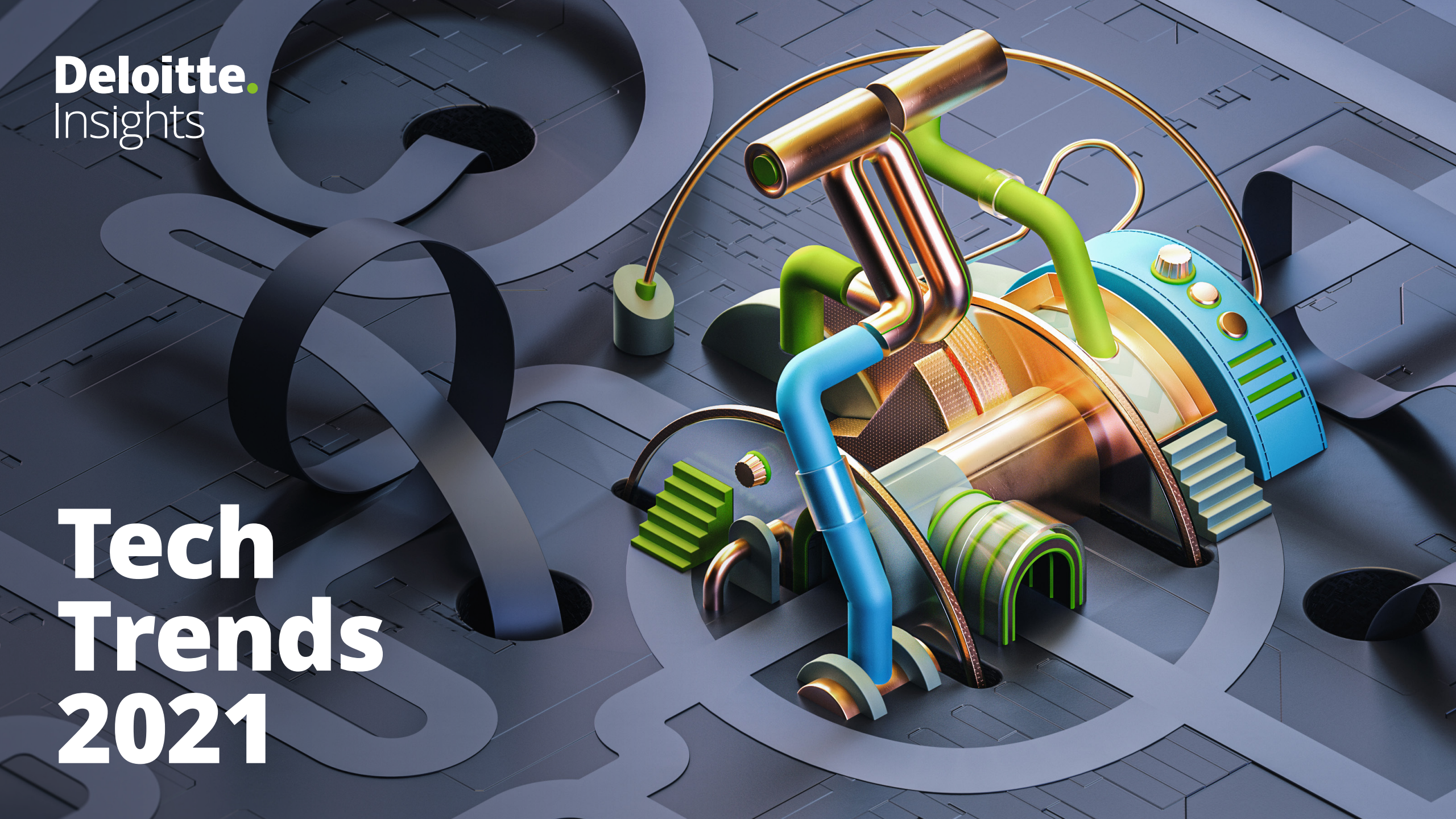
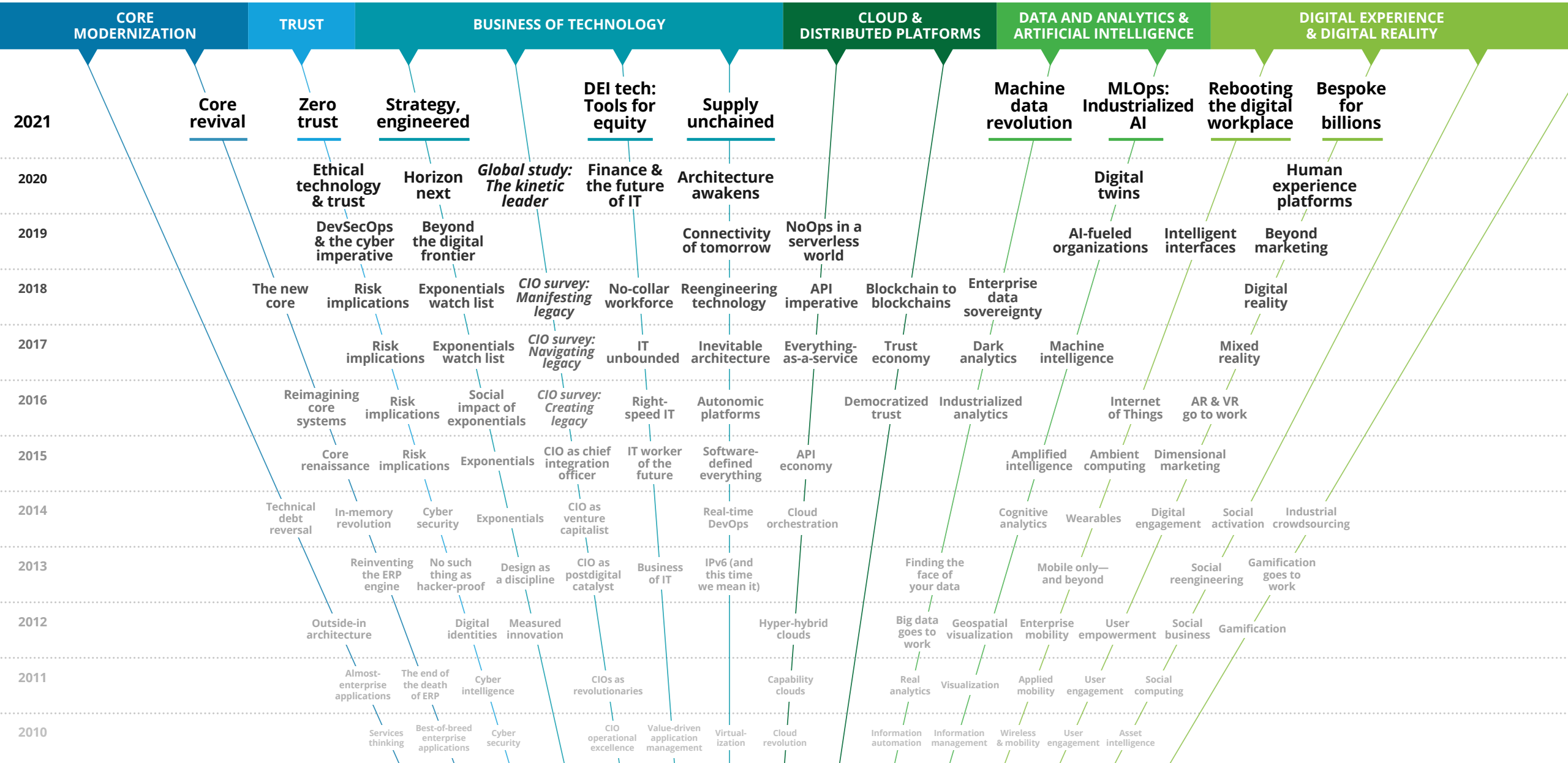
Deloitte. Insights



Tech Trends 2021

Trending the trends: Twelve years of research



Letter from the editors

As poet Robert Burns mused, the best-laid plans of mice and men often go awry. In January 2020, most of us had plans—thoughtful road maps to guide our organizations, our technology, and our lives through the months to follow. And then COVID-19 punched the entire world in the mouth, rendering useless many of these best-laid plans. Seemingly overnight, a strange, historic event disrupted our assumptions and forced us, with a shocking degree of urgency, to become more adaptable and responsive than we had thought possible.

Mindful that the pandemic's impact continues to ripple across societies, markets, and lives, we present *Tech Trends 2021*. The theme of this year's report is *resilience*. To us, this means a stubborn determination to adapt and thrive in the face of change. We have seen countless, inspiring examples of resilience this past year as organizations and entire sectors assessed their circumstances, revised their strategic plans, and marched toward the future.

We anticipate that for most, the future they find will differ markedly from the realities of January 2020. The COVID-19 crisis has driven change in an important and unexpected way. A growing number of organizations across sectors are accelerating their digital transformation efforts not only to make their operations nimbler and more efficient but to respond to dramatic fluctuations in demand and customer expectation. For example, while many supply chain leaders were confident of their ability to function during disruptions, we found out, as Warren Buffett once quipped, who was swimming naked when the tide went out. Likewise, executive-level planning discussions about the future of work had been just that: about the future. The pandemic crashed comfortable schedules from years into weeks.

With that background, this year's *Tech Trends* report discusses the opportunities, strategies, and technologies that will drive new plans during the next 18 to 24 months and beyond:

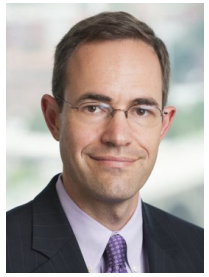
- For enterprise technology, we spotlight the importance of aligning corporate and technology strategy; we revisit the critical core and how digital nonnatives are using cloud, low-code, and platform-first strategies to juice legacy assets; and we take a deep dive into supply chain transformation.

- For data, we investigate how leading organizations are industrializing their AI initiatives with "MLOps" and, consequently, developing new approaches to managing data for machine, rather than human, consumption. We also discuss emerging trends in cybersecurity.

- For human and machine interaction, we look at emerging trends in the future of the workplace, digital experiences, and technology that supports diversity, equity, and inclusion.

Taken together, these trends suggest that there is a more hopeful dimension to the turbulent events of this past year. New technology and business plans already being executed chart a promising path toward tomorrow. Confidently leading this journey will be CIOs and other executives, who have proven they can take a punch and get back on their feet.

Now *that's* what we call resilience.



Scott Buchholz
Emerging technology research director and Government & Public Services chief technology officer
Deloitte Consulting LLP
sbuchholz@deloitte.com

Mike Bechtel
Managing director and chief futurist
Deloitte Consulting LLP
mibechtel@deloitte.com

Bill Briggs
Global chief technology officer
Deloitte Consulting LLP
wbriggs@deloitte.com
Twitter: @wdbthree

Get in touch with us

▶ **Talk with our Tech Trends team**
Reach out with questions on emerging tech and access new content.
www.deloitte.com/us/TechTrends
TechTrends@deloitte.com | @DeloitteonTech

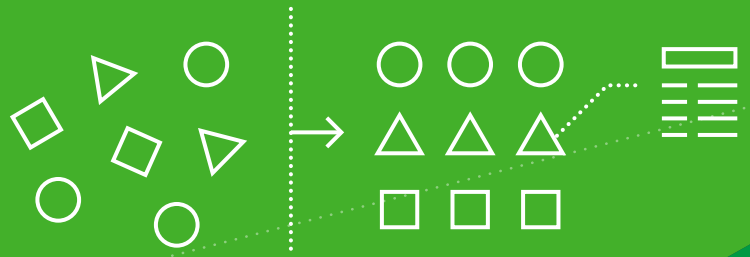
▶ **Access insights for tech leaders**
Gain new perspectives through research and success stories from our CIO Program and Executive Women in Tech leaders.
www.deloitte.com/us/CIO
www.deloitte.com/us/CIOInsider | Deloi.tt/women

▶ **Stay in touch with Deloitte Insights**
Download the Deloitte Insights and Dow Jones app to access articles, news, and the Daily Executive Briefing from our C-suite journals, and receive notifications as new content is available.
www.deloitte.com/insights | @DeloitteInsight
www.deloitte.com/insights/app

Zero trust: Never trust, always verify

BOLSTER CYBER BASICS

Beefing up basic cyber hygiene principles and practices can help companies realize the full benefits of zero trust.

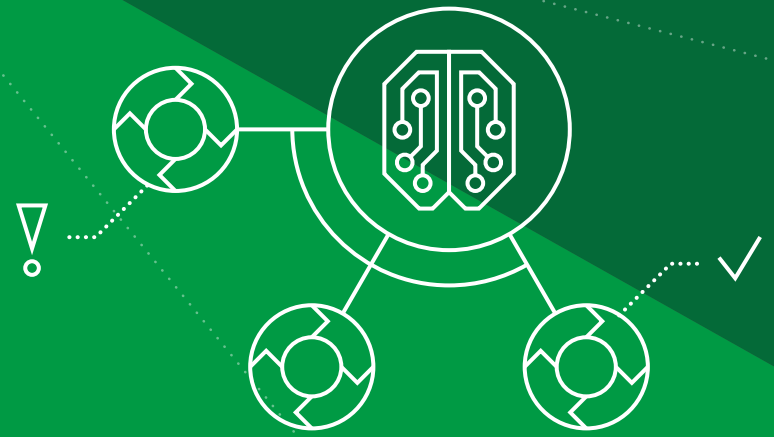


RETHINK THE CYBER ORG

Zero trust may require enterprises to rethink their organization's security approach and the skills, processes, and technology that support it.

AUTOMATE SECURITY TECH

Simplifying, integrating, and automating the security tech stack can improve the efficiency of security teams and streamline security processes and operations.



TREND 6

Zero trust: Never trust, always verify

Security in the age of the porous perimeter

Conventional castle-and-moat cybersecurity models, which rely on secure network perimeters and virtual private network-based employee and third-party remote access, are proving to be no match for evolving cyberthreats, particularly as business models and workforce dynamics evolve. For instance, the move to cloud and hybrid IT environments—along with increasing numbers of cloud-based systems, remote workers, and connected devices—are constantly expanding and dissolving the network perimeter. The anticipated growth of smart devices, 5G, edge computing, and artificial intelligence promises to create even more data, connected nodes, and expanded attack surfaces.

With cloud now mainstream, businesses managing services across multiple cloud providers are responsible for securing these technologies. As an enterprise more frequently relies on third-party vendors to host and manage data, infrastructure, and other services, the attack surface expands. In one study, 59% of companies surveyed had experienced a data breach due to a vendor or other third party;[1] another study concluded that multiparty security incidents result in 13 times the financial losses of single-party events.[2]

In fact, while perimeter-based security assumes the trustworthiness of users and devices connected to the organization's network, stolen credentials cause more than a quarter of security breaches.[3]

Consider the case of an employee who logs in regularly on weekdays from her home and occasionally on weekends from a coffee shop. When her username and password are used on a Saturday night from somewhere in Eastern Europe, traditional approaches might allow the connection. But because a *zero trust* architecture is more risk-driven and context-aware, it recognizes the inconsistency, automatically denies the access request, and raises an alert. Automated response capabilities could be triggered to temporarily disable the user's account, given the likelihood that its credentials have been compromised.

Proper design and engineering of zero trust architectures can result in simple, modular environments and straightforward user access

control and management. Streamlining the security stack can eliminate considerable management headaches, significantly reduce operational overhead, and help scale to tens of thousands of users. Similarly, onboarding employees, contractors, cloud service providers, and other vendors can become more efficient, flexible, responsive, and secure.

Carefully designed zero trust architectures that embed automation and orchestration capabilities can amplify and work in concert with other automated IT practices such as DevSecOps and NoOps. The use of APIs across the technology ecosystem can facilitate system management in a zero trust manner by providing a consistent control layer. And cloud-based services enable organizations to leverage the substantial ongoing security investments of cloud vendors.

A final key element of the zero trust approach is microsegmenting networks, data, applications, workloads, and other resources into individual, manageable units to contain breaches and wrap security controls at the lowest level possible. By limiting access based on the principle of least privilege, a minimum set of users, applications, and devices has access to data and applications.

The anticipated growth of smart devices, 5G, edge computing, and artificial intelligence promises to create even more data, connected nodes, and expanded attack surfaces.

By removing the assumption of trust from the security architecture and authenticating every action, user, and device, zero trust helps enable a more robust and resilient security posture. The organizational benefits are complemented by a considerable end-user perk: seamless access to the tools and data needed to work efficiently.

As the benefits of zero trust continue to pile up, enterprises are catching on. The global zero trust market is expected to grow to US$38.6 billion by 2024, a 20% increase from 2019.[4]

Beefing up basic cyber hygiene

The zero trust mindset shift brings with it a set of design principles that guide security architecture development and build on existing security investments and processes. To enforce access control, companies must have situational awareness of their data and

assets; companies that lag on basic cyber hygiene principles and practices may be challenged to realize the full benefits of zero trust. Fundamentals include:

- **Data discovery and classification.** Data governance, inventory, classification, and tagging are critical. To create the appropriate trust zones and access controls, organizations need to understand their data, the criticality of that data, where it resides, how it is classified and tagged, and the people and applications that should have access to it.

- **Asset discovery and attack-surface management.** Many organizations lack a real-time, updated inventory of all IT resources—including cloud resources, IP addresses, subdomains, application mapping, code repositories, social media accounts, and other external or internet-facing assets—and therefore can't identify security issues across the complete attack surface. To facilitate risk-based policy decisions surrounding their assets, it's critical for organizations to understand the enterprise IT environment.

- **Configuration and patch management.** Without the ability to efficiently manage and document baseline configurations of key technology systems, deploy appropriate patches, test patched systems, and document new configurations, companies cannot easily identify changes and control risks to these systems. Malicious actors can exploit any vulnerabilities to gain a foothold within an organization.

- **Identity and access management.** To ensure that access to technology resources is granted to the proper people, devices, and other assets, enterprises need to standardize and automate their identity life cycle management processes. They can extend their operations beyond traditional boundaries while protecting critical resources and maintaining an efficient user experience by moving the identity stack to the cloud, consuming identity-as-a-service, or implementing such advanced authentication methods as physical biometrics, behavioral monitoring, and conditional access.

- **Third-party risk management.** To fully understand their entire risk surface, organizations need greater visibility into cyber risks related to their supply chains and ecosystem partners, including suppliers to third-party vendors.

- **Logging and monitoring.** To identify potentially malicious incidents and issues, security teams need automated logging and monitoring systems with advanced AI and machine learning capabilities to help simplify the process of tracking, analyzing,

and correlating data from volumes of detailed logs as well as alerts generated by internal and external systems, security controls, networks, and processes.

Engineered security automation and orchestration

Many security operations center (SOC) teams are challenged to keep pace with the volume of information generated by their technology and security controls. They must monitor, manage, and act upon continuous alerts and streams of data generated by fragmented security architectures and disparate, disconnected tools.

The number and nature of risk factors interrogated to support zero trust authentication and authorization—users, devices, or credentials and contextual data points such as location, privileges, application requirements, and behaviors—warrants a more automated approach to monitoring, decision-making, enforcement, and auditing.

Many existing security technologies can be leveraged to build out zero trust architectures. To ensure more efficient automation and orchestration, zero trust adopters should rationalize the security stack and eliminate unnecessary and duplicative technologies or those that contribute to data overload, delay detection and response, and complicate system maintenance and management.

With a simplified security stack, existing systems and tools can be integrated via API connections to a security orchestration, automation, and response (SOAR) platform that can automate workflows and repetitive and manual tasks, and coordinate the flow of data and alerts to the SOC. SOAR platforms help add context to triggered events and can auto-remediate identified and known vulnerabilities, enabling staff to keep pace with incoming alerts and notifications, improving operational efficiency and accuracy, and decreasing response time.

Many existing security technologies can be leveraged to build out zero trust architectures.

"Migrating to zero trust architectures can seem like a heavy lift, especially in large enterprises saddled with legacy technologies and a lot of technical debt," says a senior technology leader at a large financial institution. "You have to break it into manageable chunks where you can identify a discrete win, such as deploying pervasive endpoint segmentation, and understand that win as part of your larger story of operationalizing zero trust."

Rethinking the role of the cyber organization

Zero trust represents a philosophical shift in how security is managed and likely requires cultural change across the enterprise. Creating a culture in which all key stakeholders understand their vested interest in securing the enterprise can help build confidence in zero trust.

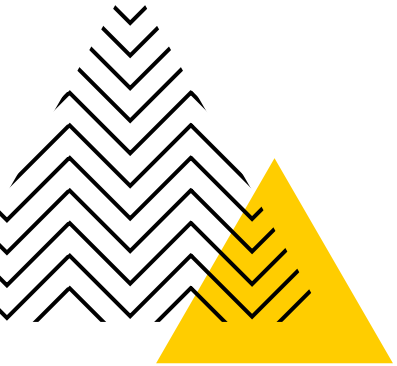
For example, zero trust could significantly change the day-to-day activities of the cyber workforce. To design and continually refine and evolve the zero trust architecture, enterprises likely will need more cyber engineering skills. And the role of the SOC will likely evolve as the security architecture takes command of manual, day-to-day tasks and processes, replacing them with more accurate machine-driven decision-making and faster response time and freeing SOC staff to focus on critical security issues and higher-risk incidents that require human analysis. Organizational structures will likely need to be reconfigured to account for new automated workflows, and it will be important to retrain security analysts to focus on strategic activities instead of tedious daily tasks.

In addition, to embed zero trust principles into every business initiative from inception, organizations will likely need more collaboration and integration between security teams and the lines of businesses they support. Business-function system owners likely will need to become more engaged in security planning. For example, to provide the security team with a better and deeper understanding of appropriate system behavior and access requirements, business partners can help identify who accesses and uses applications—and how. Business areas may need to become more intentional about system access, including limiting access privileges and making them more granular.

The way forward

The *zero trust* approach is not a product, solution, or platform—it's a philosophical shift in the way enterprises think about security. The process of migrating to an effective zero trust security architecture tends to be a marathon rather than a sprint, with organizations not only tackling foundational cybersecurity issues and embracing security automation and orchestration but preparing for the organizational and cultural changes that accompany such mindset shifts. To build confidence in zero trust, organizations will need to engage stakeholders ranging from cyber and IT to business area system owners and application end users. An iterative and incremental approach aligned to business objectives can help demonstrate the value of zero trust and enhance stakeholder confidence and acceptance.

LESSONS FROM THE FRONT LINES



Zero trust mindset enables digital growth

Like many global pharmaceutical companies, Takeda Pharmaceuticals supports better patient outcomes by innovating and collaborating across a diverse group of internal and external stakeholders—including, in its case, more than 52,000 employees and thousands of research partners, logistics partners, and other third-party service providers as well as patients, physicians, and other health care providers. The ongoing need to extend access to applications and systems to its broad external ecosystem spurred the Tokyo-based pharmaceutical giant to begin a journey toward a zero trust-based security architecture.

"We realized that the demarcation between internal and external was no longer relevant or scalable," says chief information security officer (CISO) Mike Towers. "The zero trust mindset—assuming that every request to connect is coming from an unknown access device on the internet that can't be predicted or controlled—is a much better way to move forward."[5]

Previously, access to an internal application would require granting access to the Takeda network, which inherently enabled access to a number of additional, unrelated services. "We could have tried to manually manage and restrict this additional system access, but, invariably, things will be missed over time," says Scott Sheahen, global head of information risk management. "With the zero trust approach, we eliminate superfluous system access and thereby reduce the avenues that could be exploited in a future cyberattack. Now we have granular, policy-based controls so that people have access only to needed resources."

This approach provides users with a more efficient way of navigating Takeda's complex technology environment—a mix of cloud-based applications and services and legacy systems residing on internal servers and in data centers—and eliminates the difficulty of accessing systems via multiple firewalls and VPNs. The transition to zero trust, well underway before COVID-19 struck, helped the company securely manage the sudden shift of its global workforce to a work-from-home model. "Our China workforce, the first affected by the pandemic, had less experience and comfort with work-from-home, so it was really important for us to get it right,"

Towers says. "By having shifted to zero trust-based access, we were able to aggressively and quickly move China to the work-from-home model."

Setting clear expectations with business partners is critical during the transition, says Thomas Likas, global head of security architecture and engineering. He recommends that security and IT organizations planning a zero trust migration engage with business partners from the beginning of the journey. "The business—not IT—has the best understanding of how people access and use their applications," he says. "In the zero trust world, the business will need to determine who should have access to their systems and data."

Indeed, Likas continues, "this knowledge needs to be baked into the access model from the very beginning. To business partners, this might seem like a lot of work, but as a bonus, the organization gets a solid understanding of their application landscape."

Towers believes that once leaders understand the numerous benefits, most companies will inevitably adopt the zero trust mindset. "Frankly," he says, "I don't think that businesses can digitally or technologically scale in any other way."

Zero trust secures the "new perimeter"

A zero trust approach is helping Halliburton, a global provider of products and services to the energy industry, meet its strategic business goals and objectives. Several years ago, as part of a drive to be more operationally efficient, the company began adopting cloud, mobile, and Industrial Internet of Things platforms to reduce costs and improve productivity. At the same time, Halliburton's vendors and suppliers began pushing their products and services to the cloud. "With the dispersion of our computing resources from the data center to the internet, we realized that our traditional network perimeters were dissolving," says Mary Rose Martinez, CISO and senior director for IT architecture.[6] "This impelled us to develop a zero trust strategy."

Halliburton's zero trust approach revolves around securing people, network connections, and data. "We are moving toward a reality where it doesn't really matter if employees are on the network or not," Martinez says. "The new perimeter is identity, whether user identity, endpoint device identity, or service identity."

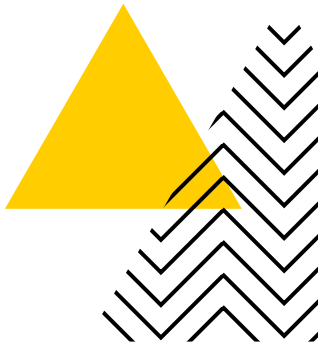
When Halliburton began its zero trust journey about two years ago, it focused first on securing mobile devices through multifactor authentication—using identity credentials, an authenticator, and registered devices. Soon after, the company migrated to cloud-

based identity providers to further secure its people. Over time, the number of applications accessible without using a VPN continues to grow. A longtime adopter of the principle of least privilege, data encryption, and other data controls, the company is also working to enhance the classification and protection of unstructured data.

The more granular security controls that are part of Halliburton's zero trust approach have created a more disciplined security posture. Because it controls user devices and endpoints, the company can push policies to any device via the internet. And because VPN access isn't required for the zero trust-enabled applications, employees have a considerably improved user experience.

Martinez is quick to emphasize that zero trust is not only a technology initiative—it is also a people initiative. For example, whether Halliburton employees are on the company network or the internet, in the office or at home, they receive a verification prompt before accessing applications protected by multifactor authentication. This workflow change required education and awareness. And it is incumbent on users to guard their credentials and devices. "Raising security awareness has to be part and parcel of the zero trust approach," Martinez says. "An ongoing education program that includes increasingly sophisticated phishing simulations can help people become more aware."

Halliburton's adoption of zero trust is an ongoing journey, with many components that are constantly moving and changing shape. "Because of the fluid nature of technological advancements, the end state will probably always be a moving target," Martinez says. "But we've laid a foundation that's both solid and adaptable, and upon which we can continue to build over time."



MY TAKE

John Kindervag

Field CTO,
Palo Alto Networks

When I worked as a security analyst, I became fascinated by how people and businesses anthropomorphized their digital environments by applying the concept of trust to computing—that somehow a device could be trusted and that it cared that it was trusted.

Back then, many CISOs and CIOs adhered to the idea—and many still do—that what's inside the corporate firewall can be trusted. This idea of *inside versus outside* became a variable that was used to determine security policy, with many organizations operating under the adage "trust, but verify." In the trust-but-verify model, trust is the default. When identity is verified, trust is assumed and access is granted.

But trust applies only to people—not digital environments. Identity credentials can be stolen, networks can be hacked, and insiders with

bad intent are often in positions of trust. This means it's impossible to know with certainty that the originator of network traffic can truly be trusted: An asserted identity is only an assertion, not an actual person.

In response to what CISOs and CIOs told me about their cybersecurity strategies, I created the concept of *zero trust*, which is framed around the principle that no network user, packet, interface, or device—whether internal or external to the network—should be trusted. Some people mistakenly think zero trust is about making a system trusted, but it really involves eliminating the concept of trust from cybersecurity strategy. By doing this, every user, packet, network interface, and device is granted the same default trust level: zero.

Zero trust should be thought of as a strategy or framework. It requires companies to rethink their philosophy and approach to trusted network users and devices. Zero trust is not a product, although zero trust-based security infrastructures can be implemented by using many different products. Nor does zero trust require organizations to rip and replace existing security infrastructure—rather, it leverages existing technology to support the zero trust mindset, with new tools added as needed.

The hallmark of zero trust is simplicity.

The hallmark of zero trust is simplicity. When every user, packet, network interface, and device is untrusted, protecting assets becomes simple. To reduce the complexity of cybersecurity environments, organizations can prioritize security technologies and tools that support simplicity by automating repetitive and manual tasks, integrating and managing multiple security tools and systems, and autoremediating known vulnerabilities.

Zero trust is a journey best taken one step at a time. I recommend that organizations begin by prioritizing the smallest possible protect surfaces—a single data set, asset, application, or service—depending on the level of sensitivity or business criticality. Then, they can create a microperimeter around each protect surface and granularly control the traffic allowed into the perimeter.

I encourage security teams to learn and practice on less sensitive protect surfaces, moving to protect increasingly more sensitive or valuable protect surfaces as they fine-tune their approaches and their confidence increases. Over time and with lots of practice, they'll be ready to migrate their most critical assets to the zero trust environment. Finally, when high-value assets are protected, teams can focus on less important assets. And by continuing to maintain a zero trust mindset, organizations can protect themselves even as security technologies and tools evolve.

EXECUTIVE PERSPECTIVES

STRATEGY // The stakes are high for CEOs when it comes to cyber risk. Beyond the damage that security breaches can have on companies, shareholders, and customers, they can end careers. CEOs are often answerable to the public for their organization's security posture, especially as it relates to consumer data, and they should thus approach this topic as the stewards of the organization's brand reputation and trust. By appointing a CRO, CISO, or other appropriate leader, they can look to new security postures such as *zero trust* that simplify protection of data, people, and networks without sacrificing user experience. Setting security priorities from the top can help the organization align on the importance of strengthening cyber defenses.

FINANCE // Reporting on cybersecurity breaches is among the CFO's more unpleasant responsibilities. When these events happen, CFOs are often on point, reporting to auditors and answering to the board, regulators, and the public. In a time when cyber risk is increasing and bad actors regularly test organizational defenses, CFOs should develop and maintain technology fluency and the awareness they will need to mitigate cyber events. Moreover, they should clearly understand the risks and rewards of their company's security posture—particularly as it applies to key strategic, physical, and financial assets—and then improve security by enabling zero trust adoption. Ultimately, the CFO—working in tandem with other risk and security leaders—can become a de facto crisis manager, working to predict and prevent threats to brand reputation, shareholder trust, and more.

RISK // Zero trust is fast becoming the modern standard for managing infrastructure, network, and data in a more secure manner. Despite the concept's broad benefits, many see it as solely a technology issue. To change that, over the next 18–24 months, CROs should consider placing zero trust adoption at the top of their agendas. CROs can first clarify the security benefits to the organization and then work with the CIO, CISO, and other leaders to enforce the new approach. Thorough adoption can eventually help risk posture and processes evolve in lockstep with innovation while reducing the frequency of cyber incidents.

ARE YOU READY?

KEY QUESTIONS

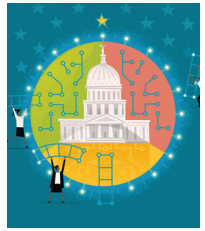
1. How far are you on your journey moving away from network and server "zones of trust"? What is your next step?

2. How could you improve the skills and capacity of your cybersecurity organization relative to today's challenges? What about tomorrow's?

3. How can you better involve business-function system owners in security planning? Would their help in identifying areas requiring more restricted access improve the overall security posture?

LEARN MORE

Cyber risk collection
Explore the latest insights on managing cyber risk and bolstering security against attacks.



States at risk: The cybersecurity imperative in uncertain times
Read a joint cybersecurity report with the National Association of State Chief Information Officers.

Resilient podcast series
Tune into an award-winning podcast series that features leaders tackling risk, crisis, and disruption.

AUTHORS

Our insights can help you take advantage of emerging trends. If you're looking for fresh ideas to address your challenges, let's talk.

Deborah Golden

US Cyber & Strategic Risk leader

Deloitte & Touche LLP

debgolden@deloitte.com

Mark Nicholson

Cyber & Strategic Risk marketplace development leader

Deloitte & Touche LLP

manicholson@deloitte.com

Kieran Norton

Cyber & Strategic Risk infrastructure security solution leader

Deloitte & Touche LLP

kinorton@deloitte.com

Arun Perinkolam

Cyber & Strategic Risk core infrastructure and network offering leader

Deloitte & Touche LLP

aperinkolam@deloitte.com

Andrew Rafla

Cyber & Strategic Risk zero trust offering leader

Deloitte & Touche LLP

arafla@deloitte.com

SENIOR CONTRIBUTOR

Wil Rockall

Partner, Deloitte MCS Limited

ENDNOTES

1. Business Wire, "Opus & Ponemon Institute announce results of 2018 third-party data risk study: 59% of companies experienced a third-party data breach, yet only 16% say they effectively mitigate third-party risks," November 15, 2018.
2. RiskRecon, *Ripples across the risk surface: A study of security incidents impacting multiple parties*, accessed November 20, 2020.
3. Verizon, *2020 data breach investigations report*, 2020.
4. MarketsandMarkets, "Zero-trust security market by solution type (data security, endpoint security, API security, security analytics, security policy management), deployment type, authentication type, organization size, vertical, and region—global forecast to 2024," accessed November 20, 2020.
5. Mike Towers (CISO, Takeda), Scott Sheahen (global head of information risk management, Takeda), and Thomas Likas (global head of security architecture and engineering, Takeda), phone interview with the authors, September 22, 2020.
6. Mary Rose Martinez (CISO and senior director for IT architecture, Halliburton), phone interview with the authors, October 2, 2020.

Acknowledgments

Executive editors

Scott Buchholz
Emerging technology research director and Government & Public Services chief technology officer
Deloitte Consulting LLP
sbuchholz@deloitte.com

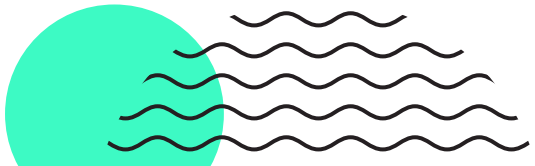
With more than 25 years of experience in technology innovation and implementation, Scott Buchholz focuses on helping clients transform the way their organizations deliver their missions and businesses through technology. He supports organizations across industries by providing advice and insights on how to evolve their technology and their organizations to improve performance, effectiveness, and efficiency.

In his role as CTO for Deloitte Consulting LLP's Government and Public Services practice, Buchholz works with clients to implement innovation across a diverse set of areas, including emerging technologies, legacy modernization, and solution architecture. As the firm's emerging technologies research director and the sponsor of *Tech Trends*, he helps identify, research, and champion the technology trends that are expected to have significant impact on the market and clients' businesses in the future. Buchholz also leads Deloitte's efforts to explore quantum computing and quantum technologies.

Mike Bechtel
Managing director and chief futurist
Deloitte Consulting LLP
mibechtel@deloitte.com

As chief futurist with Deloitte Consulting LLP, Mike Bechtel helps clients develop strategies to thrive in the face of discontinuity and disruption. He researches the novel and exponential technologies likely to materially impact the future of business, and builds relationships with the startups, incumbents, and academic institutions creating them.

Prior to joining Deloitte, Bechtel led Ringleader Ventures, an early-stage venture capital firm he cofounded in 2013. Before Ringleader, he served as CTO of the Ounce of Prevention Fund, a national not-for-profit focused on early childhood education for at-risk youth. Bechtel began his career in technology R&D at a global professional services firm where his dozen US patents helped result in him being named that firm's global innovation director. He currently serves as professor of corporate innovation at the University of Notre Dame.



Executive perspectives contributors

STRATEGY

Benjamin Finzi
US and Global Chief Executive Program leader | Deloitte Consulting LLP

Andrew Adams
Principal | Deloitte Consulting LLP

Louis DiLorenzo Jr.
Principal | Deloitte Consulting LLP

Ashok Divakaran
Principal | Deloitte Consulting LLP

Anne Kwan
Managing director | Deloitte Consulting LLP

Benjamin Stiller
Principal | Deloitte Consulting LLP

FINANCE

Steve Gallucci
US CFO Program leader | Deloitte LLP

Ajit Kambil
CFO Program global research director | Deloitte LLP

Moe Qualander
Principal | Deloitte & Touche LLP

RISK

Deborah Golden
US Cyber & Strategic Risk leader | Deloitte & Touche LLP

Irfan Saif
Deloitte US board member | Deloitte & Touche LLP

Contributors

Sachin Agarwal, Zachary Aron, Angel Ayala, Nithyasree Balasubramanian, Leo Barbaro, Amod Bavare, Hanif Bejestani, Armando Betancourt, Rupesh Bhat, Andrew Blau, Mike Brinker, Rick Burke, Michael Calienes, Sudeep Chakraborty, Enoch Chang, Ashish Chauhan, Mike Clendon, Dave Couture, Andrea D'Alessandro, Titikhya Dey, Tatiana Dominguez, Aaron Dozzi, Michael Fancher, Art Fitts, Nairita Gangopadhyay, Shubhrapratim Ghosh, Purba Ghosh, Nidal Haddad, Diogo Henriques, Sarah Jersild, Andrew Jolly, Samikhya Joshi, Sriram Kailasanathan, Alexandria Kang, Khalid Kark, Jon Kawamura, Rupert Kay, Abrar Khan, Aref Khwaja, Vamsee Kota, Yadhu Krishnan, Manish Kumar, Vishnu Kumar, Naren Kunapareddy, Santosh Kutty, Rafi Lav, Jesus Leal Truillo, Victoria Lee, Mark Lillie, David Linthicum, John Lu, Alpesh Makwana, Cesar Marto, Brian Meeker, Grace Messara, Mariahna Moore, Narasimham Mulakaluri, Sampath Murki, Sri Myneni, Aleks Ontman, Genevieve Oudar, Shruti Panda, Ann Perrin, Dalibor Petrovic, Jack Polson, Jose Porras, Vishal Prajapati, Jason Price, Megha Priya, Muthu Rajendran, Bill Roberts, Aaron Roe, Keihan Sedghi, Karen Shea, Kushagr Singh, Hariom Sinha, David Sisk, Kelly Smith, Anna Spikings, Joey Suing, René Theunissen, Jon Tidd, Arpan Tiwari, Brian Umbenhauer, Aman Vij, Jason Wainstein, Mike Wyatt, Sourabh Yaduvanshi, Abhilash Yarala, Thomas Zipprich, and the Deloitte Insights Knowledge Services team.

Research team

LEADS

Erica Cappon, Cristin Doyle, Dave Geyer, Chris Hitchcock, Emeric Kossou, Dhruv Patel, Alex Jaime Rodriguez, Katrina Rudisel, and Samantha Topper.

TEAM MEMBERS

Roudy Antenor, Shenbagamoorthy Arunachalam, Angela Chen, Serena Chen, Emma Copsey, Andrea Cuadros, Rahul Datta, Chirag Dixit, Ankush Dongre, Carrie Ge, Mayank Gupta, Mohammad Abdul Hannan, Ripu Jain, Carter Johan, Solomon Kassa, Heather Kelly, Dhir Kothari, Shantanu Kulkarni, Nitin Kumar, Siva Kuna, Madeline Mantych, Allie McIlwain, Katherine McNally, Spandana Narasimha Reddy, Rani Patel, James Patterson, Abhishek Pattnaik, Kshitij Pratap Singh, Pooja Raj, Rohit, Gabby Sanders, Rohit Singhal, Elizabeth Thompson, and Paige Zellner.

Special thanks

Stefanie Heng for being our stupendous, stern sherpa throughout the research, development, and publication process, eternally calm under pressure. Your spreadsheets, to-do lists, and nonstop emails kept all of us on track and on our toes, and your creative solutions saved us from our own chaos monkeys.

Anh Nguyen Phillips for being our relentless research leader, overseeing our overall research efforts, and deftly laying down the law. Your ability to always be reasonable, be looking out over the horizon, and be asking good questions helped us deliver under pressure with grace.

Doug McWhirter for being our wise, witty muse, continuously distilling structure from boatloads of brainstorms and brainwaves while culling through innumerable interviews, reams of research, and stampedes of SMEs. We appreciate the poise and dry humor that you bring to our research projects.

Dana Kublin for being our gifted graphical guide, taking our fantastic flights of fancy and turning them into intuitive, insightful infographics. Thanks for being our tireless translator between words and pictures, overseeing the graphics and artwork that make our trends better.

Caroline Brown, Tristen Click, and **Linda Holland** for being our consummate creative team. Your collective ability to translate jargon into English and transform chatter into infographics is second to none. Thanks for always dotting the I's and crossing the T's while going the extra mile.

Matt Calcagno, Kelly Gaertner, Natalie Martella, Abhijith Ravinutala, and **Maria Wright** for keeping the *Tech Trends* train running on time. We benefited from your help keeping us on track across interviews, secondary research, writing, content reviews, graphics, and so much more.

Cheylin Parker, Tracey Parry, Daniella Ramirez, and **Tiffany Stronsky** for our marvelous marketing, continuous communications, and provocative PR. Your ongoing encouragement makes sure that we continue to take our buzz up to 11.

Matthew Budman, Blythe Hurley, Hannah Rapp, and the entire Deloitte Insights team. We appreciate our amazing and ongoing partnership that helps *Tech Trends* reach new heights every year.

Jodi Gray, Matt Lennert, Mackenzie Odom, Joanie Pearson, Samantha Trunzo, Alexis Werbeck, and the Green Dot Agency. We appreciate your ongoing partnership that helps us get the word out and makes *Tech Trends* look fabulous.

Deloitte.
Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

www.deloitte.com/us/TechTrends

Follow @DeloitteOnTech

Deloitte Insights contributors

Editorial: Matthew Budman, Blythe Hurley, Abrar Khan, Rupesh Bhat, and Nairita Gangopadhyay

Creative: Alexis Werbeck, Dana Kublin, Tristen Click, and Victoria Lee

Promotion: Hannah Rapp

Cover artwork: Vault49

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

About Deloitte