Enterprise Research Shield

Information Sheet for Procurement

"Insights without exposure."

Why ERS?

In an era where nearly every organization wants to leverage advanced data analysis, yet remains concerned about sensitive information being exposed or used outside their control, ERS fills a critical need.

ERS is a **protection tool** – not just an analysis tool. It is specifically designed for healthcare, government agencies, and other organizations where confidentiality is legally mandated and business-critical.

Our Promise

ERS gives you the power to decode and analyze your most sensitive documents – **without a single byte of data leaving your control**. We build intelligence locally with ERS Memory Vaults, verified by Koda Trust Score.

Three Key Features

1. ERS Memory Vault – Knowledge That Stays With You

The system's analysis components develop their understanding through dedicated memory vaults (ERS Memory Vaults). All learning occurs locally and in isolation.

- **The argument:** "Your data makes ERS smarter for you, but never for anyone else."
- The system learns your medical record language and routines without information leaving your digital walls.

2. Koda Trust Score – Measurable Security

Koda Trust Score functions as a continuous health check, not a one-time stamp. It measures system integrity in real-time and provides concrete proof of your security level.

Pillar	What It Measures	Why It Matters
Data Containment	No data flows outside defined zones	Guarantees sensitive data stays where it should
Authorization	Access patterns and authorization compliance	Detects unauthorized or anomalous access
System Health	Integrity, patch level, configuration status	Ensures system is updated and unaltered
Audit Trail	What, when, by whom, with what result	Provides traceability and evidence chain for audits

Important: Score is the indicator. Actions are governed by policy thresholds that your organization configures. You own the rules.

3. Decoding Without Exposure

Many competing solutions send text to external cloud services for analysis. ERS works locally or in an isolated environment – you get the insights, but keep the secrets.

Trust Badge – Visible Status

ERS continuously displays the system's security status via a Trust Badge designed to be understandable for both technical staff and management:

Last Check	Date and time
Next Check	Date and time
Status	Normal / Elevated / Locked
Reason	One line without technical noise (if warning)

Example: *"Score 92/100 – Elevated level (new administrative login). No data flows outside zone. Action: extra logging active."*

Architecture: ERS as Auditor

ERS is built on a monitoring architecture where a central component functions as an internal auditor. This ensures:

- **Control** – continuous monitoring of all system activity
- **Traceability** – every event is logged with timestamp and responsible component
- **Compliance** – automatic verification against your security policies

Control Methodology

ERS uses enterprise-adapted control methods that minimize impact on operations:

- **Scheduled checks** – periodic auditing according to configured schedule
- **Event-driven control** – immediate verification upon risk indicators
- **Policy/Config Drift** – detects if security configuration has changed since last approved baseline
- **Update Hygiene** – checks patch level, signature verification, and change log

Data Ownership – Your Data, Your Terms

All memory is customer-owned. Period.

ERS gives you full control over how system memory is managed:

- **Time-limited memory** – configurable lifespan (e.g., 1 day, 1 week)
- **Automatic deletion** – memory is cleared according to your rules without manual handling
- **Policy-controlled** – your organization decides what is saved, for how long, and when it's removed

This is a strength, not a limitation – short-lived memory reduces risk exposure and simplifies GDPR compliance.

Logs in Your Language – Not Technical Noise

Traditional security systems present logs in technical formats like JSON, stack traces, or hexadecimal code – incomprehensible to everyone except specialists.

ERS translates everything to natural language.

Technician sees	ERS user sees
`Error: 503 Service Unavailable / timeout 3000ms`	"The system couldn't reach the database, it took too long. Retrying."
`Access_Denied_Vault_7 / severity: WARNING`	"Someone tried to open a protected folder without permission. The event has been logged."

Available in Swedish, English, and German – all logs, warnings, and reports are displayed in your chosen language.

The advantage: Managers and decision-makers can understand the security status directly in the dashboard without needing to be IT experts. It's democratization of data.

Self-Healing System – ERS Fixes Problems Automatically

ERS continuously monitors system health and can automatically resolve common operational issues – without manual intervention. All events are logged in your language so you always understand what happened.

Example notification from ERS:

> **Notice: Operational Status (History)**
>
> Time: 14:35 | Level: Yellow (Warning)
>
> *"The database is temporarily overloaded."*
>
> **Analysis:** A sudden increase in incoming data was detected.
> **Security:** No data has leaked. Koda Trust Score is unaffected.
> **Action:** I have temporarily expanded database capacity to handle the load.
> **Current status:** The system is functioning normally and no users were affected.
>
> *– Your ERS*

The result: Fewer support tickets, faster recovery, and full transparency – in your own language.

Installation

Installation takes place locally in your environment and can be performed remotely by the vendor in collaboration with your IT department.

The vendor has no access to customer data or analysis content. Service and support are based exclusively on system status, operational indicators, and security metrics.

Updates Without Exposure – Full Control With You

ERS is updated via cryptographically signed system packages installed locally in your environment. Updates never affect documents, analysis content, or ERS memories. All updates occur under customer control – you approve every step and always own the decision.

In practice, this means:

- No remote logins to customer environment
- No access to data, memories, or logs
- Automatic verification after update
- Safe rollback in case of deviation
- Full local traceability for auditing

Principle: *"We update the system – not your information."*

Integration with Existing Antivirus

ERS continuously monitors your internal network and immediately detects if malicious code attempts to enter. The system collaborates seamlessly with your existing antivirus solutions.

How it works:

- **Early detection** – ERS identifies anomalous behavior in network traffic before it becomes a problem
- **Coordinated response** – when threats are detected, your existing antivirus program is automatically activated
- **Backup action** – if the antivirus program doesn't respond, ERS handles the threat itself
- **Complementary protection** – ERS doesn't replace your antivirus program, it enhances it

Easy Server Installation

ERS is designed for smooth integration into existing IT environments. The system is easy to install on servers and requires minimal configuration to get started. Your IT department can have the system operational in a short time.

Designed for Procurement

ERS is designed to meet the requirements of public and private procurement:

- **NIS2 compatibility** – meets upcoming EU cybersecurity requirements
- **Audit documentation** – complete evidence chain for auditing
- **Configurable policy** – the organization owns and controls all thresholds and actions
- **Local operation** – no data leaves your controlled environment

Summary

Challenge	ERS Solution
Data can leak to external systems	All processing occurs locally
Difficult to prove security	Koda Trust Score with audit trail
Systems learn from others' data	ERS Memory Vaults – isolated learning
Lack of traceability during incidents	ERS as Auditor with evidence chain

Contact

For more information about ERS and how it can be adapted for your organization, contact us for a demonstration.

Mats Hamberg
Founder and CEO

Email: info@nordicintegrity.se
Phone: +46 70-037 74 59

Nordic Integrity Systems AB
ERS – Enterprise Research Shield
Insights without exposure.