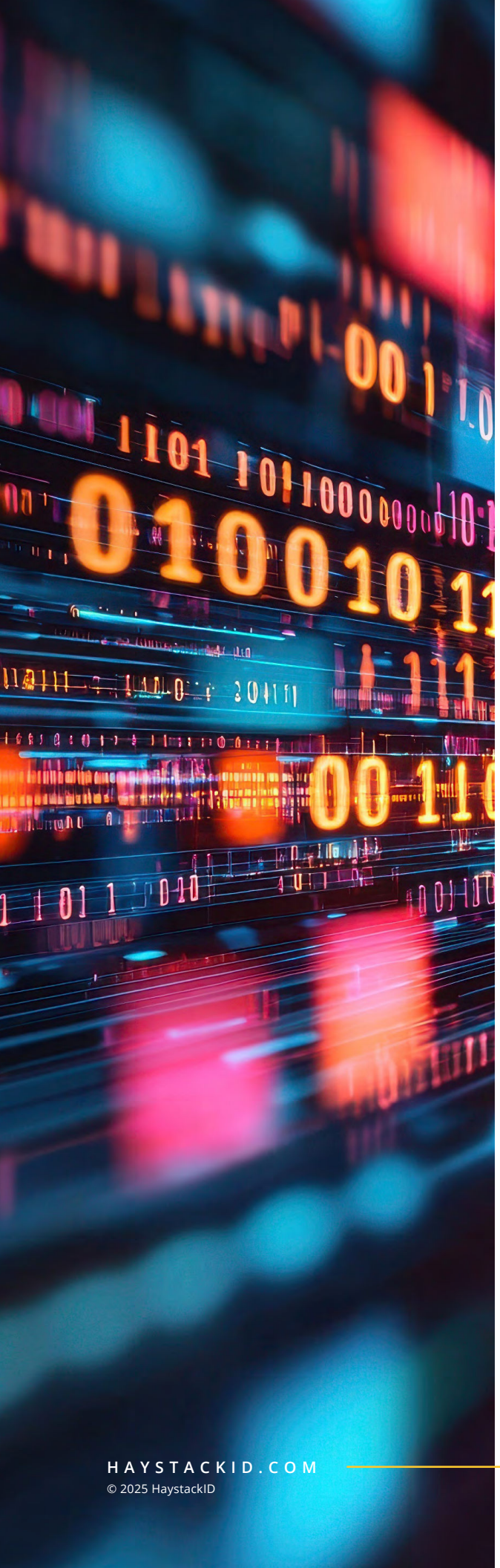
FACT SHEET

HaystackID® Remote Endpoint Analysis and Data Intelligence (READI™) Suite of Services

A Comprehensive Solution for Remote Digital Investigations

HAYSTACK®

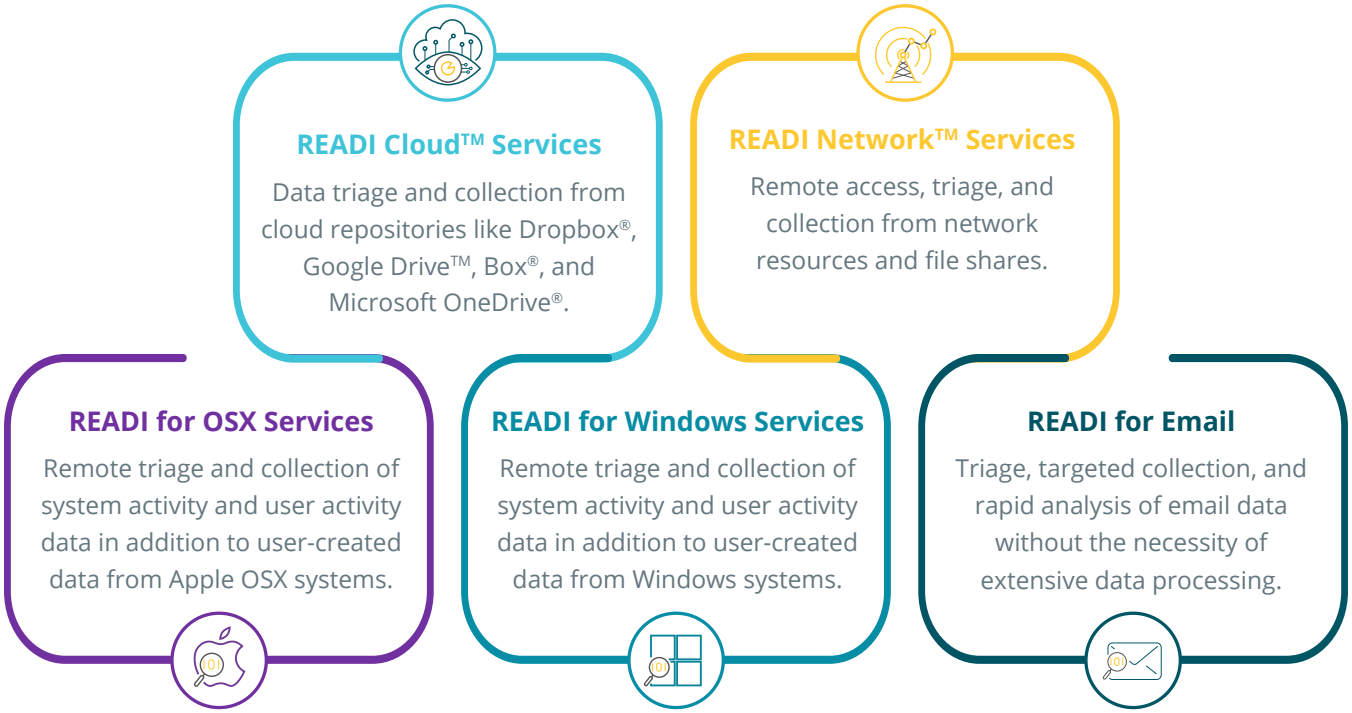


A Comprehensive Solution for Remote Digital Investigations

The **READI Suite of Services**, a critical component of HaystackID's **Forensics First** offerings, is designed to address the increasing complexity of remote digital investigations. By offering specialized solutions that enable data triage and extraction across diverse environments—including cloud services, network environments, Apple macOS® (OSX), Microsoft Windows® (Windows) systems, and selected email platforms—this suite provides essential tools for cybersecurity, information governance, and eDiscovery professionals. Whether it is the identification of critical forensic evidence or the secure handling of sensitive information, the READI Suite delivers both speed and precision in handling forensic investigations, all **without the need for physical access to the target devices**.

READI Suite Overview

The READI Suite of Services is designed to provide clients with the ability to **remotely collect, triage, and analyze data from various environments**. The suite includes solutions for **cloud services, network environments, OSX systems, Windows systems, and selected email platforms**, providing comprehensive coverage for remote forensic investigations. Key solutions in the READI suite include:



Key Benefits of the READI Suite

The READI Suite is designed to **streamline digital forensic investigations by providing a remote and efficient way to collect and triage data**. For professionals working in cybersecurity, information governance, and eDiscovery, the benefits of using the READI Suite are significant.

Key Benefits Include:

READI Solution Breakdown

READI Cloud Services

READI Cloud Services are designed for triaging, collecting, and analyzing data stored in cloud platforms. The service enables clients to remotely triage and extract data from repositories such as Dropbox, Google Drive, Box, and Microsoft OneDrive. By offering credential-based access, two-factor authentication, and self-service extraction, the service allows for seamless collection without disrupting business operations.

Key Features of READI Cloud Services Include:

- Supports multiple cloud platforms.
- Provides credential-based and two-factor authentication access.
- Offers self-service extraction with chain of custody documentation.
- Examiner-led guided extraction for complex cases.

READI Cloud Services Requirements

- Credential-based access to cloud platforms (Dropbox, Google Drive, Box, Microsoft OneDrive).
- Two-factor authentication access for cloud accounts.
- Self-service extraction and examiner-led guided extraction options.

READI Network Services

READI Network Services allow remote access to corporate network resources and file shares, enabling clients to collect and preserve data without needing physical access. This service is crucial for quickly accessing data across enterprise networks during internal investigations or regulatory inquiries.

Key Features of READI Network Services Include:

- Remote access to network resources and file shares.
- Secure data collection without disrupting business operations.
- Continuous monitoring and rapid startup process.
- Targeted preservation of key data sources.

READI Network Services Requirements

- Remote access to network resources and file shares.
- No need to ship physical equipment for data collection.
- Secure network connectivity to ensure quick and effective extraction and analysis.
- Requires administrator or unrestricted access credentials with read-only permissions.

READI for OSX

READI for OSX provides specialized capabilities for remote forensic analysis of Apple OSX systems. Whether through covert or overt installations, forensic professionals can extract key system and user data remotely. This solution is essential for investigations in environments where Macs are widely used.

Key Features of READI for OSX Include:

- Covert and non-covert installation options.
- Remote extraction of email, user activity logs, and system data.
- Focus on user-generated content, minimizing noise from system files.
- Continuous monitoring for on-demand data collection.

READI for OSX Requirements

- Quick installation of remote agents (overt and covert options available).
- Support for custodian profile extraction, email collection, and system activity log extraction.
- Full disk permissions are required to perform the triage and collection processes.
- Admin privileges are required to install the agent.

READI for Windows

READI for Windows is designed to facilitate remote forensic investigations on Windows-based systems. This service includes the remote installation of agents, registry analysis, and the extraction of system and user activity logs, ensuring that investigators can access critical data without the need for physical access.

Key Features of READI for Windows Include:

- Covert and overt agent installations.
- Extraction of user directories, system activity logs, and emails.
- Remote registry analysis for deeper forensic insights.
- Continuous monitoring and real-time data collection.

READI for Windows Requirements

- Quick installation of agents for remote access.
- Requires support for registry analysis and user activity extraction.
- Ability to extract system activity logs, user directories, and emails from remote devices.
- Local admin privileges are required to install the agent and perform the processes.

READI for Email

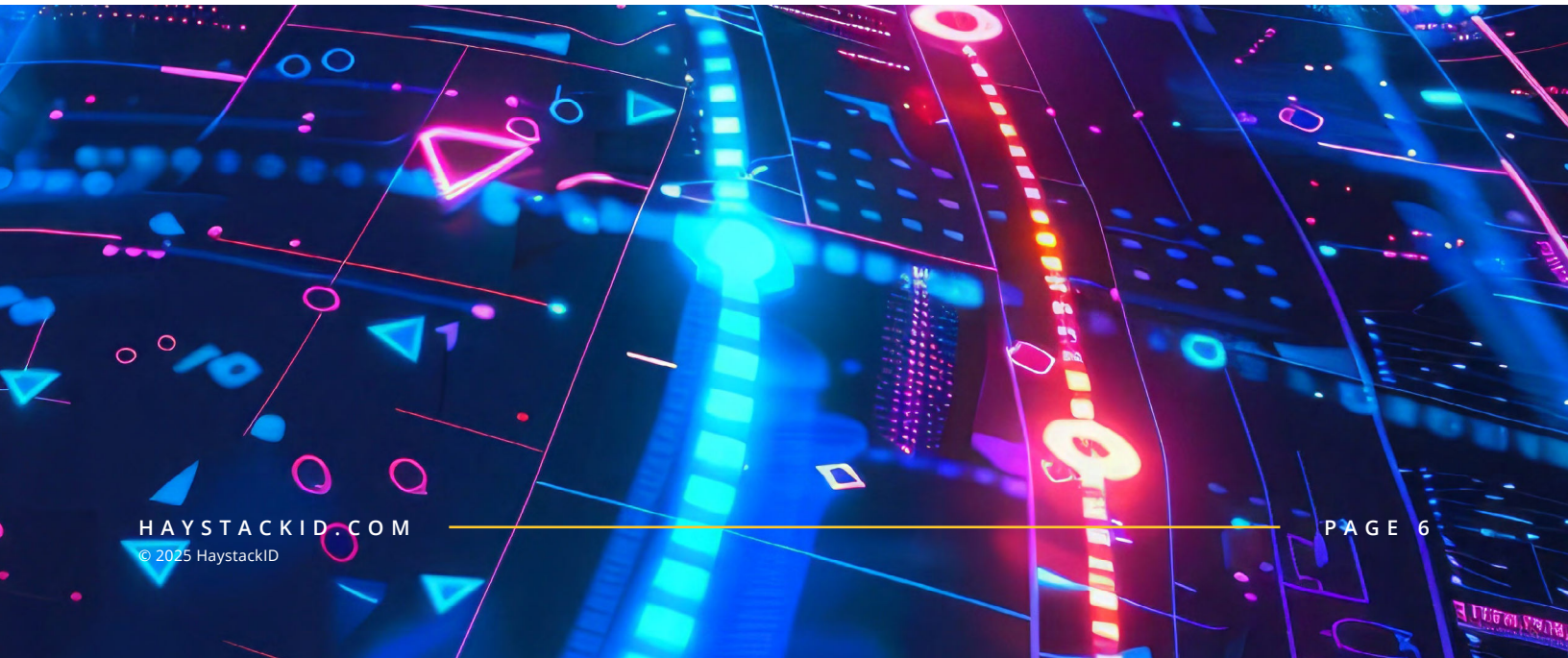
READI for Email is designed for efficient triage, targeted collection, and rapid analysis of email data without the necessity of extensive data processing. It enables forensic, eDiscovery, cybersecurity, and compliance professionals to swiftly identify relevant email artifacts and insights directly from platforms such as Google Workspace and Microsoft Office 365, significantly reducing both the cost and complexity associated with traditional email investigations.

Key Features of READI for Email:

- **Multi-Platform Support:** Provides comprehensive support for Microsoft Office 365 and Google Workspace, with planned expansions to additional cloud platforms.
- **Collection Capabilities:** Enables rapid metadata extraction, including sender, recipient, subject, timestamps, and IP logs, along with the collection of user access logs and detailed administrative action records.
- **Core Features:** Delivers immediate evidence preview and analysis capabilities, optimized workflows designed for rapid identification of critical evidence, and enhanced tools tailored specifically for incident response and regulatory compliance audits.
- **Security Features:** Ensures secure investigations through encrypted communication protocols, secure token-based authentication, granular authorization controls, and comprehensive audit logging to maintain strict compliance and data protection standards.

READI for Email Requirements

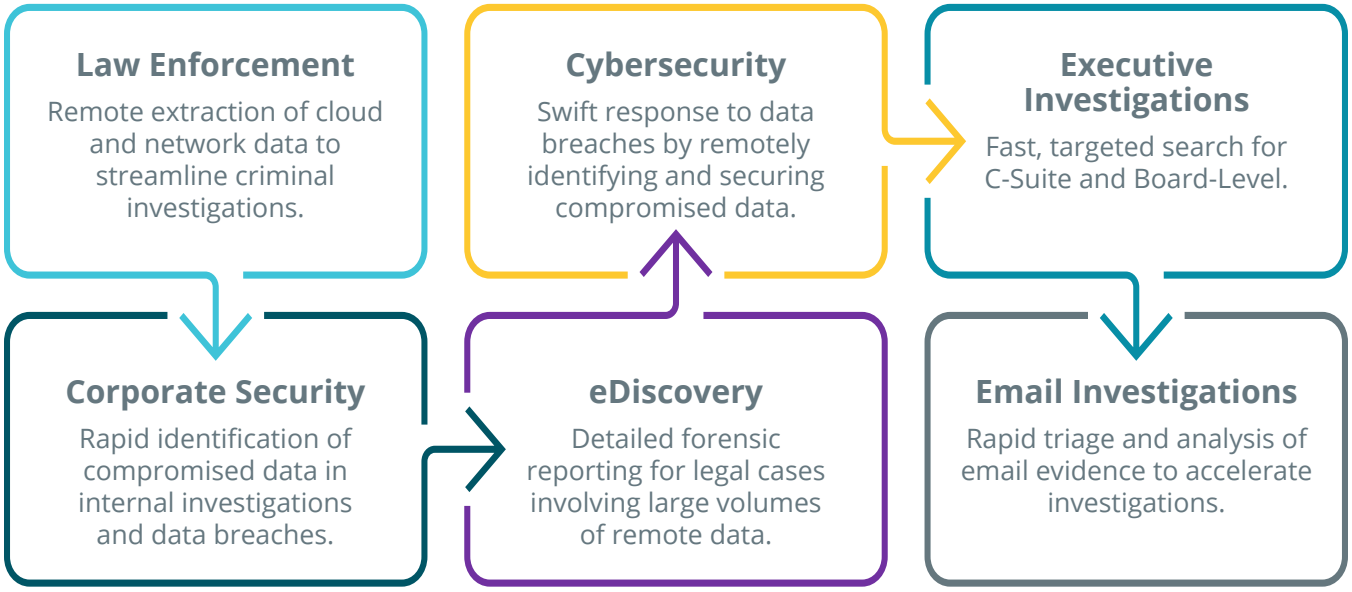
- Credential-based access is required for the supported email platforms, specifically Google Workspace and Microsoft Office 365.
- Secure token-based authentication must be implemented to ensure authorized access.
- The service offers both self-service triage and expert-guided collection options to accommodate varying investigation needs.



Use Cases

The READI Suite of Services is essential in a wide range of industries and scenarios. Whether for corporate investigations, law enforcement, or cybersecurity incident response, the suite **provides the tools necessary to efficiently handle remote data collection and analysis**.

Common Use Cases for the READI Suite Include:



Use Cases Examples

Law Enforcement: Remote Extraction of Cloud and Network Data to Streamline Criminal Investigations

Law enforcement agencies often deal with large amounts of digital data stored in various locations, such as cloud repositories, network file shares, and user devices. Collecting this data can be both time-consuming and logistically difficult, especially when dealing with remote or encrypted data sources. **The READI Suite simplifies this process by allowing investigators to remotely access, triage, and extract critical data from cloud and network environments without physical access to the devices.**

Real-World Scenario: In cases involving cybercrime, fraud, or terrorism, law enforcement agencies can use the READI Cloud and Network Services to quickly retrieve email records, file transactions, and communication logs stored in cloud systems like Dropbox or corporate networks. This allows them to act rapidly, preventing potential evidence from being altered or deleted.

Why It Matters: Time-sensitive investigations demand fast, secure data collection from distributed environments. The READI Suite empowers clients to streamline their digital evidence gathering, ensuring they can access and preserve critical evidence before it becomes inaccessible.

Corporate Security: Rapid Identification of Compromised Data in Internal Investigations and Data Breaches

Corporations face a variety of challenges when conducting internal investigations or responding to data breaches. The speed and accuracy with which an organization can identify compromised data directly impact its ability to mitigate risks, prevent further damage, and address compliance requirements. **The READI Suite enables corporate security teams to remotely access, triage, and analyze compromised data from cloud and on-premises environments.**

Real-World Scenario: During an internal investigation into employee misconduct or a potential data breach, a security team can use READI Network Services to remotely access an employee's workstation or company file shares. This allows for a quick extraction of relevant documents, communication logs, or system activity to identify the source of the breach or inappropriate activity.

Why It Matters: Data breaches or internal misconduct require quick and secure data identification. READI's remote capabilities help corporate security teams efficiently locate and preserve data to minimize business disruptions while maintaining regulatory compliance and protecting sensitive information.

eDiscovery: Detailed Forensic Reporting for Legal Cases Involving Large Volumes of Remote Data

In legal proceedings, the ability to collect, preserve, and analyze vast amounts of electronically stored information (ESI) is crucial for eDiscovery teams. Legal teams often face difficulties accessing data across a wide variety of systems, including cloud services, corporate networks, and user devices. **The READI Suite helps streamline this process by enabling remote collection, triage, and reporting from diverse data sources, ensuring legal teams have the evidence needed for court.**

Real-World Scenario: In a corporate litigation case, an eDiscovery team may need to collect data from multiple custodians across different departments, cloud systems, and devices. READI Cloud Services can remotely gather documents and emails from cloud platforms like Google Drive or OneDrive, while READI for OSX and Windows Services allow for targeted collection of user-generated data from endpoints.

Why It Matters: By offering robust remote triage and collection capabilities, the READI Suite ensures that eDiscovery professionals can quickly gather and analyze large amounts of data without physically collecting devices, reducing the time and costs associated with traditional data collection methods.

Cybersecurity: Swift Response to Data Breaches by Remotely Identifying and Securing Compromised Data

Data breaches pose a significant risk to businesses, often resulting in the loss of sensitive information and regulatory non-compliance. The speed at which compromised data can be identified and secured is critical to minimizing the impact of a breach. **With the READI Suite, cybersecurity teams can remotely access affected systems to quickly analyze and secure sensitive data, preventing further damage.**

Real-World Scenario: After discovering a potential data breach, clients can deploy READI Network and Windows Services to remotely analyze network logs, user activity, and file access histories. This allows the team to pinpoint the compromised systems, secure any further at-risk data, and identify the source of the breach.

Why It Matters: Rapid detection and response to cybersecurity incidents are crucial to preventing data loss and regulatory penalties. The READI Suite enables clients to act quickly, offering real-time remote access to critical systems and allowing for a thorough investigation and secure response without needing to be on-site.

Executive Investigations: Fast, Targeted Search for C-Suite and Board-Level Data

Executive and board-level investigations require specialized handling due to the sensitive nature of the data involved. These investigations often focus on a small group of high-profile individuals and require targeted data collection, ensuring that only relevant information is gathered while minimizing the risk of exposing non-responsive or confidential information. **The READI Suite allows forensic teams to perform these tasks remotely while maintaining a high level of security and privacy.**

Real-World Scenario: During an investigation involving a C-level executive, a legal team may need to quickly and discreetly gather data from the executive's devices or cloud storage systems. READI for OSX or Windows Services can be used to remotely install agents, collect emails, and analyze activity logs, ensuring that only relevant data is collected while protecting sensitive information.

Why It Matters: Executive investigations demand a higher level of discretion and security. The READI Suite's remote capabilities allow legal and compliance teams to gather the necessary data while protecting privacy and minimizing the risk of exposing non-relevant or sensitive information.

Email Investigations: Rapid Triage and Analysis of Email Evidence to Accelerate Investigations

Investigations involving large volumes of email data typically require significant time and resources to review and identify critical evidence. READI for Email significantly streamlines this process by allowing investigators to quickly triage, preview, and analyze critical email metadata and content without needing extensive data collection and processing.

Real-World Scenario: During corporate compliance investigations, cybersecurity incidents, or internal audits, forensic teams can utilize READI for Email to rapidly access and examine email communications, quickly identifying key individuals, suspicious behaviors, or critical information. This rapid access allows investigators to immediately pinpoint relevant email artifacts, facilitating quicker actions and decisions to prevent further issues or data loss.

Why It Matters: Speed and accuracy are critical in email investigations. By enabling investigators to swiftly access and analyze relevant email data directly at the source, READI for Email ensures timely and informed responses to sensitive incidents, reducing investigative time and resource requirements significantly.

Access Analysis and Security Audits

- Monitoring of login activities and detection of unusual behaviors.
- Security audits to track permission changes and potential unauthorized access.

Administrative Reviews

- Investigation of configuration changes and policy modifications.
- Tracking of role assignments and device management.

Compliance Monitoring

- Verification of data retention policy compliance.
- Validation of access controls and organizational policy enforcement.

Tying READI into HaystackID Global Advisory Services

The READI Suite, along with its previously announced mobile counterpart, **Mobile Elite Discovery and Analysis Lab (MEDAL™)**, seamlessly integrates with **HaystackID Global Advisory Services**, providing a strategic advantage in handling complex digital investigations. HaystackID Global Advisory supports organizations by offering expert guidance on cyber discovery, incident response, privacy and compliance, and enterprise risk management. This combined offering allows organizations to align their investigative efforts with broader business and compliance goals, ensuring that critical data challenges are met with precision and foresight.

Key Benefits of this Integration Include:

1. Expert guidance on managing risk and ensuring compliance.
2. Support for cyber discovery, privacy, and enterprise risk management.
3. Integration with HaystackID Discovery Intelligence and HaystackID Core® for seamless data management.
4. Complements HaystackID's MEDAL offerings in mobile environments.

Why READI Matters

The HaystackID READI Suite of Services offers critical solutions for professionals in cybersecurity, information governance, and eDiscovery. By providing comprehensive remote capabilities for collecting, analyzing, and securing data across cloud, network, and endpoint environments, the READI Suite ensures that digital investigations can be conducted efficiently, securely, and in compliance with legal and privacy standards. The suite's integration with HaystackID Global Advisory Services adds an additional layer of strategic oversight, helping organizations manage their most critical data challenges with confidence.

Learn More. Today.

Contact us today to learn more about how HaystackID's Remote Endpoint Analysis and Data Intelligence (READI) Suite of Services can support your forensic, legal, and cybersecurity investigations. The READI Suite offers specialized tools that ensure precision, security, and compliance for remote data collection and analysis.

About HaystackID®

HaystackID solves complex data challenges related to legal, compliance, regulatory, and cyber events. Core offerings include Global Advisory, Data Discovery Intelligence, HaystackID Core® Platform, and AI-enhanced Global Managed Review powered by its proprietary platform, ReviewRight®. Repeatedly recognized as one of the world's most trusted legal industry providers by prestigious publishers such as Chambers, Gartner, IDC, and Legaltech News, HaystackID implements innovative cyber discovery, enterprise solutions, and legal and compliance offerings to leading companies and legal practices around the world. HaystackID offers highly curated and customized offerings while prioritizing security, privacy, and integrity. For more information about how HaystackID can help solve unique legal enterprise needs, please visit HaystackID.com.

Assisted by GAI and LLM technologies.