Gartner®

Hype Cycle for Public Safety and Law Enforcement, 2023

Published 25 July 2023 - ID G00796458 - 105 min read

By Analyst(s): Michael Brown, Bill Finnerty

Initiatives: Government Verticals Digital Innovation and Application Modernization

This Hype Cycle provides insights relative to risk and rate of adoption for a range of technologies and approaches in public safety and law enforcement. Government CIOs can use this research to make informed decisions about the timing of investments to support their digital strategy.

More on This Topic
This is part of an in-depth collection of research. See the collection:

- 2023 Hype Cycles: Deglobalization, AI at the Cusp and Operational Sustainability

Analysis

What You Need to Know

The role of the CIO as a strategic partner has never been more important to public safety and law enforcement (PS&LE) organizations and the constituents they serve. Gartner data shows that 84% of public PS&LE respondents expect digital capabilities to drive operational excellence, and 60% expect an increase in their IT budgets. [1]

The PS&LE operational environment presents challenges, such as extremely competitive employment markets, and opportunities, like the surge of innovation at the peak of this Hype Cycle. [2] This Hype Cycle provides a tool that CIOs, executives and program leaders can use to understand the relative maturity of emerging technologies to adapt strategic plans and achieve their mission. For example, a public safety organization working to improve recidivism through intelligent integrated justice (see Justice and Law Enforcement Vision 2022: Intelligent Integrated Justice) would benefit from reviewing the data fabric profile in this Hype Cycle.

The Hype Cycle

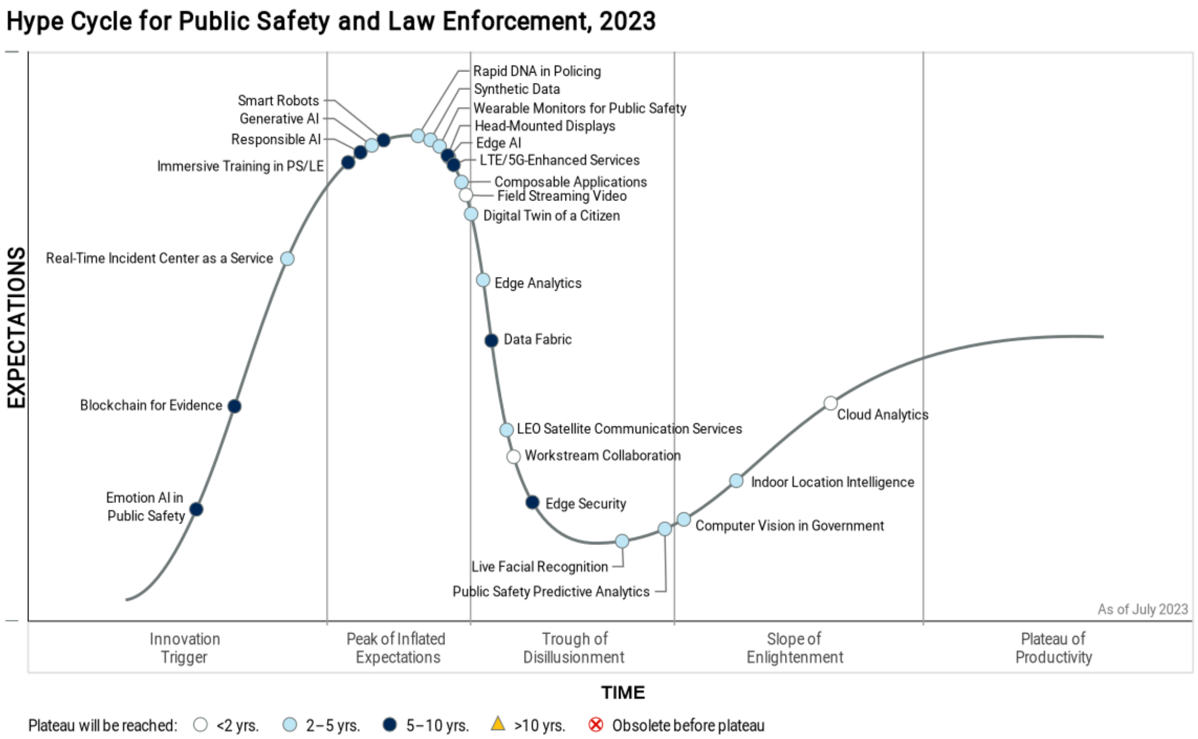
Gartner's PS&LE Hype Cycle is one of four 2023 Hype Cycles focused on government, with the Hype Cycle for Digital Government Services, Hype Cycle for Smart City Technologies and Hype Cycle for Human Services in Government. There are synergies among this research. CIOs leading jurisdictionwide efforts or partnering with other organizations should review all four for opportunities to collaborate on developing value for constituents.

The innovations selected here can aid CIOs in making choices relative to risk and investment strategy, as well as prepare for the implications of postdigital government. For example, a policing agency focused on intelligent situational awareness might consider edge analytics, field streaming video and a real-time incident center as a service. If this same agency has a conservative risk tolerance, it may consider that, of those three innovations, field streaming video is more mature and has a shorter time to reach the Plateau of Productivity. Therefore, it might seek solutions using that technology instead of others with greater risk.

A number of innovations adopted from other Gartner Hype Cycles have a PS&LE impact:

- **Synthetic data** mimics patterns without exposing original data, addressing the inability to use original datasets for privacy, security and concerns of bias.
- **Workstream collaboration** enables digital workplace efforts and promotes collaboration between PS&LE agencies and the public.
- **Edge AI** supports PS&LE organizations for real-time decision making through greater use of the Internet of Things (IoT), computer vision, machine learning and analytics in the field.
- **Smart robots** provide operational advantages as a force multiplier.
- **Digital twin of a citizen** can model the impact of programs on residents, those in custody or PS&LE employees, providing opportunities for empathy-driven approaches.
- AI has tremendous potential to improve how PS&LE organizations conduct their mission, especially the surge of **generative AI,** but entails **responsible AI** practices.

Figure 1: Hype Cycle for Public Safety and Law Enforcement, 2023



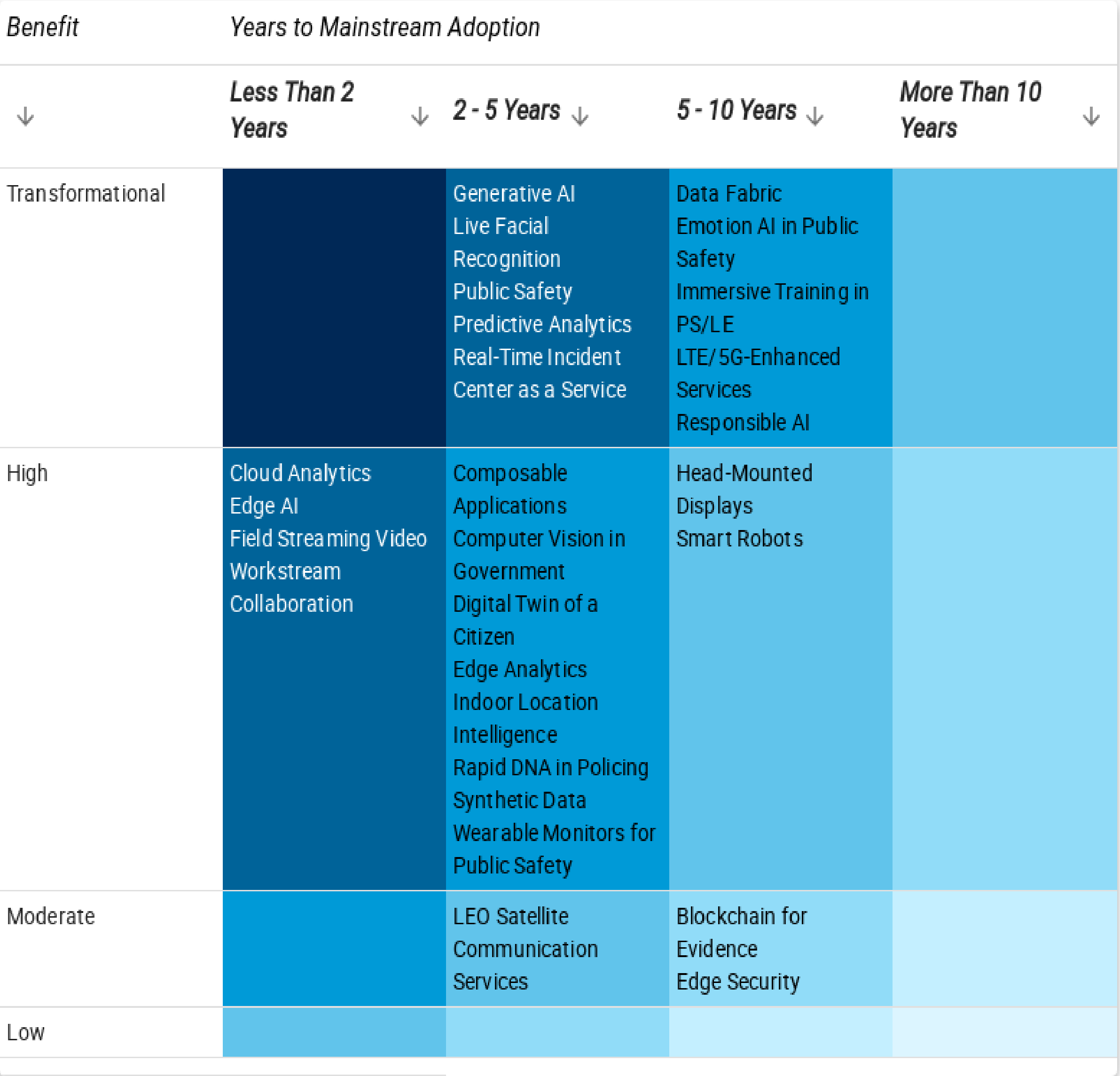
The Priority Matrix

The Priority Matrix shows the technologies mapped to the time frame by which they are expected to mature into mainstream adoption and deliver benefits, and the benefits that can be expected. For PS&LE agencies with both readiness and urgency in their digital government journey, transformational or high benefits can accrue immediately from the use of technologies in the upper-left section of the Matrix. If these technologies and approaches align with strategic initiatives, they should be considered for near-term investment. Those with similarly significant benefits, but in a less-mature state, present strategic opportunities, but should be approached more cautiously. Anticipate changing market dynamics and changing dominant players for technologies with longer times to mainstream adoption.

For example, rapid investments in technologies that accrue immediate benefits, such as cloud analytics or indoor location intelligence, should be viewed as quick wins. Conversely, solutions such as smart robots and blockchain for evidence involve complexity and are more immature, extending time to value. As with the Hype Cycle, the placement of these technologies within the Priority Matrix will vary by geography, vertical and tier of government, particularly with respect to their potential benefits assessment.

Table 1: Priority Matrix for Public Safety and Law Enforcement, 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		Generative AI Live Facial Recognition Public Safety Predictive Analytics Real-Time Incident Center as a Service	Data Fabric Emotion AI in Public Safety Immersive Training in PS/LE LTE/5G-Enhanced Services Responsible AI	
High	Cloud Analytics Edge AI Field Streaming Video Workstream Collaboration	Composable Applications Computer Vision in Government Digital Twin of a Citizen Edge Analytics Indoor Location Intelligence Rapid DNA in Policing Synthetic Data Wearable Monitors for Public Safety	Head-Mounted Displays Smart Robots	
Moderate		LEO Satellite Communication Services	Blockchain for Evidence Edge Security	
Low				

Source: Gartner (July 2023)

Off the Hype Cycle

Machine learning was removed from the Hype Cycle for 2023 to accommodate the addition of Generative AI. While machine learning and a number of other AI techniques remain applicable to PS&LE agencies, Generative AI has burst into public awareness with large language models, such as ChatGPT. Like other elements of government, Gartner has observed considerable interest by PS&LE agencies in the possibilities that Generative AI holds.

On the Rise

Emotion AI in Public Safety

Analysis By: Bill Finnerty

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

Emotion AI, also referred to as affective AI, uses AI to analyze the emotional state of a user via computer vision, audio/voice input, sensors or software logic. In public safety and law enforcement, emotion AI can analyze individuals' risk factors, including stress, anger and anxiety. The systems can then initiate preventative steps to reduce risks and improve individual safety and wellness.

Why This Is Important

Proactive engagement by public safety and law enforcement (PS/LE) with those in care, custody or on duty can be the difference between good or bad outcomes in difficult situations. The cost of these situations going badly is too high not to use technology to make improvements. PS/LE are increasingly using video, audio and wearable Internet of Things (IoT) devices, providing a plethora of data that emotion AI can analyze to proactively engage with people to improve outcomes.

Business Impact

In many parts of the world, the use of emotion AI by PS/LE is nascent. Some governments, such as in the U.K., UAE and China, have experimented or are experimenting with emotion AI,. The potential value for PS/LE if the technology matures and is accepted is quite high and can save lives. Information from these solutions could be used as part of early intervention for both wellness and accountability and could assist in detecting risks of suicide, violence and stress.

Drivers

Drivers for the use of emotion AI by PS/LE include:

- Reducing disruption to the personal lives of officers and staff related to increased stress, career challenges, healthcare costs and replacement costs.

- Reducing costs related to healthcare, personal leave and retention and improving the lives of staff as part of early detection and intervention.

- Answering societal demands for proactive action to ensure just and equitable treatment of those engaged with PS/LE.

- Increasing the availability of real-time data from the adoption of streaming video and audio, and wearables.

- Positively impacting the lives of those on duty and those receiving care or in custody through proactive intervention, rather than a reactive approach.

- Meeting data security and privacy standards for health and law enforcement through technology advances, including the adoption of cloud and AI as a service.

Obstacles

- The cost of investing in emotion AI for behavioral and sentiment analysis at scale can be seen more as an insurance policy, rather than a proactive tool to assist staff and those in care and custody.

- Officers are often concerned that new technical solutions to intervention will impact privacy and careers, so the adoption of emotion AI will be met with the same skepticism.

- Public concerns about the accuracy of and bias in emotion AI will present challenges to adoption. If the technology matures to an adequate level of accuracy, then industry and public leaders will need to overcome concerns of bias through engagement and transparency.

- The vendor adoption rate of emotion AI will be driven by market demand and require the introduction of new capabilities or partnerships. In a relatively conservative sector of government, the push for this capability may lag.

User Recommendations

Government CIOs supporting PS/LE organizations must:

- Work with leadership and human resources to proactively engage and educate the workforce in establishing acceptable use of emotion AI, including requiring interpretable AI models.

- Establish a public working group on the use of emotion AI in conjunction with executive leadership and community engagement leads.
- Engage vendors to understand roadmaps and partnerships that may enable the use of emotion AI with video management, IoT platforms, program management systems and early intervention systems.
- Establish an enterprise integration and orchestration strategy to ensure that emotion AI solutions can easily access data from video, audio, IoT and other sources.
- Pilot emotion AI with fully interpretable models using tree-based algorithms or similarly explicit techniques that allow an understanding of the models' results. As vendors are able to demonstrate positive outcomes, start to share these examples with stakeholders to be transparent and thoughtful in preparing for adoption.

Blockchain for Evidence

Analysis By: Michael Brown

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Blockchain services use distributed ledgers to ensure the integrity of digital information. Blockchain technology maintains a history of records that cannot be altered or tampered with. This immutable characteristic of a digital record is applicable to the management of evidence collected during investigations and used in subsequent court proceedings.

Why This Is Important

Digital evidence has become ubiquitous in law enforcement and court proceedings. It is essential for the administration of justice to preclude tampering and ensure the chain of custody for that evidence. It is also a requirement that digital evidence be shared with various actors in the public safety ecosystem. Blockchain and other distributed ledger technologies offer an opportunity to preclude tampering, maintain chain of custody, and widely, selectively and securely share digital evidence.

Business Impact

A shared system for authenticating digital evidence is a transactional enabler among stakeholders in the law enforcement and judicial system. Blockchain technology, which has been shown to be effective in some use cases, has growing judicial support. Present technology often requires granting access to whatever unique systems each policing agency may use. Shared blockchain evidence authentication systems can allow multiple modes of information transfer with universal validation against shared hash values for the data files.

Drivers

Use of blockchain for digital evidence is being driven by:

- **A diverse marketplace.** The market for digital evidence management products has many providers, each with a unique approach, which can create a more complex and challenging user experience. Stakeholders at national and regional levels may have to establish accounts in multiple systems with differing user experiences. Consequently, the authentication of digital evidence requires a unique legal explanation for each system. This complexity calls for a solution that blockchain can provide.

- **Reduced transactional friction.** While the hashing of digital evidence files is a routine practice, the hash values are not uniformly shared within the legal ecosystem. Blockchain's distributed ledger holds the promise of a common, shared means of authenticating digital evidence within a country or region. Nations and regions with many jurisdictions can reduce bureaucratic procedures, and more readily exchange digital evidence where a common method for integrity is in place.

- **Increasing acceptance of the technology.** Courts in China, the U.K. and various U.S. states are recognizing blockchain-based integrity assurance for evidence, minimizing the need for affidavits or other attestations of authenticity. The European Union's Lawful Evidence Collecting and Continuity Platform Development (LOCARD) successfully tested a common digital evidence infrastructure utilizing blockchain. Increasing legal acceptance of this technology will drive changes in digital evidence management products.

Obstacles

- **Stakeholder agreements —** Reaching an agreement among stakeholders for a shared system is a constraint. Joint funding, particularly where jurisdictions do not have a common tax base or funding process, is a constraint. For example, LOCARD prioritized stakeholder engagement to drive a shared vision across jurisdictions.

- **Current technology works —** Current digital evidence technology employs court-accepted techniques for data integrity.

- **Negative perceptions —** Blockchain is commonly associated with cryptocurrency. Private cryptocurrency's speculative financial nature and use in criminal activities may be off-putting for law enforcement and judicial stakeholders.

- **Not proven at scale —** Various pilot efforts have been successful, but blockchain technologies are not proven in large-scale use in government.

User Recommendations

- Assess the benefits of a shared digital evidence system by measuring the volume of digital evidence transactions among stakeholders, and estimating the costs and time losses due to friction when dealing with the various systems.

- Engage stakeholders where a shared system offers improvement by establishing a consortium and/or an advisory group and pursuing proofs of concepts.

- Overcome inflated or negative perceptions of blockchain technology by focusing on interoperability and ease of transactions of a shared system, and emphasizing blockchain as just a piece of the solution.

- Influence product change by querying current digital evidence management providers about their blockchain plans.

Real-Time Incident Center as a Service

Analysis By: Michael Brown

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

A real-time incident command center fuses information from various sources and provides visualization to improve situational awareness capability. It is a type of command-and-control-(C2)-enabling service used by public safety agencies to coordinate responses to emergencies and other events. Typically created and managed by public safety organizations through integration of databases, sensors, video and communications systems, this C2 capability is becoming available in as-a-service form.

Why This Is Important

Information fusion and C2 are common to public safety. Real-time crime centers are an early example. Recently emerging is full-spectrum incident management, enabled by information fusion and C2 technology. Service providers now offer real-time incident management as a service. Jurisdictions with earlier crime-focused capabilities will seek next-generation full incident management capability. Jurisdictions lacking resources for a command center have opportunities with as-a-service offerings.

Business Impact

Public safety mission operators and their technology support organizations are primary stakeholders. Citizens are also important stakeholders in determining acceptable use of surveillance technology. Use of the technology can alter deployment and focus of resources. Improved citizen service through better emergency response is the leading advantage. With an as-a-service offering simplifying the creation of a real-time function, some agencies may gain capability where formerly unable.

Drivers

Real-time incident command center as a service is an outgrowth of earlier approaches and is enabled by supporting technology advancements, such as:

- **Beyond real-time crime centers (RTCCs) —** RTCCs are the forerunner for real-time incident management. Earliest implementation of an RTCC dates to 2005 with many jurisdictions subsequently adopting some form of information fusion and C2 technology. The growth has been driven by citizen expectations to achieve crime reduction and government budget constraints that demand efficient use of public safety resources. While law enforcement was early in using information fusion and C2 to improve situational awareness and deployment of limited resources, more generalized use cases demand the same approach. Wildfire management, natural disasters, special events and pandemic response are some nonpolicing examples where real-time incident management is necessary.

- **Internet-Protocol-(IP)-enabled everything —** The IP enablement of much of the communications, sensor and surveillance capabilities of public safety fosters integration. Integrating information assets like databases, radio, video, Internet of Things (IoT), mass notification, geographic information systems, license plate readers and geolocation tracking cannot be trivialized. But with each of these sources being digitized, the integration problem is made simpler. The lower cost of integration, IoT and SaaS delivery model is enabling and driving the ability for public safety jurisdictions to have a more sophisticated, near-military-level operational picture and C2 capability.

Obstacles

- **Interagency cooperation —** The information fusion aspect and unified C2 of real-time incident management inherently means sharing. The information assets will be owned by multiple agencies. For regional cooperative approaches, the information assets will not even reside in a single jurisdiction.

- **Cost —** This can limit deployment to larger jurisdictions or entail cooperative relationships among smaller jurisdictions. Grants or other forms of capital investment often used for new public safety capabilities will not address recurring cost of incident management center staffing and technology subscription or maintenance fees.

- **Citizen privacy concerns —** Civil liberties advocates may have issues relative to surveillance. Increased use of video or other surveillance technology that occurs in real-time incident command centers will encounter public resistance wherever such resistance is politically permissible.

User Recommendations

Growth of the real-time incident management, increasingly enabled by as-a-service offerings, is critical to satisfy mission needs and resource utilization efficiency. CIOs supporting public safety agencies should:

- Begin interagency collaboration by itemizing information assets and owners, and determining the information value and the willingness to share.
- Estimate costs by conducting market analysis for integration products and services, and developing staffing profiles for the incident management center.

- Address possible citizen privacy concerns by engaging in outreach efforts to explain use, benefits and protections for surveillance capabilities.

Sample Vendors

Everbridge; F24; Fusus; Hexagon; Juvare; Motorola (Rave Mobile Safety); Mutualink; Verizon

At the Peak

Immersive Training in PS/LE

Analysis By: Irma Fabular

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Immersive training in public safety (PS) and law enforcement (LE) is the use of augmented reality (AR), virtual reality (VR) and/or mixed reality (MR) technologies to enhance the training of PS and LE personnel by simulating dynamic, real-world scenarios. Head-mounted displays (HMDs), smartglasses, or even a smartphone or tablet can enable immersive experience through the mix of graphic processing, AI and creativity for training applications.

Why This Is Important

The use of immersive experience technologies to train public safety and law enforcement personnel has several benefits, such as:

- Training agility — There is flexibility and ease in developing/refining hands-on, "real-life" training scenarios.
- Improved personnel safety — Physically hazardous training scenarios could be simulated.
- Lower training costs — Real-life simulation of complex scenarios is less costly and can be reused and easily enhanced in a virtual world.

Business Impact

Immersive training in PS/LE:

- Augments capabilities of complex, often costly, large-scale centralized training programs (e.g., added cost of travel expenses and productive loss).
- Facilitates ease of cross-agency training scenario development and updates.

- Requires ongoing funding for resources with digital expertise, refresh of quickly advancing technologies such as HMDs, updates to content, and seat-based pricing for training platforms.
- Introduces potential risks associated with security, privacy and personnel safety.

Drivers

- **Law enforcement reform advocacy efforts** need ongoing and more effective training programs on the use of force and de-escalation techniques, as well as empathy-based decision making. A 2021 California Peace Officer Training Annual Report highlighted investment in a standardized, virtual reality scenario-based training to emphasize elements of the State's use-of-force laws.
- **Potential "what if" threat scenarios are growing in complexity.** These would encompass natural and man-made threat scenarios that are hard to simulate such as terrorism, wildfires and riots.
- **Shortages in the availability of field officers** require efficient and effective ways of onboarding new field officers as well as providing ongoing training and certification.
- **Immersive technologies are growing in adoption and use.** Organizations such as the New York Police Department and Royal Canadian Mounted Police Department have adopted VR in their training programs.
- **Technology and service providers are continuing to invest.** The ecosystem of startups (for example, Animated Storyboards [V-Armed] and Street Smarts VR) as well as large global technology and service providers (for example, Microsoft [HoloLens 2]) that are addressing immersive training is growing. This is contributing to advancements in public-safety-relevant wearables, communications devices and software. Public-safety-specific training simulation solutions (such as Apex Officer and InVeris Training Solutions) are also growing.

Obstacles

- As training tools, immersive experience solutions are on different paths of maturity, adoption and evolution. AR is scalable and less costly to implement than VR. In comparison, VR solutions are mostly custom and high touch. They are also usually not integrated with systems of record.

- Technology advancements will require ongoing investments in equipment refresh cycles, compatibility with existing training and performance management systems, security risks, and others.

- Implications on policies, personnel adoption and expert resources can be extensive as continuous training is required in addition to updating scenarios. For example, what are the implications on certifications? What are performance and safety considerations?

- Commitment to ongoing operational funding is necessary. A balanced and pragmatic view of cost savings or cost avoidance in the context of personnel safety and societal benefits is gaining ground.

User Recommendations

- Educate training and operations leaders on the value and benefits of immersive experience training solutions by identifying peers with current programs and their successes and challenges.

- Enable productive engagement of agency leaders with solution providers by identifying use cases or scenarios prioritized for training.

- Enhance training programs by being proactive in defining technical, business and process implications of AR, VR and/or MR solutions, including organization change management.

Sample Vendors

Animated Storyboards (V-Armed); Apex Officer; Axon VR; InVeris Training Solutions; Microsoft; Street Smarts VR

Gartner Recommended Reading

Quick Answer: What Is a Metaverse?

Responsible AI

Analysis By: Svetlana Sicular

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Responsible artificial intelligence (AI) is an umbrella term for aspects of making appropriate business and ethical choices when adopting AI. These include business and societal value, risk, trust, transparency, fairness, bias mitigation, explainability, sustainability, accountability, safety, privacy, and regulatory compliance. Responsible AI encompasses organizational responsibilities and practices that ensure positive, accountable, and ethical AI development and operation.

Why This Is Important

Responsible AI has emerged as the key AI topic for Gartner clients. When AI replaces human decisions and generates brand-new artifacts, it amplifies both good and bad outcomes. Responsible AI enables the right outcomes by ensuring business value while mitigating risks. This requires a set of tools and approaches, including industry-specific methods, adopted by vendors and enterprises. More jurisdictions introduce new regulations that challenge organizations to respond in meaningful ways.

Business Impact

Responsible AI assumes accountability for AI development and use at the individual, organizational and societal levels. If AI governance is practiced by designated groups, responsible AI applies to everyone involved in the AI process. Responsible AI helps achieve fairness, even though biases are baked into the data; gain trust, although transparency and explainability methods are evolving; and ensure regulatory compliance, despite the AI’s probabilistic nature.

Drivers

- Responsible AI means a deliberate approach in many directions at once. Data science's responsibility to deliver unbiased, trusted and ethical AI is just the tip of the iceberg. Responsible AI helps AI participants develop, implement, utilize and address the various drivers they face.
- Organizational driver assumes that AI's business value versus risk in regulatory, business and ethical constraints should be balanced, including employee reskilling and intellectual property protection.
- Societal driver includes resolving AI safety for societal well-being versus limiting human freedoms. Existing and pending legal guidelines and regulations, such as the EU's Artificial Intelligence Act, make responsible AI a necessity.
- Customer/citizen driver is based on fairness and ethics and requires resolving privacy versus convenience. Customers should exhibit readiness to give their data in exchange for benefits. Consumer and citizen protection regulations provide the necessary steps, but do not relieve organizations of deliberation specific to their constituents.
- With further AI adoption, the responsible AI framework is becoming more important and is better understood by vendors, buyers, society and legislators.
- AI affects all ways of life and touches all societal strata; hence, the responsible AI challenges are multifaceted and cannot be easily generalized. New problems constantly arise with rapidly evolving technologies and their uses, such as using OpenAI's ChatGPT or detecting deepfakes. Most organizations combine some of the drivers under the umbrella of responsible AI, namely, accountability, diversity, ethics, explainability, fairness, human centricity, operational responsibility, privacy, regulatory compliance, risk management, safety, transparency and trustworthiness.

Obstacles

- Poorly defined accountability for responsible AI makes it look good on paper but is ineffective in reality.
- Unawareness of AI's unintended consequences persists. Forty percent of organizations had an AI privacy breach or security incident. Many organizations turn to responsible AI only after they experience AI's negative effects, whereas prevention is easier and less stressful.
- Legislative challenges lead to efforts for regulatory compliance, while most AI regulations are still in draft. AI products' adoption of regulations for privacy and intellectual property makes it challenging for organizations to ensure compliance and avoid all possible liability risks.
- Rapidly evolving AI technologies, including tools for explainability, bias detection, privacy protection and some regulatory compliance, lull organizations into a false sense of responsibility, while mere technology is not enough. A disciplined AI ethics and governance approach is necessary, in addition to technology.

User Recommendations

- Publicize consistent approaches across all focus areas. The most typical areas of responsible AI in the enterprise are fairness, bias mitigation, ethics, risk management, privacy, sustainability and regulatory compliance.
- Designate a champion accountable for the responsible development and use of AI for each use case.
- Define model design and exploitation principles. Address responsible AI in all phases of model development and implementation cycles. Go for hard trade-off questions. Provide responsible AI training to personnel.
- Establish operationalize responsible AI principles. Ensure diversity of participants and the ease to voice AI concerns.
- Participate in industry or societal AI groups. Learn best practices and contribute your own, because everybody will benefit from this. Ensure policies account for the needs of any internal or external stakeholders.

Sample Vendors

Amazon; Arthur; Fiddler; Google; H2O.ai; IBM; Microsoft; Responsible AI Institute; TAZI.AI; TruEra

Gartner Recommended Reading

A Comprehensive Guide to Responsible AI

Expert Insight Video: What Is Responsible AI and Why Should You Care About It?

Best Practices for the Responsible Use of Natural Language Technologies

Activate Responsible AI Principles Using Human-Centered Design Techniques

How to Ensure Your Vendors Are Accountable for Governance of Responsible AI

Smart Robots

Analysis By: Annette Jump

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

A smart robot is an AI-powered, often-mobile machine designed to autonomously execute one or more physical tasks. These tasks may rely on, or generate, machine learning, which can be incorporated into future activities or support unprecedented conditions. Smart robots can be split into different types based on the tasks/use cases, such as personal, logistics and industrial.

Why This Is Important

Smart robotics is an AI use case, while robotics in general does not imply AI. Smart (physical) robots had less adoption compared with industrial counterparts but received great hype in the marketplace; therefore, smart robots are still climbing the Peak of Inflated Expectations. There has been an increased interest in smart robots in the last 12 months, as companies are looking to further improve logistic operations, support automation and augment humans in various jobs.

Business Impact

Smart robots will make their initial business impact across a wide spectrum of asset-, product- and service-centric industries. Their ability to reduce physical risk to humans, as well as do work with greater reliability, lower costs and higher productivity, is common across these industries. Smart robots are already being deployed among humans to work in logistics, warehousing, police as well as safety applications.

Drivers

- The market is becoming more dynamic with technical developments of the last two years, enabling a host of new use cases that have changed how smart robots are perceived and how they can deliver value.
- The physical building blocks of smart robots (motors, actuators, chassis and wheels) have incrementally improved over time. However, areas such as Internet of Things (IoT) integration, edge AI and conversational capabilities have seen fundamental breakthroughs. This changes the paradigm for robot deployments.
- Vendor specialization has increased, leading to solutions that have higher business value, since an all-purpose/multipurpose device is either not possible or is less valuable.
- Growing interest in smart robots across a broad number of industries and use cases like: medical/healthcare (patient care, medical materials handling, interdepartment deliveries and sanitization); manufacturing (product assembly, stock replenishment, support of remote operations and quality control [QC] check); last-mile delivery; inspection of industrial objects or equipment; agriculture (harvesting and processing crops); and workplace and concierge robots in workplaces, hospitality, hospitals and so forth.

Obstacles

- **Companies are still struggling to identify valuable business use cases and assess ROI** for robots, especially outside of manufacturing and transportation. Therefore, the position of "smart robots" is still climbing to the Peak of Inflated Expectations.
- **Hype and expectations will continue to build around smart robots during the next few years**, as providers expand their offerings and explore new technologies, like reinforcement learning to drive a continuous loop of learning for robots and swarm management.
- **Lack of ubiquitous wireless connectivity solutions outside of smart spaces and immaturity of edge AI technologies** can inhibit the pace at which smart robots become semiautomated and mobile.
- **The need to offload computation to the cloud** will decrease from 2024, as robots will make more autonomous decisions.
- **The continuous evolution of pricing models**, like buy, monthly lease or hourly charge versus robot as a service for robotic solutions can create some uncertainty for organizations.

User Recommendations

- Evaluate smart robots as both substitutes and complements to their human workforce in manufacturing, distribution, logistics, retail, healthcare or defense.
- Begin pilots designed to assess product capability and quantify benefits, especially as ROI is possible even with small-scale deployments.
- Examine current business processes for current deployment of smart robots and also for large-scale deployment over the next three to five years.
- Consider different purchase models for smart robots.
- Dissolve the reluctance from staff by developing training resources to introduce robots alongside humans as an assistant.
- Ensure there are sufficient cloud computing resources to support high-speed and low-latency connectivity in the next two years.
- Evaluate multiple global and regional providers due to fragmentation within the robot landscape.

Sample Vendors

Ava Robotics; Geek+; GreyOrange; iRobot; Locus Robotics; Rethink Robotics; SoftBank Robotics; Symbotic; Temi; UBTECH

Gartner Recommended Reading

Emerging Technologies: Top Use Cases for Smart Robots to Lead the Way in Human Augmentation

Emerging Technologies: Top Use Cases Where Robots Interact Directly With Humans

Emerging Technologies: Venture Capital Growth Insights for Robots, 2021

Emerging Technologies: Smart Robot Adoption Generates Diverse Business Value

Generative AI

Analysis By: Svetlana Sicular, Brian Burke

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Definition:

Generative AI technologies can generate new derived versions of content, strategies, designs and methods by learning from large repositories of original source content. Generative AI has profound business impacts, including on content discovery, creation, authenticity and regulations; automation of human work; and customer and employee experiences.

Why This Is Important

Generative AI exploration is accelerating, thanks to the popularity of Stable Diffusion, Midjourney, ChatGPT and large language models. End-user organizations in most industries aggressively experiment with generative AI. Technology vendors form generative AI groups to prioritize delivery of generative-AI-enabled applications and tools. Numerous startups have emerged in 2023 to innovate with generative AI, and we expect this to grow. Some governments are evaluating the impacts of generative AI and preparing to introduce regulations.

Business Impact

Most technology products and services will incorporate generative AI capabilities in the next 12 months, introducing conversational ways of creating and communicating with technologies, leading to their democratization. Generative AI will progress rapidly in industry verticals, scientific discovery and technology commercialization. Sadly, it will also become a security and societal threat when used for nefarious purposes. Responsible AI, trust and security will be necessary for safe exploitation of generative AI.

Drivers

- The hype around generative AI is accelerating. Currently, ChatGPT is the most hyped technology. It relies on generative foundation models, also called “transformers.”
- New foundation models and their new versions, sizes and capabilities are rapidly coming to market. Transformers keep making an impact on language, images, molecular design and computer code generation. They can combine concepts, attributes and styles, creating original images, video and art from a text description or translating audio to different voices and languages.
- Generative adversarial networks, variational autoencoders, autoregressive models and zero-/one-/few-shot learning have been rapidly improving generative modeling while reducing the need for training data.
- Machine learning (ML) and natural language processing platforms are adding generative AI capabilities for reusability of generative models, making them accessible to AI teams.
- Industry applications of generative AI are growing. In healthcare, generative AI creates medical images that depict disease development. In consumer goods, it generates catalogs. In e-commerce, it helps customers “try on” makeup and outfits. In manufacturing, quality inspection uses synthetic data. In semiconductors, generative AI accelerates chip design. Life sciences companies apply generative AI to speed up drug development. Generative AI helps innovate product development through digital twins. It helps create new materials targeting specific properties to optimize catalysts, agrochemicals, fragrances and flavors.
- Generative AI reaches creative work in marketing, design, music, architecture and content. Content creation and improvement in text, images, video and sound enable personalized copywriting, noise cancellation and visual effects in videoconferencing.
- Synthetic data draws enterprises’ attention by helping to augment scarce data, mitigate bias or preserve data privacy. It boosts the accuracy of brain tumor surgery.
- Generative AI will disrupt software coding. Combined with development automation techniques, it can automate up to 30% of the programmers’ work.

Obstacles

- Democratization of generative AI uncovers new ethical and societal concerns. Government regulations may hinder generative AI research. Governments are currently soliciting input on AI safety measures.
- Hallucinations, factual errors, bias, a black-box nature and inexperience with a full AI life cycle preclude the use of generative AI for critical use cases.
- Reproducing generative AI results and finding references for information produced by general-purpose LLMs will be challenging in the near term.
- Low awareness of generative AI among security professionals causes incidents that could undermine generative AI adoption.
- Some vendors will use generative AI terminology to sell subpar "generative AI" solutions.
- Generative AI can be used for many nefarious purposes. Full and accurate detection of generated content, such as deepfakes, will remain challenging or impossible.
- The compute resources for training large, general-purpose foundation models are heavy and not affordable to most enterprises.
- Sustainability concerns about high energy consumption for training generative models are rising.

User Recommendations

- Identify initial use cases where you can improve your solutions with generative AI by relying on purchased capabilities or partnering with specialists. Consult vendor roadmaps to avoid developing similar solutions in-house.
- Pilot ML-powered coding assistants, with an eye toward fast rollouts, to maximize developer productivity.
- Use synthetic data to accelerate the development cycle and lessen regulatory concerns.
- Quantify the advantages and limitations of generative AI. Supply generative AI guidelines, as it requires skills, funds and caution. Weigh technical capabilities with ethical factors. Beware of subpar offerings that exploit the current hype.
- Mitigate generative AI risks by working with legal, security and fraud experts. Technical, institutional and political interventions will be necessary to fight AI's adversarial impacts. Start with data security guidelines.
- Optimize the cost and efficiency of AI solutions by employing composite AI approaches to combine generative AI with other AI techniques.

Sample Vendors

Adobe; Amazon; Anthropic; Google; Grammarly; Hugging Face; Huma.AI; Microsoft; OpenAI; Schrödinger

Gartner Recommended Reading

Innovation Insight for Generative AI

Emerging Tech Roundup: ChatGPT Hype Fuels Urgency for Advancing Conversational AI and Generative AI

Emerging Tech: Venture Capital Growth Insights for Generative AI

Emerging Tech: Generative AI Needs Focus on Accuracy and Veracity to Ensure Widespread B2B Adoption

ChatGPT Research Highlights

Rapid DNA in Policing

Analysis By: Michael Brown

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Early mainstream

Definition:

Rapid DNA is a technology that returns a small set of genetic marker results in 90 minutes to uniquely identify an individual. This identification is used to compare with records in central databases like the U.S. FBI's Combined DNA Index System or the Italian Banca Dati Nazionale del DNA. The technology is not new in a laboratory setting, but the adaptation to the more demanding police-booking processes is an evolutionary application.

Why This Is Important

Law enforcement use of DNA identification has been in the form of evidence analysis for investigative work, where laboratories return results over days or weeks. Due to rapid DNA speed and accuracy, this technology is sufficiently mature to join electronic fingerprinting as a standard biometric identifier collected during the arrestee booking process. The benefits of clearing unsolved crimes and preventing the inadvertent release of those who should remain in custody are substantial.

Business Impact

Law enforcement agencies that operate booking functions and the CIOs who support those agencies are impacted by rapid DNA in the following ways:

- Enhanced ability to clear unsolved crimes and prevent inadvertent release of those who should remain in custody.
- Requirements for supporting legislation in addition to modification of booking procedures, ecosystem partnerships and compliance activities.
- Significant changes to existing booking technology.

Drivers

- **Acceptance —** DNA evidence has been thoroughly challenged and ultimately widely accepted in court proceedings as far back as 1985. While expanding DNA collection may raise civil liberties concerns, the use of DNA as an authoritative form of identification is not controversial.

- **Mature policy —** Since the 2010 establishment of the Rapid DNA Program Office, the FBI has been working to introduce this technology to law enforcement. As the technology advanced, it became evident that the use of rapid DNA in a less controlled environment would be possible. In 2017, the Rapid DNA Act was signed into law in the U.S., directing the FBI to issue standards and procedures. The FBI has subsequently published the Standards for the Operation of Rapid DNA Booking Systems by Law Enforcement Booking Agencies and the National Rapid DNA Booking Operational Procedures Manual.

- **Successful testing and initial implementation —** Throughout 2019 and into early 2020, the FBI — in cooperation with law enforcement agencies in Arizona, Florida, Louisiana and Texas — completed pilot testing of the technology at booking stations. The results informed the publication of detailed standards and operational procedures. Louisiana has since implemented regular use of rapid DNA in one booking environment and is expanding to others.

- **Equipment certification —** Two rapid DNA instrument vendors have achieved FBI certification for booking station use.

Obstacles

- **Legal authority —** Supporting legislation must be enacted to allow the collection of DNA samples from all arrestees.
- **Workflow changes —** The arrestee booking workflow must be altered for DNA collection. Those changes require collaboration at various levels — local, state and federal in the U.S.
- **Certification —** System certification will be required. Operators will also require training and certification.
- **Complexity —** Technology integration for rapid DNA is complex, involving new equipment, software, network message types and interoperability with existing fingerprint systems, records management systems and jail management systems.
- **Expense —** Initial cost of the rapid DNA devices may be quite high, relative to some agencies' budgets. Unlike the introduction of live-scan fingerprint technology 30 years ago, rapid DNA also has considerable sustainment costs for reagent and swab kits that must be accounted for in agency budgets over the long haul.

User Recommendations

Rapid DNA is mature and positioned to become an everyday identification tool for law enforcement. The technology is available. Standards and procedures have been developed in one of the largest, most complex law enforcement markets. Budgets and implementations will follow. CIOs responsible for supporting law enforcement should:

- Begin planning by consulting with ecosystem partners to gain their commitment to change and embark on pilot programs and assigning staff to assist.
- Plan for technology integration by training internal staff and possibly using outside integration contractors.
- Assist in developing the necessary budget for introducing and supporting rapid DNA by coordinating with mission operational staff.

Sample Vendors

Aspen Network of Development Entrepreneurs (ANDE); Thermo Fisher Scientific

Gartner Recommended Reading

Predicts 2023: Justice and Public Safety Seizes New Opportunities to Address Evolving Demands

Capabilities Model for Law Enforcement

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)

Wearable Monitors for Public Safety

Analysis By: Bill Finnerty

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

Wearable monitors for public safety and law enforcement are Internet of Things (IoT) devices, such as watches, heart rate monitors and cameras. They are used to improve situational awareness and monitor the safety of fire, rescue, law enforcement and corrections personnel and those in their care or custody. Data from these devices is monitored on a near-real-time basis to ensure that individuals are not in physical distress and provide deeper analysis when combined with other datasets.

Why This Is Important

The health and safety of the individuals working for or in the custody or care of public safety and law enforcement are critical to the mission of the organization. However, there are significant physical and health risks that these individuals face on a regular basis. By using wearable technology and monitoring the data, public safety and law enforcement agencies can increase their situational awareness and their ability to protect these individuals or respond quickly when they are in danger.

Business Impact

Wearable technologies enable public safety and law enforcement to monitor the health and wellness of individuals, regardless of their situation or location. For example, using wearables:

- Agencies can monitor the vital signs of firefighters responding to a call, allowing supervisors to take preventative action should they start to show signs of distress.
- Corrections institutions can monitor the status of officers or inmates to ensure that they have not fallen or are having heart problems.

Drivers

- More-reliable and lower-cost options for wearable sensors are widely available.
- Improved battery life will make their use throughout an entire shift or day possible.
- Investments are being made by large technology firms, such as Apple and Samsung, in the use of wearables to support health and wellness in public safety and justice (PS&J).
- The growing number of options for implementing wearable sensors, including watch, wristband, clothing and smart patches, will make the use of sensors more convenient for public safety and law enforcement organizations.
- Innovation related to IoT sensors for health and wellness is increasing, enabled by a higher level of understanding and acceptance of the use of technology for these purposes.
- The expansion of 5G, satellite and other wireless technology makes connectivity possible in more areas at better price points.
- The collection and analysis of data from wearable technologies enables preventative care and support for those on duty, in care or in custody, versus physical or mental health support care after an incident.
- Data from wearables can contribute to early intervention systems to ensure wellness and accountability for sworn and unsworn staff.
- The adoption of a smartwatch app by PS&J vendors advances their multiexperience capabilities for core PS&J systems, such as computer-aided dispatch and records management systems.

Obstacles

- Concerns related to privacy and over surveillance/monitoring of individuals may cause staff or individuals in care or custody to reject the use of wearable technologies.
- For facilities where wireless technology has not been deployed at scale previously, the cost of deploying wireless technologies may limit connectivity and the viability of wearable sensors.
- Challenges related to connectivity or damage to the sensors used in wearable technology could mean that organizations feel that the devices cannot be relied on for mission-critical applications.
- Where benefits are not clear, wearable technology can be seen as inconvenient additional equipment to don, causing officers, paramedics or firefighters to resist adoption.

User Recommendations

- Gain buy-in for the continued use of wearable technologies by establishing an ongoing discussion with workforce leadership about the benefits and challenges related to the use of wearable technologies in pilots.
- Protect individual privacy by establishing acceptable use policies for personal data collected from wearable technologies. Include internal and external stakeholders in the development of this policy as applicable.
- Develop a clear set of criteria for experimenting or using wearable technologies by addressing management, security, data access controls, life cycle management and the ability for individuals to easily review data collected about them.
- Establish a future state roadmap by engaging vendors to determine their roadmap for supporting multiexperience capabilities based on wearable technologies.

Sample Vendors

Apple; Samsung Electronics; SlateSafety

Edge AI

Analysis By: Eric Goodness

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

Edge AI refers to the use of AI techniques embedded in non-IT products, IoT endpoints, gateways and edge servers. It spans use cases for consumer, commercial and industrial applications, such as autonomous vehicles, enhanced capabilities of medical diagnostics and streaming video analytics. While predominantly focused on AI inference, more sophisticated systems may include a local training capability to provide optimization of the AI models at the edge.

Why This Is Important

Many edge computing use cases are latency-sensitive and data-intensive, and require an increasing amount of autonomy for local decision making. This creates a need for AI-based applications in a wide range of edge computing and endpoint solutions. Examples include real-time analysis of edge data for predictive maintenance and industrial control, inferences and decision support where connectivity is unreliable, or video analytics for real-time interpretation of video.

Business Impact

The business benefits of deploying edge AI include:

- Real-time data analysis and decision intelligence
- Improved operational efficiency, such as manufacturing visual inspection systems that identify defects, wasted motion, waiting, and over- or underproduction
- Enhanced customer experience, through feedback from AI embedded within products
- Connectivity cost reduction, with less data traffic between the edge and the cloud
- Persistent functions and solution availability, irrespective of network connectivity
- Reduced storage demand, as only prioritized data is passed on to core systems
- Preserved data privacy at the endpoint

Drivers

Overall, edge AI has benefited from improvements in the capabilities of AI. This includes:

- The maturation of machine learning operationalization (MLOps) and ModelOps tools and processes support ease of use across a broader set of features that span the broader MLOps functions. Initially, many companies came to market with a narrowcast focus on model compression.
- The improved performance of combined ML techniques and an associated increase in data availability (such as time-series data from industrial assets).

Business demand for new and improved outcomes solely achievable from the use of AI at the edge, which include:

- Reducing full-time equivalents with vision-based solutions used for surveillance or inspections.
- Improving manufacturing production quality by automating various processes.
- Optimizing operational processes across industries.
- New approaches to customer experience, such as personalization on mobile devices or changes in retail from edge-based smart check-out points of sale.

Additional drivers include:

- **Increasing number of users upgrading legacy systems and infrastructure in "brownfield" environments.** By using MLOps platforms, AI software can be hosted within an edge computer or a gateway (aggregation point) or embedded within a product with the requisite compute resources. An example of this is AI software deployed (TinyML) deployed to automotive or agricultural equipment to enhance asset monitoring and maintenance.

- **More manufacturers embedding AI in the endpoint as an element of product servitization.** In this architecture, the IoT endpoints, such as in automobiles, home appliances or commercial building infrastructure, are capable of running AI models to interpret data captured by the endpoint and drive some of the endpoints' functions. In this case, the AI is trained and updated on a central system and deployed to the IoT endpoint. Examples of the use of embedded (edge) AI are medical wearables, automated guided vehicles and other robotic products that possess some levels of intelligence and autonomy.

- **Rising demand for R&D in training decentralized AI models at the edge for adaptive AI.** These emerging solutions are driven by explicit needs such as privacy preservation or the requirement for machines and processes to run in disconnected (from the cloud) scenarios. Such models enable faster response to changes in the environment, and provide benefits in use cases such as responding to a rapidly evolving threat landscape in security operations.

Obstacles

- Edge AI is constrained by the application and design limitations of the equipment deployed; this includes form factor, power budget, data volume, decision latency, location and security requirements.

- Systems deploying AI techniques can be nondeterministic. This will impact applicability in certain use cases, especially where safety and security requirements are important.

- The autonomy of edge AI-enabled solutions, built on some ML and deep learning techniques, often presents questions of trust, especially where the inferences are not readily interpretable or explainable. As adaptive AI solutions increase, these issues will increase if initially identical models deployed to equivalent endpoints subsequently begin to evolve diverging behaviors.

- The lack of quality and sufficient data for training is a universal challenge across AI usage.

- Deep learning in neural networks is a compute-intensive task, often requiring the use of high-performance chips with corresponding high-power budgets. This can limit deployment locations, especially where small form factors and lower-power requirements are paramount.

User Recommendations

- Determine whether the use of edge AI provides adequate cost-benefit improvements, or whether traditional centralized data analytics and AI methodologies are adequate and scalable.
- Evaluate when to consider AI at the edge versus a centralized solution. Good candidates for edge AI are applications that have high communications costs, are sensitive to latency, require real-time responses or ingest high volumes of data at the edge.
- Assess the different technologies available to support edge AI and the viability of the vendors offering them. Many potential vendors are startups that may have interesting products but limited support capabilities.
- Use edge gateways and servers as the aggregation and filtering points to perform most of the edge AI and analytics functions. Make an exception for compute-intensive endpoints, where AI-based analytics can be performed on the devices themselves.

Sample Vendors

Akira AI; Edge Impulse; Falkonry; Imagimob; Litmus; MicroAI; Modzy; Octonion Group; Palantir

Gartner Recommended Reading

Building a Digital Future: Emergent AI Trends

Emerging Technologies: Neuromorphic Computing Impacts Artificial Intelligence Solutions

Emerging Technologies: Edge Technologies Offer Strong Area of Opportunity — Adopter Survey Findings

Emerging Tech Impact Radar: Edge AI

Head-Mounted Displays

Analysis By: Evan Brown, Tuong Nguyen

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Adolescent

Definition:

Head-mounted displays (HMDs) are small displays or projection technology integrated into head-worn devices for augmented reality, mixed reality and virtual reality. They are worn, or mounted, on or near the face, allowing the wearer to see the optics at a viewing distance ideal for either complete immersion or information at a glance. Additionally, certain aspects of the visual content supplied by HMDs is contextual, providing various visual cues based on the wearer's current state.

Why This Is Important

HMDs are uniquely positioned to provide new opportunities utilizing augmented reality (AR), virtual reality (VR) and mixed reality (MR) technologies. HMDs do exist on a spectrum of other mobile computing and display options, such as smartphones and tablets, and complement them. But, they provide a previously unavailable hands-free experience that is especially beneficial in capital-equipment-intensive industries, as well as a level of immersion whose full benefit is still being explored.

Business Impact

HMDs open new ways to interact with the physical and digital world. Enterprises will use AR HMDs for improved guidance, inspection and assistance. VR HMDs will initially succeed in gaming and education, though enterprises will eventually derive significant value in training, design and collaboration use cases. While MR HMDs will take longer to mature, unique implementations, such as the visualization of architectural fit and digital-to-physical interaction, will streamline complex scenarios.

Drivers

- Apple's (rumored) HMD plans currently have limited impact on the pace and trajectory of the market, but will likely renew attention and accelerate adoption as the launch date draws near and applications are announced.
- Performance improvements to all-in-one VR HMDs are overcoming the need for additional hardware, and decreasing accessibility and usability barriers which limit current adoption.
- Technological advancement across the spectrum of HMDs, along with adjacent display, optics, computer vision, natural language, rendering, graphics, interface technologies and form factor improvements, have made experiences significantly more immersive. Additionally, as the technology improves, HMDs will be offered at more reasonable price points, which is necessary for widespread adoption.
- Continued investment into HMDs is planting the seed for a burgeoning software and hardware ecosystem that will help to promote enterprise adoption with improved deployment, management and integration opportunities.
- Increased desire and expectation for remote work opportunities is leading enterprises to experiment with new and novel solutions capable of emulating in-person experiences or expanding remote work possibilities.
- Initial hype surrounding the metaverse spurred significant interest and investment into the development and adoption of HMDs.
- Further development and deployment of software, particularly entertainment and gaming solutions, among new and established distribution platforms is providing increased incentive for adoption.
- Exploration of new educational opportunities is leading universities and other educational institutions to explore HMD implementations.
- Normalization of public recording via regular smartphone use and exposure will potentially reduce the cultural stigma of previous HMD attempts.

Obstacles

- Tech limitations create interoperability, social, ergonomic and battery challenges.
- Cost, form factor, usability and accessibility are hindrances, while motion sickness and eye strain remains unsolved.
- Association with, and declining interest in, the metaverse will hamper adoption.
- Key vendors failed expectations. The U.S. Army reduced purchase of and demanded improvements to Microsoft's HoloLens. Meta dropped the price of Quest Pro and Google discontinued Glass Enterprise Edition.
- Lack of a "killer app" and use case, as well as, an ecosystem of off-the-shelf enterprise software.
- Software development mostly focuses on solving inconveniences or nonexistent challenges.
- Lacking a large installed base, few are willing to significantly experiment in this space.
- Recession concerns reduce willingness to try expensive, early-stage technology.
- High-quality immersive experiences require space that many may not have.
- Single- and purpose-built devices have limited adoption potential.

User Recommendations

- Adopt tactically as most devices are purpose-built with unpredictable support and release cycles. Successful implementations focus on one specific use case as technological limitations limit multipurpose, widespread adoption.
- Ensure appropriate hardware choice. AR can be utilized for extended periods but is not fully immersive with lighting impacting visibility. VR provides a more in-depth experience but users need to limit their time in VR due to barriers around user interfaces and experience.
- Evaluate AR/MR HMDs for situations where the user's hands are occupied or when the user needs information while moving — for example, remote guidance with telestration.
- Evaluate VR HMDs as an alternative to highly specialized or high-cost, real-world scenarios.
- Track growing ROI by monitoring advancements such as improvements in display, battery life, comfort and cost. Applicable off-the-shelf software has the future potential to significantly reduce the barrier for entry, particularly for VR.

Sample Vendors

HTC; Magic Leap; Meta; Microsoft; Nreal; PICO; RealWear; Sony Interactive Entertainment; Valve; Vuzix

Gartner Recommended Reading

Emerging Technologies: Find Success With Head-Mounted Displays Despite Modest Market Growth Expectations

Emerging Technologies: The Future of the Metaverse

Emerging Tech: Three MEMS Technologies Will Enhance Metaverse User Experiences

Forecast Analysis: Semiconductors and Electronics, Worldwide

Emerging Tech: Venture Capital Growth Insights for Head-Mounted Display Technologies

LTE/5G-Enhanced Services

Analysis By: Irma Fabular

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Commercially available Long Term Evolution (LTE)/4G and 5G cellular infrastructure can enhance public safety communications and services. This infrastructure replaces or augments private land mobile radio (LMR) communications and adheres to public safety standards, such as mission-critical push-to-talk (MCPTT), for emergency response. Key characteristics include strong security, high availability 24/7, low latency, high bandwidth, nationwide coverage and interoperability.

Why This Is Important

Public safety communications infrastructures using LTE/5G technologies are important because they:

- Improve capabilities to respond and collaborate across various agencies in multiple geographic regions through a nationwide communications network
- Enhance clarity in emergency and incident management communications through the flexibility to message using voice, text and/or video
- Mitigate public and officer safety risks through strong security (no “eavesdropping” on incidents)

Business Impact

Key impacts on strategy and operations for public safety and law enforcement are as follows:

- Evolving policies and processes require strong organization change management.
- Improved cross-jurisdictional communications and interoperability can provide strong business justification to augment or replace LMR infrastructure with LTE/5G capabilities.
- Large capital investments for public safety innovation can be avoided through the use of commercially available LTE/5G infrastructure.

Drivers

- Public and personnel safety improve through enhanced emergency response collaboration, both within a single agency (such as a police agency) and across multiple agencies and jurisdictions.
- Standards for MCPTT have been established, driving continued investment by technology and service providers. For example, FirstNet PTT and Group First Response enable interoperability between LTE and LMR infrastructures in the U.S.
- The growing ecosystem of technology providers is introducing innovations that require high bandwidth and secure communications. These innovations include advancements in artificial intelligence (e.g., computer vision), data and analytics, Internet of Things (IoT; e.g., sensors and drones), and edge computing.
- The increasingly complex threat landscape requires better communication and collaboration to prevent, respond to and recover from emergencies.
- Nationwide broadband networks for public safety are garnering government attention and investment in various countries, such as the United States, Canada, the United Kingdom, South Korea and Australia.
- There is continued funding support for acceleration of 5G infrastructure rollouts and evaluation of next-generation communications systems (see U.S. Department of Defense).

Obstacles

Full adoption of LTE/5G by public safety organizations can take five to 10 years, as several obstacles are slowing down use of LTE/5G for public safety emergency response:

- Limited cellular coverage, particularly in rural and remote areas
- Organization change management, including confidence in the reliability of commercial cellular offerings
- Consensus on the ROI and business justification to transition from large capital investments in private, LMR infrastructure, systems and equipment
- Public safety government grants that often fund only capital improvements and one-time investments
- Careful scrutiny of suppliers' supply chain to secure telecommunications equipment and devices

User Recommendations

- Proactively address enhanced communications and services by incorporating LTE/5G communications technologies in strategic plans. Account for increasing use of mobile devices, which requires unique security considerations, and makes insights from all forms of data — text, video and voice — more feasible.
- Adequately estimate operational budgets by planning for using at least two communications devices to respond to incidents. For many organizations, both LMR and LTE/5G technologies will coexist for some time.
- Extend the benefits of LTE/5G for emergency communications by including the "whole of government." In addition to emergency first responders, several government and nongovernment organizations are involved in emergency response and recovery efforts, and they can also benefit from seamless communications channels.

Sample Vendors

AT&T; Lumen; Motorola; Mutualink; Rogers; Samsung; Telstra, Verizon; Vodafone

Gartner Recommended Reading

Top Strategic Technology Trends for 2023: Wireless Value Realization

Composable Applications

Analysis By: Yefim Natis, Anne Thomas, Paul Vincent

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Composable applications are built, in part or in whole, as flexible assemblies (compositions) of software components that represent well-defined business capabilities, packaged for programmatic access. The business-centric modularity of composable applications empowers democratized access to technology and business innovation. Composable applications support faster, safe and efficient digital business innovation. Advanced use of composable applications allows cross-application compositions.

Why This Is Important

Composable applications help support resilience, adaptability and growth of business in the context of increasingly frequent challenges, disruptions and opportunities. They support fast-paced business change while protecting the integrity of the outcomes, and bridge application software and business operations by using coarse-grained business-centric software modularity. Organizations that use composable applications maintain customer loyalty by better tracking their changing needs.

Business Impact

The more composable applications there are in the organization’s portfolio, the better the organization is prepared to support changing business requirements through digital innovation. In return, greater confidence in the agility of applications promotes faster business thinking. The improved agility of business technology strengthens the ability of an organization to maintain and grow its business, a high value in the modern context of fast innovation, frequent challenges and opportunities.

Drivers

- In the continuously changing business context, demand for business adaptability directs organizations toward technology architecture that supports fast, safe and efficient application change.
- The demand for active participation of business decision makers in the design of their digital experiences promotes the adoption of technology models that are accessible and useful to business experts in addition to, and in cooperation with, technical professionals.
- The need to reduce the costs of redundancy in software capabilities across applications and business units drives organizations to reusable business modularity and from there to composability.
- The increasing number of vendors offering API-centric SaaS (also known as API products or "headless" SaaS) builds up a portfolio of available business-centric packaged application components — promoting their use as building blocks of composable business applications.
- The emerging architecture of micro front ends and superapps advances the principles of composability to the multifunctional user experience, promoting broader adoption of composability in application design.
- Fast-growing competence in mainstream organizations for the management of broad collections of APIs and event streams creates a technology foundation for safe operation of a composable business technology environment.
- The emerging business model of industry cloud, promotes the architecture of modularity and composition inside and across vertical use cases.

Obstacles

- Limited experience of composable thinking and planning in most software engineering organizations complicates composable design efforts and transition plans.

- Limited practice of business-IT collaboration for application design delays the effective composable design that depends on the complementary expert talents in multidisciplinary fusion teams.

- Most legacy applications can participate in composition via their APIs and/or event streams, but their architecture provides only minimal autonomy, delaying the full positive effect of composable architecture.

- Limited development and platform tools dedicated to composable application architecture limit the early success to advanced design teams capable of adapting precursor technologies to new objectives.

- Insufficient mapping of architectural thinking and models between business and technology planners makes digital representation of business functionality less prepared to track real-world business change.

User Recommendations

- Promote modular thinking as the means to great flexibility in business and software innovation.
- Champion API-first business software design, whether or not the application is also packaging the traditional UI capabilities.
- Build competence in API and event stream management as the precursor to managing composable business software modularity.
- Prioritize the formation of business-IT fusion teams to support faster and more effective adaptive change of business applications.
- Use low-code/no-code technologies to facilitate design collaboration of business and technology experts in fusion teams.
- Build an investment case for composability by highlighting how aging digital assets endanger the future success of the business by forming barriers to innovation, competition and customer satisfaction at the pace of market change.
- Gradually modernize (or replace) existing applications toward an architecture of business-centric modularity.

Sample Vendors

Elastic Path Software; Mambu; Novulo; Olympe; Spryker Systems

Gartner Recommended Reading

Becoming Composable: A Gartner Trend Insight Report

Quick Answer: Who's Who in the Life Cycle of Composable Applications?

Case Study: Composable Platform Strategy to Drive Business Agility (Nike)

Predicts 2023: Composable Applications Accelerate Business Innovation

Use Gartner's Reference Model to Deliver Intelligent Composable Business Applications

Field Streaming Video

Analysis By: Bill Finnerty

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Field streaming video in public safety and law enforcement (PS/LE) is the process of streaming live body-worn, dash, drone, mobile phone and other video from and to field personnel and incident command centers. The goal of field streaming video is to improve situational awareness, and augment officers and commanders in identifying threats and risks through automated analysis of the video. Organizations must secure this data to maintain a chain of custody for evidentiary purposes.

Why This Is Important

Field streaming of video allows the real-time, not just after-the-fact, analysis of incident content to improve the situational awareness of personnel in the field or in a command center. Video and audio can be analyzed in real time, using computer vision to detect and respond to threats, such as weapons, anti-social behavior and illegal activities. Sentiment analysis can be used to analyze the video and audio to identify risks to the wellness and safety of officers and participants in an incident.

Business Impact

Field streaming video can be used by:

- PS/LE agencies to gain the tactical advantage during an event
- Dispatchers to engage the correct resources for a call
- Police for threat analysis and real-time intervention for officer safety and accountability
- Detectives in interview rooms to stream to other rooms
- Fire departments to assess risk from structural damage
- Emergency medical services (EMS) to share content with emergency room staff en route
- Corrections to detect risks and threats among inmates, such as fighting and contraband

Drivers

- **Advances in technology:** The use of video for analysis of incidents after they occur is commonplace in public safety and law enforcement. Field streaming video is gaining greater adoption due to advances in battery life (which is improving, but still has a ways to go). Compression algorithms, bandwidth and artificial intelligence are contributing to the opportunity to take advantage of this content to improve situational awareness and response capabilities in real time.

- **Increased threats and risks:** Officers, firefighters and EMS personnel face an increased set of threats and risks in their day-to-day jobs. Streaming video enables the use of computer vision to alert personnel of these dangers and allows commanders to take proactive steps to safeguard their people.

- **Heightened service-level expectations:** Constituents' expectations of the level of service provided by law enforcement and public safety agencies have increased as the number and quality of digital capabilities available to them grow. Constituents expect that video will be utilized to improve their safety. Video can be used to enable faster and more-effective responses to threats and risks including the use of real-time evidence to inform decisions related to issuing warrants and next best actions. It can also be used to ensure that those providing services are held accountable for their actions.

- **Resource constraints:** Public safety and law enforcement organizations in many parts of the world are facing staffing shortages. Field streaming video provides a means to add efficiencies into the incident response processes by using mobile phone, drone or other data to best determine what resources to dispatch to an incident.

Obstacles

- Although improvements in battery life are making field streaming more viable for limited periods, many current body-worn cameras are not equipped to last a full shift or to stream content via cellular networks. With the latest hardware, this is generally ameliorated via field swappability of the battery. However, even with two batteries, this hardware cannot stream for a full shift.

- Greater benefit of field streaming can be achieved by leveraging computer vision and sentiment analysis of video in real time. However, the cost of the technology, including connectivity, video analytics, artificial intelligence (AI) and storage, can be prohibitive to agencies with limited budgets. Additionally, both staff and the public may have concerns about bias related to AI that is used to analyze video.

- Both public safety and law enforcement personnel and the public have concerns about privacy rights related to recording their actions and the ethical use of this information.

User Recommendations

- Engage leadership in working with stakeholders from the workforce and public to establish acceptable use policies for field streaming video. Ensure the group explores multiple use cases for video as they relate to privacy, accountability and safety. Revisit the standards of acceptable use regularly, and stress-test solutions to match these use cases and parameters.

- Assess current products for their field streaming capabilities, and establish a plan for necessary replacement through life cycle programs. There are multiple options for connectivity available, including cellular and vehicle Wi-Fi, for which the risks and benefits that must be explored when choosing a solution.

- Establish the business use case for video analytics requirements, and work with vendors on how best to implement those solutions. Where camera providers do not have the needed capabilities in their roadmap, identify possible partners to provide these capabilities.

- Identify other government agencies that are leveraging field streaming video as potential partners for sharing video to expand insights without further investment in devices and infrastructure.

Sample Vendors

Axon; Fujitsu; Motorola; Sentinel Camera Systems; Wireless CCTV; WOLFCOM

Digital Twin of a Citizen

Analysis By: Milly Xiang, Alfonso Velosa

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

A digital twin of a citizen (DToC) is a technology-enabled proxy that mirrors the state of a person. National, state and local governments use DToC to support citizen services such as health or safety management. Its elements are the model, data, a unique one-to-one association and the ability to monitor it. It integrates data into the DToC from siloed sources such as health records, credit scores, phone logs, criminal records, customer 360 records, and sensors such as cameras.

Why This Is Important

Governments are developing DToCs to address health, safety, environment, travel and contextualized social media impacts on society. The spectrum of the complexity of the models and tools can help governments make better decisions for monitoring and supporting constituents, such as patients, prisoners, passengers or the elderly. The Chinese government has been building and improving its social credit scoring methodology. Aggregated DToCs can help map broad patterns and drive resource allocation.

Business Impact

Governments can use DToC to better orchestrate personalized services and manage crises, for example, modulate climate crisis against human loss. Aggregated data can help citizens expedite government services, especially in smart city environments. Citizens or governments can drive DToC-based crowdsourcing analysis that mirrors reality to assess government services in real time. Governments can integrate services into systems such as passport control, social credit system and shopper tracking solutions.

Drivers

- The Chinese government is gradually improving and optimizing regulatory and organizational foundations. Examples include Data Security Law of the People's Republic of China, Personal Information Protection Law of the People's Republic of China, and the upcoming National Data Bureau, to promote secure and controllable data exchange across public and private sectors.

- There is an increasing proliferation of both structured and close-to-structured data on creating digital citizen journey maps.

- Increased integration of government, financial and commercial systems, and interest in creating citizen 360 models are driving pilots of DToC in multiple areas.

- Citizens' interest in improved health and safety systems is increasing. And the need for proactive, real-time, personalized government services customized to citizens (for example, for emergency medical services) and longer-term, more complex solutions that serve elderly patients or inmates is driving investment from a broad range of government organizations. Some examples include solutions to monitor elderly patients using IoT-enabled trackers, smart camera monitoring systems that track a specific police officer, or inmate tracking solutions under home arrest.

- The flexibility of digital twin models from simple to complex models, and the ability to integrate data from siloed services, enable government agencies to build out citizen services to serve individuals as well as the public at large.

Obstacles

- Concerns around privacy and government access to citizen data are leading to citizen concerns and pushback.
- High costs for DToC projects inhibit scaled deployment, especially with a lack of commensurate benefits to citizens or government agencies.
- Conflicting government agencies' objectives, political infighting on data rights, and incompatible regulation on the use of citizen data and on how to respect rights to privacy.
- Incompatible systems across government, commercial and healthcare silos, driving high costs for data governance, integration and analytics, affecting incident handling efficiency and limiting communication.
- Lack of skills to drive the use of the citizen twin and knowledge on possible use cases in government agencies slow down adoption.
- There is an overall low awareness of DToC by government organizations and urban partners, in terms of how a DToC approach can be built and used in an effective manner.

User Recommendations

- Establish clear benefits for the government agency(ies) to justify not just the cost of developing the DToC, but also of changing the culture and adapting processes to the new data.
- Establish clear benefits to citizens such as shortening passport control lines, simplifying access to medical care, or aligning payments from citizens for use of a toll road.
- Test and validate acceptance by the public by communicating the DToC offering and its benefits.
- Build robust privacy and digital ethics policies that clarify what data is collected, who has access to it, how it is protected, and citizen remediation processes.
- Test IoT sensor and analytics capability to ensure accuracy and validity for the physical part of a DToC.
- Invest in integration skills to connect into a heterogeneous set of applications and data sources and critical incident handling.
- Build data exchanges to protect data, while enhancing the granularity of citizen data used to drive government services.

Sample Vendors

Alibaba Cloud; Apple; Google; Taiji Computer; Tencent; Vantiq; ZKBRAIN

Gartner Recommended Reading

Market Insights: Unique Regional Dynamics Require Tailored Strategies for Smart Cities in Asia

Life Cycle Management of Software-Defined Vehicles: Step 3 — Vehicle Digital Twin 2.0

Quick Answer: Privacy Basics for a Digital Twin of a Customer

Emerging Tech: Tech Innovators for Digital Twins — Digital Business Units

Sliding into the Trough

Edge Analytics

Analysis By: Peter Krensky

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Analytics is the discipline that applies logic (e.g., “rules”) and mathematics (“algorithms”) to data to provide insights that drive organization strategy and decision making. “Edge” analytics means that the analytics are executed in distributed devices, servers or gateways located outside of data centers and public cloud infrastructure closer to where the data and decisions of interest are created and executed.

Why This Is Important

Gartner client inquiries about the impact of edge on data and analytics continue to increase. With a growing relevance, by 2025, more than 50% of enterprise-managed data will be created and processed outside the data center or cloud. Demand for real-time decision making closer to where the data of interest is created and stored is one of many drivers for edge analytics.

Business Impact

The origins of edge analytics offerings were primarily in the support of decentralized deployments for device-isolated insights. However, connectivity advances, demands for cross-device analytics and innovations surrounding IoT have dramatically increased the scale and complexity of edge analytics use cases. Real-time event analytics and decision making, autonomous behavior of assets, and fault-tolerant applications hold tremendous potential value for enterprises in many industries.

Drivers

- Advantages of edge analytics include faster response times, reduced network bottlenecks, data filtering, reliability, increased access to data and reduced communications costs.

- Data sovereignty and governance issues related to sensitive/regulated data can constrain D&A teams from adopting centralized/cloud-based environments — moving data outside its originating geography can violate sovereignty regulations. By locating analytics in edge environments, the data remains in the originating locations, increasing the likelihood of compliance.

- The increase of distributed cloud and hyperconverged solutions from public cloud providers, including Amazon Web Services (AWS Outposts), Microsoft (Azure Stack Hub) and Google Cloud (Anthos), are further decentralizing previously cloud-restricted workloads. This perimeter expansion of the cloud brings compute and storage closer to the edge — creating new possibilities for edge-centric analytic workloads.

- 5G networks continue to grow in relevancy and, combined with mobile edge computing, will increase edge analytics use cases — particularly for latency-sensitive deployments.

- More analytics solutions, such as those supporting IoT use cases, need to operate in disconnected (or intermittently connected) scenarios. By bringing more powerful analytics capabilities to edge environments, these solutions need not rely on centralized data centers or cloud resources. As demand grows for “smarter” physical assets in many industries, supporting autonomous behavior will be a common requirement.

Obstacles

- Some of the disadvantages of edge analytics include increased complexity, lack of cross-device analytics, overhead of device maintenance and technical currency demands.

- Architectural design and development best practices for traditional or cloud-resident analytics typically assume or prioritize data/analytics centrality and do not carry over directly for edge analytics use cases.

- Vendor choices include two extremes in terms of provider scale — with early and unknown startups competing head-to-head with global megavendors. This drives a mix of platform/protocol standards and complicates going concern considerations for prospective buyers.

- Edge analytics can increase the complexity of enterprise standards and governance (data privacy, security, etc.), which has the potential to delay overall value realization objectives.

User Recommendations

Analytics leaders should consider edge analytics across the following five imperatives:

- Provide analytic insights for individual devices, assets or a larger distributed site even in the midst of disconnection from cloud or data center infrastructure and resources (e.g., driverless cars).
- Provide data sovereignty. Many regulations or data privacy laws require data be kept in the location of origin or the organization deems the transfer of data to introduce too many security vulnerabilities.
- Adapt to scenarios where network connectivity does not have the ability to support desired latency or stability requirements.
- Address scenarios where cross-device interdependencies serving as part of a larger system require edge-resident analytics.
- Redesign analytic strategies where it costs too much to upload the full volume of generated data and where there is no benefit to moving device-level data to a central location for aggregated analysis.

Sample Vendors

Amazon Web Services; Arundo; CloudPlugs; FogHorn; Microsoft; PTC; Samsara; TIBCO Software

Gartner Recommended Reading

Market Guide for Edge Computing

Innovation Insight for Edge AI

The Edge of the Edge Overview

Emerging Technologies Impact Radar: Edge AI

Data Fabric

Analysis By: Mark Beyer, Ehtisham Zaidi, Roxane Edjlali, Sharat Menon, Robert Thanaraj

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Definition:

A data fabric is a design framework for attaining flexible and reusable data pipelines, services and semantics. The fabric leverages data integration, active metadata, knowledge graphs, profiling, ML and data cataloging. Fabric overturns the dominant approach to data management which is "build to suit" for data and use cases and replaces it with "observe and leverage."

Why This Is Important

Data fabric leverages traditional approaches while enabling the enterprise to adopt technology advances and avoids "rip and replace." It capitalizes on sunk costs and simultaneously provides prioritization and cost control guidance for new spending for data management. It leverages concepts and existing platforms/tools or implementation approaches. It offers flexibility, scalability and extensibility in infrastructure for humans or machines to assure data is consumable across multiple use and reuse cases on-premises, multicloud or hybrid deployments.

Business Impact

Data fabric:

- Increases identification, deployment and availability of data for reuse at scale.
- Provides insights to data engineers by standardizing repeatable integration tasks, improving quality, and more.
- Adds semantic knowledge for context and meaning, and enriched data models.
- Evolves into a self-learning model that recognizes similar data content regardless of form and structure, enabling connectivity to new assets.
- Enables observability across the data ecosystem.
- Reduces maintenance, support and optimization costs associated with managing data.

Drivers

- The dearth of new staffing or personnel seeking data management roles and the attrition of experienced professionals leaving the practice area has increased the demand for more efficient data reuse.
- Demand for rapid comprehension of new data assets has risen sharply and continues to accelerate, regardless of the deployed structure and format.
- Increased demand for data tracking, auditing, monitoring, reporting and evaluating use and utilization, and data analysis for content, values and veracity of data assets in a business unit, department or organization.
- Catalogs alone are insufficient in assisting with data self-service. Data fabrics capitalize on machine learning (ML) to provide recommendations for integration design and delivery, reducing the amount of manual human labor that is required.
- Significant growth in demand and utilization of knowledge graphs of linked data, as well as ML algorithms, can be supported in a data fabric to assist with graph data modeling capabilities and use-case generic semantics.
- Organizations have found that one or two approaches to data acquisition and integration are insufficient. Data fabrics provide capabilities to deliver integrated data through a broad range of combined data delivery styles including bulk/batch (ETL), data virtualization, message queues, use of APIs, microservices and more.

Obstacles

- Organizations will keep applying budget or staff to one-off and point-to-point integration solutions.
- Differing design and semantic standards used by various vendors to document and share metadata create challenges in its integration and effective analysis to support a data fabric design.
- Fabric needs analytic and ML capabilities to infer missing metadata. This will be error-prone at first with staffing and resources assigned to competing demands in advanced analytics, data science and AI near the data consumption layer.
- Active metadata management practices lag behind data fabric adoption but are critical to its implementation.
- Diverse skills and platforms demand a cultural and organizational change from data management based upon analysis, requirements and “design then build” to discovery, response and recommendation based upon “observability and leveraging.”
- Improper split from data mesh implies choosing one approach over another and not a complementary relationship.
- Inexperience in reconciling a data fabric with legacy data and analytics governance programs will confound implementers.

User Recommendations

- "Active metadata" and leveraging the inherent practices to it is mandatory in a data fabric (covered separately).
- Invest in an augmented data catalog that permits multiple ontologies over top of business data taxonomies and is alerted to new use cases for data and the related business units utilizing data.
- Deploy data fabrics that populate and utilize knowledge graphs in targeted areas where adequate metadata and metadata management practices already exist.
- Ensure business process experts can support the fabric by enriching knowledge graph capabilities with business semantics.
- Evaluate all existing data management tools to determine the availability of three classes of metadata: design/run, administration/deployment and optimization/algorithmic metadata. When adopting new tools, favor those that share the most metadata.
- Do not permit SaaS solutions to isolate their metadata from access by PaaS solutions that orchestrate across solutions.

Sample Vendors

Cambridge Semantics; Cinchy; CluedIn; Denodo Technologies; IBM; Informatica; Semantic Web Company; Stardog; Talend

Gartner Recommended Reading

Data and Analytics Essentials: How to Define, Build and Operationalize a Data Fabric

Quick Answer: What Is Data Fabric Design?

Emerging Technologies: Critical Insights on Data Fabric

LEO Satellite Communication Services

Analysis By: Bill Ray

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Low earth orbit (LEO) satellites operate at an altitude of less than 4% of the distance compared to a traditional communication satellite. Connecting to satellites in LEO uses significantly less power, supporting low latency and faster data. However, coverage requires a large number of satellites, most of which will have a limited life span. Several companies have launched LEO services for broadband internet access, while others are focused on low-speed (and low-power) IoT connectivity.

Why This Is Important

Innovations from the smartphone industry, along with lower launch costs, make LEO constellations economically viable. The orbit makes power consumption and latency comparable to terrestrial services. As of 2Q23, Starlink is providing internet access to a million customers and OneWeb is providing global connectivity to enterprises. Other operators (including Amazon) are still working toward commercial services.

Business Impact

LEO services make broadband internet and IoT data globally available. Companies and employees can assume that internet access and IoT sensing will always be available, which would remove network access as a limit on locations to work or live. Geography will cease to be a factor in recruiting the best staff and supporting the most profitable customers. This connectivity is extending to include airplanes, ships and sea platforms, creating a ubiquitous internet (and corporate intranet).

Drivers

- LEO satellite constellations are being launched to address two distinct markets: broadband internet access and low-power IoT connectivity. These markets are being addressed by different companies using different constellations, as the requirements are quite distinct. Other customers include airlines, ships and the military.

- Satellite broadband is relatively expensive (SpaceX's Starlink charges $99 per month, plus $499 for installation) and won't compete with already installed fiber to the cabinet or home. However, we have calculated that there are enough homes without connectivity to sustain the Starlink service with reasonable penetration.

- LEO satellites can also provide backhaul for cellular services — a single satellite uplink can provide connectivity to a cell tower providing 5G, 4G, Wi-Fi or any other local access technologies. This reduces the cost of network deployment for cellular operators, extending coverage into areas that have previously been economically impossible.

- As of 2Q23, Starlink and OneWeb are both offering commercial services. But these will need to compete with offerings from Amazon's Project Kuiper network, as well as competing projects such as E-Space, SATNet and Telesat.

- The 3rd Generation Partnership Project (3GPP) is creating standards for integrating LEO services with terrestrial networks, initially for narrowband (IoT and messaging), but in recognition that supplementary coverage from space (SCS) will become an increasingly important factor in providing global connectivity.

- IoT connectivity is a different market, focusing on low cost and low power to provide global asset monitoring and tracking. While asset tracking remains the primary application, condition and environmental monitoring will also be an important use case.

Obstacles

- To provide oceanic and remote region coverage (needed by military customers), satellite-to-satellite (intraconstellation) links are required. Starlink is testing such connections, but other constellations are still at the planning stage.
- Customer equipment currently costs more than $1,000, and subscription costs will vary widely between providers.
- Maintaining 30,000 satellites, with a life of five years, requires 500 new satellites per month. Current launch vehicles, such as SpaceX's Falcon 9, can launch 60 satellites at a time. This will not be sufficient, so larger launch vehicles (such as SpaceX's Starship or Blue Origin's New Glenn) will be needed.
- Satellite operators are required to avoid interfering with incumbent deployments, limiting the radio spectrum they can use. We expect that radio spectrum access will become a key point of negotiation, and perhaps litigation, in the next five years.

User Recommendations

- Exploit the rapid development of LEO services by adding satellite connectivity into strategic workforce and business planning.
- Prepare for international availability by liaising with local regulators and resellers. LEO services are inherently global, so these will spread internationally as quickly as regulators will allow.
- Protect investment by validating the technical and financial ability of your provider to launch and maintain its constellation.
- Mitigate against requirements for proprietary equipment by planning for a reinstallation in five years, allowing for updated equipment or a change of satellite service provider.

Sample Vendors

Astrocast; Myriota; OneWeb; SpaceX

Gartner Recommended Reading

Maverick* Research: LEO Satellites Will Trigger the Revolution That 5G Has Failed to Deliver

3 World-Changing Opportunities Emerged While You Were Fighting COVID-19

Workstream Collaboration

Analysis By: Mike Gotta

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Workstream collaboration (WSC) tools create a persistent, chat-based workspace, divided into channels. Tools integrate direct and group messaging, along with meeting capabilities, file sharing, alerts, activity streams, tasks, bots, search and other plug-ins. They also come with APIs for customized applications.

Why This Is Important

WSC combines channel-based chat with task, meetings, content and application plug-in capabilities, making it a foundation for work hubs and modern teamwork. WSC is broadly deployed to improve productivity, providing means for organizations to broadly leverage generative AI, large language models, and Generative AI (ChatGPT). Advanced use for process-driven, operational or external use cases are emerging as a solution pattern called “collaborative workflow automation.” WSC tools inadequately support frontline workers today.

Business Impact

WSC is a core technology for digital workplace work hubs, often integrated with a variety of apps including visual collaboration and collaborative work management. By reducing digital friction, teams can work more productively to reduce cycle times. WCS tools acts as a policy control point for security, compliance, and overall governance. WCS can be used for a variety of work related to project, service and support, sales, and marketing activities. WSC tools are also used as chat-based “water coolers” to help team unity.

Drivers

- The shift to hybrid working and requirements for effective teamwork when workers are dispersed makes WSC tools a focal point for integration of other tools, such as visual collaboration, into a digital workplace work hub.

- WSC tools form the core for work governance efforts, because they provide a centralized experience for organizations to satisfy communication, information-sharing and work management needs, while enabling IT to centralize policy, security and compliance controls.

- WSC is becoming the launch point for new classes of collaboration experiences that are tightly coupled with teamwork. Examples include visual collaboration apps and collaborative workflow automation (CWA).

- WSC vendors are delivering generative AI/ChatGPT capabilities into their products. AI will help employees summarize chat streams, find information, auto-create posts and discover hidden expertise and experts.

- WSC expectations increasingly include requirements for more-complex work scenarios beyond everyday productivity. Desires for WSC to better support low-code no-code features and the ability to compose business components into the team experience are beginning to emerge as organizations explore CWA use cases.

Obstacles

- WSC tools are primarily designed for everyday productivity. However, some WSC vendors are shifting to address process, operational and frontline scenarios. If organizations deploy multiple tools without clear business value, the result may be increased costs and IT management complexity.
- Vendors are not collaborating on message interoperability. The use of multiple tools can create "chat silos" and lead to tool sprawl. Third-party vendors use public APIs to exchange messages between tools and can raise risk concerns.
- Frontline workers have not adopted WSC tools to the same extent as office workers.
- Employees struggle to socialize in WCS tools. "Water cooler" chat channels may not be easily discovered or sustained, making it difficult for staff to informally network with peers they work with.
- Low-code and no-code development in WSC are still emerging in terms of ease of use and output capabilities. Proprietary approaches can increase lock-in to the platform.

User Recommendations

- Assume incumbent suite vendors (Microsoft or Google) address everyday productivity needs for WSC use. Remain open to adding WSC tools for process-driven, role-based and operational business scenarios based on business use case and value. Consider frontline workers' needs as being "stretch goals" for WSC vendors.
- Prioritize internal communications, use of influencer networks, analytics, training, and best practice communities to help employees effectively use WCS tools.
- As team managers define the structure for how teams collaborate using WCS, make sure there is a high priority placed on intentional collaboration practices and etiquettes. This includes tactics to reduce "noise." Generative AI will require additional governance and peer learning for effective use.
- Assess emergence of new capabilities related to superapps, CWA, generative AI, and low-code no-code thoroughly since new technologies, development practices, work hubs, and mobile experiences can present change management and risk issues.

Sample Vendors

Alibaba Group; Coolfire Solutions; Mattermost; Microsoft; Rocket.Chat; Salesforce (Slack); Symphony

Gartner Recommended Reading

Innovation Insight for Collaborative Workflow Automation

Forecast Analysis: Social and Collaboration Software in the Workplace, Worldwide

Quick Answer: How Will AI in Microsoft 365 Copilot Impact the Workplace?

Quick Answer: How Can Digital Workplace Promote Employee Strong and Weak Ties?

Quick Answer: How Does a Superapp Benefit the Digital Employee Experience?

Edge Security

Analysis By: Neil MacDonald

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Edge security offerings protect the integrity of the hardware, operating system, application platform, application workload, its data and its network communications at distributed edge computing locations.

Why This Is Important

Like any IT system, edge computing locations are targets for attack, including data theft, data poisoning, denial of service and placement of malware (for example, Bitcoin mining). Edge security combines the requirements of data center computing security with the scale, remoteness and heterogeneity of mobile and Internet of Things (IoT) computing security.

Business Impact

For edge computing strategies to succeed, the integrity of edge computing workloads and data must be protected. Without protection, edge computing capabilities could be rendered inaccessible and the data could be stolen, copied or tampered with, and adjacent edge nodes and devices could be attacked. Edge attacks can lead to potentially catastrophic results that could threaten health and safety if monitoring and control signals are lost, tampered with or spoofed.

Drivers

- Driven by network constraints and costs as well as privacy and compliance requirements, organizations are expanding workloads to the edge — and security needs to be a part of this.
- Sensitive data and intellectual property will be stored at — and transmitted from — the edge, so must be protected.
- New security solutions and approaches are needed that securely support intermittent access and protect from physical tampering and theft.
- The standardization of edge computing software stacks around containers and Kubernetes will allow cloud-native security concepts to be modified for the edge.
- Enabling remote access/automated control of systems that control industrial processes where failures can result in injury or loss of life requires a high level of security.
- Edge hardware upgrades and replacement cycles provide opportunities for edge security improvements.

Obstacles

- The historic diversity of hardware and application platforms makes it difficult to develop a single-edge security strategy.
- The market for edge security is emerging with a large number of overlapping offerings.
- Most edge hardware devices were not designed with adequate hardware security controls.
- Security wasn't a high priority during the procurement of most edge computing offerings.
- Most edge computing platforms won't have the capacity for a standard security stack.
- Complete edge security protection strategies must address the entire stack — hardware, OS, application platform, application, data and network security and their life cycle.

User Recommendations

- Design protection that treats the network as compromised, hostile and intermittent.
- Restrict all access (including admins) to/from the edge using a zero trust network access (ZTNA), secure access service edge (SASE) or security service edge (SSE) offering.
- Make tamper-resistance and hardware life cycle management a part of security control evaluation — assuming that hardware will be attacked, tampered with, stolen, or destroyed.
- Include at least mandatory data encryption, network security, workload integrity, application control, memory protection, behavioral monitoring and intrusion detection/prevention in an edge protection strategy and product evaluation.
- Favor offerings that are centrally managed — ideally cloud-based — and provide for tightly controlled administrative access.
- Require the use of identity-based policy management for edge equipment — ideally preprovisioned, certificate-based and stored in hardware.
- Require vendors to support Linux containers and container-based security offerings, which are expected to be widely used for distributed edge computing architectures.

Sample Vendors

Amazon Web Services (AWS); Appgate; Dell Technologies; Fortinet; Hewlett Packard Enterprise (HPE); Johnson Controls (Tempered Networks); Red Hat; StorMagic; VMware; ZEDEDA

Gartner Recommended Reading

Market Guide for Single-Vendor SASE

2022 Strategic Roadmap for SASE Convergence

Building an Edge Computing Strategy

Live Facial Recognition

Analysis By: Michael Brown

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Live or automatic facial recognition technology uses computer vision to identify people of interest from a live video stream, based on preexisting photographs. Different from other forms of face recognition, live facial recognition can identify people without their cooperation in posing for a camera.

Why This Is Important

Live facial recognition can automatically identify missing people and people of interest to law enforcement. Video from fixed and mobile cameras provides ever-growing data streams that exceed human ability to effectively monitor and analyze. Policing organizations in many countries have implemented live facial recognition to bolster traditional law enforcement capabilities. As algorithms improve and privacy concerns ameliorate, live facial recognition adoption will grow more rapidly.

Business Impact

Law enforcement has aggressively implemented video surveillance as a more effective and lower-cost solution to monitor an environment and find people of interest and, ultimately, protect the public from possible threats. This use of video surveillance has exceeded any nonautomated means to analyze imagery. Live facial recognition provides an opportunity to extract more information — and more consistently — from the great volume of video streams now available.

Drivers

- **High volume of video data** — Video surveillance by law enforcement is a growing industry. AI is now the only practical means of digesting all the video information being streamed and retained by policing agencies. Many countries, including the U.K., Argentina, China, South Korea, Serbia and India, have implemented live facial recognition. Initially, the technology has been used for fixed cameras' video streams. However, police accountability measures have rapidly increased vehicle, body and drone camera use, and limited forms of live facial recognition have been tested with body cameras in the U.S.

- **New use cases** — Beyond traditional law enforcement use, the COVID-19 pandemic gave rise to additional uses of the technology. The pandemic presented new needs for rapid change in citizen behavior and government interest in monitoring compliance. Live facial recognition cameras have been coupled with thermal imaging for body temperature to identify potential virus carriers and enforce quarantine restrictions on public environments.

- **Efficiency** — Policing agencies have a charter to ensure law compliance. This has always entailed monitoring public spaces. The use of video — and now the use of AI to interpret video streams — is the technological progression of traditional patrolling. Live facial recognition is more cost-effective than hiring personnel to increase monitoring capabilities. As with other government functions, law enforcement is subject to budget limits. Consequently, demand, data and technology are coming together to increase the use of live facial recognition.

- **Algorithm improvement** — Facial recognition accuracy is the subject of at least one formal testing program by the U.S. National Institute of Standards and Technology's (NIST's) Face Recognition Vendor Test. Testing over the years has shown steady improvement in the technology.

Obstacles

- **Privacy concerns —** Public privacy concerns have led to legal restrictions on the use of facial recognition. Citizens may object to systematic monitoring and identification in public spaces. Civil liberty advocates seek to define rules for use, which delays and constrains deployment. This is apparent in the U.S., where several states and many cities have restricted the use of the technology, and in the European Commission's legislative proposal for the Artificial Intelligence Act.

- **Accuracy concerns —** Higher rates of false positives for some groups appear as bias in facial recognition. This inaccuracy has driven public objections, and not without merit. Studies by the MIT Media Lab and NIST confirmed lower accuracy for some demographic groups. Improved algorithms and more-diverse AI training datasets are increasing accuracy, but public concerns will not be easily reduced.

User Recommendations

Given the increased availability of data, the inherent monitoring function of law enforcement and evolving technological maturity, live facial recognition use will continue to grow. Technology leaders responsible for supporting law enforcement should:

- Assess permissibility and ethical appropriateness of live facial recognition by working with internal counsel before planning any use of the technology.

- Help to alleviate citizen concerns by coordinating with public relations and community outreach staff to provide transparency about how the technology will be employed and which privacy and other safeguards are in place.

- Maintain a human-decision element by jointly developing operational guidelines with mission operations staff.

- Gauge and communicate technology limitations by using independent testing data for the AI methods involved.

Sample Vendors

Cognitec; iOmniscient; NEC; Oosto

Gartner Recommended Reading

Tool: Assess How You Are Doing With Your Digital Ethics

A Comprehensive Guide to Responsible AI

Public Safety Predictive Analytics

Analysis By: Bill Finnerty, Michael Brown

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Public safety predictive analytics is the use of predictive modeling to achieve mission outcomes by public safety and law enforcement (PS&LE) agencies. Public safety predictive analytics leverages internal and external data, with due diligence being paid to limiting the impact of bias in historical datasets to improve strategic planning and tactical operational decisions by leadership and those deployed in the field.

Why This Is Important

Preventing an incident, or event, or addressing one quickly is less costly to society than reacting to and clearing up after it has occured. Predictive analytics, enabled by new models and advances in machine learning, make the shift from responsive to proactive service delivery for PS&LE agencies feasible when deployed in a transparent manner that garners public trust.

Business Impact

PS&LE can use predictive analytics to create proactive service delivery models that achieve mission outcomes. Use of predictive analytics allows for:

- Corrections institutions can reduce the use of force events because of inmate violence or the number of days needed to complete programs.
- Police departments can position resources to curb reckless driving and respond to incidents faster.
- Fire departments can identify areas of high fire risk and remove flammable ground clutter.

Drivers

- Advances in machine learning provide a broader set of models which reduces implementation and operational costs.
- Providers are increasing the value of their solutions by supplementing them with emerging technologies from partners.
- Society is holding PS&LE accountable to demonstrate equity in service delivery.
- Government organizations in general, and PS&LE agencies specifically, are struggling with staffing in the current employment market. Frequently, this results in open positions and shifts that are understaffed, affecting officer readiness.
- A growing number of analytics and public safety and justice core system providers are developing predictive analytics, location intelligence and machine learning solutions that are being delivered via SaaS model. Therefore, PS&LE agencies have less need for data science, artificial intelligence (AI) modeler or other related skills in-house.
- Through improved data sharing efforts, expanded datasets available through cross-disciplinary response efforts are making additional, previously untapped data available.

Obstacles

- The data quality and data management capabilities of PS&LE agencies may limit their ability to leverage predictive analytics.
- Public concerns over data bias and misuse of data by PS&LE agencies may cause leadership to be hesitant in experimenting with predictive analytics.
- The risk-averse nature of PS&LE agencies, particularly for those that have had negative experiences with predictive analytics previously, may manifest as hesitation to implement a new solution.
- The use of predictive analytics will require a culture change in many PS&LE agencies, which can be particularly difficult for organizations in this segment of government. In many cases, it will be necessary to shift to using insights to inform decision making, versus fully automating decisions.
- Limited data discovery and data-sharing capabilities constrain the ability to develop the needed models for predictive analytics use in PS&LE.

User Recommendations

- Implement, if not already active, a data governance program to focus on data quality and management. Use this as an opportunity to begin or further the adoption of national data standards, such as the National Information Exchange Model, and update system configuration for records management systems and computer-aided dispatch to reduce data entry errors.
- Establish an ethics advisory board for analytics and AI to promote transparency and accountability.
- Engage current vendors to understand their roadmaps for implementation of predictive analytics or what partnerships they have to bring these capabilities to their solutions or platform.
- Work with internal and external stakeholders to establish standards for the acceptable use of predictive analytics and processes to determine continual acceptance of its use.
- Include predictive analytics and AI in the risk management process. Implement regular, independent audits of predictive analytics and AI solutions to check for system bias and data misuse. Be transparent with finds and remediation efforts.

Sample Vendors

DataWalk; IBM; KeyCrime; Microsoft; Palantir Technologies; SAS Institute; Semantic AI

Climbing the Slope

Computer Vision in Government

Analysis By: Albert Gauthier, Dean Lacheca

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Early mainstream

Definition:

Computer vision (CV) is an artificial intelligence (AI) technique used to capture, process and analyze real-world images and videos to allow machines to extract meaningful, contextual information from the physical world. At all levels of government, CV can be applied to new and existing image and video source data to expand the data's relevance, accelerate the speed in providing insights and inform decision making.

Why This Is Important

Use cases for CV in government continue to grow with opportunities emerging for use in all sectors of government. With the ability to extract and classify metadata from images and videos, CV has the potential to extract the value of data in government, evolve service delivery and improve the safety and efficiency of the government workforce. The privacy implications of CV may be politically significant, requiring ethical consideration and regulatory evolution.

Business Impact

CV augments the government workforce's capabilities and its partners' streamlining and regulatory activities, and accelerates data capture. In public safety, law enforcement examples include:

- Facial recognition and identifying attributes to improve security and surveillance.
- Real-time objective recognition/identification to alert and highlight suspicious objects.
- Automated license plate readers and hot-sheet matching.
- Signature verification and fraud detection.

Drivers

- **Proliferation of cameras and other sensors:** The proliferation of government-controlled cameras and other sensors is generating exponential increases in image data, creating a critical and growing demand for methods to automate analysis, and manage and extract value from that data. This new situation is manifested by the pervasive expansion of consumer security cameras which can share images and videos with law enforcement, the prolonged and extended use of body-worn cameras (BWC), and disease surveillance and symptom detection in public facilities. New video and image content use cases have appeared across a range of government sectors, such as wildfire detection, agriculture inspections and land use mapping.

- **New business models and applications:** CV offers the potential to accelerate the manual analysis of existing image and video source data by governments. Combining CV with new data capture technologies, such as drones and lidar, allows governments to explore new ways of working. For example, physical inspections, such as infrastructure inspections of bridges, can be made safer, more efficient and cost-effective.

- **New neural network architectures, AI models and algorithm enhancements:** New generative AI allows ingestion of images and analysis at scale. Technology improvements have reduced costs and improved performance.

- **Security, compliance and accountability:** Pressure on governments to be more proactive and frictionless in service delivery, and higher degrees of accountability for public safety require innovative approaches to service delivery.

Obstacles

- Diverse and evolving compliance requirements outpace technology improvements. High-end systems are expensive to maintain and support, and building business cases with adequate ROI could be challenging.

- Integration with existing systems is problematic due to proprietary interfaces, off-the-shelf solutions and plug-and-play capabilities. Proprietary algorithms and patent pools deter innovation.

- Scaling solutions is often challenging due to the requirement for a high level of customization and service support. High demand and limited supply of qualified technical resources in CV and AI restrain the application of CV.

- Adequate, unbiased training and testing data may be hard or expensive to acquire. Government data source quality may not be high enough to deliver the expected benefits in a cost-effective way. Governments are concerned about community trust and privacy concerns/regulations with CV.

User Recommendations

- Perform an impact assessment of the applications of CV and AI to demonstrate value and ROI. Start to address quality data source issues by establishing master data and built on a data mesh framework from existing government-controlled data assets.
- Focus, initially, on a few small, high-value projects and scale the most promising systems into production using cross-disciplinary teams. Build internal CV competencies and processes for exploiting image and video assets.
- Establish enterprise governance and oversight on tools, technologies and data used in CV and AI to ensure legal, ethical, regulatory and reputational risks are addressed.
- Create clear metrics for CV initiative success, such as officer response time or illegal objects intercepted, to continuously evaluate the business value of efforts.

Gartner Recommended Reading

Case Study: Computer-Vision-Based Environmental Monitoring

Case Study: AI and Automation to Support Government Regulation for Product Safety (Denmark)

Emerging Technologies: Emergence Cycle for Computer Vision

Indoor Location Intelligence

Analysis By: Annette Zimmermann

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Indoor location intelligence refers to services and solutions that generate and analyze data in an indoor environment. It provides analytics and insight on the location (and movement) of objects and people from a historic, real-time or predictive perspective. The underlying technologies are wide-ranging and include Wi-Fi, 5G, Bluetooth low energy (BLE), infrared, ultrasound, RFID, ultrawideband (UWB), video analytics, and lidar.

Why This Is Important

The two broad use cases for indoor location intelligence are people monitoring and asset tracking, and these can be divided into hundreds of subuses. Gartner clients continue to inquire about indoor location intelligence solutions to address a wide range of business problems. Some of the most important among these include the analytics, trends and intelligence associated with counting visitors, performing time and motion studies, finding (mobile) assets, and preventing accidents.

Business Impact

We see the strongest growth of indoor location intelligence in healthcare, retail and manufacturing, followed by logistics and transportation. Each vertical presents different benefits for indoor location intelligence. In healthcare, hospitals benefit from asset tracking, patient tracking and monitoring to increase efficiencies. Manufacturing sites also benefit from multiple use cases, including forklift and people safety, while retailers can both achieve efficiencies and an improved customer experience (CX).

Drivers

- A growing number of indoor location services platforms integrate with computer vision and closed-circuit TV (CCTV) systems to perform people counting and/or measure distance between people.

- New technologies are driving indoor location intelligence forward. For example, 3D mapping and augmented reality wayfinding represent an intersection between location and immersive technologies.

- New types of sensors are emerging as well. “Battery-less” tags that use energy harvesting provide up to two-meter location accuracy at a very low cost ($0.30 to $0.40 at this time).

- Although 5G can generate submeter location accuracy with the 3rd Generation Partnership Project (3GPP) Release 17, the market is still lacking offerings by large communications service providers (CSPs) that are leveraging this release. Instead, some CSPs are leveraging camera- and lidar-based solutions to track people flow in large public venues, such as shopping centers and stadiums, to improve the CX.

Obstacles

- **Technology choice:** Some technologies provide centimeter-level location accuracy, while others’ location granularity is as wide as 4 meters to 5 meters. However, high-precision technologies tend to be more expensive and cumbersome, so there is a trade-off involved. Organizations need to precisely define their use cases to determine what accuracy level intelligence they need.

- **Data privacy:** Location data is sensitive and needs to be treated as such, especially in an external, client-facing situation. Capture and analysis of location data of visitors in large venues, such as shopping centers, museums and stadiums, often requires consent. However, location intelligence allows historical trends and flows to be gathered.

- **Privacy regulations:** These vary widely in different markets. Therefore, location data needs to be analyzed, collected and stored in compliance with local and country-specific regulations.

User Recommendations

- Demonstrate awareness of the direct trade-off between location accuracy and cost, and deploy the technology that supports your location intelligence use case. Overdelivery on accuracy will significantly increase costs, while underdelivering on accuracy will bring limited value and the project may fail.
- Assess which type of customer data you need to collect, store and process, and for what purpose. Establish different scenarios that categorize the data types. These categories should be location data of objects versus people, and be further refined by anonymized versus identifying data. This will help you determine which data privacy regime to follow.
- Employ transparency toward staff, customers, and regulatory authorities on when and what location data is processed/stored. Emphasize upon the safety aspects of your solution and the fact that personal location data is not tracked off-premises.

Sample Vendors

AiRISTA Flow; KINEXON; Motion2AI; Nexite; Purple; Quuppa; Thinaer; Ubisense; Wiliot; Zebra Technologies

Gartner Recommended Reading

Magic Quadrant for Indoor Location Services

Technology Opportunity Prism: Indoor Location Services in Commercial Spaces

Market Guide for Indoor Location Application Platforms

Cloud Analytics

Analysis By: Julian Sun, Fay Fei, Jamie O'Brien

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Cloud analytics delivers analytics capabilities as a service. It often comprises database, data integration and analytics tools. As cloud deployments continue, the ability to connect to both cloud-based and on-premises data sources in a hybrid model is increasingly important. Cloud-native architecture and multicloud deployments are also becoming popular in order to cater to the cloud ecosystem.

Why This Is Important

Adoption of cloud analytics is growing, with most analytics deployments originating in the cloud. The majority of respondents to the 2022 Gartner State of Data and Analytics Cloud Adoption Survey say they are using or plan to use the cloud for analytics and data science. Cloud capability among analytics and BI vendors is also expanding, with emerging capabilities coming from cloud-first. The cloud is an ideal place to build modular analytics capabilities that enable greater agility and reuse of existing investments in support of composable business.

Business Impact

A cloud-enabled, composable platform can innovate by assembling modular analytics capabilities on demand. More advanced analytics can complement key components of the analytics infrastructure in the cloud. The high computational power needed to process tasks such as ML and advanced analytics can be more easily accessed and scaled in the cloud. Business users can pilot cloud-first augmented analytics within a sandbox provisioned by the cloud. Cloud deployment offers faster time to value and more targeted analytics for specific business areas.

Drivers

- To better leverage scalability and elasticity from the cloud, many platforms have rearchitected themselves to be cloud-native.

- To bring more flexibility for organizations that are already using multicloud, vendors are adding more deployment options and management capabilities. These additions enable portability through microservices architectures that are readily supported via containerization across multiple clouds.

- Startups continue to join the analytics market with cloud-first or cloud-only solutions, which are complementary to established platforms.

- The range of capabilities is growing too. Reporting and data visualization were already commodified capabilities. Customers can now also subscribe to self-service data preparation; augmented data discovery; predictive modeling; other advanced capabilities, such as ML or streaming analytics; and even data/context broker services from several vendors.

- The growing cloud DBMS market naturally supports and expands the cloud analytics market as companies embrace the cloud for managing their data.

Obstacles

- Security is a top concern for organizations moving to the cloud. Organizations need to plan how they will integrate their growing cloud analytics deployments with additional data sources, provide access to more advanced (potentially open-source) analytics tools, and embed analytics in business processes. Such planning becomes even more challenging across multiple cloud and on-premises ecosystems.

- Organizations' adoption of the cloud is closely tied to data gravity. Data gravity refers to data's attractive force: As data accumulates and the need for customization, integration and access grows, data has greater propensity to "pull" data services, applications and other data/metadata to where it resides. Thus, smaller organizations with data originating in the cloud have higher adoption rates than larger organizations with data predominantly in on-premises legacy solutions.

- Even as cloud analytics becomes more predominant and mature, organizations with deployment and governance challenges face growth obstacles.

User Recommendations

- Establish a measured approach to move to the cloud incrementally — rather than simply “lifting and shifting” — as cloud analytics becomes a dominant option in most scenarios in the analytics space.
- Include innovative cloud analytics solutions in your portfolio, renovating on-premises components or complementing your on-premises platform, to gain competitive advantage through analytics and BI. Completely disregarding cloud analytics solutions means risk for many organizations, as most vendors don’t focus their R&D efforts on legacy products.
- Be aware of extra costs and the total cost of ownership (TCO) as you adopt new capabilities and offerings within your vendor’s cloud stack. Although cloud analytics solutions do not require significant upfront investment like on-premises solutions do, the former will likely be more expensive to license over four or more years. Also be aware of the performance downgrade in the cloud — benchmark the platform, and carefully plan the data integration approach.

Sample Vendors

Alibaba Cloud; Amazon Web Services; Databricks; Domo; Google; Microsoft; Oracle; Qlik; Sigma Computing; ThoughtSpot

Gartner Recommended Reading

Adopt Cloud Analytics to Drive Innovation

Use Cloud to Compose Analytics, BI and Data Science Capabilities for Reusability and Resilience

Magic Quadrant for Analytics and Business Intelligence Platforms

Critical Capabilities for Analytics and Business Intelligence Platforms

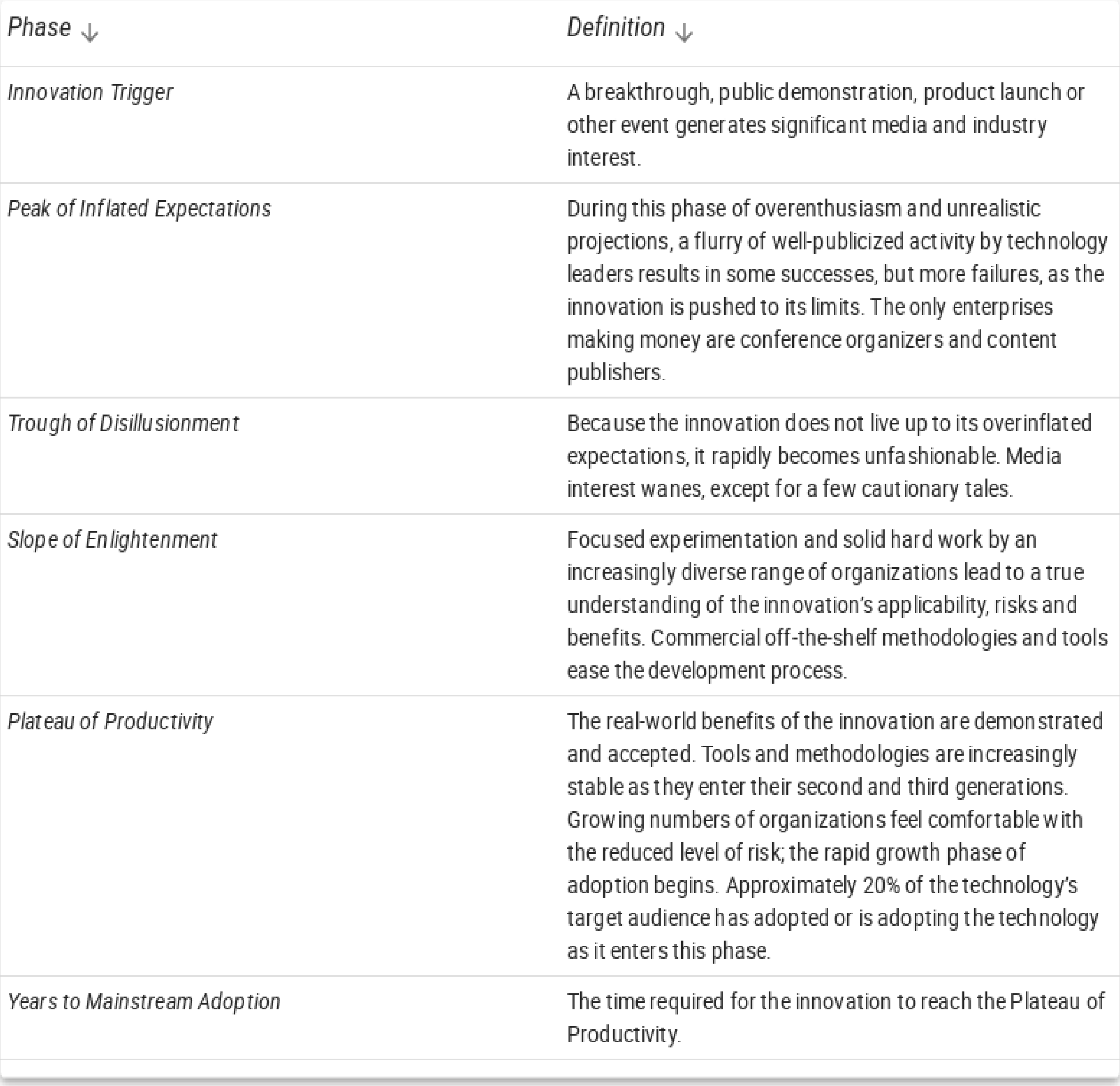
Appendixes

See the previous Hype Cycle: Hype Cycle for Public Safety and Law Enforcement, 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)

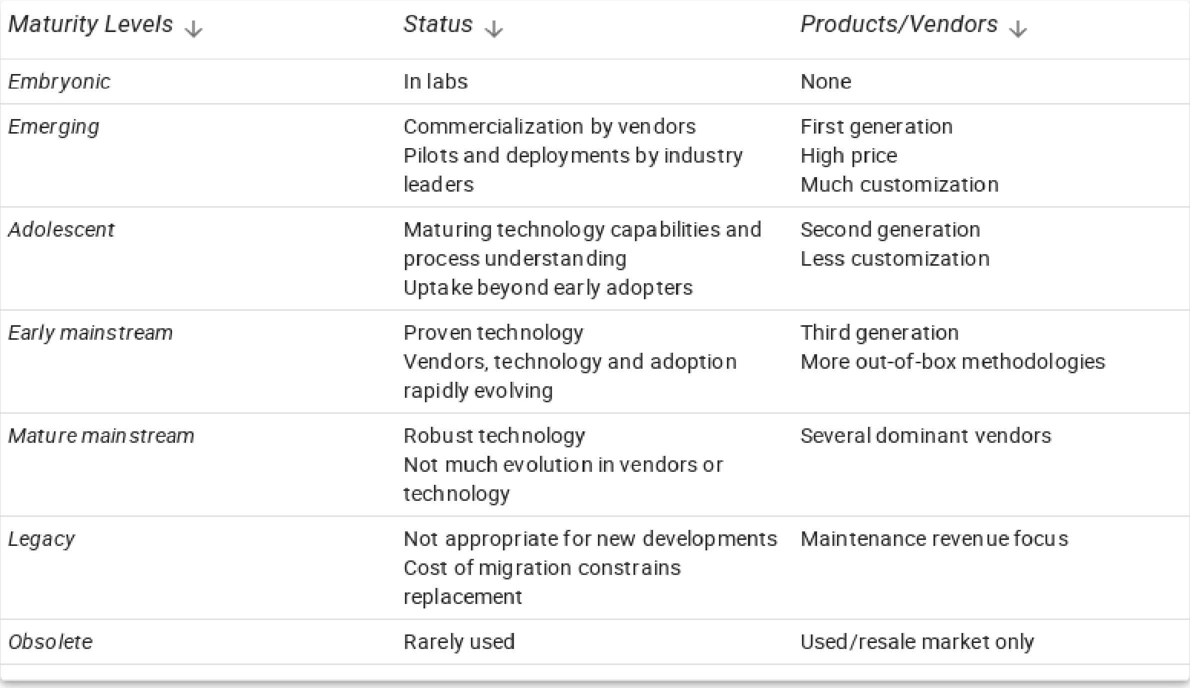
Table 3: Benefit Ratings

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)

Evidence

[1] **2023 Gartner CIO and Technology Executives Survey.** This survey was conducted to help CIOs and technology executives overcome digital execution gaps by empowering and enabling an ecosystem of internal and external digital technology producers. It was conducted online from 2 May 2022 through 25 June 2022 among Gartner Executive Programs members and other CIOs. Qualified respondents are each the most senior IT leader (such as the CIO) for their overall organization or some part of their organization (for example, a business unit or region). The total sample is 2,203 respondents, with representation from all geographies and industry sectors (public and private), including 241 from government. Disclaimer: The results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

[2] ' Vicious cycle': Inside the Police Recruiting Crunch With Resignations on the Rise, ABC News.

Document Revision History

Hype Cycle for Public Safety and Law Enforcement, 2022 - 25 July 2022

Hype Cycle for Public Safety and Law Enforcement, 2021 - 4 August 2021

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 Technology Trends in Government for 2023

Predicts 2023: Justice and Public Safety Seizes New Opportunities to Address Evolving Demands

Postdigital Government: Rethinking Technology's Role in Government

Case Study: Data Science in Public Safety and Justice for Crime Reduction

Case Study: An Ecosystem Approach to Real-Time Data Capture for Emergency Response Planning

Table 1: Priority Matrix for Public Safety and Law Enforcement, 2023

Benefit	*Years to Mainstream Adoption*			
↓	*Less Than 2 Years* ↓	*2 - 5 Years* ↓	*5 - 10 Years* ↓	*More Than 10 Years* ↓
Transformational		Generative AI Live Facial Recognition Public Safety Predictive Analytics Real-Time Incident Center as a Service	Data Fabric Emotion AI in Public Safety Immersive Training in PS/LE LTE/5G-Enhanced Services Responsible AI	
High	Cloud Analytics Edge AI Field Streaming Video Workstream Collaboration	Composable Applications Computer Vision in Government Digital Twin of a Citizen Edge Analytics Indoor Location Intelligence Rapid DNA in Policing Synthetic Data Wearable Monitors for Public Safety	Head-Mounted Displays Smart Robots	
Moderate		LEO Satellite Communication Services	Blockchain for Evidence Edge Security	
Low				

Benefit	*Years to Mainstream Adoption*			
↓	***Less Than 2 Years*** ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓

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)