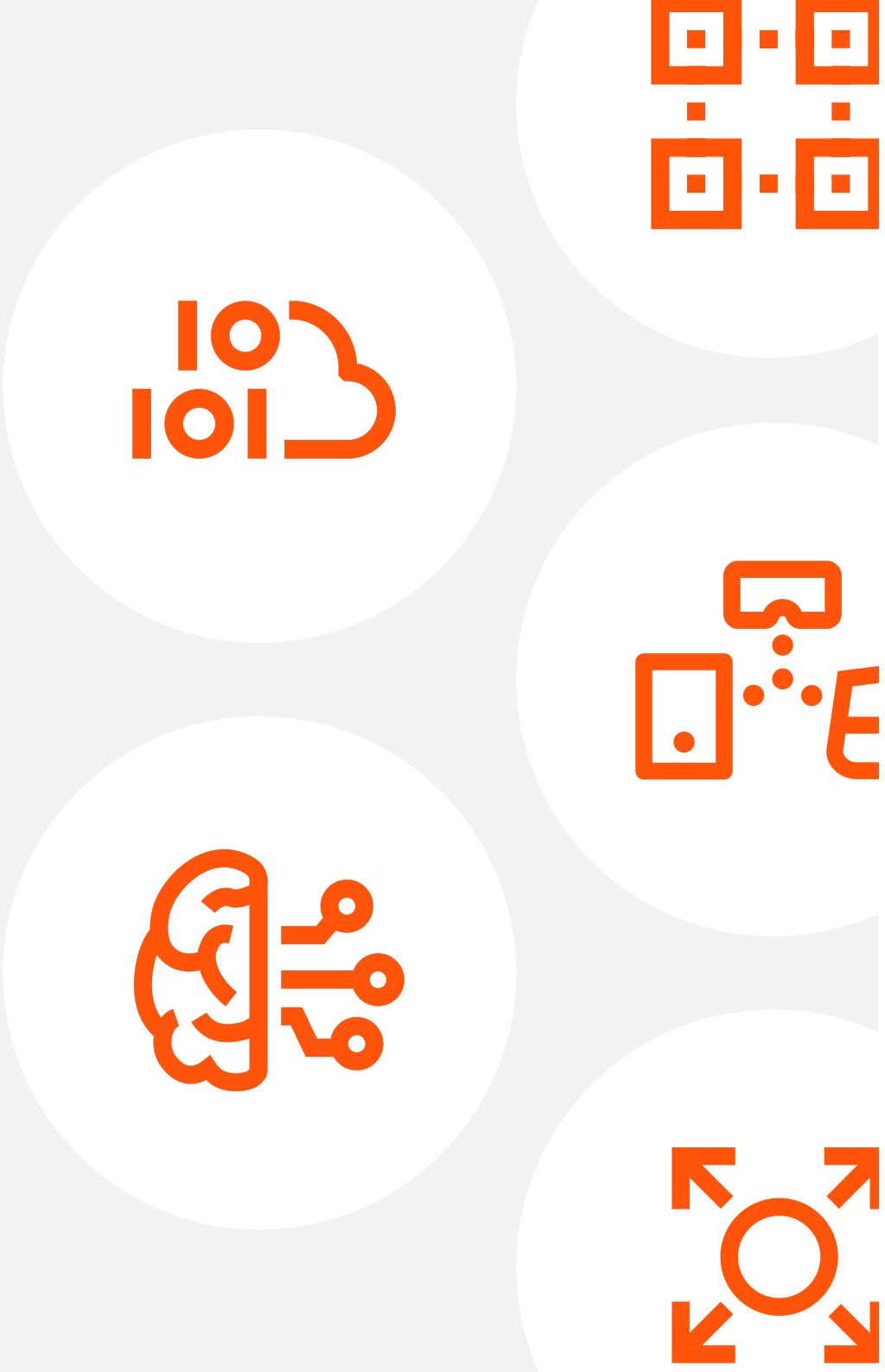
Gartner

Top 10 Strategic Technology Trends for 2020



Edited by
David W. Cearley, Distinguished VP Analyst, Gartner

Introduction

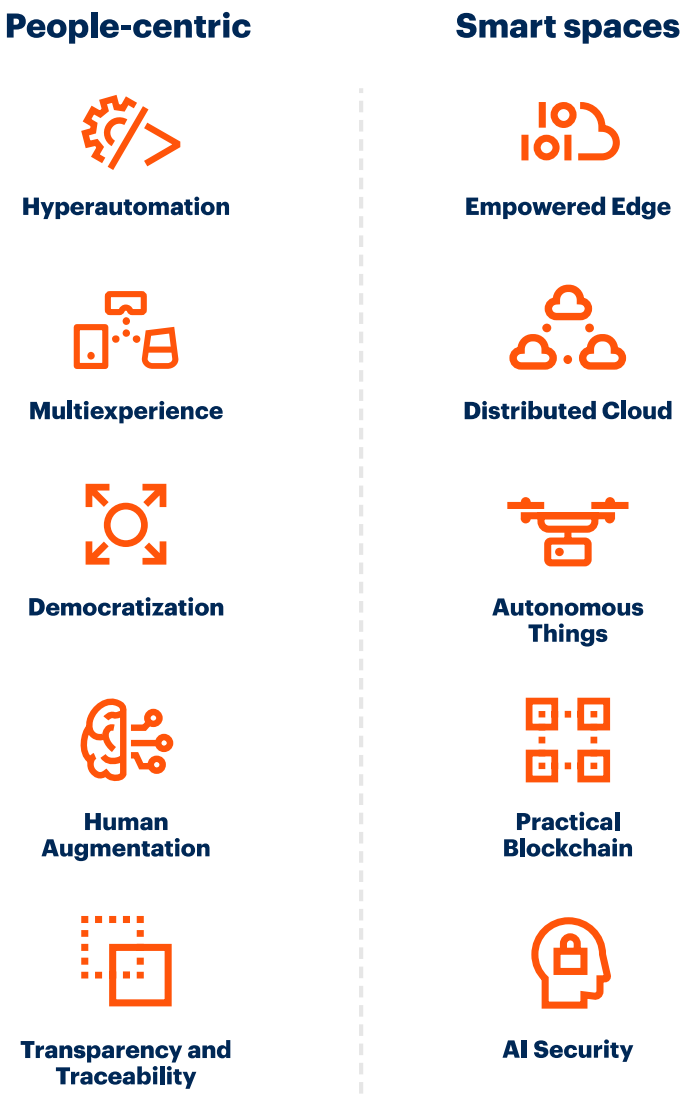
The Gartner top 10 strategic technology trends for 2020 highlight trends that will drive significant disruption and opportunity over the next five to 10 years.

For several years, the top trends focused on the intelligent digital mesh, which is a future in which smart devices deliver insightful digital services everywhere. Although intelligent digital mesh is still important, the 2020 trends are structured around the idea of "people-centric smart spaces" — which means considering how technologies will affect people (i.e., customers, employees) and the places where they live (i.e., home, office, car).

"These trends have a profound impact on the people and the spaces they inhabit," says David W. Cearley, Distinguished VP Analyst, Gartner. "Rather than building a technology stack and then exploring the potential applications, organizations must consider the business and human contexts first."

Remember, these trends don't exist in isolation; IT leaders must decide what combination of the trends will drive the most innovation and strategy.

For example, artificial intelligence (AI) in the form of machine learning (ML) with hyperautomation and edge computing can be combined to enable highly integrated smart buildings and city spaces. In turn, these combinations enable further democratization of the technology.



01

People-centric

Hyperautomation

Automation is organizations using technology to automate tasks that once required human judgment or action. Hyperautomation is a state in which organizations use a combination of AI and ML to rapidly identify and automate all possible business processes. Hyperautomation extends across a range of tools that can be automated, but also refers to the sophistication of the automation (i.e., discover, analyze, design, automate, measure, monitor, reassess).

Hyperautomation has four key implications:

Shifting scope — The scope of automation shifts from individual discrete tasks to knowledge work that drives more dynamic experiences and, ultimately, better business outcomes.

Evolving technology — The technologies required to support hyperautomation will evolve to support a broad range of business scope and incorporate more ML.

Increasing agility — As needs (and threats) evolve, organizations will need to be more agile to respond.

Engage the workforce — The workforce must be fully engaged, and perhaps more importantly, fully integrated, to capture the full value of hyperautomation.

By 2022, application integrations delivered with robotic process automation (RPA) will grow by 40% year over year.

Although automation utilizes a complex, overlapping, ultimately complementary range of tools and technologies, there are two core components:

RPA — Connects legacy systems

Intelligent business process management suites (iBPMSs) — Manage long-running processes

02

People-centric

Multiexperience

Multiexperience replaces technology-literate people with people-literate technology. In this trend, the traditional idea of a computer evolves from a single point of interaction to include multisensory and multitouchpoint interfaces like wearables and advanced computer sensors. Multiexperience moves across many human senses, which creates a richer, more immersive experience.

Eventually multiexperience will evolve into the ambient experience, but the technology faces challenges with privacy issues, as well as with individual independent creators working on different experiences. It will be a while, if ever, before a seamless experience emerges. Most likely, ambient experiences will exist in proprietary ecosystems.

A million ways to order pizza

Domino's Pizza created a multiexperience platform that moved beyond simply ordering food via its app. The company expanded the experience to include a pizza tracker and smart speaker communications, and uses technologies like autonomous vehicles and drones to deliver the food.

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

03

People-centric

Democratization

Democratization provides people with easy, low-/no-cost access to technical or business domain expertise. It focuses on four key areas — application development, data and analytics, design and knowledge — and is often referred to as “citizen access,” which has led to the rise of citizen data scientists, citizen programmers and more.

This technology trend provides advice, takes action and extends the expertise of the user. It can also reduce the timeline and resource lift for a particular project. For example, currently, application developers have to partner with a professional data scientist to create AI-enhanced solutions. With the rise of democratization, the developer could utilize an AI model or easy-to-configure development tools specifically designed to integrate AI capabilities.

These options will range in sophistication from something that can be plugged into code to tools that require more data for a specific project and its pretraining. This means that a model may be pretrained for image recognition, but needs a training dataset to recognize a particular set of images.

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.

04

People-centric

Human Augmentation

Human augmentation is the use of technology and science to heighten a person's cognitive and physical experiences. Human augmentation is not a new concept — humans have been augmenting themselves with glasses and prosthetics for hundreds of years — but the introduction of computers added a new dimension to the possibilities. For example, instead of glasses, people can choose to have corrective laser eye surgery.

Technology is now on the cusp of moving beyond augmentation that replaces a human capability and into augmentation that creates superhuman capabilities, like an implant that links a human brain directly to a computer or an exoskeleton device that offers superhuman strength.

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

Physical versus cognitive

Physical augmentation: Changes an inherent physical capability via implanting or hosting a technology element on the body

- Sensory augmentation (hearing, vision, perception)
- Appendage and biological function augmentation (exoskeletons, prosthetics)
- Brain augmentation (implants to treat seizures)
- Genetic augmentation (somatic gene and cell therapy)

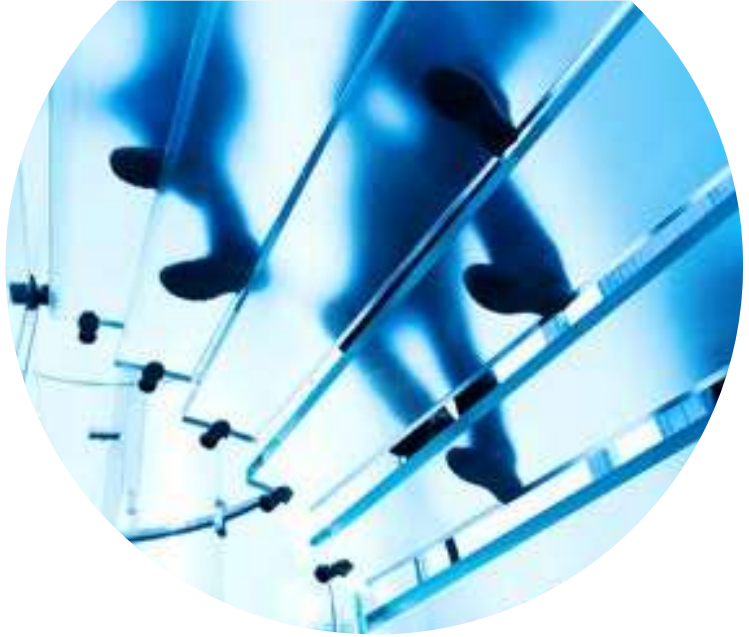
Cognitive augmentation: Enhances a human's ability to think and make better decisions

- Exploiting information and applications to enhance learning or new experiences
- Augmented intelligence scenarios (AI working with humans)
- Physical implants that deal with cognitive reasoning

05

People-centric

Transparency and Traceability



As consumers become more aware and savvy about how organizations are using their data — and organizations are using increasing amounts of AI and ML to drive business decisions — a trust crisis has emerged.

Enterprises must embrace ideas like explainable AI and transparent data policies for both ethical and business reasons. In addition to increasing legislation and potential regulatory issues, consumers will begin to judge and select organizations based on these policies.

The six 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 mechanisms in place for testing, assurance and auditability so 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?

By 2020, Gartner expects companies that are digitally trustworthy will generate 20% more online profit than those that aren't.

06

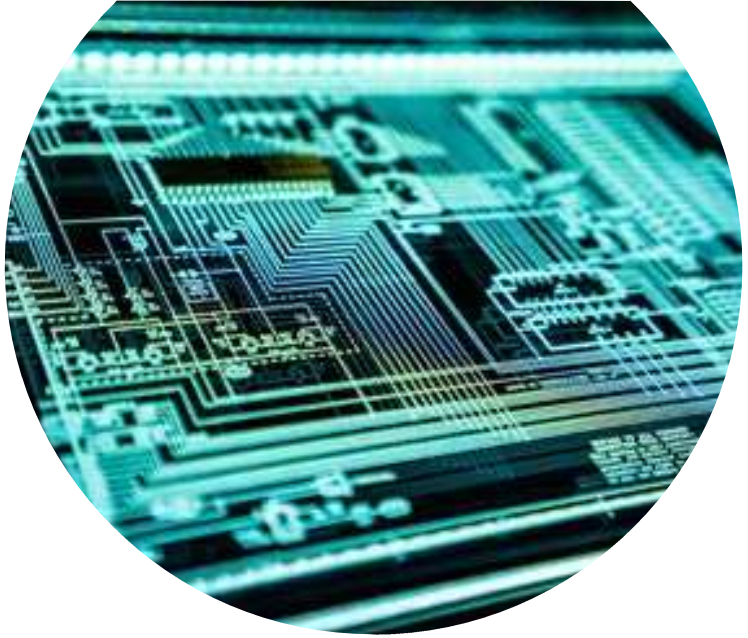
Smart spaces

Empowered Edge

Edge computing is a topology where information processing and content collection and delivery are placed closer to the sources of the information, with the idea that keeping traffic local and distributed will reduce latency. This includes all the technology on the Internet of Things (IoT).

Empowered edge looks at how these devices are increasing and forming the foundations for smart spaces. It also moves key applications and services closer to the people and devices that use them.

Through 2028, there will be a steady increase in the embedding of sensor, storage, compute and advanced AI capabilities in edge devices. However, these devices will range from simple sensors to mobile phones and autonomous vehicles, with life spans ranging from one to 40 years. This, in addition to a push to increase functionality in edge devices, creates a complex and ongoing management and integration challenge.



By 2023, there could be more than 20 times as many smart devices at the edge of the network as in conventional IT roles.

07

Smart spaces

Distributed Cloud

Distributed cloud refers to the distribution of public cloud services to locations outside the cloud provider's physical data centers, but which are still controlled by the provider. In distributed cloud, the cloud provider is responsible for all aspects of cloud service architecture, delivery, operations, governance and updates.

The evolution from centralized public cloud to distributed public cloud ushers in a new era of cloud computing. It also allows providers to deliver on the promises made by hybrid cloud, a system that blends external services from a provider and internal services running on-premises. The problem is that hybrid cloud is incredibly difficult to implement in a cost-efficient or reasonable manner.

Distributed cloud is in the early stages of development, so most providers currently offer only a small subset of services in a distributed manner, with plans to eventually offer full services.

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

08

Smart spaces

Autonomous Things

Autonomous things are physical devices that use AI to automate functions previously performed by humans. They range in size and sophistication from small drones to autonomous ships, and operate across many different environments (i.e., land, sea and air.) Increasingly, autonomous things are operating in closed environments, such as mines or warehouses, but they will eventually evolve to more open spaces.

Autonomous things operate along a spectrum from semiautonomous devices to fully autonomous cars. Further, as the number of autonomous things increases, there will be a shift from things that operate alone to a swarm of collaborative intelligent things. For example, a group of robots could operate a coordinated assembly processes.

By 2023, over 30% of operational warehouse workers will be supplemented by collaborative robots.

Honda's Safe Swarm

Honda's Safe Swarm uses vehicle-to-vehicle communication to allow cars to pass information to other cars in the vicinity. For example, alerts about an accident miles up the road could be relayed to cars several miles back, enabling them to operate collaboratively and intelligently to avoid accidents and mitigate traffic.

09

Smart spaces

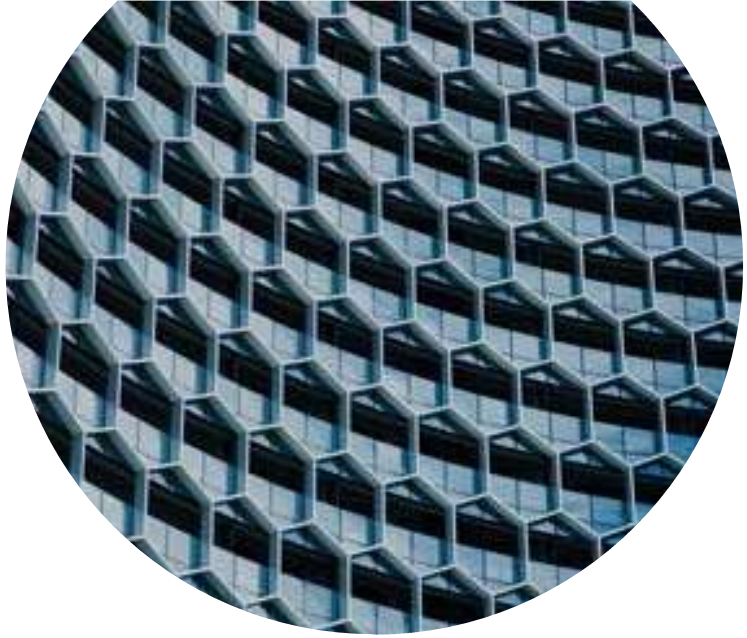
Practical Blockchain

Blockchain is a type of distributed ledger, an expanding chronologically ordered list of cryptographically signed, irrevocable transactional records shared by all participants in a network. This enables two (or more) parties who don't know each other to exchange value without a need for a centralized authority.

Complete blockchain includes five elements: Distribution, immutability, decentralization, encryption and tokenization.

Due to challenges with technology and scalability, today's organizations are taking a practical approach to blockchain that often lacks distribution and tokenization, making them "blockchain-inspired" solutions. 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 — organizations are creating private blockchains.

Everyone with permissioned access is then able to see the same information, and integration is simplified by having a single shared blockchain. Consensus is handled through more traditional private models.



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

Blockchain for shipping containers

In an effort to cut down on costly (and often unreliable) paper-based and manual systems to track goods shipped via the ocean, Maersk and IBM introduced TradeLens — a blockchain-based platform for tracking shipping containers and processing paperwork. With major shipping players now on board, the platform covers more than half of the world's ocean container cargo, reducing inefficiencies and offering visibility for all participants.

10

Smart spaces

AI Security

The increase in the number of AI solutions and potential points of attack, via IoT devices and highly connected services, creates a true security challenge.

AI security includes three key perspectives:

Protecting AI-powered systems — Securing AI training data, training pipelines and ML models

Leveraging AI to enhance security defense — Using ML to understand patterns, uncover attacks and automate parts of cybersecurity processes

Anticipating nefarious use of AI by attackers — Identifying attacks and defending against them

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

How attackers are using AI

"Hi Amy, I wanted to share some photos I took of us in Bermuda. — Love, Mom." This might seem like an email from mom, but it is actually an email from a scammer with a phishing link. In phishing attacks, ML can be used to learn the normal communication patterns of a person via social media, and then use those patterns to create attacks that mimic the communication style of the real person.