

# HaystackID®

## Faster Finds, Fewer Files

### A Smarter Approach to Email Investigations

Educational Webcast

05 | 21 | 2025

HAYSTACK®

# HaystackID Overview



**HaystackID** solves complex data challenges related to legal, compliance, regulatory, and cyber requirements. Core offerings include **Global Advisory**, **Cybersecurity**, **Core Intelligence AI™**, and **ReviewRight® Global Managed Review**, supported by its unified **CoreFlex™** service interface.

Recognized globally by industry leaders, including **Chambers**, **Gartner**, **IDC**, and **Legaltech News**, HaystackID helps corporations and legal practices manage data gravity, where information demands action, and workflow gravity, where critical requirements demand coordinated expertise, delivering innovative solutions with a continual focus on security, privacy, and integrity.

# Rene Novoa

## *Vice President of Forensics* *HaystackID*



As Vice President of Forensics for HaystackID, **Rene Novoa** has more than 20 years of technology experience conducting data recovery, digital forensics, eDiscovery, and account management and sales activities. During this time, Rene has performed investigations in both civil and criminal matters and has directly provided litigation support and forensic analysis for seven years. Rene has regularly worked with ICAC, HTCIA IACIS, and other regional task forces supporting State Law Enforcement Division accounts and users in his most recent forensic leadership roles.

# John Wilson

## *CISO and President of Forensics HaystackID*



As Chief Information Security Officer and President of Forensics at HaystackID, **John Wilson** provides consulting and forensic services to help companies address various matters related to electronic discovery and computer forensics, including leading forensic investigations, cryptocurrency investigations, and ensuring proper preservation of evidence items and chain of custody. He regularly develops forensic workflows and processes for clients ranging from major financial institutions to governmental departments, including Fortune 500 companies and Am Law 100 law firms.



# Agenda



1. The Enduring Role of Email in Investigations
2. Shifting Away from Legacy Methods
3. Precision Over Volume
4. Real-World Lessons in Email Forensics
5. Optimizing Your Workflow for the Future
6. Questions?

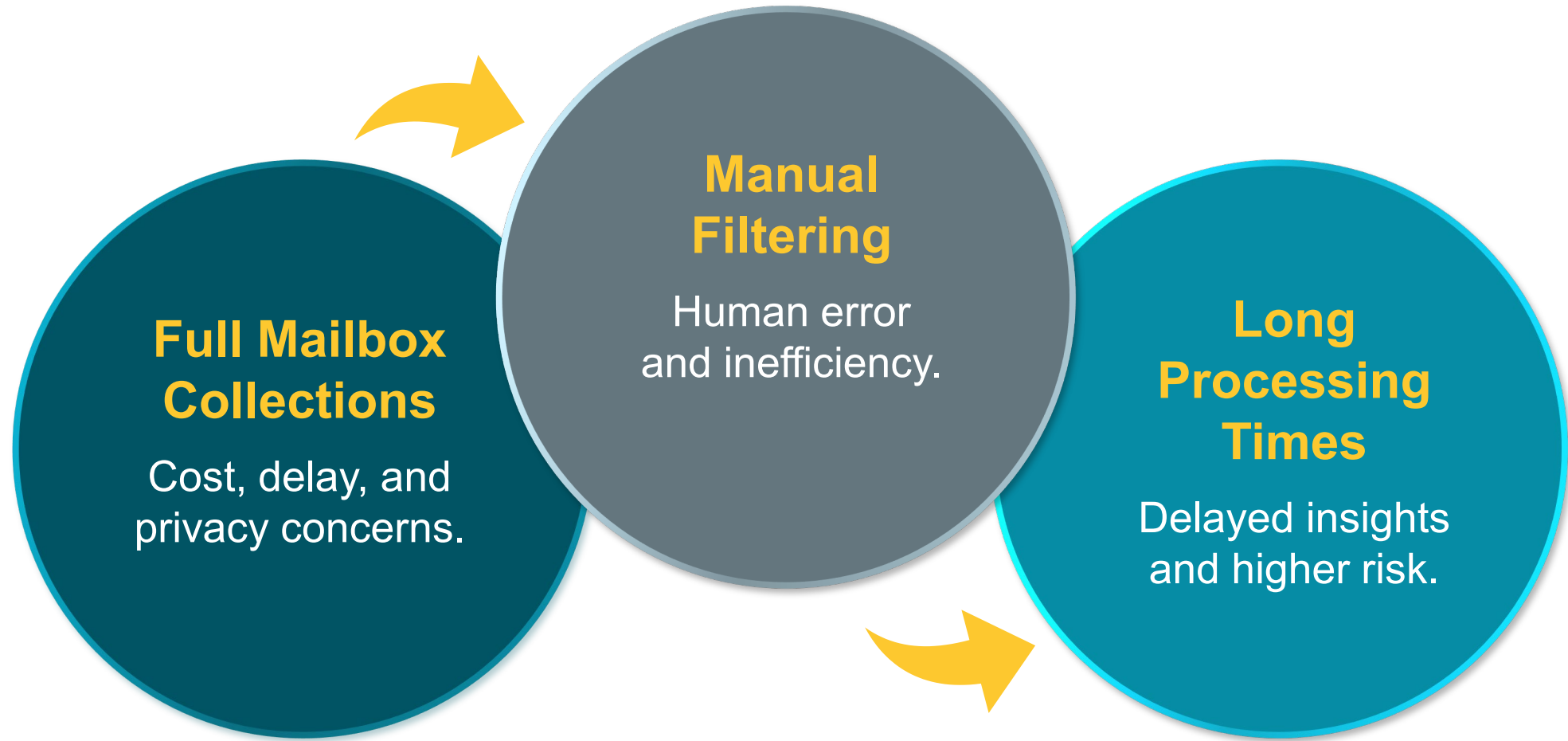
# Why Email Still Reigns Supreme in Investigations

Central to communication, evidence, and compliance trails.

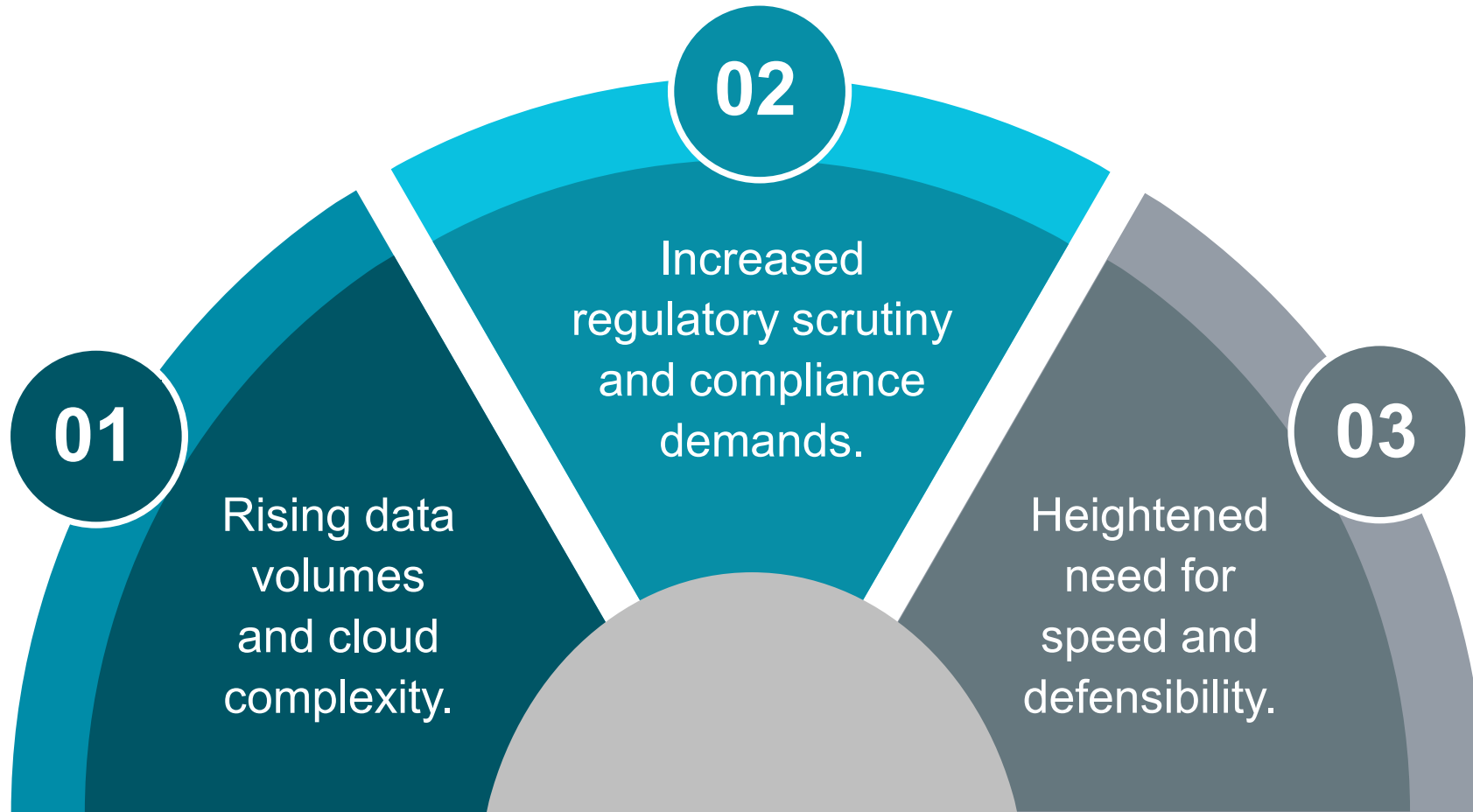
Essential in cybersecurity, eDiscovery, and regulatory response.

High potential for valuable insights, but also noise and risk.

# Legacy Methods Are No Longer Sustainable



# Modern Pressures on Legal and Forensic Teams





# Confronting the Rising Risk of Business Email Compromise (BEC)

**BEC involves unauthorized access or impersonation using email accounts.**

- **Common Tactics:** Phishing, credential theft, executive impersonation.
- **Most Damaging Form:** Account Takeover (ATO).
- **Extent of Threat:** Beyond email to HR records, intranet, and other business assets.
- **Red Flags:** Requests for sensitive information, urgent financial transactions.
- **Example:** Vendor Email Compromise (VEC) through subtle domain manipulation.



# Stay Alert!

## Email Spoofing

Fraudsters mimic legitimate email addresses with minor changes (e.g., Joe.Smith@examplecompany.com vs. Joe.smithy@examplecompany.com) to trick recipients into trusting the source.

## Spear Phishing

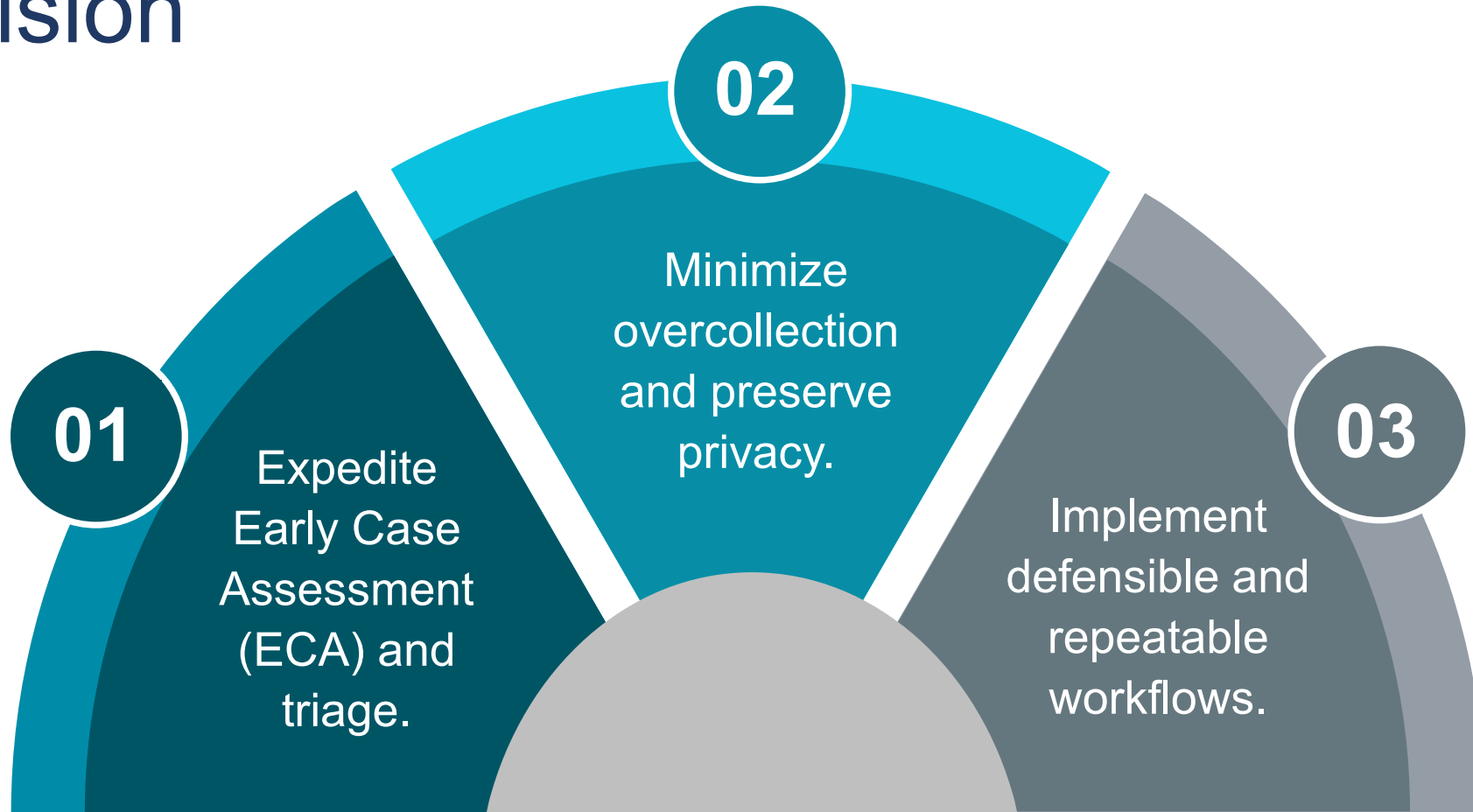
Targeted emails appear to come from known contacts, luring recipients into revealing credentials or sensitive data, granting criminals access to internal accounts, calendars, and confidential communications.

## Malware Deployment

Malicious software is used to infiltrate systems, monitor email conversations, and intercept invoice or billing details, helping criminals send perfectly timed, believable requests. Malware also steals login credentials and financial data, often undetected.



# Moving From Broad Collection to Surgical Precision



# Targeted, Tech-Enabled Email Forensics

Use of analytics and automation to isolate key communications.

Insight-driven methodologies for identifying risk indicators.

Cross-functional collaboration to streamline workflows.

# Lessons From the Field

## Insider Threat Investigation

Rapid evidence collection from email threads.

## System Misconfiguration

Timeline reconstruction through email metadata.



## BEC Detection

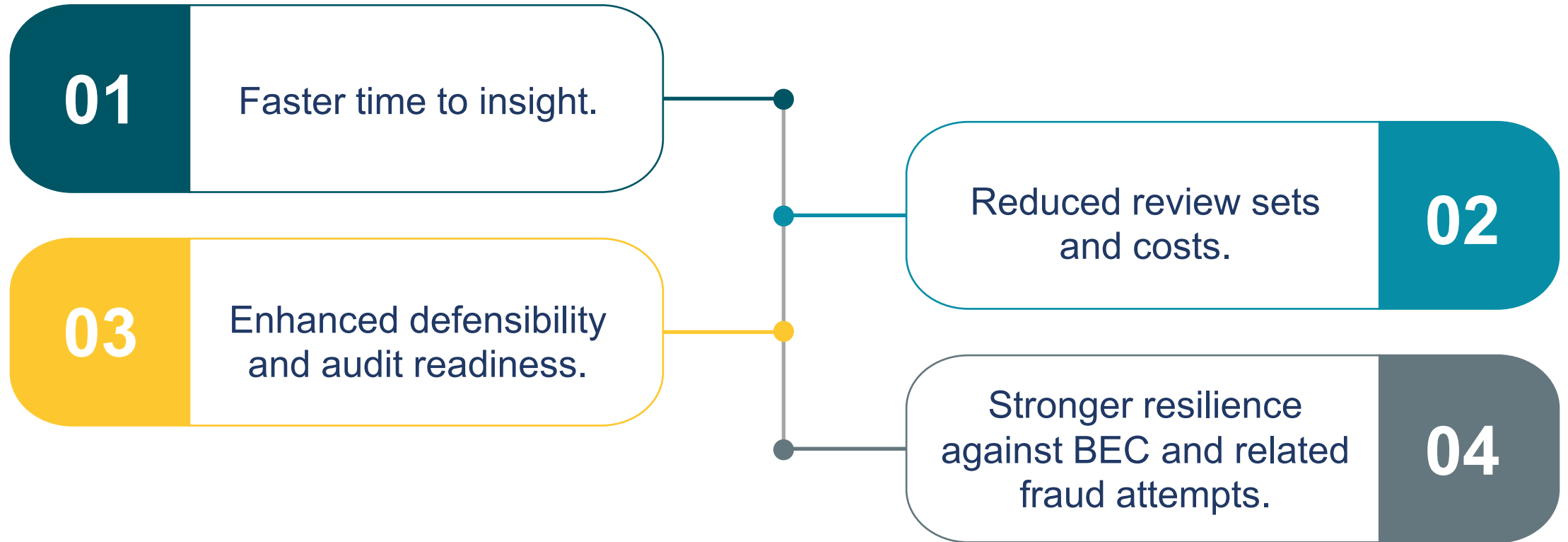
Identified impersonation via domain spoofing and header anomalies.

## Regulatory Audit

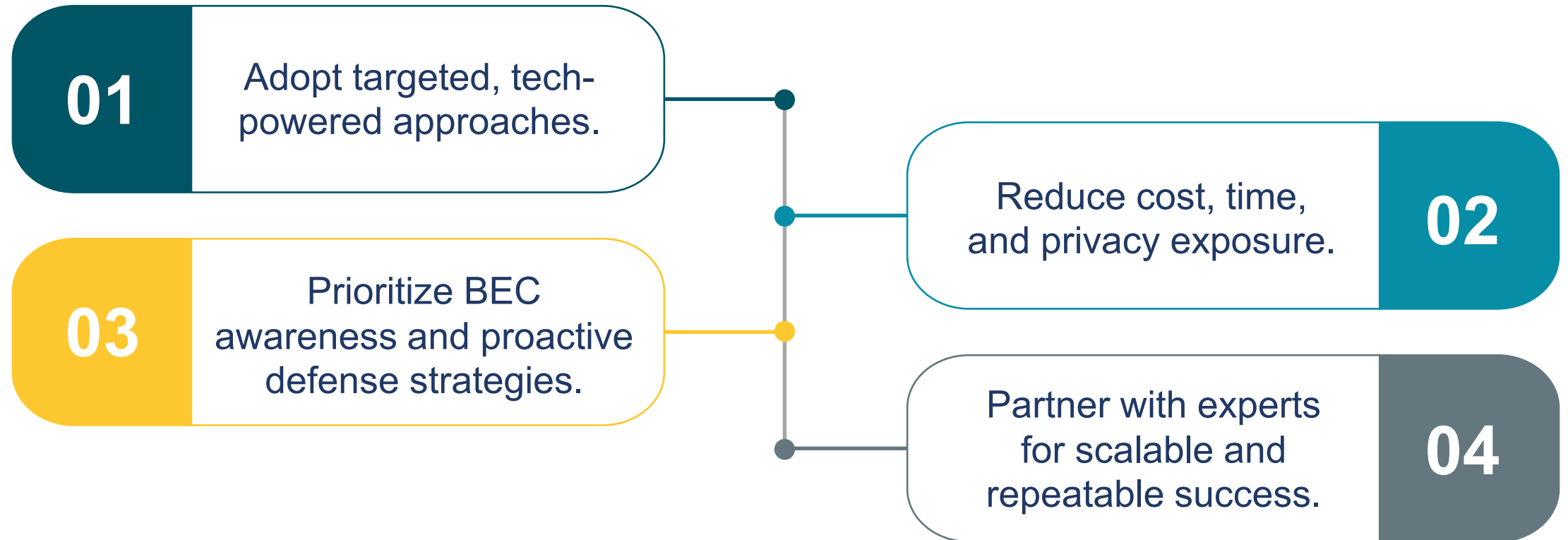
Precision search and defensible export in hours, not days.



# Outcomes from Smarter Email Tactics



# Transforming Your Email Investigation Workflow



# Let's Talk



**What challenges are you seeing in your email investigations today?**

# Questions?

Learn how we can help you at [HaystackID.com](https://HaystackID.com)  
or reach out to us at [Info@HaystackID.com](mailto:Info@HaystackID.com) / 800.267.9695



HAYSTACK<sup>®</sup>