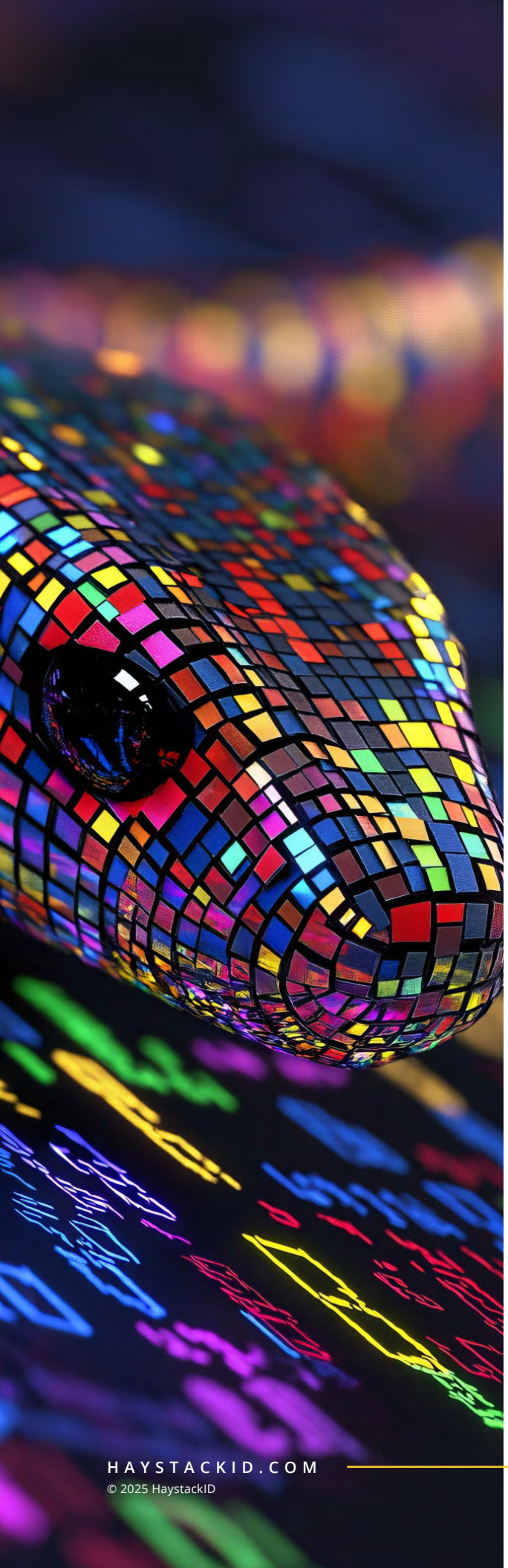
FACT SHEET

HaystackID® Cyber Compromise Assessment Service

Detect, Contain, and Prevent Digital Threats

HAYSTACK®



Service Description

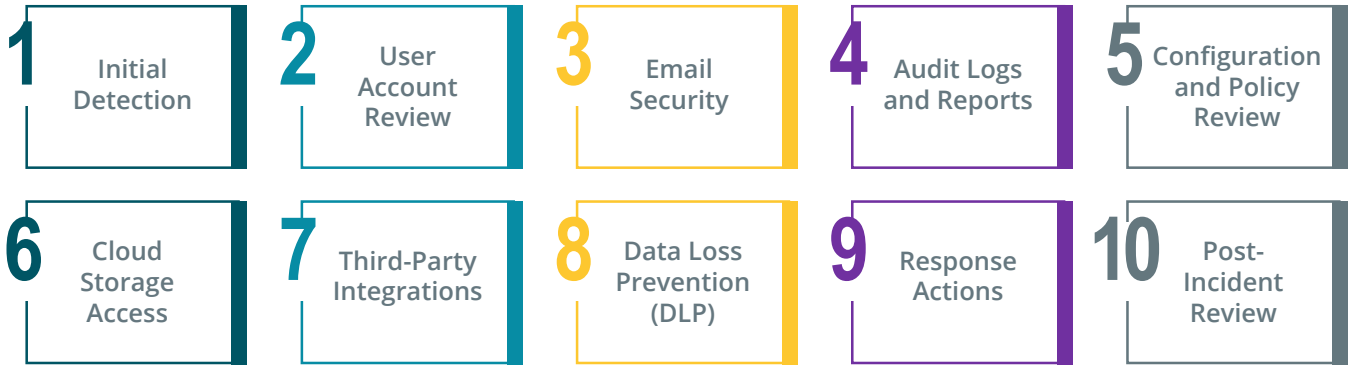
HaystackID's Cyber Compromise Assessment Service offers a robust evaluation of potential security breaches across an organization's digital ecosystem, specializing in cloud environments like Microsoft 365® (M365) and Google Workspace. This service utilizes advanced cyber forensic methodologies and industry expertise to uncover unauthorized access, data exfiltration, and system vulnerabilities while providing actionable remediation strategies.

This comprehensive assessment includes a deep dive into unusual activities, such as unauthorized logins, privilege escalations, and suspicious account behavior. It encompasses a detailed review of audit logs, user accounts, email configurations, and file-sharing settings to determine the scope and impact of the compromise. Key focus areas include configuration changes, third-party app integrations, and data loss prevention policies. The service also evaluates access to cloud storage systems like OneDrive, SharePoint, and Google Drive, addressing all potential breach vectors.

In addition to immediate containment actions - such as isolating compromised accounts and enforcing stronger authentication measures - HaystackID provides tailored recommendations to fortify your security posture. A post-incident review analyzes the breach, updates security protocols, and enhances the organization's readiness for future incidents.

By partnering with HaystackID, organizations can effectively mitigate risks, ensure compliance, and safeguard their most valuable assets.

Compromise Assessment Checklist



Initial Detection

- Review security alerts and notifications from security tools and platforms.
- Identify unusual login patterns (e.g., impossible travel, multiple failed logins, or logins from suspicious IP addresses).
- Verify alerts for credential theft attempts or brute force attacks.

User Account Review

- Audit recent changes to user accounts, including permission escalations.
- Identify newly created or unauthorized accounts.
- Confirm the enforcement and effectiveness of multi-factor authentication (MFA).
- Evaluate shared mailbox activities and access permissions.

Email Security

- Investigate suspicious email forwarding rules (e.g., auto-forwarding to external domains).
- Analyze Sent and Deleted Items folders for unusual activity.
- Check for any unauthorized email access or external forwarding setups.
- Review compromised accounts for phishing or spam email campaigns.

Audit Logs and Reports

- Analyze Entra ID (formerly Azure AD) and Google Workspace login activity for anomalies.
- Review M365 and Google Workspace audit logs for unauthorized actions.
- Examine mailbox audit logs for non-owner access or bulk actions (e.g., deletion of emails).
- Assess activity related to administrative roles and privileges.

Configuration and Policy Review

- Validate the integrity of M365 and Google Workspace security policies and configurations.
- Check for unauthorized changes to security settings, including retention and compliance policies.
- Review settings for Microsoft Defender for Office 365 or equivalent security solutions in Google Workspace.
- Inspect settings for email quarantine, spam filtering, and account lockout policies.

Cloud Storage Access

- Investigate recent activity in OneDrive, SharePoint, and Google Drive.
- Check for unusual file-sharing links or external sharing activities.
- Audit changes to access permissions for critical files or folders.

Third-Party Integrations

- Audit third-party applications connected to M365 and Google Workspace.
- Verify the legitimacy of API permissions granted to external applications.
- Ensure third-party integrations align with organizational security policies.

Data Loss Prevention (DLP)

- Inspect DLP policies for recent changes or unusual triggers.
- Monitor logs for sensitive data access and sharing events.
- Identify potential data exfiltration through email, cloud storage, or external links.

Response Actions

- Account Security: Immediately isolate compromised accounts and enforce password resets.
- MFA and Conditional Access: Strengthen authentication mechanisms and review conditional access policies.
- Stakeholder Communication: Notify affected users, IT teams, and key stakeholders about the incident.
- Cloud Access Containment: Revoke unauthorized file-sharing links and permissions in OneDrive, SharePoint, and Google Drive.

Post-Incident Review

- Conduct a detailed post-mortem to identify root causes and prevent recurrence.
- Update security configurations and enhance monitoring tools for M365, Google Workspace, and other endpoints.
- Provide targeted training for users on phishing, credential hygiene, and other cybersecurity best practices.
- Document lessons learned and refine incident response and disaster recovery plans.

By following this checklist and implementing tailored recommendations, organizations can ensure a swift and thorough resolution to security incidents while strengthening their defenses against future threats.

Learn More. Today.

Contact us today to learn more about how HaystackID can help safeguard your digital ecosystem, mitigate risks, and enhance your readiness for future cyber threats.

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.