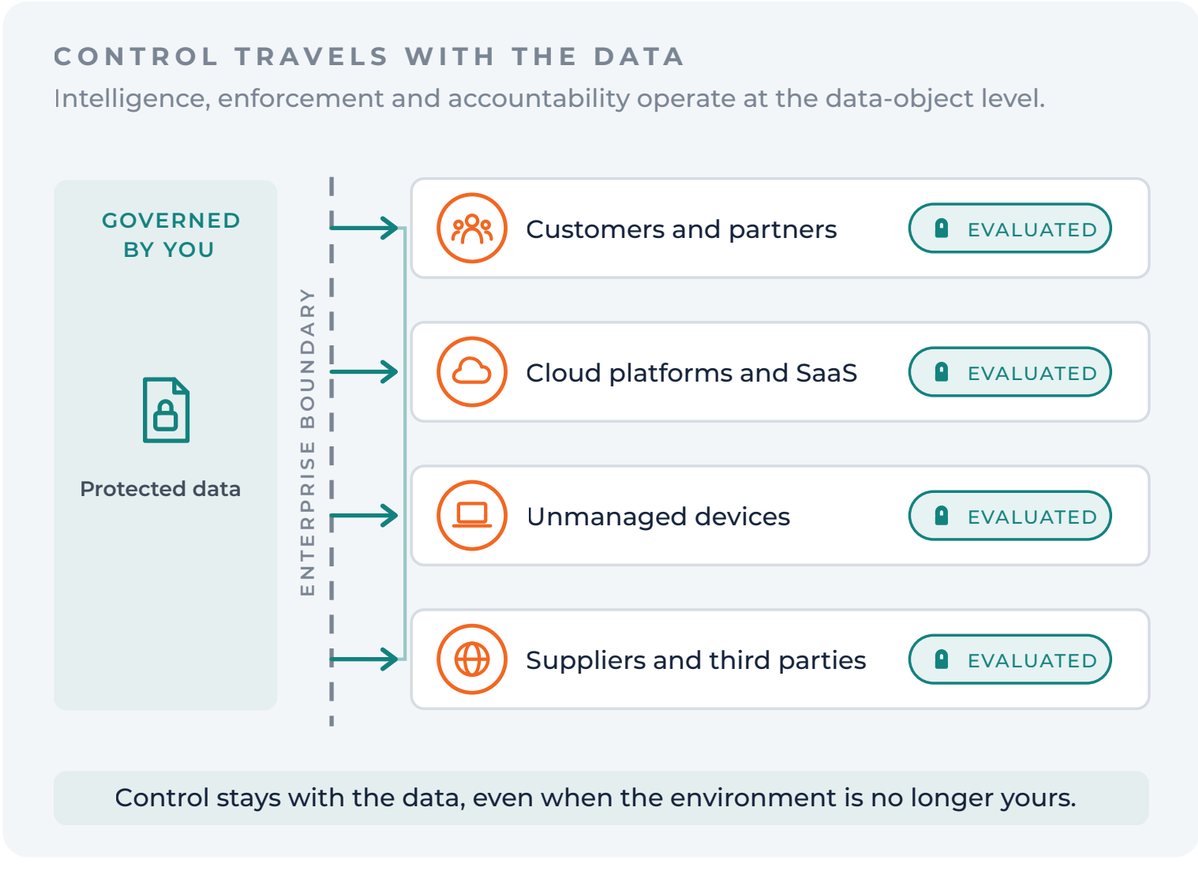
# Enterprise control reaches farther than your infrastructure.

Sensitive data leaves through ordinary work, moving to customers, partners, suppliers and platforms the business depends on.

Protected data carries more than policy. Intelligence, enforcement and accountability operate at the data-object level — evaluating each interaction, executing authorized responses when defined conditions are met, and preserving a record of access.

BUSINESS IMPACT

Greater visibility and retained control as data moves beyond your environments.




**Your infrastructure stops.**
**Your control doesn't.**

QUESTION 2 OF 3

Can we limit the consequences if our data is exfiltrated?

# Change the economics of data theft.

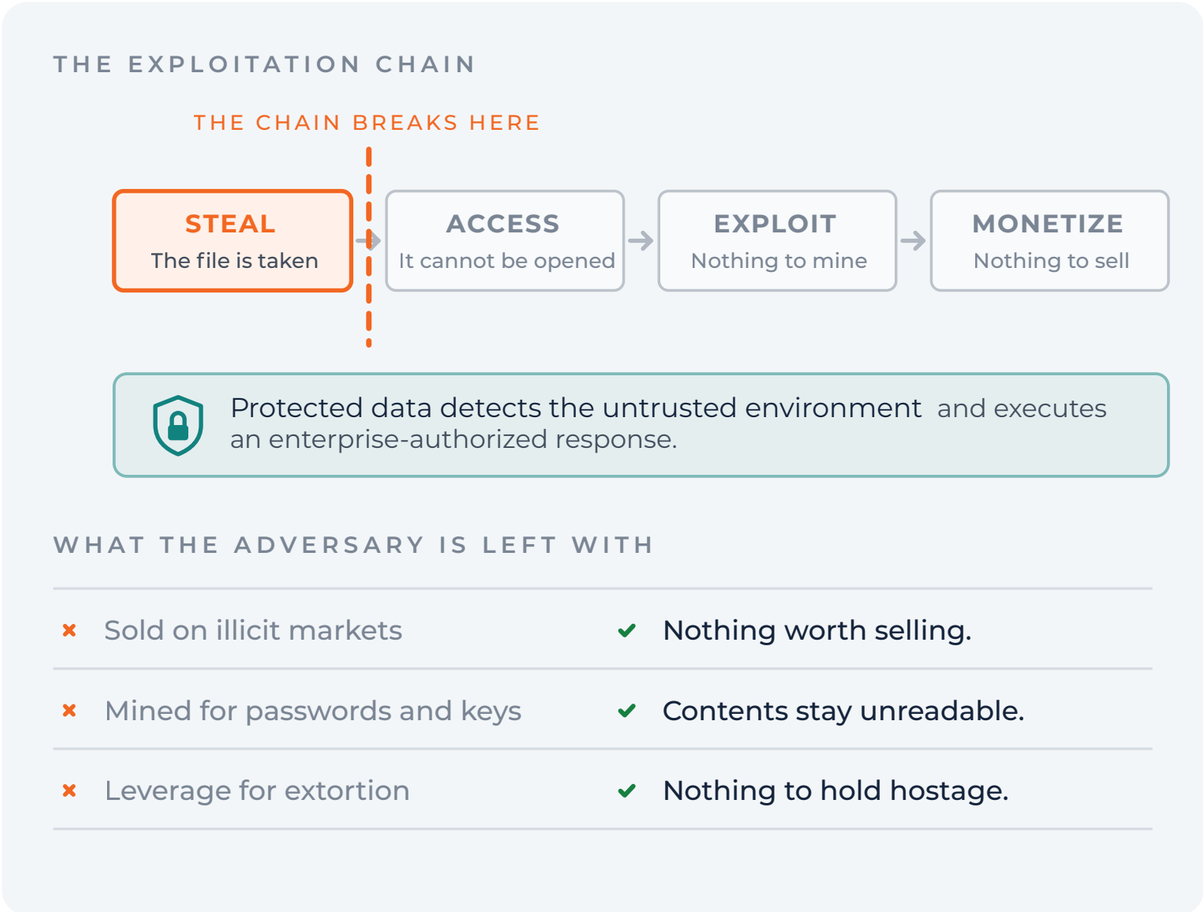
Stealing data is only the first step. Its value comes from what follows: opening it, mining it for credentials, and selling orransoming what is found.

## Make stolen protected data materially harder to exploit.

Protected data detects hostile or untrusted conditions and executes deterministic, enterprise-authorized protective actions that disrupt an adversary's ability to access and exploit the information.  Reduce the usable value of protected information after exfiltration, limiting the downstream consequences an adversary can create.

BUSINESS IMPACT

Reduce the value an adversary can realize from stolen data, and the financial impact of compromise.




**They get the file. They don’t get the usable data.**
**You get the evidence and stop feeding the Hydra.**

QUESTION 3 OF 3

If something happens, can we prove what occurred?

# A record, not a reconstruction.

After an incident, organizations often reconstruct events across multiple systems and sources.

## The record already exists.

Every interaction with protected data is preserved as it happens — who opened it, from where, and what the enterprise-authorized response was.

### WHAT THE RECORD GIVES YOU

- Access events are recorded as they happen.
- An immutable chain of custody.
- Forensic readiness from day one.

**BUSINESS IMPACT**

Answer regulators, insurers and customers with evidence rather than assurance.

ACCESS RECORD — ILLUSTRATIVE

Supplier_Contract_Q3.pdf

| | | |
|---|---|---|
| MAR 04 09:12 | Protection applied at export | POLICY APPLIED |
| MAR 04 09:14 | Shared with Supplier A | RECORDED |
| MAR 04 14:30 | Opened by 2 approved users | ALLOWED |
| MAR 11 08:05 | Opened on approved device | ALLOWED |
| MAR 19 02:47 | Open attempt, unknown environment | DENIED |
| MAR 19 02:47 | Countermeasure executed | RECORDED |
| MAR 19 02:51 | Reported to enterprise | TELEMETRY |
| MAR 20 10:00 | Access revoked for Supplier A | REVOKED |

**Preserved as it happens. Not reconstructed afterwards.**

**Actions governed.**
**Evidence preserved.**

ABOUT INTUFO

# Engineering predictable protection for data that moves.

Intufo develops enterprise security technology for high-stakes environments. Our purpose is to help organizations retain control of sensitive information wherever it travels.

Our team brings decades of experience across artificial intelligence, cybersecurity, large-scale IT operations, networking, data centers and distributed systems.  That experience informs technology designed around enterprise policy, predictable enforcement and accountable outcomes.

FOUNDER



## Shelia Burgess

***Inventor, Founder & CEO***

Leadership grounded in enterprise AI, cybersecurity and systems designed for adversarial environments.

INTUITIVE INFORMATION

## Protection informed by context. Control retained by the data

Intufo takes its name from Intuitive Information: technology to interpret defined conditions while preserving the owner's authority.

SCCAI FUSION™

## From passive data to active defense.

SCCAI FUSION™ is a Zero Trust, data-centric enterprise protection fabric that extends governed protection and control directly to sensitive data. It combines deterministic agentic AI for threat detection and response, enterprise policy control, trusted enforcement and accountability at the data-object level, enabling protected data to evaluate changing conditions and execute enterprise-preauthorized protective actions wherever it travels.

**DECADES OF EXPERIENCE**
AI · Cybersecurity · Enterprise IT

**ENTERPRISE-GOVERNED**
Policy-defined, accountable response

SEE SCCAI FUSION ON YOUR OWN DATA  info@intufo.com ›

**always know. always control.**

*Know where protected data goes. Control how it can be used.*

INTUFO

4700 Millenia Blvd., Suite 175
Orlando, Florida  32839

833-352-4012

www.intufo.com

CONTACT INTUFO →

This Executive Brief provides a high-level overview of Intufo, SCCAI FUSION™, and our approach to data-centric cybersecurity.  It is intended for informational purposes and to support executive discussion around cybersecurity risk, resilience, data protection, and enterprise control. Organizations should evaluate their own business, technical, regulatory, and operating requirements when considering any security strategy or technology.  Product capabilities, features, specifications, and availability may evolve over time.  SCCAI™, SCCAI FUSION™, SCCAI GUARD™, SCCAI VAULT™, SCCAI DATA™, and related technologies and materials are the property of Intufo, Inc. and may be protected by issued and pending intellectual property rights.

Copyright © 2026 Intufo, Inc. All rights reserved.