FACT SHEET

HaystackID® Cybersecurity Services

Defensible Response. Proactive Protection. Strategic Resilience.

HAYSTACK®

Protecting Data. Preserving Trust. Ensuring Compliance.

Overview of HaystackID Cybersecurity Services

HaystackID® delivers expert-led cybersecurity services tailored to meet the evolving challenges facing modern organizations. Backed by decades of experience in digital forensics, incident response, and regulatory compliance, our cybersecurity team helps businesses respond effectively to incidents, recover operations, and build lasting cyber resilience.

We specialize in combining legal defensibility with technical precision, offering not just security controls but also strategic advisory services that align with business continuity and governance requirements. Whether mitigating active threats or enhancing long-term readiness, HaystackID provides the guidance and support necessary to protect data, preserve trust, and ensure compliance.

Why Cybersecurity Matters

Strategic Drivers for Protection

The need for robust cybersecurity is driven by a confluence of legal, operational, and reputational risks. **These drivers form the basis for proactive, resilient cyber programs:**

- **Increasing Threat Landscape:** As threat actors become more sophisticated, the volume and impact of attacks like ransomware and phishing continue to rise. Advanced persistent threats (APTs) from nation-state groups add complexity and urgency.
- **Regulatory Compliance Pressure:** Laws like GDPR, HIPAA, and CCPA impose stringent data protection obligations. Non-compliance can trigger significant fines, litigation, and reputational damage.
- **Sensitive Data Protection:** Organizations manage high volumes of personally identifiable information (PII) and intellectual property (IP). Cybersecurity breaches can compromise customer trust, incur penalties, and jeopardize competitive advantage.
- **Financial Risk Mitigation:** Breaches can result in extensive financial harm through downtime, regulatory fines, and recovery costs. A strong cybersecurity framework reduces exposure and enables faster recovery.
- **Brand and Reputation Defense:** Trust is a fragile asset. Organizations suffering high-profile breaches may lose market share and customer confidence. Cyber resilience supports long-term brand value.
- **Digital Transformation and Cloud Security:** As cloud adoption and remote work expand, organizations face new attack surfaces. Protecting these digital ecosystems is essential for operational continuity.
- **Third-Party and Supply Chain Risk:** Supply chains and vendor networks introduce indirect vulnerabilities. Effective risk management must extend to all connected entities.
- **Human Factors and Training Needs:** Employee mistakes, such as falling for phishing scams, remain a major source of breaches. Continuous training and awareness are critical.
- **Legal and Ethical Responsibilities:** Organizations have a duty of care to protect the data entrusted to them. Demonstrating ethical and effective governance is vital to shareholder and stakeholder trust.

These strategic pressures define today's cybersecurity landscape and set the stage for tailored, real-world solutions that HaystackID is uniquely positioned to deliver.

> *Cybersecurity is no longer just a technology issue—it's a business imperative. At HaystackID, we provide clients with the confidence and capability to navigate digital threats with precision and purpose. Our approach is grounded in integrity, agility, and strategic insight, ensuring that our partners are protected not only today but prepared for what's next.*
>
> ***—Hal Brooks, CEO, HaystackID***

Key Features of Cybersecurity Services

To address the complex and rapidly evolving threat environment, HaystackID offers a portfolio of **expert-driven cybersecurity services built to respond, recover, and defend:**

CYBER INCIDENT RESPONSE

- Incident Management
- Incident Response
- Business Email Compromise (BEC)
- Restoration
- Threat Actor Communications
- Compromised Assessment
- Cyber Retainer Packages

BREACH RESPONSE

- Data Mining
- Breach Notification Services
- DSAR and Litigation Support

ASSESSMENT AND COMPLIANCE SERVICES

- Cybersecurity Assessments
- Tabletop Exercises
- Vulnerability Assessment and Penetration Testing
- Application Security Assessment

MANAGED SECURITY SERVICE

- Managed Detection and Response (MDR)
- Cloud Managed Security Service (M365/Google Workspace)

Cyber Incident Response

- **Incident Management:** Provides end-to-end support, guiding clients through containment, investigation, and regulatory response during an active breach while delivering post-incident remediation, reporting, and strategic recommendations to strengthen future resilience.
- **Incident Response:** Rapid deployment of technology and experts to contain and mitigate breaches. Services include threat identification, data sensitivity assessments, and remediation support to minimize business interruption.
- **Business Email Compromise (BEC):** Provides rapid investigation, threat containment, and forensic deep dive into unusual activities, such as unauthorized logins, privilege escalations, and suspicious account behavior. This investigation encompasses a detailed review of audit logs, user accounts, email configurations, and file-sharing settings to determine the scope and impact of the compromise.
- **Restoration:** Post-incident support includes full system restoration, including tape restoration, to ensure rapid restoration of critical systems, minimize downtime, and assist with forensic validation of recovered data.
- **Threat Actor Communications:** Structured communications with threat actors to facilitate secure, discreet engagement with adversaries during a cyber breach to support negotiation, intelligence gathering, and containment efforts—helping clients assess risk, recover data, and reduce potential impact.
- **Compromised Assessment:** Identifies, analyzes, and contains potential security breaches within an organization's environment—detecting unauthorized access, data exfiltration, and malicious activity to help restore integrity, mitigate risks, and prevent future incidents.
- **Cyber Retainer Packages:** Provides on-demand access to expert cybersecurity support for HaystackID cybersecurity service offerings—ensuring rapid action and strategic guidance when it matters most.

Breach Response

- **Data Mining:** Advanced analytics to extract meaningful insights from large datasets, aiding in proactive risk identification, fraud detection, and security threat analysis.
- **Breach Notification Services:** Comprehensive compliance support, including timely notification to affected individuals and regulatory authorities, along with expert-driven mitigation strategies.
- **DSAR and Litigation Support:** Involves the identification, collection, and review of relevant data to ensure regulatory compliance and support legal proceedings. This includes efficiently managing personal data requests under privacy laws (like GDPR or CCPA) and delivering defensible data solutions for eDiscovery, investigations, and legal matters.

Assessment and Compliance Services

- **Cybersecurity Assessments:** Conduct comprehensive cybersecurity assessments to identify vulnerabilities, evaluate risk exposure, and provide actionable recommendations to strengthen overall security posture.
- **Tabletop Exercises:** Simulate real-world cyber incidents, test response readiness, and strengthen cross-functional coordination.
- **Vulnerability Assessment and Penetration Testing:** Identify, validate, and prioritize security weaknesses across networks, applications, and infrastructure.
- **Application Security Assessment:** Identify vulnerabilities, evaluate code and architecture, and provide actionable remediation to strengthen overall security posture.

Managed Security Service

- **Managed Detection and Response (MDR):** 24/7 real-time threat monitoring using behavioral analytics, threat intelligence, and endpoint telemetry. MDR enables organizations to detect, isolate, and neutralize threats as they emerge.
- **Cloud Managed Security Service (M365/Google Workspace):** Providing continuous monitoring, threat detection, compliance enforcement, and configuration hardening across multi-cloud environments.

These capabilities form a multi-layered defense system that empowers organizations to act decisively when threats arise—and prevent them from recurring.

Practical Applications

HaystackID's cybersecurity services are tailored to meet the practical needs of organizations across sectors, **ensuring legal defensibility and operational resilience:**

- **Achieving and maintaining** compliance with regulations like GDPR, HIPAA, and CCPA.
- **Supporting** legal investigations with documented forensics and expert testimony.
- **Identifying and remediating** data exposures involving PII, PHI, and proprietary content.
- **Enhancing** board-level risk reporting and security governance.
- **Fortifying** internal controls through technical assessments and incident simulations.

These applications ensure that HaystackID's services are not just technically effective but strategically aligned with business needs.

Real-World Benefits

Partnering with HaystackID delivers tangible advantages that align with both **immediate security needs and long-term strategic goals:**

Holistic Approach
Reducing operational friction, shortening investigation duration, and significantly lowering overall cost.

Faster Incident Containment
Minimize business disruption through rapid identification and response.

Enhanced Threat Visibility
Gain real-time insights into malicious behavior and emerging vulnerabilities.

Stronger Compliance Posture
Navigate regulatory obligations confidently with audit-ready support.

Secure Data Recovery
Restore operations efficiently while ensuring data integrity and chain-of-custody.

Tailored Defense Strategies
Deploy security protocols that are customized to organizational risk profiles.

These benefits collectively enable clients to move from **reactive defense to proactive security leadership.**

Technology Highlights

HaystackID integrates advanced technologies with elite professional expertise to deliver **robust, scalable security services:**

- **AI-Powered Threat Analytics:** Detect and prioritize anomalies using machine learning algorithms.
- **Digital Forensics Platforms:** Enable breach documentation, evidence handling, and investigative support.
- **Protect Analytics AI®:** Advanced suite of AI-powered services designed to enhance the identification, analysis, and reporting of sensitive information within large, unstructured datasets, particularly those containing sensitive information like PII, PHI, technical data, and entities.
- **Secure Threat Actor Engagement Protocols:** Structured playbooks for extortion response and communication.
- **Integrated MDR Stack:** Combines endpoint detection, SIEM integration, and live response capabilities.

This fusion of automation and human expertise ensures optimal protection, detection, and recovery in dynamic threat environments.

Example Use Cases

HaystackID's solutions have proven their value in **high-stakes, real-world scenarios:**

- **Global Manufacturer Ransomware Recovery:** Deployed incident response within hours, managed secure communication with attackers, and restored operations with zero regulatory violations.
- **Law Firm BEC Incident:** Identified and contained credential compromise, accelerated MFA implementation, and architected long-term security controls to mitigate the risk of recurrence.
- **Healthcare HIPAA Breach:** Executed forensic review, determined the scope of PII exposure, and supported HIPAA-compliant notification and remediation procedures.

Each case illustrates how HaystackID's services are not only responsive but decisive in helping clients regain control and confidence.

> *At HaystackID, we don't just respond to cyber incidents—we help our clients regain control, maintain trust, and emerge stronger. Whether it's a ransomware negotiation, a business email compromise, or regulatory fallout, our forensic and incident response teams deliver real-time clarity and decisive action when every second counts.*
>
> ***—Michael D. Sarlo, Chief Innovation Officer and President of Global Investigations and Cyber Incident Response Services, HaystackID***

Availability and Deployment

HaystackID's cybersecurity services are available globally and deployable with agility. Whether responding to a critical breach or advising on proactive risk mitigation, **our teams deliver:**

- **On-demand** rapid incident response.
- **Project-based** forensic and compliance assessments.
- **Managed** cybersecurity programs for ongoing protection.
- **Remote and onsite** deployment options tailored to client needs.

With 24/7 readiness, HaystackID ensures clients can rely on real-time support whenever and wherever it is needed.

Learn More. Today.

To explore how HaystackID can support your cybersecurity strategy or assist in active threat response, visit HaystackID.com or contact a Cybersecurity Engagement Specialist today at HaystackID.com/Contact-us.

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