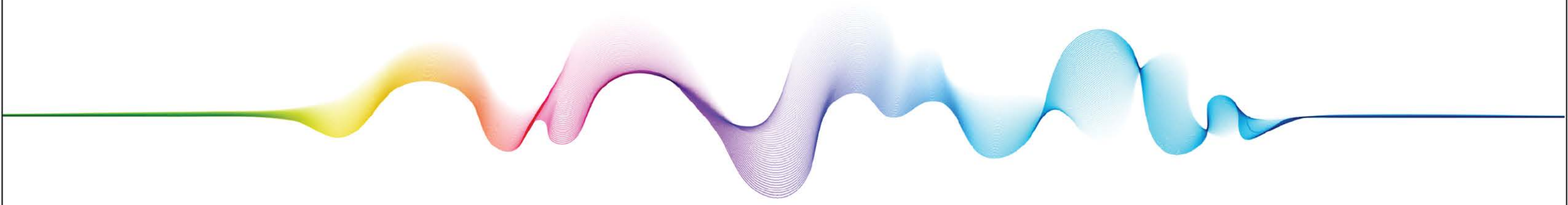
INSIGHT REPORT

OVERVIEW OF THE DATA SECURITY COMMERCIAL MARKET



TAG

CYBERSECURITY

TAG Insights Report: Overview of the Data Security Commercial Market

Prepared by
Dr. Edward Amoroso
Chief Executive Officer, TAG Infosphere
Research Professor, NYU
eamoroso@tag-cyber.com

Version 1.0
February 17, 2024

Introduction

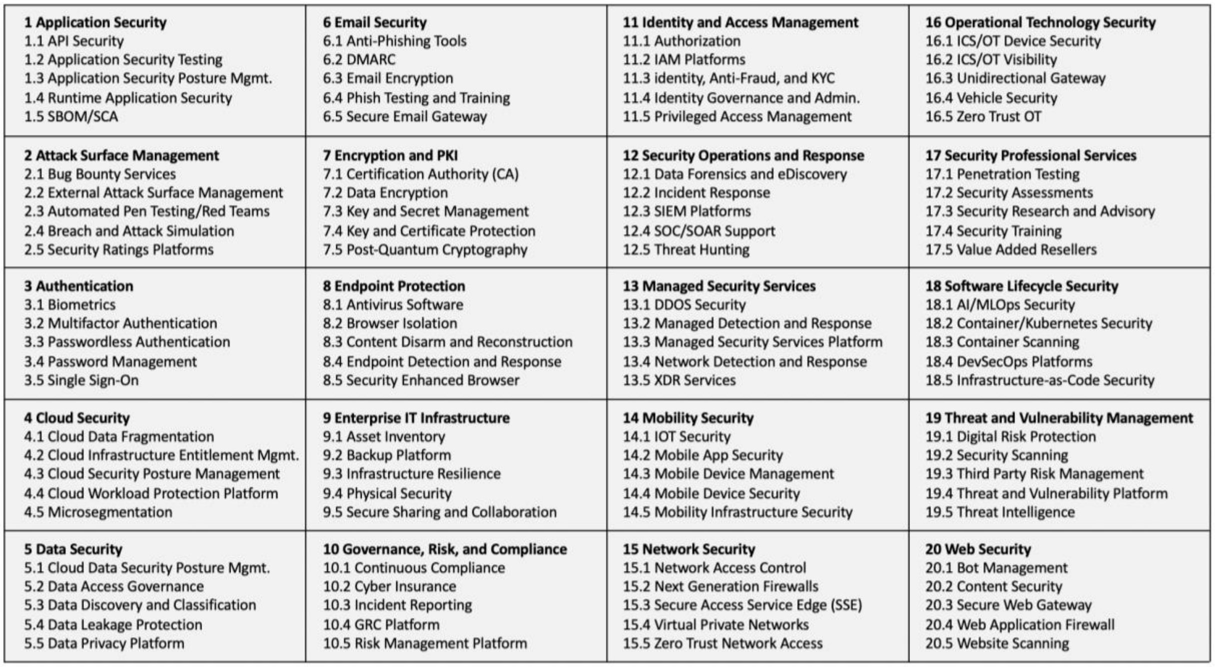
This TAG Insights Report on *Data Security* is intended to help companies, managers, practitioners, researchers, investors, and commercial vendors better understand current trends, issues, and market opportunities in this area. A list of representative commercial vendors working in various areas of data security is included. The five specific areas of covered in this report include:

1. Cloud Data Security Posture Management (CDSPM)
2. Data Access Governance
3. Data Discovery and Classification
4. Data Leakage Protection (DLP)
5. Data Privacy Platform

This report is intended for general and unrestricted use, but interested readers are encouraged to connect with the TAG research and advisory team for more information on the private TAG Research as a Service (RaaS) community that covers, discusses, and shares information on these topics in more depth and includes a wider range of startups, vendors, and companies.

TAG Taxonomy

We organize this TAG Insights Report as per our updated TAG Taxonomy which includes twenty categories of modern solution areas where stakeholders and buyers can find suitable commercial products and services for purchase and use. Each category has five subcategories that correspond to the main areas in which practitioners can focus. These subcategories are discussed below.



1 Application Security 1.1 API Security 1.2 Application Security Testing 1.3 Application Security Posture Mgmt. 1.4 Runtime Application Security 1.5 SBOM/SCA	**6 Email Security** 6.1 Anti-Phishing Tools 6.2 DMARC 6.3 Email Encryption 6.4 Phish Testing and Training 6.5 Secure Email Gateway	**11 Identity and Access Management** 11.1 Authorization 11.2 IAM Platforms 11.3 identity, Anti-Fraud, and KYC 11.4 Identity Governance and Admin. 11.5 Privileged Access Management	**16 Operational Technology Security** 16.1 ICS/OT Device Security 16.2 ICS/OT Visibility 16.3 Unidirectional Gateway 16.4 Vehicle Security 16.5 Zero Trust OT
2 Attack Surface Management 2.1 Bug Bounty Services 2.2 External Attack Surface Management 2.3 Automated Pen Testing/Red Teams 2.4 Breach and Attack Simulation 2.5 Security Ratings Platforms	**7 Encryption and PKI** 7.1 Certification Authority (CA) 7.2 Data Encryption 7.3 Key and Secret Management 7.4 Key and Certificate Protection 7.5 Post-Quantum Cryptography	**12 Security Operations and Response** 12.1 Data Forensics and eDiscovery 12.2 Incident Response 12.3 SIEM Platforms 12.4 SOC/SOAR Support 12.5 Threat Hunting	**17 Security Professional Services** 17.1 Penetration Testing 17.2 Security Assessments 17.3 Security Research and Advisory 17.4 Security Training 17.5 Value Added Resellers
3 Authentication 3.1 Biometrics 3.2 Multifactor Authentication 3.3 Passwordless Authentication 3.4 Password Management 3.5 Single Sign-On	**8 Endpoint Protection** 8.1 Antivirus Software 8.2 Browser Isolation 8.3 Content Disarm and Reconstruction 8.4 Endpoint Detection and Response 8.5 Security Enhanced Browser	**13 Managed Security Services** 13.1 DDOS Security 13.2 Managed Detection and Response 13.3 Managed Security Services Platform 13.4 Network Detection and Response 13.5 XDR Services	**18 Software Lifecycle Security** 18.1 AI/MLOps Security 18.2 Container/Kubernetes Security 18.3 Container Scanning 18.4 DevSecOps Platforms 18.5 Infrastructure-as-Code Security
4 Cloud Security 4.1 Cloud Data Fragmentation 4.2 Cloud Infrastructure Entitlement Mgmt. 4.3 Cloud Security Posture Management 4.4 Cloud Workload Protection Platform 4.5 Microsegmentation	**9 Enterprise IT Infrastructure** 9.1 Asset Inventory 9.2 Backup Platform 9.3 Infrastructure Resilience 9.4 Physical Security 9.5 Secure Sharing and Collaboration	**14 Mobility Security** 14.1 IOT Security 14.2 Mobile App Security 14.3 Mobile Device Management 14.4 Mobile Device Security 14.5 Mobility Infrastructure Security	**19 Threat and Vulnerability Management** 19.1 Digital Risk Protection 19.2 Security Scanning 19.3 Third Party Risk Management 19.4 Threat and Vulnerability Platform 19.5 Threat Intelligence
5 Data Security 5.1 Cloud Data Security Posture Mgmt. 5.2 Data Access Governance 5.3 Data Discovery and Classification 5.4 Data Leakage Protection 5.5 Data Privacy Platform	**10 Governance, Risk, and Compliance** 10.1 Continuous Compliance 10.2 Cyber Insurance 10.3 Incident Reporting 10.4 GRC Platform 10.5 Risk Management Platform	**15 Network Security** 15.1 Network Access Control 15.2 Next Generation Firewalls 15.3 Secure Access Service Edge (SSE) 15.4 Virtual Private Networks 15.5 Zero Trust Network Access	**20 Web Security** 20.1 Bot Management 20.2 Content Security 20.3 Secure Web Gateway 20.4 Web Application Firewall 20.5 Website Scanning

Figure 1. TAG Taxonomy for Cybersecurity

Overview of Data Security Solutions

The following emerging global commercial opportunities involving data security solutions are covered in this report, including the listing of several viable commercial entities providing solutions on the market today:

- Cloud data security posture management (CDSPM) supports enterprise cybersecurity by continuously monitoring and managing the security posture of data across cloud environments. It helps identify and remediate risks of data storage, access, and compliance with industry regulations, thus reducing the likelihood of data breaches and ensuring that cloud data remains secure.
- Data access governance (DAG) involves setting policies and controls over who can access data within an organization. By managing permissions and tracking access to sensitive data, Data Access Governance ensures that only authorized individuals have the ability to view or modify data, thereby reducing the risk of insider threats and unauthorized data exposure.
- Data discovery and classification support cybersecurity by identifying where sensitive data resides across the enterprise and classifying it according to its level of sensitivity. This is crucial for applying appropriate security measures,

complying with data protection regulations, and quickly responding to potential data breaches.
- Data leakage protection (DLP) tools are designed to prevent unauthorized transfer of data outside the corporate network. They monitor and control endpoint activities, filter data streams on corporate networks, and secure data in motion and at rest, thereby protecting against both intentional and unintentional data leaks that could lead to a security incident.
- Data privacy platforms support cybersecurity by ensuring that an organization's data handling practices comply with privacy laws and standards. It helps manage consent, data subject rights, and data retention policies, which reduces the risk of data misuse and the consequent legal and financial repercussions.

Focus Area: Cloud Data Security Posture Management (CDSPM)

Cloud Data Security Posture Management (CDSPM) is an integral component of cybersecurity in cloud environments. CDSPM tools systematically evaluate cloud configurations and activities against security best practices and compliance standards. They provide visibility into cloud assets, detect misconfigurations, and offer guidance for remediation.

Misconfigurations in cloud services are a primary cause of data breaches. CDSPM mitigates this risk by automatically scanning cloud environments for configuration errors, such as improperly set security groups or storage buckets lacking proper encryption. By alerting administrators to these issues, organizations can address vulnerabilities before they are exploited.

CDSPM solutions also integrate with cloud services to assess identity and access management (IAM) policies. They ensure that the principle of least privilege is adhered to, thus limiting permissions to only what is necessary for a given role. This prevents excessive access rights that could be abused in the event of a compromised account.

Compliance monitoring is another core function of CDSPM. Cloud environments must adhere to a variety of regulations depending on the data they handle. CDSPM tools map cloud configurations to compliance requirements such as GDPR, HIPAA, or PCI-DSS, providing a clear view of compliance status and highlighting areas needing attention.

Continuous monitoring offered by CDSPM ensures that any changes in the cloud environment are evaluated in real-time, maintaining an organization’s security posture amidst the dynamic nature of cloud computing. By providing insights into cloud resource utilization, CDSPM tools also aid in optimizing security investments, making sure that resources are allocated effectively for maximum security impact.

Focus Area: Data Access Governance (DAG)

Data Access Governance (DAG) is a framework for managing data access within organizations. DAG tools ensure that only the right individuals can access the right data at the right times, under the right conditions. This is achieved by implementing robust access controls and monitoring data access patterns.

By defining access policies, DAG enforces who can or cannot access certain data sets. It involves creating a structured process for access requests, approvals, and auditing. Access reviews are conducted regularly to ensure that the assigned permissions are still valid and align with the current job roles and responsibilities.

DAG solutions provide granular visibility into data access across the enterprise. They track which users are accessing data, when, and for what purpose. This audit trail is crucial for investigating security incidents and proving compliance with regulatory requirements.

Role-based access control (RBAC) is a key strategy within DAG, where access rights are grouped by role rather than assigned individually. This simplifies management and ensures consistency in access permissions. In addition, attribute-based access control (ABAC) can be implemented, where access is granted based on attributes like department, location, or data classification.

Another aspect of DAG is the management of privileged accounts. These accounts have elevated access and, if compromised, can cause significant damage. DAG tools manage, rotate, and monitor the use of privileged credentials, reducing the attack surface.

Focus Area Data Discovery and Classification

Data Discovery and Classification are processes that systematically identify and sort data across an organization's digital environment. Data discovery involves scanning storage systems and databases to locate data, while classification involves labeling the data based on its content, sensitivity, and importance to the business.

The discovery process uses automated tools to search through structured and unstructured data. These tools can recognize patterns, such as credit card numbers or personal identification information, which indicates sensitive data that requires protection. Once identified, the data is cataloged for easy retrieval and management.

Classification frameworks categorize data into tiers. For instance, public, internal, confidential, and restricted tiers might be used. Each tier corresponds to a set of security controls. By classifying data, organizations can apply the appropriate level of protection to prevent unauthorized access or disclosure.

Data discovery and classification facilitate compliance with data protection regulations. They help in mapping data flows and understanding how data is used within the organization, which is necessary for regulatory reports and audits.

The classification metadata also plays a vital role in other cybersecurity processes. Data Loss Prevention (DLP) systems use this metadata to enforce policies and prevent unauthorized sharing of sensitive data. Encryption strategies are also guided by classification levels, ensuring that high-risk data is encrypted both at rest and in transit.

Focus Area: Data Leakage Protection (DLP)

Data Leakage Protection (DLP) is an integral component of enterprise cybersecurity strategies. It encompasses tools and processes that aim to detect and prevent data breaches by monitoring, detecting, and blocking sensitive data while in use (endpoint actions), in motion (network traffic), and at rest (data storage). The primary function of DLP is to ensure that sensitive or critical information is not lost, misused, or accessed by unauthorized users.

DLP tools classify regulated, confidential, and business-critical data and identify policy violations defined by organizations or within a predefined policy pack, typically driven by regulatory compliance such as HIPAA, PCI-DSS, or GDPR. Once such data is identified and classified, DLP enforces remediation with alerts, encryption, and other protective actions to prevent end users from accidentally or maliciously sharing data that could put the organization at risk.

DLP systems provide a comprehensive view of where data resides, how it is used, and how it moves across endpoints, networks, and storage systems. This visibility allows for the effective governance of data and the ability to trace any issues or incidents to their source. Policies within DLP systems can be fine-tuned to address different departments, workgroups, or user roles to adjust for the varying levels of data sensitivity.

DLP solutions include a range of protective actions such as blocking, quarantining, and encrypting sensitive data. These actions can be applied to data at rest, ensuring that stored data is not improperly accessed or modified. For data in motion, DLP tools scan and analyze network traffic to detect sensitive data being sent outside the corporate network and can block transmissions in violation of policies. For data in use, DLP systems monitor and control user activities on devices, preventing unauthorized actions such as copying data to removable storage or printing confidential documents.

In essence, DLP serves as a safeguard against both external threats and internal vulnerabilities, securing data against exposure from cyber-attacks, insider threats, or accidental leaks. It plays a vital role in protecting intellectual property and sensitive corporate data, thus maintaining the confidentiality, integrity, and availability of enterprise data.

Focus Area: Data Privacy Platforms

Data Privacy Platforms are designed to assist organizations in managing the way they handle personal data in compliance with various data protection regulations. These platforms provide a framework for data privacy management, including tools for data discovery, consent management, policy enforcement, data subject access rights, and reporting.

A Data Privacy Platform automates the discovery and mapping of personal data across an organization’s systems, whether in the cloud or on-premises. This data mapping is essential for understanding the data flow and establishing a data inventory, which is a prerequisite for compliance with laws like GDPR, CCPA, and others that mandate organizations to know what personal data they possess and process.

Once data is identified, these platforms assist in classifying it based on sensitivity and relevance to privacy regulations. This classification is crucial for applying the correct controls to prevent unauthorized access and ensuring that data is processed lawfully, fairly, and transparently. Consent management is another critical function of Data Privacy Platforms. They track the consent status of individuals and ensure that personal data is not used without proper authorization. This aligns with the requirement of regulations that mandate clear and affirmative consent for data processing activities.

Policy management and enforcement modules within these platforms help define how personal data should be handled, accessed, and shared. They ensure policies are consistently applied across all data, reducing the risk of non-compliance. Automated workflows can handle data subject requests, such as access, rectification, erasure, or data portability, efficiently and within the legal time frames.

Data Privacy Platforms also include reporting and analytics tools to monitor compliance and provide evidence of compliance to regulators. They can generate reports on data processing activities, demonstrate the effectiveness of controls, and identify areas that may require additional measures.

These platforms are essential for managing the risks associated with data privacy and for building trust with customers and partners. They provide the necessary infrastructure to respond to privacy-related queries and complaints, thereby supporting transparency and accountability in data processing activities. By ensuring that personal data is handled in a compliant manner, Data Privacy Platforms play a crucial role in protecting the privacy rights of individuals and safeguarding the organization from data breaches, legal penalties, and reputational damage.

Companies and Contributions

The companies listed below emerged as part of our research at TAG. Our goal in listing these fine firms is to provide a starting point for buyers, advocates, stakeholders, and researchers trying to make sense of the commercial landscape for Data Security as a means for driving toward a more secure global ecosystem.

Cloud Data Security Posture Management (CDSPM) Vendors

1. BMC: Automates cloud configuration security checks and remediation without coding requirements.
2. CrowdStrike: Offers CSPM features for hybrid and multicloud environments with threat intelligence and agentless monitoring.

3. Cyscale: Specializes in cloud security mapping and management, offering a contextual CSPM solution with an emphasis on user experience.
4. F5: Protects application infrastructures in the cloud through threat detection and risk identification.
5. Lacework: Delivers CSPM solutions that provide cloud asset inventories, customizable reports, and advanced risk contextualization.
6. Palo Alto Networks: CSPM that's part of a larger CNAPP, with unique approaches to threat detection and policy management.
7. PingSafe: Provides a cloud security platform that includes tools for cloud misconfiguration and compliance monitoring.
8. Rapid7: CSPM solutions for heavily regulated sectors like healthcare, energy, and finance.
9. Runecast: AI-driven vulnerability assessment tool for detecting risks and enforcing compliance across cloud networks.
10. Stacklet: Cloud governance platform that provides network visibility, security, and optimization.
11. Trend Micro : A comprehensive cloud platform for workload protection and compliance audits.
12. Wiz: Offers cloud vulnerability management with extensive visibility and contextual threat intelligence.

Data Access Governance Vendors

1. Calamu: Calamu Protect fragments data across multiple separate storage locations.
2. Collibra Data Governance: Specializes in data stewardship management and policy management, integrating data cataloging, data lineage, and data quality tools to enhance data governance visibility and compliance.
3. Erwin Data Intelligence by Quest: Provides data awareness and knowledge to drive data governance and business enablement with features like automated metadata harvesting and data lineage documentation.
4. IBM Cloud Pak for Data: A platform supporting data governance, quality, and privacy with AI-driven data discovery, metadata enrichment, and data quality management.
5. Microfocus: Focuses on securing unstructured data against cyber threats and ensuring compliance with privacy regulations.
6. OneTrust Data Governance: Combines AI-driven data discovery and classification with an integrated data catalog and data governance policy management.
7. Oracle Enterprise Metadata Management (OEMM): Helps in harvesting, cataloging, and governing metadata across various systems, offering features like data lineage tracing and impact analysis.
8. Precisely Data Integrity Suite: Offers a comprehensive suite for data integration, observability, governance, and quality. The service includes real-time tracking of data, automated workflows, and metadata management.

9. Riskonnect GRC: Provides a comprehensive view of business risks and opportunities, offering real-time visibility and control with features like automated task management and integration with Salesforce CRM.
10. Rocket Data Intelligence: Focuses on resolving data distrust issues with metadata management, data lineage, and data governance capabilities, including end-to-end data views and role-based access control.
11. SAP GRC: Delivers real-time visibility and control over business risks with integrated risk management and access governance capabilities.
12. Thales: SafeNet Trusted Access is an access management service that combines the convenience of single sign-on with granular access security.

Data Discovery and Classification

1. AWS: Provides AWS Glue Data Catalog which offers data governance capabilities with features such as automated crawling of repositories, improved visibility, and control of data assets.
2. Boomi: Offers Data Catalog and Preparation, part of Boomi's Platform, that combines data catalog with data preparation capabilities and supports natural language queries.
3. Collibra: Collibra Data Catalog provides automated features for data discovery and classification, data curation, and data lineage as part of its Data Intelligence Cloud platform.
4. Data.world: A cloud-native SaaS platform known for its knowledge graph approach, offering AI-powered capabilities for data discovery and metadata management.
5. DataGrail: Offers a purpose-built platform for legal and security teams to manage personal data for privacy regulations.
6. Digital Guardian: Offers comprehensive data classification solutions optimized for regulatory compliance and IP protection.
7. Google: Provides a product called Cloud Data Catalog which is a fully managed service for data discovery and metadata management, providing natural language queries and integration with Google Cloud services.
8. IBM: Offers Watson Knowledge Catalog which is a metadata repository designed for AI and analytics workflows, offering intelligent cataloging and data discovery.
9. Informatica: Provides Enterprise Data Catalog that uses machine learning for automatic data scanning, ingestion, and classification, featuring advanced data dependency tracking.
10. ManageEngine: Offers a product called Endpoint DLP Plus that provides data loss prevention through data discovery and classification, file protection, and data movement controls.
11. Microsoft: Supports data discovery, classification, and protection as part of their cybersecurity solution.
12. OneTrust: Utilizes AI for the discovery and classification of data across structured, unstructured, and semi-structured data environments.
13. Qlik: Qlik Sense offers data analytics and discovery with interactive visualizations, AI-driven insights, and a high-performance SaaS and hybrid cloud platform.

14. Quest: Offers Erwin Data Catalog that automatically harvests, catalogs, and curates metadata and includes data mapping, lifecycle management, and data lineage.
15. Thales: Thales offers a product called CiperTrust that discovers and classifies sensitive data in cloud, big data, and traditional environments.
16. TrustArc: Data Inventory Hub is a privacy data inventory and mapping system which supports building and managing a data inventory
17. Varonis: Offers an all-in-one data security platform that rapidly reduces risk, detects abnormal behavior, and proves compliance.

Data Leakage Prevention (DLP) Vendors

1. Avanan: Avanan Data Loss Prevention Software offers visibility and control of sensitive data flowing in and out of an organizations' network.
2. Code42: This cloud-based service specializes in identifying insider threats and includes recovery processes.
3. Comodo: Observes activities across various channels and can be run over virtual appliances like Hyper-V or VMWare.
4. CoSoSys Endpoint Protector: Offers an on-premises solution, a cloud service, and a standalone software package, compliant with HIPAA, PCI DSS, and GDPR.
5. CTM360: CTM360 keeps its customers up to date with the latest data leaks on a global scale and alerts of any critical situations. CTM360 collaborates with various vendors across the globe to give them the maximum value and ability to extract data from cyberspace whenever possible. The platform detects and monitors files and code associated with organizations and leverages relevant response actions to remove.
6. Forcepoint: Offers broad monitoring and analysis capabilities with minimal resource consumption on endpoints.
7. Fortinet: Fortinet's comprehensive portfolio of security solutions includes advanced firewalls, secure access solutions, secure web gateways, DLP, endpoint security, cloud security, and more. Fortinet's solutions are designed to protect organizations of all sizes from the most advanced cyber threats.
8. Fortra Digital Guardian: A cloud-based system that protects sensitive data across various platforms and complies with multiple data security standards.
9. Material Security: Protects critical data in employee, partner, contractor, and VIP accounts—without hurting productivity. Material finds and redacts sensitive content in email archives and brings it back when you need it, after a simple verification step.
10. McAfee: Provides comprehensive DLP to safeguard sensitive information from leaving the corporate network.
11. Nightfall: A solution that classifies sensitive data and actively prevents data leaks and breaches.
12. Palo Alto Networks: Delivers DLP through the cloud and is designed for mobile and hybrid workforces.
13. Proofpoint: Emphasizes a people-centric approach to identifying and preventing data loss.

14. Safetica: Offers a comprehensive data loss prevention tool that focuses on user behavior to protect sensitive data.
15. SolarWinds: Focuses on access rights management and spots suspicious activity, with a 30-day free trial.
16. Symantec: Specializes in solutions to protect against data loss across various channels and storage.
17. Trellix: Provides several methods for protecting sensitive information and integrates with third-party tools.
18. Zscaler: A cloud-based suite of products and services that includes cloud, email, and endpoint DLP.

Data Privacy Platforms

1. Archer: Provides an integrated risk management platform that includes privacy features.
2. BigID: Focuses on data privacy, protection, and perspective, enabling organizations to manage and secure customer data and privacy.
3. Cybot: CookieBot Consent management platform, enables website operators to comply with the information, documentation, and consent requirements regarding online tracking of the EU ePrivacy Regulations and GDPR.
4. DataGrail: DataGrail is a purpose-built platform for legal and security teams to manage personal data for privacy regulations.
5. Imperva: Discovery and classification for both structured and unstructured data, user access privilege assessment and data access monitoring.
6. Informatica: Offers a suite of solutions designed to help discover personal and sensitive data and manage data privacy.
7. LiveRamp: A data connectivity platform supporting the safe and effective use of data with strong privacy features.
8. OneTrust: A comprehensive suite of software products designed for privacy, security, and governance compliance.
9. OvalEdge: Provides a data catalog and data governance tool that centralizes a company's data for easier management and privacy control.
10. Piwik PRO: Offers a privacy-oriented analytics suite that ensures compliance with global data protection regulations.
11. SAI360: Merges GRC software and Ethics & Compliance Learning to enhance risk management with privacy features.
12. Secuvy AI: Offers AI-driven workflows for privacy compliance, including customizable Subject Access Requests and Automated Data Maps.
13. TrustArc: Offers a platform for data privacy management and automation, helping businesses to navigate the complex landscape of privacy regulations.
14. VGS platform: Specializes in securing sensitive data through innovative methods that reduce privacy and security risks.

About TAG

TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations in cybersecurity, artificial intelligence, and sustainability to enterprise teams, government agencies, and commercial vendors.

The material in this report is comprised of the opinions of the TAG Infosphere analysts and is not to be interpreted as consisting of factual assertions. All warranties regarding the correctness, usefulness, accuracy, or completeness of this report are disclaimed herein.