Hype Cycle for Privacy, 2023

Published 24 July 2023 - ID G00793135 - 109 min read

By Analyst(s): Bernard Woo, Bart Willemsen

Initiatives: Cyber Risk; Meet Daily Cybersecurity Needs

Privacy remains a top organizational priority as regulations that impact the processing of personal data continue to emerge, including those related to the use of AI. Security and risk management leaders can use this Hype Cycle to prioritize strategic investments that support scalable adaptation.

Strategic Planning Assumptions

By 2025, 75% of the world's population will have its personal data covered by modern privacy regulations.

By 2025, 60% of large organizations will adopt privacy-enhancing computation (PEC) techniques for processing data in untrusted environments and multiparty data analytics use cases.

By 2026, fines due to mismanagement of subject rights will have increased tenfold from 2022 to over $1 billion.

Analysis

What You Need to Know

The right to privacy continues to be enshrined in law through regulatory changes worldwide. Changes are not limited to the passing or revamping of “privacy” laws and an increase in enforcement activity. Legislators worldwide have also begun debating the need to regulate new technologies that can have profound effects on individual privacy, such as artificial intelligence (AI).

Security and risk management (SRM) leaders responsible for privacy face massive increases in requirements and expectations from customers and regulators alike. The requirements are fueling increased awareness of issues of individual privacy within organizations, but there remains a range of opinions on how these should be addressed. Some organizations insist on treating them strictly as matters of compliance. Others have recognized how exhausting and costly efforts to deal with privacy issues can be, particularly if they only rely on labor-intensive manual workflows and processes.

Therefore, organizations are increasingly looking to make strategic investments to drive efficiency and scalability. The challenge of building a scalable privacy program is increased by exponential growth in data collection and analytics capabilities, driven by a wave of hype about generative AI. Although these forces have revealed previously hidden sources of value within data, they have also amplified concerns about the potential for adverse impacts on the rights and freedoms of individuals.

The evolution of the regulatory environment will continue to lead to innovative, built-for-purpose solutions and a better-defined privacy technology ecosystem. The availability and growth of new technologies provides SRM leaders with means to protect privacy in a volatile environment. As such, SRM leaders must help their organization make strategic technology investments to support a scalable approach to privacy that balances innovation with the need to satisfy regulatory requirements.

The Hype Cycle

A mature privacy posture can only be achieved through privacy management and the use of controls, as well as data-centric capabilities. The field of privacy spans various disciplines — it is much more than a matter of securing data through the use of access controls and encryption, although that is fundamental. SRM leaders with privacy responsibilities must maintain working relationships with all business units in order to promote coordinated action to increase awareness of privacy issues and facilitate compliance.

For example, opportunities can be found in business process reengineering, which is neither a security-specific nor a technology-specific discipline. The application of data minimization to the data life cycle can also help — and, similarly, is more of a discipline than a specific technology. Additionally, SRM leaders with privacy responsibilities are in a position to facilitate the achievement of business goals in the areas of analytics and business intelligence through data-centric controls like synthetic data and differential privacy.

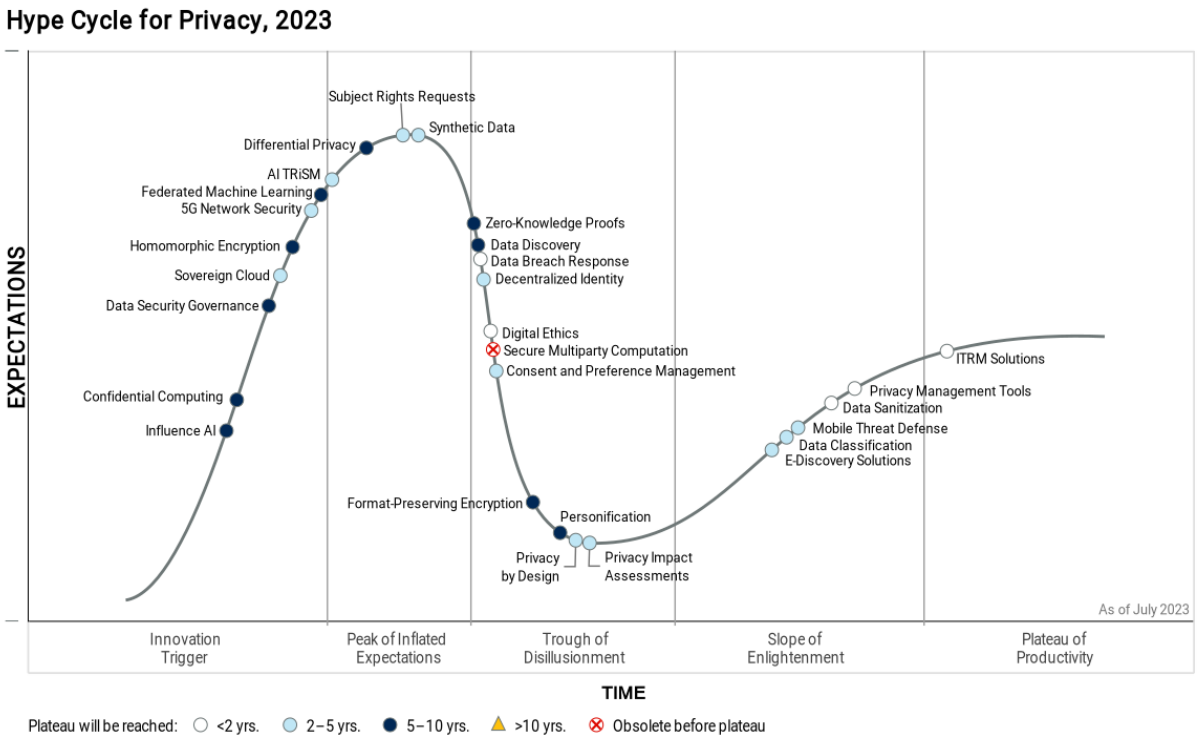
Beyond the imposition of sanctions, efforts to mitigate privacy risks focus on financial risk following a breach, the decaying of consumer trust and brand damage.

Technologies highlighted in this Hype Cycle:

- Enable or enhance control over personal data use: for example, data discovery, data classification, and subject rights requests.
- Create transparency and demonstrate compliance: for example, privacy management tools.
- Mitigate the risk of data misuse: for example, zero-knowledge proofs and homomorphic encryption.
- Mitigate the impact of unintended consequences: for example, format-preserving encryption.
- Help with consistent and repeatable decision making for risk reduction: for example, AI trust, risk and security management (AI TRiSM) and privacy by design.
- Improve the customer experience: for example, influence AI.

This year's Hype Cycle features a new entry, AI TRiSM, to reflect the growing focus on the adoption of AI. This innovation is a framework for managing the risks, including those related to privacy, associated with the use of AI within organizations.

Figure 1: Hype Cycle for Privacy, 2023



The Priority Matrix

The types of technology on this Hype Cycle vary widely, as do their benefits. Rather than leading operations, these technologies should be applied only after gap and risk assessments, and should play a supporting role.

Addressing privacy risk requires a focus on the individual — that is, the data subject. Benefits depend on the types of threats prevented and the types of business activities enabled. Data discovery and data classification, for example, identify personal data and its associated sensitivity to enable application of controls at the data layer. These approaches can also benefit the generic risk treatment of confidential data.

Other approaches, such as privacy by design, AI TRiSM and influence AI, represent cultural changes within organizations that affect the processing of personal data. The impacts of these innovations are not easily quantified.

Proactive risk reduction can be achieved through competent data life cycle governance and pseudonymization techniques, such as encryption, masking and tokenization.

Customer trust levels can be enhanced with a positive privacy user experience (UX) that includes the management of subject rights requests, and consents and preferences.

Evolving technologies are associated with secure multiparty computing and analytics activities that benefit from privacy preservation through the use of differential privacy and homomorphic encryption.

Compliance demonstration is aided by purpose-built privacy management tools.

New business and IT contexts, such as 5G networking, mean that SRM leaders responsible for privacy need to keep evolving to address new privacy threats (as do vendors). Fortunately, as a result of the need for both privacy and business benefits, new technologies are emerging as vendors improve their offerings and broaden their combinations of capabilities.

Table 1: Priority Matrix for Privacy, 2023

(Enlarged table in Appendix)

Benefit	Years to Mainstream Adoption			
	Less Than 2 Years	2 - 5 Years	5 - 10 Years	More Than 10 Years
Transformational		Decentralized Identity	Data Security Governance Homomorphic Encryption Influence AI	
High	Data Breach Response Digital Ethics ITRM Solutions Privacy Management Tools	AI TRiSM Data Classification E-Discovery Solutions Privacy Impact Assessments Subject Rights Requests Synthetic Data	Federated Machine Learning Personification	
Moderate	Data Sanitization	5G Network Security Consent and Preference Management Mobile Threat Defense Privacy by Design Sovereign Cloud	Confidential Computing Data Discovery Differential Privacy Format-Preserving Encryption Zero-Knowledge Proofs	
Low				

Source: Gartner (July 2023)

Off the Hype Cycle

- Cloud access security brokers (CASBs) have reached the Plateau of Productivity.
- Cloud data protection gateways have reached the Plateau of Productivity.
- Data discovery and management has been split into data discovery and data storage management services (DSMS). Only the former appears on this Hype Cycle. Data discovery is a foundational capability for supporting a scalable privacy program, whereas DSMS describes an approach for managing an organization's IT infrastructure.
- Influence engineering has been renamed influence AI.
- Secure instant communications have reached the Plateau of Productivity.

On the Rise

Influence AI

Analysis By: Andrew Frank

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

Influence AI is the production of models designed to automate elements of digital experience that guide user choices at scale by learning and applying techniques of behavioral science. Influence AI replaces the previous innovation profile called “Influence Engineering.”

Why This Is Important

Generative AI (GenAI) has shattered preconceptions about the communication limits of AI in general. Marketers are moving beyond efficiency and savings toward more effective uses of content to influence behavior, which we refer to as Influence AI. Mastering these techniques offers disproportionate control over market-shaping consumer choices but carries substantial risks and needs for ethical governance.

Business Impact

Organizations are adapting the foundational models of genAI to marketing’s commercial goals by adding data and analytics to nudge customer choices with relevant content and experiences that guide decisions. Emotion AI, content intelligence and federated learning models are powering new approaches to promotion, pricing, customer experience and product design with positive and negative implications.

Drivers

- **Proof of AI’s persuasive abilities.** Independent research has clearly demonstrated that AI can learn and model persuasive techniques that exploit cognitive biases in human decision making.
- **Acceleration of general AI development.** Although many have called for a pause, there’s no sign that AI developers will slow down as competition and investment build behind the latest technology bonanza.

- **Marketing's lead.** Marketing, with its dependence on communication and content to influence behavior, is the first target and adopter of GenAI products in most organizations.
- **Evolving consumer expectations.** Chatbots and digital people are trending, replacing legacy search prompts in search engines and advancing personalization techniques with more empathic inferences.
- **Adoption pressures.** The public deployment of ChatGPT and other GenAI applications has brought awareness of AI's uncanny abilities to millions globally, putting adoption pressure on organizations.
- **Awareness of risks.** Misuse of AI to produce deepfakes and other toxic content that attacks organizational reputations has become a boardroom concern.
- **ESG pressure.** As corporations face increasing demands to address environmental and societal impacts, success often depends on nudging consumers toward more sustainable and ethically sourced product choices and away from misinformation. The success of investments in more sustainable, healthier products and more equitable business practices is highly dependent on modifications in consumer behavior which can be reinforced with effective nudges by Influence AI.
- **Reactions to data loss.** Pressure is mounting on marketing organizations to deliver better results while losing key data sources such as browser cookies and device IDs. This is driving greater dependence on advanced analytics and content strategy to make up for loss of data.

Obstacles

- **Immaturity and danger.** Approaches to leveraging GenAI with other technologies like emotion AI are still experimental and high-risk.The potential for AI to exploit people's vulnerabilities to encourage bad choices or reinforce destructive behaviors or biases — even if this was not the intention of designers — creates poorly understood moral risks.
- **Popular backlash.** Developers and the press have raised alarms about the many dangers of AI development moving too fast, leading many organizations to take a cautious approach. High-profile blunders, such as accidental leaks of proprietary information, also signal caution. Reactions to perceived manipulative technology have been especially harsh.

- **Legal ambiguities.** Proposed regulations with nebulous scope create new legal hazards for companies contemplating use of AI for influence. The impact of new regulations on providers is also unknown.
- **Lack of skills.** Sourcing expertise needed for advanced applications of AI in marketing remains challenging.

User Recommendations

- Identify an ethicist role in the organization that reports directly to the board before experimenting with Influence AI. Work with them on articulation of guidelines and principles.
- Establish or locate a governance structure within your organization where opportunities for influence AI are best investigated. Discover use cases and debate the goals and extent of potential commitments. Solicit cross-functional representation.
- Recruit user test groups from within and outside your organization for research and experimental projects, or seek providers for such projects. Be transparent about goals and technologies. Assume such research requires informed consent and privacy controls.
- Motivate staff to learn the basics of prompt engineering and other skills needed to build and test GenAI applications. Develop a sense of scope as projects costs and complexity vary widely.
- Build a knowledge center and include assessment of competitors' and platform providers' activities. Play defense as well as offense.

Gartner Recommended Reading

Predicts 2023: AI, Social Toxicity and Disappearing Customers Forge the Future of Marketing

Use Generative AI to Enhance Content and Customer Experience

Board Brief on Generative AI

Beyond the Hype: The Impact of Generative AI on Marketing

Confidential Computing

Analysis By: Mark Horvath, Bart Willemsen

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

Confidential computing is a security mechanism that executes code in a hardware-based trusted execution environment (TEE), also called an enclave. Enclaves isolate and protect code and data from the host system (plus the host system's owners), and may also provide code integrity and attestation.

Why This Is Important

As privacy concerns and fines increase:

- Confidential computing combines a chip-level TEE with conventional key management and cryptographic protocols to enable unreadable computation. This enables a variety of projects where cooperation between different groups is critical, without sharing data or IP.
- The ongoing adoption of public cloud computing and the increased availability and viability of enclave technology allow data to be used in the cloud in a more trusted manner.
- Cross-border transfers are a complex, key component to many businesses, addressed directly by confidential computing.

Business Impact

Impacts include:

- Confidential computing may mitigate one of the major barriers to cloud adoption for highly regulated businesses, sensitive data workloads, or any organization concerned about unauthorized third-party access to data in use in the public cloud. This includes potential access by the infrastructure provider.

- Confidential computing allows a level of data confidentiality and privacy controls between competitors, data processors and data analysts that is very difficult to achieve with traditional cryptographic methods.

Drivers

- Cloud adoption is increasing alongside ongoing concerns regarding potential access to personal data by cloud service providers (CSPs).
- Global data residency restrictions are ongoing, with a need to segment content away from even the CSP with a level of independent assurance.
- Competitive concerns — not just around personal data, but also intellectual property — are spurring the adoption of confidential computing. This includes the need for confidentiality and protection against any third-party access, protection of the method of processing (including algorithmic functions) and protection of the data itself.
- Confidential computing has been mentioned as a viable protection mechanism by several authorities and standards bodies for these specific use cases. Correct implementation will help keep regulatory scrutiny at bay.
- Hyperscaler cloud providers are increasingly offering options that allow virtualized confidential computing, which allows apps to run without recoding or refactoring.

Obstacles

- Complexity of the tech and lack of trained staff or understanding of best implementation methods may hinder adoption and/or weaken deployment (e.g., key management/handling is done incorrectly, unaddressed side channel vulnerabilities).
- Trust is slow to build and quick to evaporate, especially when confidential computing is paired with occasional hardware vulnerabilities.
- Some forms of confidential computing are not usually plug-and-play, and are currently mostly reserved for high-risk use cases such as machine learning. Varying by vendor and technology, you may require a high level of effort but see only marginal security improvement over more pedestrian controls like Transport Layer Security (TLS), multifactor authentication (MFA), and customer-controlled key management services.
- Offerings directly from CSPs vary greatly in robustness, performance and reliability. Not all named confidential computing offers similar protection.
- Confidential computing that leverages cloud-native key management (KM) may be at risk of inadequate privacy because the CSP manages and has access to the keys. Therefore, using third-party KMaaS becomes more important.
- Confidential computing currently only integrates with the client's deployed technology. It is rare to find SaaS or BPaaS vendors offering integration to confidential computing — hence reducing protection choices.

User Recommendations

- Design (or duplicate) a sample application using one of the available abstraction mechanisms and deploy it into an instance with an enclave. Perform processing on datasets that represent the kinds and amounts of sensitive information you expect in real production workloads. This way, you can determine whether confidential computing affects application performance and seek ways to minimize negative results.
- Examine confidential computing for projects in which multiple parties, who might not necessarily trust each other, need to process (but not access) sensitive data in a way that all parties benefit from the common results. None of the parties should control the TEE in this scenario.
- Look for vendors that enable integration to a broader enterprise key management system and complementary encryption and PEC techniques.

Sample Vendors

Alibaba Cloud; Anjuna Security; Fortanix; Google; IBM; Intel; Microsoft; VectorZero

Gartner Recommended Reading

Three Critical Use Cases for Privacy-Enhancing Computation Techniques

Achieving Data Security Through Privacy-Enhanced Computation Techniques

Solution Criteria for Cloud Integrated IaaS and PaaS

Securing the Data and Advanced Analytics Pipeline

How to Make Cloud More Secure Than Your Own Data Center

Data Security Governance

Analysis By: Brian Lowans, Andrew Bales, Joerg Fritsch, Bart Willemsen

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Definition:

Data security governance (DSG) enables the assessment and prioritization of business risks, caused by data security, privacy, and compliance issues. This enables organizations to establish data security policies that support business outcomes and balance business needs against associated business risks. These risks arise from security, data residency and privacy issues, as data is processed across ecosystems or shared with partners.

Why This Is Important

DSG enables the assessment, prioritization and mitigation of business risks caused by security, privacy, and other compliance issues, as data proliferates across on-premises and multicloud architectures. DSG establishes a balance between business priorities and risk mitigation through data security policies that can be applied across the whole IT architecture.

Business Impact

DSG offers a balanced approach to define how data is accessed and used to support business performance objectives and client experience, while enforcing appropriate data security and privacy controls to mitigate risks. DSG requires collaboration among chief information security officers (CISOs), chief data and analytics officers (CDAOs), and business leaders, through a data security steering committee (DSSC). This would help break down communication barriers and contribute toward business outcomes.

Drivers

- It is essential to use DSG as a continuous process to manage, assess and prioritize business risks, and create focused data security policies that can mitigate those risks.
- Data security policies are needed to guide the implementation of consistent data access privileges security controls across a portfolio of datasets.
- DSG must be leveraged to address internal and external requirements to manage user access privileges to each dataset in terms of privacy, confidentiality, integrity, availability, business purpose, and life cycle risks.
- Organizations need to develop processes to create and orchestrate data security policies across multiple independent data security and identity access management (IAM) products, to minimize data security policy gaps and inconsistencies.
- No single product mitigates business risk sufficiently, emphasizing the need for centralized creation and coordination of data security policies.
- It is essential to leverage adequate privacy impact assessments (PIA) through DSG to mitigate data residency and sovereignty risks.

Obstacles

- Business stakeholders have fragmented responsibilities for managing data. Unless they create data security policies together with DSG, they will fail to balance business outcomes and risk mitigation.
- The deployment of data security, IAM and application products are purchased and managed by different leaders.
- Each product applies independent security controls, as IAM products do not control access to data. Data security products often operate on either unstructured or structured data, apply controls to specific platforms, and use custom data discovery technology. This reduces the effectiveness of DSG because it is not possible to deploy consistent data security policies.
- The security team must orchestrate data security policies manually across the portfolio of available security product controls. This also requires regular data risk assessments (DRA) to assess gaps and inconsistencies that need to be reported as stronger business risks, or to support new policies or product deployments.

User Recommendations

- Use DSG to create and manage consistent data security policies across your portfolio of datasets, according to the level of business risks defined.
- Use DSG to analyze business risks and their impacts due to specific security monetization choices, by using infonomics to evaluate the financial impacts on business outcomes.
- Use principles such as Gartner's financial data risk assessment (FinDRA) to establish prioritization of security investment options.
- Ensure cooperation and collaboration between the CDAO and the CISO, to reduce redundancy and waste in evaluating data management and security.
- Apply data security policies across all data security, IAM and application management products that interact with each dataset.
- Consider leveraging the DSSC to reach out to your CIO, CDAO or risk officer to extend your DSG operating model with connected governance. This would help with the most complex, cross-enterprise and geographic risk governance programs.

Gartner Recommended Reading

Use the Data Security Governance Framework to Balance Business Needs and Risks

4 Critical Steps to Accelerate the Adoption of Data Security Governance

Use a Data Security Steering Committee to Realize Data Security Governance Objectives

A Data Risk Assessment Is the Foundation of Data Security Governance

3 Steps to Effectively Capture and Communicate the Business Value of Cybersecurity Initiatives

Sovereign Cloud

Analysis By: Rene Buest, Gregor Petri, Neville Cannon

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Sovereign cloud is the provision of cloud services within a jurisdiction meeting data residency requirements and operational autonomy. It is intended to ensure that data, infrastructure and operations are free from control by external jurisdictions, and protected from foreign government influence and access.

Why This Is Important

The public sector and commercial organizations increasingly depend on cloud services, leading to greater demand for control and autonomy, and hence more offerings to comply with regulations. In many jurisdictions, data residency, data protection and privacy laws are increasing. Laws combined with increasing geopolitical tensions, different economic ideologies, and proliferating cybersecurity risks from a variety of directions, including state actors, are steadily elevating interest in sovereignty.

Business Impact

Concerns about the sovereignty of data, infrastructure and operations hosted in foreign-owned cloud service offerings have led to newly announced sovereign cloud offerings. Legislative mandates are being applied to limit the ability of organizations to use nondomestic vendor services. These impact buying decisions and investments organizations are willing to make in cloud offerings. As a result, end users could find themselves in a fragmented market without access to the resources they need to support their digital business initiatives.

Drivers

- Governments and commercial organizations are becoming increasingly aware of and concerned about their dependence on foreign cloud infrastructure providers and SaaS offerings. Reasons for this are souring of geopolitical relationships, tighter privacy and data protection regulations, data sovereignty, data control and operational autonomy, as well as technological sovereignty and independence.
- The market for digital and cloud technology and services is dominated by U.S. and Chinese technology and service providers. As a result, all non-U.S. and non-Chinese organizations and companies mainly have to access foreign services and technology to build and run digital business models. Hence, data is being stored within nondomestic cloud and digital service providers, which creates political uneasiness.
- As digital services become increasingly important and critical, cloud customers and regional trade bodies worry about retaining control over their data and infrastructure to stay compliant with local regulations as well as their operational autonomy.
- Some more regulated industries and governments are particularly concerned by the U.S. and Chinese legal frameworks that might allow these governments to access cloud-stored data under specific circumstances.
- Businesses increasingly depend on technology platforms they don't control. Although the risk of deplatforming remains small, the growing number of platforms enterprises use and the businesses' growing dependence on platforms increase the consequences of deplatforming.

Obstacles

- In the short to medium term, the market dynamics make it almost impossible for domestic cloud providers to present a viable alternative to hyperscale cloud offerings, as the capabilities of hyperscaler far exceed most domestic cloud offerings. Considerable technical obstacles exist if domestic clouds are expected to deliver the maturity and level of scalability, reliability and functionality of hyperscale offerings.
- Too few skilled engineers exist to replicate the design capabilities of hyperscale cloud offerings to build comparable domestic cloud offerings. With lower levels of skills being available, security and operational maturity will be compromised, potentially leading to greater security and failure risks.
- An increasing number of announcements of sovereign cloud offerings from global cloud providers hit the market, all based on various approaches and delivery models.
- Individual governments each defining their own requirements for sovereign cloud offerings may lead to compliance regimes that break public cloud scale and innovation.

User Recommendations

- Subject proposals for the sovereign cloud to the same level of risk assessment that current cloud computing offerings are subjected to. Do not assume that the sovereign cloud conveys any additional security measures in itself.
- Differentiate between different sovereign cloud approaches by type of workload, data and infrastructure when making cloud deployment decisions. Doing so, classify various delivery models between the cloud provider approaches to meet sovereignty requirements. Make sure to establish a consistent, repeatable and defensible process when assessing sovereign offerings.
- Explore evaluating locally provided cloud services for workflows that can be provided locally and leverage third-party solutions to protect data and ensure it is compliant with local requirements.
- Assess any considered sovereign cloud offerings against long-term viability, also in case legal requirements change or global offerings start to directly cater to national sovereignty requirements.

Sample Vendors

Bleu (joint venture of Capgemini and Orange); Delos Cloud; Google Cloud + T-Systems; Microsoft; Oracle; S3NS; Whale Cloud Technology

Gartner Recommended Reading

What Are the Different Provider Approaches to 'Sovereign Cloud' Demands?

What We Are Hearing About Cross-Border Data Transfers

Product Manager Insight: Three Cloud Deployment Models to Address Your Customers' Key Sovereignty Requirements

Quick Answer: Is the Risk of Relying On the New E.U.-U.S. Privacy Framework Too High for Organizations?

Three Critical Use Cases for Privacy-Enhancing Computation Techniques

Homomorphic Encryption

Analysis By: Mark Horvath, Bart Willemsen

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

Homomorphic encryption (HE) uses algorithms to enable computations with encrypted data. Partial HE (PHE) supports only limited use cases, such as subtraction and addition, but with little performance impact. Fully homomorphic encryption (FHE) supports a wider range of repeatable and arbitrary mathematical operations; however, it worsens performance.

Why This Is Important

HE offers an unparalleled advance in privacy and confidential data processing, although this is largely at the database level. Benefits include the ability to:

- Perform analytics on data while in an encrypted state, so that the processor never sees the data in the clear, yet delivers accurate results.
- Share and pool data among competitors.
- Share all or part of users' data, while protecting their privacy.
- Systems based on lattice encryption, which are quantum-safe.

Business Impact

Even in restricted form (PHE), HE enables businesses to use data, send it to others for processing and return accurate results, without fear it will be lost, compromised or stolen. Any data intercepted by a malicious actor is encrypted and unreadable, even by the coming generation of quantum computers.

Applications include:

- Encrypted search
- Data analytics
- Machine learning (ML) model training
- Multiparty computing
- Securing, long-term record storage, without concerns about unauthorized decryption

Drivers

- The enhanced enforcement of data residency restrictions worldwide is forcing organizations to protect data in use, rather than only when it is in transit or at rest.
- Globally maturing privacy and data protection legislative frameworks demand that more-precise attention be paid to sensitive data. As a result, data pooling, sharing and cross-entity analysis use cases increasingly benefit from forward-looking and sustainable technologies, such as HE.
- Aside from primarily financial use cases (e.g., cross-entity fraud analytics), other industries can benefit as well. One example is the healthcare industry, where analysis of sensitive data across various entities happens often with data protected while in use.
- Solving issues of trust and cooperation with secure multiparty computation (sMPC) will benefit internal and external protection of data.
- The oncoming availability of quantum computing (QC), as highlighted by NIST and the Canadian Forum for Digital Infrastructure Resilience, threatens to compromise the confidentiality of almost all data. This includes digital communication previously considered protected by conventional cryptography. For example, there are signals that malicious actors may retain exfiltrated encrypted data in expectation of the ability to decrypt it years later and re-engage with victims for extortion and ransom demands. Timely adoption of HE in data protection will sustainably protect data, even when previously compromised in (conventionally) encrypted form.

Obstacles

- The application of various forms of HE to daily use cases leads to a degree of complexity, slows operations and requires highly specialized staff.
- The market's unfamiliarity with this technology stands in the way of speedy adoption.
- Although PHE can be a Turing-complete implementation, which means an arbitrary set of instructions could be executed, no vendor has a robust implementation that exploits this capability.
- Some scenarios will never be a good match for HE — for example, those that require security in components beyond analytics and processing, such as production databases and proprietary algorithms.

User Recommendations

- Brainstorm opportunities with your technical and executive teams. For example, come up with a list of five to 10 use cases for HE to improve the adoption of core solutions.
- Treat potential HE projects as experiments, keeping in mind the early stage of the technology's development and the significantly not-real-time nature of HE products. Consider these experiments proofs of concept (PoCs) to build experience, until the technology matures.
- Continue with existing security controls. HE does not necessarily negate the need for other security controls, observance of data residency requirements or access control.
- Assess the core benefits of using HE in combination with other quantum-safe or privacy-enhancing computation techniques.
- Integrate in-use protection via forms of HE into messaging and third-party analytics services.
- Assess the merits of piloting HE by using a vendor's solution, which could offer functionality without the time investment associated with a custom solution.

Sample Vendors

CryptoLab; Duality; Enveil; IBM; Inpher; IXUP; LiveRamp; Lorica; Ziroh Labs

Gartner Recommended Reading

Emerging Technologies: Homomorphic Encryption for Data Sharing With Privacy

Emerging Technologies and Trends Impact Radar: Security

Three Critical Use Cases for Privacy-Enhancing Computation Techniques

What Executives Need to Do to Support the Responsible Use of AI

Achieving Data Security Through Privacy-Enhanced Computation Techniques

5G Network Security

Analysis By: Sylvain Fabre, Peter Liu, Nat Smith

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

5G network security mechanisms improve 4G security with enhancements such as new mutual authentication capabilities, enhanced subscriber identity protection, and addressing new threats from emerging technologies such as cloud-native architecture, network slicing and edge.

Why This Is Important

Securing 5G networks is a priority with the rise of private mobile networks (PMNs) deployments, vertical applications, cloud architecture and massive IoT connections in 5G are creating new vulnerabilities and challenges, such as DDoS attacks. 5G network security provides a unified authentication framework that is both open (e.g., with the support of EAP) and access-network-agnostic (e.g., supporting both 3GPP access networks, and non-3GPP access networks such as Wi-Fi and cable networks).

Business Impact

5G network security provides guaranteed security levels for more demanding applications. For example, the home control feature verifies device location when in a visited network, preventing some spoofing attacks. 5G mitigation against bidding down attacks prevents a fake base station from pretending not to support higher 5G security features (aka IMSI-catcher). Flexible security policies attached to other 5G chargeable features, such as slice as a service and guaranteed low latency, allow for premium security services.

Drivers

- With the wider ecosystem delivering industrial 5G use cases, better security tools that have varying security competencies and credentials are required in order to provide SLAs and service assurance (including end-to-end security).
- It can be part of liability exposure in enterprises looking to deploy private 5G.
- Regulations around user data privacy are increasing.
- Increased scrutiny on 5G infrastructure vendors, and heightened competition between them for perceived security levels, are also driving 5G network security.
- Legacy networks and new bearers such as satellite, as well as devices with lower security capabilities will interconnect with 5G networks, and need to be able to handle such connections safely.
- Cloud-based delivery of 5G network infrastructure and services — including packet core, network slicing and edge computing — requires cross-domain security.
- Demand for edge enterprise solutions will accelerate 5G security adoption.
- 5G service-based architecture (SBA) infrastructure virtualization, automation and orchestration, as well as multivendor solutions, increase risk exposure for CSPs and enterprises.
- CSPs can offer different security options, for example, using slicing.

Obstacles

- 5G end-to-end security presents new challenges many operators are not entirely prepared for, for example, based on some of the 5G hacks on misconfigured containers.
- Some security settings are optional, so implementation security levels may vary between.
- CISOs may not realize the need to secure their on-premises 5G private mobile networks, understand the additional threats in 3GPP-based infrastructure, and rely on their vendors, who tend to focus on performance and project delivery rather than security.
- Supply chain security concerns remain for 5G as open-source approaches add complexity. Not all network components are (yet) known and defense models may have to broaden as implementation progresses.
- Backward compatibility with 4G/LTE means some legacy security issues affect 5G (for example, GPRS Tunneling Protocol [GTP] attacks).
- 5G runs on commodity hardware and containerization, creating a larger attack surface compared to 4G, with most of the 5G hacks that have been demonstrated attacking those areas.
- Deployment scenarios for private 5G have different risk profiles and security needs.

User Recommendations

- Avoid overreliance on 5G security, solve all issues known in 4G and continue ongoing security initiatives, as many of 5G security features are designed to protect the network rather than secure user data.
- Assess and anticipate increased risk of attacks such as DDoS by improving the design of 5G network infrastructure and endpoints, as well as recovery procedures.
- Implement layered DDoS defense by using best-of-breed scrubbing, cloud web application firewall, bot mitigation, DNS protection, ISP and on-premises DDoS appliances.
- Initiate effective mitigation by correlating network traffic, application availability and server performance.
- Complement 5G infrastructure security with distributed AI/ML anomaly detection algorithms for zero days, covering newer domains such as core slicing.
- Implement edge protection concepts used in application security for elasticity, focused on app-layer protection.
- Implement 5G end-to-end security by managing algorithm strength, secret keys negotiation, confidentiality protection, cross-domain slice orchestration and heterogeneous network layers.

Sample Vendors

A10 Networks; Fortinet; Microsoft; Netcracker; Nokia; Palo Alto Networks; SentinelOne; Trend Micro; VIAVI Solutions; ZScaler

Gartner Recommended Reading

Infographic: 5 Steps for Vendors to Scope and Run Successful POCs for Enterprise 5G PMNs

Gartner Attractiveness Index for Private Mobile Networks Technologies

8 Critical Functionalities for Enterprise 5G Private Mobile Network Management and Orchestration

Federated Machine Learning

Analysis By: Ben Yan, Svetlana Sicular, Pieter den Hamer, Mike Fang

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

Federated machine learning aims at training a machine learning (ML) algorithm on multiple local datasets contained in local nodes without the explicit sharing of data samples. Federated ML helps to protect privacy, enables ML and specifically deep neural networks (DNNs) to use more data, resolves data transfer bottlenecks, and empowers collaborative learning for better accuracy.

Why This Is Important

Federated ML (FedML) highlights an important innovation in (re)training ML algorithms in a decentralized environment without disclosing sensitive business information. FedML enables more personalized experiences with local learning in smartphones, softbots, autonomous vehicles or IoT edge devices, and also facilitates organizations to build collaborative learning models across data silos.

Business Impact

FedML enables collaborative ML by sharing local model improvements at a central level, while keeping the data locally. It especially benefits the Internet of Things (IoT), cybersecurity, privacy, data monetization and data sharing in regulated industries. For example, the U.S. Department of Health and Human Services recently reported an average improvement of 16% and a 38% increase in generalization over local models, as a collaboration result of 20 institutes.

Drivers

- The proliferation of privacy regulations requiring protection of local data.
- With the increasing hype around edge AI, the data becomes distributed across multiple, heterogeneous edge devices and clouds. FedML allows organizations to keep the data in place.
- Data volumes are still growing rapidly, making it more challenging to collect and store big data centrally. This is especially pronounced in the IoT scenarios, where sensor data is collected on the devices and often there is no time or reason to pass it centrally.
- Due to scalability issues, excessive power consumption, connectivity and latency, we see a move toward edge infrastructure in the form of FedML.
- Organizations need collaboration with upstream and downstream partners to improve the overall operation efficiency.
- As large language model (LLM) evolves, research on federated LLM emerges so that a group of organizations could collaborate to train LLM together.
- Swarm (federated) learning is emerging as a promising approach in decentralized ML, uniting edge computing, peer-to-peer networking and coordination, enabled by blockchain.
- FedML is often combined with other privacy enhancing computation techniques as complete secured computing solutions.

Obstacles

- Building trust between organizations for collaborative learning models takes time.
- The incentive mechanism needs to be defined and agreed with all parties engaged to keep participants motivated and keep the FedML group in the long run.
- System and data heterogeneity requires a lot of coordination and standardization among systems to be fully functional.
- Enabling FedML requires a complete end-to-end infrastructure stack that integrates capabilities across DataOps, ModelOps, deployment and continuous tracking/retraining, necessitating a high degree of implementation maturity.
- Creating a new, more accurate and unbiased central model from local model improvements can be nontrivial, as the diversity or overlap between local learners and their data may be hard to assess and may vary greatly.
- FedML is still not widely known in the enterprise, as it lacks marketing on the vendor and researcher sides.
- Security and privacy validation concerns require additional steps.

User Recommendations

- Apply FedML to create and maintain decentralized smart services or products, while protecting the privacy of users and preventing the need to centrally collect massive amounts of data.
- Explore FedML use cases with upstream and downstream partners and look for opportunities to improve overall operation efficiency.
- Give a head start to decentral ML applications by deploying a common, centrally pretrained model while still providing personalization and contextualization by locally retraining the model based on local data and feedback.
- Enable continuous improvement of decentralized ML applications with collaborative learning by repeatedly collecting local model improvements to create a new, improved central model and then redeploying it for decentral usage and fine-tuning.
- Keep a central reference model to ensure “cognitive cohesion” across distributed models — that is, by avoiding decentralized models that veer off too far from its original purpose.

Sample Vendors

Alibaba Group; Devron; Ederlabs; F-Secure; Google; Intel; NVIDIA; Owkin; WeBank

Gartner Recommended Reading

Innovation Insight for Federated Machine Learning

Quick Answer: Why Is Federated Learning Prominent in China?

Explore Secured, Accurate and Green AI With Federated Machine Learning

At the Peak

AI TRiSM

Analysis By: Avivah Litan, Jeremy D'Hoinne, Bart Willemsen

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

AI trust, risk and security management (AI TRiSM) ensures AI model governance, trustworthiness, fairness, reliability, robustness, efficacy and data protection. AI TRiSM includes solutions and techniques for model interpretability and explainability, data and content anomaly detection, AI data protection, model operations and adversarial attack resistance.

Why This Is Important

AI models and applications deployed in production should be subject to protection mechanisms. Doing so ensures sustained value generation and acceptable use based on predetermined intentions. Accordingly, AI TRiSM is a framework that comprises a set of risk and security controls and trust enablers that helps enterprises govern and manage AI models and applications' life cycle — and accomplish business goals. The collateral benefit is enhanced compliance with forthcoming regulations, like the EU AI Act.

Business Impact

Organizations that do not consistently manage AI risks are exponentially inclined to experience adverse outcomes, such as project failures and breaches. Inaccurate, unethical or unintended AI outcomes, process errors and interference from malicious actors can result in security failures, financial and reputational loss or liability, and social harm. AI misperformance can also lead organizations to make suboptimal business decisions.

Drivers

- ChatGPT democratized third-party-provisioned generative AI and transformed how enterprises compete and do work. Accordingly, the risks associated with hosted, cloud-based generative AI applications are significant and rapidly evolving.

- Democratized, third-party-provisioned AI often poses considerable data confidentiality risks. This is because large, sensitive datasets used to train AI models are shared across organizations. Confidential data access must be carefully controlled to avoid adverse regulatory, commercial and reputational consequences.
- AI risk and security management imposes new operational requirements that are not fully understood and cannot be addressed by existing systems. New vendors are filling this gap.
- AI models and applications must be constantly monitored to ensure that implementations are compliant, fair and ethical. Risk management tools can identify and eliminate bias from training data and AI algorithms.
- AI model explainability must be constantly tested through model observations. Doing so ensures original explanations and interpretations of AI models remain active during model operations. If they don't, corrective actions must be taken.
- Detecting and stopping adversarial attacks on AI requires new methods that most enterprise security systems do not offer.
- Regulations for AI risk management — such as the EU AI Act and other regulatory frameworks in North America, China and India — are driving businesses to institute measures for managing AI model application risk. Such regulations define new compliance requirements organizations will have to meet on top of existing ones, like those pertaining to privacy protection.

Obstacles

- AI TRiSM is often an afterthought. Organizations generally don't consider it until models or applications are in production.
- Enterprises interfacing with hosted, large language models (LLMs) are missing native capabilities to automatically filter inputs and outputs — for example, confidential data policy violations or inaccurate information used for decision making. Also, enterprises must rely on vendor licensing agreements to ensure their confidential data remains private in the host environment.
- Once models and applications are in production, AI TRiSM becomes more challenging to retrofit to the AI workflow, thus creating inefficiencies and opening the process to potential risks.
- Most AI threats are not fully understood and not effectively addressed.

- AI TRiSM requires a cross-functional team, including legal, compliance, security, IT and data analytics staff, to establish common goals and use common frameworks — which is difficult to achieve.
- Although challenging, the integration of life cycle controls can be done with AI TRiSM.

User Recommendations

- Set up an organizational task force or dedicated unit to manage your AI TRiSM efforts. Include members who have a vested interest in your organization's AI projects.
- Work across your organization to effectively manage best-of-breed toolsets for enterprise-managed AI and applications that use hosted AI as part of a comprehensive AI TRiSM program.
- Avoid, to the extent possible, black-box models that stakeholders do not understand.
- Implement solutions that protect data used by AI models. Prepare to use different methods for different use cases and components.
- Establish data protection and privacy assurances in license agreements with vendors hosting LLM models — for example, Microsoft or OpenAI.
- Use enterprise-policy-driven content filtering for inputs and outputs to and from hosted models, such as LLMs.
- Incorporate risk management mechanisms into AI models and applications' design and operations. Constantly validate reliable and acceptable use cases.

Sample Vendors

AIShield; Arize AI; Arthur; Fiddler; ModelOp; Modzy; MOSTLY AI; Protopia AI; SolasAI; TrojAI

Gartner Recommended Reading

Use Gartner's MOST Framework for AI Trust and Risk Management

Top 5 Priorities for Managing AI Risk Within Gartner's MOST Framework

Differential Privacy

Analysis By: Bart Willemsen

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Differential privacy is an approach to using or sharing data while withholding or distorting certain elements about individual records in the dataset. It uses exact mathematical algorithms that randomly insert noise into the data, and add parameters for distinguishability, closeness and diversity of outcomes at each query. When applied correctly, this prevents the disclosure of identifiable information while ensuring that the resulting analysis does not significantly change informationwise.

Why This Is Important

Concerns continue to exist about privacy and the use of personal data in algorithms to serve content or personalize recommendations. As regulatory measures are employed to prevent unauthorized use of personal data, businesses are looking for ways to protect personally identifiable information while still using the data. One technology that can be deployed to accomplish this is differential privacy.

Business Impact

Business data holds value and much of it is personal data. Regulations that constrain the use of personal data are increasing, and the liability for misusing personal data can be substantial. Businesses need to ensure their reputation reflects a company that protects customer data. There are many techniques to address problems in preserving privacy when training AI models. Differential privacy ensures the privacy of individual rows of data while supporting meaningful analysis of aggregate data.

Drivers

- Differential privacy helps to not only reduce risk but also unlock data for AI that was previously too difficult to access.
- Businesses need to uncover value from data without crossing the boundaries of ethical or regulatory restrictions on the use of personal data.
- It is increasingly likely that more restrictive regulations will be enacted, including on the use of personal data in training of algorithms and on how algorithms handle personal data in turn.
- The risk from sophisticated, state-sponsored bad actors that target theft of personal information to facilitate fraudulent actions, remains on the rise.
- Business reputations and trust can be significantly damaged by information breach or misuse.
- Exposure is not limited to datasets in control of the business, as malicious actors can increasingly combine data sources to reidentify individuals even if the data used by the business is anonymized.
- With differential privacy, source data is not altered because the answer to each query is treated “on the fly,” protecting the data in use while retaining source data integrity.
- With differential privacy, information value is maintained in a controllable manner via a privacy budget, delivering the desired level of anonymity.
- Some providers have started to add collaborative differential privacy capabilities in their offerings for further privacy protections.

Obstacles

- Solutions that reference the use of differential privacy are not always comparable or equally easily implemented.
- Privacy protection solutions use a variety of techniques and they vary in effectiveness. Organizations often lack a framework to consistently determine the appropriate approach based on use-case requirements, technology maturity and fit.
- Most tools cover anonymity in different degrees and focus on the extent to which reidentification can occur. Other deployments add measures to diversity and closeness of outcome, apart from reidentification protection. This can cause confusion in comparison.
- Lack of familiarity with differential privacy — and the skilled staff to effectively deploy and manage it — hinders adoption. This is exacerbated by how jurisdictions define and determine “anonymous” versus “pseudonymous” data differently.
- Lack of transparency around setting of the privacy budget (the extent to which controls are implemented) undermines trust, whereas increased transparency could elevate trust.

User Recommendations

- Explore the use of differential privacy techniques to decrease the likelihood of sensitive data exposure.
- Use a privacy impact or data protection impact assessment to establish whether additional means are necessary and relevant to the use case.
- Compare differential privacy with other privacy-enhancing computation techniques when operating in high-performance environments that require a high level of precision in analytics models.
- Prioritize differential privacy techniques if you’re operating in a highly regulated industry, such as financial services or healthcare.
- Explore differential privacy techniques when using data across regions where privacy regulations may vary, and always be transparent about where you have set the privacy budget.

Sample Vendors

Immuta; LeapYear; LiveRamp; PHEMI Systems; Privitar; Tumult Labs

Gartner Recommended Reading

Three Critical Use Cases for Privacy-Enhancing Computation Techniques

Subject Rights Requests

Analysis By: Nader Henein

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Subject rights requests (SRRs) are a set of legal rights that enable individuals to make demands and, in some instances, changes for clarity regarding the uses of their data. Organizations handling data must address SRRs in a defined time frame. These rights come in three categories — informative, corrective and restrictive. Their execution implicitly requires multiple capabilities of a modern privacy management program, such as personal data discovery, automation and mapping.

Why This Is Important

The percentage of the world's population with access to fundamental privacy rights will soon exceed that with access to clean drinking water. For security and risk management (SRM) leaders in digital enterprises, subject rights management is a standard requirement and a prerequisite for building trust. Vendors in the SRR market provide capabilities that serve organizations in many areas to deliver partial- or full-process automation from initial capture request to response.

Business Impact

The impact of poor or delayed response to SRR is threefold:

- Fines are levied by regulators for failure to comply. These rulings also mandate executing requests without delay.
- Trust between the organization and its customers is eroded. The loss of trust may also prompt requests such as deletion or limitations on processing.
- Long waits for a response negatively impact customer experience (CX) and sentiment.

Drivers

- Organizations must securely and effectively handle their customers' personal data to garner loyalty and avoid fines and litigation.
- Similar to "organic" or "cruelty-free" standards, privacy has become a conviction-based motivator, as individuals are making buying decisions based on how an organization handles their personal data.
- Large multinationals have adopted conviction-based motivators across their core products and supply chain.
- Fear of regulatory fines is the least of some organizations' concerns. Rapid mobilization through social media, followed by a violation of trust, has seen a mass consumer exodus far in advance of regulatory action.

Obstacles

- A sense within the leadership that the organization will not receive enough requests to justify upfront investment in resourcing.
- A degree of automation is needed to address SRRs at scale. It is important to maintain the capacity to respond in a time frame that complies with regulatory mandates and matches customers' expectations.

User Recommendations

- Ensure request fulfillment follows a repeatable and scalable process for compliance and efficiency.
- Nurture customer loyalty and support regulatory compliance by delivering a transparent, user-centric experience for SRR fulfillment.
- Establish the foundational metrics around SRRs. This should include the amount of time it takes to respond to a single request, the cost of a request — often calculated based on the person-hour rate of the team processing SRRs and any other resources involved — and the scale denoting the number of requests an organization can fulfill (given available resources) in the requisite time frame defined by applicable laws. Examples of time frames include 30 to 90 days under the General Data Protection Regulation (GDPR) and 45 to 90 days under the California Consumer Privacy Act (CCPA).
- Propose a level of automation in SRR fulfillment in line with the projected outlay. Identify areas within the response chain that would benefit from improvement.

Sample Vendors

DataGrail; Fair&Smart; IntraEdge; Mine; OneTrust; Osano; Securiti; WireWheel

Gartner Recommended Reading

Market Guide for Subject Rights Request Automation

State of Privacy — Regional Overview Across North America

State of Privacy — The European Union

State of Privacy — China

Synthetic Data

Analysis By: Arun Chandrasekaran, Anthony Mullen, Alys Woodward

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Synthetic data is a class of data that is artificially generated rather than obtained from direct observations of the real world. Synthetic data is used as a proxy for real data in a wide variety of use cases including data anonymization, AI and machine learning development, data sharing and data monetization.

Why This Is Important

A major problem with AI development today is the burden involved in obtaining real-world data and labeling it. This time-consuming and expensive task can be remedied with synthetic data. Additionally, for specific use-cases like training models for autonomous vehicles, collecting real data for 100% coverage of edge cases is practically impossible. Furthermore, synthetic data can be generated without personally identifiable information (PII) or protected health information (PHI), making it a valuable technology for privacy preservation.

Business Impact

Adoption is increasing across various industries. Gartner predicts a massive increase in adoption as synthetic data:

- Avoids using PII when training machine learning (ML) models via synthetic variations of original data or synthetic replacement of parts of data.
- Reduces cost and saves time in ML development.
- Improves ML performance as more training data leads to better outcomes.
- Enables organizations to pursue new use cases for which very little real data is available.
- Is capable of addressing fairness issues more efficiently.

Drivers

- In healthcare and finance, buyer interest is growing as synthetic tabular data can be used to preserve privacy in AI training data.
- To meet increasing demand for synthetic data for natural language automation training, especially for chatbots and speech applications, new and existing vendors are bringing offerings to market. This is expanding the vendor landscape and driving synthetic data adoption.
- Synthetic data applications have expanded beyond automotive and computer vision use cases to include data monetization, external analytics support, platform evaluation and the development of test data.
- Increasing adoption of AI simulation techniques is accelerating synthetic data.
- There is an expansion to other data types. While tabular, image, video, text and speech applications are common, R&D labs are expanding the concept of synthetic data to graphs. Synthetically generated graphs will resemble, but not overlap the original. As organizations begin to use graph technology more, we expect this method to mature and drive adoption.
- The explosion of innovation in AI foundation models is boosting synthetic data creation. These models are becoming more accessible and more accurate.

Obstacles

- Synthetic data can have bias problems, miss natural anomalies, be complicated to develop, or not contribute any new information to existing, real-world data.
- Data quality is tied to the model that develops the data.
- Synthetic data generation methodologies lack standardization.
- Completeness and realism are highly subjective with synthetic data.
- Buyers are still confused over when and how to use the technology due to lack of skills.
- Synthetic data can still reveal a lot of sensitive details about an organization, so security is a concern. An ML model could be reverse-engineered via active learning. With active learning, a learning algorithm can interactively query a user (or other information sources) to label new data points with the desired outputs, meaning learning algorithms can actively query the user or teacher for labels.
- If fringe or edge cases are not part of the seed dataset, they will not be synthetized. This means the handling of such borderline cases must be carefully accommodated.
- There may be a level of user skepticism as data may be perceived to be “inferior” or “fake.”

User Recommendations

- Identify areas in your organization where data is missing, incomplete or expensive to obtain, and is thus currently blocking AI initiatives. In regulated industries, such as healthcare or finance, exercise caution and adhere to rules.
- Use synthetic variations of the original data, or synthetic replacement of parts of data, when personal data is required but data privacy is a requirement.
- Educate internal stakeholders through training programs on the benefits and limitations of synthetic data and institute guardrails to mitigate challenges such as user skepticism and inadequate data validation.
- Measure and communicate the business value, success and failure stories of synthetic data initiatives.

Sample Vendors

Anonos (Statice); Datagen; Diveplane; Gretel; Hazy; MOSTLY AI; Neuromation; Rendered.ai; Tonic.ai; YData

Gartner Recommended Reading

Innovation Insight for Synthetic Data

Innovation Insight for Generative AI

Data Science and Machine Learning Trends You Can't Ignore

Cool Vendors in Data-Centric AI

Case Study: Enable Business-Led Innovation with Synthetic Data (Fidelity International)

Sliding into the Trough

Zero-Knowledge Proofs

Analysis By: Mark Horvath, Bart Willemsen

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Zero-knowledge proofs (ZKPs) are privacy-preserving messaging protocols that enable entities to prove that information available to either or both of them is correct, without the requirement to transmit or share the underlying (identifiable or otherwise sensitive) data. ZKPs enable entities to prove information validity without the requirement to transmit personal or confidential data.

Why This Is Important

Following increasingly imminent digital threats and legislative data protection requirements, security and risk management (SRM) leaders must support use cases that enable digital business while ensuring in-use protection. These protocols limit the requirement for mass decryption/encryption of data elements, which benefits the efficiency of work — including potential adoption of blockchain-based systems.

Business Impact

ZKPs are being applied for many use cases, especially in the context of authentication and transaction verification. Other use cases include payments, decentralized identity, custody management, anti-money-laundering (AML), know your customer (KYC), consumer identity and access management (IAM), age verification, etc. With the addition of ZKPs to blockchain platforms, SRM leaders can cover information security use cases that require confidentiality, integrity and availability (CIA). Some blockchain platforms have evolved to include this.

Drivers

- Traditional data protection techniques typically focus on data in motion (i.e., transport layer security) and data-at-rest encryption. Data-at-rest encryption, as commonly implemented, does not provide strong protection from data theft and privacy disclosures. It is unable to secure data in use and data sharing scenarios.

- New use cases and maturing privacy legislation worldwide present new privacy and cybersecurity concerns that require data-in-use protection. There are also scenarios where the data itself does not need to be shared. ZKPs enable such data-in-use protection.
- Concerns about data security in several scenarios, including collecting and retaining sensitive personal information, processing personal information in external environments such as the cloud and information sharing.
- Privacy violations (due to the exposure of sensitive information).
- Need for mitigation of sensitive data leakage and cyberattacks.

Obstacles

- Even with a variety of web applications (e.g., ZKProof), ZKPs remain in an emerging state. They still require a common framework for applications to leverage.
- Only a limited number of practical implementations have emerged to date.
- The variety of methodologies and the multiplicity of approaches to data management inhibit adoption. ZKPs will need to scale at the rate of blockchain transactional volumes to be effective.
- ZKPs require integration into applications. Downstream applications, such as CRMs and databases, will need some modification.
- Some ZKPs, like ZK-SNARK, have a dependency on existing encryption/hashes (ECDSA in this case) as part of their implementation. This adds a potential complexity in upgrading them to quantum-safe protocols and limits available staff/experts.

User Recommendations

- Work with SRM leaders to gain a deeper understanding of the nature of these controls, understanding that ZKP techniques are a paradigm shift.
- Be realistic with the current immaturity of ZKP solutions and approaches when evaluating ZKP benefits for privacy protection.
- Evaluate how ZKP controls may impact transaction authentication and, ultimately, consumers.
- Assess the impact on the broader information management strategy.

- Assess the architectural implications for using ZKP with different blockchains and distributed ledgers.

Sample Vendors

DropSecure; Evernym; IBM; Ligero; Microsoft; Ping Identity; QEDIT; Sedicii; StarkWare

Gartner Recommended Reading

Three Critical Use Cases for Privacy-Enhancing Computation Techniques

Emerging Tech: Assess Zero-Knowledge Proof Technologies to Strengthen Competitive Advantage in Decentralized Ecosystems

Predicts 2022: Privacy Risk Expands

Top Strategic Technology Trends for 2022: Privacy-Enhancing Computation

Data Breach Response

Analysis By: Nader Henein, Bernard Woo

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Early mainstream

Definition:

Data breach response, augmentation and the associated disclosure are the activities required to assess and notify regulatory authorities and, depending on the impact, the affected individuals when personal data is compromised. Disclosure is mandated by omnibus laws, such as the European Union's General Data Protection Regulation (GDPR), Australia's Notifiable Data Breaches (NDB) scheme, or subject- and region-specific laws, like the individual U.S. state breach notification legislation.

Why This Is Important

Appropriate management of a breach impacting personal data can substantially reduce fines and potentially strengthen ties with affected consumers. It demonstrates that the organization is proactively taking ownership of the situation. However, delayed response, limited transparency and overly legal communications often elicit regulatory investigations, resulting in reputational damage and customer loss.

Business Impact

Data breach response can have a critical impact on an organization's resilience. Breaches often create significant chaos as key executive team members pivot from preexisting priorities to address the reputational, regulatory and likely financial impacts of the breach. Further, newer legislation imposes statutory sentences on company directors for inadequate or negligent handling of personal data.

Drivers

- Modern privacy regulations have raised the bar for data breach notification. When personal data is impacted, disclosure to a supervisory authority within days of discovery is often required.
- In the U.S., all 50 states have breach notification laws in place and many states, such as New York and California, have amended their laws in the past two years. Amendments typically expand the data in the scope of the legislation and the responsibilities surrounding disclosure.
- Regulatory evolution illustrates the need for organizational commitment and resource allocation.
- Organizations must constantly align the technical and operational elements of incident response (IR) with new legal and regulatory requirements.
- Elevating the capacity to disclose a data breach to regulators and potentially affected individuals in an accelerated time frame is something many organizations still need to prepare for.
- Though many organizations are driven by fine avoidance, incidents are bound to happen, and a well-developed response program can pay back in dividends with fine reductions of over 50%.
- An emerging trend is rapid consumer mobilization following an incident. The impact of mass customer exodus, often led by social media, is expected to suppress regulatory fines. Also, it does not offer the organization the option of an appeal through the courts.

Obstacles

- Establishing and testing a data breach program is an expense without an immediate return. It will pay off only if something goes wrong. This often causes the program to be deprioritized in place of more pressing or revenue-generating tasks.
- Data breach service retainers are not commonly available because of the variability and uncertainty of the type of breach, the data involved and the number of records that makes each breach scenario unique.
- Even with a strong program, the time to discover an incident can range from months to years — although it is improving over time.
- Tensions between the general counsel and chief information security officers (CISOs) over limiting information may become available through discovery following an incident. This could negatively impact the organization's capacity to effectively handle a breach.
- Data breach response requires a combination of technical acumens, such as forensics analysis of how the breach occurred, the number and type of records involved, and appropriate remediation. Data breach response must be paired with coordinated organizational processes.

User Recommendations

- Assess whether an incident will trigger regulatory actions. Meet the threshold for a privacy violation.
- Record and maintain the details about incidents (not just violations), as some jurisdictions have stringent record-keeping requirements.
- View data breach response as a multidisciplinary process involving documented procedures and simulated drills, such as tabletop exercises. Doing so will ensure tasks are well-defined and responsibilities are clear. The process should also involve coordination and transparency between various teams and integration into the larger IR training to provide breach disclosure and rapid response requirements.
- Augment your organization's ability to address data breaches in an efficient and timely manner to fulfill regulatory and data-subject disclosure requirements.

Sample Vendors

BigID; BreachRx; Canopy; OneTrust; RadarFirst; Securiti

Gartner Recommended Reading

Toolkit: Cybersecurity Incident Response Plan

Toolkit: Security Incident Response Roundtable Scenario for Privacy

Data Discovery

Analysis By: Michael Hoeck

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Data discovery solutions discover, analyze and classify structured and unstructured data to create actionable outcomes for security enforcement and data life cycle management. Using elements of metadata, content and contextual information, combined with expression- and machine-learning-based data models, data discovery solutions provide actionable guidance and processes to advance data management and security initiatives.

Why This Is Important

Data discovery solutions improve organizations' ability to manage ever-expanding repositories of structured and unstructured data in on-premises, hybrid and cloud infrastructures. They increase visibility of disparate and unorganized sources of information. They enable compliance teams to improve insight into policy adherence and sensitive information, including personal data (PD); and enable security teams to improve visibility of sources of data access risk.

Business Impact

Data discovery solutions can have the following business impacts:

- Accelerate the identification of sensitive data to improve the outcomes of an organization's security controls and privacy initiatives.
- Advance data life cycle management activities by assigning retention policies with data discovery categorization and classification results.

- Reduce business risk through advanced capabilities to eliminate and quarantine sensitive information, and identify data lineage and access permissions issues.

Drivers

- Organizations want to mitigate business risks associated with data processing activities (including data breach, data exfiltration, PD and intellectual property exposure, auditing and regulatory fines), identify sensitive data and implement effective data life cycle initiatives
- There is a need to minimize the blast radius of a cyberattack's access to sensitive information through data classification coupled with security controls, defensible deletion and minimization efforts.
- Organizations want to be able to align and monitor proper data access based on categorization and classification of all data.
- Retention policies can be difficult to establish, refine and consistently enforce without clear data inventory knowledge and awareness of potential sensitive data risk.
- The demands associated with the growing number and complexity of compliance and privacy regulations, such as the EU's General Data Protection Regulation (GDPR), the California Privacy Rights Act (CPRA), Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, and financial services compliance, have greatly increased interest in, and awareness of, data discovery software.
- The potential value of contextually enriched data is capturing the interest of data and analytics teams.

Obstacles

- For its broad set of use cases, capabilities and benefits, funding and budget for data discovery solutions may require a collaborative effort across multiple departments, including security, privacy, compliance, legal and IT teams.
- Successful results of using data discovery software may be affected by a lack of data life cycle management policy buy-in or consensus from key internal constituencies, including executive sponsorship.
- Action-oriented retention policies are required to defensibly delete data identified by data discovery software.
- It can be challenging to get the organization to commit to aligning administrative costs for data discovery solutions and their management with an ongoing business program and investment, rather than a singular project-based activity.

User Recommendations

- Use data discovery software to enable IT, security operations, privacy, compliance and line-of-business (LOB) teams to make better informed decisions regarding classification, data management and content migration.
- Use data discovery software to better grasp the risks of data footprints, including where data resides and who has access to it, and to expose another rich dataset through subsequent classification and content analysis to drive business decisions.
- Develop strong data life cycle management principles by establishing, updating and enforcing retention policies using the information gathered and remediation actions from data discovery software.
- Identify the potential risks of unknown data stored in structured database repositories often associated with applications that enable the storage of free-form text.
- Create data visualization maps to better identify the value of data and the risks to it, including the data owner, using data discovery software.

Sample Vendors

ActiveNav; BigID; Concentric AI; Congruity360; Data443; DataGrail; Netwrix; Securiti.ai; Spirion; Varonis

Gartner Recommended Reading

How to Succeed With Data Classification Using Modern Approaches

State of Privacy: The Privacy Tech Driving a New Age of Data Wealth

2022 Strategic Roadmap for Storage

Market Guide for E-Discovery Solutions

Decentralized Identity

Analysis By: Michael Kelley, Akif Khan, Arthur Mickoleit

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Decentralized identity (DCI) allows an entity to control their own digital identity by using decentralized identifiers (DIDs) to connect and authenticate themselves to other entities. Private keys and verifiable credentials (VCs) are contained in digital wallets, supported by an identity trust fabric for making DIDs discoverable. By establishing trust, privacy and security, DCI is an attractive alternative to traditional models of storing, sharing and verifying identity data.

Why This Is Important

Identity fragmentation is a problem due to service providers (banks, retailers and governments) forcing consumers to create individual identities for every service. DCI offers an attractive approach with increased security, privacy and usability compared to traditional digital identity approaches like federated identity. While legislative efforts to secure privacy and ensure interoperability are multiplying around the world, standards continue to be refined, and DCI use cases continue to emerge.

Business Impact

Users gain greater control of their identities and data, and service providers gain higher trust, speed and confidence. Currently, providers collect huge amounts of identity information about users to increase assurance to an acceptable level. DCI can provide trust, security, privacy and convenience, and can provide portability of identity data for end users without needing centralized data, reducing risks of data breaches, account takeovers and privacy compliance violations.

Drivers

- Vendor investments in DCI: Due to the volume and influence of vendors investing in this space, there is high potential to drive the DCI market forward, and significant investments have been made by IBM, Microsoft and Ping Identity. In addition, Gartner has been tracking more than 80 startups and vendors of DCI technologies and DCI components (e.g., digital wallets and trust fabrics).
- Government activity: Public sectors are increasingly shaping digital identity trends around DCI. The EU, national governments like Finland or Canada, as well as states and provinces like Utah and Ontario are actively pursuing and investing in DCI use cases that span public and private sector interests.
- Privacy regulations: Countries continue to formalize the requirement for user privacy, specifically for collecting and securing large amounts of user data through regulations. DCI provides a more user-centric way of complying with privacy regulations through decentralized user data.
- Client and overall market interest in DCI: Interest is increasing due to attractive elements such as the ability to enable new digital business opportunities while maintaining client privacy. For example, using DCI to share verified claims, such as age/income, employment status, professional credentials, educational credentials without exposing sensitive personal data.
- Standards: Standards are maturing, led by entities such as the World Wide Web Consortium (W3C), the Decentralized Identity Foundation (DIF), the OpenWallet Foundation and OpenID for verifiable credentials to create a consistent approach to DCI. Expanding and maturing standards will help move the market forward.
- User experience: Asking users to repeatedly go through identity proofing and affirmation processes for every online interaction with a service provider is a broken model. Significant friction can be removed from UX if users could assert their identity using a digital wallet with full control over their identity data.

Obstacles

- Authority of issuers: Ensuring that an organization is authoritative to issue a VC (e.g., only an accredited facility issuing educational credentials).
- Adoption: Service providers may resist accepting identity claims via DCI unless they see user adoption, and users may be reluctant to adopt DCI wallets unless they see meaningful use cases for them.
- Interoperability: Adoption is slow due to most development taking place in pockets and a continued lack of standards.
- Technical challenges: Concerns about performance, interoperability, scalability and maturity, as well as wallet standards.
- Regulations: More work is required for how verifiable claims can be used in regulated use cases such as KYC, as required in financial services, online gambling and other industries. Governments are exploring regulatory needs for citizen interactions.
- User interface challenges, ID proofing and account recovery processes are vulnerable for security and privacy, and will require standard approaches.

User Recommendations

- Explore use cases for verifiable claims by identifying tasks and processes that are expensive, complex and time-consuming in the real world, which will benefit from a verifiable claims approach.
- Build a business case for trialing acceptance of DCI by targeting reduced identity proofing and affirmation costs and an improved UX.
- Identify attainable use cases through following successful POCs, such as a DCI solution focused on remote employee onboarding, educational credentials, health credentials and passwordless authentication.
- Partner with existing vendors to understand the possibilities and potential of DCI. Track government activities around use cases for citizen IDs.
- Be cautious of overly optimistic vendor claims. Evaluate the technical security aspects of centralized and partially decentralized identity trust fabrics or using blockchain platforms under consideration. In particular, examine vendor plans for support of standards, such as W3C, DIF and the OpenWallet Foundation.

Sample Vendors

1Kosmos; Evernym; IBM; IdRamp; Microsoft; Nuggets; Ping Identity; Scytale; SecureKey; Wise Security Global

Gartner Recommended Reading

Guidance for Decentralized Identity and Verifiable Claims

Innovation Insight for Decentralized Identity and Verifiable Claims

Predicts 2023: Users Take Back Control of Their Identities With Web3 Blockchain

Top Trends in Government for 2022: Digital Identity Ecosystems

Digital Ethics

Analysis By: Pieter den Hamer, Frank Buytendijk, Svetlana Sicular, Bart Willemsen

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Digital ethics comprises the systems of values and moral principles for the conduct of electronic interactions among people, organizations and things. It applies to areas such as AI, data and analytics, and social media.

Why This Is Important

Digital ethics, especially around topics like privacy, bias, polarization and veracity, is a concern to many. The voice of society is getting louder, with responsible AI coming into sharp focus for individuals, organizations and governments. People, increasingly aware that their data is valuable, are frustrated by lack of transparency, misuse and breaches. Organizations are acting to mitigate ethical risks around data, AI and other digital areas, while more governments are encouraging and regulating responsible use of these in digital society.

Business Impact

Digital ethics strengthens an organization's positive influence and reputation among customers, employees, partners and society. Areas of business impact include innovation, product development, customer engagement, corporate strategy and go-to-market. Intention is key. If ethics is simply a way to achieve business performance, it comes across as disingenuous. The goal to be an ethical organization serves all parties and society more broadly, and leads to better business trust and performance.

Drivers

- The media is frequently featuring high-profile stories about the impact of data, AI and other technology on business and society at large. Board members and other executives are increasingly sharing concerns about the unintended consequences of innovative technology use.
- For many technologies, ethics was often an afterthought. However, with the emergence of artificial intelligence, the ethical discussion is now taking place both before and during a technology's widespread implementation. AI ethics aims to establish responsible use of AI and to harness AI's growing powers.
- The current hype around generative AI, including ChatGPT and similar alternatives, is raising awareness about ethical and legal issues surrounding the veracity and (intellectual) ownership of data, including training data. In addition, the potential impact of inaccurate, misleading or insensitive output is fueling ethical concerns.
- Government commissions and industry consortia are actively developing guidelines for ethical use of AI. Examples include the EU's AI Act, the Netherlands' Fundamental Rights and Algorithm Impact Assessment (FRAIA), and the U.S.'s National AI Research Resource (NAIRR) Task Force and National Artificial Intelligence Initiative to advance trustworthy AI in the U.S.
- Over the past few years, a growing number of organizations declared their AI ethics principles, frameworks and guidelines. Many are in the process of going from declaration to execution.
- Universities across the globe have added digital ethics courses and have launched programs to address ethical, policy and legal challenges posed by new technologies.
- Digital ethics is expanding to address concerns about rising energy consumption. In the case of nonrenewable energy, it is focusing on the carbon footprint of digital technology (particularly, machine learning and blockchain).

Obstacles

- Because of the ambiguous, pluralist and contextual nature of digital ethics, organizations often struggle to operationalize it and expend significant effort to implement best practices.
- Organizations see digital ethics as a moving target because of confusion around society's expectations. An organization's position and beliefs may even steer digital ethics against the majority's opinion.
- Digital ethics is too often reactive, narrowly interpreted as compliance, reduced to a checklist, confined to technical support for privacy protection, and/or viewed only as explainable AI.
- AI ethics is currently the main focus of digital ethics. Supporting technology (e.g., to protect privacy or mitigate bias) needs to mature further and apply to the broader scope of ecosystems rather than singular technologies.
- Across people, regions and cultures, opinions differ on what constitutes "good" and "bad" and what doing the right thing means. Even in organizations that recognize ethics as an important issue, consensus between internal and external stakeholders (such as customers) is sometimes illusive.

User Recommendations

- Identify specific digital ethics issues and opportunities to turn awareness into action.
- Discuss ethical dilemmas from diverse points of moral reasoning. Anticipate and account for ethical consequences. Ensure that you are comfortable defending the use of a technology, including any unintended negative outcomes.
- Elevate the conversation by focusing on digital ethics as a source of societal and business value, rather than simply focusing on compliance and risk. Link digital ethics to concrete business performance metrics.
- Ensure that digital ethics is leading and not following the adoption of new, transformative technology such as AI. Address digital ethics upfront "by design" to create methods that identify and resolve ethical dilemmas as early as possible.
- Organize training in ethics, and run workshops to create ethical awareness within all AI initiatives. These should emphasize the importance of an ethical mindset and clear accountability in AI design and implementation.

Gartner Recommended Reading

Tool: Assess How You Are Doing With Your Digital Ethics

Tool: How to Build a Digital Ethics Curriculum

AI Ethics: Use 5 Common Guidelines as Your Starting Point

How to Manage Digital Ethical Dilemmas

How to Operationalize Digital Ethics in Your Organization

Secure Multiparty Computation

Analysis By: Joerg Fritsch, Bart Willemsen, Brian Lowans

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Secure multiparty computation (SMPC) is a method of distributed computing and cryptography that enables entities (e.g., applications, individuals, organizations or devices) to work with data, while keeping data or encryption keys in a protected state. Specifically, SMPC allows multiple entities to share insights while keeping identifiable or otherwise sensitive data confidential from each other.

Why This Is Important

Security and risk management (SRM) leaders struggle to achieve a balance between data security and privacy when processing (personal) data. This is further complicated by regulations and business objectives. Historically, data protection has focused on securing data at rest and in transit. However, SMPC-based methods introduce data protection in use, much like homomorphic encryption. It supports processing of data confidentially in analytics and business intelligence, using untrusted computing environments.

Business Impact

Due to their reliance on data for artificial intelligence (AI)-based decision making and the sharing of insight from those decisions among multiple parties, SRM leaders need privacy-enhancing approaches to protect data amid an evolving landscape of maturing data protection regulations. SMPC supports the secure enablement of business, enabling organizations to uncover and exchange information, while addressing security and privacy concerns.

Drivers

- Traditional data-at-rest encryption, as commonly implemented, does not provide strong protection against theft and data breaches. It is incapable of securing data in use and data-sharing scenarios.
- SMPC-enabled data security enables the protection of data while in use, providing SRM leaders with another data protection technique. This can be applied to new and existing use cases (e.g., multiparty information sharing).
- New use cases — such as big data analytics, AI or machine learning (ML) model training — present new privacy and cybersecurity concerns that require data-in-use protection.
- Concerns about data security in several scenarios, including collecting and retaining sensitive personal information, are driving SMPC adoption.
- SMPC helps ease fear of privacy law violations (due to the accidental exposure of sensitive information).
- SMPC supports the mitigation of sensitive data leakage, and the overall reduction and mitigation of cyberattacks.

Obstacles

- Commercial SMPC implementations have not reached the end customer traction they could have had because implementations do not frequently match clients' needs. For example, commercial implementations may only be applicable to selected identifiers, or be only practical to protect smaller amounts of data, such as encryption keys.
- Low-end customer awareness or traction for products based on SMPC technologies outside certain niches (e.g., encryption key management or DSaaS for advanced analytics of numerical data).
- When compared with existing techniques (i.e., cryptography based on hardware-generated and stored keys), end customers could have potential issues with audits, like when their accreditation authority is not familiar with SMPC.
- If the obstacles are not addressed successfully to reignite end customer interest, SMPC will most likely head into obsolescence and will need to be removed from the Hype Cycle for data security.

User Recommendations

- Work with developers/architects to establish a high-level position on SMPC relevance and a vision for future adoption, including proofs of concept (POCs).
- Evaluate use cases such as cloud computing, focusing on confidentiality with data in a cloud environment; privacy-enhancing (personal) data analytics initiatives; and cryptographic key protection, including encryption key management initiatives (i.e., for protection of data at rest). Also look at secure and private data mining for data and analytics use cases, including data lake security and blockchain security (e.g., wallet protection and/or quorum-based multisignature operations).

Sample Vendors

Baffle; Cybernetica; Inpher; IXUP; LiveRamp; Nth Party; Ziroh Labs

Gartner Recommended Reading

Three Critical Use Cases for Privacy-Enhancing Computation Techniques

Consent and Preference Management

Analysis By: Tia Smart

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Consent and preference management platforms consolidate end-user choices regarding how their personal data should be handled. Choices are synchronized across legacy, active and incoming repositories, both on-premises and in the cloud. The intent is to extend visibility and control to digital visitors, allowing them to determine and change how much of their data to expose, to whom and for what purpose. This also empowers marketers to respect customers' choices with a minimum of manual overhead.

Why This Is Important

Protections for personal data collected digitally continue to expand across the globe as more countries and U.S. states consider legislation similar to or stronger than GDPR, CCPA, CPRA and CPA. Technologies and organizations must quickly adapt to the global transformation. Consent and preference management platforms (CPMPs) empower organizations to comply with new laws, preserve and extend essential capabilities, and demonstrate to customers and stakeholders that they care about privacy.

Business Impact

- As new legislation is introduced worldwide, organizations must use CPMPs to demonstrate to consumers that they value their privacy and are in compliance to avoid costly violations and consumer mistrust.
- Protecting your organization from compliance violations while maintaining the ability to utilize customer data for business purposes can be technically and operationally challenging. CPMPs help to address these issues.

Drivers

- **New laws and variations in legislation.** With additional countries and regions seeking to implement their own consumer privacy laws, tracking laws in each country and region is a tedious but integral task to ensure compliance. CPMPs address specific requirements, such as auditing websites, enforcing consent choices and making data available for subject rights requests.
- **Reliance on first-party data.** The shift to an increased dependence on first-party data instead of third-party cookies forces organizations to reevaluate the enterprise's data structure. Managing consent and preference choices throughout the ever-convoluted enterprisewide structures takes time, and some CPMPs try to solve this. CPMPs' importance is ever more apparent in countries like the U.S., where implicit consent is still allowed in most states. Organizations need to take a state-by-state approach or risk messing up direct marketing opportunities available to them.
- **Societal norms and consumer expectations.** Consumers now expect to have control over their personal data as well as transparency from organizations on how it is used. However, consent flow banners and dialogues can significantly downgrade user experience, driving the need for better design solutions enabled by certain CPMPs.

Obstacles

- **Ever-changing global laws and best practices.** With regions and countries implementing their own data privacy legislations, organizations must adapt to each one to remain in compliance. CPMPs tend to oversell their ability to make managing consent options simple, often downplaying the complexity of managing an organization's internal and external databases.
- **Lack of UX design support.** Forcing too many privacy choices on consumers degrades UX and leads to high opt-out and abandonment rates. Yet, having too few choices limits the ability to tailor experiences. To strike the right balance requires cross-functional, collaborative activities across the organization.
- **Complex technology architectures.** Digital transformation acceleration efforts propelled organizations to rethink how technology solutions work together and how data flows throughout the ecosystem. Adopters need to factor in the number of connections — both native and customized (e.g., APIs, ETL) — that are needed to effectively use a CPMP.

User Recommendations

- Prioritize consent management policies and initiatives as a critical priority for all functions. Establish a cross-functional customer data and privacy council to review and update policies and processes for the enterprise to follow.
- Avoid “dark patterns” or deceptive language for consent dialogues that attempt to influence users’ choices (see the FTC’s Press Release).
- Use a “telescoping” approach to disclosures and preference dialogues that allow users to go as deep as they choose into specific details. Offer consistent, easy access to preference settings that can be viewed and changed on demand to ensure that you are undertaking a privacy-by-default approach.
- Compare and assess CPMP offerings against your organization’s highest-priority data privacy protection and integration requirements and internal costs.
- Develop a CPMP where the market cannot effectively connect and integrate with legacy internal tools.
- Take a modular approach to adoption and avoid excessively broad project scopes. Anticipate sufficient time to resolve unforeseen complications in these projects.

Sample Vendors

BigID; Didomi; Ketch; OneTrust; PossibleNOW; Syrenis; TrustArc

Gartner Recommended Reading

Market Guide for Consent and Preference Management

Market Guide for Consent and Preference Management for Marketers

Format-Preserving Encryption

Analysis By: Brian Lowans, Joerg Fritsch

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Format-preserving encryption (FPE) protects data at rest and in use, and when accessed through applications while maintaining the original data length and format. It's used to protect fields in a variety of databases and document types on-premises and on public cloud services. FPE is an important anonymization technique to support data protection and privacy compliance requirements and reduces the risks of data residency, hacking or insider threats by controlling access to data.

Why This Is Important

FPE can be used to protect data at the point of ingestion, storage in a database or access through data pipelines. It is deployed to protect data stored or processed across a variety of databases and select document types on-premises or on cloud service platforms (CSPs). However, it is still a blunt-force access control, and, when applied, it will protect data wherever it resides or is accessed.

Business Impact

FPE is widely accepted to address privacy and financial compliance requirements and security threats without having to extensively modify databases or applications. It provides a strong, agile method to prevent unauthorized user access to data on-premises and in public CSPs. This helps organizations meet data protection and privacy regulations and data residency requirements to protect personal, health, credit card and financial data, and to adhere to data breach disclosure regulations.

Drivers

- The national institute of standards and technology special publication (NIST SP) 800-38 standard for FPE using FF1 or FF3-1 mode is widely accepted to support privacy and financial regulations, even though modes FF2 and FF3 have suffered security flaws.
- Adoption is increasing due to the fast-growing need to provide data protection, data residency restrictions, and increasing number of privacy laws across the globe.
- Organizations increasingly want to analyze data, while keeping it anonymized. But some staff will need access to cleartext which is driving the need for FPE to provide business-friendly access controls that leverage augmented data cataloging.
- The ability to mix the implementation of FPE with data masking, and multicloud database activity monitoring (DAM) is also increasing its dynamic adoption for different use cases such as test and development.
- There is an increasing need to deploy FPE with multicloud key management as a service (KMaaS) to provide strong and consistent enterprise key management (EKM) policies to support international privacy and data residency requirements.

Obstacles

- Encryption is frequently not coordinated across all data silos, and organizations struggle to track data flow across their architectures. This will result in clear-text access to sensitive data in other data stores that cannot be secured with FPE.
- Conflict of interest could be an issue; for example, database administrators (DBA) or application owners that have been loaded with security responsibilities without thinking about the proper segregation of duties (SOD) of DBAs from security controls.
- Encryption keys not managed by resilient life cycle best practices and EKM could lead to the loss of larger amounts of data if the encryption keys are lost.

User Recommendations

- Ensure FPE is deployed and managed as part of EKM.
- Deploy FPE FF1 or FF3-1 to implement data security policy rules for user access in coordination with other security controls, according to Gartner's data security governance (DSG) framework.
- Review how FPE interacts with applications, establish whether this can be used to control which user identities are allowed to see the data in clear text, and try to leverage augmented data cataloging to support business access requirements.
- Evaluate the impact on the performance and functionality of applications accessing the database.
- Identify any impacts on application and database functionality, such as search and sorting.
- Monitor and audit all user and administrator access to sensitive data, even when FPE is deployed.
- Augment the data security strategy with DAM, where feasible, to monitor data movement and access behavior when accessed from a database.

Sample Vendors

Baffle; Comforte; OpenText; Oracle; PKWARE; Prime Factors; Protegrity; SecuPi; Thales Group; Titaniam

Gartner Recommended Reading

Use the Data Security Governance Framework to Balance Business Needs and Risks

Use Enterprise Key Management to Provide Stronger Data Security and Privacy

Select the Right Key Management as a Service to Mitigate Data Security and Privacy Risks in the Cloud

Preparing for the Quantum World With Crypto-Agility

Getting the Most Out of Your Investment in Encryption

Personification

Analysis By: Andrew Frank

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Personification allows marketers to deliver targeted digital experiences to individuals based on their inferred membership in a characteristic customer segment without collection or processing of personal data.

Why This Is Important

Digital advertisers' and publishers' continuing struggle with privacy-related compromises in efficiency and accountability is eroding the economic foundations of open web content. Personification techniques are needed to resolve long-standing tensions between privacy and relevance in advertising, and restore diversity and transparency to the media market.

Business Impact

Ad targeting and measurement approaches based on coarse topic-level interest and demographic segmentation have not caught on with marketers. More sophisticated approaches based on persona modeling aim to restore balance and competition among publishers and tech providers. This will lead to a healthier media economy, greater choice, control and accountability for marketers, and better experiences for consumers.

Drivers

- The expansion of privacy laws and platform restrictions has led to a crisis of confidence among marketers in their ability to measure and optimize outbound communications.
- The cost of compliance with an expanding patchwork of varying privacy laws escalates the urgency for a global privacy-safe solution to targeting and measurement.
- Cookie alternatives from Google, the Interactive Advertising Bureau (IAB), and others are adopting variations on the personification theme to balance privacy with effectiveness.
- Technical advances such as federated learning, data clean-room collaboration and privacy-enhancing computation hold promise for personification improvements.
- Businesses with extensive first-party data such as retail, travel and telecommunications are under pressure to find ways to monetize their data without running afoul of privacy regulations or consumer expectations.
- Privacy regulators would like to rein in big tech providers without causing economic damage.
- Platforms and tech providers are actively pursuing personification solutions they hope will take regulatory pressure off their martech and advertising businesses and improve their privacy reputations.
- Productivity gains from generative AI are driving vendors and marketers toward visions of personalized content that require effective targeting to optimize.

Obstacles

- The technical challenges of personification are significant. Profiling and segment inferencing can compromise privacy and consensus is lacking on how much protection or precision is “good enough.”
- Inertia in the current media ecosystem impedes deep shifts in technology.
- Regional fragmentation besets topics in privacy law. Issues of consent and legitimate interest draw conflicting interpretations of legal and ethical boundaries.
- Concerns beyond privacy include bias and exploitation that may emerge as unintended side-effects of opaque segmentation schemes.
- Transparency and control are hard to reconcile with personification techniques. Black box machine learning algorithms conflict with laws requiring explainability.
- Alternatives to personification, such as contextual targeting and consent-based identifiers, have gained followings. More far-reaching concepts, such as decentralized ledger-based identity schemes, could make current approaches obsolete before they reach maturity.

User Recommendations

- Focus data and analytic resources on customer segmentation strategies using experimental design and machine learning to refine persona definitions emphasizing consented, nonpersonal and synthetic data.
- Study or appoint someone to study, report on and engage with Google’s Privacy Sandbox and similar privacy-preserving persona targeting initiatives.
- Reevaluate personalization strategies and designs to minimize personal data requirements while maximizing opportunities for needs discovery, contextual relevance and persona-based creative impact.
- Engage IT and partners in investigating data collaboration innovations enabled by federated learning and other collaborative modeling technologies.
- Deploy segment recognition and decisioning algorithms in client applications and ad units where their inferences can remain private and reported anonymously.

Sample Vendors

Adobe; Analytic Partners; Epsilon; Google; LiveRamp; TransUnion

Gartner Recommended Reading

3 Scenarios for Privacy's Impact on Targeted Advertising

Emerging Technologies: When and How to Use Synthetic Data

Privacy by Design

Analysis By: Bart Willemsen, Bernard Woo

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Privacy by design (PbD) is a set of principles about proactively creating a culture of privacy, by embedding it often and early in technology (e.g., application or customer interaction design), as well as into procedures and processes (e.g., through privacy impact assessments, data minimization and subsidiarity). There is no finite list of principles, yet PbD as a best practice is globally applicable to the basis of any privacy program.

Why This Is Important

Privacy is one of the core tenants for organizations that are seeking to earn trust with their customers and drive increased revenue opportunities. In addition, the number of new or significantly revamped regulations continues to increase worldwide. Organizations can expect to operate more efficiently by adopting PbD and embedding privacy considerations throughout their processing activities.

Business Impact

Privacy must be built-in. A proactive risk-based approach helps enhance consumer trust, prevent violations (such as costly data breaches) before they occur, and reduce the damage from them if they do (such as fines or brand damage). All technology design must account for the protection of any personal data at the core to mitigate privacy risk, which is at unprecedented heights with the current data volumes processed.

Drivers

- Systems must be designed so that the collection of privacy-sensitive data is transparent to the data subject. Some technology-focused ideas for implementing PbD are reducing retention length and amount of personal data (data minimization), working on the original data (rather than on copies) and applying anonymization or pseudonymization where possible, alongside purpose-based access controls (PBAC).
- The need persists to continuously evaluate the risks of reidentification and traceability, and include data location in the considerations for clarity on regulatory impact. Moreover, implementing PbD can lead to other positive changes such as designating a privacy officer with reach or procurement activities for new IT services, and frequently conducting privacy impact assessments.
- PbD and one of its subcomponents, privacy engineering, enable an approach to a business process and technology architecture that combines various methodologies in design, deployment and governance. Properly implemented, it yields an end result with an easily accessible functionality to fulfill the Organisation for Economic Co-operation and Development's (OECD's) privacy principles. It also helps mitigate the impact of a personal data breach by reimagining defense in depth from a privacy-centric vantage point.
- The process involves ongoing recalculation and rebalancing of the risk to the individual data owner while preserving optimum utility for personal data processing use cases. As a result, organizations can rely on the right data being available at the right time with maximized information retention and trust in a compliant operation.
- Stakeholders will also benefit from reducing the data footprint and accompanying breach exposure risk reduction. Further, PbD allows consistent delivery to subjects upon a privacy promise as well as collateral enhanced customer trust and engagement levels.

Obstacles

- Adoption and widespread recognition of PbD has been hampered by a lack of industry-recognized principles and consistent regulatory framework support. The Information and Privacy Commissioner (IPC) of Ontario described seven key elements: proactivity, privacy by default, privacy embedded into design, full functionality, end-to-end security, visibility and transparency, and user centricity. In the U.S., a report by the Federal Trade Commission (FTC) of 2012 is the most visible early support for the PbD principle, yet worldwide standards are not yet being created
- Only over the past few years, legislative requirements start to include "data protection by design and/or by default," implying a PbD approach to all activities. Precedent-shaping rulings are slowly increasing in number and depth. Vendors have added statements like "product X was designed with PbD in mind," sometimes with little reference material to support the claim. Only when privacy is truly a more organic part of the development process, the need for and benefit rating of PbD increase.

User Recommendations

- Tackle privacy by design in manageable steps; a wholesale shift will be too much to handle. Privacy by design is a cultural change about the processing of personal data. This pertains both to existing operations and to innovations.
- Adjust the existing operations through business process reengineering. Especially in innovative developments and new processes, the change begins by asking questions such as: Can we achieve the purpose set out by using less personal data? Can we end the personal data life cycle sooner? Can we provide the same functionality or customer experience without using the identifiable data? Can we adequately protect what we process? Do customers understand what we are processing about them and why?
- Identify use cases where privacy-enhancing computation (PEC) techniques can be adopted to support the embedding of privacy into current and future operational activities.

Gartner Recommended Reading

Use a Privacy Impact Assessment to Ensure Baseline Privacy Criteria

16 Frequently Asked Questions on Organizations' Data Protection Programs

5 Privacy Imperatives for Executive Leaders

Quick Answer: How Can Executive Leaders Manage AI Trust, Risk and Security?

Privacy Impact Assessments

Analysis By: Bart Willemsen

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Privacy impact assessments (PIAs) enable organizations to identify and treat privacy risk. Typically conducted before implementing new processing activities and/or major changes, the PIA starts with a quick scan (looking at the process owner and description, types of data processed for specific purposes, and retention periods per purpose). A full PIA adds legal grounds, potential impact on data subjects, and mitigating measures to ensure a controlled personal data processing environment.

Why This Is Important

An ongoing shift in the regulatory privacy landscape mandates that organizations develop foundational insight into what personal data they process, why and how it is protected. Few organizations have the means to demonstrate insight in and control over personal data across the various repositories and silo types, let alone how they're used or intended to be used. This insight, however, is vital to proportionate and adequate deployment of privacy and security controls.

Business Impact

A PIA improves regulatory compliance, control over personal data throughout the data life cycle, and helps determine access management as well as data end of life following a deliberate intent toward purposefully processing people's data. Assisting in prevention of (internal) data breaches and personal data misuse, it helps security and risk management (SRM) leaders quantify risk to subjects and timely apply suitable mitigating controls. Conducting PIAs frequently and consistently provides a basis for responsible and transparent data management.

Drivers

- PIAs are one of the cornerstones of an effective privacy program. However, many organizations conduct PIAs manually, using spreadsheets and questionnaires. With increasing volumes and the need for repetition of PIAs, a manual approach becomes unmanageable.
- Overstandardization traps the skills needed to conduct PIAs with a few people rather than making them part of an organization's data-handling fabric.
- PIA automation tools allow for (API-driven) triggers to initiate the assessment process, collecting the needed information at every step and tracking it through a predefined workflow all the way until a case is closed or flagged for remediation.
- When done well, the PIA sits at the heart of connecting legal requirements and business process reengineering to practical operationalization in privacy by design and enablement of adequate security control application.
- The results of a PIA will help assess records of processing activities (RoPAs), and through intelligence of data fabric from data and analytics leaders, SRM leaders can further automate the intended personal data life cycle in terms of where it should and should not be available. In other words, the PIA outcome with purpose-based processing activities determines purpose-based access controls (PBAC). In addition, it facilitates automation of the determined data end-of-life moments.
- The entire PIA process eases data governance initiatives to a more controlled state, yet the current main drivers still primarily come from regulatory requirements. Additional frameworks do help, like the 2023 revamped ISO 29134.

Obstacles

- Often considered a tedious task because of poorly conceived manual workflows and a one-size-fits-all mentality, there is a certain PIA fatigue in organizations where this activity has been mandatory for a longer period of time.
- Business partners' view of a checkbox mentality does not help the quality of the PIA.
- Others simply underestimate its relevance and position and do not complete accurate PIAs or fail to frequently keep them updated, making the initial attempt an ultimately futile one.
- PIA automation tools are hard to tailor to an organization's needs in the absence of knowledgeable and trained staff. As a result, even an automated approach fails to fulfill the purpose for subsequent automation and alignment of the personal data life cycle governance or management activities that are ideally connected to the PIA.

User Recommendations

- Appoint and mandate business process owners with responsibility over their respective personal data processing activities, and actively involve them in optimizing the process for fluency and detail.
- Require PIAs to be conducted as a mandatory, frequently reiterated activity. Triage the necessity for PIAs in change processes and the introduction of new processing activities.
- Include the PIA's results — especially from large projects — in the corporate risk register for monitoring and follow-up. Depending on scope and focus, it may also help to integrate high-risk PIA activities to overarching business impact assessments.
- Extend the assessment's effectiveness to processing of personal data carried out by service providers by demanding that they complete and periodically revise a full PIA.
- Use a centrally provisioned tool for consistently conducting PIAs (for example, as an internal automated workflow process), or require the PIA to be conducted as a manual exercise when a less-mature procedure suffices.

Sample Vendors

DataGrail; OneTrust; PrivacyPerfect; RESPONSUM; Securiti; Smart Global Governance; TrustArc; WireWheel

Gartner Recommended Reading

Toolkit: Assess Your Personal Data Processing Activities

Use a Privacy Impact Assessment to Ensure Baseline Privacy Criteria

Ignition Guide to Implementing a Privacy Impact Assessment Process

Climbing the Slope

E-Discovery Solutions

Analysis By: Michael Hoeck

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

E-discovery solutions facilitate the identification, collection, preservation, processing, review, analysis and production of electronically stored information (ESI). ESI fulfills legal and compliance requirements for discovery that result from a variety of judicial and investigative scenarios. E-discovery solutions include software vendor offerings for a customer's own on-premises or cloud deployment, as well as hosted offerings provided by software vendors and services providers.

Why This Is Important

Data growth, new content sources, timely responses to data requests and demands to drive down legal operational costs have made e-discovery solutions essential for organizations. Use cases include litigation, employee and other internal investigations, public records requests, subject rights requests, regulatory demands, and post-data-breach investigations. Highly regulated and litigious industries must especially pay close attention to e-discovery requirements.

Business Impact

E-discovery solutions help by:

- Supporting multiple cases/investigations conducted by enterprises.
- Reducing the overhead associated with managing legal hold notifications and preserving related data.
- Integrating with new discoverable sources such as workstream collaboration and meeting solutions.
- Expanding use cases such as breach investigations and privacy regulation responses.

- Enabling insourcing of e-discovery for faster turnaround and lower cost than using service providers or law firms.

Drivers

- Growing volumes of litigation and internal, administrative and regulatory investigations.
- Accelerating data growth and complexity of data sources, combined with more use cases for e-discovery.
- Increasing emphasis to reduce the cost of legal operations.
- Integration of e-discovery solutions with cloud office solutions simplifies the abilities of legal and compliance teams to directly access, set legal holds and conduct general e-discovery processes.
- Responsibility of legal teams and related e-discovery efforts in response to data breach scenarios.
- Reduced reliance on IT and improved self-service capabilities for legal and compliance users.
- Public sector requirements to manage Freedom of Information Act (FOIA) and Public Records Act (PRA) requests.
- Expanding number of privacy regulations and the related requirement to conduct subject rights requests.

Obstacles

- Legal and IT need to learn to partner with one another for e-discovery technology selection, deployment and ongoing processes.
- Buyers and budgets for e-discovery solutions generally come from different departments in organizations.
- Pricing models for e-discovery solutions are inconsistent and can be complex, lacking the transparency required to properly budget cost.
- The large variety of e-discovery solutions from dedicated software manufacturers and service providers may complicate selection.

- E-discovery technology maturity of legal and compliance teams must be clearly defined before starting the selection process to help narrow the field of vendors to consider.
- The need to fully assess the types of investigations to be performed by in-house staff to properly scope requirements.
- Continued sprawl of discoverable data sources such as the expanded use of digital communication tools (e.g., mobile devices, workstream collaboration and meeting solutions).

User Recommendations

- Improve e-discovery processes by selecting solutions that integrate directly with the most commonly investigated ESI sources, apply in-place legal holds and provide rich review experiences of that data.
- Narrow solution options by aligning the vendor's available deployment architectures, such as on-premises, SaaS, infrastructure as a service (IaaS) or platform as a service (PaaS), and other certifications or authorizations, such as FedRAMP.
- Balance selection of solutions from e-discovery software manufactures and service providers by aligning the legal department skill set to the complexity of e-discovery efforts.
- Fully qualify e-discovery solution costs by engaging with each vendor to obtain a detailed, accurate breakdown of all costs.
- Eliminate multiple solution purchases by creating a cross-functional team of IT and legal personnel.
- Work together with the legal, compliance, IT and security operations teams, with shared responsibility for information governance, e-discovery, data privacy, and security tasks and responsibilities.

Sample Vendors

Consilio; DISCO; Epiq Systems; Everlaw; Exterro; IPRO (ZyLAB); Logikcull; Nuix; OpenText; Relativity

Gartner Recommended Reading

Market Guide for E-Discovery Solutions

Data Classification

Analysis By: Ravisha Chugh, Bart Willemsen, Andrew Bales

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Data classification is the process of organizing information assets using an agreed-upon categorization, taxonomy or ontology. The result is typically a large repository of metadata useful for making further decisions. This can include the application of a tag or label to a data object to facilitate its use and governance, either through the application of controls during its life cycle, or the activation of metadata using data fabric.

Why This Is Important

Data classification facilitates effective and efficient prioritization of data within data governance and data security programs concerned with value, access, usage, privacy, storage, ethics, quality and retention. It is vital to security, privacy and data governance programs. Data classification helps organizations distinguish the sensitivity of the data that they process, promotes a risk-based approach and improves the effectiveness of data protection controls.

Business Impact

Data classification supports a wide range of use cases, such as:

- Implementation of data security controls
- Privacy compliance
- Enablement of purpose-based access controls
- Risk mitigation
- Master data and application data management
- Data stewardship

- Content and records management
- Data catalogs for operations and analytics
- Data discovery for analytics and application integration
- Efficiency and optimization of systems, including tools for individual DataOps

Drivers

- Data classification approaches — which include classification by type, owner, regulation, sensitivity and retention requirement — enable organizations to focus their security, privacy and analytics efforts on important datasets.
- When properly designed and executed, data classification serves as one of the foundations supporting ethical and compliant processing of data throughout an organization.
- Data classification is also an essential component of data governance, as by classifying the data, organizations can establish data retention, data access and data protection policies that can help reduce the risk related to data exfiltration.

Obstacles

- Data classification initiatives have often failed because they were dependent on manual efforts by users with insufficient training.
- Data classification adoption is typically a reflection of the security posture of the organization. If the purpose of data classification is not clearly defined for employees using natural language, engagement in the data classification program is minimized.
- Data classification often fails due to poor communication. Program objectives, policies and procedures should be effectively communicated to all necessary stakeholders to avoid resistance to data classification initiatives.
- Although many vendors offer automated data classification tools that can classify more data more accurately while minimizing user effort, they are not 100% accurate — especially if they use machine learning or artificial intelligence algorithms for which models require ongoing training.

User Recommendations

- To identify, tag and store all of their organization's data, security and risk management leaders and chief data officers should collaboratively architect and use classification capabilities.
- Implement data classification with user training as part of a data governance program.
- Use a combination of user-driven and automated data classification for success in a data classification program.
- Determine organizationwide classification use cases and efforts, and, at minimum, keep all stakeholders informed.
- Combine efforts to adhere to privacy regulations with security classification initiatives. Information can be classification-based by nature (i.e., personally identifiable information, protected health information or PCI information), or by type (i.e., contract, health record or invoice. Records should also be classified by risk category, so as to indicate the need for confidentiality, integrity and availability. Additionally, records can be classified to serve specific purposes.

Sample Vendors

BigID; Concentric AI; Congruity360; Microsoft; Netwrix; OneTrust; SecuritiAI; Spirion; Varonis

Gartner Recommended Reading

Building Effective Data Classification and Handling Documents

Improving Unstructured Data Security With Classification

How to Succeed With Data Classification Using Modern Approaches

Video: What Is Data Classification, and Why Do I Need It?

Mobile Threat Defense

Analysis By: Dionisio Zumerle

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

Mobile threat defense (MTD) protects organizations from threats targeting iOS and Android mobile devices. It provides prevention, detection and remediation for the device, its network connections and its applications. To prevent and detect enterprise threats, such as malware, MTD products use a variety of techniques, including detection based on behavioral analysis. Offerings come from a variety of vendors, including endpoint protection platform (EPP) vendors and stand-alone MTD providers.

Why This Is Important

MTD improves mobile security hygiene by identifying vulnerable devices, malicious apps and networks. It also provides visibility into mobile device behavior that can indicate malicious activity, which can be correlated with other observables and threat intelligence to improve enterprisewide detection and response capabilities. Among other threats, MTD can counter mobile phishing. Financial services and other high-security and regulated industries are the primary adopters of this technology.

Business Impact

- MTD can integrate with an existing UEM deployment for streamlined remediation or can be deployed as a stand-alone tool.
- MTD can provide security assurance for regulated industries, enterprises that need to use a varied and fragmented set of mobile operating system versions, and organizations that choose not to manage the mobile devices to which they provide enterprise access.

Drivers

- Many enterprises deploy MTD to counter advanced and targeted attacks. In practice, MTD provides more traditional security hygiene, such as app vetting and device vulnerability management.
- Protection from mobile phishing is a major driver for adoption. Phishing attacks on mobile devices can circumvent traditional enterprise measures such as email security via SMS and instant messaging applications such as WhatsApp.
- Emerging use cases envisage MTD as a component of zero trust architecture and of an extended detection and response (XDR) system. This is in addition to the use of MTD for mobile phishing protection.
- For unmanaged iOS and Android devices, MTD provides security assurance suitable for BYOD and work-from-home scenarios. When a user launches a work application on a device, the application allows access only when MTD is running on the device. In particular, Microsoft's MAM-WE implementation of this option has gained popularity to enable Outlook and other Microsoft applications on unmanaged devices.
- Endpoint security vendors are expanding their EPP offerings to include support for iOS and Android.

Obstacles

- MTD adoption has been slower than what the mobile security hype purported. The lack of evidence of mobile security issues that have led to major enterprise breaches does not make MTD a priority for enterprises.
- Regulated industries and enterprises with high-security requirements adopt MTD solutions. Among mainstream organizations, MTD product adoption is largely limited to those wanting to improve their overall security hygiene or provide device posture information for bring your own device (BYOD) equipment, rather than those aiming to counter malicious mobile threats.
- Mobile operating systems (especially iOS and iPadOS) limit the visibility and remediation actions that security tools can take on these platforms.

User Recommendations

- Prioritize MTD adoption in high-security and regulated sectors, and in organizations with large or fragmented Android device fleets. Prioritize devices of users that handle sensitive data and those that are frequently mobile.
- Establish a security baseline for mobile devices using UEM before investing in MTD products. Use MTD for app vetting and device vulnerability management to demonstrate immediate benefits, rather than expect them to counter advanced malicious threats or uncover major breaches.
- Integrate MTD with incumbent unified endpoint management (UEM) tools to extend zero trust principles onto mobile devices. Favor the app-based option and leave proxy-based deployment for high-security and business-only scenarios.
- Use MTD products to protect enterprise infrastructure where BYOD policies are in operation, and for other use cases in which devices must stay unmanaged. Emphasize strategic vendor fit over product differentiation, except for high-security contexts and situations with specific mobile security needs.

Sample Vendors

BETTER; BlackBerry; CrowdStrike; Jamf; Lookout; Microsoft; Samoby; Sophos; Tehtris; Zimperium

Gartner Recommended Reading

Market Guide for Mobile Threat Defense

Data Sanitization

Analysis By: Rob Schafer

Benefit Rating: Moderate

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Data sanitization is the disciplined process of deliberately, permanently and irreversibly removing or destroying the data stored on a memory device to make it unrecoverable. A device that has been sanitized has no usable residual data, and even with the assistance of advanced forensic tools, the data will never be recovered.

Why This Is Important

It only takes one data-bearing device falling through a crack in what is otherwise a robust ITAD data security process to find your data for sale on the internet. Robust, consistent and pervasive data sanitization must be a core C-level requirement for all IT organizations, in light of growing concerns about data privacy and security, leakage, and regulatory compliance. Moreover, the ever-expanding capacity of storage media and volume of edge computing and Internet of Things (IoT) devices is compounding this imperative for a consistently robust data sanitization process.

Business Impact

While data sanitization will not necessarily result in increased revenue or cost savings, it will minimize the risk of significant monetary and brand damage that can result from serious IT asset disposition (ITAD)-related data breaches. The benefit rating is moderate, because data sanitization has become an increasingly accepted process to minimize the material business risks of data security.

Drivers

- **Data security compliance:** Regardless of the targeted end state of deinstalled IT hardware, data sanitization or physical hard-drive destruction/shredding are critical activities to ensure compliance with both internal and external privacy and security requirements. These processes are often most effectively and reliably executed by an experienced ITAD vendor. Given the critical risk to your brand that less-than-robust data sanitization processes represent, certification is required that the data was sanitized to common industry standards.

- **Sustainability and the circular economy:** The rapidly growing focus on sustainability, and specifically the circular economy, is driving a shift away from physical destruction to the sanitization/wiping of data-bearing devices. This, in turn, can extend the useful life span of IT assets by 50% to 100%, mitigating up to half their total greenhouse gas emissions.

- **Data sanitization standards and encryption:** Companies are leveraging international standards such as the U.S.-based NIST 800-88 or the U.K.'s ADISA, and requiring NAID's AAA Certification (not just NAID membership) of ITAD service providers. To minimize chain-of-custody security risks (such as loss in transit to the ITAD vendor's facility), many ITAD managers (especially in the financial and healthcare sectors) require that some form of data sanitization be performed on-site. Some that do not require on-site data sanitization will instead enforce data encryption on all data-bearing devices to minimize chain-of-custody security risks.

- **Holistic, pervasive data sanitization:** Comprehensive data sanitization is being applied to all devices with storage components (e.g., enterprise storage and servers, PCs, mobile devices, and increasingly, edge computing and some IoT devices). Lack of robust data sanitization competency is often due to handling asset life cycle stages as isolated events, with little coordination between business boundaries (such as finance, security, procurement and IT).

- **Remote data sanitization:** For mobile devices, a remote data-wiping capability is commonly implemented via a mobile device manager. Although this should not be considered a fail-safe mechanism, its reliability should be adequate for most lost or stolen mobile devices.

Obstacles

- **Complacency:** The "business-as-usual" syndrome: "We've always done it this way and never had a problem." The rapid increase in data security requirements (e.g., General Data Protection Regulation [GDPR], Health Insurance Portability and Accountability Act [HIPAA], and the California Consumer Privacy Act [CCPA]) dictate a thorough (annual) review of data security and sanitization processes.
- **Cost:** Robust data sanitization is costly compared to the many lower-cost "trust me" alternatives (e.g., the "friend" who promises his processes are robust). Remember: This is about the integrity of your brand in the market.
- **Lack of executive awareness and focus:** Too often, C-level executives confidently say they have world-class data sanitization processes in place, yet haven't had a thorough review/audit of those processes in several years. Large organizations may well have a robust, disciplined data sanitization process in place, but in certain remote locations those processes may not be consistently enforced.

User Recommendations

- Follow an IT risk management life cycle approach that includes explicit, documented decisions about data archiving, sanitization, and device reuse and retirement.
- Collaborate with data sanitization stakeholders (e.g., IT, security, privacy, compliance, legal, IT asset managers) to create appropriate end-to-end data sanitization standards and processes, based on data sensitivity, for all data-bearing devices.
- As different media require different sanitizing methods, ensure that your internal IT organization or external ITAD vendor provides a certificate of data destruction to your security standards (e.g., NIST 800-88).
- Assess and minimize the security risks of portable data-bearing devices (e.g., mobile assets, USB drives, IoT devices).
- For externally provisioned services (e.g., SaaS, IaaS, PaaS), analyze end-of-contract implications and data-exit processes, and request that providers supply their data destruction, storage reuse and recycling practices and certifications.

Sample Vendors

Blancco; Iron Mountain (ITRenew)

Gartner Recommended Reading

Market Guide for IT Asset Disposition

Market Guide for Mobile Threat Defense

Privacy Management Tools

Analysis By: Bart Willemsen

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

Privacy management tools help organizations facilitate compliance insights and check processing activities against regulatory requirements. They bring structure to privacy processes and workflows, enhance insight into data flows and governance maturity, and monitor and track the privacy program's maturity progression.

Why This Is Important

The increasing maturity of data protection legislation globally forces organizations to maintain awareness and control of personal data processing operations. Roughly two-thirds of jurisdictions worldwide have requirements similar to the EU's trendsetting GDPR in place. They range from U.S. state laws like the CCPA or the CPRA to national initiatives like Brazil's LGPD and China's PIPL. The differences in detail across requirements make managing compliance overviews manually almost impossible.

Business Impact

Privacy management tools give business leaders oversight and accountability about handling personal data, and enable transparency and control over those activities. They contain audit capabilities to demonstrate compliance especially across multiple jurisdictions. Point solutions are more and more integrated into suites to account for an increasingly automated enablement of a privacy UX, vendor risk management, records of processing activities (ROPAs), data intelligence inventories, and more.

Drivers

- In almost all cases, passed or proposed privacy laws have been heavily influenced by the GDPR. Therefore, they are introducing concepts such as subject rights, explicit consent and timely breach disclosure. Regulatory changes are likely to continue over the coming two to three years, establishing the fundamental basis for privacy at the legislative level.
- Individuals' awareness and demand for privacy continue to rise, often through confrontation with a widespread use of new technology. Amid these ongoing pressures, organizations must adapt their privacy programs to allow better scale and performance while staying within budgets that are still tight. They should do so without exposing the business to loss through fines or reputational damages.
- The privacy landscape is becoming increasingly complex. Gartner estimates that by 2025, 75% of the world's population will have its personal data covered under modern privacy regulations. Even further, we calculate that by that time over 80% of organizations worldwide will face modern privacy and data protection requirements. Fundamental capabilities carrying even an immature privacy program include those for ROPAs, privacy impact and compliance assessments, several elements of the privacy UX and incident or data breach management.
- To implement a consistent and holistic privacy program, organizations require two sets of capabilities — privacy management capabilities and data-centric control capabilities. Some organizations opt to tackle data issues first: discovery, classification, authorization and access controls, and operationalizing end of life.
- Finally, an in-control privacy-first posture as well as transparency and control over personal data processing activities are simply good for business. They enhance brand protection, customer trust and represent an ethical approach to data and the people behind that data.

Obstacles

- After time, a sense of “good enough” can lead to delays in adoption of privacy management tools, or worse, an absence of (automated) integration to reap the maximum benefit.
- On the other hand, some organizations already have point solutions for privacy UX components, data breach response or impact assessments in place. They might overlook opportunities for more mature complementary capabilities in an integrated suite. Attempts to integrate loose components from various vendors can often be disappointing, if only remaining manual workload is considered.
- Ongoing developments, including the “shift-left” movement where certain capabilities are automated at a code level, are often technical in nature. This hinders adoption even when they could ultimately increase immediate and long-term benefits.
- As the absence of immediate sanctions or investigations makes pressure seem to subside, some organizations continue to take a wait-and-see approach and rely on a set of unmanageable practices.

User Recommendations

- Incorporate the demands of a rapidly evolving privacy landscape into the organization’s data strategy by developing a common baseline driven by applicable regulatory guidelines and privacy frameworks available.
- Maintain a focus on overarching capabilities with relevance across the board, including privacy impact assessments (PIAs), ROPAs, consistent vendor risk management and a people-centric privacy UX.
- Accept, adapt and evolve with the new business challenges and needs to privacy by leading with a cost-optimized set of privacy capabilities.
- Assess the extent to which privacy management tools fit the organization’s criteria for standardization needs. For example, they can help in certification preparations against the EuroPriSe framework, ISO 27701, or aligning with others like the NIST Privacy Framework, cloud codes of conduct, etc.

Sample Vendors

DataGrail; Ketch; OneTrust; RESPONSUM; Securiti; TrustArc; WireWheel

Gartner Recommended Reading

State of Privacy — The European Union

State of Privacy — China

State of Privacy — Regional Overview Across North America

5 Privacy Imperatives for Executive Leaders

Entering the Plateau

ITRM Solutions

Analysis By: Sema Yuce, Michael Kranawetter

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

IT risk management (ITRM) solutions operationalize the risk management life cycle. Their main use cases are IT risk and control assessment; regulatory, industry and policy compliance; U.S. federal assessment and authorization; and cyber-risk management. ITRM solutions have core capabilities ranging from workflow management, risk analysis, reporting and digital asset discovery to data integrations and third-party connectors. ITRM is a capability of governance, risk and compliance (GRC) software.

Why This Is Important

The ITRM market maturity level has reached mainstream with the necessity to manage risk from an integrated perspective. With a clear focus on GRC-related processes and security risk exposures, buyers have maintained interest in ITRM, though attention has started shifting toward emerging, specialized cyber-risk management solutions, Many organizations use ITRM solutions to manage technology risk, typically with a business and enterprise risk context.

Business Impact

ITRM solutions provide cost savings by replacing manual coordination of risk and compliance governance in the digital environment. They track deviations against standards and facilitate monitoring risk indicators. Buyers align data with cyber-risk initiatives or adopt dedicated cyber-risk management solutions. ITRM is integrated as a capability within GRC or enterprise risk management (ERM) solutions, simplifying risk reporting and enhancing decision making for the board and senior management.

Drivers

- Ongoing business transformation initiatives have put the spotlight on IT operational dependencies, alongside wider digitisation initiatives.

- Organizations using ITRM solutions to manage more than IT compliance risk and governance are shifting attention to emerging ones such as cyber-risk management solutions.
- The prioritization of business context aligns with a steadily increasing maturity in the risk management discipline, leading to a strong integration of IT risk into enterprise risk management solutions.

Obstacles

Key obstacles for the adoption of ITRM solutions include:

- Balancing between immediate needs and mid- to long-term requirements as buyer organizations scale.
- A lack of process definition and an updated asset and process inventory.
- Not knowing what is the best value in using automation.
- Risk workflows or technical data consolidation.

User Recommendations

- Ensure your processes have reached a level of sufficient maturity as a buyer before looking to automate them through adoption of technology, as it often causes more confusion and loss of investment.
- Select vendors based on their ability to scale and flex with your risk management journey.
- Include in your prework to deploy ITRM solutions the labor associated with populating asset, process, risk and control repositories. This is significant.
- Generate interest in ITRM/GRC solutions to automate risk-related activities, as they combine vendor risk, corporate compliance, operational risk or audit management solutions with other risk and compliance activities. The main advantage of this is the integration of risk data, workflow and dashboards as well as different risk managers from different parts of the organization.

Appendixes

See the previous Hype Cycle: Hype Cycle for Privacy, 2022

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 2: Hype Cycle Phases

(Enlarged table in Appendix)

Phase	Definition
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the innovation's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the innovation are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the innovation to reach the Plateau of Productivity.

Source: Gartner (July 2023)

Table 3: Benefit Ratings

Benefit Rating ↓	*Definition* ↓
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (July 2023)

Table 4: Maturity Levels

(Enlarged table in Appendix)

Maturity Levels	*Status*	*Products/Vendors*
Embryonic	In labs	None
Emerging	Commercialization by vendors Pilots and deployments by industry leaders	First generation High price Much customization
Adolescent	Maturing technology capabilities and process understanding Uptake beyond early adopters	Second generation Less customization
Early mainstream	Proven technology Vendors, technology and adoption rapidly evolving	Third generation More out-of-box methodologies
Mature mainstream	Robust technology Not much evolution in vendors or technology	Several dominant vendors
Legacy	Not appropriate for new developments Cost of migration constrains replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (July 2023)

Document Revision History

Hype Cycle for Privacy, 2022 - 2 August 2022

Hype Cycle for Privacy, 2021 - 13 July 2021

Hype Cycle for Privacy, 2020 - 23 July 2020

Hype Cycle for Privacy, 2019 - 11 July 2019

Hype Cycle for Privacy, 2018 - 17 July 2018

Hype Cycle for Privacy, 2017 - 20 July 2017

Hype Cycle for Privacy, 2016 - 20 July 2016

Hype Cycle for Privacy, 2015 - 24 July 2015

Hype Cycle for Privacy, 2014 - 18 July 2014

Hype Cycle for Privacy, 2013 - 31 July 2013

Hype Cycle for Privacy, 2012 - 25 July 2012

Hype Cycle for Privacy, 2011 - 25 July 2011

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Understanding Gartner's Hype Cycles

Tool: Create Your Own Hype Cycle With Gartner's Hype Cycle Builder

Top Trends in Privacy Driving Your Business Through 2024

Market Guide for Subject Rights Request Automation

State of Privacy — The European Union

State of Privacy: The Privacy Tech Driving a New Age of Data Wealth

Table 1: Priority Matrix for Privacy, 2023

Benefit ↓	*Years to Mainstream Adoption*			
	Less Than 2 Years ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓
Transformational		Decentralized Identity	Data Security Governance Homomorphic Encryption Influence AI	
High	Data Breach Response Digital Ethics ITRM Solutions Privacy Management Tools	AI TRiSM Data Classification E-Discovery Solutions Privacy Impact Assessments Subject Rights Requests Synthetic Data	Federated Machine Learning Personification	
Moderate	Data Sanitization	5G Network Security Consent and Preference Management Mobile Threat Defense Privacy by Design Sovereign Cloud	Confidential Computing Data Discovery Differential Privacy Format-Preserving Encryption Zero-Knowledge Proofs	
Low				

Source: Gartner (July 2023)

Table 2: Hype Cycle Phases

Phase	*Definition*
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the innovation's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the innovation are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the innovation to reach the Plateau of Productivity.

Phase ↓	Definition ↓

Source: Gartner (July 2023)

Table 3: Benefit Ratings

Benefit Rating ↓	Definition ↓
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (July 2023)

Table 4: Maturity Levels

Maturity Levels ↓	*Status* ↓	*Products/Vendors* ↓
Embryonic	In labs	None
Emerging	Commercialization by vendors Pilots and deployments by industry leaders	First generation High price Much customization
Adolescent	Maturing technology capabilities and process understanding Uptake beyond early adopters	Second generation Less customization
Early mainstream	Proven technology Vendors, technology and adoption rapidly evolving	Third generation More out-of-box methodologies
Mature mainstream	Robust technology Not much evolution in vendors or technology	Several dominant vendors
Legacy	Not appropriate for new developments Cost of migration constrains replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (July 2023)