Top 10 Strategic Technology Trends for 2020

Published: 21 October 2019 **ID:** G00432920

Analyst(s): David Cearley, Nick Jones, David Smith, Brian Burke, Arun Chandrasekaran, CK Lu

Strategic technology trends have the potential both to create opportunity and to drive significant disruption. Enterprise architecture and technology innovation leaders must evaluate these top trends to determine how combinations of trends can power their innovation strategies.

Key Findings

- Strategic technology trends have significant potential to create and respond to disruption and to power both transformation and optimization initiatives.
- Artificial intelligence (AI) is a foundational catalyst for advanced process automation and human augmentation and engagement.
- Physical environments including factories, offices and cities will become “smart spaces” within which people will interact through multiple touchpoints and sensory channels for an increasingly ambient experience.
- Dealing with privacy, digital ethics and security challenges generated by AI, the Internet of Things (IoT)/edge, and other evolving technologies will become critical to maintain trust and avoid legal entanglements.

Recommendations

Enterprise architecture and technology innovation leaders must:

- Center their innovation efforts on people and use tools such as personas, journey maps, technology radars, and roadmaps to evaluate opportunities, challenges and time frames for adoption.
- Build an overarching view across functional and process silos and exploit a complementary set of tools including RPA, iBPMS, DTO, application development, and AI domains that guide how the tools are used and the systems they create are integrated.
- Embrace multiexperience and implement development platforms and design principles to support conversational, immersive and increasingly ambient experiences.

- Establish governance principles, policies, best practices and technology architectures to increase transparency and trust regarding data and the use of AI.

Table of Contents

List of Figures

Strategic Planning Assumptions

By 2022, 70% of enterprises will be experimenting with immersive technologies for consumer and enterprise use, and 25% will have deployed them to production.

By 2022, 35% of large businesses in the training and simulation industry will evaluate and adopt immersive solutions, up from less than 1% in 2019.

By 2021, at least one-third of enterprises will have deployed a multiexperience development platform to support mobile, web, conversational and augmented reality development.

By 2024 75% of large enterprises will be using at least four low-code development tools for both IT application development and citizen development initiatives.

By 2022, at least 40% of new application development projects will have artificial intelligence co-developers on the team.

By 2021, automation of data science tasks will enable citizen data scientists to produce a higher volume of advanced analysis than specialized data scientists.

By 2025, a scarcity of data scientists will no longer hinder the adoption of data science and machine learning in organizations.

By 2022, 30% of organizations using AI for decision making will contend with shadow AI as the biggest risk to effective and ethical decisions.

Through 2023, 30% of IT organizations will extend BYOD policies with “bring your own enhancement” (BYOE) to address augmented humans in the workforce.

By 2020, we expect that companies that are digitally trustworthy will generate 20% more online profit than those that aren’t.

By 2020, we expect that 4% of network-based mobile communications service providers (CSPs) globally will launch the 5G network commercially.

By 2024, most cloud service platforms will provide at least some services that execute at the point of need.

By 2023, blockchain will be scalable technically, and will support trusted private transactions with the necessary data confidentiality.

Through 2022, over 75% of data governance initiatives will not adequately consider AI’s potential security risks and their implications, resulting in quantifiable financial loss.

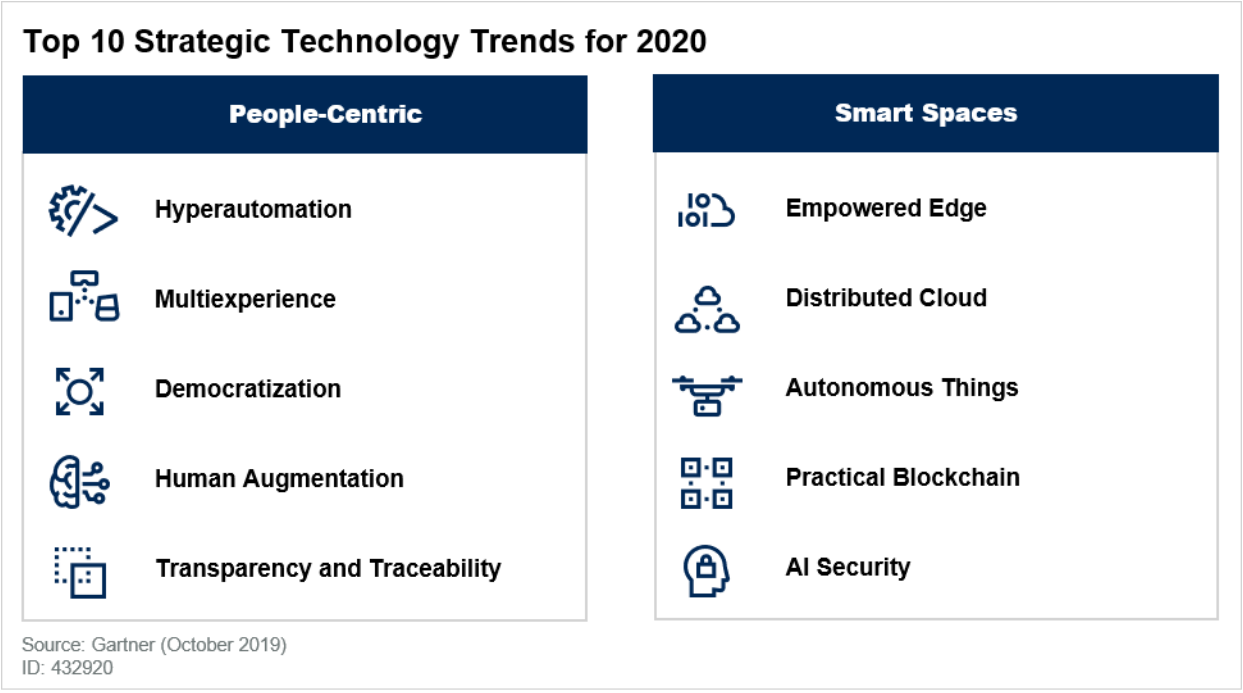
Through 2022, 30% of all AI cyberattacks will leverage training-data poisoning, AI model theft or adversarial samples to attack AI-powered systems.

Analysis

This document was revised on 27 November 2019. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

Gartner’s annual top 10 strategic technology trends (see Figure 1) highlight trends that enterprises need to consider as part of their five-year strategic technology planning process. These trends have a profound impact on people and the spaces they inhabit. Strategic trends have broad impact across industries and geographies, with significant potential for disruption. In many cases, the trends aren’t yet widely recognized or the conventional wisdom regarding the trends is shifting (see Note 1). Through 2025, technologies related to these trends will experience significant changes, cross critical tipping points and reach new levels of maturity that expand and enable repeatable use cases and reduce risk. Technology innovation leaders must examine the business impact of our top 10 strategic technology trends and seize the opportunities to enhance existing, or create new, processes, products and business models. Prepare for the impact of these trends — they will transform industries and your business.

Figure 1. Top 10 Strategic Technology Trends for 2020



The top 10 strategic technology trends are a critical ingredient in driving a continuous innovation process as part of a ContinuousNext strategy.[1] Technology innovation leaders must adopt a mindset and new practices that accept and embrace perpetual change. That change may be incremental or radical, and may be applied to existing or new business models and technologies.

Technology is changing people's lives, enabling the ongoing digitalization of business and driving organizations to continually refresh their business models. In this long march to digitalization, technology is amplifying continuous change at an ever-increasing velocity. Organizations need to consider how these strategic trends can be applied across two continuous and complementary cycles:

- **Continuous operations** exploit technology to run the business today, modernize it and improve efficiency, and incrementally grow the business. Existing business models and technology environments set the stage upon which innovation opportunities are explored and will ultimately influence the cost, risk and success of implementing and scaling innovation efforts.
- **Continuous innovation** exploits technology to transform the business and either create or respond to disruptions affecting the business. This innovation cycle looks at more radical changes to business models and supporting technologies as well as new business models and technologies that extend the current environment.

Trends and technologies do not exist in isolation. They build on and reinforce one another to create the digital world. Combinatorial innovation explores the way trends combine to build this greater

whole. Individual trends and related technologies are combining to begin realizing the overall vision embodied in the intelligent digital mesh.[2] For example, AI in the form of machine learning (ML) is combining with hyperautomation and edge computing to enable highly integrated smart buildings and city spaces. In turn, this enables further democratization of the use of technology as business users and customers self-serve to meet their individual needs. CIOs and IT leaders are challenged with a number of "*and* dilemmas" such as delivering existing services *and* innovating new services. You can turn "*and* dilemmas" into "*and* opportunities" by applying "*and* thinking," where the combined effect of multiple trends coalescing is to produce new opportunities and drive new disruption. Combinatorial innovation is a hallmark of our top 10 strategic technology trends for 2020.

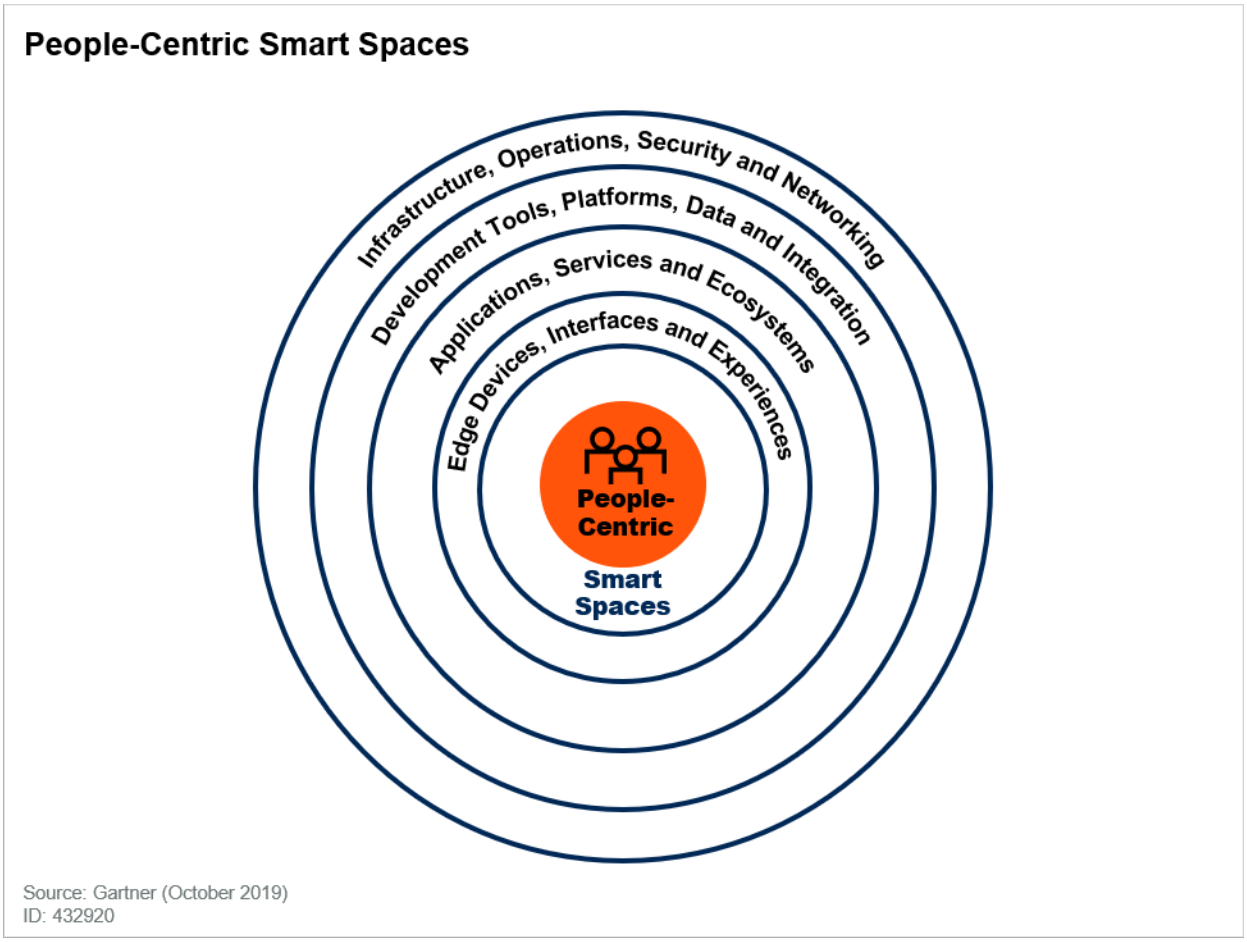
People-Centric Smart Spaces Build on the Intelligent Digital Mesh

The future will be characterized by smart devices delivering increasingly insightful digital services everywhere. We call this the "intelligent digital mesh." It can be described as:

- The **intelligent** theme explores how AI — with a particular emphasis on machine learning — is seeping into virtually every existing technology and creating entirely new technology categories. The exploitation of AI will be a major battleground for technology providers through 2022. Using AI for well-scoped and targeted purposes delivers more flexible, insightful and increasingly autonomous systems.
- The **digital** theme focuses on blending the digital and physical worlds to create a natural and immersive digitally enhanced experience. As the amount of data that things produce increases exponentially, compute power shifts to the edge to process stream data and send summary data to central systems. Digital trends, along with opportunities enabled by AI, are driving the next generation of digital business and the creation of digital business ecosystems. In this intelligent digital world, massive amounts of rich and varied data are generated, thus necessitating a greater focus on digital ethics and privacy and on the transparency and traceability that they require.
- The **mesh** theme refers to exploiting connections between an expanding set of people and businesses — as well as devices, content and services — to deliver digital business outcomes. The mesh demands new capabilities that reduce friction, provide in-depth security and respond to events across these connections.

Intelligent digital mesh has been a consistent theme of Gartner's strategic technology trends for the past few years, and it will continue as an important underlying force over the next five years. However, this theme focuses on the set of technical characteristics of the trend. It is also important to put the trends in the context of the people and organizations that will be impacted. Rather than building a technology stack and then exploring the potential applications, organizations must consider the business and human context first. We call this "people-centric smart spaces" and this structure is used to organize and evaluate the primary impact of the strategic trends for 2020 (see Figure 2).

Figure 2. People-Centric Smart Spaces



By putting people at the center of your technology strategy you are highlighting one of the most important aspects of technology — how it impacts your customers, employees, business partners, society or other key constituencies.[3] A people-centric approach should start with understanding these key target constituencies and the journey they undertake to interact with or support your organization. This is the first step to understanding how and where you will apply strategic technology trends to drive desired business outcomes:

- **Personas:** The persona is a useful tool to describes a target individual or group. The persona encapsulates a set of motivations, preferences, biases, needs, wants, desires and other characteristics that can be used as a backdrop to evaluate how applications of technology might impact that group. Personas have been used for many years and have gained broadest adoption in design and marketing areas, where understanding the motivations of a target audience are particularly important.[4] The persona sets the context for evaluating the potential impact on people and the resulting business outcome. Personas can be used to anticipate the valuable business moments that emerge as people traverse technology-enabled smart spaces.[5]

Persona-based analysis is a powerful tool that helps leaders diagnose and take action against digital-business-disruption opportunities. Enterprise architecture and technology innovation leaders can help business and IT leaders to consider the human side of digital business strategy decisions with personas.

- **Journey Maps:** A second useful tool is the defining of "journey maps." A journey map is a model that shows the stages that target personas go through to accomplish a task or complete a process. Customer journey maps diagram the stages a customer might go through to buy products, access customer service, or complain about a company on social networks. One can also consider internal journey maps that diagram the stages employees go through in onboarding or in complying with a regulatory requirement. Journey maps that look at how multiple constituencies interact around a process are even more powerful. For example, a journey map for a customer purchase might consider not only the customer view, but also that of a salesperson or a fulfillment group. Journey maps provide even more concrete context for technology-driven innovation. Technology innovation professionals should consider the pain points, inefficiencies, gaps, and opportunities to delight and create new digital business moments for all the relevant constituents.

The concept of smart spaces builds on the people-centric notion. People exist in spaces such as their homes, their cars, an office building, a conference room, a hospital or a city. A smart space is a physical environment in which humans and technology-enabled systems interact in increasingly open, connected, coordinated and intelligent ecosystems. Multiple elements — including people, processes, services and things — come together in a smart space to create a more immersive, interactive and automated experience for a target set of personas. Journey maps should consider not only the motivations of relevant personas and the desired business outcomes, but also the spaces that people will traverse as part of their interactions in the digital world.

People-centric smart spaces represent the core target for applying technology trends. Surrounding this focus, technology innovation leaders should consider a concentric ring of trends that progress from those that directly touch the human to those that are more hidden with a derivative impact. Thinking of the technology environment from the center out, proceeding from people and ultimately focusing on the back-end infrastructure, is a subtle but useful shift from the traditional bottom-up view of a technology stack. Driving architecture from the center out ensures requirements at each level are driven by business outcomes and the architecture is inherently more adaptable:

- People interact with others and with the digital spaces through edge devices and multiple user experiences (interfaces) across these edge devices as a natural part of their everyday lives.
- Applications, services, and ecosystems deliver value to people in those spaces through edge devices and experiences.
- Development tools, digital platforms, data, AI/ML services, integration and related technologies are used to create the applications and services that deliver value through edge devices. These tools provide a dynamic, flexible and modular foundation to create the applications, services and ecosystems.

- Infrastructure, operations, networking and security are the foundation upon which the technology-enabled world is built. It must deliver value at each layer as it ultimately supports people.

Our top 10 strategic technology trends for 2020 are organized into people-centric and smart spaces categories. This is a loose organization intended to convey where the primary impact and manifestation of the trend will be seen. However, virtually all of the trends will have an impact on both the people and smart spaces concepts.

- **People-Centric:**
  - **Hyperautomation** deals with the application of advanced technologies including AI and machine learning to increasingly automate processes and augment humans.
  - **Multiexperience** deals with the way that people perceive, interact and control the digital world across a wide range of devices and sensory touchpoints.
  - **Democratization** explores how to create a simplified model for people to consume digital systems and tap into automated expertise beyond their training or experience.
  - **Human augmentation** explores how humans are physically and cognitively augmented by these systems.
  - **Transparency and traceability** focuses on the data privacy and digital ethics challenges and the application of design, operational principles, and technologies to increase transparency and traceability to enhance trust.
- **Smart Spaces:**
  - **Empowered edge** emphasizes how the spaces around us are increasingly populated by sensors and devices that connect people to one another and to digital services.
  - **Distributed cloud** examines a major evolution in cloud computing where the applications, platforms, tools, security, management and other services are physically shifting from a centralized data center model to one in which the services are distributed and delivered at the point of need. The point of need can extend into customer data centers or all the way to the edge devices.
  - **Autonomous things** explores how physical things in the spaces around people are enhanced with greater capabilities to perceive, interact, move, and manipulate these spaces with various levels of human guidance, autonomy and collaboration.
  - **Practical blockchain** focuses on how blockchain can be leveraged in practical enterprise use cases that are expanding over the next three to five years.
  - **AI security** deals with the reality of securing the AI-powered systems that are behind the people-centric trends.

Trend No. 1: Hyperautomation

Automation refers to the use of technology to facilitate or perform tasks that originally required some form of human judgment or action. The term "tasks" refers not only to tasks and activities in the execution, working or operational environment, but it also encompasses tasks in thinking, discovering and designing these automations themselves.

Hyperautomation refers to the combination of multiple machine learning, packaged software and automation tools to deliver work. The propensity to use particular types of automation will be highly dependent on the organization's existing IT architecture and business practices. Hyperautomation refers not only to the breadth of the palette of tools, but also to all the steps of automation itself (discover, analyze, design, automate, measure, monitor, reassess).

Hyperautomation is an unavoidable market state in which organizations must rapidly identify and automate all possible business processes with several implications:

- **The scope of automation changes.** The automation focus now spans automating individual, discrete tasks and transactions based on static and rigid rules, to automating more and more knowledge work. In turn, those levels of automation enable enhanced and more dynamic experiences and better business outcomes.
- **A range of tools will be used to manage work and coordinate resources.** Increasingly, organizations will use an evolving set of technologies to support an ever-expanding business scope. The tools include task and process automation, decision management, and packaged software — all of which will incorporate more and more machine learning technologies.
- **Architecting for agility is required.** This means organizations need the ability to reconfigure operations and supporting processes in response to evolving needs and competitive threats in the market. A hyperautomated future state can only be achieved through hyperagile working practices and tools.
- **Workforce engagement is needed to reinvent how employees deliver value.** Without engaging employees to digitally transform their operations, the organization is destined to gain only incremental benefits. This means overcoming the challenges associated with silos and the way the organization allocates resources and integrates the capabilities of its partners and suppliers.

RPA and iBPMS Are Key Components of Hyperautomation

Hyperautomation requires selection of the right tools and technologies for the challenge at hand. Understanding the range of automation mechanisms, how they relate to one another, and how they are combined and coordinated, is a major focus for hyperautomation. This is complicated because there are currently many multiple, overlapping and yet ultimately complementary technologies including:

- **Robotic process automation (RPA):** RPA is a useful way to connect legacy systems that don't have APIs with more modern systems (see Note 2). It will move structured data from system A to system B better than people and addresses integration challenges with legacy systems. The

scope of these processes is typically a short-lived task associated with moving that data. RPA tools can also augment knowledge workers undertaking day-to-day work, removing mundane and repetitive tasks. Tightly defined integration scripts structure and manipulate data, moving it from one environment to the next. Because the integration is based on interacting with the metadata that drives the screens of existing applications, these tools are usually more accessible to business end users.

- **Intelligent business process management suites (iBPMSs).** Beyond RPA, iBPMSs manage long-running processes. An intelligent business process management suite is an integrated set of technologies that coordinates people, machines and things. An iBPMS relies on models of processes and rules to drive a user interface and manage the context of many work items based on those models. Integration with external systems is usually achieved via robust APIs. Alongside the processes, strong decision models can simplify the environment and provide a natural integration point for advanced analytics and machine learning. iBPMS software supports the full life cycle of business processes and decisions: discovery, analysis, design, implementation, execution, monitoring and continuous optimization. An iBPMS enables citizen developers — most commonly business analysts — and professional developers to collaborate on iterative development and improvement of process and decision models.

These technologies are highly complementary, and Gartner increasingly sees them deployed side by side.

iBPMS platforms can choreograph complex styles of work — for example, adaptive case management or processes driven by complex events.[6] This is increasingly important, particularly in the context of digitalized processes that coordinate the behaviors of people, processes and the "things" that are part of the Internet of Things. The rapidly changing operational context in a digitalized process requires actionable, advanced analytics to more-intelligently orchestrate business processes across the virtual and physical worlds.

A key thing to recognize is that the organization is becoming more model-driven, and the ability to manage the interconnected nature and complex versioning of these models is an important competency. To derive the full benefits of hyperautomation, organizations need an overarching view across their functional and process silos. Indeed, developing more and more sophisticated models is akin to developing a digital twin of an organization (DTO).

The Digital Twin of an Organization

A digital twin of an organization visualizes the interdependence between functions, processes and key performance indicators (KPIs). A DTO is a dynamic set of software models of a part of an organization. It relies on operational and/or other data to understand and provide continuous intelligence on how an organization operationalizes its business model connected directly to its current state and deployed resources. Critically, a DTO responds to changes in how expected customer value is delivered.

A DTO draws from a real-world environment with real people and machines working together to generate continuous intelligence about what is happening throughout the organization. Effectively, a

DTO provides a contextual framework for business process and decision models. It helps capture where enterprise value links to the different parts of an organization and how its business processes impact value creation. As such, the DTO becomes an important element for hyperautomation. A DTO allows users to model and explore scenarios, choose one, and then make it real in the physical world.[7]

Machine Learning and NLP Explode the Range of Hyperautomation Possibilities

AI techniques in various forms, including machine learning and natural language processing (NLP), have rapidly expanded hyperautomation possibilities. Adding the ability to interpret human speech quickly at runtime, identify patterns in documents or data, and/or dynamically optimize business outcomes dramatically alters the range of automation possibilities. Indeed, when combined with RPA- and iBPMS-related products, they are starting to affect many industries and enable the automation of what was once deemed the exclusive domain of knowledge workers. But, rather than replacing those workers, AI technologies are mostly augmenting their ability to deliver value. These AI technologies have created a mini arms race as vendors attempt to leapfrog each other. AI technologies have:

- **Improved machine vision functionality in most RPA tools.** Indeed, machine learning has enabled a major step forward in RPA through a type of computer vision. For example, it can recognize a "Submit" button and virtually press it, regardless of where it might appear on the screen. This has been extended to identifying all the text on screen (just like optical character recognition [OCR]). Taking this a step further, tools are emerging that can separate the labels on an image from the dynamically populated text fields. This innovation then enables the RPA tool to interact with image-based interfaces as though they were directly accessed applications.
- **Optimized business KPIs.** An iBPMS or RPA tool can easily call a machine learning model or NLP functionality directly from within the short-term task or longer-running business process. Increasingly, machine learning and NLP are being directly embedded into iBPMS tools with preintegrated functionality making it easier to do the associated data science (plug-and-play machine learning) or call external services from the mega cloud vendors such as Amazon, Google, IBM and Microsoft.
- **Appeared in a plethora of adjacent and supporting technologies.** These include advanced OCR and intelligent character recognition (ICR) to interpret handwriting. NLP is enabling more and more self-service automation as customers interact directly with chatbots and virtual personal assistants (VPAs).
- **Automated processes discovery.** Machine learning is enabling vendors to discover working practices and their different variants in the workplace. Task mining tools, sometimes referred to as "process discovery," help organizations achieve deep insight into their task flows to get the microview of the task steps or activities that could then be automated by RPA or an iBPMS.[8]

The addition of machine learning and NLP to RPA and iBPMS tools provides the ability to industrialize the digital customer and employee experience by connecting those interactions directly to automated back-office operations and supplier ecosystems. Moreover, this enables a contextually aware, situationally adaptive approach — where the set and order of interactions

among participants are uniquely choreographed based on the goals of the business, its partners, and its customers, and on operations intelligence that continuously updates and analyzes in real time. An iBPMS can proactively personalize contextually aware interactions at scale while supporting rapid transformation and/or improvement of the customer and employee journey. Furthermore, AI supports an iBPMS in automating and orchestrating business processes that shape themselves as they run. These processes can therefore be considered adaptive and intelligent, executing the best, next action instead of the same repeatable sequence of actions.

Related Research:

- "Navigate Optimal Routes for Process Automation With RPA, iBPMS and iPaaS"
- "Market Guide for Technologies Supporting a DTO"
- "Develop 3 Levels of Service for Your Center of Expertise to Scale DigitalOps and Robotic Process Automation"
- "Artificial Intelligence Trends: Process Augmentation"
- "The State of RPA Implementation"
- "Best Practices for Robotic Process Automation Success"
- "Create a Digital Twin of Your Organization to Optimize Your Digital Transformation Program"
- "Comparing Digital Process Automation Technologies Including RPA, BPM and Low-Code"

Trend No. 2: Multiexperience

Through 2028, the user experience will undergo a significant shift in how users perceive the digital world and how they interact with it. Conversational platforms are changing the way in which people *interact* with the digital world. Virtual reality (VR), augmented reality (AR) and mixed reality (MR) are changing the way in which people *perceive* the digital world. This combined shift in both perception and interaction models leads to the future multisensory and multitouchpoint experience.

> The model will shift from one of technology-literate people to one of people-literate technology. The burden of translating intent will move from the user to the computer.

The ability to communicate with users across many human senses will provide a richer environment for delivering nuanced information.

The "computer" in a multiexperience world is the environment around the user, including many touchpoints and sensory inputs. The multitouchpoint aspect of the experience will connect people across edge devices, including traditional computing devices, wearables, automobiles, environmental sensors and consumer appliances.[9] The multisensory aspect of the experience will use all human senses as well as advanced computer senses (such as heat, humidity and radar) as

appropriate across this rich sea of devices. In the future, the very notion of “computer” will seem like a quaint and antiquated idea as the spaces that we inhabit become multisensory and multitouchpoint interfaces.

The long-term manifestation of multiexperience is also called the ambient experience. However, this will happen only slowly through 2029 and beyond. Privacy concerns in particular may dampen the enthusiasm and impact of adoption. On the technical front, long life cycles of many consumer devices, and the complexity of having many creators developing elements independently, will be an enormous barrier to seamless integration. Don’t expect automatic plug and play of devices, applications and services. Instead, there will be proprietary ecosystems of devices in the near term.

Focus on targeted use of immersive experiences and conversational platforms for highly specific scenarios as they evolve through 2024. These experiences and platforms will overlap with one another, incorporating a full array of sensory input/output channels delivered in various device scenarios. These may be targeted experiences on specific devices, but opportunities will grow for more robust scenarios across multiple devices and sensory channels to support specific environments (e.g., an ambient experience in a manufacturing plant). Complement these targeted solutions with an evolving multiexperience development platform that incorporates more sensory channels and more device targets well beyond the web and mobile targets of more traditional development platforms.

Immersive Experiences

Immersive experience is constructed using a variety of techniques and software tools, including AR, VR, MR, multichannel human-machine interface (HMI) and sensing technology. Immersive experience is distinguished from other experience methods by its ability to simulate realistic scenarios and environments that give users the visualization and the actionable information to practice operations and to interact with virtual people or objects. These experiences include a wider range of immersions from simple AR overlays on a smartphone to fully immersive virtual reality environments.

VR provides a 3D environment that surrounds a user and responds to an individual’s actions in a natural way. This may be through an immersive head-mounted display (HMD) that blocks the user’s entire field of vision. HMDs enrich the immersive experience by blending the digital and the physical. But the current-generation product has many constraints, including heavy power consumption, clumsy designs, awkward UI, latency and limited field of view.

Smartphones can also be an effective platform for mobile VR and AR. Accessories exist to turn smartphones into HMDs. But an HMD configuration is not vital to experience AR — AR can combine digital overlays on a real-world video experience. The smartphone’s screen becomes a “magic window” that displays graphics overlaid on top of real-world things. AR superimposes contextual information that blends augmented data on top of real-world objects (such as hidden wiring superimposed on an image of a wall). Although this approach has limitations compared with HMD-based approaches, it represents a widely available, easy-to-use and cost-effective entry point for AR.

The visual aspect of the experience is important, with imaging sensors capturing traits of the physical world allowing systems to render and overlay virtual objects onto this real world. However, other sensory models, such as touch (haptic feedback) and sound (spatial audio) are often important as well. This is particularly so with AR/MR in which the user may interact with digital and real-world objects while maintaining a presence in the physical world. Gesture and posture recognition provide hand and body tracking, and touch-sensitive feedback may be incorporated. The emerging AR cloud will make integration of AR/VR/MR experiences richer by providing a standardized spatial map of the real world.[10]

Although the potential of VR, AR and MR is impressive, there will be many challenges and roadblocks. Identify key target personas and explore targeted scenarios. For example, explore the needs of, and business value for, a target user in different settings, such as at home, in a car, at work, or with a customer. By 2022, 70% of enterprises will be experimenting with immersive technologies for consumer and enterprise use, and 25% will have deployed them to production. Three use cases show clear value:[11]

- **Product design and visualization.** This can be an internal-facing or external-facing use case. Immersive experience technologies enable designers and customers to conceptualize, design, explore and evaluate products virtually, without the need for physical prototypes, while taking into consideration the users' constraints and environment. This use delivers improved R&D collaboration across teams, shorter product development cycles and better product designs through simulations. This use case is prevalent in real estate and automotive development, although it can be applied to products of all kinds.
- **Field service and operations.** This is a remote and AR-/MR-based use case. Immersive experience technologies support frontline workers completing their tasks on-site, providing augmentation to improve efficiency. To date, this use case has been mainly for maintenance and repair, parts visualization and visual guidance. By 2023, two out of three large field service organizations will equip field technicians with immersive applications to improve efficiency and customer satisfaction, up from less than 1% in 2019.
- **Training and simulation.** This is an internal-facing, indoor and VR-based use case. It helps employees to learn new, or improve existing, skills.[12] It enables more flexible, efficient and self-service training, and the use of role-play training for first responders and other frontline-facing scenarios. This use case includes training for mission-critical tasks and advanced operational skills. By 2022, 35% of large businesses in the training and simulation industry will evaluate and adopt immersive solutions, up from less than 1% in 2019.

The Language Factor

A conversational platform provides a high-level design model and execution engine in which user and machine interactions occur. As with immersive experience, other input/output (I/O) mechanisms will be added to exploit sight, taste, smell and touch for a multisensory interaction. This is already happening with both Google and Amazon adding screens and cameras to their smart speakers. The use of expanded sensory channels will support capabilities, such as emotion detection through facial expression analysis or analyzing data from accelerometers to identify abnormal movements

that may indicate a health condition. But exploitation of these other sensory channels will be isolated and limited through 2023.

Conversational platforms have reached a tipping point: The usefulness of the systems has exceeded the friction of using them. But they still fall short. Friction is created when users need to know which domains the UI understands and what its capabilities are within those domains. A key challenge that conversational platforms face is that users must communicate in a very structured way. This is often a frustrating experience. Rather than enabling a robust two-way conversation between the person and the computer, most conversational platforms are mainly one-directional query or control systems that produce a very simple response. This is beginning to change as vendors work to create a more natural conversational flow.

Over time, more conversational platforms will integrate with growing ecosystems of third-party services that will exponentially drive the usefulness of these systems. Primary differentiators among conversational platforms will be the robustness of their conversational models and the API and event models used to access, invoke and orchestrate third-party services to deliver complex outcomes.

The Multiexperience Development Platform

A multiexperience development platform (MXDP) offers front-end development tools and back-end services that enable rapid, scalable development of seamless, targeted and ambient experiences across devices, modalities, and touchpoints. The design time and runtime tools and services are delivered via a unified development platform that has loosely coupled front- and back-end architectures.

MXDPs are not “build once, run everywhere” or “omnichannel” solutions.

> The core value of an MXDP lies in its ability to coalesce software development life cycle activities across a range of apps to address the digital user journey. The need for this ability will only increase as the number of apps, devices and modes of interaction increases.

The best practice for providing an optimized experience is to build connected, fit-for-purpose apps that align the design, function and capabilities of the app to individual personas and modalities. Unlike a one-size-fits-all application experience that attempts to support every feature that every type of user wants from the software, fit-for-purpose apps focus in on the customer moments or steps in the journey that users perform to attain a goal or outcome. This approach provides the opportunity to create smaller purpose-built apps that are easier to design, develop and deploy. This approach also allows the app to be focused on whatever touchpoint the user prefers when performing tasks, whether it’s a web-based app running on a laptop, a mobile app on a phone or a conversational interface.

An effortless experience should ensure that a particular persona has a consistent experience when moving from one device to another or using multiple devices simultaneously in a more ambient experience. Multiexperience design requires the back end to be flexible enough to support the different capabilities and workflows of every app. Because users don't always use the same devices, and often switch from one device to another during their working day, the back end must offer a continuous experience.[13]

Related Research:

- "Market Guide for Conversational Platforms"
- "3 Immersive Experience Use Cases That Provide Attractive Market Opportunities"
- "Survey Analysis: Insights to Kick-Start an Enterprise Multiexperience Development Strategy"
- "Critical Capabilities for Multiexperience Development Platforms"
- "Magic Quadrant for Multiexperience Development Platforms"
- "Architecting and Integrating Chatbots and Conversational Platforms"
- "Market Guide for Augmented Reality"
- "Architecture of Conversational Platforms"

Trend No. 3: Democratization

Democratization is focused on providing people with access to technical expertise (e.g., ML, application development) or business domain expertise (e.g., sales process, economic analysis) via a radically simplified experience and without requiring extensive and costly training. The notion of "citizen access" (e.g., citizen data scientists, citizen integrators) as well as the evolution of citizen development and no-code models are examples of democratization. Development of expert systems or virtual assistants based on AI and decision models is another important aspect of democratization.[14] These systems provide advice or take actions on behalf of people to extend their knowledge or expertise beyond their experience or training.

It is important to note that the target for the democratization trend could be any person inside or outside the enterprise including customers, business partners, corporate executives, salespeople, assembly line workers, professional application developers, and IT operations professionals. There are four key aspects to the democratization trend that are accelerating in 2020 through 2023:

- **Democratization of Application Development.** AI PaaS provides access to sophisticated AI tools to leverage custom-developed applications. These solutions provide AI-model-building tools, APIs and associated middleware that enable the building/training, deployment and consumption of machine learning models running on prebuilt infrastructure-as-cloud services. These cover vision, voice, and general data classification and prediction models of any type.
- **Democratization of Data and Analytics.** The tools used to build AI-powered solutions are expanding from tools targeting data scientists (AI infrastructure, AI frameworks and AI

platforms) to tools targeting the professional developer community (AI platforms and AI services) and the citizen data scientist. This includes tools to generate synthetic training data, which helps address a substantial barrier to ML model development.[15]

- **Democratization of Design.** In addition, low-code application development platform tools used to build AI-powered solutions are themselves being empowered with AI-driven capabilities that assist professional developers and automate tasks related to the development of AI-enhanced solutions. This expands on the low-code, no-code phenomenon with automation of additional application development functions to empower the citizen developer.
- **Democratization of Knowledge.** Non-IT professionals increasingly have access to powerful tools and expert systems that empower them to exploit and apply specialized skills beyond their own expertise and training. Dealing with the issues around "shadow AI" in this user-led environment will be a challenge.

Democratization of Application Development

The market is rapidly shifting from one in which professional data scientists must partner with application developers to create most AI-enhanced solutions to one in which professional developers can operate alone using predefined models delivered as a service. This provides the developer with an ecosystem of AI models, as well as easy-to-configure development tools tailored to integrating AI capabilities and models into a solution.

Some AI PaaS services are complete models that a developer can simply call as a function, pass the appropriate parameters and data, and obtain a result. Others may be pretrained to a high level but require some additional data to customize the models. For example, a model may be pretrained for image recognition but requires a training dataset to recognize a particular set of images. The advantage of these partially trained models is that they require much smaller datasets of relevant enterprise data for refined training.

> Not only does the evolution of these AI platforms and suites of AI services enable a wider range of developers to deliver AI-enhanced solutions, but it also delivers much higher developer productivity.

This reduces waste and inefficiency in the development life cycle of AI projects. The pretrained models can be accessed via API calls or event triggers.

Application teams must determine which AI services to use from external providers. Next, define an architecture for how the organization's data science teams will develop custom domain and company-specific AI services as part of the AI service ecosystem. This will make the cloud service provider decision even more complex, as it requires the selection of the underlying platforms, frameworks and infrastructure to build, train and deploy these models. We expect increasing demand to lead to standardization of the deployment of these custom models across multiple environments.

Low-Code, No-Code and the Citizen Developer

Low-code application development is not new, but a confluence of digital disruptions has led to an influx of tools to meet rising demand for rapid application development platforms. There is a wide range of vendors providing these solutions,[16] spanning simple forms creation to full stack application platforms. Low-code development offerings are part of this tool spectrum as well and are primarily targeted at enabling citizen developers in the lines of business. By 2024, low-code application development will be responsible for more than 65% of application development activity. Also, by 2024, 75% of large enterprises will be using at least four low-code development tools for both IT application development and citizen development initiatives.

Another level of democratization occurs as AI is applied to automate various application development and testing functions. Through 2020, assisted development and testing will emerge to simplify these functions. By 2022, we expect more mainstream use of virtual software engineers to generate code. Google's AutoML is one example of how augmented analytics will enable developers to automatically generate new models without the involvement of a professional data scientist. By 2022, at least 40% of new application development projects will have artificial intelligence co-developers on the team.

> Ultimately, highly advanced AI-powered development environments automating both functional and nonfunctional aspects of applications will give rise to a new age of the "citizen application developer."

In this new age, nonprofessionals will be able to use AI-driven tools to automatically generate new solutions. We expect that AI-powered systems will drive a new level of flexibility. They will enable nonprofessionals to rapidly create much more dynamic, open and complex solutions.

Augmented Analytics and the Citizen Data Scientist

Augmented analytics uses ML- and AI-assisted data preparation, insight generation, and insight explanation to allow businesspeople to act as "citizen data scientists" exploring and analyzing data without the assistance of professional data scientists. It democratizes analytics and AI in three key ways:

- **Augmented data generation and preparation,** which uses ML automation to augment data creation, profiling, quality, harmonization, modeling, manipulation, enrichment, cataloging and metadata development. This is also transforming all aspects of data management, including automating data integration and database and data lake administration.
- **Augmented analytics as part of analytics and business intelligence (BI),** which enables business users and citizen data scientists to automatically discover, visualize and narrate relevant findings without building models or writing algorithms. These findings may include

correlations, exceptions, clusters, segments, outliers and predictions. Users explore data via autogenerated visualizations and conversational interfaces.

- **Augmented analytics uses ML to automate aspects of data science and AI modeling,** such as feature engineering, automated machine learning (autoML) for model selection, model operationalization, model explanation and, ultimately, model tuning and management. This reduces the need for specialized skills to generate, operationalize and manage models.

Organizations can use citizen data scientists or semitrained business experts to fill the data science and ML talent gap. By 2021, automation of data science tasks will enable citizen data scientists to produce a higher volume of advanced analysis than specialized data scientists. Gartner predicts that, by 2021, augmented analytics will be a dominant driver of new purchases of analytics and BI — as well as data science and machine learning — platforms, and of embedded analytics. We also expect that, by 2025, a scarcity of data scientists will no longer hinder the adoption of data science and machine learning in organizations. Organizations increasingly augment and outsource data science work.

Augmented analytics will also be a key feature of analytics embedded in autonomous things that interact with users — especially autonomous assistants using conversational interfaces. This emerging way of working enables businesspeople to generate queries, explore data, and receive and act on insights in natural language (voice or text) via mobile devices and personal assistants. However, this is only the initial use of augmented analytics in autonomous things. Augmented analytics enables the embedding of an augmented data science function in any type of autonomous thing. When the autonomous thing requires analytics to operate, it can tap into the embedded augmented analytics function to respond.

In a typical analytics scenario, people often default to exploring their own biased hypotheses, missing key findings and drawing their own incorrect or incomplete conclusions. This may adversely affect decisions and outcomes. Augmented analytics enables the exploration of more hypotheses and the identification of hidden patterns. It also removes personal bias. However, AI algorithms are not inherently unbiased, and care must be taken not to inadvertently introduce new biases through limited training sets.[17]

Dealing With Shadow AI

Shadow AI refers to a natural consequence of democratization where individuals without formal training exploit easy-to-use tools to develop their own AI-powered solutions and provide peer-to-peer support to others in similar efforts. Like “shadow IT” where business users bring their own consumer technologies to work or create their own spreadsheet or analytical models with BI tools, “shadow AI” has both a positive and a negative side. Democratization opens up new opportunities for the citizen data scientist, integrator and developer. Business users can dynamically create powerful AI-powered models and analytics with increasingly easy-to-use tools. While this can be a productivity bonanza and enable the business to more-rapidly adapt and drive new business opportunities, there is also a challenge with unleashing these powerful tools on an untrained audience.

Shadow AI takes “bring your own” to a more granular level by allowing “bring your own data” and “bring your own algorithm” outside the ownership, control or stewardship of IT. Shadow AI is not an inherently bad thing as long as practices and training are in place. By 2022, 30% of organizations using AI for decision making will contend with shadow AI as the biggest risk to effective and ethical decisions.

Related Research:

- “Predicts 2019: The Democratization of AI”
- “Low-Code Development Technologies Evaluation Guide”
- “Four Real-World Case Studies: Implement Augmented DSML to Enable Expert and Citizen Data Scientists”
- “Innovation Insight for AI-Augmented Development”
- “Augmented Analytics Feature Definition Framework”
- “Top 10 Data and Analytics Technology Trends That Will Change Your Business”
- “How to Enable Self-Service Analytics”
- “Predicts 2019: Democratization of IT Requires Different Strategies for Integration”

Trend No. 4: Human Augmentation

Human augmentation refers to the enhancement of human capabilities and capacity through the use of technology and science. Humans have always used technology and science in this fashion. Even before the introduction of the computer, technologies such as the typewriter, copy machine and printing press augmented the human ability to create, copy and publish text. Glasses, hearing aids and false teeth are all historical examples of human augmentation.

The computer era has added new dimensions to human augmentation. Word processing, desktop publishing, webpages, blogs and social media greatly extend our ability to create and publish text. With the rise of new technologies such as IoT, AI, smart speakers and VR emerging from computer science, and technologies such as CRISPR[18] emerging from biological science, entirely new opportunities for human augmentation are emerging.

Human augmentation explores how technology can be used to deliver cognitive and physical improvements as an integral part of the human experience. Instead of computers and applications being something outside the normal human experience, they become a natural — and sometimes necessary — part of the day-to-day human experience. Moreover, human augmentation also includes bioengineering factors that go beyond exploitation of computers and applications. We are already on this path to a certain extent. For many people, smartphones are an essential tool and constant companion. Social networks and electronic connections like email have become a primary link between people. Pharmaceuticals have augmented humans since well before the advent of computers. Human augmentation is a prime example of combinatorial innovation which brings together many trends including:

- Hyperautomation and the development of expert systems to democratize access to skills beyond current experience and training.
- Empowered edge devices and autonomous things, which exist in spaces around humans and augment their capabilities.

Cognitive and Physical Augmentation

Human augmentation impacts how we move, perceive, and interact in both physical and digital spaces, as well as how we process, analyze and store information. Augmentation can be broadly categorized into physical and cognitive categories, although the boundaries between them will blur over time.

Physical augmentation enhances humans by changing their inherent physical capabilities by implanting or hosting a technology element on their bodies. Automotive, mining, oil and gas, and other industries are using wearables to improve worker safety. Wearables are also driving workplace productivity in industries like retail, travel and healthcare. Physical augmentation also includes using biology or other means to alter the human body. In some cases, physical augmentation replaces a human capability that an individual has lost (e.g., a prosthetic leg); but, in some cases, those replacement capabilities may surpass natural human abilities. Physical augmentation can be considered along a number of dimensions:

- **Sensory Augmentation —** Hearing, vision and other augmentation devices or implants to improve perception. Virtual, augmented and mixed reality are a current example of sensory augmentation. In the emerging technology space, various companies are experimenting with smart contact lenses to detect glucose levels in tears and intraocular pressure.[19] Researchers are also experimenting with developing an "electronic nose" that mimics a human nose.[20]
- **Appendage and Biological Function Augmentation —** Use of exoskeletons and prosthetics to replace or enhance these capabilities is an expanded area of human augmentation. Surgical augmentation of the eyes has been popular with professional golfers.[21] Cochlear implants can replace nonfunctioning auditory nerves, and a similar technology has been used to replicate eyes. The cosmetics industry leads in enhancing nails, hair, eyes and the shape of body parts using passive implants. Arguably, the pharmaceutical industry has been augmenting human biological functions for years. Nootropics refers to the use of natural or synthetic substances that may improve mental skills, although the use of such substances outside of treatment for a specific medical condition is highly controversial.
- **Brain Augmentation —** Implants such as a vagus nerve stimulator to treat seizures currently exist.[22] Brain implants are being explored for a variety of uses including memory storage[23] and brain implants to decode neural patterns and synthesize speech.[24] Neuralink is trying to develop a brain implant that would connect the human brain to computer networks.[25]
- **Genetic Augmentation —** Somatic gene and cell therapies are used today and seen as morally acceptable. For example, gene therapy to treat children with severe combined immune deficiency is an accepted treatment. In the future, easy access to and the low cost of CRISPR technologies may enable broad genetic engineering, although the ethical issues are significant.[26]

Cognition is the process by which humans acquire knowledge through sensory input, life experiences, learning, and thinking about that input, experience and education. Cognitive skills are used to understand, process, remember, and apply information to make decisions and take actions. Cognitive augmentation enhances a human's ability to think and make better decisions. Cognitive augmentation can occur through accessing information and exploiting applications on traditional computer systems and the emerging multiexperience interface in smart spaces. This includes augmented intelligence scenarios, where humans and artificial intelligence work together to enhance cognitive performance, including decision making and learning. In addition, physical augmentation that enhances human senses or brain capacity or capability feed into new models for cognitive augmentation. This includes the use of smart drugs and brain implants to store memories.[23]

> Human augmentation offers the opportunity to achieve digital transformation through human transformation.

Wearables are an example of physical augmentations today. As the maturity and adoption of wearables increase, consumers and employees will begin looking at other physical augmentations to enhance their personal lives (i.e., health and fitness) or to do their jobs more efficiently (i.e., exoskeletons and implants). Over the next 10 years, increasing levels of physical and cognitive human augmentation will become prevalent as individuals seek personal enhancements. This in turn will create a new "consumerization" effect where employees seek to exploit their personal enhancements — and even extend them — to improve their office environment. Through 2023, 30% of IT organizations will extend BYOD policies with "bring your own enhancement" to address augmented humans in the workforce.

Cultural and Ethical Aspects of Human Augmentation

Human augmentation will be a primary means by which individuals interact with each other and with the smart spaces that surround them. Business leaders and IT leaders should plan for how their organizations will adopt, exploit and adapt to the coming changes. As consumers and employees integrate more of their lives into one intelligence-amplifying human augmentation, organizations will have to address issues of data transparency, privacy and autonomy.[27]

When choosing human augmentation technologies and methodologies, enterprises must examine five major areas:

- **Security.** Human augmentation technologies must achieve and maintain a known and acceptable state of security-related risk. This risk is across an attack surface that's no longer tied to a specific device or physical location, but may travel with the human subject.
- **Privacy.** Human augmentation provides the ability to access intimate knowledge and data about the human it's enhancing. That data must be protected.
- **Compliance.** Government and regulatory agencies are issuing regulations and providing compliance requirements on a frequent basis, which makes compliance extremely complex for

global enterprises, especially because agencies are still trying to grasp the implications of human augmentation technologies.

- **Health impact.** Human augmentation has the potential for long-term mental and physical implications that may not be immediately understood.
- **Ethics.** Implementing human augmentation technologies and processes poses serious ethical issues. These include ethical considerations and assessments for determining specific vulnerabilities, risks and moral issues. For example, does the digital divide widen as affluent individuals can augment themselves and their children while less affluent people cannot? Answers to these societal issues will become increasingly important.

Enterprises of all types and sizes are considering human augmentation to achieve various business outcomes through multiple business use cases with different time horizons. Consequently, they must consider the lessons, recommendations and principles of human experimentation as they intentionally begin to exploit human augmentation capabilities for human transformation. Enterprises should strike a balance between two classic ethical principles — precautionary and proactionary — and adopt what Gartner calls the "cautionary principle":

- The **precautionary principle** states that "if an action or policy might cause severe or irreversible harm to the public or to the environment, in the absence of a scientific consensus that harm would not ensue, the burden of proof falls on those who would take the action."[28]
- The **proactionary principle** was formulated by Max More and is a key tenet of the "transhumanism" movement. It presents several imperatives when imposing restrictive measures: "Assess risks and opportunities according to available science, not popular perception. Account for both the costs of the restrictions themselves, and those of opportunities foregone. Favor measures that are proportionate to the probability and magnitude of impacts, and that have a high expectation value. Protect people's freedom to experiment, innovate, and progress."[29]
- The **cautionary principle** balances between precautionary and proactionary. It recommends that organizations move forward with innovation, but only in a way that does not risk the individual, company or environment as a whole.

Related Research:

- "Maverick* Research: Architecting Humans for Digital Transformation"
- "Emerging Technology Analysis: Smart Wearables"
- "Technology Investments for Frontline Workers Will Drive Real Business Benefits"
- "Hype Cycle for Emerging Technologies, 2019"
- "Market Insight: Increase User Engagement for Voice-Enabled Virtual Assistants Through a More Targeted User Experience"

Trend No. 5: Transparency and Traceability

Digital ethics and privacy are growing concerns for individuals, organizations and governments. Consumers are increasingly aware their personal information is valuable and are demanding control. Organizations recognize the increasing risk of securing and managing personal data, and governments are implementing strict legislation to ensure they do.

Artificial Intelligence and the use of ML models to make autonomous decisions raises a new level of concern, with digital ethics driving the need for explainable AI and the assurance that the AI system is operating in an ethical and fair manner. Transparency and traceability are critical elements to support these digital ethics and privacy needs.

Transparency and traceability are not a single product or a single action. It refers to a range of attitudes, actions, and supporting technologies and practices designed to address regulatory requirements, enshrine an ethical approach to use of AI and other advanced technologies, and repair the growing lack of trust in companies.

Transparency and traceability require a focus on six key elements of trust:

- **Ethics —** Does the organization have strong moral principles on the use of personal data, algorithms and the design of systems that go beyond regulations and are transparent to all interested parties?
- **Integrity —** Does the organization have a proven track record of designing systems that reduce or eliminate bias and inappropriate use of personal data?
- **Openness —** Are the ethical principles and privacy commitments clear and easily accessible — and do changes to such policies bring the appropriate constituencies into the decision-making process?
- **Accountability —** Are there mechanisms for testing, assurance and auditability such that privacy or ethical concerns can be identified and addressed? This applies not only to adherence to regulatory requirements, but also to new ethical or privacy concerns that arise from future technologies.
- **Competence —** Has the organization implemented design principles, processes, testing and training so that concerned constituencies can feel comfortable that the organization can execute on its promises?
- **Consistency —** Are policies and processes handled consistently?

Explainable and Ethical AI and Algorithms

Algorithmic decisions drive everything organizations and consumers do: recruiting, buying products and services, what content they see on the web, being accepted or rejected for loans, even going to jail.[30] Biased or incorrect algorithms promote bad business decisions and risk serious backlash from employees, investors and customers. They could potentially even cause serious harm and result in corporations facing criminal penalties. Legal risks include gender and racial bias and other forms of

discriminatory activities. Lack of explainability or an inability to prove lack of bias means business activities can't be justified in public or in court.

Opaque algorithms (deep neural networks [DNNs], for example) incorporate many implicit, highly variable interactions into their predictions that can be difficult to interpret. Bias in AI raises concerns of accountability and fairness. Consequently, the AI community and enterprise leaders are concerned with detecting and explaining the consequences of bias that might endanger society and the business. For example, bias in AI causes polarization of political opinions, persistence of discredited beliefs and false associations between business moments.

Explainable AI is the set of capabilities that describes a model, highlights its strengths and weaknesses, predicts its likely behavior, and identifies any potential biases. It can articulate the decisions of a descriptive, predictive or prescriptive model to enable accuracy, fairness, accountability, stability and transparency in algorithmic decision making. Explainable AI provides the technical foundation to support AI governance. AI governance is the process of assigning and assuring organizational accountability, decision rights, risks, policies and investment decisions for applying AI, predictive models and algorithms.

Augmented analytics solutions with explainable AI features are not only showing data scientists the input and output of a model, but are also explaining why the system selected particular models and what are the techniques applied by augmented data science and ML. Without acceptable explanation, autogenerated insights and models, or black boxes combined with AI bias, can cause concerns about regulation, reputation, accountability and fairness, and lead to distrust in AI solutions.

Transparency and traceability are something that enterprises need to embrace themselves, but they will become increasingly important aspects of how organizations evaluate the packaged applications and services they purchase using AI. By 2025, 30% of government and large-enterprise contracts for purchase of digital products and services using AI will require the use of explainable and ethical AI.

Data Privacy, Ownership and Control

People are increasingly concerned about how their personal information is being used by organizations in both the public and private sector; and the backlash will only increase for organizations that are not proactively addressing these concerns.

While the private sector is increasingly bound by privacy legislation, law enforcement and security services have far fewer controls. Police services use facial recognition to identify people of interest. They use automatic number plate recognition (ANPR) to track vehicles of interest. They also use data from fitness trackers to establish people's location and heart rate at the time of a crime.[31] They've even used Face ID to unlock a suspect's phone.[32] With billions of endpoints collecting information, law enforcement can identify who you are, where you are, what you're doing and even what you're thinking.

> Any discussion on privacy must be grounded in the broader topic of digital ethics and the trust of your customers, constituents and employees. While privacy and security are foundational components in building trust, trust is actually about more than just these components.

As defined by Oxford Dictionaries, trust is a firm belief in the reliability, truth or ability of someone or something. Trust is often seen as the acceptance of the truth of a statement without evidence or investigation; but, in reality, trust is typically earned from demonstrable actions over time and not provided blindly.

Ultimately an organization's position on privacy must be driven by its broader position and actions on ethics and trust. Shifting from privacy to ethics moves the conversation beyond "are we compliant?" toward "are we doing the right thing?" and "are we showing that we are trying to do the right thing?" The move from compliance-driven organizations to ethics-driven organizations can be described as the hierarchy of intent.[33]

People are justifiably concerned about the use of their personal data and are starting to fight back. Misguided personalization attempts, media coverage and lawsuits have made one thing clear to customers: Their data is valuable. And so, they want to take back control. Customers may opt out of services, pay in cash or bitcoin, use VPNs to mask their location, provide false information or simply fade out of the relationship.

Right to be forgotten (RTBF) legislation exists in many jurisdictions including Europe, South Africa, South Korea and China. The right to data portability empowers customers to more easily take their personal data — and business — elsewhere. The highly valuable personal information that organizations have spent a decade to effectively leverage is disappearing. Failure to incorporate privacy into a personalization strategy can bring unwanted results, such as customer churn, lack of loyalty and distrust, as well as brand reputational damage. In some cases, regulatory intervention could occur if customers feel their privacy is being threatened.

Companies that misuse personal data will lose the trust of their customers. Trustworthiness is a key factor in driving revenue and profitability. Building customer trust in an organization is difficult, but losing it is easy. However, organizations that gain and maintain the trust of their customers will thrive. We expect that companies that are digitally trustworthy will generate more online profit than those that aren't. However, not all of the transparency and trust elements can be easily automated. Greater human effort will be required to provide accountability, and points of contact for questions and to redress when things go wrong.

Best Practices and Regulations Are Emerging

The EU's General Data Protection Regulation (GDPR) redefines the ground rules for privacy and has had a global impact. It allows for fines of up to 4% of annual global revenue or €20 million, whichever is highest. We expect that, before year-end 2021, more than a billion euros in sanctions for GDPR noncompliance will have been issued. Many other nations are in the process of developing or implementing privacy legislation, and this evolving patchwork of privacy laws around the world will continue to challenge organizations in the way they interact with customers, citizens and employees.

Legislation is also driving data residency issues in jurisdictions including China, Russia, Germany and South Korea. Organizations must assess the data residency requirements of the countries in which they operate to determine a data residency strategy. Local data centers are an option, but often an expensive one; and, in many cases, there are legal and logical controls available under which safe cross-border transfers of personal data can be possible. Cloud service providers are locating data centers in countries where data residency is either driven by legislation or by customer preferences.

Explainable and ethical AI is becoming a political and regulatory issue. The U.K. government Centre for Data Ethics and Innovation has started a review of algorithmic bias in financial services industry. U.S. politicians are proposing regulations as well.

Implementing the principles of "privacy by design" positions your products and services as more privacy-friendly than those of competitors. This creates a value proposition based on trust. A 2017 survey indicates 87% of consumers say they will take their business elsewhere if they don't trust that a company is handling their data responsibly.[34] Other standards groups such as the IEEE Standards Association have been building a variety of standards for ethical considerations in AI and autonomous systems as well as standards for personal data and AI agents.[35] Enterprises should track the advancement of these principles and adopt them as needed to demonstrate ethics, consistency and competency.

Related Research:

- "Top 10 Data and Analytics Technology Trends That Will Change Your Business"
- "Build Trust With Business Users by Moving Toward Explainable AI"
- "Hype Cycle for Artificial Intelligence, 2019"
- "Build AI-Specific Governance on Three Cornerstones: Trust, Transparency and Diversity"
- "Modern Privacy Regulations Could Sever or Strengthen Your Ties With Customers"
- "The CIO's Guide to Digital Ethics: Leading Your Enterprise in a Digital Society"
- "Use These Privacy Deliverables in Every IT Development Project"
- "Build for Privacy"
- "Hype Cycle for Privacy, 2019"

Trend No. 6: The Empowered Edge

Edge computing describes a computing topology in which information processing and content collection and delivery are placed closer to the sources, repositories and consumers of this information. Edge computing draws from the concepts of distributed processing. It tries to keep the traffic and processing local to reduce latency, exploit the capabilities of the edge and enable greater autonomy at the edge.

Much of the current focus on edge computing comes from the need for IoT systems to deliver disconnected or distributed capabilities into the embedded IoT world for specific industries such as manufacturing or retail. However, edge computing will come to be a dominant factor across virtually all industries and use cases as the edge is empowered with increasingly sophisticated and specialized compute resources and more data storage. Increasingly complex edge devices including robots, drones, autonomous vehicles and operational systems are accelerating this shift in focus.

The evolution of edge-oriented IoT architectures, with intelligence migrating toward endpoints, gateways and similar devices, is underway. However, today's edge architectures are still somewhat hierarchic, with information flowing through well-defined layers of endpoints to the near edge, sometimes the far edge and, eventually, centralized cloud and enterprise systems.

Over the long term, this neat set of layers will dissolve to create a more unstructured architecture consisting of a wide range of "things" and services connected in a dynamic flexible mesh linked by a set of distributed cloud services. In this scenario, a smart "thing," such as a drone, might communicate with an enterprise IoT platform, a government drone tracking service, local sensors and city-level local cloud services, and then conduct peer-to-peer exchanges with nearby drones for navigational purposes.

The edge, near edge and far edge connect to centralized data centers and cloud services. Edge computing solves many pressing issues, such as high bandwidth costs and unacceptable latency. The edge computing topology will enable the specifics of digital business and IT solutions uniquely well in the near future.

> The evolution of distributed cloud will increasingly provide a common or complementary set of services that can be centrally managed but delivered to the edge environment for execution.

Mesh architectures will enable more flexible, intelligent and responsive, and peer-to-peer IoT systems — although often at the cost of additional complexity. A mesh architecture is also a consequence of many distributed networked ecosystems. Fundamental shifts to digital business and products will have to exploit intelligent mesh architectures for competitive advantage. The evolution from centralized to edge to mesh will also have a major impact on product development and evolving teams' skills on both cloud and edge designs. Mesh standards are immature, although groups such as the IEEE and the OpenFog Consortium are working in the mesh architecture area.

As endpoints grow in number and become more sophisticated, AI-driven, and able to run operating systems such as Linux, mesh architectures will become more popular. New mesh architectures will introduce significant complexity into IoT systems and will likely make tasks such as designing, testing and support more challenging. In addition, the mesh often implies more peer-to-peer activities, which will involve partners and ecosystems stretching beyond individual products.

Through 2028, we expect a steady increase in the embedding of sensor, storage, compute and advanced AI capabilities in edge devices. However, the edge is a heterogeneous concept. It ranges from simple sensors and embedded edge devices to familiar edge computing devices, such as mobile phones, and highly sophisticated edge devices, such as autonomous vehicles. Different types of edge devices used in different scenarios can have very different life spans, ranging from one year to 40 years. These factors combined with the rapid push by vendors to drive more functionality into edge devices create a complex and ongoing management and integration challenge.

Intelligence will move to the edge across a spectrum of endpoint devices including:

- Simple embedded edge devices (e.g., appliances, industrial devices)
- Edge input/output devices (e.g., speakers, screens)
- Edge computing devices (e.g., smartphones, PCs)
- Complex embedded edge devices (e.g., automobiles, power generators)

These edge systems will connect with hyperscale back-end services directly or through intermediary edge servers or gateways (see Note 3).

Data, Analytics and AI at the Edge

By 2022, as a result of digital business projects, 75% of enterprise-generated data will be created and processed outside the traditional, centralized data center or cloud — an increase from the less than 10% generated today. This move toward distributed data forces organizations to strike a different balance between collecting data centrally for processing and connecting to the data where it is generated to perform local processing. Modern use cases demand that data management capabilities move toward the edge — bringing the processing to the data, rather than always collecting the data for centralized processing. But the distributed “connect” paradigm brings a lot of challenges with it. For example:

- If data persists at the edge, then in what form will it be stored?
- How will governance controls be enforced there?
- How will it be integrated with other data?

Data and analytics leaders need to modernize how data assets are described, organized, integrated, shared and governed to address these challenges.

Although not all aspects of data management will need to happen at the edge, modern use cases increasingly will push requirements in that direction (see “Technology Insight: Edge Computing in

Support of the Internet of Things"). The highly distributed nature of modern digital business applications, including architectures for IoT solutions, promises to challenge organizations' abilities to manage and process data at a level of scale and complexity for which most are unprepared. This shift to edge computing will have several impacts:[36]

- Data and analytics use cases and solutions require support for new distributed data architecture that is beyond data and analytics leaders' current data management capabilities.

  Include distributed data stores and processing in your data management to ensure you can offer support where data resides.

- Distributed data requires distributed data management capabilities, compelling data and analytics leaders to rebalance their ability to bring processing to data at the edge.

  Extend data persistence capabilities with cloud-based data stores, distributed parallel processing platforms and embedded database technology.

- Edge computing and other distributed environments will challenge data management technology provider capabilities, resulting in data and analytics leaders more closely scrutinizing how they navigate related technology markets.

  Assess incumbent and prospective vendors based on ability to process and govern distributed data.

Communicating to the Edge — The Role of 5G

Connecting edge devices with one another and with back-end services is a fundamental aspect of IoT and an enabler of smart spaces. 5G is the next-generation cellular standard after 4G Long Term Evolution (LTE; LTE Advanced [LTE-A] and LTE Advanced Pro [LTE-A Pro]). Several global standards bodies have defined it — International Telecommunication Union (ITU), 3rd Generation Partnership Project (3GPP) and ETSI. Successive iterations of the 5G standard also will incorporate support for NarrowBand Internet of Things (NB-IoT) aimed at devices with low-power and low-throughput requirements. New system architectures include core network slicing as well as edge computing.

5G addresses three key technology communication aspects, each of which supports distinct new services, and possibly new business models (such as latency as a service):

- Enhanced mobile broadband (eMBB), which most providers will probably implement first.
- Ultrareliable and low-latency communications (URLLC), which addresses many existing industrial, medical, drone and transportation requirements where reliability and latency requirements surpass bandwidth needs.
- Massive machine-type communications (mMTC), which addresses the scale requirements of IoT edge computing.

Use of higher cellular frequencies and massive capacity will require very dense deployments with higher frequency reuse. As a result, we expect that most public 5G deployments will initially focus on islands of deployment, without continuous national coverage. We expect that, by 2020, 4% of

network-based mobile communications service providers globally will launch the 5G network commercially. Many CSPs are uncertain about the nature of the use cases and business models that may drive 5G. We expect that, through 2022, organizations will use 5G mainly to support IoT communications, high-definition video and fixed wireless access. The release of unlicensed radio spectrum (Citizens Broadband Radio Service [CBRS] in the U.S., and similar initiatives in the U.K. and Germany) will facilitate the deployment of private 5G (and LTE) networks. This will enable enterprises to exploit the advantages of 5G technology without waiting for public networks to build out coverage.

Identify use cases that definitely require the high-end performance, low latency or higher densities of 5G for edge computing needs. Map the organization's planned exploitation of such use cases against the expected rollout by providers through 2023. Evaluate the available alternatives that may prove adequate and more cost-effective than 5G for particular IoT use cases. Examples include low-power wide-area (LPWA), such as 4G LTE-based NB-IoT or LTE Cat M1, LoRa, Sigfox and Wireless Smart Ubiquitous Networks (Wi-SUN).

Digital Twin of Things at the Edge

A digital twin is a digital representation of a real-world entity or system. The implementation of a digital twin is an encapsulated software object or model that mirrors a unique physical object (see Note 4). Data from multiple digital twins can be aggregated for a composite view across a number of real-world entities such as a power plant or a city.

Well-designed digital twins of assets could significantly improve enterprise decision making. They are linked to their real-world counterparts at the edge and are used to understand the state of the thing or system, respond to changes, improve operations and add value.

Organizations will implement digital twins simply at first and evolve them over time, improving their ability to collect and visualize the right data, apply the right analytics and rules, and respond effectively to business objectives. Digital-twin models will proliferate, with suppliers increasingly providing customers with these models as an integral part of their offerings.

Related Research:

- "The Future Shape of Edge Computing: Five Imperatives"
- "Ask These Four Questions About Enterprise 5G"
- "Digital Business Will Push Infrastructures to the Edge"
- "Five Approaches for Integrating IoT Digital Twins"
- "Why and How to Design Digital Twins"
- "The Technical Professional's Guide to Edge Infrastructure"
- "How Edge Computing Redefines Infrastructure"

Trend No. 7: Distributed Cloud

A distributed cloud refers to the distribution of public cloud services to different locations outside the cloud providers' data centers, while the originating public cloud provider assumes responsibility for the operation, governance, maintenance and updates. This represents a significant shift from the centralized model of most public cloud services and will lead to a new era in cloud computing.

Cloud computing is a style of computing in which elastically scalable IT-enabled capabilities are delivered as a service using internet technologies. Cloud computing has long been viewed as synonymous with a "centralized" service running in the provider's data center; although, private and hybrid cloud options emerged to complement this public cloud model. Private cloud refers to the creation of cloud-style services dedicated to individual companies often running in their own data centers. Hybrid cloud refers to the integration of private and public cloud services to support parallel, integrated or complementary tasks. The aim of the hybrid cloud was to blend external services from a provider and internal services running on-premises in an optimized, efficient and cost-effective manner.

Implementing a private cloud is hard. Most private cloud projects do not deliver the cloud outcomes and benefits organizations seek.[37] Also, most of the conversations Gartner has with clients about hybrid cloud are actually not about true hybrid cloud scenarios. Instead, they are about hybrid IT scenarios in which noncloud technologies are used in combination with public cloud services in a spectrum of cloud-like models. Hybrid IT and true hybrid cloud options can be valid approaches, and we recommend them for certain critical use cases. However, most hybrid cloud styles break many of the cloud computing value propositions, including:

- Shifting the responsibility and work of running hardware and software infrastructure to cloud providers
- Exploiting the economics of cloud elasticity (scaling up and down) from a large pool of shared resources
- Benefiting from the pace of innovation in sync with the public cloud providers
- Using the cost economics of global hyperscale services
- Using the skills of large cloud providers in securing and operating world-class services

Distributed Cloud Delivers on the Hybrid Cloud Promise

The location of the cloud services is a critical component of the distributed cloud computing model. Historically, location has not been relevant to cloud definitions, although issues related to it are important in many situations. With the arrival of the distributed cloud, location formally enters the definition of a style of cloud services. Location may be important for a variety of reasons, including data sovereignty and latency-sensitive use cases. In these scenarios, the distributed cloud service provides organizations with the capabilities of a public cloud service delivered in a location that meets their requirements.

In hyperscale public cloud implementations, the public cloud is the "center of the universe." However, cloud services have been distributed worldwide in the public cloud almost since its inception. The providers now have different regions around the world, all centrally controlled, managed and provided by the public cloud provider. The distributed cloud extends this model outside cloud-provider-owned data centers. In the distributed cloud, the originating public cloud provider is responsible for all aspects of cloud service architecture, delivery, operations, governance and updates. This restores cloud value propositions that are broken when customers are responsible for a part of the delivery, as is usually the case in hybrid cloud scenarios. The cloud provider does not need to own the hardware on which the distributed cloud service is installed. But in a full implementation of the distributed cloud model, the cloud provider must take full responsibility for how that hardware is managed and maintained.

We expect distributed cloud computing will happen in three phases:

- **Phase 1:** A like-for-like hybrid mode in which the cloud provider delivers services in a distributed fashion that mirror a subset of services in its centralized cloud for delivery in the enterprise.
- **Phase 2:** An extension of the like-for-like model in which the cloud provider teams with third parties to deliver a subset of its centralized cloud services to target communities through the third-party provider. An example is the delivery of services through a telecommunications provider to support data sovereignty requirements in smaller countries where the provider does not have data centers.
- **Phase 3:** Communities of organizations share distributed cloud substations. We use the term "substations" to evoke the image of subsidiary stations (like branch post offices) where people gather to use services. Cloud customers can gather at a given distributed cloud substation to consume cloud services for common or varied reasons if it is open for community or public use. This improves the economics associated with paying for the installation and operation of a distributed cloud substation. As other companies use the substation, they can share the cost of the installation. We expect that third parties such as telecommunications service providers will explore the creation of substations in locations where the public cloud provider does not have a presence. If the substation is not open for use by others outside the organization that paid for its installation, then the substation represents a private cloud instance in a hybrid relationship with the public cloud.

The distributed cloud supports continuously connected and intermittently connected operation of like-for-like cloud services from the public cloud "distributed" to specific and varied locations. This enables low-latency service execution where the cloud services are closer to the point of need in remote data centers or all the way to the edge device itself. This can deliver major improvements in performance and reduce the risk of global network-related outages, as well as support occasionally connected scenarios. By 2024, most cloud service platforms will provide at least some services that execute at the point of need.

Getting to Distributed Cloud

The distributed cloud is in the early stages of development. Many providers aim to offer most of their public services in a distributed manner in the long term. But for now, they provide only a

subset — and often a small subset — of their services in a distributed way. Some of the providers' approaches do not support the full delivery, operation and update elements of a full distributed cloud. Providers are extending services to third-party data centers and out to the edge with offerings such as Microsoft Azure Stack, Oracle Cloud at Customer, Google's Anthos, IBM Red Hat and the previously announced AWS Outposts. Enterprises should evaluate the potential benefits and challenges of three approaches they are likely to see:

- **Software:** The customer buys and owns a hardware platform and software layer with a subset of the providers' cloud services. The provider does not take responsibility for the ongoing operations, maintenance or update of the software or the underlying hardware platform. Users are responsible, doing it themselves or using a managed service provider. Although a software approach provides a like-for-like model between the public service and the on-premises implementation, the other challenges with the hybrid cloud remain. Some customers consider it an advantage that they are in control of service updates.
- **Portability Layer:** The provider delivers a portability layer typically built on Kubernetes as the foundation for services across a distributed environment. In some cases, the portability layer is simply using containers to support execution of a containerized application. In other cases, the provider delivers some of its cloud services as containerized services that can run in the distributed environment. The portability approach ignores the ownership and management of the underlying hardware platform, which remains the responsibility of the customer.
- **Distributed Service:** The provider delivers a like-for-like version of some of its cloud services in a hardware/software combination, and the provider commits to managing and updating the service. This reduces the burden on the consumer who can view the service as a "black box." However, some customers will be uncomfortable giving up all control of the underlying hardware and software update cycles. Nevertheless, we expect this approach will dominate over time.

The Edge Effect

The fundamental notion of the distributed cloud is that the public cloud provider is responsible for the design, architecture, delivery, operation, maintenance, updates and ownership, including the underlying hardware. However, as solutions move closer to the edge, it is often not desirable or feasible for the provider to own the entire stack of technology. As these services are distributed onto operational systems (for example, a power plant), the consuming organization will not give up ownership and management of the physical plant to an outsider provider. However, the consuming organization may be interested in a service that the provider delivers, manages and updates on such equipment. The same is true for mobile devices, smartphones and other client equipment. As a result, we expect a spectrum of delivery models with the provider accepting varying levels of ownership and responsibility.

Another edge factor that will influence the distribution of public cloud services will be the capabilities of the edge, near-edge and far-edge platforms that may not need or cannot run a like-for-like service that mirrors what is found in the centralized cloud. Complementary services tailored to the target environment, such as a low-function IoT device, will be part of the distributed cloud

spectrum (e.g., AWS IoT Greengrass). However, at a minimum, the cloud provider must design, architect, distribute, manage and update these services if they are to be viewed as part of the distributed cloud spectrum.

Related Research:

- "The Edge Completes the Cloud: A Gartner Trend Insight Report"
- "Hype Cycle for Cloud Computing, 2019"
- "Define and Understand New Cloud Terms to Succeed in the New Cloud Era"
- "Prepare for AWS Outposts to Disrupt Your Hybrid Cloud Strategy"
- "Rethink Your Internal Private Cloud"
- "When Private Cloud Infrastructure Isn't Cloud, and Why That's Okay"
- "Cloud Computing Primer for 2019"

Trend No. 8: Autonomous Things

Autonomous things are physical devices that use AI to automate functions previously performed by humans. The most recognizable forms of autonomous things are robots, drones, autonomous vehicles/ships and appliances. AI-powered IoT elements, such as industrial equipment and consumer appliances, are also a type of autonomous thing. Each physical device has a focus for its operation as it relates to humans. Their automation goes beyond the automation provided by rigid programming models, and they exploit AI to deliver advanced behaviors that interact more naturally with their surroundings and with people. Autonomous things operate across many environments (land, sea and air) with varying levels of control. Autonomous things have been deployed successfully in highly controlled environments such as mines. As the technology capability improves, regulation permits and social acceptance grows, autonomous things will increasingly be deployed in uncontrolled public spaces.

Common Technology Capabilities

Autonomous things are developing very rapidly, partly because they share some common technology capabilities. Once the challenges to developing a capability have been overcome for one type of autonomous thing, the innovation can be applied to other types of autonomous things. The following common capabilities and technologies were inspired by the 2020 NASA Technology Taxonomy:[38]

- **Perception:** The ability to understand the physical space in which the machine is operating. This includes the need to understand the surfaces in the space, recognize objects and their trajectories, and interpret dynamic events in the environment.
- **Interaction:** The ability to interact with humans and other things in the physical world using a variety of channels (such as screens and speakers) and sensory outputs (such as light, sound and haptics).

- **Mobility:** The ability to safely navigate and physically move from one point to another in the space through some form of propulsion (such as walking, cruising/diving, flying and driving).
- **Manipulation:** The ability to manipulate objects in the space (such as lifting, moving, placing and adjusting) and to modify objects (for example, by cutting, welding, painting and cooking).
- **Collaboration:** The ability to coordinate actions through cooperation with different things and to combine actions to complete tasks such as multiagent assembly, lane merges and swarm movements.
- **Autonomy:** The ability to complete tasks with a minimum of external input, and to respond to a dynamically changing space without recourse from cloud-based processing or other external resources.

When exploring particular use cases for autonomous things, start with an understanding of the space or spaces in which the thing will operate and the people, obstacles, terrain and other autonomous objects it will need to interact with. For example, navigating a street is much easier than a sidewalk because streets have lines, stoplights, signs and rules to follow. Next, consider the outcomes you are trying to achieve with the autonomous thing. Finally, consider which technical capabilities will be needed to address this defined scenario.

Combining Autonomous Capabilities and Human Control

Autonomous things operate along a spectrum of autonomy, from semiautonomous to fully autonomous. The word "autonomous," when used to describe autonomous things, is subject to interpretation. When Gartner uses this term to describe autonomous things, we mean that these things can operate unsupervised within a defined context or to complete a task. Autonomous things may have various levels of autonomy. For example, a self-directing vacuum cleaner may have limited autonomy and intelligence, while a drone might autonomously dodge obstacles.

It's expedient to use the levels of autonomy often applied to evaluating autonomous vehicles when considering use cases for any autonomous things:[39]

- **No automation —** Humans perform all the control tasks.
- **Human-assisted automation —** Humans perform all the control tasks, but some control-assist features are included in the design. The operator is still in charge of the thing, but specific functions may be automated to simplify control.
- **Partial automation —** Humans are responsible for control tasks and monitoring the environment, but some control tasks are automated. The thing will be able to operate autonomously for short periods, or within specific circumstances, but the operator is in constant control.
- **Conditional automation —** Control tasks are automated, but humans are required to take over control tasks at any time at the request of the automation system. Autonomous operation is possible, within certain operational bounds. The thing may be left to complete specific tasks, but human intervention may be necessary at short notice.

- **High automation —** Control tasks are automated under selected conditions, but humans are required to take over control tasks when operating outside of those selected conditions. The thing is designed to complete required tasks autonomously, and is capable of doing so, but may require human intervention if circumstances change beyond specific bounds.
- **Full automation —** Control tasks are automated under all conditions. Humans may request to take over control tasks. The thing can complete all expected tasks without human intervention, and is capable of adjusting the process to account for changing parameters to the point of deciding when a task can only be partially completed.

Another consideration is the degree of direction or control that might be either required or desirable regardless of the level of autonomy. Even with autonomous things that are fully autonomous and can operate completely independently of any outside agency such as a human, it may be desirable to insert a level of control or direction. In the case of an autonomous vehicle, for example, a human would direct the destination and potentially other aspects of the driving experience and be able to take control if desired. Consider autonomy and control as two complementary aspects to define with regard to specific autonomous things use cases.

Autonomous, Intelligent and Collaborative

As autonomous things proliferate, we expect a shift from stand-alone intelligent things to a swarm of collaborative intelligent things. In this model, multiple devices will work together, either independently of people or with human input. For example, heterogeneous robots can operate in a coordinated assembly process.[40] In the delivery market, the most effective solution may be to use an autonomous vehicle to move packages to the target area. Robots and drones aboard the vehicle could then affect final delivery of the package. The U.S. Defense Advanced Research Projects Agency (DARPA) is leading the way in this area and is studying the use of drone swarms to attack or defend military targets.[41] Other examples include:

- Intel's use of a drone swarm for the opening ceremony of the Winter Olympic Games in 2018[42]
- SAFE SWARM by Honda, where vehicles communicate with infrastructure and one another to predict hazards and optimize traffic flows[43]
- Boeing Loyal Wingman program deploys a series of drones that fly alongside a piloted vehicle that can be controlled from plane it is escorting[44]

Explore ways that AI-driven autonomous capabilities can power virtually any physical device in the organization or the customer's environment. Although autonomous things offer many exciting possibilities, they cannot match the human brain's breadth of intelligence and dynamic general-purpose learning. Instead, they focus on well-scoped purposes, particularly for automating routine human activities. Create business scenarios and customer journey maps to identify and explore the opportunities that will deliver compelling business outcomes. Seek opportunities to incorporate the use of intelligent things in traditional manual and semiautomated tasks. Examples of business scenarios include:

- **Advanced agriculture.** Projects such as the U.S. National Robotics Initiative are pushing agriculture automation to the next level.[45] Examples include creating planning algorithms for robots to autonomously operate farms.
- **Safer automobile transportation.** High-technology firms (such as Alphabet, Waymo, Tesla, Uber, Lyft and Apple) and traditional automotive companies (such as Tesla, General Motors, Mercedes-Benz, BMW, Nissan, Toyota and Ford) hope that, by removing the human error element, self-driving cars will lower the number of automobile accidents. We anticipate more than 1 million Level 3 and above cars will be produced annually by 2025.[46]
- **Autonomous shipping.** Maritime companies such as Kongsberg Maritime are experimenting with various level of autonomous ships. Using an automated system built by Kongsberg, Fjord1 has automated two ferries operating between Anda and Lote in Norway. Kongsberg is also working on autonomous container ships.[47]
- **Search and rescue.** A variety of autonomous things can operate to support search and rescue in various environments. For example, "snakebots" made up of multiple connected and redundant units can maneuver in tight spaces that are logistically impossible or unsafe for people to explore. The Robotics Institute at Carnegie Mellon University is experimenting with a variety of forms and locomotion models.[48]

Related Research:

- "Hype Cycle for Connected Vehicles and Smart Mobility, 2019"
- "Hype Cycle for Drones and Mobile Robots, 2019"
- "Toolkit: How to Select and Prioritize AI Use Cases Using Real Domain and Industry Examples"
- "Swarms Will Help CIOs Scale Up Management for Digital Business"
- "Use Scenarios to Plan for Autonomous Vehicle Adoption"
- "Supply Chain Brief: Favorable Regulations Will Accelerate Global Adoption of Autonomous Trucking"

Trend No. 9: Practical Blockchain

A blockchain is an expanding list of cryptographically signed, irrevocable transactional records shared by all participants in a network.[49] Each record contains a time stamp and reference links to previous transactions. With this information, anyone with access rights can trace back a transactional event, at any point in its history, belonging to any participant. A blockchain is one architectural design of the broader concept of distributed ledgers. Blockchain and other distributed ledger technologies provide trust in untrusted environments, eliminating the need for a trusted central authority. Blockchain has become the common shorthand for a diverse collection of distributed ledger products.

Blockchain potentially drives value in a number of different ways:

- Blockchain removes business and technical friction by making the ledger independent of individual applications and participants and replicating the ledger across a distributed network to create an authoritative record of significant events. Everyone with permissioned access sees the same information, and integration is simplified by having a single shared blockchain model.
- Blockchain also enables a distributed trust architecture that allows parties that do not know or inherently trust one another to create and exchange value using a diverse range of assets.
- With the use of smart contracts as part of the blockchain, actions can be codified such that changes in the blockchain trigger other actions.

Blockchain has the potential to reshape industries by enabling trust, providing transparency and enabling value exchange across business ecosystems — potentially lowering costs, reducing transaction settlement times and improving cash flow. Assets can be traced to their origin, significantly reducing the opportunities for substitutions with counterfeit goods. Asset tracking also has value in other areas, such as tracing food across a supply chain to more easily identify the origin of contamination or tracking individual parts to assist in product recalls. Another area in which blockchain has potential is identity management. Smart contracts can be programmed into the blockchain where events can trigger actions; for example, payment is released when goods are received.

According to the 2019 Gartner CIO Survey, 60% of CIOs expect some kind of blockchain deployment in the next three years.[50] In terms of industries that have already deployed blockchain or plan to deploy it in the next 12 months, financial services leads the way (18%), followed by services (17%) and transportation (16%).[51] It is likely that organizations in these industries have a greater need than organizations in other industries for the simpler use cases that limited use of some blockchain components can support, such as record keeping and data management.

Blockchain Will Be Scalable by 2023

Blockchain remains immature for enterprise deployments due to a range of technical issues including poor scalability and interoperability. Blockchain's key revolutionary innovation is that it eliminates all need for trust in any central or "permissioned" authority. It achieves that largely through decentralized public consensus, which is not yet used in enterprise blockchain, where organizations and consortia govern membership and participation. But enterprise blockchain is proving to be a key pillar in digital transformation that supports evolutionary and incremental improvements in trust and transparency across business ecosystems (see "Blockchain Unraveled: Determining Its Suitability for Your Organization").

By 2023, blockchain will be scalable technically, and will support trusted private transactions with the necessary data confidentiality. These developments are being introduced in public blockchains first. Over time, permissioned blockchains will integrate with public blockchains. They will start to take advantage of these technology improvements, while supporting the membership, governance and operating model requirements of permissioned blockchains (see "Hype Cycle for Blockchain Technologies, 2019").

Blockchain adds little value unless it is part of a network that exchanges information and value. The network collaboration challenges have initially driven organizations to turn to consortia to derive the most immediate value from blockchain. Choosing a consortium requires due diligence across numerous risk criteria before sharing data and engaging with an outside party. Understanding and evaluating these risks will be critical in extracting value from consortia involvement. Four types of consortia exist: technology-centric; geographically centric; industry-centric and process-centric. One option is to work with an industrywide consortium, but other types of consortia are also worth exploring. Organizations need to carefully consider how these consortia will impact the enterprise participation in particular industries and the competitive landscape.

Blockchain Use Cases

Gartner has identified multiple use cases for blockchain. These include:

1. **Asset Tracking.** These use cases cover the tracking of physical assets through the supply chain to identify location and ownership accurately. Examples include tracking of automobiles through loan processes, artworks postsale, and locations of ocean freight and spare parts.
2. **Claims.** This category covers automated claims processing in areas such as automobile, agriculture, travel, and life and health insurance. It also includes other claims, such as processing product recalls.
3. **Identity Management/Know Your Client (KYC).** This category covers uses where records must be securely tied to an individual. Examples include managing records of educational achievement, patient health, election identity and national identities.
4. **Internal Record Keeping.** In these use cases, the data to be secured remains within an individual organization. Examples include master data management, internal document management, purchase order and invoice records, and treasury record keeping.
5. **Loyalty and Reward.** This category includes use cases for tracking loyalty points (for retailers, travel companies and others) and providing internal rewards, such as to employees or students.
6. **Payment/Settlement.** Use cases in this category involve a payment between parties, or settlement of a trade. Examples include royalty payments, stock settlements, interbank payments, commercial lending, procure-to-pay processing and remittance processing.
7. **Provenance.** Similar to the asset-tracking use case, this covers recording the movement of assets, but the aim is to show the full history and ownership of the asset, rather than its location. Examples include: tracking biological samples and organs; establishing the provenance of wine, coffee, fish and other foods; certifying the authenticity of components; and tracking pharmaceuticals through their life cycle.
8. **Shared Record Keeping.** This category includes use cases where data needs to be shared securely between multiple participants. Examples include corporate announcements, multiparty hotel booking management, recording of flight data and regulatory reporting.
9. **Smart Cities/the IoT.** This group includes use cases that use blockchain to provide data tracking and to control functions for smart spaces or IoT solutions. These include peer-to-peer

energy trading, administration of electric vehicle charging, smart grid management and control of wastewater systems.

10. **Trade Finance.** These use cases aim to streamline the process of financing trades, including managing letters of credit, simplifying trade finance and facilitating cross-border trade.

11. **Trading.** Use cases in this group aim to improve the process for buying and selling assets, including dealing in derivatives, trading of private equity and sports trading.

As this technology evolves, Gartner predicts that at least three other use cases will become more viable and could prove the revolutionary benefits that blockchain enables:

- **Blockchain-based voting** will benefit from improvements such as blockchain-related security, management of forks, system governance and ledger interoperability. Blockchain could also improve the tracking and traceability of voting tallies and voter rolls.
- **Blockchain-based, self-sovereign digital identity** will also become more realistic. This could rationalize the maze of the many-to-many suboptimal identity verification systems and relationships used across the globe.
- **Cryptocurrency payments and remittance services** will be used in countries with hyperinflation, with cryptocurrency preserving purchasing power and financial well-being.

Despite the challenges, the significant potential for disruption and revenue generation means you should begin evaluating blockchain, even if you don't aggressively adopt the technologies in the next few years. A practical approach to blockchain development demands:

- A clear understanding of the business opportunity threat and potential industry impact
- A clear understanding of the capabilities and limitations of blockchain technology
- A reevaluation of your enterprise and industry trust architecture
- The necessary vison and skills to implement the technology as part of core business strategy
- A willingness and capability for customers to accept and adopt new operational constructs

Identify how the term "blockchain" is being used, both internally and by providers. Develop clear definitions for internal discussions. Use caution when interacting with vendors that have ill-defined/ nonexistent blockchain offerings or thinly veiled repackaging of legacy offerings as blockchain solutions.

Use Gartner's spectrum model of blockchain evolution[52] to better assess ledger developments, including related initiatives, such as consensus mechanism development, sidechains and blockchains. Resources permitting, consider distributed ledger as a proof of concept (POC) development. But, before starting a distributed ledger project, ensure your team has the business and cryptographic skills to understand what is and isn't possible. Identify the integration points with existing infrastructures to determine the necessary investments, and monitor the platform evolution and maturation.

Related Research:

- "Hype Cycle for Blockchain Technologies, 2019"
- "Blockchain Technology Spectrum: A Gartner Theme Insight Report"
- "The Future of Blockchain: 8 Scalability Hurdles to Enterprise Adoption"
- "Use Gartner's Blockchain Conceptual Model to Exploit the Full Range of Possibilities"

Trend No. 10: AI Security

Over the next five years AI, and especially ML, will be applied to augment human decision making across a broad set of use cases. At the same time, there will be a massive increase in potential points of attack with IoT, cloud computing, microservices and highly connected systems in smart spaces. While this creates great opportunities to enable hyperautomation and leverage autonomous things to deliver business transformation, it creates significant new challenges for the security team and risk leaders. There are three key perspective to explore when considering how AI is impacting the security space:

- **Protecting AI-powered systems.** This requires securing AI training data, training pipelines and ML models.
- **Leveraging AI to enhance security defense.** This uses ML to understand patterns, uncover attacks and automate aspects of the cybersecurity processes while augmenting the actions of human security analysts.
- **Anticipating nefarious use of AI by attackers.** Identifying these attacks and defending against them will be an important addition to the cybersecurity role.

Protecting AI-Powered Systems

AI presents new attack surfaces and thus increases security risks. Just as security and risk management leaders would scan their assets for vulnerabilities and apply patches to fix them, application leaders must monitor ML algorithms and the data they ingest to determine whether there are extant or potential corruption ("poisoning") issues. If infected, data manipulation could be used to compromise data-driven decisions that demand data quality, integrity, confidentiality and privacy.

ML pipelines have five phases that need to be protected: data ingestion; preparation and labeling; model training; inference validation; and production deployment. There are various types of risk across each of these phases that organizations need to plan for. Through 2022, 30% of all AI cyberattacks will leverage training-data poisoning, AI model theft or adversarial samples to attack AI-powered systems.[53]

- **Training-data poisoning:** Hackers might have unauthorized access to training data and cause an AI system to fail by feeding it incorrect or compromised data. Training-data poisoning is more widespread in online learning models, which build and update their inputs as new data comes in. ML systems trained on user-provided data are also susceptible to training-data poisoning attacks,[54] whereby a malicious user feeds bad training data with the goal of

corrupting the learning model. Reduce data-poisoning risk by limiting the amount of training data each user contributes and examining output for shifts in predictions after each training cycle.

- **Model theft:** Competitors can reverse-engineer ML algorithms or implement their own AI systems to use the output of your algorithms as training data. If competitors or bad actors can observe data being fed into the AI and the output being reported, they can use this data to develop their own ML models to engage in supervised learning and reconstruct the algorithm.[55] Researchers showed that certain deep learning algorithms are particularly vulnerable to such imitation and manipulation.[55] Detect model thefts by examining logs for unusual quantities of queries or a higher diversity of queries, and protect the prediction machines by blocking attackers and preparing a backup plan.
- **Adversarial samples:** Classifiers are susceptible to a single sample of input/test data, which can be altered slightly to cause an AI classifier to misclassify it. Most ML classifiers such as linear classifiers (logistic regression, naive Bayes classifiers), support vector machines, decision trees, boosted trees, random forest, neural networks and nearest neighbor are vulnerable to adversarial samples.[56] These alterations can be so refined that a human observer does not notice the modification, yet the classifier still makes a mistake. Proactively defend against adversarial samples by deploying a diverse set of prediction machines. Generate adversarial samples and include them in your training dataset.

Leveraging AI to Enhance Cybersecurity Defense

As the rate and type of attacks expand, cybersecurity professionals will find it increasingly difficult to keep up with demand for greater use of AI to filter and automate defense activities. Security tool vendors are using ML to enhance their tools, decision support and response operations. With the commoditization of research, frameworks and compute power, well-designed ML is within reach for vendors with access to large quantities of relevant, high-quality training data. Assess solutions and architecture, and challenge vendors on the latest ML-related attack techniques, including data poisoning, adversarial inputs, generative adversarial networks and other security-relevant innovations in ML.

ML-based security tools can be a powerful addition to your toolkit when aimed at a specific high-value use case such as security monitoring, malware detection or network anomaly detection. Supervised, unsupervised and reinforcement learning are successfully used in security today to address malware, phishing, network anomalies, unauthorized access of sensitive data, user behavior analytics, vulnerability prioritization and more. However, the best tools do not simply use ML, but they deliver better outcomes. It is important to carefully evaluate and test vendors' claims to ensure they are delivering the value promised.[57]

> Well-designed security techniques based on ML are harder to evade by attackers than rule-based techniques. However, the

> probabilistic nature of ML can potentially generate many false positives, make alerts more difficult to triage and increase the complexity of tuning.

Generally speaking, using ML in defense forces attackers to change their techniques. Typically, attacks become more complex and therefore more costly, but not impossible. In response, security tool vendors and cybersecurity professionals develop new ML techniques to thwart these new attack techniques. This long-standing back and forth will continue, and security teams need to be prepared for the escalating tactics.

Attackers are innovating quickly to improve attacks on ML techniques used in security solutions. They will attempt to poison training data and trick predictive algorithms into misclassification. Be ready for attackers to adapt their techniques and evade detection by security techniques based on ML. Do not rely on ML as a single prevention technique in security solutions.

ML-based security tools are not designed to fully replace existing traditional tools. Invest in ML-based tools to augment security analysts. Ideally the ML-based tools will automate at one level while freeing security analysts to focus on the more sophisticated and novel attack scenarios.

ML algorithms can also be used to improve tracking and cataloging data while providing more accurate reporting and improving overall efforts to achieve compliance with privacy regulations such as GDPR. The power of ML comes from algorithms that can identify patterns in and across datasets. This capability can unearth otherwise hidden information that could drive a company out of GDPR compliance. Chatbot technology and natural language processing can be used for compliance dashboards, threat triage, security operations center (SOC) playbooks and reporting automation. By automating the process of discovering and properly recording all types of data and data relationships using AI applications, organizations can develop a comprehensive view of compliance-related personal data tucked away in all structured and unstructured sources. Developing a comprehensive view using traditional solutions and manual processes would be a near impossible task.[58]

Anticipating Nefarious Use of AI by Attackers

The next frontier of AI-related security concerns is emerging as attackers begin to use ML and other AI techniques to power their attacks. Attackers have just started to leverage ML. They explore ML in many security areas and are helped by the commoditization of ML tools and the availability of training data.

> Every new, exciting innovation in ML can and will be used nefariously. Attackers will use ML to improve targeting, exploits,

the discovery of new vulnerabilities, the design of new payloads and evasion.

Organizations must understand how adversaries may attack security solutions based on ML at training and prediction stages, and how ML accelerates innovation in attacker methods.[59]

Attackers leverage ML to accelerate innovation in attacker techniques. The commoditization of tools for ML has led to many experiments on how to use these for nefarious purposes. One positive industry development is that researchers have started to use some curation on AI publications and code because of the potential use for malicious activity.[60] Nevertheless, security professionals should be aware of these developments and plan mitigations accordingly.

The first application for ML in attacks to explore is phishing. ML lends itself very well to digesting large quantities of data, such as email or social media content. In phishing attacks, ML can be useful for identifying targets, learning normal communication patterns, and then leveraging that information to phish using the same communication styles. This works well for social media, since there is often no lack of data that can be automatically parsed. In 2018, Cyxtera built an ML-based phishing attack generator that trained on more than 100 million particularly effective historic attacks to optimize and automatically generate effective scam links and emails.[61] Cyxtera claims that, by using AI based on open-source libraries and trained on public data, it was able to bypass an AI-based detection system 15% of the time, whereas traditional approaches achieved this only 0.3% of the time.

Identity deception is typically one aspect of phishing. The attacker's intention is to gain the recipient's trust. The good news for attackers is that huge advancements in ML make identity deception credible beyond what was expected a few years ago. ML can be used to simulate someone's voice in "vishing" attacks, or in voice authentication systems. ML can be used to fake people in video. This form of nefarious ML use is commonly referred to as "deepfakes." Nefarious ML can learn what's normal and adjust attacks within this "learned normal." It can learn, simulate and abuse writing styles, social graphs and communication patterns for deception.

Another recent example of nefarious use of ML is DeepExploit. DeepExploit uses Metasploit. It trains on servers and finds the best payloads per target host (based on host info). Then it applies fully automated intelligence gathering, exploitation, postexploitation and reporting. It leverages ML (and signatures) to determine web products (intelligence gathering). Evidently, ML can determine the used platforms/applications with more detail than signatures. DeepExploit then uses a pretrained model to exploit this particular server.[62]

Related Research:

- "Anticipate Data Manipulation Security Risks to AI Pipelines"
- "AI as a Target and Tool: An Attacker's Perspective on ML"
- "How to Prepare for and Respond to Business Disruptions After Aggressive Cyberattacks"

- “How to Prepare for Cyber Warfare”
- “Zero Trust Is an Initial Step on the Roadmap to CARTA”

Evidence

[1] “Setting the ContinuousNext Foundation in Your Team”

[2] “Seize the Technology Advantage With Combinatorial Digital Innovation”

[3] “How to Build Segments and Personas for Multichannel Marketing”

[4] “How Digital Products Drive Change in Product Design”

[5] “Toolkit: Workshop for Creating EA Personas in Digital Business Diagnostic Deliverable Analysis”

[6] “Business Events, Business Moments and Event Thinking in Digital Business”

[7] “From Digital Transformation to ContinuousNext: Key Insights From the 2018 Gartner Symposium/ITxpo Keynote”

[8] “Market Guide for Process Mining”

[9] “Emerging Technology Analysis: Smart Wearables”

[10] “Augmented Reality Is the Operating System of the Future. AR Cloud Is How We Get There,” Forbes.

[11] “3 Immersive Experience Use Cases That Provide Attractive Market Opportunities”

[12] “Could You Fire Someone in Virtual Reality?” TWiT Tech Podcast Network. YouTube.

[13] “Adopt a Mesh App and Service Architecture to Power Your Digital Business” and “API Mediation Is the Key to Your Multiexperience Strategy”

[14] “How to Use Machine Learning, Business Rules and Optimization in Decision Management”

[15] “Drive Data Scientists’ Productivity With Data Preprocessing Techniques”

[16] “Low-Code Development Technologies Evaluation Guide”

[17] “Seek Diversity of People, Data and Algorithms to Keep AI Honest” and “Control Bias and Eliminate Blind Spots in Machine Learning and Artificial Intelligence”

[18] “What Is CRISPR Gene Editing, and How Does It Work?” The Conversation.

[19] "Universal Smart Contact Lenses Market 2018, Breathtaking CAGR of Approximately 10.4%, Foreseeing 2023," Medgadget.

[20] "AI Helps Electronic Nose Distinguish Scents," Daily Sabah.

[21] "The Eyes Have It," The Independent.

[22] "Vagus Nerve Stimulator (VNS) Implantation for Children," UPMC Children's Hospital of Pittsburgh.

[23] "Military-Funded Study Successfully Tests 'Prosthetic Memory' Brain Implants," Live Science.

[24] "Speech Synthesis From Neural Decoding of Spoken Sentences," Nature. (Paid subscription required.)

[25] "Elon Musk Hopes to Put a Computer Chip in Your Brain. Who Wants One?" CNN Digital.

[26] "The Untold Story of the 'Circle of Trust' Behind the World's First Gene-Edited Babies," American Association for the Advancement of Science.

[27] "Maverick* Research: Architecting Humans for Digital Transformation"

[28] "Precautionary vs. Proactionary Principles," Institute for Ethics and Emerging Technologies.

[29] "Proactionary Principle," Wikipedia.

[30] "AI Is Sending People to Jail — and Getting It Wrong," MIT Technology Review.

[31] "Police Use Fitbit Data to Charge 90-Year-Old Man in Stepdaughter's Killing," The New York Times.

[32] "The FBI Used a Suspect's Face to Unlock His iPhone in Ohio Case," The Verge.

[33] "The CIO's Guide to Digital Ethics: Leading Your Enterprise in a Digital Society"

[34] "Consumer Intelligence Series: Protect.me," PwC.

[35] "IEEE Global Initiative for Ethical Considerations in Artificial Intelligence (AI) and Autonomous Systems (AS) Drives, Together With IEEE Societies, New Standards Projects; Releases New Report on Prioritizing Human Well-Being," IEEE Standards Association.

[36] "Start Moving Data Management Capabilities Toward the Edge"

[37] "Rethink Your Internal Private Cloud" and "When Private Cloud Infrastructure Isn't Cloud, and Why That's Okay"

[38] "2020 NASA Technology Taxonomy," NASA.

[39] "SAE International Releases Updated Visual Chart for Its 'Levels of Driving Automation' Standard for Self-Driving Vehicles," SAE International.

[40] "Performance of Collaborative Robot Systems," NIST.

[41] "OFFensive Swarm-Enabled Tactics (OFFSET)," DARPA.

[42] "Inside the Olympics Opening Ceremony World-Record Drone Show," Wired.

[43] "SAFE SWARM," Honda.

[44] "Boeing Unveils 'Loyal Wingman' Drone," Defense News.

[45] "National Robotics Initiative 2.0: Ubiquitous Collaborative Robots (NRI-2.0)," National Science Foundation (NSF).

[46] "Forecast Analysis: Autonomous Vehicle Net Additions, Internet of Things, Worldwide"

[47] "Norway's Autonomous Ships Point to New Horizons," Computer Weekly.

[48] "Snake Robots Crawl to the Rescue, Part 1," The American Society of Mechanical Engineers (ASME).

[49] D. Furlonger, C. Uzureau. "The Real Business of Blockchain: How Leaders Can Create Value in a New Digital Age." Harvard Business Review Press. 15 October 2019.

[50] See Figure 1 in "2019 CIO Agenda: Blockchain's Emergence Depends on Use Cases."

[51] See Figure 5 in "2019 CIO Agenda: Blockchain's Emergence Depends on Use Cases."

[52] "Understanding the Gartner Blockchain Spectrum and the Evolution of Technology Solutions"

[53] "Anticipate Data Manipulation Security Risks to AI Pipelines"

[54] "Certified Defenses for Data Poisoning Attacks," arXiv.org, Cornell University.

[55] "Stealing Machine Learning Models via Prediction APIs," SEC'16 Proceedings of the 25th USENIX Conference on Security Symposium.

[56] "Adversarial Vulnerability for Any Classifier," arXiv.org, Cornell University.

[57] "Assessing the Impact of Machine Learning on Security"

[58] "Market Insight: Address GDPR Compliance With AI Applications"

[59] "AI as a Target and Tool: An Attacker's Perspective on ML"

[60] The ML behind thispersondoesnotexist.com was not published because it was incredibly good at generating realistic photos, and because of the power that such deception techniques can have when used for nefarious purposes. Another example where results were not published because they are too good and can be used nefariously is described in "The AI Text Generator That's Too Dangerous to Make Public," Wired.

[61] "AI Can Help Cybersecurity — If It Can Fight Through the Hype," Wired.

[62] Another initiative worth mentioning in this regard is GyoiThon, another pentest tool that claims to use ML. GyoiThon submits a large number of requests, not unlike DeepExploit, and claims to have an ML engine (naive Bayes) that determines the application. The source code can be found at GitHub.

Note 1 Strategic Technology Trends

Strategic technology trends create opportunities for incremental, transformative and even disruptive innovation. Companies must examine the business impact of these trends and adjust business models and operations appropriately or risk losing competitive advantage to those who do. These are trends that IT cannot afford to ignore for a variety of reasons, such as:

- High potential for impact/disruption
- Reaching tipping points and/or rapidly evolving
- Significant market activity and interest
- Need to take a first/fresh look, next five years
- Different from tactical (today), emerging (five to 10 years) and far horizons (more than 10 years)

Note 2 Robotic Process Automation

RPA learns about processes by recording keystrokes and mouse clicks associated with routine labor related to structured applications and databases. RPA tools then mimic the activities and decisions of human operations. The tools often cannot handle unstructured data, such as emails and text. They are also brittle, and changes to the underlying applications (for example, field changes and moved buttons) can break the scripted process.

Note 3 Intelligence at the Edge

The edge continues to grow in complexity. Intelligence will move to the edge across a spectrum of endpoint devices. The line will blur between categories such as:

- **Simple embedded edge devices.** This category includes switches, light bulbs, industrial equipment, consumer electronics and appliances. Many existing devices in this category may have little more than simple sensors and actuators. The trend is to drive more local compute and storage, as well as more advanced sensors. In the consumer market, these simple devices are morphing into more sophisticated devices. These include smart thermostats that can also act as hubs for home automation systems and smart refrigerators that act in a similar way but

add more sophisticated sensors, local compute/storage and display technologies. The typical life of consumer devices in this category is five to 20 years, while industrial assets often have a life of 40 years. These long lead times create an environment with an enormous span of capabilities in the installed base.

- **Edge I/O devices.** This category includes devices such as speakers, cameras and screens. It includes simple I/O-focused devices that rely heavily on capabilities delivered from local servers and gateways or from external cloud services. Many of these devices will have greater local capabilities, particularly in the form of embedded chips for AI and other specialized tasks. We expect they will have a life of three to 10 years.
- **Edge computing devices.** This category includes mobile devices, notebooks, PCs, printers and scanners. These devices typically have a reasonable level of compute and storage function. They will include an expanding array of sensors and more sophisticated AI chips in the next few years. This category of device has a typical life of one to five years, so it has the greatest potential for rapid updates. These devices will often act as localized processing or storage systems for other edge devices in the environment.
- **Complex embedded edge devices.** This category includes automobiles, tractors, ships, drones and locomotives. Capabilities vary widely in the installed base but these devices will increasingly become “mini-networks.” They will have extensive sensors, compute, storage and embedded AI functionality with sophisticated communication mechanisms back to gateways, servers and cloud-based services. These devices with have a life of three to 20 years, or even longer. This, and the rapid expansion of advanced capabilities in new devices, will create complexities for delivering a consistent set of functionality across a fleet of devices. This will result in the delivery of as-a-service models in many sectors to promote more rapid refresh of devices.

Note 4 The Elements of a Digital Twin

The essential elements of a digital twin are:

- **Model:** The digital twin is a functional system model of the real-world object. The digital twin includes the real-world object’s data structure, metadata and critical variables. More complex composite digital twins can be assembled from simpler atomic digital twins.
- **Data:** The digital twin’s data elements relating to the real-world object include: identity, time series, current data, contextual data and events.
- **Uniqueness:** The digital twin corresponds to a unique physical thing.
- **Ability to monitor:** The digital twin can be used to query the state of the real-world object or receive notifications (for example, based on an API) in coarse or granular detail.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp