# Enterprise Research Shield

*Informationsblatt für die Beschaffung*

*"Erkenntnisse ohne Einblick."*

## Warum ERS?

In einer Zeit, in der nahezu jede Organisation fortschrittliche Datenanalyse nutzen möchte, aber gleichzeitig besorgt ist, dass sensible Informationen offengelegt oder außerhalb ihrer Kontrolle verwendet werden, erfüllt ERS einen kritischen Bedarf.

ERS ist ein **Schutzwerkzeug** – nicht nur ein Analysewerkzeug. Es wurde speziell für das Gesundheitswesen, Behörden und andere Organisationen entwickelt, bei denen Vertraulichkeit gesetzlich vorgeschrieben und geschäftskritisch ist.

## Unser Versprechen

ERS gibt Ihnen die Möglichkeit, Ihre sensibelsten Dokumente zu entschlüsseln und zu analysieren – **ohne dass ein einziges Byte Daten Ihre Kontrolle verlässt**. Wir bauen Intelligenz lokal auf mit ERS Memory Vaults, verifiziert durch den Koda Trust Score.

## Drei Schlüsselfunktionen

### 1. ERS Memory Vault – Wissen, das bei Ihnen bleibt

Die Analysekomponenten des Systems entwickeln ihr Verständnis durch dedizierte Speichertresore (ERS Memory Vaults). Alles Lernen erfolgt lokal und isoliert.

- **Das Argument:** "Ihre Daten machen ERS schlauer für Sie, aber niemals für jemand anderen."
- Das System lernt Ihre Krankenaktensprache und Routinen, ohne dass Informationen Ihre digitalen Mauern verlassen.

### 2. Koda Trust Score – Messbare Sicherheit

Der Koda Trust Score funktioniert als kontinuierlicher Gesundheitscheck, nicht als einmaliger Stempel. Er misst die Systemintegrität in Echtzeit und liefert konkrete Nachweise für Ihr Sicherheitsniveau.

| Säule | Was sie misst | Warum es wichtig ist |
|---|---|---|
| **Dateneindämmung** | Keine Datenflüsse außerhalb definierter Zonen | Garantiert, dass sensible Daten dort bleiben, wo sie hingehören |
| **Autorisierung** | Zugriffsmuster und Autorisierungskonformität | Erkennt unbefugten oder anomalen Zugriff |
| **Systemzustand** | Integrität, Patch-Level, Konfigurationsstatus | Stellt sicher, dass das System aktualisiert und unverändert ist |
| **Audit-Trail** | Was, wann, von wem, mit welchem Ergebnis | Bietet Nachverfolgbarkeit und Beweiskette für Audits |

**Wichtig:** Der Score ist der Indikator. Maßnahmen werden durch Richtlinienschwellenwerte gesteuert, die Ihre Organisation konfiguriert. Sie bestimmen die Regeln.

### 3. Entschlüsselung ohne Offenlegung

Viele konkurrierende Lösungen senden Text zur Analyse an externe Cloud-Dienste. ERS arbeitet lokal oder in einer isolierten Umgebung – Sie erhalten die Erkenntnisse, behalten aber die Geheimnisse.

## Trust Badge – Sichtbarer Status

ERS zeigt kontinuierlich den Sicherheitsstatus des Systems über ein Trust Badge an, das sowohl für technisches Personal als auch für das Management verständlich ist:

| | |
|---|---|
| **Letzte Prüfung** | Datum und Uhrzeit |
| **Nächste Prüfung** | Datum und Uhrzeit |
| **Status** | Normal / Erhöht / Gesperrt |
| **Grund** | Eine Zeile ohne technisches Rauschen (bei Warnung) |

***Beispiel:*** *"Score 92/100 – Erhöhte Stufe (neue administrative Anmeldung). Keine Datenflüsse außerhalb der Zone. Maßnahme: Zusätzliche Protokollierung aktiv."*

## Architektur: ERS als Auditor

ERS basiert auf einer Überwachungsarchitektur, bei der eine zentrale Komponente als interner Auditor fungiert. Dies gewährleistet:

- **Kontrolle** – kontinuierliche Überwachung aller Systemaktivitäten
- **Nachverfolgbarkeit** – jedes Ereignis wird mit Zeitstempel und verantwortlicher Komponente protokolliert
- **Compliance** – automatische Verifizierung gegen Ihre Sicherheitsrichtlinien

## Kontrollmethodik

ERS verwendet unternehmensangepasste Kontrollmethoden, die die Auswirkungen auf den Betrieb minimieren:

- **Geplante Prüfungen** – periodische Audits gemäß konfiguriertem Zeitplan
- **Ereignisgesteuerte Kontrolle** – sofortige Verifizierung bei Risikoindikatoren
- **Richtlinien-/Konfigurationsabweichung** – erkennt, ob die Sicherheitskonfiguration seit der letzten genehmigten Baseline geändert wurde
- **Update-Hygiene** – überprüft Patch-Level, Signaturverifizierung und Änderungsprotokoll

## Dateneigentum – Ihre Daten, Ihre Bedingungen

### Sämtlicher Speicher gehört dem Kunden. Punkt.

ERS gibt Ihnen die volle Kontrolle darüber, wie der Systemspeicher verwaltet wird:

- **Zeitbegrenzter Speicher** – konfigurierbare Lebensdauer (z.B. 1 Tag, 1 Woche)
- **Automatische Löschung** – Speicher wird nach Ihren Regeln ohne manuelle Handhabung gelöscht
- **Richtliniengesteuert** – Ihre Organisation entscheidet, was gespeichert wird, wie lange und wann es entfernt wird

*Dies ist eine Stärke, keine Einschränkung* – kurzlebiger Speicher reduziert die Risikoexposition und vereinfacht die DSGVO-Konformität.

## Protokolle in Ihrer Sprache – kein technisches Rauschen

Traditionelle Sicherheitssysteme präsentieren Protokolle in technischen Formaten wie JSON, Stack Traces oder Hexadezimalcode – unverständlich für alle außer Spezialisten.

**ERS übersetzt alles in natürliche Sprache.**

| Techniker sieht | ERS-Benutzer sieht |
|---|---|
| `Error: 503 Service Unavailable / timeout 3000ms` | "Das System konnte die Datenbank nicht erreichen, es dauerte zu lange. Erneuter Versuch." |
| `Access_Denied_Vault_7 / severity: WARNING` | "Jemand hat versucht, einen geschützten Ordner |

| Techniker sieht | ERS-Benutzer sieht |
|---|---|
| | ohne Berechtigung zu öffnen. Das Ereignis wurde protokolliert." |

**Verfügbar auf Schwedisch, Englisch und Deutsch** – alle Protokolle, Warnungen und Berichte werden in Ihrer gewählten Sprache angezeigt.

**Der Vorteil:** Manager und Entscheidungsträger können den Sicherheitsstatus direkt im Dashboard verstehen, ohne IT-Experten sein zu müssen. Es ist Demokratisierung von Daten.

### Selbstheilendes System – ERS behebt Probleme automatisch

ERS überwacht kontinuierlich den Systemzustand und kann häufige Betriebsprobleme automatisch beheben – ohne manuellen Eingriff. Alle Ereignisse werden in Ihrer Sprache protokolliert, sodass Sie immer verstehen, was passiert ist.

#### Beispielbenachrichtigung von ERS:

> **Hinweis: Betriebsstatus (Verlauf)**
> Zeit: 14:35 | Stufe: Gelb (Warnung)
> *"Die Datenbank ist vorübergehend überlastet."*
> **Analyse:** Ein plötzlicher Anstieg eingehender Daten wurde erkannt.
> **Sicherheit:** Keine Daten sind ausgetreten. Der Koda Trust Score ist nicht betroffen.
> **Maßnahme:** Ich habe die Datenbankkapazität vorübergehend erweitert, um die Last zu bewältigen.
> **Aktueller Status:** Das System funktioniert normal und keine Benutzer waren betroffen.
> *– Ihr ERS*

**Das Ergebnis:** Weniger Support-Tickets, schnellere Wiederherstellung und volle Transparenz – in Ihrer eigenen Sprache.

## Installation

Die Installation erfolgt lokal in Ihrer Umgebung und kann vom Anbieter in Zusammenarbeit mit Ihrer IT-Abteilung remote durchgeführt werden.

**Der Anbieter hat keinen Zugriff auf Kundendaten oder Analyseinhalte.** Service und Support basieren ausschließlich auf Systemstatus, Betriebsindikatoren und Sicherheitsmetriken.

## Updates ohne Einblick – Volle Kontrolle bei Ihnen

ERS wird über kryptografisch signierte Systempakete aktualisiert, die lokal in Ihrer Umgebung installiert werden. Updates beeinflussen niemals Dokumente, Analyseinhalte oder ERS-Speicher. Alle Updates erfolgen unter Kundenkontrolle – Sie genehmigen jeden Schritt und behalten immer die Entscheidung.

**In der Praxis bedeutet dies:**

- Keine Remote-Anmeldungen in der Kundenumgebung
- Kein Zugriff auf Daten, Speicher oder Protokolle
- Automatische Verifizierung nach dem Update
- Sicheres Rollback bei Abweichung
- Vollständige lokale Nachverfolgbarkeit für Audits

**Prinzip:** *"Wir aktualisieren das System – nicht Ihre Informationen."*

## Integration mit bestehendem Virenschutz

ERS überwacht kontinuierlich Ihr internes Netzwerk und erkennt sofort, wenn Schadsoftware versucht einzudringen. Das System arbeitet nahtlos mit Ihren bestehenden Antivirenlösungen zusammen.

**So funktioniert es:**

- **Früherkennung** – ERS identifiziert anomales Verhalten im Netzwerkverkehr, bevor es zum Problem wird
- **Koordinierte Reaktion** – bei erkannten Bedrohungen wird Ihr bestehendes Antivirenprogramm automatisch aktiviert
- **Backup-Maßnahme** – wenn das Antivirenprogramm nicht reagiert, behandelt ERS die Bedrohung selbst
- **Ergänzender Schutz** – ERS ersetzt nicht Ihr Antivirenprogramm, es verstärkt es

## Einfache Serverinstallation

ERS ist für eine reibungslose Integration in bestehende IT-Umgebungen konzipiert. Das System ist einfach auf Servern zu installieren und erfordert minimale Konfiguration für den Start. Ihre IT-Abteilung kann das System in kurzer Zeit in Betrieb nehmen.

## Konzipiert für die Beschaffung

ERS ist darauf ausgelegt, die Anforderungen öffentlicher und privater Beschaffung zu erfüllen:

- **NIS2-Kompatibilität** – erfüllt kommende EU-Cybersicherheitsanforderungen
- **Audit-Dokumentation** – vollständige Beweiskette für Audits
- **Konfigurierbare Richtlinie** – die Organisation besitzt und kontrolliert alle Schwellenwerte und Maßnahmen
- **Lokaler Betrieb** – keine Daten verlassen Ihre kontrollierte Umgebung

## Zusammenfassung

| Herausforderung | ERS-Lösung |
|---|---|
| Daten können zu externen Systemen gelangen | Alle Verarbeitung erfolgt lokal |
| Schwierig, Sicherheit nachzuweisen | Koda Trust Score mit Audit-Trail |
| Systeme lernen aus Daten anderer | ERS Memory Vaults – isoliertes Lernen |
| Mangelnde Nachverfolgbarkeit bei Vorfällen | ERS als Auditor mit Beweiskette |

## Kontakt

Für weitere Informationen über ERS und wie es für Ihre Organisation angepasst werden kann, kontaktieren Sie uns für eine Demonstration.

**Mats Hamberg**
*Gründer und Geschäftsführer*

E-Mail: info@nordicintegrity.se
Telefon: +46 70-037 74 59

**Nordic Integrity Systems AB**
ERS – Enterprise Research Shield
*Erkenntnisse ohne Einblick.*