
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.

© 2026 HaystackID

Our 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.**

These **three layers** form the foundation of HaystackID's information security approach, working together to protect customer data, reduce risk, and support secure, reliable eDiscovery throughout the information lifecycle.

Certifications, Attestations, and Compliance Audits

- ISO 27001:2022 Certified
- SOC 3 Certified (Five Trust Services Criteria)
- SOC 2 Type 2 Certified (Five Trust Services Criteria)
- HITRUST r2 Certified
- HIPAA and HITECH Act Compliance
- General Data Protection Regulation (GDPR) Adherence
- EU-U.S., UK Extension, and Swiss-U.S. Data Privacy Framework (DPF) Certifications
- International Traffic in Arms Regulations (ITAR) Compliance
- NIST 800-171/DFARS Compliance



PHYSICAL

Protecting facilities, employees, and infrastructure through layered physical safeguards.



NETWORK

Securing systems, networks, and customer data through encryption, monitoring, and layered security controls.



POLICY

Supporting security through governance, compliance, documented policies, and continuous oversight.

© 2026 HaystackID

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/Contractor Security Considerations

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

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

Enterprise Environments and Equipment

HaystackID operates internationally, utilizing secure data center environments to support its global operations. 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 are regularly reviewed and tested to identify, assess, and address potential vulnerabilities within our physical security infrastructure. 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.

© 2026 HaystackID

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 use 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
Privacy and Regulatory Compliance Monitoring (GDPR/ Data Privacy Frameworks)	Virus and Malware Protection	Vulnerability Identification and Management (Including Penetration Testing)

© 2026 HaystackID

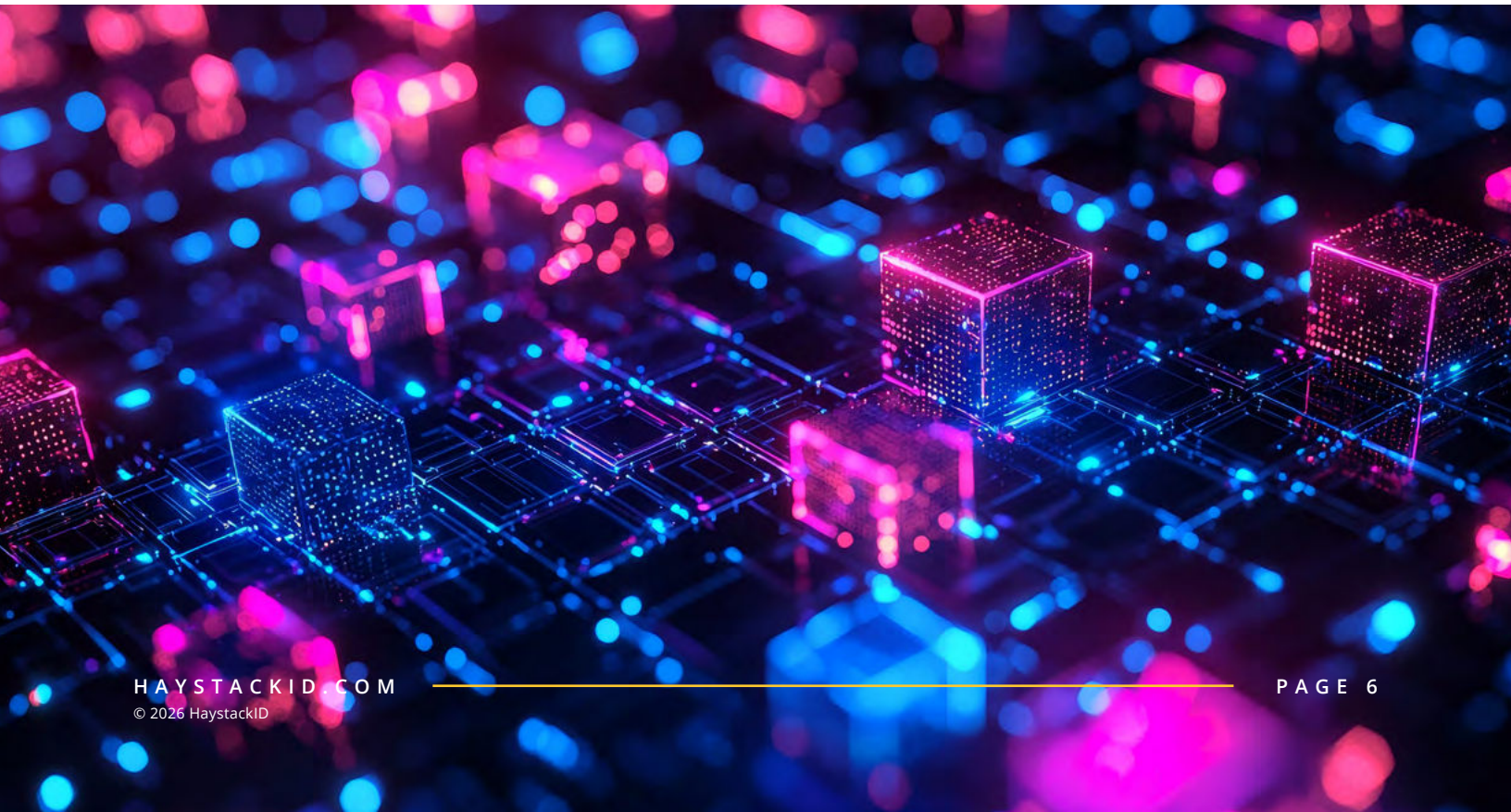
Policy Security

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



© 2026 HaystackID

Worldwide Reach. Local Expert Touch.

REACH

Our strategically located teams and data centers provide responsive support for complex matters across North America and Europe.

- 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

9 Global Advisory Practices

3 Discovery Management Platform (HaystackID Core®) Offerings

16 Forensics First Offerings

10 Global Managed ReviewRight Services

DEPTH



Expert and Experienced Management Team



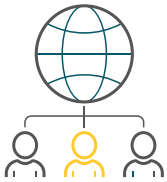
AI Expertise and Coverage



Cybersecurity Expertise and Coverage



Forensics Expertise and Coverage



Reviewer Expertise and Coverage

35,000+ Network of Global Attorneys

2,000+ Active Reviewers at Any One Time

35+ Review Managers and Directors

33+ Languages Supported

Together, these capabilities reflect HaystackID's commitment to **protecting customer data** through secure technology, experienced professionals, and proven operational excellence. By combining physical, network, and policy security with global expertise, we help organizations manage their most sensitive information with confidence.

© 2026 HaystackID

Learn More Today.

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

About HaystackID®

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 and eDiscovery AI® technology. 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. Learn more at HaystackID.com.

Assisted by GAI and LLM technologies.

© 2026 HaystackID