

# Enterprise Research Shield

*Informationsblad för upphandlare*

*"Insikter utan insyn."*

## Varför ERS?

I en tid där nästan alla organisationer vill dra nytta av avancerad dataanalys, men samtidigt är oroliga för att känslig information ska exponeras eller användas utanför organisationens kontroll, fyller ERS ett kritiskt behov.

ERS är ett **skyddsverktyg** – inte bara ett analysverktyg. Det är specifikt utformat för sjukvård, myndigheter och andra organisationer där sekretess är lagstadgad och affärskritisk.

## Vårt löfte

ERS ger er kraften att avkoda och analysera era känsligaste dokument – **utan att en enda byte data lämnar er kontroll**. Vi bygger intelligens lokalt med ERS Memory Vaults, verifierat av Koda Trust Score.

## Tre nyckelfunktioner

### 1. ERS Memory Vault – Kunskap som stannar hos er

Systemets analyskomponenter utvecklar sin förståelse via dedikerade minnesvalv (ERS Memory Vaults). All inlärning sker lokalt och isolerat.

- **Argumentet:** "Er data gör ERS smartare för er, men aldrig för någon annan."
- Systemet lär sig ert journalspråk och era rutiner utan att information lämnar era digitala väggar.

### 2. Koda Trust Score – Mätbar trygghet

Koda Trust Score fungerar som en kontinuerlig hälsokontroll, inte en engångsstämpel. Den mäter systemets integritet i realtid och ger er konkret bevis på säkerhetsnivån.

Pelare	Vad den mäter	Varför det är viktigt
<b>Data Containment</b>	Inga dataflöden utanför definierade zoner	Garanterar att känslig data stannar där den ska
<b>Behörighet</b>	Åtkomstmönster och behörighetsefterlevnad	Upptäcker obehörig eller avvikande åtkomst
<b>Systemhälsa</b>	Integritet, patchnivå, konfigurationsstatus	Säkerställer att systemet är uppdaterat och oförändrat
<b>Revisionsunderlag</b>	Vad, när, av vem, med vilket resultat	Ger spårbarhet och beviskeda vid granskning

**Viktigt:** Score är indikatorn. Åtgärder styrs av policy-trösklar som er organisation själv konfigurerar. Ni äger reglerna.

### 3. Avkodning utan exponering

Många konkurrerande lösningar skickar text till externa molntjänster för analys. ERS arbetar lokalt eller i isolerad miljö – ni får insikterna, men behåller hemligheterna.

## Trust Badge – Synlig status

ERS visar kontinuerligt systemets säkerhetsstatus via en Trust Badge som är utformad för att vara begriplig för både teknik och ledning:

<b>Senaste kontroll</b>	Datum och tidpunkt
<b>Nästa kontroll</b>	Datum och tidpunkt
<b>Läge</b>	Normal / Förhöjd / Låst
<b>Orsak</b>	En rad utan tekniskt brus (vid varning)

**Exempel:** "Score 92/100 – Förhöjd nivå (ny administrativ inloggning). Inga dataflöden utanför zon. Åtgärd: extra loggning aktiv."

## Arkitektur: ERS som Auditor

ERS bygger på en övervakande arkitektur där en central komponent fungerar som en intern revisor. Detta säkerställer:

- **Kontroll** – kontinuerlig övervakning av all systemaktivitet
- **Spårbarhet** – varje händelse loggas med tidstämpel och ansvarig komponent
- **Regelefterlevnad** – automatisk verifiering mot era säkerhetspolicyer

## Kontrollmetodik

ERS använder enterprise-anpassade kontrollmetoder som minimerar påverkan på drift:

- **Schemalagda kontroller** – periodisk revision enligt konfigurerat schema
- **Händelsestyrd kontroll** – omedelbar verifiering vid riskindikationer
- **Policy/Config Drift** – upptäcker om säkerhetskonfiguration ändrats sedan senaste godkända baseline
- **Update Hygiene** – kontrollerar patchnivå, signaturverifiering och förändringslogg

## Dataägarskap – Er data, era villkor

Allt minne är kundägt. Punkt.

ERS ger er full kontroll över hur systemminne hanteras:

- **Tidsbegränsat minne** – konfigurerbar livslängd (t.ex. 1 dygn, 1 vecka)
- **Automatisk radering** – minne rensas enligt era regler utan manuell hantering
- **Policy-styrt** – er organisation bestämmer vad som sparas, hur länge, och när det tas bort

Detta är en styrka, inte en begränsning – kortlivat minne minskar riskexponering och förenklar GDPR-efterskrivning.

## Loggar på ert språk – inte tekniskt brus

Traditionella säkerhetssystem presenterar loggar i tekniska format som JSON, stack traces eller hexadecimal kod – obegripligt för alla utom specialister.

ERS översätter allt till naturligt språk.

Tekniker ser	ERS-användaren ser
Error: 503 Service Unavailable / timeout 3000ms	"Systemet fick ingen kontakt med databasen, det tog för lång tid. Försöker igen."
Access_Denied_Vault_7 / severity: WARNING	"Någon försökte öppna en skyddad mapp utan behörighet. Händelsen är loggad."

Tillgängligt på svenska, engelska och tyska – alla loggar, varningar och rapporter visas på det språk ni väljer.

**Fördelen:** Chefer och beslutsfattare kan förstå säkerhetssläget direkt i dashboarden utan att behöva vara IT-experter. Det är demokratisering av data.

## Självläkande system – ERS åtgärdar problem automatiskt

ERS övervakar kontinuerligt systemets hälsa och kan automatiskt åtgärda vanliga driftproblem – utan manuell intervention. Alla händelser loggas på ert språk så att ni alltid förstår vad som hänt.

### Exempel på notis från ERS:

#### Notis: Driftstatus (Historik)

Tid: 14:35 | Nivå: Gul (Varning)

"Databasen är tillfälligt överbelastad."

**Analys:** En plötslig ökning av inkommande data noterades.

**Säkerhet:** Ingen data har läckt ut. Koda Trust Score är opåverkat.

**Åtgärd:** Jag har tillfälligt utökat databasens kapacitet för att hantera trycket.

**Status nu:** Systemet fungerar normalt och inga användare påverkades.

– Din ERS

**Resultatet:** Färre supportärenden, snabbare återställning, och full transparens – på ert eget språk.

## Installation

Installation sker lokalt i er miljö och kan genomföras på distans av leverantören i samverkan med er IT-avdelning.

**Leverantören har ingen åtkomst till kunddata eller analysinnehåll.** Service och support baseras uteslutande på systemstatus, driftindikatorer och säkerhetsmetrik.

## Uppdateringar utan insyn – full kontroll hos er

ERS uppdateras via kryptografiskt signerade systempaket som installeras lokalt i er miljö.

Uppdateringar påverkar aldrig dokument, analysinnehåll eller ERS-minnen. All uppdatering sker under kundens kontroll – ni godkänner varje steg och äger alltid beslutet.

### Detta innebär i praktiken:

- Inga fjärrinlogningar till kundmiljö
- Ingen åtkomst till data, minnen eller loggar
- Automatisk verifiering efter uppdatering
- Säker återställning vid avvikelse
- Full lokal spårbarhet för revision

**Princip:** "Vi uppdaterar systemet – inte er information."

## Samverkan med befintligt virusskydd

ERS övervakar kontinuerligt ert interna nätverk och upptäcker omedelbart om skadlig kod försöker ta sig in. Systemet samarbetar sömlöst med era befintliga antiviruslösningar.

### Så fungerar det:

- **Tidig upptäckt** – ERS identifierar avvikande beteende i nätverkstrafiken innan det blir ett problem
- **Samordnad respons** – vid hot aktiveras ert befintliga antivirusprogram automatiskt
- **Reservåtgärd** – om antivirusprogrammet inte agerar tar ERS själv hand om hotet
- **Kompletterande skydd** – ERS ersätter inte ert antivirusprogram, utan förstärker det

## Enkel serverinstallation

ERS är utformat för smidig integration i befintlig IT-miljö. Systemet är lätt att installera på servrar och kräver minimal konfiguration för att komma igång. Er IT-avdelning kan ha systemet driftsatt inom kort tid.

## Anpassat för upphandling

ERS är utformat för att möta kraven i offentlig och privat upphandling:

- **NIS2-kompatibilitet** – uppfyller kommande EU-krav på cybersäkerhet
- **Revisionsunderlag** – komplett beviskedja för granskning
- **Konfigurerbar policy** – organisationen äger och styr alla tröskelvärden och åtgärder
- **Lokal drift** – ingen data lämnar er kontrollerade miljö

## Sammanfattning

Utmaning	ERS-lösning
Data kan läcka till externa system	All bearbetning sker lokalt
Svårt att bevisa säkerhet	Koda Trust Score med revisionsunderlag
System lär sig på andras data	ERS Memory Vaults – isolerad inlärning
Bristande spårbarhet vid incidenter	ERS som Auditor med beviskedja

## Kontakt

För mer information om ERS och hur det kan anpassas för er organisation, kontakta oss för en demonstration.

### Mats Hamberg

*Grundare och ansvarig VD*

E-post: [info@nordicintegrity.se](mailto:info@nordicintegrity.se)

Telefon: 070-037 74 59

### Nordic Integrity Systems AB

ERS – Enterprise Research Shield

*Insikter utan insyn.*