Hype Cycle for Public Safety and Law Enforcement, 2021

Published 4 August 2021 - ID G00746619 - 119 min read

By Analyst(s): Bill Finnerty, Michael Brown

Initiatives: Government Digital Transformation and Innovation

This Hype Cycle provides insights relative to risk and rate of adoption for emerging 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.

Strategic Planning Assumption(s)

Analysis

What You Need to Know

Public safety and law enforcement agencies are facing unprecedented disruption due to the COVID-19 pandemic, social unrest, natural disasters and other events. The use of technology and data have been essential for public safety and law enforcement agencies in overcoming these challenges, and the role of CIO as strategic partner has never been more important. According to the 2021 Gartner CIO survey, 77% of CIOs working in public safety and law enforcement have seen their relationship with top executive leaders strengthen. [1] With this improved relationship, CIOs must now lead their organizations to sustain the accelerated adoption of digital government. This Hype Cycle provides a key tool that CIOs, executives and program leaders can use to understand the relative maturity and adoption rates of emerging technologies and approaches to adapt their strategic plans. It can also help to meet the challenges their organizations face and keep the focus on outcomes for citizens.

The Hype Cycle

Gartner's public safety and law enforcement Hype Cycle is part of a series of Hype Cycles focused on government, including the Digital Government Hype Cycle and Smart Cities Hype Cycle. There is some overlap between these research notes; CIOs leading jurisdictionwide efforts or partnering with other government organizations should review each Hype Cycle in context.

There are a number of trends impacting public safety and law enforcement agencies adopting digital government (see Top Trends in Public Safety and Law Enforcement for 2021). These trends impact the technologies and approaches that organizations must take to achieve their mission. The Innovation Profiles selected here can aid CIOs in making the best choices for their organization relative to risk and investment strategy. For example, a policing agency focused on intelligent situational awareness might consider the Innovation Profiles of computer vision in government, field streaming video and real-time incident center as a service as means to improve their operational capacity in this area. If this police agency has established a moderate risk tolerance for IT investment, it may consider that computer vision in government 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 that introduce greater risk.

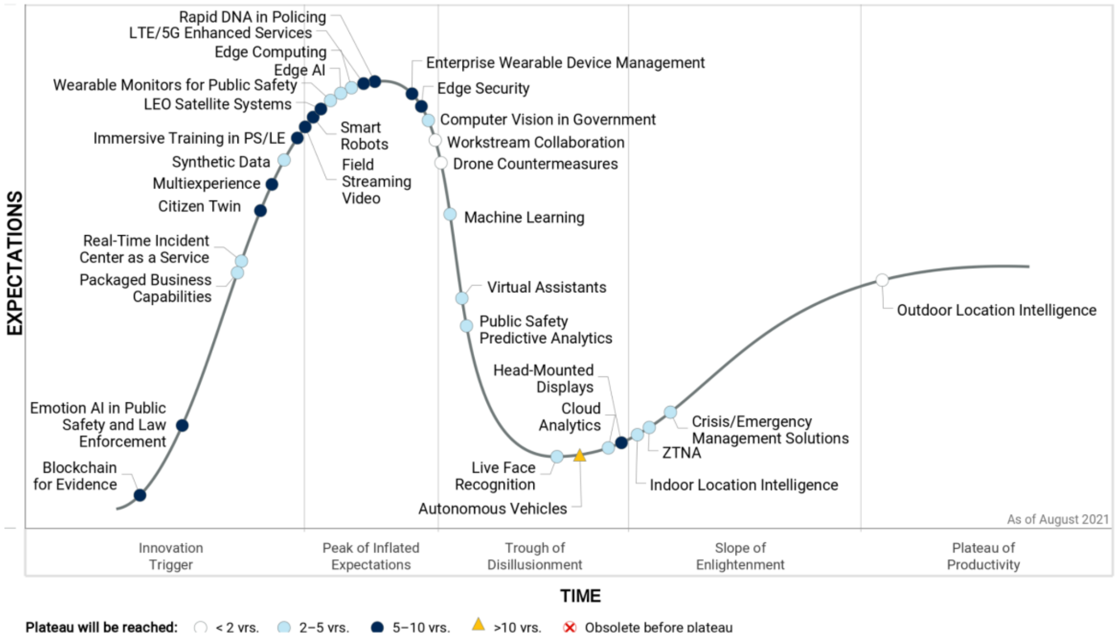
There are a number of innovation profiles that are adopted from other Gartner Hype Cycles that will have a significant impact on public safety and law enforcement (see Table 1).

Table 1: Innovation Profiles Adopted from Other Hype Cycles

Innovation Profile(s)	Impact
Synthetic data	Address significant analytics challenges in public safety and law enforcement such as bias in historic datasets or the small data problem
Workstream collaboration tools	Enable digital workplace efforts and promote better collaboration and coordination between law enforcement agencies and with the public
Edge computing and edge AI	Support public safety and law enforcement organizations in real-time decision making by enabling greater use of IoT*, computer vision, machine learning and analytics in the field
Smart robots and autonomous vehicles	Provide operational advantages as a force multiplier, but they will also present new challenges for organizations
* IoT = Internet of Things	

Source: Gartner (August 2021)

Figure 1: Hype Cycle for Public Safety and Law Enforcement, 2021



Source: Gartner (August 2021)

Downloadable graphic: Hype Cycle for Public Safety and Law Enforcement, 2021

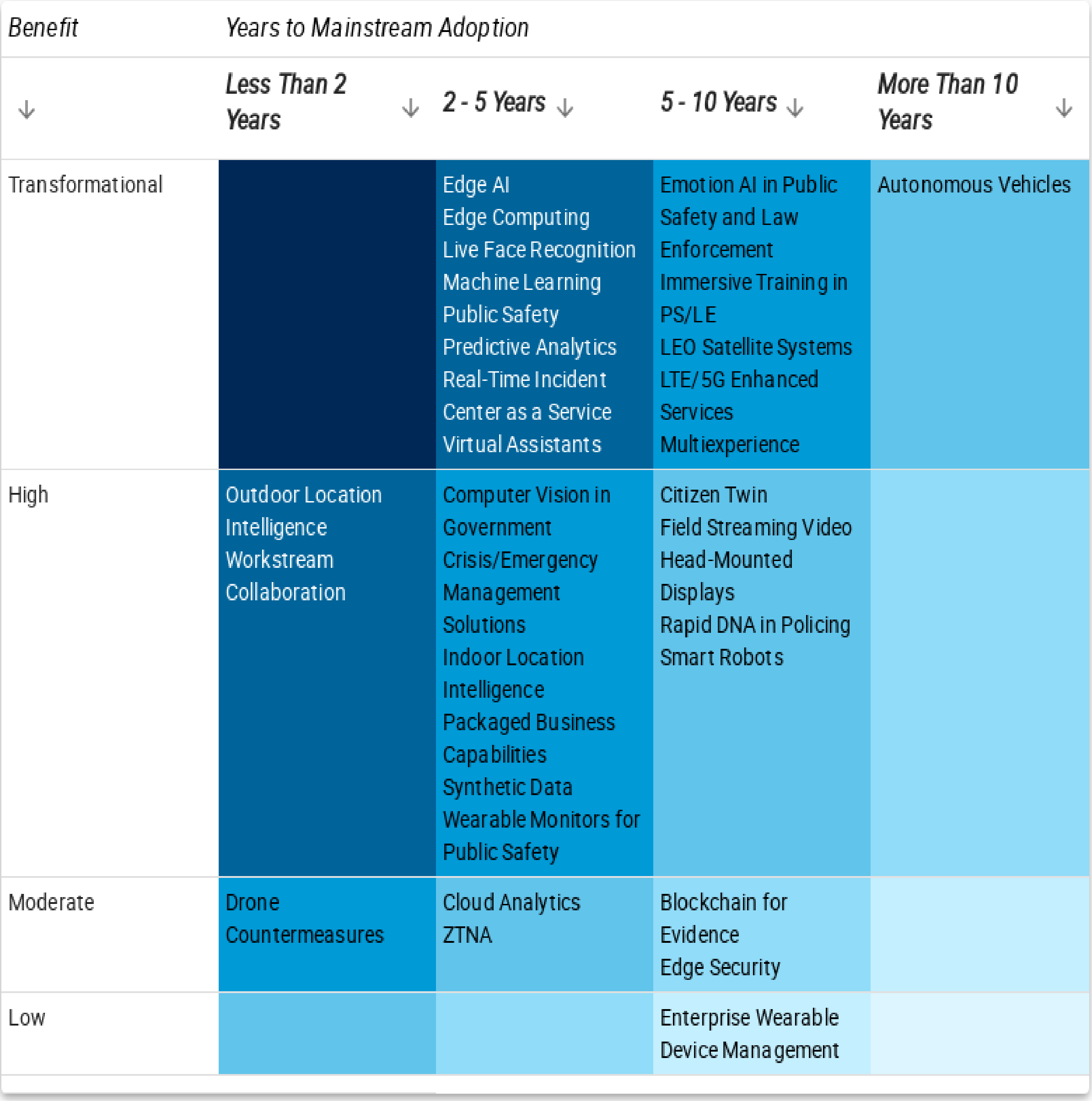
The Priority Matrix

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 level and depth of benefits that can be expected from them. For those technologies in the upper-left section of the Priority Matrix, transformational or high benefits can accrue immediately. Those with similarly significant benefits, but in a less mature state, present strategic opportunities, but should be approached somewhat more cautiously as they introduce more risk. Technologies with longer times to mainstream adoption should be anticipated to have changing market dynamics and changing dominant players over that horizon.

For example, rapid investments in technologies that accrue immediate benefits, such as outdoor location intelligence, should be viewed as quick wins. Conversely, solutions such as swarming robotics involve complexity that will extend time to value. Technologies such as smart robots and head-mounted displays offer high potential, particularly in improving situational awareness, but are relatively immature. 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 2: Priority Matrix for Public Safety and Law Enforcement, 2021

(Enlarged table in Appendix)



Benefit	*Years to Mainstream Adoption*			
↓	*Less Than 2 Years* ↓	*2 - 5 Years* ↓	*5 - 10 Years* ↓	*More Than 10 Years* ↓
Transformational		Edge AI Edge Computing Live Face Recognition Machine Learning Public Safety Predictive Analytics Real-Time Incident Center as a Service Virtual Assistants	Emotion AI in Public Safety and Law Enforcement Immersive Training in PS/LE LEO Satellite Systems LTE/5G Enhanced Services Multiexperience	Autonomous Vehicles
High	Outdoor Location Intelligence Workstream Collaboration	Computer Vision in Government Crisis/Emergency Management Solutions Indoor Location Intelligence Packaged Business Capabilities Synthetic Data Wearable Monitors for Public Safety	Citizen Twin Field Streaming Video Head-Mounted Displays Rapid DNA in Policing Smart Robots	
Moderate	Drone Countermeasures	Cloud Analytics ZTNA	Blockchain for Evidence Edge Security	
Low			Enterprise Wearable Device Management	

Source: Gartner (August 2021)

On the Rise

Blockchain for Evidence

Analysis By: Michael Brown

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

Blockchain is a data security technique based on a shared, distributed ledger that can be used to ensure the integrity of digital information. Blockchain technology maintains a history of records that cannot be altered or tampered with. This immutable characteristic to a digital record is applicable to the management of evidence collecting during investigations, and is used in subsequent court proceedings.

Why This Is Important

Digital evidence has become a ubiquitous aspect of law enforcement and court proceedings. It is essential for the administration of justice to preclude tampering, and to 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 offers the opportunity to preclude tampering, maintain a chain of custody, and to widely, selectively and securely share digital evidence.

Business Impact

Stakeholders and impacts are within the law enforcement ecosystem:

- Policing agencies, prosecutors, defense counsel and courts are key participants in evidence exchange.
- 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 of existing digital evidence products, the bureaucracy of the legal ecosystem and increasing acceptance of the technology:

- **Diverse marketplace —** The market for digital evidence management products has many providers, each with a unique approach. 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 authentication mechanism is in place.

- **Acceptance —** Courts in China, the U.K., and various U.S. states are recognizing blockchain-based authentication of evidence, minimizing the need for affidavits or other attestations of authenticity. The European Union's (EU) Lawful Evidence Collecting and Continuity Platform Development (LOCARD) effort intends to create 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 implementation of a shared system is a leading constraint. For example, EU LOCARD prioritizes stakeholder engagement to drive the shared vision across jurisdictions.

- **Funding —** Joint funding, particularly where jurisdictions involved do not have a common tax base or funding process, is a constraint.

- **Low transaction speed —** Blockchain's peer-to-peer technology, has relatively low transaction speeds. This can be a challenge where the volume of digital evidence artifacts is high.

- **Current technology works** — Digital evidence technology used today employs accepted techniques for data integrity.

- **Negative perceptions** — Blockchain is commonly associated with cryptocurrency. Cryptocurrency's speculative financial nature and use in criminal activities creates a negative impression among conservative law enforcement and judicial stakeholders.

User Recommendations

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.

- 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.
- Overcome inflated or negative perceptions of blockchain technology by focusing on interoperability and ease of transactions of a shared system, emphasizing blockchain as just a piece of the solution.
- Influence product change by querying current digital evidence management providers about their blockchain plans.

Emotion AI in Public Safety and Law Enforcement

Analysis By: Bill Finnerty

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

Emotion artificial intelligence (AI) technologies use AI to analyze the emotional state of a user via computer vision, audio/voice input, sensors and/or software logic. In public safety and law enforcement, emotion AI can be leveraged to analyze individuals' risk factors, including stress, anger and anxiety. The systems can then initiate preventative steps for those in custody and those delivering service to reduce risks and improve individual safety and wellness.

Why This Is Important

Proactive engagement by public safety and law enforcement with those in care, custody or on duty can be the difference between difficult situations having good or bad outcomes. The cost of these situations going badly is too high not to leverage technology to make improvements. Video, audio and wearable IoT are being increasingly used by public safety and law enforcement, providing a plethora of data to be analyzed and used by emotion AI to proactively engage with people to improve outcomes.

Business Impact

In many parts of the world, the use of emotion AI by law enforcement and public safety is nascent; however, there are examples of governments that have/are experimenting with emotion AI, such as the U.K., UAE and China. The potential for use, if the technology matures and is accepted, in public safety and law enforcement is quite high, as data from the system could be used as part of early intervention systems and interview systems that assist in detecting risks of suicide, violence and stress.

Drivers

Drivers for the use of emotion AI by public safety and law enforcement include:

- The impacts of not addressing the safety and wellness of officers and staff are expensive in the form of disruption to personal lives, increased stress, career challenges, healthcare costs and replacement costs. Emotion AI offers the ability to reduce these costs and improve the lives of staff as part of early detection and intervention.
- Societal demands for proactive action to ensure fair and equitable treatment of those engaged with public safety and law enforcement.
- Increased availability of real-time data from the adoption of streaming video and audio, and wearables, in public safety and law enforcement.

- The opportunity to positively impact the lives of those on duty and those receiving care or in custody through proactive intervention, rather than a reactive approach.
- The increased availability and adoption of cloud and AI as a service that meets data security and privacy standards for health and law enforcement.

Obstacles

There are a number of obstacles to the adoption of this emerging use case for AI in public safety and law enforcement:

- The cost of investing in emotion AI for 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 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 public safety and law enforcement organizations must:

- Work with leadership and human resources to proactively engage 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 and IoT platforms.

- Establish an enterprise integration strategy to ensure that data from video, audio, IoT and other sources can easily be accessed by emotion AI solutions.
- Pilot emotion AI with fully interpretable models, using tree-based algorithms or similarly explicit techniques, that allow you to understand the results of the model. As vendors are able to demonstrate positive outcomes, start to share these examples with stakeholders to be transparent and thoughtful in preparing for adoption.

Packaged Business Capabilities

Analysis By: Yefim Natis

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Packaged business capabilities (PBCs) are encapsulated software components that represent a well-defined business capability, recognizable as such by a business user and packaged for programmatic access. The definition does not specify the size, functional scope or internal architecture of the implementation, but PBCs are only as useful as they are modular, discoverable, autonomous and ready for composition (integration).

Why This Is Important

As the pandemic disruption forced organizations to seek increased business adaptability, many turned to the model of the composable business. PBCs are a foundational element of the composable application architecture. They act as the building blocks for composition and recomposition of application experiences. When combined with the democratized application composition tools, PBCs empower fast, safe and efficient application and business innovation by the business-IT fusion development teams.

Business Impact

- Adoption of PBCs improves the ability of organizations to involve business professionals in design of application experiences and to make changes to applications by way of recomposition instead of new coding.
- Composable applications, using PBC architecture, equip organizations to innovate faster, safer and smarter, which in turn delivers business resilience, efficiency and adaptability.

Drivers

- Increasing pace of business change, demanding faster, safer and more efficient application innovation.
- Increasing participation of business professionals in software engineering, requiring more business-oriented expression in software modeling, replacing or augmenting the traditional programmatic orientation.
- Increasing democratization of platform technologies, bringing more business professionals to application design work.
- Increasing orientation of vendor applications (SaaS) to API-first and API-only (“headless”) design, leading organizations toward composition and integration instead of the basic customizations of vendor applications.
- Increasing sophistication of agile development practices and product-style application delivery demands more advanced modularity, autonomy, orchestration and discovery for application capabilities.

Obstacles

- Lack of clarity in understanding the fundamentals of composable application architecture, which leads to false starts or “composability-washing” initiatives that do not deliver the expected results.
- Lack of democratized composition tools, which leaves too much of the attempted composition initiatives with technology professionals, limiting the direct business professional participation. This in turn generates designs that are less reflective of the nuance of the required business change and compromise the delivery pace and quality of the outcomes.
- Lack of experience operating fusion teams, which reduces their effectiveness and compromises both technology and business aspects of the products.
- Cultural resistance to change, fear of the shifting business priorities and common familiarity bias — all form obstacles to rapid adoption of architecture of composability and the PBCs.

User Recommendations

- Prioritize expertise in API management, event brokering, integration, business-IT collaboration and democratized tooling to achieve preparedness for composable business applications experience.
- Reject any new monolithic solutions proposed by vendors or in-house developers, and plan to renovate or replace the old ones to enable their participation in composition.
- Accelerate product-style delivery of application capabilities, using agile and DevOps techniques over traditional methods.
- Prioritize democratized tools in support of development, integration (composition) and governance of composed application experiences.
- Give preference to vendor offerings that deliver API-first and API-only (headless) application services.
- Transform the IT organization to the role of a partner and strategic guide to business units, trusted to deliver efficient, safe and fast services to help advance organizations’ business objectives.

Gartner Recommended Reading

Innovation Insight for Composable Modularity of Packaged Business Capabilities

Strategic Architecture Roadmap for Composable Enterprise Applications (Presentation)

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

Kick-Start Your Composable Business Journey With 2 Key Strategies

How to Design Enterprise Applications That Are Composable by Default

Real-Time Incident Center as a Service

Analysis By: Michael Brown

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

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, sensor, video and communications systems, that outcome is becoming available in as-a-service form.

Why This Is Important

Information fusion and C2 are ubiquitous to public safety. Early examples include real-time crime centers. Full-spectrum incident management, enabled by information fusion and C2 technology, has emerged. 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 wherewithal for a command center now have opportunities with as-a-service offerings.

Business Impact

Public safety mission operators and their technology support organizations are primary stakeholders. Citizens are stakeholders regarding surveillance aspects such as video or license plate readers. 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:

- Next-generation real-time crime centers (RTCC) — 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 the initial use of 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.

- IP-enabled everything — The IP enablement of much of the communications, sensor and surveillance capabilities of public safety fosters integration. Bringing together information assets like databases, radio, video, 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 more simple. 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 will 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, 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

Fusus; Hexagon; Mutualink; Rave Mobile Safety; Verizon

Citizen Twin

Analysis By: Alfonso Velosa

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

A digital twin of a citizen is a digital representation of an individual. National, state and local governments use citizen twins to support citizen services such as health or safety management. The citizen twin core elements are the model, data, a unique one-to-one association, and ability to monitor it. It integrates data into the twin from siloed sources such as health records, credit scores, phone location logs, criminal records, customer 360 records and infrastructure such as cameras.

Why This Is Important

Governments are developing digital twins of citizens to monitor the environment citizens live in and address health, safety, travel and social media impacts on society. The spectrum of complexity of the models and tools can help governments make better decisions for monitoring and supporting patients, prisoners, passengers or the elderly. Some governments, such as China's, are building a scoring methodology. Aggregated citizen twins can help map broad patterns and drive resource allocation.

Business Impact

- Governments will use digital twins to better orchestrate citizen services and other digital services, and even manage crises, such as pandemic protection.
- Aggregate data can help citizens access and expedite government services
- Citizens or governments can drive citizen-twin-based crowdsourcing sentiment analysis to assess government services in near to real time.
- Integrate government services to other systems including the Chinese social credit systems and shopper tracking solutions.

Drivers

- 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.
- Citizen interest in systems that help drive their health and safety, such as vaccination passports or solutions to monitor elderly patients using IoT-enabled trackers.
- An increased desire for personalized services from government and other organizations.
- The need to implement proactive services, such as healthcare, mental health, fraud detection, and so forth, with a particular driver for government services for COVID-19 pandemic responses.
- Investment by a broad range of law enforcement, justice and corrections authorities, for example for smart camera monitoring systems that track to 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 governments agencies to build out citizen services both in aggregate as well as servicing individuals.
- The need for both real-time services customized to citizens, for example for emergency medical services, and longer term, more complex solutions that serve elderly patients or inmates.

Obstacles

- Strong concern for privacy and the merits of government access to citizen data is leading to grassroots citizen pushback or government regulations such as the EU Privacy Directive or California Consumer Privacy Act (CCPA) to limit access to citizen data.
- Cost and scope slither without clear benefits to citizens or government agencies, as government bureaucracies increase the types and quantity of data collection.
- Government curation of aggregated citizen data creating a security risk for government data and a potential privacy and safety risk for the individual citizen.
- 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 different government, financial, commercial and healthcare silos driving exorbitant costs for integration, analytics and visualization.
- Lack of skills in the government agencies to drive the use of the citizen twin.

User Recommendations

- Build robust privacy and digital ethics policies that clarify what data is collected, who has access to it, how it is protected, and what citizen remediation actions exist or comply with existing remediation processes.
- Establish clear benefits to citizens such as certifying all passengers on an airplane or train are healthy or vaccinated, simplifying medical triage to get a citizen to medical care, or aligning toll payments to a citizen's car for use of a toll road or during city congestion fees.
- Test IoT sensor and analytics capability to ensure accuracy and validity for the physical part of a citizen digital twin.
- Invest in integration skills to connect into a heterogeneous set of applications and data sources.
- Build data exchanges to protect data, while enhancing the granularity of citizen data support personalized and contextualized citizens services through the government ecosystem.

Sample Vendors

Alibaba Cloud; Apple; Google; Tencent; Vantiq

Gartner Recommended Reading

Getting Started With a Digital Twin of Government

Top 10 Plausible Directions Resulting from COVID-19

Top Trends in Government for 2021: Hyperconnected Public Services

Top Trends in Government for 2021: Data Sharing as a Program

Top Trends in Government for 2021: Multichannel Citizen Engagement

Multiexperience

Analysis By: Jason Wong

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Multiexperience describes interactions that take place across a variety of digital touchpoints (such as web, mobile apps, conversational apps, AR, VR, MR and wearables) using a combination of interaction modalities in support of a seamless and consistent digital user journey. Modalities include no-touch, voice, vision and gesture. Multiexperience is part of a long-term shift from the individual computers we use today to a multidevice, multisensory and multilocation ambient computing experience.

Why This Is Important

Multiexperience (MX) is the new "omnichannel" for a digital-first world. Through 2030, the digital user experience (UX) will undergo a significant shift in terms of how customers, partners, citizens and employees experience their environments. MX is about the shift both in UX perception and in interaction models, which leads to a multisensory, multidevice, multilocation and multitouchpoint digital journey.

Business Impact

To achieve digital business transformation, it is essential to understand and exploit multiexperience. Applying multiexperience design to digital experiences removes friction and effort for the users — both customers and employees. Adopting MX will allow organizations to be more agile — delivering positive business outcomes by serving customers and employees in ways that best suit their needs and expectations.

Drivers

- Organizations are shifting their delivery models from projects to products, but beyond products is the experience — the collection of feelings, emotions and memories. Web and mobile apps are already commonplace, but they are undergoing UX changes driven by new capabilities like progressive web apps, WebXR and artificial intelligence (AI) services. Conversational platforms allow people to interact more naturally and effortlessly with the digital world. Virtual reality (VR), augmented reality (AR) and mixed reality (MR) are changing the way people interact with and perceive the physical-digital world.

- As organizations continue to invest in customer experience (CX) and employee experience (EX), they will need to apply MX front-end architecture and technology strategies to be more agile at serving business needs and user expectations. When MX discipline is applied with great UX in support of CX and EX strategies, total experience (TX) transformation is achieved. TX requires MX to be executed with CX, EX and UX in harmony and synchronicity.

- The long-term manifestation of MX is a composable digital experience that is adaptive, seamless, collaborative, consistent, personalized and ambient. This will happen over the next five years — and has already been accelerated by the COVID-19 pandemic, which has increased reliance on digital touchpoints and no-touch modes of interaction. In this new decade, MX is needed to deliver transformative and memorable experiences for customers, employees and all users of your digital products and services.

Obstacles

- Privacy concerns may dampen the enthusiasm and impact of MX adoption. Users will need to consent to sharing their location, accepting notifications and being tracked across their devices.
- On the technical front, the fragmentation of many consumer devices and the inconsistency of interoperability standards are enormous barriers to seamless MX integration of front-end technologies.
- The skills needed for MX development, such as immersive interaction design, are still lacking in most enterprise software engineering teams.
- Don't expect automatic plug-and-play of off-the-shelf devices, applications and services for MX. Instead, proprietary ecosystems of MX solutions will exist in the near term.

User Recommendations

Application and software engineering leaders should:

- Identify three to five high-value, proof-of-concept projects in which MX design can lead to more effortless, compelling and transformative experiences.
- Use personas and journey mapping to address the requirements of diverse business use cases. Use external-facing and internal-facing scenarios to support a unified digital experience.
- Collaborate with UX design teams to create a design system that spans desired MX touchpoints and modes of interaction. This ensures that MX development teams can accurately and consistently apply visual, behavioral and written guidelines.
- Establish a multidisciplinary fusion team including (but not limited to) IT, product managers, UX designers and business stakeholders.
- Focus on understanding how unified digital experiences impact the business, and use evolving MX technologies to create targeted solutions for customers or internal constituencies.

Gartner Recommended Reading

How to Apply Design and Architecture to Multiexperience Application Development

Transcend Omnichannel Thinking and Embrace Multiexperience for Improved Customer Experience

Multiexperience Will Be the New Normal for Consuming Analytics Content in the Augmented Era

Synthetic Data

Analysis By: Anthony Mullen, Alexander Linden

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, i.e., not obtained from direct observations of the real world. Data can be generated using different methods such as statistically rigorous sampling from real data, semantic approaches, generative adversarial networks or by creating simulation scenarios where models and processes interact to create completely new datasets of events.

Why This Is Important

One of the major problems with AI development today is the burden in obtaining real-world data and labeling it so AI models can be trained effectively. This is remedied by synthetic data. Furthermore, synthetic data is critical in removing personally identifiable information (PII).

Business Impact

Adoption is increasing across various industries, along with use in natural language processing (NLP) applications. We predict 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 as it is cheaper and faster to obtain.
- Improves ML performance as more training data leads to better training outcomes.

Drivers

- In healthcare and finance, buyers' interest is growing as synthetic data can be used to preserve privacy in AI training data.
- To meet increasing demand for synthetic data for natural language automation training, especially 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 simulation techniques is accelerating synthetic data.
- While row/record, 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.

Obstacles

- Synthetic data still has significant flaws. It can have bias problems, miss natural anomalies, be complicated to develop or may not contribute any new information to existing, real-world data.
- Data quality is tied to the model that develops the data.
- Buyers are still confused over when and how to use the technology with other data pipeline tools. As the number of techniques in data and model pipeline increases, buyers struggle to determine what techniques to use to achieve their aims (e.g., synthetic data, federated learning, differential privacy) and how to use them together.
- 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/teacher for labels.

User Recommendations

- Identify areas in your organization where data is missing, incomplete or expensive to obtain, and thus, currently blocking AI initiatives. In regulated industries, such as pharma 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.
- Begin with a sampling approach and leverage data scientists to ensure statistical validity of the sample and distribution of the synthetic data.
- Leverage specialist vendors while the technology matures.
- Mature toward the simulation-driven approach, emphasizing creating agents and processes within a simulation framework to generate permutations of interactions that result in synthetic data.

Sample Vendors

AI.Reverie; Bitext; MOSTLY AI; Neuromation; Tonic; Twenty Billion Neurons (TwentyBN)

Gartner Recommended Reading

Top Trends in Data and Analytics for 2021: From Big to Small and Wide Data

2021 Strategic Roadmap for Enterprise AI: Natural Language Architecture

Cool Vendors in AI Core Technologies

At the Peak

Immersive Training in PS/LE

Analysis By: Irma Fabular

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

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, artificial intelligence (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 — 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

Use of immersive experience for public safety training requires balancing of benefits, costs and risks:

- Augments capabilities for large-scale training.
- Facilitates ease of cross-agency training scenario development and updates.

- Requires ongoing funding for resources with digital expertise and for refresh of quickly advancing technologies such as HMDs.
- Introduces potential risks associated with security, privacy and personnel safety.

Drivers

The top drivers to the growing interest in immersive experience solutions for public safety and law enforcement training are as follows:

- **Law enforcement reform advocacy** for ongoing and more effective training programs on the use of force and de-escalation techniques. A recent presentation to the Los Angeles Police Commission recommended the use of blending learning techniques (that is, on-site and online) to optimize training for law enforcement officers.
- **Growing complexity of potential, “what if” threat scenarios.** These would encompass natural and man-made threat scenarios that are hard to simulate such as terrorism, wildfires and riots.
- **Shortage in availability of field officers.** Operational staffing needs require efficient and effective ways of onboarding new field officers as well as providing ongoing training and certification.
- **Growing adoption and use.** Organizations such as the New York Police Department and Royal Canadian Mounted Police Department have adopted VR in their training programs.
- **Continued investments by technology and service providers.** The ecosystem of startups (for example, V-Armed and Street Smarts) as well as large global technology and service providers (for example, Microsoft HoloLens) 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) are also growing.

Obstacles

- As training tools in public safety and law enforcement, immersive experience solutions are in different paths of maturity, adoption and evolution. In general, AR is less costly and complex to implement than VR. The combination of AR and VR (that is, MR) is most nascent.

- Advancements in areas such as 5G and AI will require ongoing investments in equipment refresh cycles, compatibility with existing training and performance management systems, security risks, and others.
- Implications on policies and personnel adoption can be extensive as continuous training is accelerated. What are 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 still evolving.

User Recommendations

- Educate training and operations leaders in 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.

Field Streaming Video

Analysis By: Bill Finnerty

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Field streaming video in public safety and law enforcement is the process of streaming live body-worn, dash, drone, mobile phone and other video to field commanders and incident command centers. The goal of field streaming video is to improve situational awareness and enable augmentation of officers and commanders in identifying threats and risks through automated analysis of the video. Simultaneously organizations must maintain a chain of custody for the evidence to meet legal requirements.

Why This Is Important

Field streaming of video allows the real-time, not just postfacto, analysis of incident content to improve the situational awareness of commanders 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. And they can be analyzed using sentiment analysis to identify risks to the wellness and safety of officers and participants in an incident.

Business Impact

Public safety and law enforcement agencies can use field streaming of video to gain the tactical advantage in a situation. Law enforcement can use the video for threat analysis and real-time intervention for officer safety and accountability. Fire departments can use video to assess risk from structural damage. EMS can share the content with emergency room staff to augment care en route. Corrections can use the video to detect risks and threats from inmates, such as fighting and contraband.

Drivers

- **Advances in technology:** The use of video for postfacto analysis of incidents 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 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 grows. Constituents expect that video will be utilized to improve their safety, whether that be to enable faster and more effective responses to threats and risks, or ensure that those providing services are held accountable for their actions.

Obstacles

- Although improvements in battery life are making field streaming more viable, many current cameras, particularly body-worn cameras, are not equipped to last a full shift or to stream content via cellular networks. Additionally, they do not have the networking features to support streaming. This will require that these cameras are replaced to provide this new capability.
- 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 and storage, can be prohibitive to agencies with limited budgets or those facing challenges with defunding.
- Both public safety and law enforcement personnel and the public have concerns about privacy rights related to recording their actions.

User Recommendations

- Engage leadership in establishing policies for acceptable uses of field streaming video. This can be achieved by working with representatives of the workforce and the public to explore use cases for video as they relate to privacy, accountability and the safety of the staff and public involved in an incident. 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. These options have 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 needed capabilities in their roadmap, identify possible partners to provide these capabilities.

Gartner Recommended Reading

Axon; Sentinel Camera Systems; WatchGuard; Wireless CCTV; WOLFCOM

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 (create predictable outcomes and learn within a range of defined parameters or unpredictable outcomes but within a specific range of parameters). 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 certainly imply AI. Smart robots have had less adoption compared with industrial counterparts but received great hype in the marketplace, which is why smart robots are still climbing the Peak of Inflated Expectations. The pandemic increased interest in smart robots, as they can provide logistic support and automation, and support social distancing, while enterprises can demonstrate ROI, without significant capital expenditure.

Business Impact

Smart robots will make their initial business impact across a wide spectrum of asset-centric, product-centric and service-centric industries. Their ability to reduce physical risk to humans from doing specific tasks, 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 and social venues, 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.

- Specialization also is very important to success, as no smart robot can address all industry-specific use cases.

- The COVID-19 pandemic has accelerated smart robot adoption, and typical use cases include:

- Logistics and warehousing — Medical/healthcare: Patient care, medical materials handling, interdepartment deliveries and sanitization; Goods delivery due to social distancing and quarantine with COVID-19; Manufacturing: Product assembly, stock replenishment, support of remote operations and quality control (QC) check; Last-mile delivery; Inspection of industrial objects or equipment; Surgical robots; Agriculture: Harvesting and processing crops; Reception/concierge in hospitality, retail, hospitals, airports and so forth.

Obstacles

- Despite some advancements in AI, product and material experimentation in 2020, the progress beyond proofs of concept (POCs) is relatively slow. Companies are still trying to identify valuable business use cases and assess ROI for robots. Therefore, the position of "smart robots" still remains on the Innovation Trigger curve.
- 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 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 into which smart robots can be deployed now and in three to five years for large-scale deployment.
- 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

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

Gartner Recommended Reading

Emerging Technologies Venture Capital Growth Insights: Robots

Emerging Technologies: Smart Robots Will Augment Human Workers, Not Replace Them

Market Trends: 4 Technologies That Will Revolutionize Drones and Robots

LEO Satellite Systems

Analysis By: Bill Ray

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Low Earth orbit (LEO) extends to around 1,300 km, significantly closer than geostationary orbit, which is more than 35,000 km from Earth. Connecting to satellites in LEO uses significantly less power, supporting low latency and faster data. However, coverage may require a large number of satellites, most of which will have a limited life span (around five years). Several companies are in the process of launching LEO services for broadband internet access and low-speed IoT connectivity.

Why This Is Important

Companies like Amazon and SpaceX have invested heavily in satellite services intended to provide internet access to consumers and enterprises. Innovations from the smartphone industry have reduced the price of satellites significantly, and the cost of launch is also declining, making these constellations economically viable. As of 2Q21, Starlink was already providing internet access to tens of thousands of users, with plans to rapidly scale up the service and exploit its first-mover advantage.

Business Impact

LEO services will make broadband internet, and IoT data gathering, globally available. Companies and employees can assume that internet access will always be available, removing network access as a limit on locations to work or live. Remote offices will always be able to get a reliable connection, and home workers will be able to live where they like. In time, this connectivity will extend to include aeroplanes, 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.

- Despite the widescale deployment of terrestrial wired and wireless services, there are still millions of homes and businesses that lack sufficient internet access, even in developed markets. Satellite broadband is relatively expensive (SpaceX's Starlink is charging $99 per month plus $499 installation) and won't compete with already-installed fibre to the cabinet or home. However, Gartner has calculated that there are enough homes without connectivity in the U.S., Europe and Australasia to sustain the Starlink service.

- Other customers will include airlines, ships and the military. 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.

- Starlink is the first mover, with more than 1,000 satellites deployed by 2Q21. However, in time, it will need to compete with offerings from Amazon as well as regionally-backed projects including OneWeb (U.K.), Telesat (Canada), Sfera (Russia) and Hongyan (China).

- IoT connectivity is a different market, focusing on low cost and low power to provide global asset monitoring and tracking. Companies like Myriota already offer a sensor with a five-year battery life and satellite connectivity, while Lacuna Space uses chips and radios conforming to the existing Lora standard, reducing the cost of a satellite-connected IoT sensor to a few dollars. Asset tracking is certainly the killer application, but condition and environmental monitoring will also be an important use case.

Obstacles

- To provide oceanic and remote region coverage (needed by military customers), links from satellite to satellite are required. Only the Iridium narrowband constellation currently has such links, although other companies are testing and designing them.
- Customer equipment currently costs more than $2,000. Developments in antenna design and mass production should reduce that cost, which needs to get below $500 for widespread adoption.
- Maintaining 30,000 satellites, with a life of five years, requires 500 new satellites per month. Current launch vehicles, such as the SpaceX Falcon 9, can launch 60 satellites at a time. This will not be sufficient, so larger launch vehicles (such as the SpaceX 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 future and strategic planning.
- Check the location of teleports to predict early-service availability; early services will only be available within 500 km of a teleport (earth station).
- Prepare for international availability by liaising with local regulators and resellers. LEO services are inherently global, so 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.

Sample Vendors

OneWeb; Starlink; Telesat Canada

Gartner Recommended Reading

Market Trends: LEO Satellites Will Provide Practical Connectivity to Remote and Mobile Offices

Emerging Technologies: LEO Mega Constellations — Market Disruption Ahead

Wearable Monitors for Public Safety

Analysis By: Bill Finnerty

Benefit Rating: High

Market Penetration: 5% to 20% 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 thermometers used to improve situational awareness and monitor the safety of fire, rescue, law enforcement and corrections personnel, as well as 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 or otherwise in danger.

Why This Is Important

The health and safety of the individuals in custody or care of, or working for, 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.
- 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.
- Increased innovation related to IoT sensors in the postpandemic world, enabled by acceleration of technology and a higher level of understanding and acceptance of the use of technology, supports health and wellness.
- The expansion of 5G and other wireless technology makes connectivity possible in more areas at better price points.
- The advantages of preventative care and support for those on duty, in care or in custody, versus that of physical or mental health support care after an incident, are enabled through the collection and analysis of data from wearable technologies.
- Data from wearables can contribute to early interventions systems to ensure wellness and accountability for sworn and unsworn staff.
- There is a need to improve the safety of all involved in or with public safety and law enforcement organizations.

Obstacles

- Concerns over privacy and over surveillance/monitoring of individuals may cause staff or individuals in care or custody to reject the use of wearable technologies.
- Particularly facilities where wireless technology has not been deployed at scale previously, the cost of deploying wireless technologies into a facility may limit connectivity and the viability of wearable sensors.
- Challenges related to connectivity or damage of 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 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.

Edge AI

Analysis By: Alan Priestley

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Edge AI refers to the use of AI techniques embedded in IoT endpoints, gateways and edge servers, in applications ranging from autonomous vehicles to streaming analytics. While predominantly focused on AI inference, more sophisticated systems may include a local training capability to provide in-situ optimization of the AI models.

Why This Is Important

An increasing number of edge computing use cases are latency sensitive (autonomous navigation), data intensive (video analytics), 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 video analytics which, driven by the rapid growth in use of surveillance cameras and the need for real-time interpretation of captured video, is starting to see adoption.

Business Impact

The business benefits of deploying edge AI include:

- Improved operational efficiency, such as manufacturing visual inspection systems.
- Enhanced customer experience.
- Reduced latency in decision making, with the use of local analytics.
- Communication cost reduction, with less data traffic between the edge and the cloud.
- Increased availability even when the edge is disconnected from the network.
- Reduced storage demand through a more reactive exploitation of the data.
- Preserved data privacy at the endpoint.

Drivers

- Increasing demand for the deployment of DNN-based data analytics close to or at the point of data capture, either in edge computers or endpoint devices.
- Edge AI implementations are impacted by application and design constraints of the equipment being deployed; this includes form factor, power budget (i.e., battery powered versus mains powered), data volume, decision latency, location, and security requirements.
- AI systems can be hosted within an edge computer, gateway or aggregation point and data captured at an IoT endpoint may need to be transferred. In this architecture, the IoT endpoint is a peripheral to the AI system. The endpoint acts as a data gatherer that feeds this data to the AI system. An example of this is environmental sensors deployed for a smart agriculture application.
- AI embedded in the IoT endpoint. In this architecture, the IoT endpoint is capable of running AI models to interpret data captured by the endpoint and drives some of the endpoints' functions. In this case, the AI model (e.g., a machine learning model) is trained and updated on a central system and deployed to the IoT endpoint. An example is a medical wearable that leverages sensor data and AI to help visually impaired people navigate the world in their daily lives.
- R&D into training AI models at the edge for decentralized machine learning.

Obstacles

- Systems deploying AI techniques can be nondeterministic. This can limit the ability to control and replicate analysis results, and may impact applicability in certain use cases, especially where safety and security requirements are important.
- The autonomy implicit in an AI deployment can lead to questions of trust, especially where the operation of the AI models is not transparent.
- The deployment of edge AI solutions can raise governance and privacy concerns. While analyzing data at or close to its point of capture can alleviate some privacy concerns, it may not mitigate them completely.
- Training DNNs 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 new AI developments are applicable to their IoT deployments, or whether traditional centralized data analytics and AI methodologies are adequate.
- Evaluate when to consider AI at the edge versus a centralized solution. Applications that have high communications costs are sensitive to latency or ingest high volumes of data at the edge are good candidates for AI.
- Assess the different technologies available to support edge AI and the viability of the vendors offering them. Many potential vendors are startups, which may have interesting products but limited support capabilities.
- Use edge gateways and servers as the aggregation and filtering point to perform most of the edge analytics functions. Make an exception for compute-intensive endpoints, where AI-based analytics can be performed on the devices themselves.

Sample Vendors

Baidu; Google; Intel; Microsoft; NVIDIA; Qualcomm

Gartner Recommended Reading

Emerging Technologies: Neuromorphic Computing Impacts Artificial Intelligence Solutions

Emerging Technologies: Critical Insights on AI Semiconductors for Endpoint and Edge Computing

Forecast: AI Semiconductors, Worldwide, 2019-2025, 1Q21 Update

Emerging Technologies and Trends Impact Radar: Artificial Intelligence

Edge Computing

Analysis By: Bob Gill, Philip Dawson

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

Edge computing describes a distributed computing topology in which data storage and processing are placed in an optimal location relative to the location of data creation and use. Edge computing locates data and workloads to optimize for latency, bandwidth, autonomy and regulatory/security considerations. Edge-computing locations extend along a continuum between the absolute edge, where physical sensors and digital systems converge, to the “core,” usually the cloud or a centralized data center.

Why This Is Important

Edge computing has quickly become the decentralized complement to the largely centralized implementation of hyperscale public cloud. Edge computing solves many pressing issues, such as unacceptable latency and bandwidth requirements, given the massive increase in edge-located data. The edge-computing topology enables the specifics of the Internet of Things (IoT), digital business and distributed IT solutions, as a foundational element of next-generation applications.

Business Impact

Edge computing improves efficiency and cost control through processing close to the edge (e.g., better automation and quality control), and more business opportunities and growth (e.g., customer experience and new real-time business interactions). Early implementations have succeeded in enterprises that rely on operational systems and data outside core IT, such as the retail and industrial sectors.

Drivers

Drivers to the adoption and implementation of edge computing include:

- Growth in cloud adoption has exposed the disadvantages of extreme centralization. Latency, bandwidth requirements, the need for autonomy, and data sovereignty or location requirements may be optimized by placing workloads closer to the edge and data produced at the edge, rather than centralizing in a hyperscale data center.
- Data growth from interactive applications and systems may not be economically funneled into the cloud.
- Applications featuring customer engagement and analysis favor local processing for speed and autonomy.
- IoT use cases are expanding from the industrial sector to other verticals, driving a move toward a hierarchical and distributed model.

Obstacles

- Extreme diversity of devices and application types amplify complexity issues
- Widespread application of the topology and explicit application and networking architectures are not yet common outside vertical applications, such as retail and manufacturing
- Lack of understanding of benefits/use cases
- Lack of standards
- Although the physical infrastructure for edge is maturing rapidly, the overall management and orchestration challenges of distributed applications are beyond vendor-supplied, component management offerings. The tasks of managing, securing, maintaining and updating the physical infrastructure, software and data requires considerable development before management and orchestration can be considered mature.

User Recommendations

- Create and follow an enterprise edge strategy by focusing first on business benefit and holistic systems, not solely pointing to technical solutions or products.
- Establish a modular, extensible edge approach through the use of emerging edge frameworks and architectures, which allow for the mixing and matching of technologies based on enterprise direction, not simply "what comes with the vendor solution."
- Accelerate time-to-benefit and derisk technical decisions through the use of vertically aligned system integrators (SIs) and independent software vendors (ISVs) that demonstrate an understanding of and ability to implement and manage the full orchestration stack from top to bottom.
- Evaluate the deployment of "edge as a service" options, which promise to deliver "business-outcome-based solutions" that adhere to specific SLAs, while shifting deployment, complexity and obsolescence risk to the provider.

Gartner Recommended Reading

2021 Strategic Roadmap for Edge Computing

Cool Vendors in Edge Computing, 2021

LTE/5G Enhanced Services

Analysis By: Irma Fabular

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Enhanced public safety communications and services can be achieved through the use of commercially available Long Term Evolution (LTE)/4G and 5G cellular infrastructure. This replaces or augments private land mobile radio (LMR) communications and adheres to public safety standards such as mission-critical push-to-talk 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

- **Policies and processes** will evolve, requiring strong organization change management. Communications infrastructures need to be “battle-tested.”
- **Improves cross-jurisdictional communications and interoperability.** Public safety organizations can augment LMR infrastructure with LTE/5G capabilities.
- **Ongoing innovation in communications.** Avoids large capital investments for ongoing innovation.

Drivers

- Public and personnel safety are improved through enhanced capabilities to collaborate on emergency response within a single agency (such as a police agency) or multiple agencies and jurisdictions.
- Standards for mission-critical push-to-talk (MCPTT) requirements have been established, which drive continued investments by technology and service providers. For example, FirstNet PTT and Group First Response enable interoperability between LTE and LMR infrastructures.
- The increasing ecosystem of technology providers is introducing innovation that requires high-bandwidth, secured communications. These include advancements in artificial intelligence (for example, computer vision), data and analytics, Internet of Things (IoT) (for example, sensors and drones) and edge computing.
- The increasing complexity of threat landscapes requires greater communications and collaboration to prevent, respond and recover from emergencies.
- There are government-sponsored programs and investments in a Nationwide Public Safety Broadband Network (NPSBN) such as in the United States, Canada and Australia.
- There is continued support and funding for 5G pilots. For example, use of drones in New Zealand and the Marine Corps Air Station in San Diego pilots are underway.

Obstacles

Full adoption of LTE/5G by public safety organizations can take five to 10 years. 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 reliability of commercial, cellular offerings
- Consensus on the ROI and business justifications to transition from large capital investments in private, LMR infrastructure, systems and equipment
- Public safety government grants that often fund capital improvements and one-time investments only
- Careful scrutiny of suppliers' supply chain to secure telecommunications equipment and devices

User Recommendations

CIOs and other technology leaders supporting public safety and law enforcement must:

- Be proactive in addressing enhanced communications and services by incorporating LTE/5G communications technologies in strategic plans. Some strategic planning considerations include the fact that use of mobile devices will continue to increase, which requires greater security, and insights from all forms of data — text, video and voice — will be 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 personnel are involved in response and recovery efforts, who can benefit from seamless communications channels.

Sample Vendors

AT&T; Lumen; Motorola; MutuaLink; Rogers; Samsung; Verizon; Vodafone

Gartner Recommended Reading

How to Plan the Role of 5G in Your Smart City Initiatives

Market Guide for 4G and 5G Private Mobile Networks

Rapid DNA in Policing

Analysis By: Michael Brown

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Adolescent

Definition:

Rapid DNA is an identification technology that returns a small set of genetic marker results in 90 minutes sufficient 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 setting of police booking processes is an evolutionary use.

Why This Is Important

Law enforcement use of DNA identification has typically been in the form of evidence analysis for investigative work, in which laboratories return results over days and weeks. With its speed and accuracy, rapid DNA technology is poised to join electronic fingerprinting as a standard biometric identifier collected during the arrestee booking process. The benefits for 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 in the following ways:

- Enhanced ability to clear unsolved crimes and prevent inadvertent release of those who should remain in custody

- Requiring supporting legislation in addition to modification of booking procedures, ecosystem partnerships and compliance activities

- Significant changes to existing booking technology

Drivers

Rapid DNA is being advanced by several factors:

- **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 its Rapid DNA Program Office, the FBI has been working to introduce this technology to law enforcement. As the technology advanced, it became evident that 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. Shortly after the passage of the statute, the FBI published the Requirements for Rapid DNA in the Booking Environment, a succinct early delivery on the mandate.

- **Successful testing** — 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 of that testing have informed the publication of detailed standards and operational procedures.

- **Equipment certification** — One of the two rapid DNA instrument vendors has achieved FBI certification for booking station use. The second instrument vendor has been certified for use in forensic laboratories and is pursuing the additional booking station certification.

Obstacles

Obstacles are typical of any new law enforcement process:

- **Legal authority** — Supporting legislation must be enacted to allow 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 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 positioned to become an everyday identification tool for law enforcement. 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 assignment of staff.

- Plan for technology integration by training internal staff and possibly using outside integration contractors.

- Assist in developing the necessary budget for the introduction and support of rapid DNA by coordinating with mission operational staff.

Sample Vendors

ANDE; Thermo Fisher Scientific

Gartner Recommended Reading

Rapid DNA Analysis in U.S. Public Safety

Enterprise Wearable Device Management

Analysis By: Chris Silva

Benefit Rating: Low

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Enterprise wearable device management is the set of management functions to centrally monitor, update and configure wearable devices, such as head-mounted displays (HMDs), VR headsets, smartwatches and other body-worn sensors. These tools are commonly used by end-user computing (EUC) teams, and exist as a subset of management capabilities in unified endpoint management (UEM) tools.

Why This Is Important

Wearable devices have gained a permanent place in the role of many field, logistics, medical and other vertical-industry-specific and highly specialized applications. The push to remote and hybrid work in 2020 opened new use cases for wearable devices, though IT leaders' demand for wearable-specific management remains modest, in line with the adoption of wearable devices as workers' primary device.

Business Impact

The benefits of wearable-specific management capabilities mirror those of other endpoints that UEM tools manage; the ability to deliver consistent configuration and support, at scale. These devices can be configured manually with significant overhead needed to do so. The analytics and telemetry data that can be gathered from devices when managed in a capable, cross-platform tool can support better investment and planning decisions on hardware and identifying use cases.

Drivers

- Supporting remote learning for highly specialized curricula; in one example, HMDs were shipped to medical students learning remotely to maintain continuity of learning when physical presence in the school's anatomy and dissection lab is not possible.

- The need to measure and track physical vital signs as part of COVID-19 protocols for return to work and in hybrid workplaces is driving demand for wearables.

- Support for managing wearable devices using the Android operating system has been common in UEM tooling for some time. The support has traditionally been limited to devices with a business-only or primarily business or industrial use cases. Gartner has witnessed vendors adding support for primarily consumer-focused devices like the Oculus family of devices from Facebook, in recognition of the broad availability of, and interest in, these devices in enterprise contexts.

Obstacles

- Forty percent of IT leaders highlighted to Gartner that cost savings is a No. 1 or No. 2 priority coming out of 2020. Gartner has observed wearable pilots and programs being curtailed or limited, respectively. Gartner believes that this drop in overall interest will be time-limited and does not represent a shift in the importance of wearables in the long-term end-user computing strategies of organizations.

- Many of the devices being eyed for these purposes, such as fitness bands and smartwatches, may not benefit from, or be directly addressable by, enterprise wearables management.

User Recommendations

To minimize unnecessary investment, IT leaders must:

- Source wearable device management from existing endpoint management vendors, and avoid proprietary tools when possible; the fortunes of dedicated enterprise wearable device manufacturers have been subjected to great volatility during the past two years.
- Implement the viability of managing and supporting wearables as a key element of decisions concerning sourcing wearable hardware.

Sample Vendors

42Gears; Augmate; BlackBerry; Microsoft; Samsung; VMware; Vuzix

Gartner Recommended Reading

Forecast Analysis: Wearable Electronic Devices, Worldwide

Market Definition and Methodology: Wearable Electronic Devices

Emerging Technologies: Head-Mounted Displays for Augmented, Mixed and Virtual Reality

Peer Connect Perspectives: Implementing Wearables Within an Organization

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 access at distributed edge computing locations.

Why This Is Important

Like any IT system, edge computing locations will be targets for attack, including data theft, data poisoning, denial of service and placement of malware (for example, Bitcoin mining). Edge computing security combines the requirements of data center computing security with the scale, location and variety of heterogeneous mobile and 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 some workloads to the edge and security needs to be a part of this.

- Sensitive data and intellectual property will be stored at the edge and transmitted from the edge and needs to be protected.

- New solutions and approaches are needed that securely support intermittent access and protect from physical tampering and theft.

Obstacles

- The 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 confusing offerings.
- Most edge hardware devices were not designed with adequate security controls.
- Most edge hardware devices were procured outside the visibility and control of information security and 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.

User Recommendations

- Design protection that treats the network as compromised, hostile and intermittent.
- Make tamper-resistance a part of security control evaluation, assuming that hardware will be attacked, tampered with or stolen.
- Map your protection requirements for edge — including data encryption, network security, workload integrity, application control, memory protection, behavioral monitoring and intrusion detection/prevention — to help with vendor selection.
- Favor offerings that are centrally managed, ideally cloud-based, and provide for tightly controlled administrative access.
- Require the use of identity-based policy management using provisioned unique identities of edge equipment, typically certificate-based.
- Restrict access to the edge platform using a zero trust network access or SASE offering.
- Require vendors to support Linux containers and container-based security offerings, which are expected to be widely used along with VMs for distributed edge computing architectures.

Sample Vendors

Amazon Web Services; Appgate; Dell Technologies; Fortinet; Hewlett Packard Enterprise (HPE); IBM Red Hat; StorMagic; Tempered; Venafi; VMware

Gartner Recommended Reading

2021 Strategic Roadmap for SASE Convergence

4 Steps to Successful Edge Computing Deployments

Computer Vision in Government

Analysis By: Dean Lacheca

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Computer vision (CV) is a process that involves capturing, processing and analyzing real-world images and videos to allow machines to extract meaningful, contextual information from the physical world. CV in government is the application of the technology, by all levels of government, to new and existing government image and video source data to expand the data's relevance, accelerate speed to insight and improve decision making.

Why This Is Important

Interest and use cases for CV in government continues to grow. Currently, public safety, law enforcement and local government lead adoption of CV; however, opportunities exist for use in all sectors of government. CV has the potential to unlock the value of underutilized data in government, as well as support the redesign of government service delivery. The privacy implications of CV may be politically significant, requiring close regulatory and ethical attention.

Business Impact

Computer vision will augment the capabilities of the government workforce and its partners. Beyond public safety, law enforcement and smart city use cases, opportunities also include:

- Automating and streamlining regulatory activities
- Accelerating speed to value of some labor-intensive tasks
- Redesigning service delivery and data capture

- Reducing data errors
- Improving citizen experience, and in some cases, the risk to the workforce and citizens

Drivers

- CV offers the potential to accelerate the manual analysis of existing government image and video source data by governments.
- 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 increased availability of video and image content has opened up new use cases across a range of government sectors, from environment to defense to emergency management and response. Examples include wildfire detection, agriculture inspections and land use mapping.
- Combining CV with new data capture technology 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.
- CV has enabled a number of COVID-19-triggered use cases to support social distancing compliance, PPE compliance, people counting and occupancy and fever screening.
- Pressure on governments to be more proactive and frictionless in service delivery requires innovative approaches to service delivery.

Obstacles

- Price, performance and reliability — high-end systems are expensive to maintain and support, and building business cases with adequate ROI remains challenging.
- Integration with existing systems is problematic due to a lack of open interfaces, off-the-shelf solutions and plug-and-play capabilities.
- Governments concerned about community trust and privacy concerns/regulations can limit the ability to apply CV solutions.
- Scaling solutions is often challenging due to the requirement for a high level of customization and service support.
- Adequate, unbiased training and testing data may be hard or expensive to acquire, especially in areas where available open-source CV datasets are declining.
- Government data source quality may not be high enough to deliver the expected benefits in a cost-effective way.
- Proprietary algorithms and patent pools deter innovation.
- The operationalization of the AI techniques (such as deep learning) that underlie CV is challenging.

User Recommendations

- Start to address quality data source issues by developing a quality source dataset from existing government-controlled feeds.
- Critically assess change management impacts of CV projects on the organization and its people.
- Focus initially on a few small projects, using fail-fast approaches, and scale the most promising systems into production using cross-disciplinary teams.
- Test production systems early in the real-world environment since lighting, color, object disposition and movement can break CV solutions that worked well in the development cycle.
- Build internal CV competencies and processes for exploiting image and video assets. This will enable the organization to make better procurement choices and lay the groundwork for more advanced innovation and product development opportunities.
- Exploit third-party CV tooling and services to accelerate data preparation and reduce costs.
- Evaluate legal, regulatory, commercial and reputational risks associated with CV projects at the outset.

Workstream Collaboration

Analysis By: Mike Gotta

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early 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 tools improve aspects of teamwork, especially intrateam messaging. They combine support for channel-based chat, information sharing, task coordination and meetings in order to act as team activity hubs. They help coordinate work, regardless of where team members are located — a key feature for hybrid working. Although still not popular among frontline workers, WSC tools will increasingly impact operational work and external collaboration.

Business Impact

WSC tools help team communication, information sharing, task coordination and management of the overall work process by acting as new work hubs. They also act as governance points for security and compliance, helping to safeguard organizational communications and content.

Business use cases include project management, service and support, sales, marketing and operational scenarios.

WSC tools also help maintain continuity as hybrid teams split their time between remote and on-premises working.

Drivers

- The shift to hybrid working models makes WSC tools essential to satisfy communication, information-sharing and task coordination needs, and creates synergies with collaborative work management tools. It also supports work governance, security and compliance, sometimes via third-party add-ons.
- COVID-19 has prompted a significant increase in the number of remote workers, who need a common work hub to support individual and team productivity in lieu of in-office interactions.
- Online meetings with audio and video support are a fundamental requirement for organizations, and this has resulted in tremendous reliance on WSC tools for everyday productivity.
- Many WSC tools natively support, or are easily integrated with, content services to provide workgroup management of files, which also aids remote working.
- Additional integration capabilities of WSC tools enable plug-ins for other needs, such as tasks, meetings and intranet services. They also enable developers to create more custom extensions.

Obstacles

- Although Microsoft and Google offer native WSC tools, not all business scenarios can be accommodated by everyday productivity suites. This can prompt organizations to adopt multiple WSC tools, which increases costs and complicates IT management.
- WSC vendors are not collaborating on message interoperability. Use of multiple tools to ensure workers can communicate creates “chat silos” and can lead to “tool sprawl.” Although third-party vendors use public APIs to exchange messages between tools, risks arise if these vendors lack contractual relationships with WSC tool vendors.
- Frontline workers have not adopted WSC tools to the same extent as office workers. WSC tool vendors need to better address the distinct needs of frontline workers and adjust their offerings.

User Recommendations

- Assume everyday productivity needs can be satisfied by the incumbent productivity suite vendor (Microsoft or Google) when evaluating WSC tools. Remain open to adding WSC tools for process-driven and operational-role-based work when assessing business use cases that are not productivity-centric. Consider frontline workers’ needs as being “stretch goals” for many WSC tool vendors.
- Prioritize a strong focus on employee communications, a champion program, analytics, training and promotion of best practices based on successful use of WSC tools by staff, in order to reinforce new ways of working.
- Onboard new team members using WSC solutions and establish the right usage behaviors early.
- Reduce “noise” and fatigue by educating staff about chat etiquette and communicating best practices for using WSC tool features by, for example, showing them how to fine-tune alerts and notifications.

Sample Vendors

Cisco; Coolfire; Google; Mattermost; Microsoft; Rocket.Chat; Salesforce (Slack)

Gartner Recommended Reading

Market Guide for Workstream Collaboration

Forecast Analysis: Workstream Collaboration, Worldwide

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

Sliding into the Trough

Drone Countermeasures

Analysis By: Nick Ingelbrecht

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Drone countermeasures are systems and devices designed to detect, neutralize or retaliate against drone incursions.

Why This Is Important

Drone countermeasures constitute a fast-growing market of technologies to address the problem of intrusive, illegal or dangerous drone threats. Drone countermeasures are important to all industries and public agencies with a public safety/security remit. Such countermeasures include electronic jamming, guns, nets and high-power lasers or microwaves to disable or destroy UAVs, as well as disruption systems and underwater countermeasures for submersible drones.

Business Impact

Drone countermeasures impact all industries and public agencies with a public safety/security remit. Drone countermeasures impact will be critical to protect sensitive locations, critical infrastructure, transportation hubs (especially airports) and major public gatherings.

Drivers

- The adoption of drone countermeasures has been accelerated by high-profile disruption of civil airports, prison incursions and the proliferation of low-cost-drone activity. Often ground-based security perimeters can easily be circumvented, and demand for drone countermeasure products will evolve in response to illicit surveillance activities related to criminal activity, stalking, as well as deterrents to the drone transportation of drugs and contraband.

- Law enforcement, military and security officials responsible for protecting major events and sensitive locations (including prisons, critical infrastructure, police, airfields and mobile military units) are paying increased attention to drone threat assessments and countermeasures in their security planning. There is also an expanding market for VIP protection, gated communities, yachts and ports.
- Drone threats extend to the illicit collection of sensitive information, the carriage of dangerous payloads, their use as listening devices and hacking platforms, and disrupt operations.
- Given the unrestricted sales of drones, mainstream adoption of countermeasures is accelerating fast, even though legal frameworks and countermeasure technologies are still evolving. Over time, drone countermeasures will evolve into a basic security requirement. By 2023, 90% of commercial airports will have drone detection technology installed, up from 5% in 2019. Further ahead, swarm attacks pose a significant emerging threat vector.

Obstacles

- Buyers have to sift through a fragmented competitive market landscape of the various countermeasure solutions on offer, against lack of comprehensive industry standards and competing vendor claims.
- High prices and poor performance of some products have slowed adoption of drone countermeasures.
- Countermeasures may also be ineffective against small, fast-moving drones in dense urban environments, where advanced detection is impaired by buildings.
- Varied regulations in different countries may prevent or restrict the use of drone countermeasures.

User Recommendations

- Include drone threats in your cyber and physical security risk assessment(s), and prioritize the need for countermeasures specific to the environment (e.g., military versus civilian; potential target value and attack vectors; geographic; and regulatory), including the potential for drones to be used as listening devices or man-in-the-middle attack vectors for malware injection.
- Specify multisensor, multilayered approaches (radar tracking and thermal, acoustic, optical analytics, and RF/microwave sensors).

- Validate vendor claims via proofs of concept, vendor shootouts or demonstrations in your locale against a wide variety of different drone threats.
- Evaluate the emerging threat of drone swarms that could overwhelm standard countermeasures and run scenarios of different types of attacks.
- Evaluate the legal and physical risk from injury or property damage resulting from drone countermeasures, due to uncontrolled descent or fragmentation of target drones. Signal-jamming solutions need to be fully automated to be effective, whether "kill" type jammers or "return home" systems.

Sample Vendors

Aaronia; Advanced Protection Systems; Airspace Systems; Arcarithm; Black Sage; Dedrone; DJI; DroneShield; Raytheon Technologies; SRC

Gartner Recommended Reading

Prepare for Drone Incursions With a Multilayered Countermeasures' Strategy

Emerging Technologies: Top Use Cases for Future-State Physical Security Infrastructure

Best Practices in Implementing Video Surveillance, Analytics and Response Systems in Physical Security

Hype Cycle for Drones and Mobile Robots, 2020

Top Trends in Public Safety and Law Enforcement for 2021

Machine Learning

Analysis By: Farhan Choudhary, Carlie Idoine, Shubhangi Vashisth

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Machine learning is an AI discipline that solves business problems by utilizing statistical models to extract knowledge and patterns from data. There are three major approaches that relate to the types of observation provided. These are supervised learning, where observations contain input/output pairs (also known as "labeled data"); unsupervised learning (where labels are omitted); and reinforcement learning (where evaluations are given of how good or bad a situation is).

Why This Is Important

According to Gartner's 2019 AI in Organizations survey, machine learning (ML) is the AI initiative for which more POCs and production systems are conducted. Over the past few years, ML has gained a lot of traction because it helps organizations to make better decisions at scale with the data they have. ML aims to eliminate traditional trial-and-error approaches based on static analysis of data, which is often inaccurate and unreliable, by generalizing knowledge from data.

Business Impact

Machine learning drives improvements and new solutions to business problems across a vast array of business, consumer and social scenarios like:

- Automation
- Price optimization
- Customer engagement
- Supply chain optimization
- Predictive maintenance
- Fraud detection

Machine learning impacts can be explicit or implicit. Explicit impacts result from machine learning initiatives. Implicit impacts result from products and solutions that you use without realizing they contain machine learning.

Drivers

- As organizations continue to adopt these technologies, we recently see focus on aspects that relate to ML explainability and operationalization. Augmentation and automation (of parts) of the ML development process improve productivity of data scientists and enable citizen data scientists in making ML pervasive across the enterprise.

- In addition, pretrained ML models are increasingly available through cloud service APIs, often focused on specific domains or industries.

- Data science and machine learning education is becoming a standard at many academic institutions, therefore fueling the supply of newer talent eager to venture into this space.

- There's always active research in the area of machine learning in different industries — manufacturing, healthcare, corporate legal, defense and intelligence. Thus, its applicability is far and wide.

- Newer learning techniques such as zero, one, few or end shot learning are emerging that take away the burden of having high volumes of quality training data for ML initiatives. This lowers the barrier to entry and experimentation for organizations.

- New frontiers are being explored in synthetic data, new algorithms (e.g., deep learning variations) and new types of learning. These include federated/collaborative, generative adversarial, transfer, adaptive and self-supervised learning, all aiming to broaden ML adoption.

Obstacles

- The triggers of its massive growth and adoption have been growing volumes of data, advancements in compute infrastructure and the complexities that conventional engineering approaches are unable to handle.

- Even though ML is one of the particularly popular AI initiatives in the last few years, it is not the only one. Organizations also tend to rely on other AI techniques such as rule-based engines, optimization techniques, physical models to achieve decision augmentation or automation.

- A significant portion of ML models at an organization doesn't make it into production, therefore adding to technical debt and risks mistrust in the initiative, often delaying value realization from ML at organizations.

- The application of ML is often oversimplified as just model development but it's not so. Several dependencies which are overlooked, such as data quality, security, legal compliance, ethical and fair use of data, serving infrastructure, and so forth, have to be considered in ML initiatives.

User Recommendations

- Build up and extend descriptive analysis toward predictive and prescriptive insights, which can be excellent candidates for machine learning.

- Assemble a (virtual) team that prioritizes machine learning use cases, and establish a governance process to progress the most valuable use cases through to production.

- Utilize packaged applications if you find one that suits your use case requirements. These often can provide superb cost-time-risk trade-offs and significantly lower the skills barrier.

- Explicitly manage MLOps and ModelOps for deploying, integrating and monitoring analytical, ML and AI models.

- Adjust your data management and information governance strategies to enable your ML team. Data is your unique competitive differentiator, and adequate data quality, such as the representativeness of historical data for current market conditions, is critical for the success of ML.

Sample Vendors

Amazon Web Services (AWS); Databricks; Dataiku; DataRobot; Domino; Google Cloud Vertex AI; H2O.ai; Microsoft Azure; SAS; TIBCO Software

Gartner Recommended Reading

Magic Quadrant for Data Science and Machine Learning Platforms

Critical Capabilities for Data Science and Machine Learning Platforms

Toolkit: RFP for Data Science and Machine Learning Platforms

3 Types of Machine Learning for the Enterprise

Understanding MLOps to Operationalize Machine Learning Projects

Virtual Assistants

Analysis By: Van Baker

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Virtual assistants (VAs) help users with tasks previously handled by humans. VAs use semantic and deep learning models, natural language processing, prediction models, recommendations and personalization to interact with people via voice or text conversations. Increasingly, they also automate processes and workflows. VAs learn from user behaviors, build data models, and recommend and complete actions to support VA users. VAs can be deployed in simple as well as complex use cases.

Why This Is Important

Conversational interactions are inherently appealing to both customers and members of the workforce. The ability to converse with applications to retrieve information or accomplish transactions is a natural extension of human-to-human interactions to human-to-machine interactions. A well implemented virtual assistant is always available, cannot be distracted, and can be very efficient in assisting humans in accomplishing tasks and retrieving necessary information.

Business Impact

VAs, RPA, event brokers and other technologies are automating the enterprise. VAs use contextual multiturn conversations to drive business workflows. Integration with enterprise applications enhances the handling of complex tasks by VAs. Consumer VAs led to enterprise VAs embedded in SaaS platforms. Business channels such as websites, mobile apps and messaging are commonplace. Voice-based VAs are becoming the focus of conversational AI providers. Additionally, use of VAs can expand hours of operation and improve customer response time.

Drivers

- Customer expectation for access to customer service anytime, anywhere. This is especially true for online e-commerce businesses that have seen extreme growth in response to the pandemic.

- Consumer expectation for access to product information anytime, anywhere. E-commerce is a 24/7 business and consumers expect to get their answers whenever they engage.

- Employee access to information on a real-time basis via conversational queries, resulting in enhanced productivity because of increased use of business-critical information.

- Increasing demand for technology that is easy to understand and interact with. While this is true for all workers, it is especially needed by remote workers in the enterprise.

- A strong desire by businesses to automate business workflows and processes wherever automation can deliver value to the business.

- The ability to initiate communication with your workforce in response to event triggered conditions or transactions. This facilitates more timely response to changing business conditions by removing the need for workers to initiate transactions.

- The ability of conversational AI platforms to deliver more complex transaction capabilities spanning multiple users and business processes.

- Improved access to the business across multiple channels addressing the preferences of particular customer segments, allowing them to select their channel and modality of choice.

- Improving capability for conversational AI platforms to use natural language generation. This allows the virtual assistants to initiate interaction with customers and employees rather than just reacting to user requests.

- VA tools are becoming available that enable the automatic ingestion of unstructured and structured data to enhance and improve the language models.

- Enabling technologies are making creation of VAs easier such as low-code tools, automated identification of intents and entities, and the use of APIs for complex integrations.

Obstacles

- Poor or inadequate language models for the use case that is deployed. The virtual assistants need to be able to respond to an extraordinary variety of users' questions. They should also be able to handle off-topic questions to some degree.
- Inadequate conversational AI platforms that do not have the capabilities needed to deliver virtual assistants. Many platforms lack the ability to handle complex transactions, context switching, multi-intent utterances, strong integration, process automation and other functionality needed for virtual assistance level capabilities.
- A design approach that oversimplifies use cases for virtual assistants. Many dialogue designs assume consistency in the way that people ask questions or do transactions that do not exist. This often leads to successful pilot development efforts that fail upon deployment.
- The need for ongoing continual retraining of the language models is often overlooked or ignored leading to poor performance over time.

User Recommendations

- Assess the continual rapid evolution of the technologies that support the creation and deployment of virtual assistants. These technologies are evolving at a very rapid pace that is not expected to slow in the near term.
- Deliver significant levels of integration and business process automation in conjunction with virtual assistant conversational capability as the platforms in the market are becoming increasingly sophisticated. Many conversation AI platforms include workflow automation capabilities as part of their offering.
- Evaluate that VAs will have voice and text capabilities with voice becoming the dominant modality.
- Define a chatbot strategy at the enterprise level and decouple the technical decisions from it.
- Pick your core services by favoring modular technical solutions that allow the same.

Gartner Recommended Reading

When Should I Use Embedded Conversational Assistants?

Making Sense of the Chatbot and Conversational AI Platform Market

Craft a Chatbot Initiative Based on Your Business Requirements and Solution Complexity

Roles and Responsibilities for Scaling Chatbot Initiatives

Solution Criteria for Enterprise Conversational AI Platforms

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 agencies. Current use cases are leveraging data related to incidents, weather and resources in corrections, traffic management, policing, fire prevention and emergency medical services to make strategic planning and tactical operation decisions. However, the use of historical data must be limited to avoid bias.

Why This Is Important

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

Business Impact

Public safety and law enforcement agencies that use predictive analytics can change service delivery models to proactively achieve mission outcomes. Through the use of predictive analytics:

- Corrections institutions can reduce the risk of violence in facilities 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 and reduce implementation and operational costs.
- Solutions providers are supplementing their solutions with emerging technologies from ecosystems partners to gain competitive advantage.
- Untapped data is available to public safety and law enforcement for analysis.
- Society is pushing public safety and law enforcement to demonstrate equity in service delivery.
- There is demand for government organizations in general, and public safety and law enforcement agencies specifically, to reduce costs and operate more efficiently.
- A growing number of providers are developing predictive analytics, location intelligence and machine learning solutions that are being delivered in a SaaS model. Therefore, public safety and law enforcement agencies are not required to have data science, artificial intelligence (AI) modeler or other related skills in-house.

Obstacles

- The data quality and management capabilities of public safety and law enforcement agencies may limit their ability to leverage predictive analytics.
- Public concerns over data bias and misuse of data by public safety and law enforcement may cause leadership to be hesitant in experimenting with predictive analytics.
- The risk averse nature of public safety and law enforcement 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 public safety and law enforcement agencies, which can be particularly difficult for organizations in this segment of government.

User Recommendations

- Establish, 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 NIEM.
- Engage existing 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.
- Establish guidelines for adopting predictive analytics solutions that build trust by requiring models that are explainable to leadership, staff and constituents.
- 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 activity to remediate any findings.

Sample Vendors

IBM; KeyCrime; Microsoft; Palantir; SAS; Semantic AI

Gartner Recommended Reading

Top Trends in Data and Analytics for 2021: Smarter, More Responsible and Scalable AI

Digital Ethics by Design: A Framework for Better Digital Business

Market Insight: Public Safety Ecosystems Accelerate Digital Transformation

Live Face Recognition

Analysis By: Michael Brown

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Live or automatic face recognition technology uses computer vision to identify persons of interest from a live video stream, based on pre-existing photographs. Live face recognition is differentiated from other forms of face recognition by the ability to identify people without their cooperation in posing for a camera.

Why This Is Important

Live face recognition can automatically identify missing persons and persons of interest to law enforcement. Video from fixed and mobile cameras is providing ever-growing data streams that exceed human ability to effectively monitor and analyze. Policing organizations in a number of countries have implemented the technology to bolster traditional law enforcement capabilities. As algorithms improve and if privacy concerns can be ameliorated, adoption will grow more rapidly.

Business Impact

Law enforcement has aggressively implemented video surveillance as a more effective and lower-cost means to monitor for persons of interest and to protect the public. That use of video surveillance has outstripped any nonautomated means to analyze imagery. Live face recognition provides an opportunity to extract more information, more consistently, from the great volume of streaming video now available.

Drivers

Live face recognition is being advanced by several factors:

- **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. A host of countries, including the U.K., Argentina, Russia, China, South Korea, Serbia and India, have implemented live face recognition. Initially, the technology has been used for fixed cameras' video streams. However, police accountability measures have rapidly increased vehicle and body camera use, and limited forms of live face 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 use of the technology. The pandemic presented needs for rapid change in citizen behavior and government interest in monitoring compliance. Live face recognition has been used to enforce quarantine restrictions on public movement. Live face recognition cameras have been coupled with thermal imaging for body temperature to identify potential virus carriers.

- **Efficiency —** Policing agencies have a charter to ensure compliance with laws. That work 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. Compared with personnel costs to increase monitoring capabilities, live face recognition is more cost-effective. Law enforcement, as with other government functions, is subject to budget limits. Consequently, demand, data and technology are coming together to increase use of live face recognition.

- **Algorithm improvement —** Face recognition technology 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 shows steady improvement in the technology.

Obstacles

Live face recognition has two key challenges:

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

- **Accuracy concerns —** Higher rates of false positives for some groups appear as bias in face 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 allayed.

User Recommendations

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

- Assess permissibility and ethical appropriateness of live face recognition by working with internal counsel before planning any use of the technology.
- Help to allay citizen concerns by coordinating with public relations and community outreach staff to explain 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 use of independent testing data for the AI methods involved.

Gartner Recommended Reading

Digital Ethics: Use Facial Recognition Technology Responsibly

Autonomous Vehicles

Analysis By: Jonathan Davenport

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

Autonomous vehicles use various onboard sensing and localization technologies, such as lidar, radar, cameras, GPS and map data, in combination with AI-based decision making, to drive without human intervention. While self-driving passenger cars are getting most of the attention these days, the technology can also be applied to vehicles that transport goods.

Why This Is Important

Autonomous vehicles have the potential to change transportation economics, cutting operational costs and increasing vehicle utilization. In urban areas, cheap fares and high quality of service may cannibalize private car ownership. Road safety will also be increased as the AI systems will never be distracted, drive drunk or speed. Autonomous features on privately owned vehicles enable productivity and recreational activities to be undertaken, while the vehicle handles the driving operations.

Business Impact

- Autonomous vehicles have the potential to disrupt established automotive business models.
- Technology companies are building high-performance computers on which to run their self-driving software platforms.
- After the office and home, vehicles will become a living space, like airplanes, where digital content is both created and consumed.
- Over time, staff members currently undertaking driving roles must be retrained and redeployed to other, higher-value-adding roles within the company.

Drivers

- Some progress is being made toward autonomous vehicle regulations and standards. Automated lane-keeping system (ALKS) technology has been approved by the United Nations Economic Commission for Europe (UNECE). This forms the first binding international regulation for SAE Level 3 vehicle automation, with a maximum operational speed of 37 mph. Likewise, the German government aims to enact laws that enable autonomous vehicles to operate without special permits by 2022. Companies like Intel, Waymo and Aurora are working on the IEEE 2846, which will create a standard that describes the scenarios to be considered when developing autonomous road-safety-related models.

- To take advantage of the new regulatory landscape, automakers are beginning to announce Level 3 solutions. These autonomous vehicles provide drivers with safety and convenience features, reduce vehicle fuel consumption and improve traffic management. Honda is the first company to announce a commercially available Level 3 vehicle, though only 100 will be produced.

- Improvements are also being made to the perception algorithms and broader self-driving systems for Level 4 vehicles that will operate as robotaxis. Fully driverless operations have started, with Waymo operating in Arizona and WeRide operating in California without safety drivers. The flexibility of vehicle operational design domains (ODDs) has been showcased — e.g., Mobileye's perception algorithm required minimal additional training when it tested vehicles in new locations. Mobileye has developed its self-driving software on the roads in Israel, but showcased its autonomous technology in both Munich and Detroit. Likewise, Yandex has made great strides, showcasing how its autonomous vehicles are capable of handling the harsh weather conditions of winters in Moscow.

Obstacles

- Designing an AI system that is capable of driving a vehicle is hugely complex. As a result, the cost of bringing a commercial autonomous vehicle to market has been greater than companies could have previously envisioned. This has required significant investments to be made in companies. Acquisitions have occurred, and further market consolidation is expected — e.g., Walmart has invested $2.75 billion in Cruise; Cruise acquired Voyage in March 2021; Aurora acquired Uber's ATG in December 2020; Amazon acquired Zoox for $1.2 billion in June 2020; Apple bought self-driving startup Drive.ai in June 2019.
- When autonomous vehicles are commercially deployed, autonomous vehicle developers, not the human occupants, will be liable for the autonomous operations of the vehicle. This raises important issues, should a vehicle be involved in an accident.
- Challenges increasingly include regulatory, legal and societal considerations, such as permits for operation and the effects of human interactions.

User Recommendations

Governments must:

- Craft national legislation that ensures that autonomous vehicles can safely coexist with an older fleet of nonautonomous vehicles.

Autonomous mobility operators should:

- Support consumer confidence in autonomous vehicle technology by remaining focused on safety to deliver on the vision of an accident-free road environment.

Self-driving system developers should:

- Seek out use cases, such as mining, agriculture or airports, where autonomous vehicles can operate in restricted areas safely without regulatory restrictions. Use these implementations to drive early revenue and gather data and insights to improve the performance of self-driving systems.

Traditional fleet operators looking to adopt autonomous technology into their fleets should:

- Minimize the disruptive impact on driving jobs (bus, taxi and truck drivers) by developing policies and programs to train and migrate these employees to other roles.

Sample Vendors

Baidu; Cruise; Mobileye; Waymo; Yandex; Zoox

Gartner Recommended Reading

Market Trends: Monetizing Connected and Autonomous Vehicle Data

Forecast Analysis: Autonomous Vehicle Net Additions, Internet of Things, Worldwide

Utilize Partnerships to Secure a Winning Position in the Autonomous Driving Ecosystem

Market Insight: Use Situationally Aware Platforms to Enable Safe Autonomous Vehicle Handovers

Tech Providers 2025: Product Leaders Must Strategize to Win in the Evolving Robotaxi Ecosystem

Cloud Analytics

Analysis By: Julian Sun, Austin Kronz

Benefit Rating: Moderate

Market Penetration: More than 50% of target audience

Maturity: Early 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 or multicloud deployments are also becoming popular in order to cater to the cloud ecosystem.

Why This Is Important

There is growing adoption of cloud analytics. Most analytics deployments are originating in the cloud, and the majority of organizations say they are using or plan to use the cloud for analytics and data science. The cloud capability among analytics and BI vendors is also growing with emerging capabilities coming from cloud first. Cloud becomes an ideal place to build modular analytics capabilities that enable greater agility and reuse of existing investments in support of composable business.

Business Impact

- The cloud-enabled composition platform can achieve innovation by assembling modular analytics capabilities.
- More advanced analytics can complement key components of the analytics infrastructure in the cloud. The high computational load due to machine learning in advanced analytics can be carried in the cloud.
- Business users can pilot the cloud-first augmented analytics with an analytics sandbox provisioned by the cloud. It is a faster time to value and more targeted analytics deployment 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 also adding more deployment options and management capabilities. This enables portability with microservices architectures that are readily supported via Kubernetes across multiple clouds.
- Analytics solutions, such as Microsoft Power BI, are attracting organizations of all sizes to the cloud. There is a growing range of solutions available with most of the vendors in the market providing solutions as alternatives to on-premises products.
- Moreover, startups continue to join the BI market with cloud-only solutions, which are complementary to established platforms.
- The range of capabilities is growing too. Reporting and data visualization were already commodified capabilities. But customers can now also subscribe to self-service data preparation, augmented data discovery, predictive modeling, other advanced capabilities such as machine learning or streaming analytics, and even data/context broker services from several vendors.
- The growing cloud DBMS is also helping support and expand this market.

Obstacles

- Security is the No. 1 concern for organizations when moving to the cloud, but organizations need to plan how they will integrate their growing cloud analytics deployments with additional data sources, provide access to third-party analytic tools, and embed analytics in business processes. All of these are in hybrids of on-premises and cloud.
- Organizations' adoption of the cloud is closely tied to data gravity. Data gravity is the concept that as the amount of data grows, and the levels of customization, integration and access needs increase, data has greater propensity to "pull" data services, applications and even other data/metadata to where that data resides. It follows that smaller organizations with data originating in the cloud have higher adoption rates than larger organizations with their data center of gravity predominantly in on-premises legacy solutions.
- Hype around cloud analytics continues to be high, but is now facing growth obstacles as organizations struggle with deployment challenges.

User Recommendations

- Establish a designed approach to move to the cloud incrementally rather than simply "lift and shift." as cloud analytics is becoming a dominant option in most scenarios in the analytics space.
- Include innovative cloud analytics solutions in their portfolio, renovating components or complementing their on-premises platform if organizations want 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 the extra cost they need to spend and the TCO while adopting other products in the same cloud stack as the vendors are adding new capability in the clouds. From a cost perspective, although not requiring significant upfront investment like on-premises solutions do, cloud analytics solutions will likely have a more expensive licensing cost when considering periods of four or more years.

Sample Vendors

Alibaba Cloud; Sigma Computing; Mode; Microsoft; Oracle; Qlik

Gartner Recommended Reading

Achieve Bimodal Equilibrium With Cloud Analytics

Adopt Cloud Analytics to Drive Innovation

Composable Analytics Shapes the Future of Analytics Applications

Magic Quadrant for Analytics and Business Intelligence Platforms

Critical Capabilities for Analytics and Business Intelligence Platforms

Head-Mounted Displays

Analysis By: 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. They are worn or mounted on or near the head so their displays can be seen by the wearer at an ideal viewing distance. Additionally, aspects of the visual content will be contextual information that translates the wearer's state into visual cues.

Why This Is Important

In both AR and VR cases, HMDs are a hands-free display option for individuals and enterprises. In other words, HMDs exist on a spectrum of other computing and display options such as smartphones and tablets; and complement these devices. For AR, benefits are potentially high for frontline workers that benefit from a hands-free display — especially in capital-equipment-intensive industries. For VR, HMDs provide a level of immersion unavailable to traditional display devices.

Business Impact

HMDs can provide a hands-free and immersive way to interact with the physical and digital world.

Large enterprises see value in AR HMDs for cases such as increasing first-time fix, productivity and work order completion, and improved safety. VR HMDs's value is mostly for entertainment, but businesses are seeing more adoption for training, product design and reviews. MR HMD are further down the timeline for use cases such as accurately visualizing architectural fit for structures or machinery.

Drivers

- Mass-market penetration won't be achieved until key elements such as content availability and device usability and accessibility are vastly improved. Facebook's AR HMD plans and Apple's rumored head-worn device currently have limited impact on the pace and trajectory of HMDs, but will likely accelerate adoption as the launch dates draw near and applications are announced.
- We have moved the HMD profile forward by one position to represent the continued momentum due to market factors such as:
- Strong sales — 2020 was a strong year for HMD sales. The global pandemic spurred HMD sales (especially for consumer VR HMDs).

- Increased accessibility and usability — All-in-one VR HMDs continue to provide a significant stepping stone in VR adoption. Moreover, features such as Oculus Link extend content library access. This accessibility will be further increased by adding wireless capability (Air Link).

- Burgeoning ecosystem — The value chain for AR and VR is evolving. The net benefit is improvements that promote enterprise adoption (such as better deployment, management and integration).

- Technology improvement — Continued technology improvements across the spectrum of HMD and adjacent technologies display and optics technologies, computer vision-based applications, natural language technologies, rendering and graphics technologies, interfaces and more have made experiences much more immersive.

Obstacles

- Single-purpose and purpose-built devices will have limited adoption potential (for example, within certain tasks within the enterprise)

- Current AR, MR and VR use cases do not reflect the enormous potential of HMDs

- Current technology limitations will introduce barriers such as interoperability, form factor, legal and social limitations (such as safety and fashion), ergonomics and battery life

- Enterprise adoption is limited by lack of enterprise-ready solutions

- Limited collaboration and investment will occur among hardware providers

User Recommendations

- Use HMDs as an extension of your current endpoint devices (laptops, smartphones, tablets, monitors) spectrum.

- Evaluate AR/MR HMDs for situations where the user’s hands are occupied with a task or when the user is moving while accessing information — for example, to review work instructions, schematics or customer data.

- Assess the cost of VR experiences against the benefits. The cost of service and customization for VR experiences can come at a high cost, but there are also barriers around user interfaces (how to interact with virtual, 3D objects) and user experience (motion sickness and other adverse, physical reactions due to sensory mismatch).
- Adopt HMDs tactically — current devices are purpose-built hardware with rapid (yearly) product release cycles.
- Evaluate ROI potential by monitoring HMD advancement such as improvements in display (resolution, brightness, response time, field of view), better battery life, comfort and lower cost.

Sample Vendors

Facebook; Google; HTC; Microsoft; RealWear; Vuzix

Gartner Recommended Reading

Emerging Technologies: Head-Mounted Displays for Augmented, Mixed and Virtual Reality

Product Manager Insight: OEMs and ODMs Must Adopt a Platform Strategy for the Augmented Reality Market

Forecast Analysis: Wearable Electronic Devices, Worldwide

Climbing the Slope

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, process and analyze data in an indoor environment. They provide 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, Bluetooth low energy (BLE), infrared, ultrasound, RFID, ultrawideband (UWB) 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. Since the COVID-19 outbreak, interest in this technology has further accelerated with the proliferation of social distancing solutions. These solutions can include different elements to help employees return to work, such as special tracking devices, analytics software or mobile apps.

Business Impact

We see strongest growth of indoor location intelligence in healthcare, retail and manufacturing, followed by hospitality, public transport/airports and the public sector. Each vertical presents different benefits/impacts for indoor location intelligence. In healthcare, hospitals benefit from asset tracking, patient tracking and monitoring, and staff tracking to increase efficiencies and lower cost, while visitors benefit from indoor navigation and a better customer experience.

Drivers

We have positioned this profile two positions further in the post-trough area. The drivers identified are:

- The COVID-19 pandemic induced proliferation of indoor location intelligence during 2020 as organizations with a lot of external traffic such as retail shops, airports, stadiums, etc., turned to location intelligence to adhere to social distancing guidance.

- Lidar emerged as a new technology to measure distance between assets or people for location intelligence. Some vendors started to integrate lidar into their existing wireless location technology portfolio. Moreover, a growing number of indoor location services platforms integrate with computer vision and 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.

Obstacles

- Technology choice: Some technologies provide centimeter accuracy versus 4 to 5 meters, but the high-precision technologies tend to be more expensive. Hence, there is a trade-off and organizations need to precisely define their use cases to determine what accuracy level they need.

- Data privacy: Location data is sensitive data 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. Also, privacy regulations vary widely in different markets, therefore location data needs to be handled differently in one location compared to another.

User Recommendations

- Be cognizant of the direct trade-off between location accuracy and cost, and deploy the technology that supports your use case. Overdelivery on accuracy will significantly increase costs, while underdelivering on accuracy will bring no value and the project may fail.

- Determine which type of customer data you need to collect, store and process, and for what purpose. Set up different scenarios that categorize the data types. These categories should be location data of objects vs. people, and then further refined by anonymized vs. identifying data. This will help you determine which data privacy regime to follow.

- Be transparent toward staff on when and what location data is processed/stored, emphasizing the safety aspects of your solution and the fact that personal location data is not tracked off-premises.

Sample Vendors

AiRISTA Flow; CenTrak; Purple; Quuppa; Ubisense; Zebra Technologies

Gartner Recommended Reading

Magic Quadrant for Indoor Location Services, Global

Competitive Landscape: Indoor Mapping

Market Guide for Indoor Location Application Platforms

Architecting for Location

ZTNA

Analysis By: John Watts, Lawrence Orans, Neil MacDonald

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Zero trust network access (ZTNA) creates an identity- and context-based logical access boundary around applications. Applications are hidden from discovery and access is restricted via a trust broker to a set of named entities. The broker verifies identity, context and policy adherence of specified participants and devices before allowing access, and prohibits lateral movement in the network. This removes public visibility of applications and significantly reduces the attack surface area.

Why This Is Important

ZTNA is a key technology for enabling user-to-application segmentation through a trust broker, to enforce a security policy that allows organizations to hide private applications and services and enforces a least-privilege access model for applications. It is a synthesis of concepts in the Cloud Security Alliance's Software-Defined Perimeter (SDP) guide, Google's BeyondCorp vision and O'Reilly's Zero Trust Networks book.

Business Impact

ZTNA yields immediate benefits by shielding services from attackers. In contrast to basic VPN products, ZTNA removes full network access and improves user experience, flexibility and adaptability. It enables more granular user-to-application segmentation through simplified policy management. Cloud-based ZTNA offerings improve scalability and ease of adoption. Early products on the market focused on web applications, but have expanded to work with a wider range of applications and protocols.

Drivers

- The need to support digital business transformation scenarios ill-suited to legacy access approaches, such as access to applications, services and data located outside the enterprise.

- Need for flexibility to quickly expand capacity as the sudden shift to remote work in 2020, with the onset of the COVID-19 pandemic, strained legacy on-premises VPN infrastructure.

- The rise of zero trust initiatives within organizations, which resulted in the need for more precise access and session control in on-premises and cloud applications.

- A desire for vendor consolidation, to remove point solutions and adopt more products from vendors with SASE frameworks, resulting in ZTNA additions to existing SWG or CASB services.

- A need to connect third parties such as suppliers, vendors and contractors to applications securely without exposing the network over VPN, or to connect the application to the internet for access.

- Mergers and acquisitions enabled by the ability to extend application access to acquired companies preclosure without needing to deploy endpoints or connect networks directly between the two companies.

Obstacles

- Cost: ZTNA is typically licensed per named user on a per user per year basis and may cost more than traditional VPNs.
- Limited support: Not all products support all applications. For example, some only support web, RDP and SSH protocols.
- Agent or agentless ZTNA: Some providers only offer one way to consume ZTNA. This limits applicable use cases.
- Weak identity management: Organizations with no federated identity support in the cloud find limitations with use cases as many providers rely on third-party identity providers for user authentication.
- Lack of on-premises trust brokers: Cloud-based trust brokers work well for remote access, but may not be preferred to extend the same policies on-premises. While providers exist that have both cloud and on-premises trust brokers, they are far and few between.
- Limited knowledge of acceptable application access rights for users: Organizations must map the correct application accesses upfront to get full benefit of ZTNA.

User Recommendations

- Open applications and services without requiring the use of a VPN or DMZ.
- Normalize the user experience for application access both on and off the corporate network.
- Implement application-specific access for employees and IT contractors as an alternative to VPN-based access.
- Extend access to systems prior to a merger, without having to configure site-to-site VPN and firewall rules.
- Allow access on personal devices by reducing full bring your own device (BYOD) management requirements and enabling more secure direct application access.
- Cloak systems from hostile networks, such as collaboration systems exposed to the internet.
- Permit users in potentially dangerous areas of the world to interact with applications and data to reduce or eliminate risk.
- Secure access to enclaves of Internet of Things (IoT) devices if the device can support a lightweight SDP agent or a virtual-appliance-based connector on the IoT network segment for connection.

Sample Vendors

Akamai; Appgate; Cato Networks; Ivanti; Netskope; Perimeter 81; Proofpoint; SAIFE; Zscaler

Gartner Recommended Reading

Market Guide for Zero Trust Network Access

Solving the Challenges of Modern Remote Access

Quick Answer: Cost Effectively Scaling Secure Access While Preparing for a Remote Workforce

Quick Answer: How to Securely Enable Access for Unmanaged Devices

2021 Strategic Roadmap for SASE Convergence

Crisis/Emergency Management Solutions

Analysis By: Roberta Witty, David Gregory

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Through a unified management console, crisis/emergency management (C/EM) solutions provide consistent monitoring, orchestration and management of a crisis through all its phases while maintaining compliance with government, regulatory and industry emergency management standards. C/EM solutions are used to manage data, resources, expenditures, communications and tasks before, during and after a crisis, and analyze the changing crisis conditions to enable situational awareness.

Why This Is Important

C/EM solutions help organizations implement a standardized, best-practice model (including organizationwide managerial controls) to contain and minimize a crisis/incident. This helps protect organizations' reputation in the eyes of all stakeholders — employees, customers, citizens, partners, suppliers, auditors, regulators, etc. They also reduce staff training time and ensure better integration with the broader internal and external community involved in recovering from a disaster.

Business Impact

A crisis is a situation that threatens, or is perceived to threaten, organizational resources and operations, resulting in threat to life/safety, disruption to business services, damage to reputation and brand, etc. Organizations must prepare for large and small crises (which can quickly escalate to a larger event) by developing a crisis management program to contain and minimize their impacts. A C/EM solution instantiates a command-and-control structure for all types of crises.

Drivers

- Due to COVID-19, organizations are realizing the value in using C/EM solutions for crisis management as well as preevent risk monitoring. We expect that crisis management capabilities will become part of day-to-day operations solutions so that risks can be anticipated early, and action to mitigate or respond can be better executed to protect reputation in the eyes of all stakeholders.

- C/EM solutions establish a command-and-control structure and process for all types of crisis events and improve organizations' ability to protect public/workforce safety and restore services as quickly as possible.

- C/EM solutions codify the roles, responsibilities and decision-making authority involved with a crisis.

- These solutions also improve the efficiency of crisis/emergency command and related emergency responses via continuous communication and progress assessments.

- C/EM solutions ensure effective management of relationships and communications with internal stakeholders, visitors, the public and external stakeholders, including communications between critical infrastructure service providers and government agencies during regional and nationwide disasters.

- C/EM solutions support administration of response, recovery and restoration phase actions for the event through task and workforce management; media communications, including national services and social media traffic; and expenses incurred during the crisis to better ensure repayment from business interruption insurance policies and government disaster management funding.

- C/EM solutions enable management of program documentation that needs to be submitted to national authorities; all crisis-related data, ensuring it is tracked for postevent analysis; and postincident reviews for regulatory reporting and overall process improvement.

Obstacles

- Finding one C/EM solution to meet all crisis use cases (e.g., pandemics, cyberattacks, IT outages, traditional natural disasters, terrorist attacks, supply chain outage and other man-made events) may not be possible. Implementing multiple solutions, on the other hand, hinders whole-of-enterprise impact analysis of a potential hazard/threat as well as enterprisewide management of the crisis event, due to different buyers within the organization (e.g., BCM, corporate security leaders, IT leaders, cybersecurity leaders, supply chain leaders).

- Integrating a C/EM solution with other resilience-related solutions, such as hazard/threat intelligence, BCMP, EH&S, EMNS, supply chain risk management, integrated risk management and IT resilience orchestration solutions, is highly complex.

- Industry-specific requirements may not be available in a solution that meets most but not all C/EM needs of the organization.

User Recommendations

- Establish an enterprisewide effort to identify all C/EM program needs so that as few C/EM solutions as possible need to be implemented.

- Assess the extent to which the functionality of purpose-built C/EM, BCMP, IT service management and IT resilience orchestration solutions best supports your organization's C/EM program requirements.

- Heavily weigh the ease-of-configuration functionality when selecting a C/EM solution so you can add your day-to-day business processes to the solution, allowing you to move toward a single solution for both crisis and day-to-day business operations use.

- Assess the C/EM solution's application and data integration methods to ensure it can meet the integration needs of your organization to support situational awareness.

- Choose a platform that adheres to public-sector emergency management protocols as well as environmental, health and safety (EH&S) public service protocols. This helps ensure timely and efficient responses that minimize damage.

Sample Vendors

4C Strategies; Esri; Everbridge; Fusion Risk Management; IntraPoint; Juvare; LiveProcess; Swan Island Networks; Tableau; Veoci

Gartner Recommended Reading

Market Guide for Crisis/Emergency Management Solutions and COVID-19 Safe Return to Work

Market Guide for Business Continuity Management Program Solutions, 2021

Entering the Plateau

Outdoor Location Intelligence

Analysis By: Bill Finnerty

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Outdoor location intelligence (OLI) is the process of deriving meaningful insight from geospatial data relationships — people, places or things — to solve particular challenges like demographic analysis, store placement, asset tracking, people movement and contact, environmental analysis. and traffic planning. OLI consists of a combination of GIS software, web mapping solutions, geospatial services and platforms, position technologies such as GPS, and location-based data.

Why This Is Important

Location is one of the most significant means of contextualizing user and sensor data. OLI, founded in geospatial and location intelligence, presents an ever-growing set of use cases in marketing, smart cities, Industrie 4.0, healthcare and other sectors.

Cloud, whether PaaS or SaaS, and web mapping solutions provide expanded opportunities for organizations to leverage and scale OLI at competitive prices, making the entry point for experimentation within reach of a larger number of organizations.

Business Impact

OLI can reveal previously unidentified opportunities, based on location and spatial relationships, for business and government. Opportunities manifest as improved operations, new approaches to marketing and engagement, and enhanced decision making. Cases can be found across many sectors, including government, retail, hospitality and transportation — for example, combining business and location data to visualize customer and revenue data on maps to identify sales and marketing opportunities.

Drivers

- Increasing amounts of spatially contextualized data, frequently generated by IoT sensors, provides enhanced opportunities to leverage geospatial and location intelligence to improve service, engagement and decision making. Access to this spatial data through open data portals, data marketplaces and location intelligence platforms is growing, generating more opportunities for its use.

- Maturing OLI tools increasingly support business line functionality. In addition to GIS vendors and those embedding OLI in applications, business intelligence and other data visualization solutions regularly provide OLI capabilities. Solutions frequently enable “citizen analysts” to leverage OLI data for spatial analysis to improve operations, discover new business and service delivery opportunities, and communicate with customers and constituents.

- Through the growth of location intelligence platforms, a larger number of organizations are able to use machine learning capabilities to analyze the vast amount of spatial data available to them. These machine learning capabilities are driving the development of more-advanced location intelligence solutions, such as improved routing and traffic analysis that benefits commuters, logistics companies and public safety organizations.

Obstacles

- Privacy and data laws, although being challenged as part of the pandemic response, require organizations to be mindful of their use of personal data in OLI initiatives or face societal backlash.

- The cost of data can price projects without a clear ROI beyond an organization’s reach. However, data-as-a-service offerings can provide some controls.

User Recommendations

- Empower business units in leveraging OLI by providing the platform to improve decision making, service delivery and business processes.

- Inspire business stakeholders to leverage OLI in new ways by providing relative examples and use cases, while also insisting that they clearly define the business value or ROI for any initiatives.

- Establish a spatial data management strategy, or include spatial data in an existing data strategy, to improve quality and use of spatial data. Use the strategy to expose data catalogs to maximize data reuse and promote data sharing.

- Include spatial data in existing data governance processes.
- Create a framework for determining the best means for acquiring data. Include options for using open data, developing new datasets, utilizing data as a service or purchasing new data.
- Grow the skills of citizen analysts to improve understanding of spatial analysis and relative capabilities by establishing a spatial data and analysis training program.

Sample Vendors

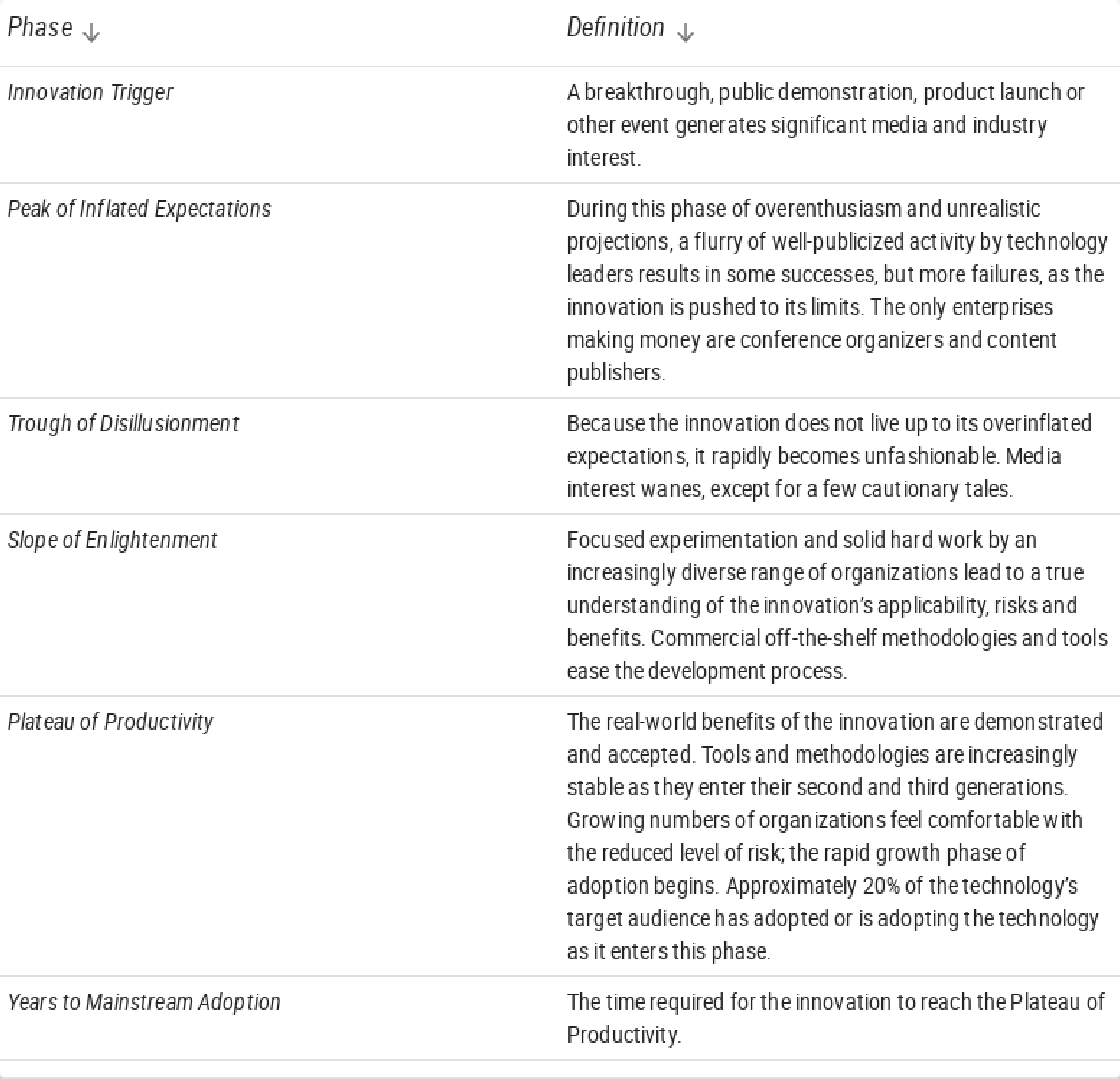
Alteryx; CARTO; Descartes Labs; DECE Software; Esri; HERE Technologies; Mapbox; Microsoft; Planet; Qlik

Appendixes

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 3: 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 (August 2021)

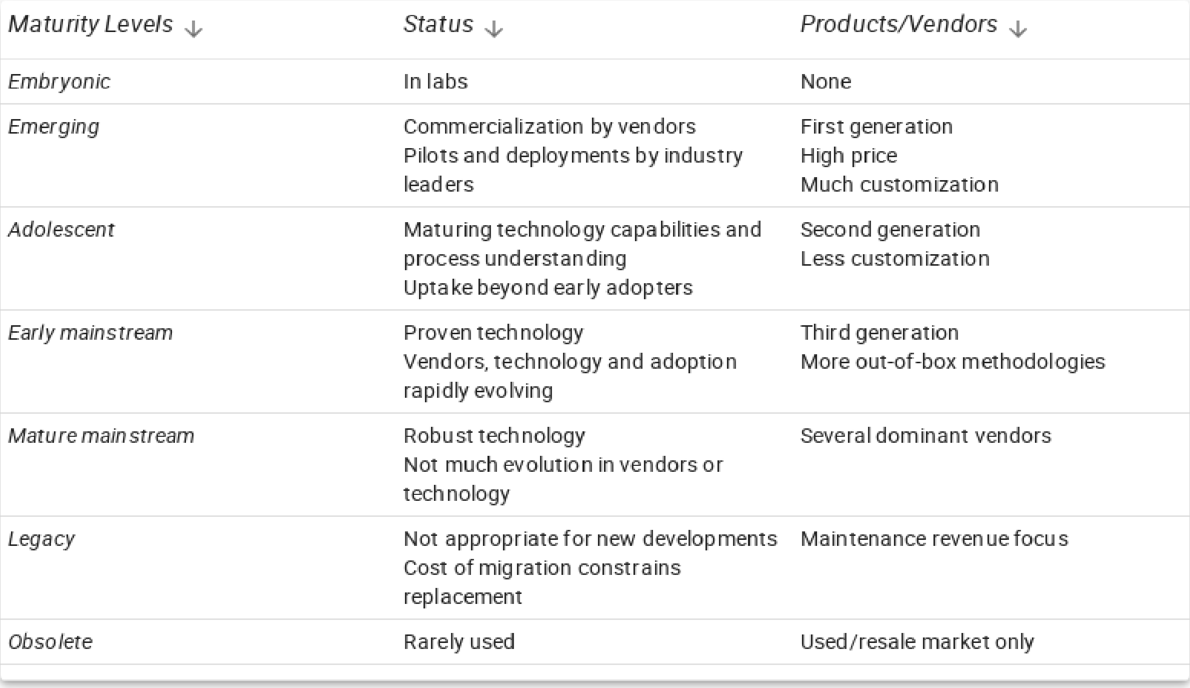
Table 4: Benefit Ratings

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 (August 2021)

Table 5: 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 (August 2021)

Evidence

[1] The 2021 Gartner CIO Survey was conducted online from 14 July 2020 through 14 August 2020 among Gartner Executive Programs members and other CIOs. Qualified respondents are each the most senior IT leader (CIO) for their overall organization or a part of their organization (for example, a business unit or region). The total sample was 1,877, with representation from all geographies and industry sectors (public and private), including 97 from Brazil.

The survey was developed collaboratively by a team of Gartner analysts, and was reviewed, tested and administered by Gartner's Research Data and Analytics team. Disclaimer: Results do not represent "global" findings or the market as a whole but reflect sentiment of the respondents and companies surveyed.

Q: How would you characterize the following changes related to your enterprise's IT leadership as a result of the COVID-19 pandemic?

Recommended by the Authors

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

Understanding Gartner's Hype Cycles

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

Hype Cycle for Smart City Technologies and Solutions, 2021

Hype Cycle for Digital Government Technology, 2021

Table 1: Innovation Profiles Adopted from Other Hype Cycles

Innovation Profile(s)	Impact
Synthetic data	Address significant analytics challenges in public safety and law enforcement such as bias in historic datasets or the small data problem
Workstream collaboration tools	Enable digital workplace efforts and promote better collaboration and coordination between law enforcement agencies and with the public
Edge computing and edge AI	Support public safety and law enforcement organizations in real-time decision making by enabling greater use of IoT*, computer vision, machine learning and analytics in the field
Smart robots and autonomous vehicles	Provide operational advantages as a force multiplier, but they will also present new challenges for organizations
* IoT = Internet of Things	

Source: Gartner (August 2021)

Table 2: Priority Matrix for Public Safety and Law Enforcement, 2021

Benefit	*Years to Mainstream Adoption*			
↓	***Less Than 2 Years*** ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓
Transformational		Edge AI Edge Computing Live Face Recognition Machine Learning Public Safety Predictive Analytics Real-Time Incident Center as a Service Virtual Assistants	Emotion AI in Public Safety and Law Enforcement Immersive Training in PS/LE LEO Satellite Systems LTE/5G Enhanced Services Multiexperience	Autonomous Vehicles
High	Outdoor Location Intelligence Workstream Collaboration	Computer Vision in Government Crisis/Emergency Management Solutions Indoor Location Intelligence Packaged Business Capabilities Synthetic Data Wearable Monitors for Public Safety	Citizen Twin Field Streaming Video Head-Mounted Displays Rapid DNA in Policing Smart Robots	

Benefit	*Years to Mainstream Adoption*			
↓	***Less Than 2 Years*** ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓
Moderate	Drone Countermeasures	Cloud Analytics ZTNA	Blockchain for Evidence Edge Security	
Low			Enterprise Wearable Device Management	

Source: Gartner (August 2021)

Table 3: 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 (August 2021)

Table 4: 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 (August 2021)

Table 5: 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 (August 2021)