E-MAIL-RISIKEN STOPPEN, BEVOR SIE ENTSTEHEN

KI-GESTÜTZTE PRÄVENTION DIREKT IM E-MAIL-WORKFLOW.

Für IT-Entscheider und Security-Verantwortliche, die menschliche Fehler reduzieren, BEC-Risiken minimieren und Compliance sicherer steuern wollen.

KOMMT IHNEN DAS BEKANNT VOR?

Die größten E-Mail-Risiken sind selten offensichtlich: Sensible Daten landen beim falschen Empfänger. Klassische DLP-Lösungen greifen oft zu spät oder zu ungenau. Gleichzeitig kommen Angriffe wie BEC oder CEO-Fraud über scheinbar legitime Absender und bleiben dadurch lange unbemerkt.

DIE LÖSUNG: RAPTOR AI VON RPOST

RaptorAI ist die fehlende Intelligenzschicht Ihrer E-Mail-Security. Es analysiert Kontext, Verhalten und Beziehungen direkt im Workflow und orchestriert bei Bedarf sofort die passende Schutzmaßnahme.

MAXIMALE AKZEPTANZ & COMPLIANCE

Die nahtlose Integration im E-Mail-Client vermeidet Medienbrüche und Portalzwänge und unterstützt Nutzerakzeptanz und Compliance im Alltag.

PRÄVENTION DURCH AGENTIC AI

Als proaktiver Sicherheits-Agent verhindert RaptorAI Datenlecks und Identitäts- missbrauch direkt am Point of Decision, bevor eine kritische E-Mail versendet wird.

KONTROLLE ÜBER EIGENE GRENZEN HINAUS

Der globale Schutzhorizont erkennt Risiken auch auf Empfängerseite, etwa kompromittierte externe Konten, und erlaubt den weltweiten Entzug von Dokumentenzugriffen per Klick.

WARUM KLASSISCHE SECURITY NICHT REICHT

	KLASSISCHE SECURITY / GATEWAY	MIT RAPTOR AI
Zeitpunkt	Prüft reaktiv nach dem Versand	**Präventiv:** Echtzeit-Check im Entwurf
Datenbasis	Fokus auf Signaturen & Blacklists	**Multimodal:** Analyse von Text, IPs & Metadaten
Identität	Erkennt Absendermissbrauch kaum	**Behavioral AI:** Enttarnt Anomalien & CEO-Fraud
Fehlversand	Übersieht Fehladressierungen meist	**Context-Check:** Abgleich von Empfänger & Inhalt
Steuerung	Blockiert starr oder lässt durch	**Orchestrator:** Schlägt RMail/RSign-Schutz vor

SO FUNKTIONIERT ES

ANALYSE

RaptorAI analysiert jeden E-Mail-Entwurf vor dem Versand – semantisch und multimodal (Inhalt, Empfänger, Verhalten).

WARNUNG

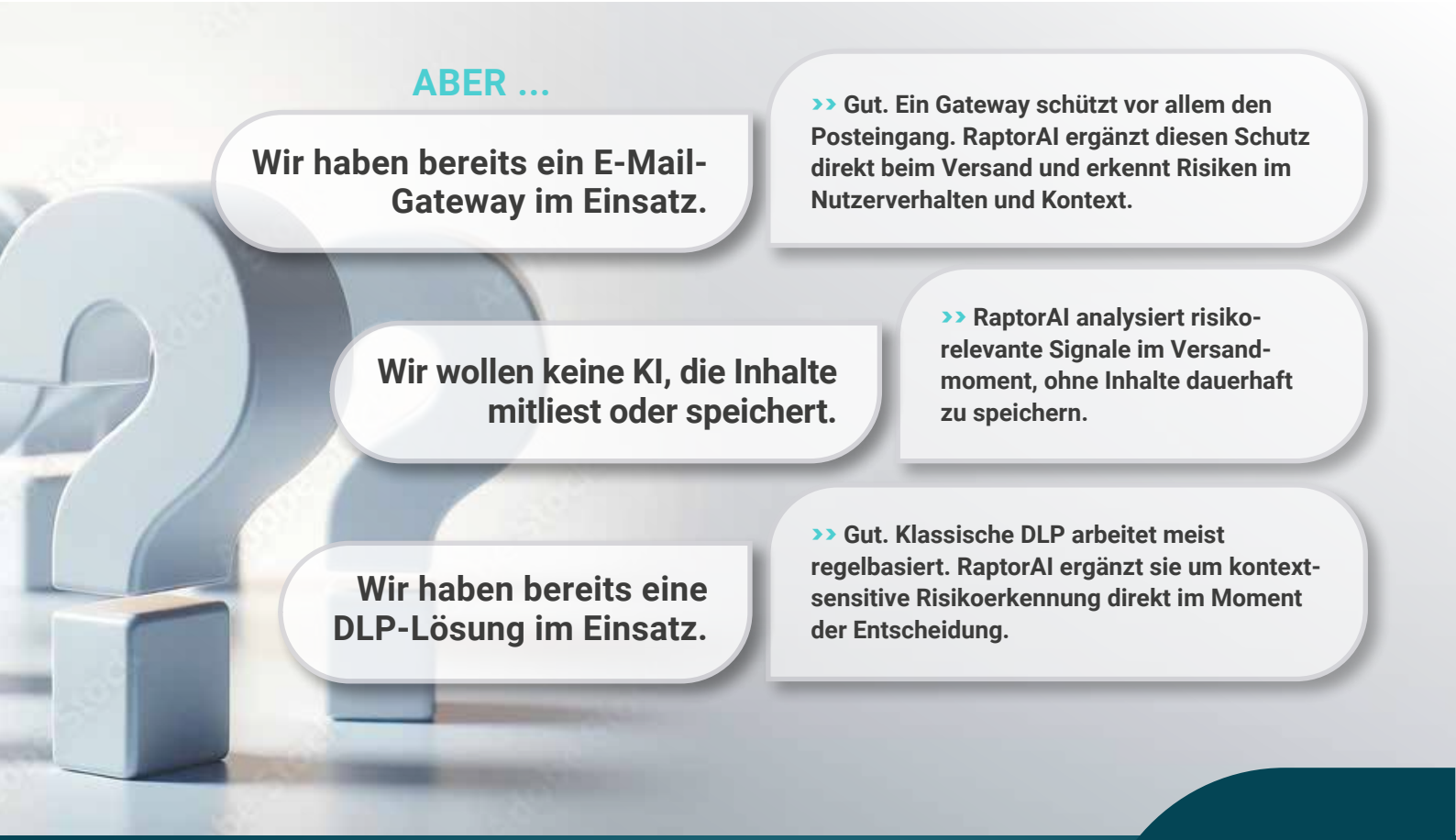
Bei Anomalien (z. B. untypischer Standort oder falsche Empfängerrolle) erscheint eine Warnung direkt im E-Mail-Client.

ENTSCHEIDUNG

Der Nutzer entscheidet: Senden, korrigieren oder blockieren. Die KI unterstützt den Menschen, statt ihn durch starre Automatismen zu bevormunden.

STEUERUNG

Die KI erkennt sensible Inhalte und schlägt direkt die passende Folgemaßnahme vor; etwa eine RMail-Verschlüsselung oder eine RSign-Signatur.



ABER ...

Wir haben bereits ein E-Mail-Gateway im Einsatz.

›› **Gut. Ein Gateway schützt vor allem den Posteingang. RaptorAI ergänzt diesen Schutz direkt beim Versand und erkennt Risiken im Nutzerverhalten und Kontext.**

Wir wollen keine KI, die Inhalte mitliest oder speichert.

›› **RaptorAI analysiert risikorelevante Signale im Versandmoment, ohne Inhalte dauerhaft zu speichern.**

Wir haben bereits eine DLP-Lösung im Einsatz.

›› **Gut. Klassische DLP arbeitet meist regelbasiert. RaptorAI ergänzt sie um kontextsensitive Risikoerkennung direkt im Moment der Entscheidung.**

WARUM USER 2000?

Die USER 2000 AG ist IT-Dienstleister aus Ratingen mit über 30 Jahren Erfahrung in den Bereichen Managed Services, Cybersecurity und Cloud. **Als exklusiver RPost-Distributor für den DACH-Raum** bietet USER 2000 direkten Herstellerzugang, Beratung, Support und Umsetzung aus einer Hand.

Wir zeigen Ihnen gerne, wie RaptorAI Ihren bestehenden Schutz sinnvoll ergänzt, inklusive passender Lizenzempfehlung.

www.user2000.de | info@user2000.de | +49 2102 1237720