

Top Strategic Technology Trends for 2021

Published 19 October 2020 - ID G00735310 - 48 min read

By Analysts [Brian Burke](#), [Frances Karamouzis](#), [Gilbert van der Heiden](#), [Arun Chandrasekaran](#), [David Cearley](#), [Bart Willemsen](#), [Brent Stewart](#), [Ramon Krikken](#), [Jay Heiser](#), [Erick Brethenoux](#), [Jason Wong](#), [Michael Chiu](#), [Michelle Duerst](#), [Don Scheibenreif](#), [Manjunath Bhat](#), [Tony Harvey](#), [Nicole Sturgill](#), [Laurie Shotton](#), [Stephanie Stoudt-Hansen](#), [Gene Alvarez](#), [Dennis Gaughan](#), [Andrew White](#), [David Smith](#), [Ed Anderson](#), [David Wright](#), [Yefim Natis](#)

Initiatives: [Technology Innovation](#)

The unprecedented socioeconomic challenges of 2020 demand the organizational plasticity to compose the future. IT leaders must focus on people centricity for stakeholders both internal and external by providing location-independent services, while operating in a resilient delivery model.

Additional Perspectives

- [Invest Implications: Top Strategic Technology Trends for 2021](#)
(20 October 2020)
- [Summary Translation: Top Strategic Technology Trends for 2021](#)
(10 November 2020)

Overview

Opportunities

- Organizations have an opportunity to do more to engage, enable and delight people. They can use the Internet of Behaviors (IoB) to influence people's actions. They can use a total experience strategy to improve the experience of customers, partners and employees. And they can use privacy-enhancing computation to address customers' data privacy concerns.
- Many people now work remotely in a digital-first mode. So IT leaders must provide location-independent services. The distributed cloud enables them to provide services at the point of need. Those with a digital-first approach have a new opportunity with anywhere operations. Meanwhile, the cybersecurity mesh enables anyone to access any digital asset securely, no matter where either is located.
- The need for operational resiliency across business functions, technology and service delivery has never been greater. Organizations that deliver highly digitized business capabilities in a composable and modular way have the biggest opportunities. They'll gain competitive advantage by using

artificial intelligence (AI) engineering techniques to operationalize AI. And they'll increase efficiencies and efficacy by automating processes and augmenting decisions through hyperautomation.

Recommendations

IT leaders responsible for technology innovation must:

- Ensure stable and consistent IoB deployments by establishing a framework for privacy, security, ethics and interconnectivity. Engage people by designing a total customer and employee experience. Identify use cases for privacy-enhancing computation in untrusted environments that require, for example, sharing of personal data across the business ecosystem.
- Remove barriers to using the distributed cloud by changing practices to allow service providers to control assets and services on-premises and at the edge. Drive business model innovation using a digital-first, location-independent strategy. Promote the use of the cybersecurity mesh by moving the perimeter to the asset.
- Deliver resilient operations by emphasizing modularity. Establish repeatable AI engineering practices to realize the business value of AI. Automate everything that can be automated.




Analysis

We're used to change in the digital age, but few of us could have predicted the changes and upheaval that the global pandemic has brought. The pandemic has completely changed how many of us live and work, and some of these changes may be permanent. Organizations require the plasticity to shape-shift to the new reality. As an IT leader, you must compose the future for your organization in these unprecedented times. This is where our top strategic technology trends for 2021 come in. We've selected them for their transformative potential. They fall into three themes (see Figure 1):

- People centricity
- Location independence
- Resilient delivery

Figure 1. Top Strategic Technology Trends for 2021

Top Strategic Technology Trends for 2021

 People Centricity	 Location Independence	 Resilient Delivery
<ul style="list-style-type: none"> • Internet of Behaviors • Total Experience • Privacy-Enhancing Computation 	<ul style="list-style-type: none"> • Distributed Cloud • Anywhere Operations • Cybersecurity Mesh 	<ul style="list-style-type: none"> • Intelligent Composable Business • AI Engineering • Hyperautomation
Combinatorial Innovation		

Source: Gartner
735310_C

Gartner

As your organization journeys from responding to the crisis to exploiting opportunities and on to driving growth, it must focus on the three main areas that form the themes of our top strategic technology trends for 2021:

- **People centricity.** People are our most precious assets. Many people are now working remotely, across all areas of the business ecosystem. They can't function without digitized processes in a secure, trusted mode. People may work individually or in teams. They represent a broad spectrum of stakeholders (employees, customers, suppliers, partners, the local community or online influencers). Our people centricity theme focuses on people's behaviors, experience and privacy.
- **Location independence.** The pandemic has greatly increased the need for location independence. New ways of working mean that employees, customers, suppliers and everyone across the business ecosystem can be located anywhere. Our location independence theme addresses the technology shifts that are driving a distributed cloud structure that facilitates anywhere operations in both business and IT. This theme also describes how a cybersecurity mesh shifts the security perimeter to the individual.
- **Resilient delivery.** This theme isn't about "bouncing back" — it's about having the ability to nimbly adapt or pivot in a dynamic business or IT environment. The theme's underlying assumption is that volatility exists, so it's vital to have the skills, capabilities, techniques, operational processes and systems to constantly adapt to changing patterns. This means organizations must be composable with modular, adjustable, autonomous components. They must use sophisticated technologies such as AI, engineering the approach with a disciplined focus to achieve sustained resiliency. And business and IT processes must be automated, hence the relentless zeal for hyperautomation.

But trends and technologies don't exist in isolation — they build on and reinforce one another. In combinatorial innovation, trends combine to create a whole that's larger than its individual parts. We selected our trends for 2021 partly based on their combined effects. The trends reinforce one another to enable organizational plasticity with an adaptable and resilient business and technology foundation. Combined, our 2021 trends focus on social and personal demand from anywhere to be realized through optimal delivery.

People Centricity

Internet of Behaviors

Analysis by Bart Willemsen, Brent Stewart, Frances Karamouzis

SPA: By year-end 2025, over half of the world's population will be subject to at least one loB program (private, commercial or governmental).

Description:

The loB consists of multiple approaches to capture, analyze, understand and respond to all kinds of digital representations of behaviors. A range of public- and private-sector organizations will seek to use the loB's digital capture ability to affect or influence the behaviors of individuals or collective demographic groups. This goes beyond operant conditioning, which focuses on reward and punishment (see Note 1). In the loB, influence can also take the form of adjusted information feeds, for example.

The loB combines multiple sources of intelligence such as commercial customer data, citizen data processed by public-sector and government agencies, social media, public domain deployments of facial recognition, and location tracking. Additional sources can include things such as temperature and other physical measurements in both private and public domains. From analysis of data in these myriad resources, it's possible to tag an increasingly broad array of people's behavior as an "event."

Emerging technology innovations and algorithm developments enable more precise monitoring and interpretation of behaviors. The loB combines existing technologies that focus on the individual directly (e.g., facial recognition, location tracking and big data) and connects the resulting data to other indirectly identifiable information (e.g., cash purchases, automotive telemetry, vacuum bot layout data and device usage data). Thus, the loB is partly based on the Internet of Things (IoT). In the IoT, physical things are "instructed" to perform certain actions under certain conditions. In the loB, people's behaviors are monitored and incentives or disincentives are applied to influence them to perform toward a desired set of operating parameters. A program can apply value judgments to behavioral events based on the behavior desired by the program's deployer.

Why Trending:

The loB is trending because:

- Technological capability has increased.
- The ability to synergistically combine data from various sources has improved significantly.
- Organizations have deployed a variety of approaches demonstrating the art of the possible and enabling an analysis of the various deployments.

The Facebook/Cambridge Analytica scandal is an early display of the loB. Cambridge Analytica combined digital assets, data mining, data brokerage and behavior analytics with strategic information feeds before and during electoral processes. ¹ Investigative and U.S. congressional hearings showed that Cambridge Analytica used the analysis of behaviors to adjust information feedback to influence the way people voted. Another example is China's social credit system (SCS), a nationwide loB implementation. ² The SCS has an approximate reach of 1.4 billion people, about 18% of the world's population.

In response to the pandemic, organizations are deploying additional behavior intelligence sources at a faster pace. Examples include temperature measurements, face recognition deployments, contact tracing and location-tracking systems. The focus is on combining physical and digital behavior data to influence behaviors that will reduce the spread of infection.

Implications:

The most consistent and pervasive implication of the loB will be extensive ethical and societal debate worldwide. Various loB programs exist, each with different goals and outcomes. In each program, the interpretation and tolerance of the loB program are vastly different. For example, motorists have long accepted that their car insurance premiums will be higher if they have a high accident rate or commit driving offenses. However, they may be much less likely to tolerate the use of in-vehicle telemetry to dynamically track whether they exceed speed limits. Insurers could even include automated triggers that inform law enforcement when customers speed. Similarly, health insurance customers accept higher premiums if they smoke heavily. However, they may be much less likely to tolerate higher premiums triggered by wearable devices that detect exercise levels below insurer-defined minimum values or weekly grocery shopping that reveals food purchases deemed unhealthy.

Different privacy laws exist in different regions. The implications of these laws will affect the scope, scale and reach of loB deployments and the approach to them. The success of deployments will be highly correlated to the mutual benefits of all involved parties, as well as the collective view of trust and acceptable uses of data. So, there won't be *one* loB.

The insurance industry uses behavior-influencing business models. Examples in the U.S. include Allstate (Drivewise), State Farm (HiRoad) and Root Insurance, which all employ usage and behavioral data to dynamically adjust the pricing of car insurance premiums. The Root Insurance app includes driving telematics features to track factors such as speed, braking and cornering. Car rental and leasing

agencies in Europe have also experimented with black-box deployments to observe driving styles with the aim of reducing fuel consumption and the risk of accidents.

Similar models are likely to expand into health insurance and financial services, with reputation or scoring algorithms inspired by Airbnb and Uber. Organizations usually frame these models as a benefit — for example, customers will receive a reduced premium for good behavior. We expect that experimental attempts will soon appear in other areas, driven by commerce and governments.

Actions:

- Examine how loB deployments are affecting your organization by tracking them and exploring their effects — it's likely your organization will be within the sphere of influence of at least one loB program.
- Maximize success and the public's trust by assessing the benefits and risks for both organizations and individuals when designing loB deployments.
- Ensure stability and consistency by establishing a framework for privacy, security, ethics and interconnectivity. Require all connected entities to subscribe and adhere to the framework to further reduce unintended consequences.

Further Reading:

[Move to Contextual Privacy in Digital Society](#)

[Geopolitical Ideologies Are Shaping Our Digital Future](#)

Total Experience

Analysis by Jason Wong, Michael Chiu, Michelle Duerst, Brent Stewart, Don Scheibenreif

SPA: By 2024, organizations providing a total experience will outperform competitors by 25% in satisfaction metrics for both customer and employee experience.

Description:

Total experience (TX) is a strategy that creates superior shared experiences by interlinking the multiexperience (MX), customer experience (CX), employee experience (EX) and user experience (UX) disciplines. Organizations need a TX strategy because they must continuously enhance their CXs and EXs, especially as these interactions have become more mobile, virtual and distributed, mainly because of COVID-19. TX is about more than improving the experience of one constituent — it improves experiences at the intersection of multiple constituents to achieve a transformational business outcome. These intersected experiences are key business moments. They require organizations to rethink how they change behavior and technologies by addressing the feelings, emotions and memories that make up the CX and EX, as well as the experience of partners and other constituents.

Excellence in the activities of any one of the CX, EX, UX and MX disciplines can result in operational effectiveness, but competitors can imitate these activities, resulting in competitive parity. In contrast, TX strategy is composed of tightly linked, differentiated groups of activities across these disciplines that mutually reinforce each other. They are harder for competitors to copy and thus more sustainable. ³

TX removes the silos in which CX, EX, UX and MX activities traditionally run. This creates business advantages and resiliency in the digital experience economy. TX links and mutually reinforces these activities at a higher level to form superordinate activity clusters with strategic fit. This leads to superior CXs and EXs, as well as more positive business outcomes. Internally, TX exponentially increases the value of each discipline because the individual practices improve based on lessons from the others.

Why Trending:

Twenty years into the experience economy, expectations and demands from customers and employees continue to change. That's because CXs and EXs are constantly evolving, driven by new interactions. This leads to participation, then to engagement, and on to satisfaction, loyalty and advocacy. UX is about the usability and design of apps and products to reduce effort, increase engagement and drive satisfaction. MX is about the technical implementation across a wide range of devices, touchpoints and modalities of interaction. Organizations were investing in these disciplines before the pandemic, such as with an omnichannel strategy. But the pandemic has increased the need to transform the digital experience, moving from keyboards and screens to multiple modalities using conversational, immersive and touchless environments. The business moments in which experiences between customers, employees, partners and "things" are inextricably interlinked are particularly important.

TX can solve business problems with mutual benefits for all. When linkages are made, advantages can be gained:

- **UX and EX:** Employees with a high-quality UX are at least 1.5 times more likely to have high levels of work effectiveness, productivity, intention to stay and discretionary effort. ⁴
- **EX and CX:** Seventy-seven percent of employees Gartner surveyed see a strong relationship between their daily experience and the quality of CX. ⁵

Businesses recovering from the pandemic must look for strategies that help them capitalize on the new experiential disruptors and achieve differentiation. COVID-19 is driving a big increase in remote, mobile, virtual, and distributed customer and employee interactions. For example, during the first few days of the lockdown in Italy, the country's overall online sales doubled. ⁶ Supporting employees working remotely risks increasing the long-standing silos separating CX, EX, UX and MX. Continuing to rely on pre-COVID-19 approaches to these disciplines for interactions is a dubious path to success in the "next normal" environment. Additionally, information on best practices in CX, EX, UX and MX silos is widely available, so organizations often follow the same practices. TX identifies new activities for the organization that are different from those of competitors, and novel ways of interlinking and mutually reinforcing activities.

Implications:

TX solves complex business challenges by transforming experiences. Verizon's store experience transformation in response to COVID-19 is an excellent example of what a TX strategy can achieve. To improve CX, specifically customer safety, Verizon enhanced both UX and MX, while keeping in mind EX. It started by deploying an online appointments system and integrated it with its My Verizon app. When customers get within 75 feet of a store, they receive a notification. This guides them through a check-in process. It tells customers how long they may have to wait outside to ensure social distancing and improve the CX within the store. Verizon also introduced more digital bill-payment kiosks to minimize direct interactions between customers and employees. Verizon uses MX and EX to enable employees to use their tablets for co-browsing with customers' devices and guide them without having to touch the hardware. ⁷

A TX strategy ensures the right leaders across CX, EX, UX and MX collaborate to identify and remove impediments, uncover opportunities in their disciplines and work toward an integrated solution. TX must include each experience discipline. An organization needs representation from all four disciplines to remove impediments, link the disciplines and drive the TX transformation. Representation is vital to:

- **Align with customers.** With a strong CX, the solution will resonate more with customers.
- **Enable employees.** With a strong EX, employees will be more engaged and enabled, and there'll be more support for the solution.
- **Adopt the solution.** With a strong UX, the solution will be intuitive to use.
- **Implement the solution.** With MX, the solution will improve performance and be versatile.

Actions:

- Engage with CX, EX, UX and MX leaders or centers of excellence across your organization to form a TX "fusion team" that crosses activity silos.
- Identify critical gaps in customer and employee interactions exposed by the pandemic. Determine new targeted business outcomes to address using TX.
- Find important business moments that have been held back by their CX, EX, UX or MX, then apply TX.

Further Reading:

[Build Links Between Customer Experience, Multiexperience, User Experience and Employee Experience Success in the Digital Experience Economy Requires Connecting MX, UX, CX and EX](#)

[Transcend Omnichannel Thinking and Embrace Multiexperience for Improved CX](#)

Privacy-Enhancing Computation

Analysis by Bart Willemsen, Ramon Krikken

SPA: By 2025, 50% of large organizations will adopt privacy-enhancing computation for processing data in untrusted environments and multiparty data analytics use cases.

Description:

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.

Each technology provides specific secrecy and privacy guarantees, and some can be combined for greater efficacy.

Why Trending:

Global data protection legislation is maturing and, with the unstoppable pervasiveness of personal data, every organization that processes personal data faces ever-higher privacy and noncompliance risks.⁸ At the same time, organizations now realize the economic potential of their data repositories.^{9,10} The demand for processing data in untrusted environments and performing multiparty data sharing and analytics is rapidly growing. The increasing complexity of analytics engines and architectures mandates a by-design privacy capability, rather than a bolt-on approach. Unlike common data-at-rest security controls, privacy-enhancing computation protects data in use, thus enabling the use cases described previously, while maintaining secrecy or privacy. As a result, organizations can implement data processing and analytics that were previously impossible because of privacy or security concerns.

Implications:

Hyperscale cloud providers have started to offer trusted execution environments. Organizations can use them to provide enhanced security and privacy in cloud environments. Other technologies, such as homomorphic encryption, secure multiparty compute and private information retrieval have transitioned from academic research projects to commercial solutions. Adoption is nascent, but implementations

exist in fraud analysis, intelligence operations, finance and healthcare. These implementations follow one of two use-case patterns:

- A third-party organization analyzes data from one or more organizations, without these organizations providing full access to their data
- Multiple organizations pool their data for joint analytics without having access to each other's underlying data

Actions:

- Identify candidates for privacy-enhancing computation by assessing data processing activities that require the use of highly sensitive personal data for data monetization, fraud analytics and business intelligence use cases.
- Assess the differences in effectiveness and implementation needs of differential privacy, homomorphic encryption, secure multiparty computation, trusted execution environments and other approaches for these use cases.

Further Reading:

[Hype Cycle for Privacy, 2020](#)

[Hype Cycle for Data Security, 2020](#)

[Achieving Data Security Through Privacy-Enhanced Computation Techniques](#)

Location Independence

Distributed Cloud

Analysis by David Smith, Ed Anderson, David Wright, Arun Chandrasekaran, David Cearley

SPA: By 2025, more than 50% of organizations will use a distributed cloud option at the location of their choice, enabling transformational business models.

Description:

Distributed cloud is the distribution of public cloud services to different physical locations while operation, governance and evolution of the services remain the responsibility of the public cloud provider.

Distributed cloud addresses the need for customers to have cloud computing resources closer to the physical location where data and business activities happen. This could be, for example, in an enterprise

data center, a telco 5G network or even on a manufacturing floor. The use cases for this option are normally associated with:

- Low-latency scenarios such as high-speed trading
- Data cost reduction scenarios such as data gathering and use for machine learning
- Data residency scenarios where law dictates that data must remain in a specific physical location

Distributed cloud brings together edge, hybrid and new use cases for cloud computing. It represents the future of cloud computing and addresses the issue of location in that future. Distributed cloud is a key enabler of the anywhere operations trend. Although cloud computing doesn't restrict location, most people view it as tied to its most common configuration — "centralized."

As distributed cloud evolves, we predict a time when customers will ask a cloud provider for cloud resources that comply with certain general performance requirements (e.g., capacity, latency, residency or cost). Distributed cloud also signals a future in which physical resources are repurposed to host distributed cloud services (e.g., smart buildings, and new opportunities to use assets owned by telcos and governments). It potentially supports the sale of excess compute capacity in a data center back to a cloud provider (similar to selling solar-generated power back to a utility).

Why Trending:

Interest in hybrid cloud computing is rising. The main reason for this is that many customers need to deal with technologies they already own and operate, often within their own data centers.

These customers can't abandon existing technologies in favor of complete and immediate migration to the public cloud. Sunk costs, latency requirements, regulatory and data residency requirements, and even the need for integration with noncloud, on-premises systems hold them back. Instead, they use a combination of private-cloud-inspired and public cloud styles of computing. This creates a hybrid IT environment.

Organizations are advancing use cases of cloud computing in ways that deliver it at the point of need using distributed cloud. It's vital to identify and exploit evolving models of cloud computing deployment to take advantage of business opportunities.

Uncertainty caused by the COVID-19 pandemic has given cloud computing the opportunity to prove itself. It has delivered well, removing doubts. It has demonstrated resilience and agility, unlike other modern constructs such as just-in-time delivery.

Implications:

Distributed cloud can solve different types of problems as shown by the “distributed cloud continuum” and the following five styles:

- **On-premises public cloud:** Deployment into a customer’s private data center. The control plane for operation and the security perimeter are defined by, and in the control of, the public cloud provider’s public cloud. Most initial deployments will keep access credentials private to the customer.
- **IoT edge cloud:** Delivery of a distributed cloud substation designed to interact directly with edge devices, or enable edge devices to host public cloud services. This style includes IoT consumer and industrial capabilities, and supports use cases such as collection, dissemination and movement. As with on-premises public cloud, these resources may be restricted in access and visibility to a single company if needed. Most cloud providers offer edge support and data-oriented edge devices. Most don’t yet offer fully distributed cloud options, but are evolving them.
- **Metro area community cloud:** Delivery of cloud substations as local capabilities for a city or metro area. The delivery isn’t necessarily in a data center and is open to enable virtual private cloud connections. Multiple customers connect to these local resources. Amazon Web Services (AWS) and Microsoft have moved into zone-based approaches that support this option.
- **5G mobile edge cloud:** Delivery and integration of a distributed cloud substation into a 5G telco/carrier network. This model uses the telco’s customer relationships, partner network and 5G speeds. Example providers include AWS, Microsoft, Google and IBM.
- **Global network edge cloud:** Delivery of a variety of distributed cloud substations designed to integrate with global network infrastructure, such as points of presence, cell towers, content delivery networks, routers and hubs. Any network point of connectivity, transport or interaction could potentially host such a substation. Typically, this will require specific hardware designs to support. This style isn’t yet generally available.

Actions:

- Communicate the benefits of using the distributed cloud to change stakeholders’ mindsets. This will be vital before any organization will allow another company to control its assets on-premises.
- Use distributed cloud models as an opportunity to prepare for the next generation of cloud computing by targeting location-dependent use cases. Exploit the flexibility offered by the increased deployment options of cloud computing.
- Identify use cases for future phases of distributed cloud (such as low latency, tethered scale and data residency) that are enhanced by using distributed cloud substations.

Further Reading:

[‘Distributed Cloud’ Fixes What ‘Hybrid Cloud’ Breaks](#)

Define and Understand New Cloud Terms to Succeed in the New Cloud Era

How to Bring the Public Cloud On-Premises With AWS Outposts, Azure Stack and Google Anthos

Anywhere Operations

Analysis by Manjunath Bhat, Tony Harvey

SPA: Through 2023, 40% of organizations will blend virtual and physical experiences, leading to increased workforce productivity and customer reach.

Description:

Anywhere operations describes a business operating model designed to reach customers anywhere, enable employees anywhere and use digital technologies to deliver business services anywhere. It challenges the conventional wisdom that it's necessary to be in a specific location, interacting face to face, to maximize value and efficiency. It drives a next normal in which employees, contractors, business partners, customers and end consumers will be remote from each other.

A digital-first, location-independent mindset is a prerequisite to anywhere operations. 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.

Technologies that enable a perimeterless digital workplace provide the foundation for anywhere operations. 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:
 - Artificial intelligence for IT operations (AIOps), endpoint management, SaaS management platforms, self-service and zero-touch provisioning

Why Trending:

Organizations that emerge successfully from the COVID-19 pandemic will have an anywhere operations foundation. Organizational preparedness and resilience to cope with the crisis depend largely on the maturity and readiness of digital capabilities. The 2020 Gartner CEO Survey indicates that before COVID-19, half of CEOs expected a downturn. However, only 9% braced for the impact.¹¹ The crisis has accelerated plans for digital transformation and digital workplace initiatives that organizations either put on hold or defunded:

- Most of the infrastructure and operations leaders at a virtual Gartner forum said they resumed their plans to roll out cloud services for employee collaboration and digital experience monitoring in addition to zero-trust security capabilities.¹²
- In a Gartner poll of 317 CFOs and finance leaders, almost a quarter of respondents said they would move at least 20% of their on-site employees to permanent remote positions.¹³
- Consumers' demand for digital services increased because of stay-at-home orders and physical distancing norms caused by COVID-19. Organizations that move to digital business models to support their customers and employees will rebound faster than others.

Implications:

Anywhere operations isn't only about remote working as there are practical needs that demand physical proximity to people and equipment. In such cases, anywhere operations uses contactless interactions but preserves the unique value of the personal interaction.

The optimal experience for employees and customers will depend on their specific contexts. The context can be categorized as spaces that organizations either control or don't control. For example, factories and retail stores are examples of environments that organizations can control. Users' homes, personally owned devices and public spaces are examples of environments that organizations can't control. Anywhere operations must contextualize the delivery of value across each of these environments.

The workplaces of the future will evolve in response to the pandemic regardless of whether they're offices for knowledge workers or automobile manufacturing plants. The changes will include the adoption of remote support technologies using mobile devices, wearables and augmented reality headsets. Contactless and passwordless interactions using IoT sensors, smart cards enabled by near-field communication and wearables will become the norm for mundane transactions such as unlocking physical access to restricted spaces, and operating elevators or vending machines.

Several banks now have a mobile-only presence. For example, Banco Sabadell in México and DBS Bank in Singapore provide digital services going beyond funds transfer and paying bills to include account opening. This is an example of democratized access to services by making services more accessible to consumers anywhere. The surge in online learning through massive open online courses using streaming technologies democratizes access to knowledge and high-quality education.

To support frontline workers, digital collaboration tools such as Microsoft Teams and Google Meet enable employees to share information in real time. For example, Microsoft Teams includes a Walkie Talkie mode (a push-to-talk experience) that enables users to broadcast messages to their “channels.” First responders and paramedics can use this feature to stay in touch with each other in emergency situations regardless of their location and on the smartphones they already use. Anywhere operations augments frontline customer service technicians by combining a voice-controlled input interface and augmented reality glasses.

Actions:

- Enhance employee experience in a perimeterless work environment using digital experience monitoring, endpoint analytics, self-service provisioning and remote troubleshooting tools.
- Enable frontline workers to be productive by giving them augmented reality wearables for remote support and voice-controlled collaboration tools.
- Adopt team structures, processes, skills and tools to drive business model innovation using a digital-first, location-independent strategy.
- Invest in distributed cloud and edge technologies that enable the building of a blended workplace to seamlessly move work environments between physical and virtual locations.

Further Reading:

[4 Steps to Implement a Perimeterless Digital Workplace](#)

[Tool: Prepare I&O for the Everywhere Enterprise](#)

[I&O Leaders Must Transform Their Teams to Lead With SaaS Cloud](#)

Cybersecurity Mesh

Analysis by Jay Heiser

SPA: By 2025, the cybersecurity mesh will support over half of digital access control requests.

Description:

The cybersecurity mesh is a distributed architectural approach to scalable, flexible and reliable cybersecurity control. Most assets and devices are now located outside the old “walls” of the organization. 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. This architecture allows the identity to become the security perimeter. It’s a key enabler of the anywhere operations trend.

The cybersecurity mesh centralizes policy orchestration and decision making in a distributed policy enforcement architecture:

- The decision component quickly and reliably verifies the identity, context and policy adherence of the specified participants. This component is a cloud-delivered trust service.
- The enforcement component (agents or proxies) applies the decision to the IT asset. This component is located in the public cloud or immediately in front of or with the asset, whichever is most practical.

This modular architectural approach to cybersecurity is rapidly becoming the default choice for:

- The identify fabric
- Content control (secure web gateway [SWG] and email security)
- Security configuration management (mobile device management, endpoint protection platforms and cloud workload protection platforms)
- Event management (endpoint detection and response, and extended detection and response)

The scalability and flexibility of the cybersecurity mesh are critical for some of the fastest-growing cybersecurity markets, including ZTNA, cloud access security brokers (CASBs) and SASE. The cybersecurity mesh is the security architecture for a cloud-oriented, API-based world.

Why Trending:

The COVID-19 pandemic has accelerated the multidecade process of turning the digital enterprise inside out. We’ve passed an inflection point — most organizational cyberassets are now outside the traditional physical and logical security perimeters. However, as the extended enterprise weakens our ability to control access to our critical digital assets, citizen and consumer expectations about data protection continue to grow.

In the past, a few security servers demonstrated the feasibility of making real-time trust decisions for distributed digital assets, but the approach had limited applicability. Today, cloud-based security services provide this function. Cloud computing offers the scalability and accessibility necessary to host security services that can reliably and conveniently support a global cybersecurity mesh. Although many cybersecurity professionals were originally skeptical about the security of the public cloud, years of safe service have changed that perception.

Two main factors make the mesh approach attractive:

- All assets are dispersed across the network, requiring a distributed approach.
- The foundational technologies now exist to make it practical.

The cybersecurity mesh is a convergence of new need and new security services. Although security leaders understood this architectural model 20 years ago, they lacked incentive and a convenient set of technologies. It was too much work for too little benefit. That has changed. Now, with security services, the cloud can protect the cloud. As a result, dependence on cloud-based trust services is far more acceptable than it was several years ago. Gartner's research indicates that 80% of organizations expect to be using security as a service by 2023. ¹⁴

As anywhere operations continues to evolve, the cybersecurity mesh will become the most practical approach to ensure secure access to, and use of, cloud-located applications and distributed data from uncontrolled devices. The modularity and, therefore, composability of this architecture make it well-suited to integration in a growing variety of extended-enterprise scenarios.

Implications:

The market for internet security is under pressure to adapt to digital transformation changes in end-user organizations. The most profound impact of this on organizations is the rapid migration to offerings using the cybersecurity mesh, especially network security as a service supporting or incorporating ZTNA. The demands for simplicity, scalability, flexibility and low latency are also driving a convergence of the security and WAN edge markets. The framework for handling this convergence is SASE, a cloud-based service delivery model. Organizations that want to prepare for a graceful transition to the next decade must reconceptualize their networking approach to a model that enables plasticity. For many organizations, the cultural issues of "this is not how we do security" will be more challenging than the actual implementation of a service-delivered model that defines both security and performance through software.

Organizations that will be successful tomorrow are already using multiple forms of cybersecurity mesh services. They're also exploring additional use cases. This flexible security architecture is a pragmatic fit for the awkward access control needs of application-to-application authentication and the support of device-to-application authentication.

Actions:

- Use cloud-delivered services to provide location-independent cybersecurity controls, encompassing the organization's anywhere operations.
- Transition from clumsy traditional VPNs by using cloud-delivered ZTNA for reliable and scalable secure remote access.

- Explore a gateway approach to SaaS access control, using a CASB or SWG, when adaptive access control and real-time traffic inspection are required.
- Challenge network security engineers to develop organizational zero-trust service delivery models for secure and high-performance access to cloud applications.

Further Reading:

[Top Security and Risk Management Trends](#)

[Emerging Technology Analysis: SASE Poised to Cause Evolution of Network Security](#)

[Guide to Cloud Security Concepts](#)

Resilient Delivery

Intelligent Composable Business

Analysis by Andrew White, Gene Alvarez, Dennis Gaughan, Yefim Natis

SPA: By 2023, organizations that have adopted a composable approach will outpace competition by 80% in the speed of new feature implementation.

Description:

An intelligent composable business is one that drives superior business outcomes that are timely, relevant and contextual. It does so by having the plasticity to fundamentally reengineer business decisions and orchestrate capabilities that adapt at the pace of business change. Organizations, driven by the ever-increasing pace of that change, are accelerating their digital business strategies. As a result, they need to quickly make business decisions in support of business moments, informed by relevant data. They must then adapt their capabilities to act on those decisions in near real time. To do this, organizations must rethink how they make decisions. They must build a roadmap to an architecture that:

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

Why Trending:

Business moments warrant a new way to make decisions and respond to environmental conditions at the speed of business. Decision making no longer occurs solely along functional lines within organizations. It occurs along collaborative pathways across multiple communities that are engaged

based on the context of what's happening, the related outcomes and the decisions to be made. Collaborations are increasingly between humans and machines. Reengineering the decision is about rethinking how decision making occurs in every context within an organization and assuming it will occur with machine augmentation enabled by a rich fabric of data and insights.

How decisions are made is at the center of every business moment and every digital transformation. Gartner surveyed almost 5,000 employees to assess the analytic and technology activities in their jobs. It found that more than 40% of employees have become "technology producers" to aid, improve or speed decision making.¹⁵ And data and analytics are at the heart of how decisions are made. To succeed in today's digital economy, organizations must make data-driven decisions that:

- Are informed by external events and data
- Are enriched by collective knowledge
- Are repeatable
- Tap into and build on communal learning
- Can adapt rapidly to new scenarios

But these newly reengineered decisions require a new platform for development, assembly and deployment. Current or monolithic application and app development environments aren't helping. DevOps and other new operational practices are helping, but a new architecture is needed. Composable applications provide the building blocks to assemble needed packaged business capabilities to help execute decisions. They provide the flexibility to adapt as information emerges or assumptions change.

Composability provides an application, AI, and a data and analytics platform for building and operating recomposable digital experiences. A range of services supports and operationalizes composable business moments and their attendant decisions. The intelligent composable business makes this happen by assembling and combining packaged business capabilities and packaged data capabilities that the organization has bought or developed. It's guided in that assembly by the intention of the decision to be made to exploit the business moment and the actions needed to successfully execute that decision to deliver a positive business outcome.

Implications:

Decision making is not about dashboards or reports; it's about increasing autonomy, enrichment and augmentation of how decisions are made (by human or machine) at every level of the organization. Intelligent composable business will unleash creativity and innovation. It will also reduce costs, while driving the discovery of new business value and business models founded on data value and on being data-driven. Data and analytics, including AI and applications, will merge at the point of a business moment, turned into value for all stakeholders.

Composable business moments that emerge in customer engagement, employee interactions, machine transactions or ecosystem partnerships will be reengineered to exploit these new capabilities. They will be adaptable and resilient, and capable of being recomposed as needed, enabling organizational plasticity. For example, they'll enable an organization to shift from a primarily B2B business model to include B2C commerce capability to remain in business when COVID-19 has shut the main route to customers. Or they'll provide a retail bank with the ability to identify trends in customer behavior, enabling it to decide to quickly assemble a new service (which may be a new assembly of existing services). This will enable it to target new customers or perhaps defend against nontraditional market entrants and increase top-line revenue.

This trend paves the way for:

- New business models
- Autonomous operations
- Redesigned digital business moments
- New products, services and channels, which will result in significant shifts in market and industry dynamics, public-sector service levels and mission attainment

This trend recognizes the increased importance of technology in delivering business capabilities. It uses the broader technology skill set that exists inside and outside the traditional IT organization.

Actions:

- Start your reengineering practice by examining how your organization makes business decisions. Identify the most important decisions that affect your business — those in which you can have immediate impact.
- Identify application friction points where the pace of business change exceeds the pace of technology change. Use those gaps to begin your modernization roadmap. Assess new application vendors not only on features, but on the abilities of their application platforms to extend and integrate core application capabilities.
- Develop a unified application and data and analytics strategy. Ensure it embeds the concept of reengineered composable decision making at the core of digital business and your accelerating transformation.

Further Reading:

[Improve Decision Making Using Decision Intelligence Models](#)

[How to Activate Metadata to Enable a Composable Data Fabric](#)

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

AI Engineering

Analysis by Erick Brethenoux

SPA: Through 2023, at least 50% of IT leaders will struggle to move their AI predictive projects past proof of concept to a production level of maturity.

Description:

AI engineering is a discipline focused on the governance and life cycle management of a wide range of operationalized AI and decision models. These include machine learning, knowledge graphs, rules, optimization, and linguistic and agent-based models. AI engineering methods also enable the governance and procedures for retuning, reusing, retraining, interpreting or rebuilding AI models. These methods aim to provide an uninterrupted flow between the development, operationalization and full maintenance of AI models. AI engineering ensures the efficient operationalization of AI techniques, which is vital for AI to generate significant value over time.

AI engineering also deals with the combination of AI techniques (or composite AI). Organizations are combining different AI techniques to:

- Improve the efficiency of learning
- Broaden the level of knowledge representations
- Solve a wider range of business problems more efficiently

As AI techniques don't only solve problems but are starting, creatively, to generate solutions, generative AI techniques are also coming under the purview of the AI engineering discipline. Organizations can use generative AI algorithms to create models of things that don't exist in the real world. Generative models have the potential to affect many creative activities. These range from content creation (art, stories and marketing materials) to many types of design (architecture, engineering, pharmaceuticals, fashion, industrial and process). Organizations can use generative models for the inverse design of materials to target specific properties. They can also use them to create synthetic data.

Why Trending:

Marketing hype and unreasonable expectations are still increasing confusion about AI. As a result, many organizations struggle to put a realistic value on this important source of innovation and differentiation. Business leaders tend to overestimate the impact of AI and underestimate its complexity. This means it's important to manage their expectations, or risk costly project failures. Organizations face challenges — involving integration, security and privacy issues — that prevent them from efficiently moving their AI practices from prototypes to production.

AI engineering brings together various disciplines from across the organization to tame that hype, while providing a clearer path to value when operationalizing the combination of multiple AI techniques. Generative models have the potential to fundamentally change the creative process based on trial and error with technology that accelerates and improves design processes.

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.

Implications:

Lack of AI engineering will increase organizations' inability to move AI projects beyond pilots into production, which could result in fatigue and skepticism of AI as a transformative technology. Most AI projects fail because those running them address operationalization too late, as a DevOps consideration. A Gartner survey indicated that one of the top three barriers to AI implementation is the complexity of AI solution integration with existing infrastructure.¹⁶ AI efforts face significant maintainability, scalability and governance challenges once in production.

But combining AI techniques offers two main benefits in the short term:

- It brings the power of AI to a broader group of organizations that don't have access to large amounts of historical or labeled data but possess significant human expertise. Composite AI is one of the strategies for dealing with "small data."
- It helps to expand the scope and quality of AI applications because more types of reasoning challenges and required intelligence can be embedded in composite AI.

Other benefits, depending on the techniques applied, include better interpretability and support for augmented intelligence.

In the longer term, generative AI techniques will fundamentally change industries including manufacturing, architecture, aerospace, pharmaceuticals and the media. The benefits to society are potentially significant; for example, AI research is underway to support the formulation of new drugs for pandemics.

A robust AI engineering strategy will facilitate the performance, scalability, interpretability and reliability of AI models, while delivering the full value of AI investments.

Actions:

- Minimize the technical debt and complex maintenance procedures for operationalizing AI models. Do so by establishing AI engineering practices aimed at reviewing and revalidating the models' business value on an ongoing basis.
- Align all stakeholders with measurable business outcomes and the trustworthiness of results by including the three core teams — business, data science and IT — throughout the life cycle of the AI model.
- Strengthen your AI production efforts by identifying the AI skills within your organization, addressing integration issues in the prototype phases and combining AI techniques to achieve their full representational power.
- Use domain knowledge and human expertise to provide context to, and complement, data-driven insights. Do so by using composite AI and applying decision design principles with business rules, knowledge graphs or physical models in conjunction with machine learning models.

Further Reading:

[What Is Artificial Intelligence? Seeing Through the Hype and Focusing on Business Value](#)

[Use Gartner's 3-Stage MLOps Framework to Successfully Operationalize Machine Learning Projects](#)

[Use 3 MLOps Organizational Practices to Successfully Deliver Machine Learning Results](#)

Hyperautomation

Analysis by Frances Karamouzis, Nicole Sturgill, Laurie Shotton, Stephanie Stoudt-Hansen

SPA: By 2024, organizations will lower operational costs by 30% by combining hyperautomation technologies with redesigned operational processes.

Description:

Business-driven hyperautomation is a disciplined approach that organizations use to rapidly identify, vet and automate as many business and IT processes as possible. Hyperautomation involves the orchestrated use of multiple technologies, tools or platforms. Examples of these include AI, machine learning, event-driven software architecture, robotic process automation (RPA), intelligent BPM suite, integration platform as a service, low-code tools, and other types of decision, process and task automation tools.

Why Trending:

Hyperautomation has been trending at an unrelenting pace over the past few years, mainly because of the pent-up demand for operationally resilient business processes. Organizations have a tremendous

amount of “collective” debt (technical, process, data, architecture, talent and social) that significantly affects their value proposition and brand (see Note 2 for our definition of collective organizational debt). The cause is an extensive and expensive set of business processes underpinned by a patchwork of technologies that are often not optimized, lean, connected, consistent or explicit.

Business executives are demanding a path to digital operational excellence. This is creating huge unmet demand for speed, efficacy and democratization of process automation and data integration. This has triggered an enormous backlog of requests from business stakeholders for automation using one or more technologies.

In 2019, CEOs were demanding a path to digital operational excellence — they ranked outdated work processes as their top challenge.¹⁷ In 2020, the pandemic accelerated a “default is digital” requirement, with many employees needing to work from home and digital customer service becoming a necessity. COVID-19 demands resilience, efficiency, agility and productivity. To enable this, organizations had to digitize their documents/artifacts and ensure their business and IT process workflows were digital. This created great demand to automate as many processes as possible for speed, efficacy and minimal-level processing. The trend is moving toward operational resiliency.

Implications:

The collective impact of these business and IT realities is the launch of many initiatives (often disparate and siloed) aimed at applying automation across knowledge work for either efficiency, efficacy or business agility. Gartner estimates that more than 70% of large commercial organizations have dozens of hyperautomation initiatives underway.

The organizational zeal for using hyperautomation has led to many new offerings, vendors and commercial models across an extensive number of technology markets. Gartner is tracking well over 200 different hyperautomation offerings, many of which are targeted or from pure-play providers. Beyond that, digital giants such as Microsoft, SAP and IBM have entered seemingly targeted software categories such as RPA.

Another indicator of demand is the equity investment in some hyperautomation technologies. For example, the total funds AI startups have raised over time reached \$61.6 billion in 2Q20.¹⁸ If we add investment in other high-growth technology areas such as RPA, chatbots and conversational platforms, the impact is clear — the levels are unprecedented.

In September 2020, we conducted a poll of business and IT stakeholders that showed investment in AI has continued unabated despite the crisis. Seventy-five percent of respondents said they would continue or start new AI investments in the next six to nine months, and 66% said they would increase or not change AI investment strategies in place at the start of the crisis.¹⁹

Hyperautomation is irreversible and inevitable. Everything that can be automated will be automated. Competitive pressures for efficiency, efficacy and business agility are forcing organizations to address

back-, middle- and front-office operations. Organizations that resist the pressures will struggle to remain competitive or to differentiate.

Actions:

- Plan for a mandate that everything that can be automated will be automated.
- Use automation to optimize and accelerate experimentation of new value streams.
- Demand holistic mapping of collective initiatives, rather than islands of task automation.
- Prioritize IT investments based on an iterative multiyear journey involving many business-driven hyperautomation initiatives.
- Architect and plan for multiple concurrent initiatives to drive operational resiliency, efficiency, agility and productivity, while optimizing ongoing management, governance and debt.
- Use fusion teams throughout the iterative process of designing, building, scaling and governing your hyperautomation roadmap.

Further Reading:

[Tool: Banking and Insurance Use Cases to Drive Hyperautomation](#)

[Move Beyond RPA to Deliver Hyperautomation](#)

[The CIO's Guide to RPA and Introduction to Hyperautomation](#)

Evidence

¹ [Facebook Data Misuse and Voter Manipulation Back in the Frame With Latest Cambridge Analytica Leaks](#), TechCrunch.

² [How China Surveils the World](#), MIT Technology Review.

³ [What Is Strategy?](#) Harvard Business Review.

⁴ See Figure 2 in [Proven Design Principles to Deliver a High-Value Employee User Experience](#)

⁵ See Figure 2 in [How Customer Centricity Improves Both Customer and Employee Experience](#)

⁶ [Consumer Spending Tracker for MULOC Retailers](#), IRI.

⁷ [Verizon's CIO Is Helping the Telecom Giant Adapt Swiftly to a Contactless World](#), Forbes.

⁸ Respondents to the 2020 Gartner Security and IAM Solution Adoption Trend Survey named the following as the top three factors likely to affect their organizations' information security function and controls in the next three to five years:

- Increasing regulations
- An evolving threat landscape
- IoT and system security

Gartner conducted the study online during March and April 2020. The study's aim was to learn which security solutions were benefiting organizations and which factors were affecting organizations' choice of such solutions. The 405 respondents came from North America, Western Europe and the Asia/Pacific region. Their companies were in different industries and had annual revenue below \$500 million. Respondents were at manager level or above (excluding the C-suite) and had primary involvement in, and responsibility for, risk management.

Gartner analysts developed the study collaboratively with the primary research team that follows security and risk management.

⁹ Seventy-eight percent of respondents to the 2021 Gartner View From Board of Directors Survey considered analytics to be a top three game-changing technology for their industry.

Gartner conducted the study to understand how boards of directors viewed the effect on their organizations of digital-business-driven business model evolution.

Gartner conducted the research online during May and June 2020 among 265 midsize, large or global enterprises in the U.S., Europe and the Asia/Pacific region. The respondents were board directors or members of corporate boards of directors. Respondents who served on multiple boards answered for the largest company, defined by its annual revenue, for which they were board members.

¹⁰ Most respondents to the 2019 Gartner Chief Data Officer Survey shared data assets internally and externally as part of a short-term plan for generating economic benefits from available data assets.

Gartner conducted the study to explore the business impact of the chief data officer (CDO) role and the office of the CDO. Gartner conducted the research online from September through November 2019 among 293 respondents across the world. Respondents were CDOs or chief analytics officers, or had the responsibilities of an executive-level data and analytics (D&A) leader (if their organization lacked an official C-level D&A title). Gartner obtained the survey sample from a variety of sources, including LinkedIn. The greatest number came from a Gartner-curated list of more than 2,000 CDOs and other high-level D&A leaders.

¹¹ [2020 Gartner CEO Survey: The Year of Recession](#)

¹² On 31 March and 1 April 2020, Gartner hosted a virtual forum for 49 heads of infrastructure and operations based in North America on their response to the COVID-19 pandemic. Gartner asked the participants: “Has COVID-19 enabled you to accelerate planned initiatives?” Most of the 29 respondents said “Yes.” The survey sample was small, so view the results as indicating a direction only.

¹³ This is a finding from a Gartner poll conducted in an April 2020 webinar. See [Gartner CFO Survey Reveals 74% Intend to Shift Some Employees to Remote Work Permanently](#). Gartner Newsroom.

¹⁴ Gartner asked respondents to its 2020 Security & IAM Solution Adoption Trends Survey:

“Are any of your organization’s information security products delivered as a service?”

Of the 396 respondents, 43% were delivering them as a service and 37% planned to within three years. We excluded those who answered “don’t know” from the results.

Gartner conducted the study online during March and April 2020. The study’s aim was to learn which security solutions were benefiting organizations and which factors were affecting organizations’ choice of such solutions. The 405 respondents came from North America, Western Europe and the Asia/Pacific region. Their companies were in different industries and had annual revenue below \$500 million. Respondents were at manager level or above (excluding the C-suite) and had primary involvement in, and responsibility for, risk management.

Gartner analysts developed the study collaboratively with the primary research team that follows security and risk management.

¹⁵ Gartner conducted the 2020 Digital Friction Survey online. The 4,977 respondents worked in a range of functions, industries and regions, and at different levels. A team of Gartner researchers developed the survey. Gartner’s Quantitative Analytics and Data Science team reviewed, tested and administered it.

¹⁶ The 2019 Gartner AI in Organizations Survey aimed to uncover the keys to successful AI implementations and the main barriers to the operationalization of AI. Gartner conducted the survey online during November and December 2019 among 607 respondents from organizations in the U.S., Germany and the U.K. Gartner established quotas to ensure the sample was a good representation across industries and company sizes. Surveyed organizations had developed AI or intended to deploy it within three years.

Respondents:

- Were part of their organizations’ corporate leadership or reported to corporate leadership
- Had a high level of involvement with at least one AI initiative
- Were responsible for one of the following in their organizations:

- Determining AI business objectives
- Measuring the value derived from AI initiatives
- Managing the development and implementation of AI initiatives

Gartner analysts developed the study collaboratively with Gartner's primary research team. See [Survey Analysis: Moving AI Projects From Prototype to Production](#).

¹⁷ Respondents to Gartner's Second Annual Tech CEO Survey, 2020 ranked the following as their top five challenges:

1. Outdated work processes
2. Outdated organizational structures
3. Misaligned talent management processes
4. Misaligned leadership styles
5. Ineffective coordination across the executive team

Gartner conducted the survey online between December 2019 and February 2020. The 285 respondents were in North America (the U.S.), Western Europe (Italy, France, Germany, Spain, the U.K.) and the Asia/Pacific region (Australia, India, New Zealand, Singapore).

The respondents' organizations operated in the high-tech industry. Respondents were CEOs/managing directors, owners or COOs/C-level executives of operations or equivalent.

¹⁸ [Artificial Intelligence Startups Raised \\$61.6bn in Total Funding, a 35% Jump in a Year](#), insideBIGDATA.

¹⁹ On 24 September 2020, Gartner conducted a poll of attendees of our webinar, [Drive Strategic Mandates for AI in the Enterprise](#). Approximately 200 business and IT professionals responded to our polling questions.

Note 1: Operant Conditioning

In 1937, psychologist B.F. Skinner coined the term operant conditioning, thereby formalizing the age-old learning method of reward and punishment. Through operant conditioning, an individual makes an association between a specific behavior and a consequence that shapes human behavior.

Note 2: Collective Organizational Debt

Collective organizational debt is made up of many elements, including:

- **Technical debt** — Deviation of an application from any nonfunctional requirement.
- **Process debt** — Suboptimal activity or process that might have some benefits, but generates a sustained negative impact on cycle time, error rates, quality, consistency, complexity or customer experience.
- **Data debt** — Lack of, or suboptimal access to, current or accurate data within the demand latency period.
- **Architecture debt** — Suboptimal solutions from an optimized architectural construct. This may lead to security issues, latency and redundancy (in applications, infrastructure, instances, APIs, licensing or subscription costs).
- **Talent debt** — Lack of talent (human workers, augmented humans or virtual workers) in either the quantity, quality or ability to scale to fuel optimization or growth.
- **Social debt** — Suboptimal activity or a sustained negative impact on the organization's ability to address social, societal and community issues.

© 2021 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by [Gartner's Usage Policy](#). Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "[Guiding Principles on Independence and Objectivity](#)."