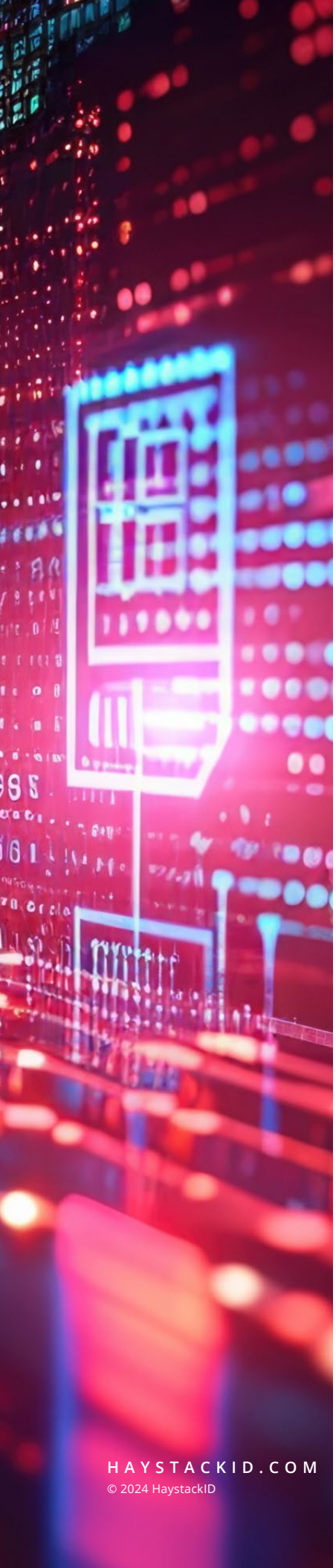

FACT SHEET
Understanding HaystackID® Security
An Overview of Protection, Policies, and Privacy
HAYSTACK®



Understanding HaystackID® Security

HaystackID focuses on meeting customer needs while protecting the confidentiality, availability, and integrity of customer data through a three-fold information security approach. This approach includes physical security layers, network security layers, and security policy layers applied to both internal and external environments, including active and passive protection measures. This approach provides clients with trusted and reliable solutions so they can focus on eDiscovery without worrying about the security and privacy of electronically stored information. HaystackID employs a holistic physical security approach that ranges from employee qualifications and practices to data center access and equipment, follows industry best practices, and complies with certification and compliance audits to maintain the highest standards in data security. From an access management perspective, HaystackID follows strict protocols, regularly revises certificates, keys, and passwords, leverages multi-factor authentication and endpoint encryption, and supports critical network security features. HaystackID's security policies are developed and routinely tested to minimize risk and provide customers with confidence in all data security areas. Understanding security is essential for Cyber Discovery, Information Governance, and eDiscovery professionals to ensure the protection of data throughout the information lifecycle.

HaystackID Security Approach

One of HaystackID's primary focuses is to meet customer needs with offerings, processes, and protocols that protect the **confidentiality, availability,** and **integrity** of customer data. We do this through a three-fold information security approach that includes *physical, network, and security policy layers*. These layers of information security are applied to both internal and external environments and include both active and passive protection measures.

This information security approach provides our customers with trusted and reliable solutions so they can focus on the conduct of electronic discovery without having to divert focus to concerns on the security and privacy of electronically stored information. Certifications, attestations, and compliance audits have also validated this approach.

As security is not an achievement but an ongoing process, HaystackID is committed to maintaining and validating the highest standards from CEO to contractor to ensure our customers have peace of mind that their data is secure throughout the entire information lifecycle.

Certifications, Attestations, and Compliance Audits

- ISO 27001 Certified
- SOC 2 Type 2 Certified (Five Trust Services Criteria)
- HIPAA and HIPAA HITECH Act Compliance
- PCI DSS Compliance
- General Data Protection Rule (GDPR) Adherence
- EU-US and Swiss-US Privacy Shield Certifications
- International Traffic in Arms Regulations (ITAR) Compliance
- NIST 800-171/DFARS Compliance

Physical Security: From Employees to the Enterprise

Employee and Contractor Physical Security

HaystackID employs a holistic physical security approach that ranges from employee qualifications and practices to data center access and equipment, all modeled on ISO 27000 standards.

HaystackID employs extensive background screening and other best practice Human Resource (HR) processes to ensure all company and contracted individuals are correctly qualified, familiar with security policies and procedures, and routinely updated and evaluated on physical security requirements.

These updates and evaluations range from workspace audits to formal security training.

Employee and contractor security responsibilities remain valid after project completion or termination and are documented in our employee handbook.

Employee/Contractor Security Considerations

- Background Checks
- Non-Disclosure Agreements
- Conflict Checks
- Asset Management Controls
- Physical and Environment Security
- Access Control
- Information Security Incident Management

Enterprise Environments and Equipment

HaystackID operates internationally, maintaining data centers across three continents. All HaystackID locations apply and monitor company security policies to ensure that only those qualified (employees, contractors, and visitors) to enter, access, and interact with customer data are able to access secure areas. These secure areas are locked and controlled through a combination of badged access controls, security cameras, and routine auditing to proactively prevent unauthorized access.

From a production environment perspective, data and equipment housed by HaystackID are located in our secure data centers. Our production sites reside in a dedicated and segregated portion of the data centers with additional physical security measures in place. All equipment resides in locked racks, with limited IT personnel having access for on-site maintenance. Additionally, our data centers are designed to compartmentalize any potential combustion events and address such events with full fire detection and suppression systems. Also, regular inspections are conducted to ensure the maintenance of physical protection of data center facilities from not only fires but also floods, earthquakes, explosions, civil unrest, and other potential disasters per SOC 2 Type 2 compliance requirements. Complementing this physical security layer are security policies that have been developed and are routinely tested to ensure no vulnerabilities exist on any level of our physical security structure. Additionally, removable media is only used in controlled areas, and removable media is tracked, managed, and stored following IT asset management standards and procedures. Unusable and retired physical media is managed to customer specification, including data removal, disablement (irrecoverable and inaccessible), and shredding by approved vendors.

Worldwide Reach. Local Expert Touch.

Reach

- Worldwide eDiscovery Reach
- Global Reviewer Support
- Data Centers in the US and EU
- Forensics Teams in the US and EU
- Project Teams 24x7x365 Coverage

Breadth

5 eDiscovery-centric Service Lines

4 Global Advisory Practices

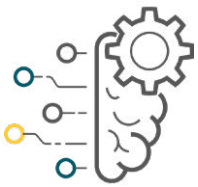
3 Discovery Management Platform (HaystackID Core®) Offerings

6 Mobile Elite Discovery and Analysis Lab (HaystackID MEDAL™) Offerings

10 Global Managed ReviewRight Services

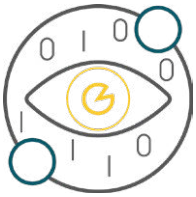
Depth

Expert and Experienced Management Team

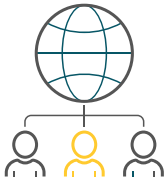


AI Expertise and Coverage

Cybersecurity Expertise and Coverage



Forensics Expertise and Coverage



Reviewer Expertise and Coverage

32,000+ Assessed Review Professionals

2,000+ Active Reviewers at Any One Time

35+ Dedicated Review Managers and Directors

32+ Languages Supported Worldwide

Network Security: From Endpoint to Encryption

HaystackID employs numerous levels of security to ensure all data is protected from unauthorized access. Security measures include hardware firewalls for the networks, and multiple layers of security have been implemented to secure data with file system security encoded into the application layer of our software applications. All network links between offices and data centers are secure Multiprotocol Virtual Private Network (MPLS-VPN) links that maintain no public Internet visibility.

HaystackID also employs three levels of security to protect hosted applications from unauthorized access. External access is controlled by an SSL VPN for each user. Access to applications is controlled by group policy. Moreover, a project manager, in conjunction with the IT component of our operations team, determines and manages case access. Additionally, HaystackID uses multiple monitoring servers to monitor all Internet lines, firewalls (all ports), routers, switches, and servers. Critical application servers are also monitored. These network security elements, supported by our physical and policy layers of security, help ensure customer data's confidentiality, availability, and integrity. From an access management perspective, HaystackID follows strict protocols for accessing servers, storage, network configurations, and data in all enterprise environments.

HaystackID follows industry best practices by regularly revising certificates, keys, and passwords. We also leverage multi-factor authentication and endpoint encryption to augment our need-to-know, role-based data access model.

HaystackID also provides industry best practice support for crucial network security features. Details on these critical security features can be provided as required by our Operations and IT Team security experts to support Requests for Information (RFI), Requests for Proposal (RFP), and Requests for Security Verification.

Industry Best Practice Support and Implementation Approaches

- Application Security Monitoring
- Business Continuity and Disaster Recovery
- Incident Management and Reporting
- Legal Compliance Monitoring (Privacy Shield/GDPR)
- Virus and Malware Protection
- Vulnerability Identification and Management (Including Penetration Testing)

Security Policies: Best Practices for Best Results

HaystackID security policies are developed and routinely tested to detect, identify, locate, report, and remedy any potential vulnerability in our security structure's physical and network security layers. These policies are monitored and managed to minimize risk and provide customers confidence in all data security areas, from employee to enterprise and endpoints to encryption.

Security Policies: Key Areas of Focus

- Chain of Custody Tracking and Management
- Disclosure of Data
- Information Collection, Usage, Storage, and Destruction
- Legal Basis for Processing Personal Data (GDPR)
- Personal Data Management
- Retention of Data
- Transfer of Data
- Security of Data

Learn More. Today.

Contact us today to learn more about our how our threefold approach to information security can ensure the confidentiality, availability, and integrity of your data.

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.