DIGITAL REALTY

WHITE PAPER

High-Tech Companies Tackle Business Challenges with Hybrid Cloud

Executive Summary

Tech companies comprise one of the fastest growing industry segments—and their adoption of digital technologies is a critical factor behind their growth. But research shows they have a long way to go when it comes to specific digital transformation (DX) initiatives. Furthermore, tech companies face significant headwinds such as new data privacy regulations, cyber and insider security threats, and IT skill shortages. In order to take greater advantage of DX and tackle these challenges, tech businesses are leveraging the cloud—specifically hybrid cloud. Hybrid cloud provides tech companies with the means to drive down IT costs, greater agility and speed when embracing new business opportunities, and the ability to protect critical business data and applications from external and internal threats.

The tech sector experienced substantial volatility in 2018, with valuation for many of the top publicly traded companies taking a huge hit. But growth quickly returned to the sector. A look over the past five years shows that high-tech companies delivered total shareholder return (TSR) of 14%—fourth highest of 33 industries included in analysis by Boston Consulting Group (BCG).[1]

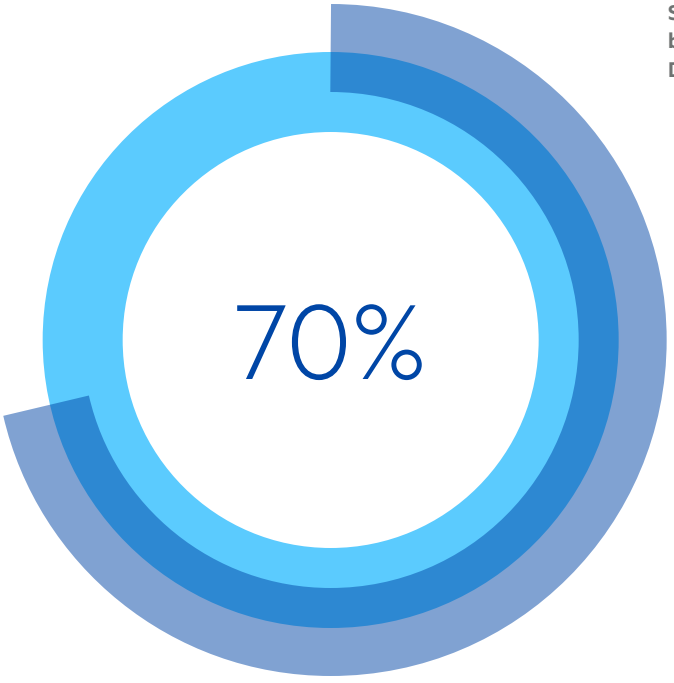
One of the factors behind this growth is the adoption of digital technologies, such as artificial intelligence (AI), Internet of Things (IoT), and cloud services. Surprisingly, at the top of the list are semiconductor companies—NVIDIA, Broadcom, and AMD—rather than Google, Facebook, Amazon, and others that one might expect to be in the lead position. For these top-tier technology leaders, their digital strategy is aligned with measureable business objectives.

Business Challenges Facing High-Tech Companies

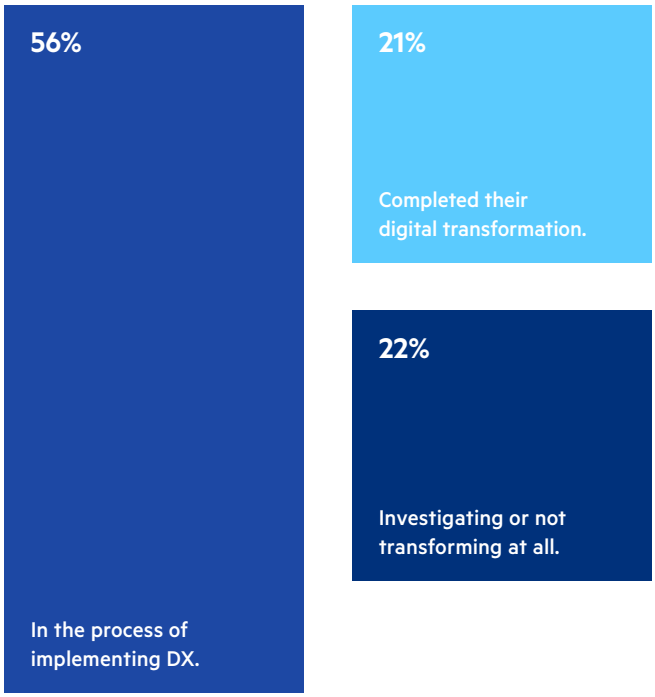
The tech market is highly competitive and, ironically, technology is often a key differentiator. But just as these technologies offer business advantages, they also create new challenges and exacerbate legacy systems issues. Let's examine some of the more prevalent issues that are facing tech businesses today:

Struggling with Digital Transformation

Digital transformation (DX) is at the heart of what is driving business acceleration today. Forty-five percent of CEOs indicate that the pace of innovation has significantly accelerated over the past three years—and 49 percent say it has accelerated.[2] Seventy percent of businesses are pursuing DX initiatives this year,[3] with customer experience as a primary reasoning for many of the businesses.



Seventy percent of businesses are pursuing DX initiatives this year



That being said, the level of DX maturity seems to be overestimated by many organizations. Forrester recently found that **21 percent of companies feel they have completed their company's digital transformation, 22 percent are investigating or not transforming at all, and 56 percent say they are in the process of implementing DX**.[4]

However, DX claims appear to be overstated when specific DX solution areas are examined. For example, while businesses assert emerging technologies are critical to DX, only 17 percent have initiated an artificial intelligence (AI)-driven project.[5] Surprisingly, Software-as-a-Service (SaaS) applications are another area where the adoption lags behind claims.[6] Real-world implementation of other DX areas such as big data, Internet of Things (IoT), and software-defined networking (SDN) also are overinflated.

The takeaway for the majority of enterprises is that the vast potential of DX still remains untapped. Tech organizations failing to keep pace with industry peers will find themselves playing catch up and missing business opportunities, especially given the accelerating pace of innovation today.

While most businesses and executives contend digital transformation is a priority, many digital technologies such as AI, machine learning, and even SaaS remain underutilized.[7]

Increasing Scrutiny of Data Privacy

Data privacy and governance take on new meaning in the post-General Data Protection Regulation (GDPR) world. While prior data privacy regulations created measurable challenges for businesses, the EU's GDPR puts violators on full notice. Fines and penalties now have teeth and the EU is already handing them out. The most public of these fines being the $57 million fine from a French data authority, though others have also found themselves on the receiving end of levies for varying violations—some for data breaches and others for how they manage and use data.[8] With California's Consumer Privacy Act also looming on the horizon, even more businesses will need to heed data privacy issues and institute new data governance processes to remain compliant.[9]

The sheer amount of data generated in the tech sector puts many of these companies at a higher risk than companies in other industries. Even though GDPR has been in place for more than a year, many businesses admit they are still noncompliant—and this certainly includes those in tech.[10]

Four elements of GDPR are often cited as areas that require redress in order to demonstrate compliance with the privacy law: 1) documentation of all personally identifiable information (PII) processed, stored, or deleted and the ability to provide it to individuals upon request, 2) hiring data protection officers (an expensive undertaking), 3) identification and reporting of data breaches within 72 hours, and 4) allowing customers to download and move their data—including the ability to move it to a competitor.[11] Of course, these issues apply to all data—whether it resides on-premises or in the cloud.

More than half of businesses in a recent survey by the International Association of Privacy Professionals estimate that they are noncompliant with aspects of GDPR.[12]

An Evolving Cyber Threat Landscape

Research shows that tech companies and their employees have a higher-risk appetite than their peers in other industries.[13] They tend to be early adopters of digital technologies that are still maturing and, in some cases, more vulnerable to attacks and exploits. Tech companies also tend to have open environments and cultures that stimulate creativity and collaboration but provide greater risk of exposure—users, devices, access points, and applications. Indeed, many technology-dependent industries are experiencing significant pressure from executive management to become 100% cloud based.[14]

Using the National Institute of Standards and Technology (NIST) Cybersecurity Framework as its basis of measurement, a recent study found that while tech companies slightly lag other industries in the percentage of companies categorized as security leaders, they have a much higher percentage of security beginners.[15] For those in the beginning stages of security maturity, the level of risk significant substantially. And with tech companies near the forefront in industry sectors pushing for cloud adoption, the risks extend from on-premises to the cloud.

Nearly 80 percent of organizations are introducing digital innovations faster than they can secure them against cyberattacks.[16]

Malicious and Negligent Insider Threats

Tech companies promote innovation and collaboration, and their workforces typically embody these traits. While tangible benefits are attached to these activities, they also come with certain risks. Insider threats—both malicious and negligent—are among these threats. One report pegs the total percentage of data breaches tied to insider threats at 58 percent.[17] The total average cost of a data breach is a whopping $3.86 million.[18]

Insider threats take different forms, from malicious to negligent.[19] The intentions of malicious insiders vary—from personal gain, to a desire to take revenge against a perceived injustice, to industrial espionage. Negligent insiders, which compromise the majority of insider threats,[20] are employees or contractors who unintentionally expose business-critical data or systems. Whether malicious or negligent, the list of potential insider vulnerabilities increase as cloud services and app adoption expand.

36%
Have a threat program in place.

50%
Are in the process of constructing a threat program.

Organizations are recognizing the magnitude of insider threats and are building formal insider threat programs—36 percent have one in place and another 50 percent are in the progress of constructing one.[21]

Recruiting and Retaining Top Talent

Nearly all indicators show that IT budgets are increasing—and this holds across all industry segments. As IT infrastructure investments expand, so do the required IT skills. This can prove to be a significant challenge for organizations embracing digital technologies in the face of a global IT skills shortage. Half of organizations in a Forbes survey cite an IT skills shortage as the key challenge to IT transformation.[22]

There is also a demonstrable talent shortage when it comes to cloud services. Employer demand for skilled cloud workers rose 33 percent over the past three years, whereas job seeker interest in cloud infrastructure, security, architecture, and analyst roles reached almost 108% and thus falls short of meeting this demand.[23] Thus, even when there are executive or board mandates to embrace the cloud, there are no assurances that an organization can given the shortage of professionals with the requisite skill sets and experience. Yet, at the same time, the cloud also offers organizations the ability to optimize IT staffing efficiencies by relocation and automating certain time-consuming IT infrastructure workflows and tasks.

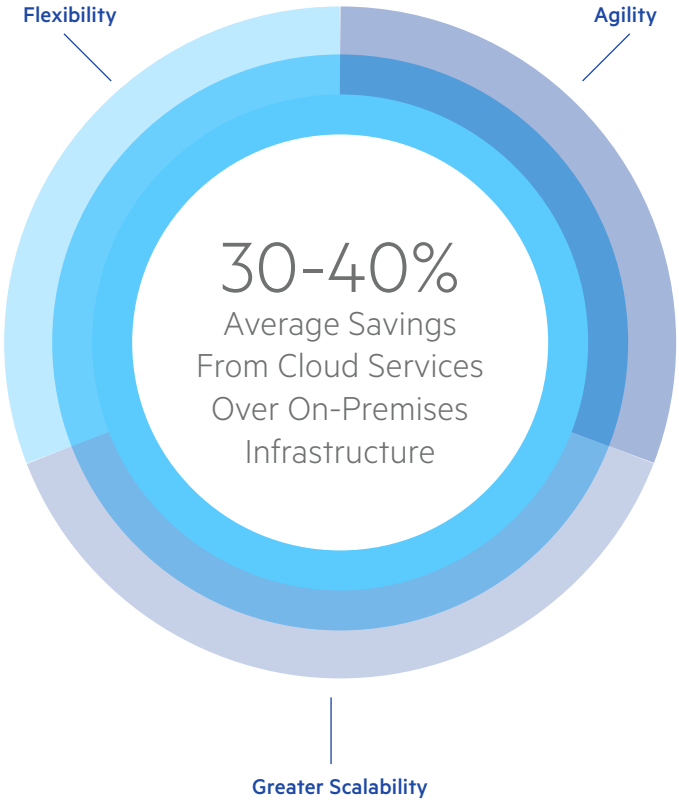
60%

of companies hiring full-time security and cloud infrastructure staff in the past 12 months found it challenging.[24]

Leveraging the Cloud to Leapfrog Business Challenges

In response to these business challenges, tech companies are turning to the cloud for answers. The earliest adoption of cloud technologies largely revolved around the ability to acquire inexpensive compute and storage resources, but that has changed in recent years.

Leveraging public and private cloud services, digital innovators are turning increasingly to the cloud as the platform for enabling AI, IoT, and much more.[25] **Cloud services speed up time to market by providing greater scalability, flexibility, and agility. They also provide a more cost-effective compute infrastructure model—an average savings of 30 to 40 percent over on-premises infrastructure.**[26] And by using cybersecurity and compliance tools and frameworks native to the cloud, organizations can lower their security risk and demonstrate compliance with data privacy regulations. Security monitoring—for outsider and insider threats—can be managed through these native tools by employing AI-enabled capabilities that lower false positives while increasing detection and prevention rates.



Cloud services speed up time to market

It should be no surprise that 10 percent of revenue for the top 50 software companies comes from cloud services.[28]

Tech companies are quick to recognize the advantages that the cloud offers. Like other industry peers, they see it as a means for modernizing IT infrastructure while reducing costs by moving from CAPEX to OPEX. AI, IoT, and other advanced digital initiatives can be deployed easier and faster via the cloud. And by leveraging the orchestration, automation, built-in security and compliance capabilities of the cloud, tech companies shrink deployment times while demonstrating compliance with data privacy and other government and industry regulations. Tech businesses also view the cloud as a way to address increased cybersecurity risks, leveraging security services hubs and security orchestration and automation.

Despite rapid adoption rates, the maturity of cloud adoption remains low. **Only 20 percent of enterprise workloads and data have been moved to the cloud today.**[27]

High-Tech Companies Must Lay a Solid Hybrid Cloud Foundation

Many organizations—including tech businesses—are coming to the realization that public-only cloud models are not always the best way to meet their compute and storage infrastructure business requirements. Instead, they are embracing hybrid multi-cloud architectures that concurrently utilize private and public cloud deployments. For data processing, businesses leverage private clouds—enabling them to avoid the high costs of egress fees typically attached to public cloud providers. For scalability, they employ hybrid cloud computing, providing the scalability to accommodate spikes in business without increasing CAPEX. Companies process and store critical intellectual capital and critical business data in the private cloud.

77% Of enterprises have at least one application residing in the cloud.[29]

The hybrid cloud market is estimated to grow at a 24 percent compound annual growth rate (CAGR) through 2023.[30]

But to effectively tap a hybrid-cloud model, businesses require transparent visibility and unified management across and between both public and private cloud deployments. This optimizes operational efficiencies—including the use of IT/cloud staff—while improving risk management. It also provides a scalable infrastructure that can seamlessly accommodate fluctuations in compute and storage requirements. Finally, by placing compute resources in closer proximity of end users and with each other, companies can decrease network and application latency.

Some of the questions IT leaders for tech businesses should ask when evaluating their cloud options include:

- **Do we have the right technology in place to provide transparent visibility and centralized management of each cloud deployment?**
- **Do we have the IT/cloud/security skills in-house to manage a migration of data and applications into the cloud?**
- **Do we need additional technologies and processes to manage increased insider threat risks due to cloud adoption?**
- **In what ways will our cloud adoption increase cybersecurity risks? How can our cloud adoption lower our cybersecurity risks?**
- **Do we have the in-house IT/cloud/security skills to embrace a hybrid-cloud model? Will migration of data and applications to the cloud enable us to get more out of our existing IT staff?**

1 Awais Ali, et al., "Despite a Volatile 2018, Tech Is Still Performing Strongly," BCG, February 25, 2019.

2 "The Post-Digital Era Is Upon Us: Are You Ready for What's Next?" Accenture, accessed May 28, 2019.

3 Rich Castagna, "Top drivers of digital transformation projects have inward focus," Search CIO, January 3, 2019.

4 Ted Schadler, "The Sorry State of Digital Transformation in 2018," Forrester, May 2, 2018.

5 Ted Schadler, "The Sorry State of Digital Transformation in 2018," Forrester, May 2, 2018.

6 Ted Schadler, "The Sorry State of Digital Transformation in 2018," Forrester, May 2, 2018.

7 Ted Schadler, "The Sorry State of Digital Transformation in 2018," Forrester, May 2, 2018.

8 Adam Satariano, "Google Is Fined $57 Million Under Europe's Data Privacy Law," The New York Times, January 22, 2019.

9 Joe Stanganelli, "California's CCPA Law: Why CISOs Need to Take Heed," Security Now, July 26, 2018.

10 Joe Stanganelli, "California's CCPA Law: Why CISOs Need to Take Heed," Security Now, July 26, 2018.

11 Szuyin Leow, "GDPR Industry Focus: How Does GDPR Impact the Tech Industry," LogiGate, February 26, 2018.

12 Nancy Couture, "How data governance can support data privacy compliance," CIO, February 7, 2019.

13 "Global Cyber Executive Briefing," Deloitte, accessed on May 28, 2019.

14 Louis Columbus, "State of Enterprise Cloud Computing, 2018," Forbes, August 30, 2018.

15 "Cybersecurity in the Technology Industry: A Path for Accelerating Progress," Protiviti, accessed May 28, 2019.

16 "Ninth Annual Cost of Cybercrime Study," Accenture and Ponemon Institute, March 6, 2019.

17 Suzanne Widup, "New report puts healthcare cybersecurity back under the microscope," Verizon, March 2, 2018.

18 "2018 Cost of a Data Breach Study: Global Overview," Ponemon Institute, accessed May 28, 2019.

19 Jamie Graves, "Seeing and Addressing Insider Threats Across Your Distributed Network," Fortinet Blog, January 29, 2019.

20 "Ninth Annual Cost of Cybercrime Study," Accenture and Ponemon Institute, March 6, 2019.

21 "2018 Report: Insider Threat," Cybersecurity Insiders and Crowd Research Partners, accessed 28, 2019.

22 Hugo Moreno, "How IT Service Management Delivers Value to the Digital Enterprise," Forbes, March 16, 2017.

23 "Shortage in cloud talent as cloud job seekers lag employer demand," CIO Dive, December 6, 2018.

24 Joe McKendrick, "Tech skills in most demand this year: data, cloud, and cybersecurity," ZDNet, January 7, 2019.

25 Dave Bartoletti, "Predictions 2019: Cloud Computing Comes of Age as the Foundation for Enterprise Digital Transformation," Forrester, November 8, 2018.

26 Nagendra Bommadevara, et al., "Cloud adoption to accelerate IT modernization," McKinsey, April 2018.

27 Nagendra Bommadevara, et al., "Cloud adoption to accelerate IT modernization," McKinsey, April 2018.

28 "25 Fastest Growing Cloud Companies," PwC, accessed May 28, 2019.

29 Louis Columbus, "State of Enterprise Cloud Computing, 2018," Forbes, August 30, 2018.

30 "Hybrid Cloud Market 2019," Heraldkeeper, February 8, 2019.

About

Digital Realty supports the data center, colocation and interconnection strategies of more than 2,300 firms across its secure, network-rich portfolio of data centers located throughout North America, Europe, Latin America, Asia and Australia. Digital Realty's clients include domestic and international companies of all sizes, ranging from cloud and information technology services, communications and social networking to financial services, manufacturing, energy, healthcare and consumer products.

Sales

P (877) 378 3282
E sales@digitalrealty.com

DIGITAL REALTY