SOLUTION BRIEF

Email Encryption

Protect Sensitive Information, Prevent Data Leaks, and Stay Compliant

Sensitive data leaves organizations through email every day, often by accident, often without anyone noticing until it becomes a compliance event. IRONSCALES Email Encryption closes that gap by extending the IRONSCALES platform from inbound threat defense to outbound data protection, automatically encrypting messages and attachments when sensitive content is detected. Policy-driven enforcement replaces reliance on user behavior, while a frictionless recipient experience keeps external collaboration simple.

How it Works:

IRONSCALES email encryption offers two deployment paths to match your security posture:

Elective Encryption — Sender-initiated encryption via Outlook add-in or a [secure] keyword in the subject line, for ad hoc sensitive communications.

Policy-Based Encryption — Configurable content policies that detect sensitive data patterns in message bodies, attachments, and recipient fields. Policies are defined using keyword lists, regex patterns, and data identifiers tied to your regulatory requirements.

Recipients access encrypted messages through a secure portal using one-time passcode authentication. No account creation. No software to install. Forwarding is restricted; secure reply and reply-all are supported. This is a meaningfully simpler recipient experience than market alternatives who require portal accounts.

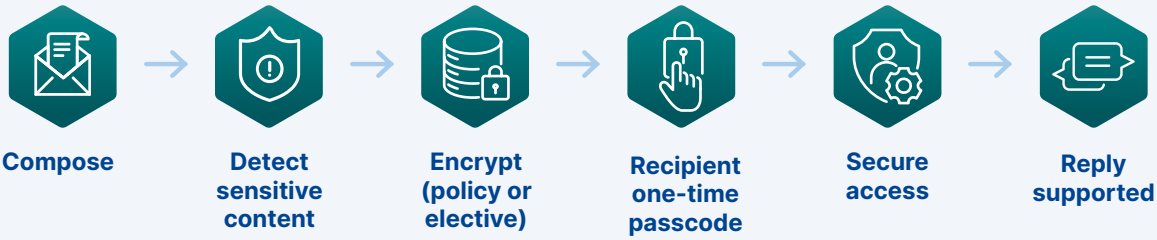
The Compliance Gap:

Organizations handling PHI, PCI, financial records, or student data face overlapping mandates from HIPAA, GDPR, PCI DSS, SEC, FERPA, and NAIC, each carrying enforcement mechanisms that go well beyond fines. Breach costs include incident response, legal exposure, customer attrition, and cyber insurance repricing. And the majority of these exposures trace back to outbound email: a misaddressed message, a reply-all with an attachment, or sensitive data sent in plaintext because nobody remembered to encrypt it.

Why Outbound Security Can't Wait:

- The "human element" was involved in roughly 60% of breaches. (Verizon DBIR 2025)
- Third-party involvement in breaches doubled, increasing from 15% to 30%. (Verizon DBIR 2025)
- Breaches caused by **insider error** still took **213 days** on average (IBM, Cost of a Data Breach 2025)
- Average cost per record for **customer PII** was **USD $160/record** (IBM, Cost of a Data Breach 2025)

How IRONSCALES Does Encryption



What You Get:

- **Policy-Driven Encryption:** Automatically encrypts outbound emails and attachments when sensitive data patterns are detected in the message body, recipient, or attachment. Protection is applied consistently at the point of send, reducing accidental disclosure from misaddressed emails, reply-all mistakes, and unencrypted attachments.
- **Flexible Sender Controls:** Senders can initiate encryption on demand via Outlook add-in or subject-line keyword for ad hoc workflows. Combined with policy-based triggers, this gives teams both automation and flexibility without requiring separate tools or training.
- **Frictionless Recipient Access:** Recipients open encrypted messages through a secure portal using one-time passcode authentication. No account creation, no software install, no friction. Forwarding is restricted while secure reply and reply-all remain available, keeping external collaboration functional without compromising control.
- **Compliance-Ready Enforcement**: Establishes consistent, auditable outbound controls aligned with HIPAA, GDPR, PCI DSS, and other regulatory frameworks. Repeatable policy enforcement makes it easier to demonstrate compliance during audits and reduces reliance on individual user behavior.
- **Multi-Tenant Scale for MSPs and Enterprises:** Centralized policy management, reusable templates for regulated industries, and standardized rollout across users or tenants. Reduces support tickets, simplifies onboarding, and creates a new compliance-driven service tier for MSP partners.

One Platform. Inbound and Outbound:

IRONSCALES is the only cloud email security platform that combines adaptive AI-powered inbound threat detection (BEC, ATO, phishing), security awareness training, DMARC management, and now outbound email encryption in a single console. No MX record changes. No separate vendor for encryption. For MSPs, that means centralized policy management across tenants and a new compliance-driven revenue stream without adding operational overhead.

About IRONSCALES

We are the leader in AI-powered email security protecting over 17,000 global organizations from advanced phishing threats. As the pioneer of adaptive AI, we detect and remediate attacks like business email compromise (BEC), account takeovers (ATO), and deepfake attacks that other solutions miss. By combining the power of AI and continuous human insights, we safeguard inboxes, unburden IT teams, and turn employees into a vital part of cyber defense across enterprises and managed service providers. IRONSCALES is headquartered in Atlanta, Georgia.