Gartner

Top Strategic Technology Trends for 2021

Edited by
Brian Burke, Research Vice President, Gartner

Introduction

Disruption is the hallmark of 2020. Although many leaders are used to some level of constant change, COVID-19 impacted the world in ways no one could have predicted. In turn, organizations have had to pivot and strategize, adapt and change in new ways.

As organizations continue to respond to the crisis and explore new ways to operate and drive growth, the Gartner top strategic trends highlight areas of opportunity and ways for organizations to differentiate themselves from competitors.

Organizations that are prepared to pivot and adapt will weather all types of disruptions. As always, these strategic technology trends do not operate independently of each other, but rather they build on and reinforce each other. Together they enable organizational plasticity that will help guide organizations in the next five years.

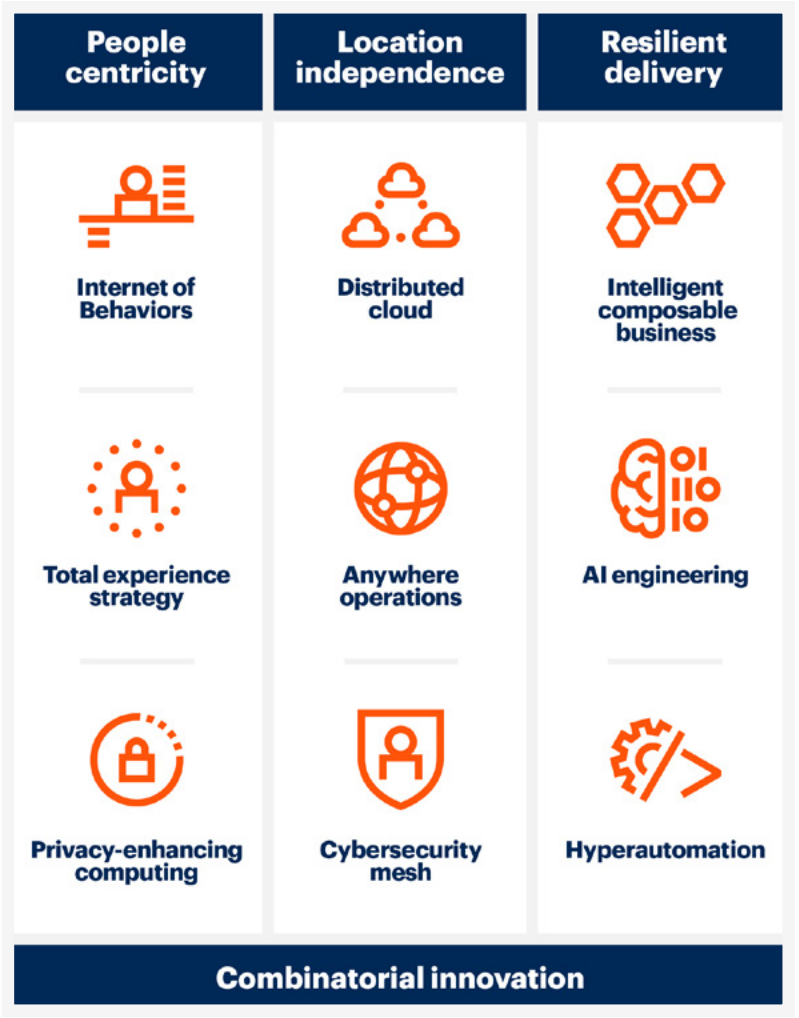
"The unprecedented socioeconomic challenges of 2020 demand the organizational plasticity to transform and compose the future."

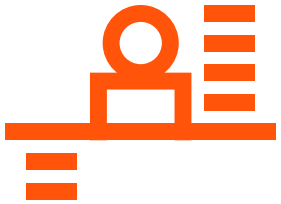
Brian Burke
Research Vice President, Gartner

This year's trends fall along three themes: People centricity, location independence and resilient delivery.

- **People centricity:** Despite the pandemic changing how many people work and interact with organizations, people are still at the center of all business — and they need digitalized processes to function in today's environment.
- **Location independence:** COVID-19 has shifted where employees, customers, suppliers and organizational ecosystems physically exist. Location independence requires a technology shift to support this new version of business.
- **Resilient delivery:** Whether a pandemic or a recession, volatility exists in the world.

Organizations that are prepared to pivot and adapt will weather all types of disruptions. As always, these strategic technology trends do not operate independently of each other, but rather they build on and reinforce each other. Together they enable organizational plasticity that will help guide organizations in the next five years.





People centricity

Internet of Behaviors

The Internet of Behaviors (IoB) captures the “digital dust” of people’s lives from a variety of sources, and that information can be used by public or private entities to influence behavior. The data can come from a range of sources, from commercial customer data to social media to facial recognition, and as more and more data becomes available, the IoB will capture increasing amounts of information. Additionally, the technology that puts all the data together and draws insight is growing increasingly sophisticated.

The IoB presents significant and pervasive social and ethical implications. Collecting data to influence behaviors has the potential to be a powerful tool, and its social reception might depend on just how heavy-handed organizations are with what they’re trying to do.

The IoB captures the ‘digital dust’ of people’s lives.

For example, while drivers may not object to having speed, braking and cornering tracked in exchange for lower insurance premiums, they might not be as receptive to law enforcement also being able to track that information. At the end of the day, the IoB must offer a mutual benefit to both parties or risk being rejected by consumers.

For certain geographical areas, much of the scope and execution of an IoB will depend on local privacy laws, which may affect how data can be used and in what way.

People centricity

Total experience

Total experience combines traditionally siloed disciplines like multiexperience (MX), customer experience (CX), employee experience (EX) and user experience (UX), and links them to create a better overall experience for all parties. Not only does this streamline the experience for everyone, because organizations are optimizing across all experiences, it offers an excellent opportunity to differentiate an organization from competitors.

With an overall goal of transforming the entire experience, total experience enables organizations to lean into the challenges created by COVID-19 and identify new activities that they can integrate and build on.

Total experience in practice

A large telecommunications company transformed its entire experience to improve safety and satisfaction.

First, it deployed an appointment system via an existing app. When customers arrived for their appointment and came within 75 feet of the store, they received two things:

1. A notification to guide them through the check-in process.
2. An alert letting them know how long it would be before they could safely enter the store and maintain social distance.

To enhance employee safety, the company also deployed technology that allowed associates to co-browse customer hardware without physically touching the device.

People centricity

Privacy-enhancing computation

Privacy-enhancing computation comprises three types of technologies that protect data while it's being used to enable secure data processing and data analytics:

- The first provides a trusted environment in which sensitive data can be processed or analyzed. It includes trusted third parties and hardware-trusted execution environments (also called confidential computing).
- The second performs processing and analytics in a decentralized manner. It includes federated machine learning and privacy-aware machine learning.
- The third transforms data and algorithms before processing or analytics. It includes differential privacy, homomorphic encryption, secure multiparty computation, zero-knowledge proofs, private set intersection and private information retrieval.

This enables organizations to safely share data in untrusted environments, an increasingly in-demand desire as the amount of data grows alongside the need to protect that data.

What is homomorphic encryption?

Homomorphic encryption (HE) is a cryptographic method that enables third parties to process encrypted data and return an encrypted result to the data owner, while providing no knowledge about the data or the results. HE enables algorithm providers to protect proprietary algorithms and data owners to keep data private. Homomorphic encryption is still maturing. In practice today, fully homomorphic encryption is not fast enough for most business implementations.

Location independence

Distributed cloud

Distributed cloud provides public cloud options to different physical locations. Essentially, the public cloud company maintains, operates and evolves the services, but physically executes at the point of need. This helps with latency issues, and also privacy regulations that require certain data to remain in a specific geographical location. It allows customers to benefit from public cloud and avoid costly and complicated private cloud solutions.

The many styles of distributed cloud:

- **On-premises public cloud:** This is a popular vendor offering, but it offers only a fraction of the provider's full suite and remains relatively immature.
- **Internet of Things (IoT) edge cloud:** Distributed services that interact directly with edge devices.
- **Metro-area community cloud:** The distribution of cloud services into nodes in a city or metro area connecting to multiple customers.
- **5G mobile edge cloud:** The delivery of distributed cloud services as part of a 5G telco/carrier network.
- **Global network edge cloud:** The delivery of cloud services designed to integrate with global network infrastructure such as cell towers, hubs and routers.

Location independence

Anywhere operations

Anywhere operations refers to an IT operating model designed to support customers everywhere, enable employees everywhere and manage the deployment of business services across distributed infrastructure. The model for anywhere operations is “digital first, remote first.”

However, it’s not as simple as just operating remotely — the model must offer unique value-add experiences. Providing a seamless and scalable digital experience requires changes in the technology infrastructure, management practices, security and governance policies, and employee and customer engagement models.

This technology foundation comprises five building blocks:

Collaboration and productivity: Workstream collaboration, meeting solutions, cloud office suites, digital whiteboarding and smart workspaces

Secure remote access: Passwordless and multifactor authentication, zero trust network access (ZTNA), secure access service edge (SASE) and identity as the new security perimeter

Cloud and edge infrastructure: Distributed cloud, the IoT, API gateways, AI at the edge and edge processing

Quantification of the digital experience: Digital experience monitoring, workplace analytics, remote support and contactless interactions

Automation to support remote operations: TAIOps, endpoint management, SaaS management platforms, self-service and zero-touch provisioning

Location independence

Cybersecurity mesh

The cybersecurity mesh is a distributed architectural approach to scalable, flexible and reliable cybersecurity control. COVID-19 has accelerated an existing trend wherein most assets and devices are now located outside traditional physical and logical security parameters. The cybersecurity mesh enables any person or thing to securely access and use any digital asset, no matter where either is located, while providing the necessary level of security.

As organizations accelerate digital business, security must keep pace with the rapid change. Cybersecurity mesh enables a security model that retains the plasticity necessary to operate in the current conditions and offers security without hindering growth for the company. These tools are already being deployed in some capacity by leading organizations.

The need to support a world of increasingly distributed digital assets and users is the main thing driving the growth of the cybersecurity mesh.

Resilient delivery

Intelligent composable business

Organizations have spent the past years focusing on efficiency, which meant when hit with a major disruption like COVID-19, many business processes were too brittle to quickly adapt and they simply broke.

During the rebuilding process, leaders must design an architecture that:

- Enables better access to information
- Can augment that information with new insights
- Is composable, modular, and can change and respond more quickly as decisions are made

But what does this change look like in action? Decision making must change to focus on increasing the autonomy and augmentation of decisions. Technology platforms must change to prioritize democratization and composition, resulting in more personalized application experiences. Application vendors' products must change from single solutions to preassembled collections of business capabilities. Business units must change from deploying packaged applications to assembling capabilities that deliver more role-specific application experiences.

Additionally, CIOs must become strategic advisors to the CEO and board to advise them on how this level of plasticity is key to the future of the composable business.

Resilient delivery

AI engineering

AI projects often fail due to issues with maintainability, scalability and governance. However, a robust AI engineering strategy will facilitate the performance, scalability, interpretability and reliability of AI models while delivering the full value of AI investments. Without AI engineering, most organizations will fail to move AI projects beyond proofs of concept and prototypes to full-scale production.

AI engineering stands on three core pillars: DataOps, ModelOps and DevOps.

DevOps deals mainly with high-speed code changes, but AI projects experience dynamic changes in code, models and data, and all must be improved. Organizations must apply DevOps principles across the data pipeline for DataOps and the machine learning model pipeline for MLOps to reap the benefits of AI engineering.

What is responsible AI?

From the governance perspective of AI engineering, responsible AI is emerging as an umbrella term for many aspects of AI implementations. These include AI value, risk, trust, transparency, ethics, fairness, interpretability, accountability, safety and compliance. Responsible AI signifies the move from declarations and principles to the operationalization of AI accountability at the organizational and societal levels.

Resilient delivery

Hyperautomation

Hyperautomation is a process in which businesses automate as many business and IT processes as possible using tools like AI, machine learning, event-driven software, robotic process automation, and other types of decision process and task automation tools.

Organizations are often dragged down by "organizational debt," which includes technical, process, data, architecture, talent, security and social debt. Collectively this debt affects value proposition and brand. The cause is an extensive and expensive set of business processes underpinned by a patchwork of technologies that are often not optimized, lean, connected or consistent.

However, in a world where digital acceleration is the name of the game, business leaders are clamoring for digital operational excellence. This was further accelerated by

> **"Hyperautomation is irreversible and inevitable. Everything that can and should be automated will be automated."**
>
> **Brian Burke, Research Vice President, Gartner**

COVID-19, which rapidly pushed organizations to allow more remote, digital-first options. Hyperautomation is the key to both digital operational excellence and operational resiliency for organizations. To enable this, organizations had to digitize their documents/artifacts and ensure their business and IT process workflows were digital. They need to automate tasks, processes and orchestrate automation across functional areas.

Learn more.
Dig deep.
Stay ahead.

Complimentary content:
→ Visit Smarter With Gartner

Stay ahead of the pressing topics, technology and trends that impact your organization's growth and transformations.

Become a client:

U.K.: 03330 607 044
U.S.: 1 855 811 7593
→ gartner.com/en/become-a-client

Gartner®