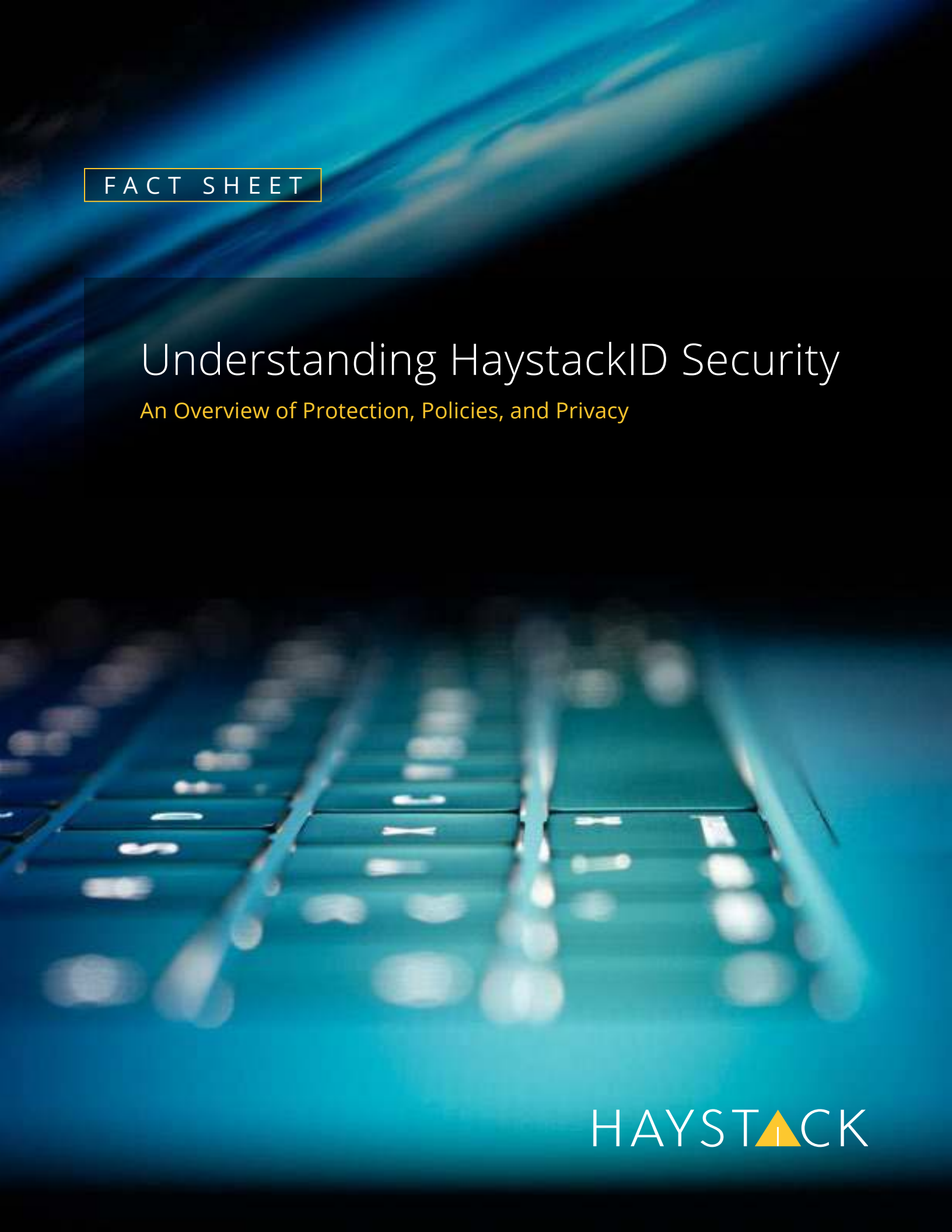
FACT SHEET

Understanding HaystackID Security

An Overview of Protection, Policies, and Privacy



HAYSTACK

HaystackID Security

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 security layers, network security layers, 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 is designed to provide 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. This approach has also been validated by certifications, attestations, and compliance audits.

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

- **International Traffic in Arms Regulations (ITAR) Compliance**
- **HIPAA and HIPAA HITECH Act Compliance**
- **SSAE-16 SOC II Compliance**
- **ISO 27001 Compliance**
- **ISO 14001 Compliance (Germany)**
- **ISO 9001 Compliance (Germany)**
- **PCI DSS Compliance**
- **EU-US and Swiss-US Privacy Shield Certifications**
- **General Data Protection Rule (GDPR) Adherence**

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 properly qualified and familiar with security policies and procedures and are 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 Security

HaystackID currently operates out of multiple international locations with data centers on two 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 one of our five 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 maintenance of physical protection of data center facilities from not only fires, but from floods, earthquakes, explosions, civil unrest, and other potential disasters (In Accordance With SSAE-16 (SOC1) 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 is managed to customer specification to include data removal, data disablement (irrecoverable and inaccessible) and shredding by approved vendors.

U.S. Offices (14)	+ Chicago	+ San Diego
+ Washington DC (HQ)	+ Minneapolis	+ Charlotte
+ Boston	+ Portland	+ Nashville
+ New York	+ San Francisco	+ Atlanta
+ Detroit	+ Los Angeles	+ Miami
International Offices (6)	+ Dusseldorf	+ Shanghai
+ London	+ Munich	
+ Dublin	+ Paris	
Worldwide Data Centers (8)	+ Chicago	+ Dusseldorf
+ Washington, DC	+ Minneapolis	+ Frankfurt
+ Boston	+ London	+ Hong Kong

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 Multi Protocol Virtual Private Network (MPLS-VPN) links maintaining no visibility from the public Internet.

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 the confidentiality, availability, and integrity of customer data. From an access management perspective, HaystackID follows strict protocol from 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, rolebased data access model.

HaystackID also provides industry best practice support of 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 physical and network security layers of our security structure. These policies are monitored and managed to minimize risk and provide customers confidence in all data security areas, from employee to enterprise and from 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 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 is a specialized eDiscovery services firm that helps corporations and law firms find, understand, and learn from data when they face complex, data-intensive investigations and litigation. With an earned reputation for mobilizing industry-leading computer forensics, eDiscovery, and attorney document review experts, our Forensics First, Early Case Insight, and ReviewRight services augmented by our Cybersecurity Consulting and Enterprise Managed Solutions, accelerate and deliver quality outcomes at a fair and predictable price.

HaystackID serves more than 500 of the world's leading corporations and law firms from North American and European locations. Our combination of expertise and technical excellence, coupled with a culture of white glove customer service, makes us the alternative legal services provider that is big enough to matter but small enough to care. Learn more at HaystackID.com.