#techvision2021

Security Technology Vision 2021

# Driving Resilience

## with Cyber Digital Twins

Voices of Change

From insights to action, the path to extraordinary value starts here.

accenture

# Executive Summary

Cyberattacks are escalating at a staggering rate globally. Accenture Security reported a triple-digit increase (125 percent) in intrusion volume across industries and geographies in the first half of 2021—driven by web shell activity, targeted ransomware, supply chain intrusions and dark web actors challenging IT and OT networks.[1, 2]

Tackling any one of these challenges is daunting, but the full onslaught could readily overwhelm an unprepared enterprise. Urgent action is needed. Fortunately, the security industry can seize the upper hand in resilience through a powerful technology innovation: intelligent cyber digital twins.

**When used in the cybersecurity space, intelligent cyber digital twins (i.e., contextual and progressively federated) provide the power to stop cyberattacks cold.** (See sidebar on "Types of digital twins" for definitions.) Security executives can use them now to fortify existing security practices without touching production environments, for example, by constructing a twin of the attack surface that can be used to mimic adversarial movements and assess the risk to business processes.

In time, intelligent cyber digital twins can be used to extend the security mindset throughout the organization and across business ecosystems by modeling and analyzing application security architectures or assessing security impacts of pending changes to a cloud environment. And ultimately, security executives can innovate with intelligent cyber digital twins to reinvent security approaches, build trust into the data supply chain, and secure the intelligent data mesh of the future mirrored world. (See sidebar "Envisioning a Mirrored World" for a description of this trend.)

In short, intelligent cyber digital twins provide much-needed capabilities to address a range of security challenges across the connected enterprise and its supply chain—allowing security teams to approach security with more rigor and operate with more confidence. In addition, transforming security approaches will enable business collaboration and intelligent data sharing at scale in an interconnected world, unlocking new growth opportunities.

According to our Accenture Technology Vision 2021, Leaders Wanted: Experts at Change at a Moment of Truth,[3] 80 percent of surveyed Chief Security Officers (CSOs) and Chief Information Security Officers (CISOs) across industries are already applying some form of digital twin technology in their security programs for uses such as prediction, extracting insights, simulation or testing. Yet only a fraction (12 percent) are actively using *intelligent* digital twins embedded with AI or machine learning in the majority (70 percent or more) of their organization's digital twin initiatives, indicating a significant opportunity for growth.

Intelligent cyber digital twins are a catalyst for the security industry to shift from reactive to resilient, from singular to collaborating forces of preventive security defense measures across a digital ecosystem.

**Are you ready to lead the security change forward?**

# Types of digital twins

Digital twins are virtual models of objects, systems, or processes that businesses use to generate analytics and insights. They've evolved from **singular** digital twins (e.g., of a jet engine or a house), into today's **contextual** tools embedded with artificial intelligence (AI), which makes it possible to explore what-if scenarios or make predictions based on real-time data (e.g., digitally manage a fleet of airplanes or a system spanning houses in a city built by a contracting company).

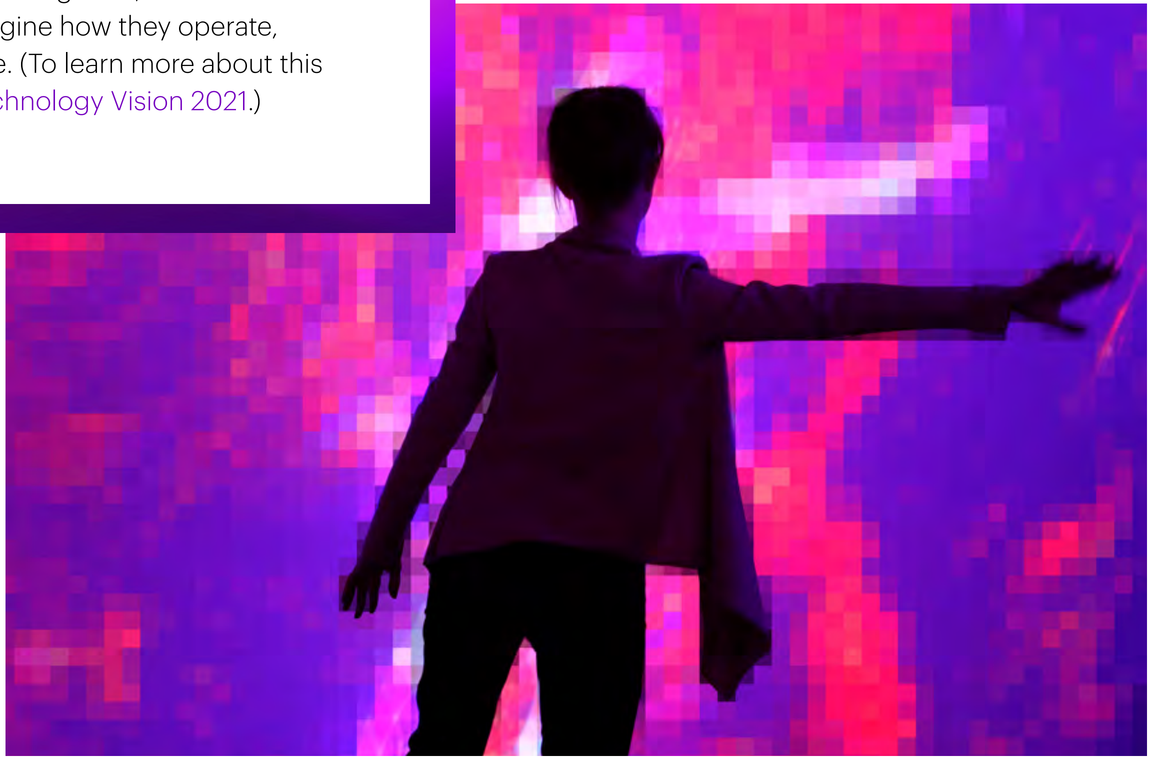
This evolution will continue: In the next few years, compute and store will be intertwined, enabling **federated** data models with many intelligent digital twins residing on edge, fog, and multi-cloud computing systems across domains (e.g., all houses and some buildings in a region or state interacting with utility companies). Further into the future, these intelligent digital twins will all be connected together to create a digital twin ecosystem and enable a **collaborative grid** (e.g., an entire model of a city, region, state with all houses, buildings, hospitals, police departments and fire stations) powered by autonomous data nodes as part of a secured, intelligent data mesh.

Whether centralized, distributed, federated, peers, edge or any other form of data topology, an intelligent data mesh could be configured to include any forms of digital twins and analytics or any other data domains in a secured and trusted manner.

# Envisioning a Mirrored World: Powered by massive, intelligent digital twins

Today, the technologies threaded through all aspects of the business generate massive amounts of data. Companies are increasingly unlocking the trapped value of this data by feeding it into intelligent digital twins, in some cases models of whole factories, supply chains, business processes, product or process life cycles, as well as the supporting application and IT infrastructure.

This is giving enterprises new capabilities to simulate, predict, and automate system behaviors, evaluate risk and impact, remove efficiency barriers, and optimize quality attributes like sustainability and security. As more of the physical world is represented in digital space, it will evolve toward massive networks of intelligent digital twins and create a Mirrored World in which enterprises can bring data and intelligence together, ask and answer big questions, and reimagine how they operate, collaborate, and innovate. (To learn more about this trend, see Accenture Technology Vision 2021.)



# Win with Intelligent Defense

Despite spending significant time and money, today's enterprise defenses are challenged with the mounting complexity, frequency, and scale of cyberattacks.

## Whether geopolitical actions, nation state campaigns, fraudulent schemes or ransomware, attackers are getting bolder in their ambitions and better at exploiting weaknesses—creating costly security headaches for companies.

It might be a single bad actor intent on hacking an enterprise system or a nation state attempting to wreak havoc on critical infrastructure, such as transportation or energy grids. The threats are coming at an increasing rate.

At the same time, many companies are forging ahead with compressed technology transformation—including a rapid move to cloud—to operate and compete at an unprecedented speed and scale while unlocking greater flexibility, agility and new growth opportunities. Yet this migration and hybrid IT surface is also stretching the enterprise in new ways that need to be secured, including a new usage of native cloud services along with adjusted application security and cyber security controls. Add to this the rapid uptake of Internet of Things (IoT) devices, edge and fog computing, and increased capacity of 5G networks, and the attack surface is stretched even further across multiple domains of information technology (IT) and operational technology (OT). The result? More potential for hacks like Colonial Pipeline or SolarWinds that have substantial business and societal impacts.

64%

of security leaders expect their organization's investment in intelligent digital twins to increase over the next three years.

Source: Accenture Technology Vision 2021 survey

**But now an important shift is in the works, thanks to intelligent cyber digital twins. It's an innovation that helps put the security industry into a more proactive position—allowing enterprises to run with confidence on localized IT and OT infrastructure, or with cloud applications and native cloud services.**

Using intelligent cyber digital twins, organizations can safely and effectively become more resilient through three actions:

## Fortify

Near term, security leaders can better protect underlying infrastructure and systems by using intelligent cyber digital twins to understand attackers' mindsets and potential attack patterns, and to simulate attacks and their impact on business processes and sensitive targets.

## Extend

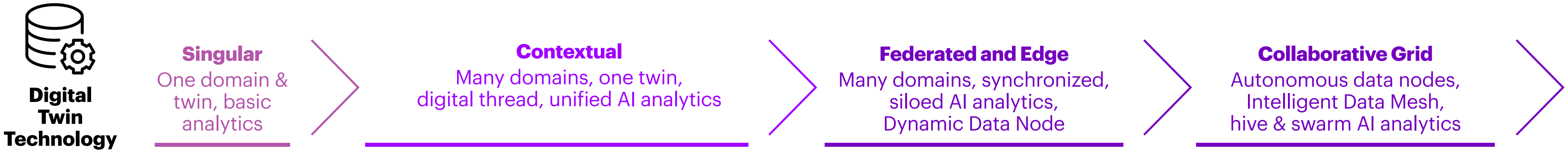
In the next three to five years, security leaders can embrace security by design with dynamic and predictive analytics, which in turn will change the very nature of how security teams work. This includes using intelligent cyber digital twins to evaluate changes constantly in the infrastructure—between on-premise data centers, connected devices, edge computing, and multi-cloud environments.

## Reinvent

Looking further into the future, security leaders can secure a fully interconnected Mirrored World by using intelligent cyber digital twins to preserve trust in the data flow, and architecting security into the forthcoming intelligent data mesh.[4]

The following sections examine the opportunities and implications of each area, followed by suggestions for how to effectively apply intelligent cyber digital twins for enterprise security.

## The journey of digital twins technology



**Digital Twin Technology**

**Singular**
One domain & twin, basic analytics

**Contextual**
Many domains, one twin, digital thread, unified AI analytics

**Federated and Edge**
Many domains, synchronized, siloed AI analytics, Dynamic Data Node

**Collaborative Grid**
Autonomous data nodes, Intelligent Data Mesh, hive & swarm AI analytics

Much of today's digital twin use is focused on enterprise siloes or specific use cases to drive efficiency for **singular** digital twins. However, **contextual** intelligent digital twins of larger, more complex entities are emerging, including models of entire factories and interlaced production lines, city infrastructure and populations, transportation and mobility, sustainable supply chains and the related impact on multiple business processes, the life cycles of compound products, buildings and their tenants, or stores and their customers' digital twins.

As these are linked together in the next three to five years, companies will move toward using **federated and edge-based** intelligent digital twins, as well as any data topology that best fits the business data and application layout. In the future, as the Mirrored World becomes ubiquitous, this will evolve into a **collaborative grid** of intelligent digital twins, passing data and analytics between collaborated digital twins' nodes.

Of critical importance, each type of digital twin requires embedded security from the start, especially as companies move into the fully emulated world. Otherwise, the future could quickly become a confusing hall of mirrors. **Knowing this, security leaders can begin clearing hurdles now by adding security intelligence into how all their digital twins work, think and manage sensitive data**. The business evolution from federated and edge to collaborative grid will also require managing security—integrity, confidentiality, availability—into the fabric of the business.

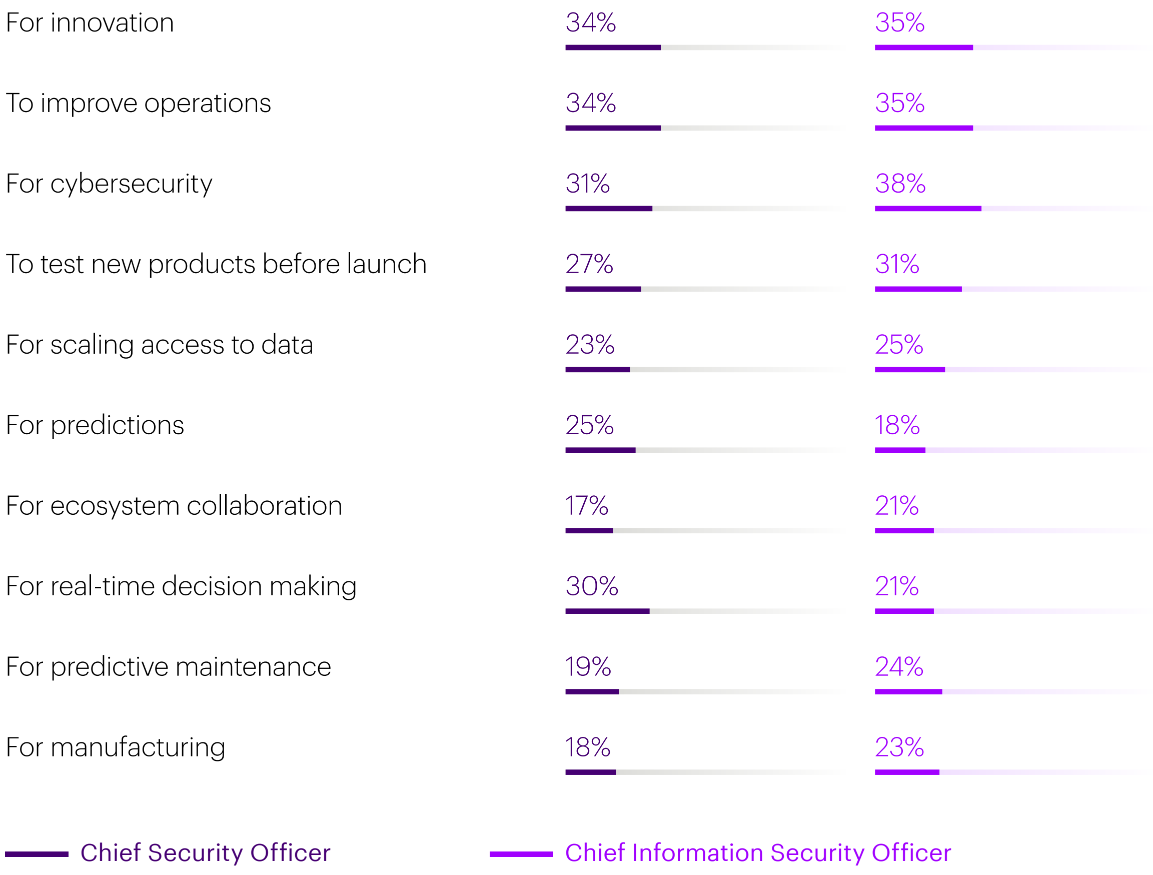
# Fortify

## Welcome to the Security Sandbox

In the immediate term, think of intelligent cyber digital twins as a sandbox for security innovations— enabling security leaders to meet critical enterprise requirements, forecast and manage IT and OT security as well as cloud application security across a range of use cases (see Figure 1).

**What-if scenarios**—Currently, security teams test the security of a system or process just before deployment, and in many cases evaluate changes on deployed applications. Intelligent cyber digital twins change this model by making it possible to evaluate changes *as if* they were made on the real deployed application, without touching the actual application—a much-needed capability sought by security leaders. Companies can simulate risks on demand at scale and do shadow analysis on the digital replica of an enterprise, monitoring cyber and security aspects in relation to business processes, in a way that precisely reflects their real-world business impacts—all without affecting production environments. This enables enterprises to explore the security of a future configuration or architecture—understanding strengths or weaknesses, susceptibility to attacks, and where risks are concentrated to continuously improve defense implementation measures and security controls investment strategies.

**Figure 1: Security executives are using digital twins for a variety of use cases.**



Source: Accenture Technology Vision 2021 survey

Facebook, for example, has created a simulator, called WW, based on the company's real code base. In WW, AI-powered bots mimic both innocent Facebook users as well as bad actors attempting to conduct a range of harmful behaviors—like scamming people. Facebook engineers can then implement various strategies to stop or constrain this behavior in the simulator and test the effect on the bots.[5] Likewise in the manufacturing industry, manufacturers can use intelligent cyber digital twins to ensure software integrity prior to updating software patches over the air to market-deployed products, such as vehicles or electronics.

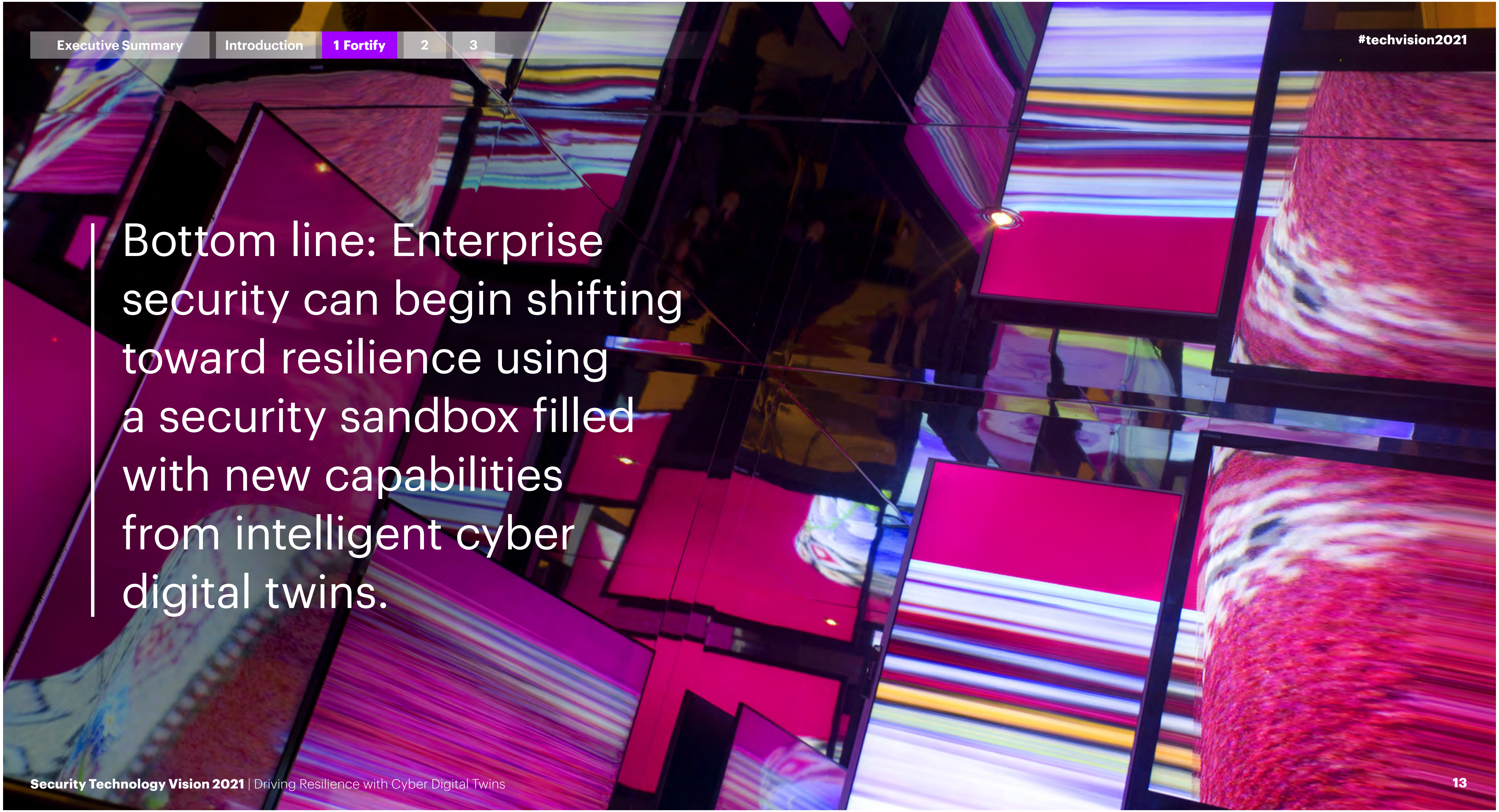
**Predictive analytics**—More often than not, current security practices yield 20/20 hindsight. However, security leaders can use insights from cyber evidence to anticipate what might be a problem tomorrow or even further into the future by cascading digital twins' interactions. This ability to evaluate and reduce risk proactively keeps the enterprise one step ahead of adversaries.

On a larger scale, intelligent cyber digital twins support scenario planning for resilience. Security teams can impersonate the possible moves of adversaries and defuse incidents before they happen. Armed with AI-driven analytics, security teams will have information on what attackers can exploit and foresight on how the adversary could move and where to best stop the attack paths. These simulations will replace postulations about the future with data-driven decision making, helping to provide assurance that the infrastructure and business is resilient.

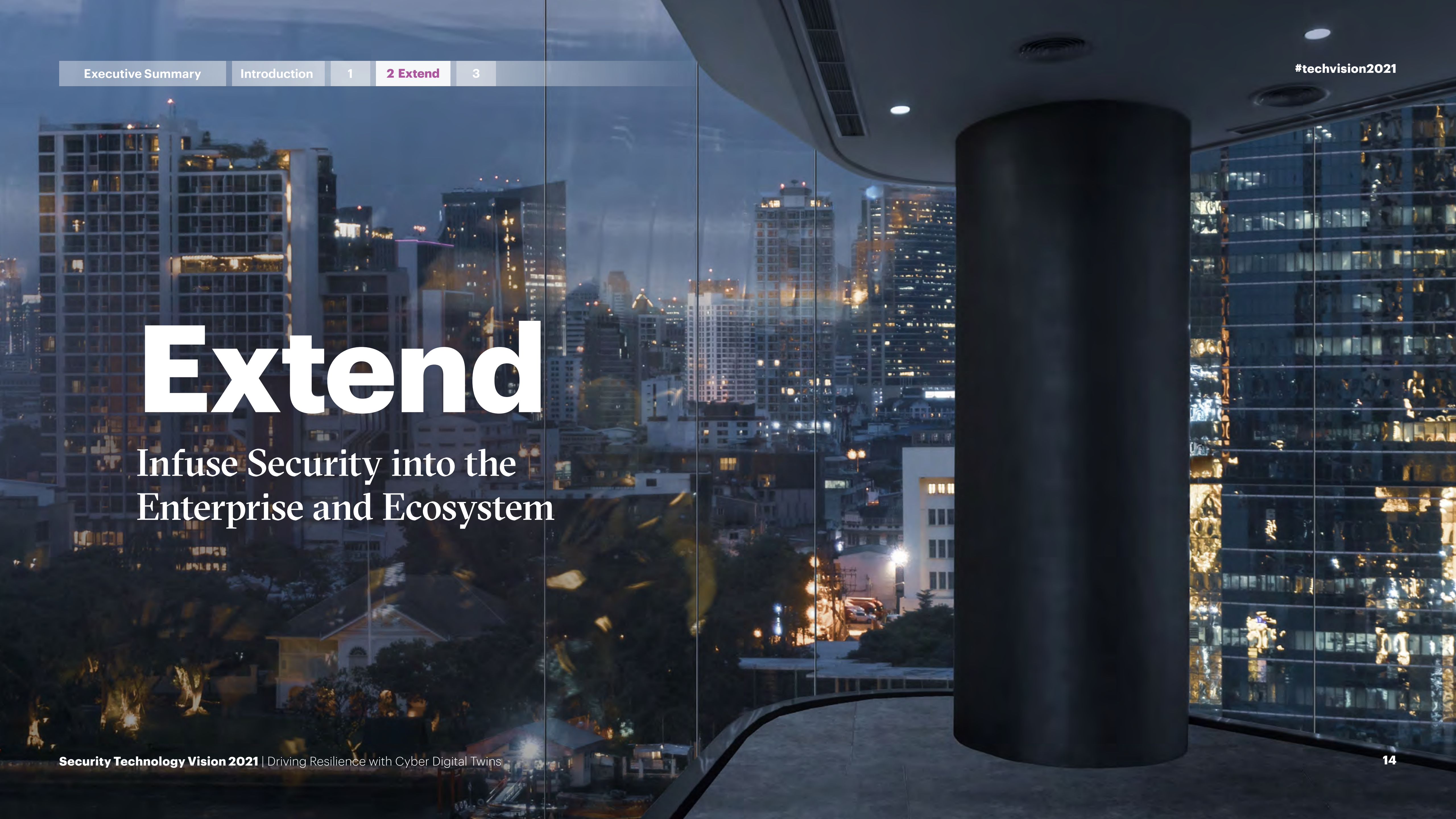
**Prioritized action**—With threats emanating from every direction, security teams can spend significant time on prevention and remediation activities but still not take the biggest risks off the table. The AI and analytics in intelligent cyber digital twins make it possible to ask key questions and prioritize actions based on risk, cost, importance of asset, or ease of remediation to manage an incident more effectively. This not only improves a security leader's ability to focus security resources on the right tasks, but also to measure how much risk has been reduced and which technologies are most effective in reducing that risk.

Today, for instance, it's difficult to map cyber risks to business processes for operational technology/industrial control systems (OT/ICS). The time-consuming and manual effort quickly becomes obsolete. To meet this challenge, Accenture Labs collaborated with OTORIO on a proof of concept with Accenture's intelligent cyber digital twin platform (CyTwin).* Using real-world manufacturing data from a pulp and paper mill, the team showed which industrial processes in the physical world posed the greatest security risks, accounting for actual cyber-attack possibilities and OT underlying risk elements.[6] Accenture CyTwin automatically prioritized the risks to address first and recommended the best way to overcome each challenge. Further integration with managed security services in OT/ICS environments would enable predictive adversarial detection based on the impact to a company's specific business processes.

* Accenture CyTwin is an intelligent cyber digital twin solution developed by Accenture Labs that offers companies clear, consolidated visibility into their security postures. By ingesting data and doing advanced analytics, CyTwin shows companies the pathways attackers could exploit to penetrate their critical systems and tracks lateral movement through a network. It also estimates the impact of potential breaches at scale and helps businesses to prioritize remediation actions that mitigate the biggest risks.



Bottom line: Enterprise security can begin shifting toward resilience using a security sandbox filled with new capabilities from intelligent cyber digital twins.



# Extend

## Infuse Security into the Enterprise and Ecosystem

Beyond fortification, in the next three to five years intelligent cyber digital twins can improve the approach to the early stages of system, application and data design by making sure the security architecture and subsequent controls will deliver the required security for business resilience and agility.

The security automation built into the twins will also free up security teams to focus on higher-level, more strategic work. In particular, the simulation capabilities will give cyber defenders a superpower, boosting their readiness according to the defended targets, complexity of the cyberattack surface, and other risk assessment algorithms. It's a continuous opportunity to improve the scope and scale of security across the enterprise and into the ecosystem of business partners.

**Security by design**—Security leaders can extend the philosophy of DevSecOps, a methodology that weaves security into individual software application development sprints, into a broader security-by-design mentality across the enterprise infrastructure and even the company culture by adding a DataSecOps layer. Intelligent cyber digital twins make this possible by proactively assessing the architecture and controls of any IT decision for its future security value—whether it's a routine security patch or application upgrade; a more complex system migration or infrastructure consolidation due to merger/acquisition; or a net-new development of product and service innovations.

Take the ongoing efforts for enterprise cloud migration. As companies transition more of their core systems (i.e., mainframes, ERP systems, etc.) to the cloud, they must not only protect the migration process, but also rearchitect for secure business operations in the cloud. This includes taking advantage of the built-in security features offered by cloud providers, making it possible to develop in a native cloud environment that is secure from inception. For example, intelligent cyber digital twins can be used to assess, architect, and simulate cloud solutions to determine the best fit for a company's business requirements, while prioritizing security recommendations, requirements, and security controls investments at key steps in a cloud migration journey.

Longer term, the automation possibilities available through intelligent cyber digital twins can mechanize certain actions and even auto-remediate through managed security services (MSS) overlooking the infrastructure. Enterprises at this higher state of maturity will be able to design fail-safe and secure scenarios into critical systems, which will boost the security industry to proactive self-healing.

85%

of security officers agree that AI combined with digital twins will allow their organizations to scale [up defenses and situational awareness] in ways that are not otherwise possible.

Source: Accenture Technology Vision 2021 survey

**Strengthening ecosystem security**—Intelligent cyber digital twins will make it easier to share contextual and federated data at scale with business partners. (See the "Secure Us to Secure Me" trend in Accenture Technology Vision 2019 for more information on this business need.) In a hyperconnected world, enterprises are only as strong as the weakest link. Case in point: The security of the global software supply chain came into hyper-focus after the SolarWinds compromise.

Using intelligent cyber digital twins, security leaders could automatically route relevant cyber-activity details to ecosystem partners, IT/OT managers, cloud providers, industry consortiums or government agencies. Other entities might be experiencing similar or corollary events, and the insights could be helpful for the whole ecosystem to predict and neutralize future attacks.

**Securing domain-based business opportunities**—Ultimately, collaborated and intelligent cyber digital twins could interact across different domains, unlocking new business opportunities or customer value. Agreeing on the interrelationship of ontologies and how to set those up across the domain would be the first step.

Take the travel industry as an example: Currently, travelers must prove their identity at multiple checkpoints—when purchasing a ticket online, checking in at the physical airport, going through airport security, getting on a plane, exiting through customs, and checking in at a hotel—each experience requiring independent registration, proofing and sharing of data.

An intelligent cyber digital twin that protects a digital twin of an opted-in person could expedite and improve this experience by correlating geographical and digital identity information in advance across multiple companies and governmental agencies, with the individual determining what data can be shared with each domain partner. Of course, this type of service would need to adhere to governance and compliance limitations on data movement or data sovereignty, such as the case of privacy or other data regulation, which would also be managed by the intelligent cyber digital twins.

Another example comes from the retail industry. Imagine transforming a retail customer loyalty program in the world of intelligent digital twins. Loyalty customers already expect retailers to know their preferences but could take it further to create bespoke experiences in a store that are correlated to a customer's movements. The store layout would be extracted from the location and layout services and form a local digital twin on the store's edge computer. The retailer could access an active identified customer preference just-in-time from the loyalty system and incentivize the customer to move to another section of the store to examine and potentially buy the related products, according to real-time inventory pulled from the inventory system. In this example, securing such a grid of consumer and stores' digital twins would require a cyber counterpart. This would ensure privacy and roaming conditions would be adhered and managed since consumers might interact with the digital store, as well geolocated brick-and-mortar stores with different security and privacy policies.

Bottom line: By extending the capabilities of intelligent cyber digital twins, enterprises can speed the shift to resilience through security by design, increased ecosystem partner security, and secure product or service innovations.

# Reinvent

## Securing the Mirrored World and Intelligent Data Mesh

In the future, nearly everything in the physical world—city infrastructure, buildings and homes, factories and agricultural fields, transportation grids, supply chains, retailer stores, consumer products, and more—will be represented as a twin. Melding these sophisticated digital twins will usher in the Mirrored World and fundamentally change the way businesses and governments operate and innovate.

Without security baked into the core management of intelligent digital twins, however, the progression will result in a real-world-sized playground for cyberattacks—the potential for hacks will be anywhere and everywhere, and they will be extremely difficult to secure. Fortunately, security leaders can get ahead of the game starting now. How? By aggressively adopting a zero-trust security approach that requires all users to be continuously authenticated, authorized and validated before being granted or keeping access to applications and data. Applied to digital twins this means continually securing the twins, the data, and the analytics at each juncture. This will unlock the full potential of the future collaborative grid.

**Securing the data flow**—It's no secret that it will be very challenging to secure the data moving between intelligent digital twins, including the AI that manages the analytics and makes the predictions. But it's a necessity as mistakes will be amplified in the Mirrored World: Tampering with the AI of one twin, for example, could have an exponential misinformation effect.

The trustworthiness of the data supply chain will be of paramount importance. Data lineage—where transparency into the origin of the data and insights into the "breadcrumb trail" of where it's been and what happened to it along the way—will be more critical than ever. Security leaders can use intelligent cyber digital twins to smartly manage this data lineage in distributed ecosystems from end to end, controlling the data supply chain that comes in and the data value chain that goes out to other entities.

In time, entire industries, networks of business ecosystems, nation states and governmental agencies will harvest massive amounts of data from intelligent digital twins—forming a need for secure and responsible governance. It will be essential to maintain data sovereignty, protect citizens' privacy, adhere to data regulations policy, and gain insights without bringing all the data into one system. Sharing trusted data will lead to trusted decision-making at the IT, OT, and application levels—enabling multiple stakeholders to address big problems together in the physical world.

90%

of security leaders agree that trust is a crucial element in transforming the relationship between people and emerging technologies and must be built into design and experience. Intelligent cyber digital twins are a tool to demonstrate that trust.

Source: Accenture Technology Vision 2021 survey

As shown in Figure 2, one solution lies in a flexible "mesh" of integrated and intelligent digital twins—with each **data node** encapsulated securely, creating data building blocks that are secure by design. This approach would help to ensure trusted collaboration, plus endless scaling and permutations of data interactions. With secure data nodes, enterprises could manage data governance, map data flow configurations, and collaborate across ecosystems to solve real-world problems.

Imagine this approach applied in a future smart city. Intelligent digital twins would manage the interactions of buildings, vehicles, drones, infrastructure and more. And the data nodes representing each entity would be fully secured. Now imagine an accident occurs on one of the city streets and first responders (i.e., fire fighters, police officers, medical professionals, other field units, etc.) need to be routed quickly to the emergency. How could multiple intelligent digital twins representing these different field units interact in a secure, trusted manner?

An intelligent, peer-to-peer mesh could provide a divide-and-conquer approach to each group of first responders with the ability to manage their relative responsibility, while interacting securely with the digital twins of other units. In this case, the intelligent cyber digital twins could perform complex situational analysis in real-time, in which some will employ analytics performed at-the-edge to support each field unit, while other analytics will be performed over the cloud.

Figure 2: Securing the data nodes will lead to a secure and intelligent data mesh (Copyright Accenture)

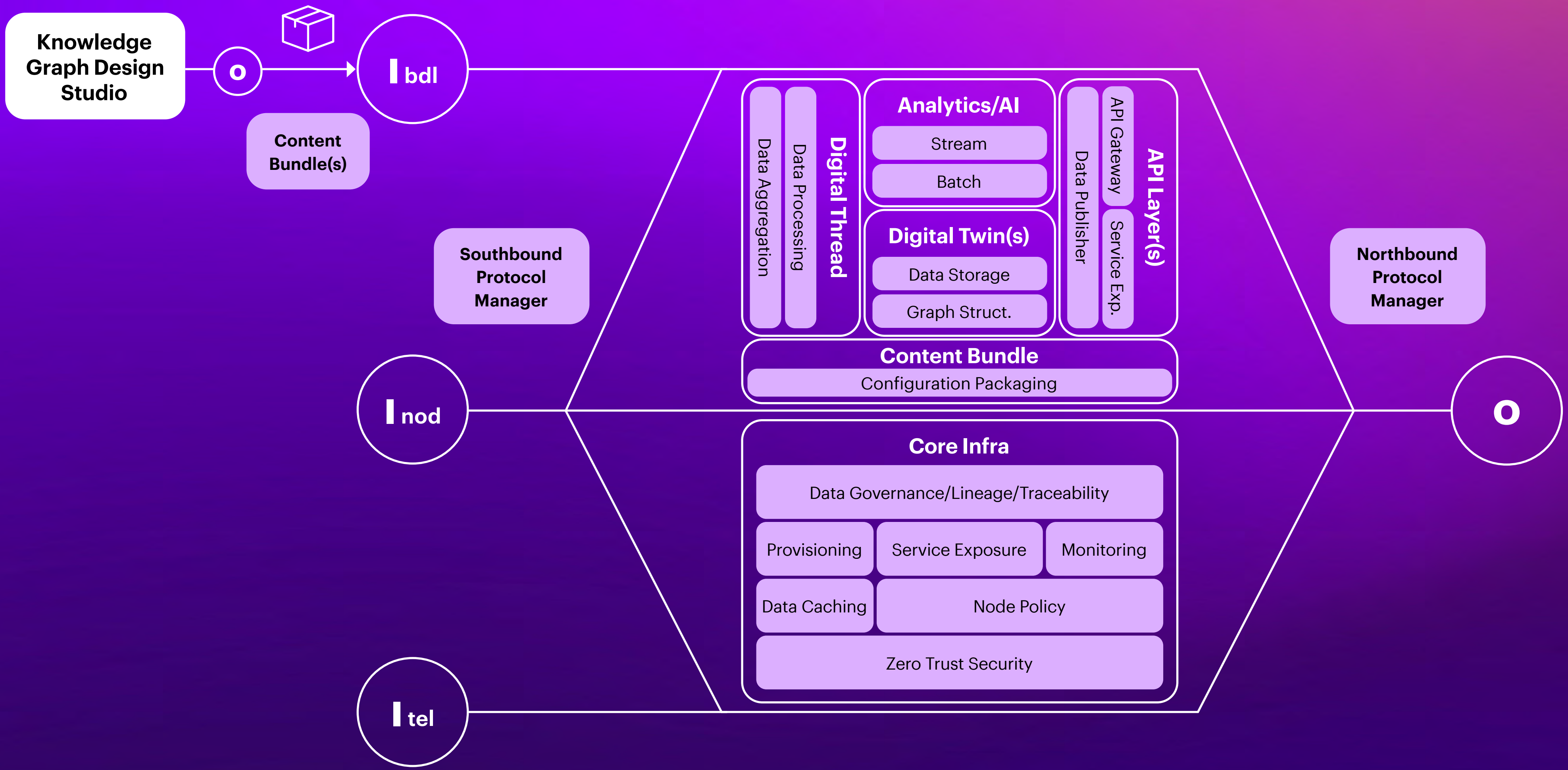
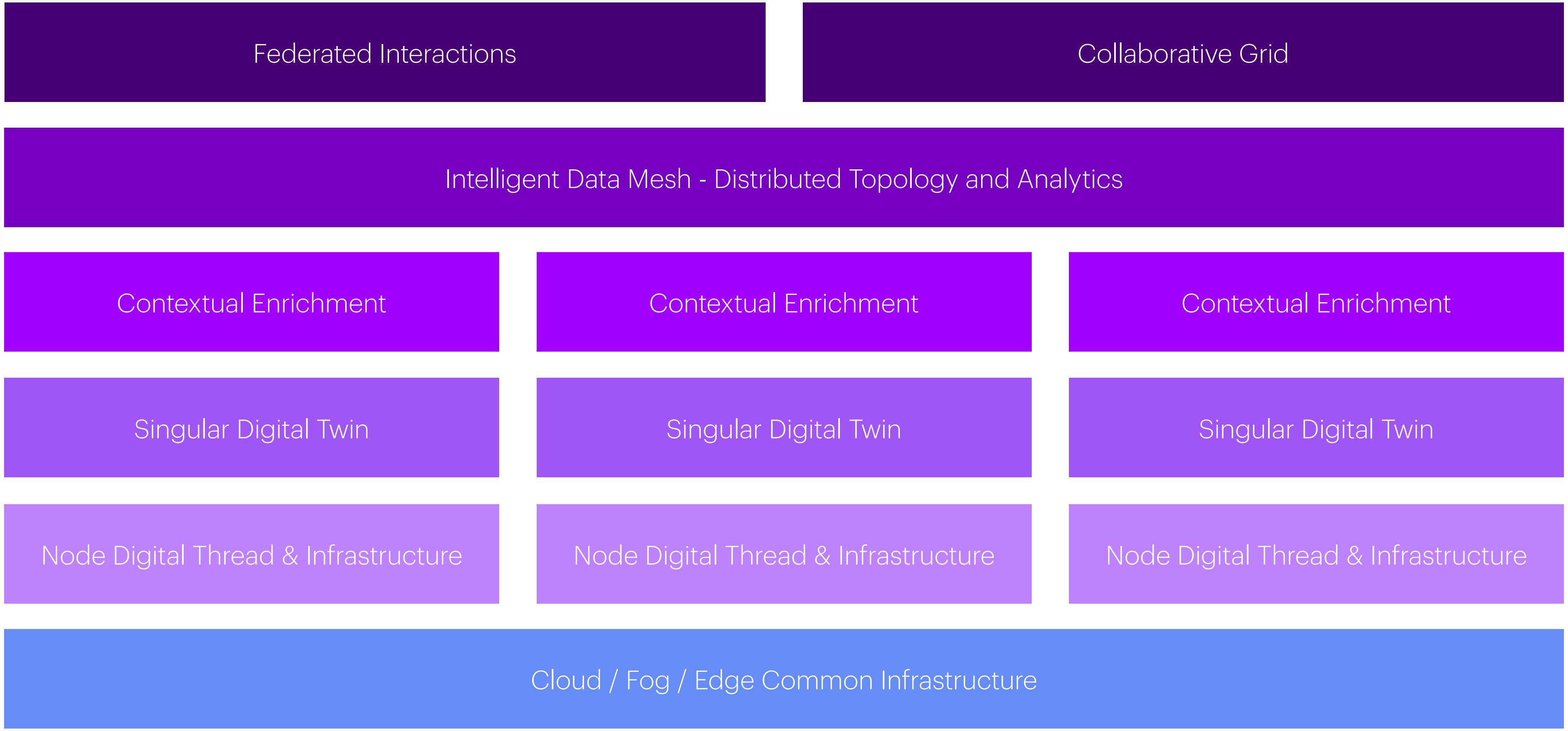


**Figure 3: Modular architecture of secured data nodes, digital twins and intelligent data mesh (Copyright Accenture)**



Federated Interactions

Collaborative Grid

Intelligent Data Mesh - Distributed Topology and Analytics

Contextual Enrichment

Contextual Enrichment

Contextual Enrichment

Singular Digital Twin

Singular Digital Twin

Singular Digital Twin

Node Digital Thread & Infrastructure

Node Digital Thread & Infrastructure

Node Digital Thread & Infrastructure

Cloud / Fog / Edge Common Infrastructure

> Bottom line: To maximize the shift to resilience, security executives must embrace security across their entire portfolio of intelligent digital twins, protecting the data itself and how its structured. Starting now will give the business the agility it needs in the forthcoming Mirrored World.

# Conclusion

## Fully resilient and ready for the future

Whether your organization's security function needs to fortify, extend, or reinvent, intelligent cyber digital twin technology will provide the critical capabilities to reach the next level of resilience.

**Are you ready to make the shift?**

# Decision Points

According to our Accenture Technology Vision 2021 survey, business and IT executives are already using digital twins in a variety of ways across their organizations (see Figure 4). To move from reactive to resilient, security executives must secure these assets now while taking additional steps toward using intelligent cyber digital twins.

**Figure 4: Digital twins usage by enterprise role**

| | Chief Information Officer | Chief Innovation Officer | Chief Marketing Officer | Chief Technology Officer | Chief Supply Chain Officer | Chief Strategy Officer | Director, IT |
|---|---|---|---|---|---|---|---|
| For innovation | 40% | 41% | 32% | 33% | 29% | 37% | 31% |
| To improve operations | 34% | 31% | 33% | 29% | 24% | 38% | 34% |
| For strategy development | 30% | 32% | 31% | 32% | 25% | 36% | 24% |
| For monitoring | 24% | 26% | 21% | 23% | 32% | 25% | 25% |
| For real-time decision making | 21% | 22% | 23% | 25% | 30% | 24% | 18% |
| For predictive maintenance | 22% | 24% | 21% | 19% | 30% | 19% | 16% |

Source: Accenture Technology Vision 2021 survey

# Fortify/Tactical

## Where is my enterprise with digital twin usage today?

- Identify where the business is using digital twins or where they could strategically move to an intelligent digital twin to gain more agility and insights. Within the security program, determine which areas could benefit from intelligent cyber digital twins to improve current security practices and optimize existing investments in security.

- Introduce data management practices that enable intelligent digital twins and apply security by design approaches into business implementations. Build in the controls and guardrails for data governance and protection from the beginning.

- Use intelligent cyber digital twins to evaluate risks at scale in critical business processes: the quick data ingestion and rapid discovery will make it easier to block, tackle and remove incorrect configurations and limit impacts in production.

- Demonstrate proactive risk management strategies through intelligent digital twin analytics. Prioritize security actions automatically from highest to lowest risk at any point in time according to visible security-to-business alignment over the intelligent cyber digital twins.

# Extend/Strategic

## What should our company do to increase security effectiveness internally and across our business ecosystem?

- Leverage the ongoing results from what-if scenarios and risk simulations to identify exploitable vulnerabilities of the infrastructure and to evaluate architecture or vendor future changes that will measurably improve security posture.
- Introduce new security investments and practices with confidence, knowing ROI on the transformation journey before spending the money.
- Federate data sharing with business partners to better secure the broader ecosystem. Move to automated/managed security services between ecosystem business partners and eventually across domains.

# Reinvent/Visionary

## How should our company secure the Mirrored World?

- Protect both enterprise and broader ecosystem of connected digital twins, including the AI that makes predictions or monitors situational awareness.
- Improve trustworthiness of data and minimize tampering across all interactions.
- Secure the stability and integration of the data supply chain feeding into collaborative- or mesh-based ecosystems of digital twins.
- Architect security by design into the intelligent data mesh by securing the data nodes.

# Authors

**Lisa O’Connor**
Managing Director
Global Lead
Cybersecurity Research and Development
Accenture Labs
lisa.oconnor@accenture.com

**Kelly Bissell**
Senior Managing Director
Global Lead
Accenture Security
kelly.bissell@accenture.com

**Marc Carrel-Billiard**
Senior Managing Director
Technology Innovation Lead
marc.carrel-billiard@accenture.com

**Ethan Hadar**
Managing Director
Chief Research Officer
Accenture Labs - Europe
ethan.hadar@accenture.com

# References

1 2021 Cyber Threat Intelligence Report. (2021, July 15). Accenture: https://www.accenture.com/us-en/insights/security/cyber-threat-intelligence-report-2021

2 Triple digit increase in cyberattacks: What next? (2021, August 4). Accenture: https://www.accenture.com/us-en/blogs/security/triple-digit-increase-cyberattacks

3 Accenture Technology Vision 2021 survey of 305 Chief Security Officers (CSOs) and Chief Information Security Officers (CISOs)

4 Accenture Technology Vision 2019: Secure US to Secure ME. (2019, February 7). Accenture: https://www.accenture.com/us-en/insights/technology/cybersecurity-digital-ecosystem

5 Ahlgren, J., Berezin, M.E., Bojarczuk, K., Dulskyte, E., Dvortsova, I., George, J., Gucevska, N., Harman, M., Laemmel, R., Meijer, E. and Sapora, S., 2020, June. WES: Agent-based user interaction simulation on real infrastructure. In Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops (pp. 276-284). Facebook: https://research.fb.com/publications/wes-agent-based-user-interaction-simulation-on-real-infrastructure/

6 A Moment to Innovate. (2021, March 3). Accenture: https://www.accenture.com/us-en/blogs/technology-innovation/billiard-a-moment-to-innovate-turning-data-into-action-with-intelligent-digital-twins

## Research Methodology

Accenture Research conducted a survey of 305 Chief Security Officers (CSOs) and Chief Information Security Officers (CISOs) as part of global research for Accenture Technology Vision 2021 to capture insights from business and IT executives into the adoption and use of emerging technologies. The survey, fielded from December 2020 through January 2021, helped identify the key issues and priorities for technology adoption and investment.

## About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services—all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 569,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at **www.accenture.com**

## About Accenture Labs

Accenture Labs incubates and prototypes new concepts through applied R&D projects that are expected to have a significant impact on business and society. Our dedicated team of technologists and researchers work with leaders across the company and external partners to imagine and invent the future.

Accenture Labs is located in seven key research hubs around the world: San Francisco, CA; Washington, D.C.; Dublin, Ireland; Sophia Antipolis, France; Herzliya, Israel; Bangalore, India; Shenzhen, China and Nano Labs across the globe. The Labs collaborates extensively with Accenture's network of nearly 400 innovation centers, studios and centers of excellence to deliver cutting edge research, insights and solutions to clients where they operate and live. For more information, please visit **www.accenture.com/labs**

Disclaimer - This content is provided for general information purposes and is not intended to be used in place of consultation with our professional advisors. This document refers to marks owned by third parties. All such third-party marks are the property of their respective owners. No sponsorship, endorsement or approval of this content by the owners of such marks is intended, expressed or implied.