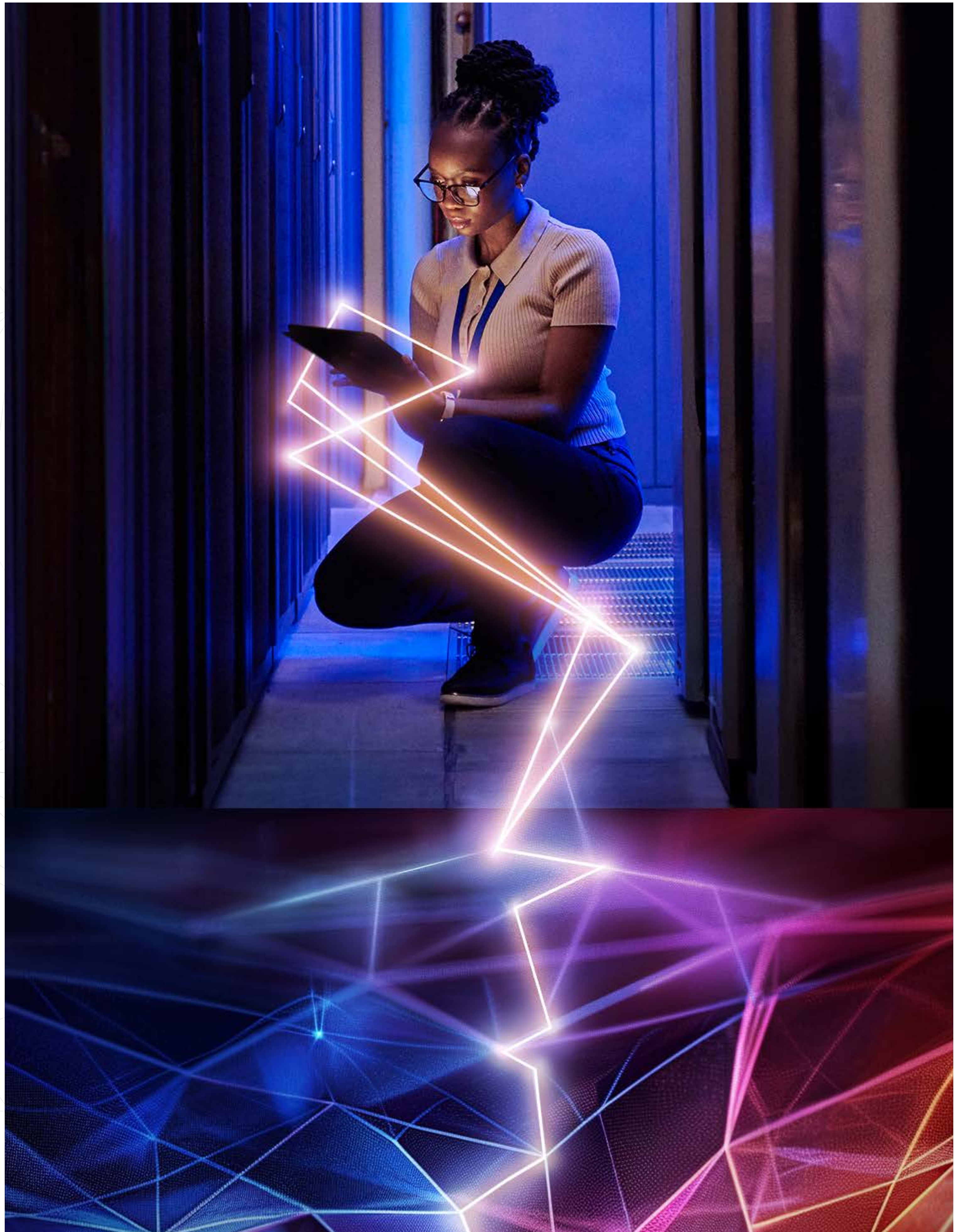
# Securing the Digital Core in the Gen AI Era

Cybersecurity as a strategic enabler of reinvention

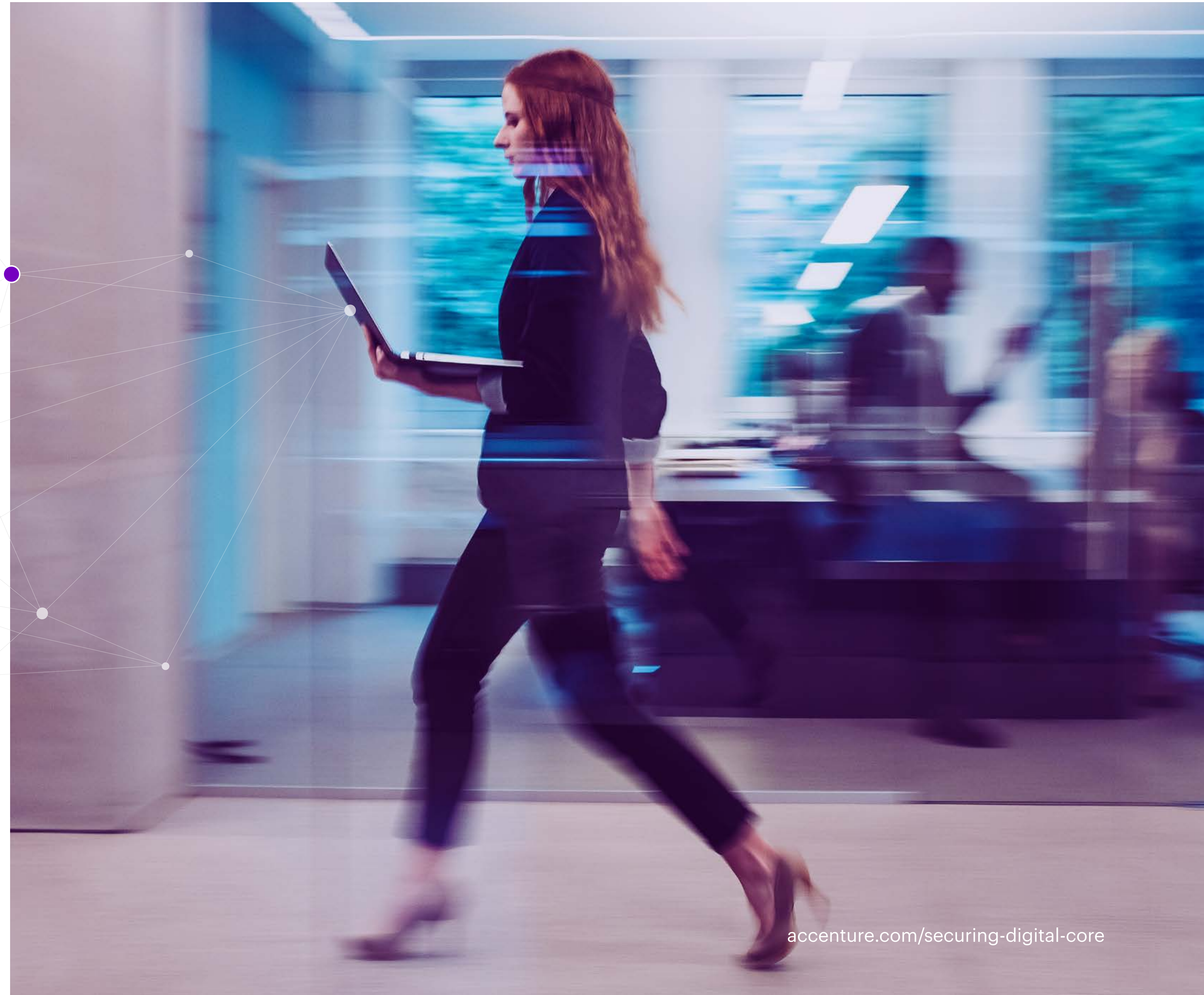
accenture



# Contents

# Executive summary

Companies are racing to build their digital cores to reinvent every part of business with generative AI. However, many are falling behind when it comes to securing critical technology layers from unauthorized access or attacks.



accenture.com/securing-digital-core

**Security is integral to a digital core as its three sets of technologies—digital platforms, a data and AI backbone and the digital foundation where security resides—constantly interact with each other to power reinvention. In our recently published research, Reinventing with a Digital Core, we found organizations with industry-leading capabilities—defined as the top quartile in our Digital Core Index—experienced a 20% higher revenue growth rate and a 30% increase in their profitability.**

Evolving to such an industry-leading state requires leveraging the right mix of tools and practices for agility and innovation, along with security capabilities and resilience. Of that mix, security can move beyond a static defense mechanism. If companies integrate security measures into the fabric of their evolving digital landscape, it can become enabler of business growth and transformation.

That's easier said than done. We found, on average, a 23-point lag in security capabilities[1] based on our Digital Core Index for companies that have yet to achieve an 'industry-leading' digital core. These organizations fall behind their leading competitors in key areas such as securing development, security and operations (DevSecOps), implementing Zero Trust identity and network models, automating security configurations, conducting threat modelling and protecting cyber-physical and edge systems.

As generative AI and other disruptive technologies accelerate innovation and redefine industries, they also expand the threat landscape, opening more avenues for malicious actors. In the race to adopt these technologies, companies often prioritize speed over security—neglecting early security integration, which increases risks and prolongs remediation efforts. This reactive approach also accumulates technical debt, leading to costs far greater than if security had been embedded from the start.

Today, organizations rely on 76 security tools, on average, to manage their security posture, a number that is growing[2]. For example, the amount of new or modified configuration settings from cloud service providers is now in the thousands every month, with security teams scrambling to keep systems secure and up to date. Such complexities often create redundancy, increase the risk of misconfigurations and complicate integration efforts, diminishing the efficiency of security outcomes. Combined with talent shortages, this means some 4.8 million cybersecurity jobs worldwide are unfilled—hindering the effective scaling of security solutions[3].

The Digital Core Index assesses organizations' enterprise technology stacks across each of the seven pillars of the digital core, using 39 subcomponents to develop our Digital Core Index (normalized to a scale of 100). Capability points represent the relative sophistication of a given technology. Gaps represent technology modernization activities needed to achieve the next level of capability.

# How can organizations close this security maturity gap?

Security is a competitive differentiator—it fosters an environment where trust, resilience and adaptability are at the forefront. This allows organizations to navigate reinvention confidently while seizing new opportunities for progress and competitive advantage.

Building robust security is a journey, not a sprint. Organizations can activate three strategic levers to transform their security to run at the speed and scale the business needs while driving down costs and reducing technical debt.

## Lever 01

### Streamline

Organizations must consolidate vendors and adopt integrated tools while retiring legacy ones. Harnessing the capabilities of generative AI can dramatically reduce the number of security tools in use. This technology can streamline processes, automate routine tasks and enhance decision-making by providing advanced insights and threat analysis.

## Lever 02

### Modernize

Security must modernize its tools and strategies to keep pace with the evolving digital landscape. For example, by adopting Infrastructure as Code (IaC) with built-in security scanning for code repositories and pipelines, security configurations can be standardized and testing seamlessly integrated into the development process. Transitioning to Software-as-a-Service (SaaS) and cloud-hosted security management systems can not only cut down on the time and costs associated with managing hardware, servers and updates, but also enhance threat detection, improve compliance and accelerate deployment.

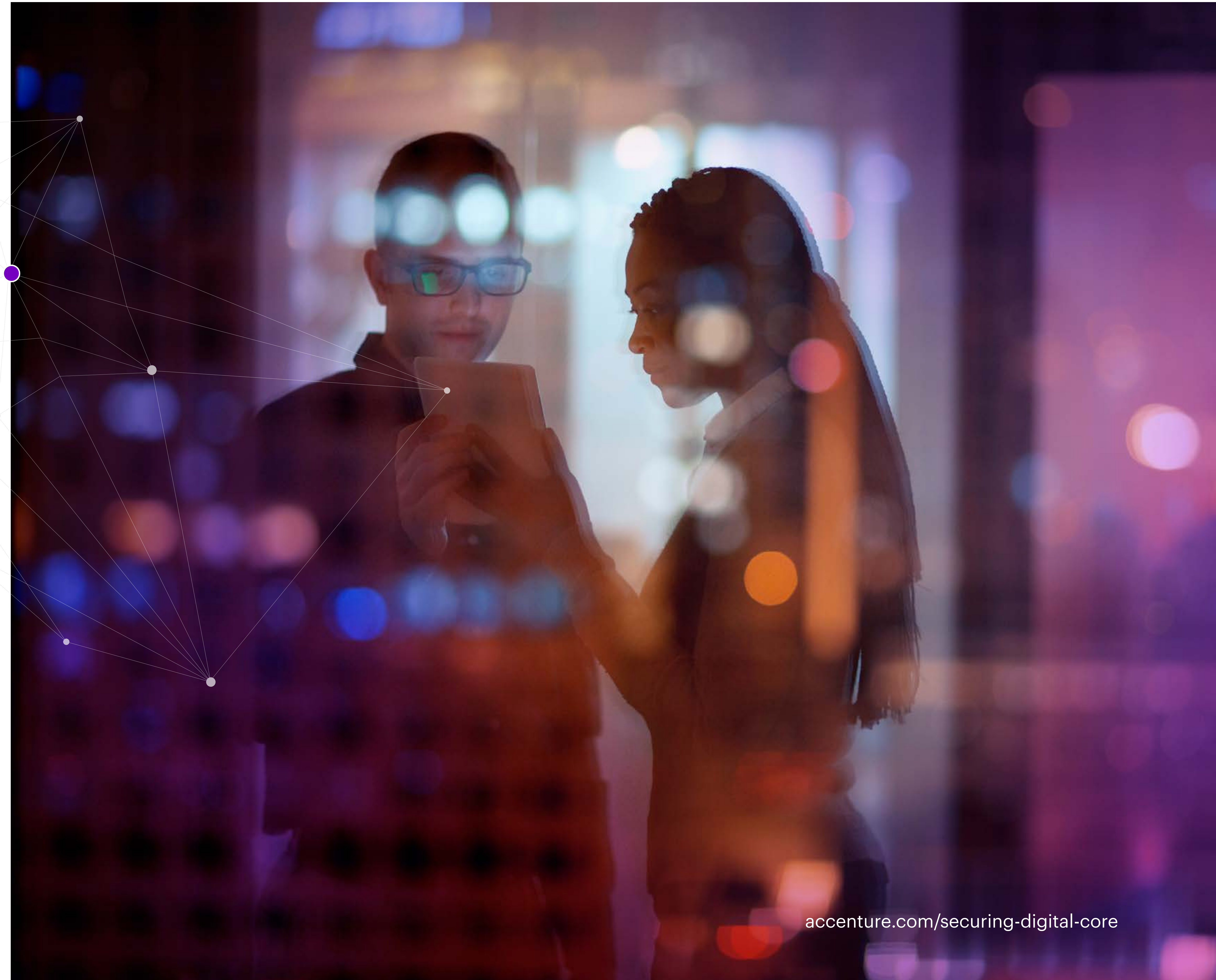
## Lever 03

### Scale and evolve

Automation and Cybersecurity-as-a-Service (CSaaS) can help scale security. For example, using generative AI-driven defense solutions for threat testing such as automated red teaming and penetration testing. These tools are especially timely as regulations for such technologies are coming down the pike. They aim to address security risks, discrimination and bias, privacy concerns, and potential impacts on careers and labor markets. Leading platform companies and hyper scalers are already rolling out security features based on them.

# Why reinvention puts you at risk

Getting security right is one of the key enablers to becoming reinvention ready, as it builds a foundation of trust and resilience that allows for confident innovation.



**Companies are trying to figure out how new technologies change their business, and consequently, how to embed them deep within their digital core to accelerate reinvention. At Accenture we define reinvention readiness as a continuous state of supporting current business, driving efficiency and effectiveness. At the same time, responding to the ongoing needs of the organization and quickly adopting the latest technology innovations. Therefore, security must be equally agile to address any new threats or emerging needs.**

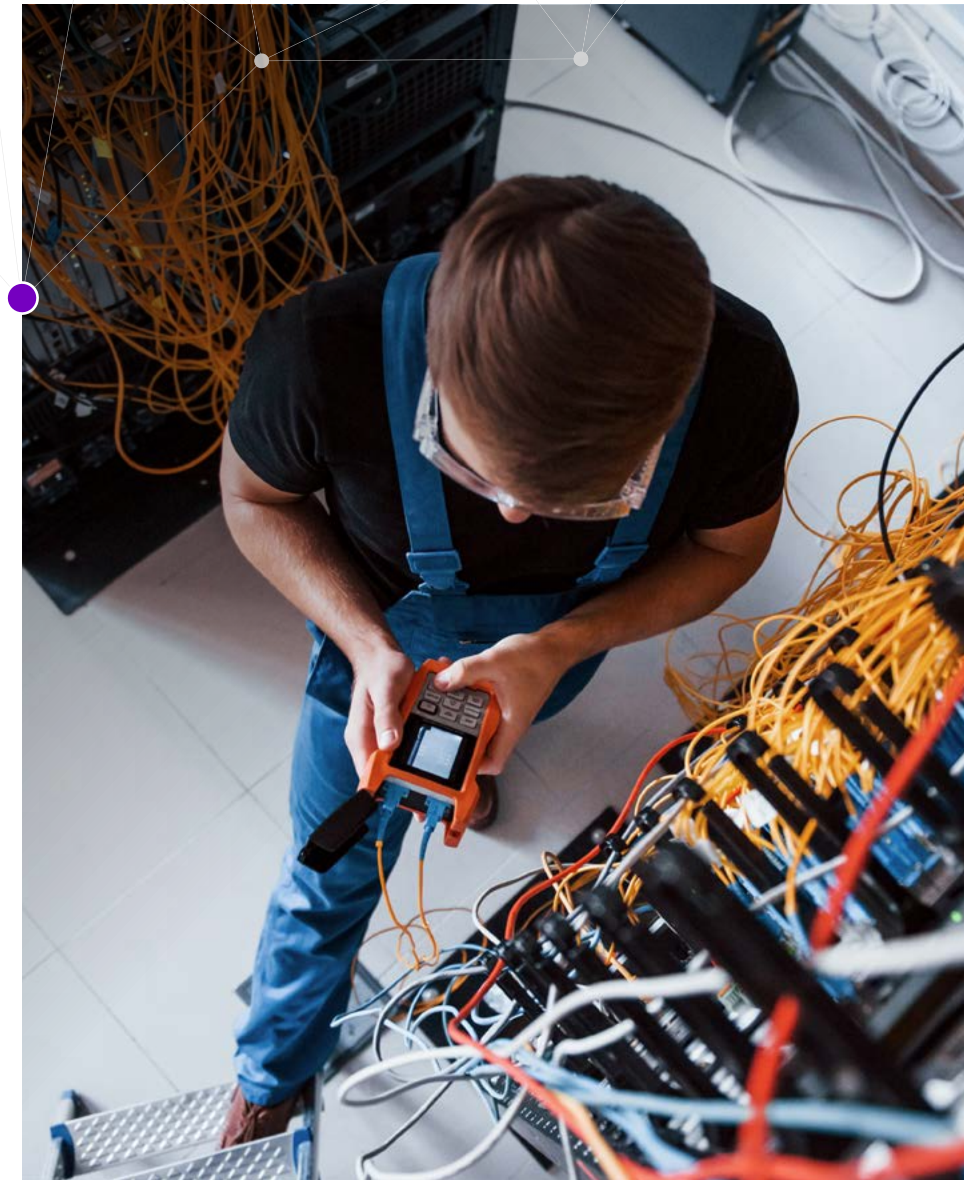
To utilize the full power of generative AI and enterprise technology transformation, you need a reinvention-ready digital core. A digital core is made of seven different and always working parts that help organizations keep reinventing themselves. Digital platforms, data and AI,  and a digital  foundation, which includes cloud first infrastructure, security, composable integration and a continuum control plane (Figure 1).

Organizations with a reinvention-ready digital core follow three tenets: they maintain industry-leading levels of capability, they shift investments toward strategic innovation, and they proactively manage their technical debt.

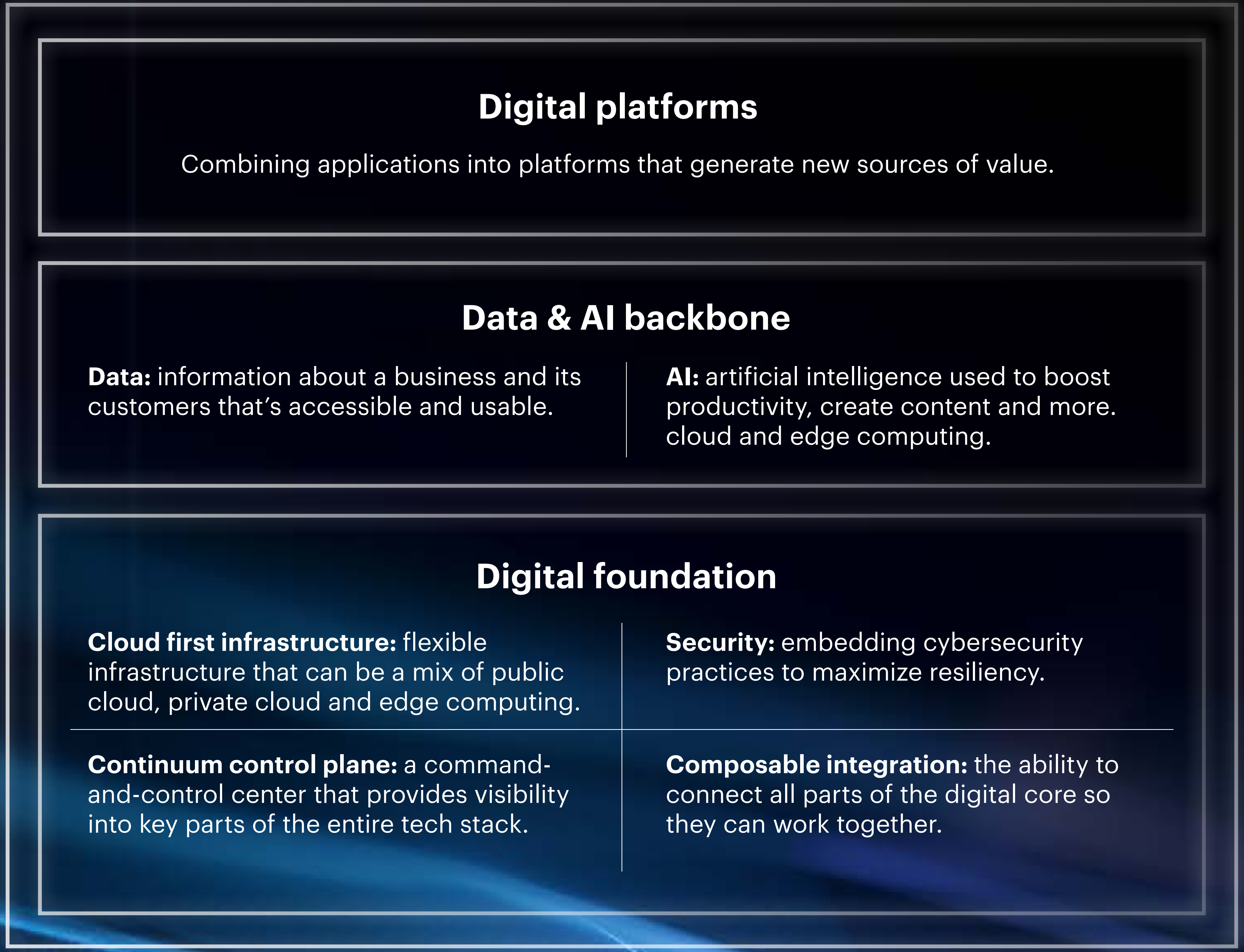
Security is an integral part of the digital core—embedded into the very foundation and integrated throughout each layer. Without security, the digital core is vulnerable, making it harder and more expensive to reinvent and drive competitiveness. Today, continuous business reinvention is usually powered by technological enablement that reaches into the business and across platforms, partners and customers, spanning multiple environments and architectures. Our research shows that 83% of organizations are speeding up their transformation/reinvention efforts[4], with 99.7% of executives saying they are committed to establishing new levels of performance in their industry[5].

54%

of financial services executives say that efforts to transform or reinvent the business and enhance customer experience have introduced more tech risks[6].



## Figure 1: Components of a digital core



### Digital platforms

Combining applications into platforms that generate new sources of value.

### Data & AI backbone

**Data:** information about a business and its customers that's accessible and usable.

**AI:** artificial intelligence used to boost productivity, create content and more. cloud and edge computing.

### Digital foundation

**Cloud first infrastructure:** flexible infrastructure that can be a mix of public cloud, private cloud and edge computing.

**Security:** embedding cybersecurity practices to maximize resiliency.

**Continuum control plane:** a command-and-control center that provides visibility into key parts of the entire tech stack.

**Composable integration:** the ability to connect all parts of the digital core so they can work together.

## What is a digital core?

A digital core is a new way to think about and work with technology.

Accenture defines a digital core as the critical technological capability that can create and empower an organization's unique reinvention ambitions. Building this tailored digital core requires integrating advanced digital platforms, a seamless data and AI backbone and a secure foundation using radical new engineering principles.

This fit-for-purpose digital core enables an organization to accelerate ahead of competition and achieve their ambitions in the most efficient fashion—using the right mix of cloud practices for agility and innovation; data and AI for differentiation; applications and platforms to accelerate growth, next-generation experiences and optimized operations—with security by design at every level.

# Is security keeping up?

As organizations race to embrace emerging technologies to enable new offerings and experiences, they often prioritize speed over security.

## On average, there's a 23-point lag in security capabilities for organization that have yet to achieve an 'industry-leading' digital core.

**In fact, seven in 10 executives say they implement security controls only for critical functions or deploy it after transformation is finalized and vulnerabilities are detected[7]. This has a knock-on effect. When robust security measures and strategies are not included 'by design' from the outset as the business adopts new technologies, the company's digital core becomes vulnerable to threats and technical debt grows as the list of fractional security solutions expands. This makes remediation increasingly costly and time-consuming and limits business agility.**

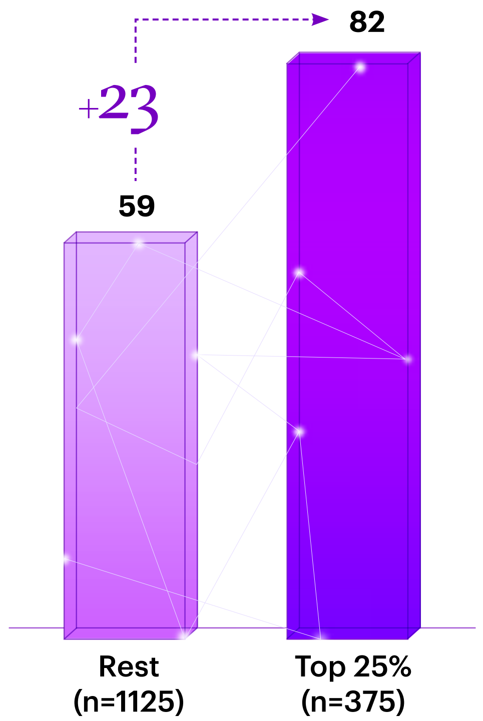
On average, there's a 23-point lag in security capabilities between those organizations with an 'industry-leading' digital core—defined as the top 25% in our Digital Core Index, and those in the bottom quartile (Figure 2). Most organizations fall behind on measures such as use of DevSecOps and Zero Trust identity and networks, security configuration, threat modelling and securing cyber-physical systems.

This gap is further exacerbated by the challenge of technical debt. The total technical debt in the US alone is estimated to exceed $1.5 trillion[8]. Security is part of this problem, with 34% of organizations citing it as a top contributor to technical debt, according to our research. It arises from quick solutions to security problems that eventually need to be redone because they are not effective. Besides, point-security tools that do not integrate with or provide context to other security tools, reduce security posture and visibility while increasing cost.

Moreover, security complexity and talent shortages add another layer of difficulty. Organizations report that they rely on an average of 76 security tools to manage their security posture[9]. This complicates transformation efforts. Combined with talent shortages—there are 4.8 million unfilled cybersecurity jobs worldwide[10]—this complexity significantly hinders organizations' ability to scale effectively.

### Figure 2: Security maturity gap

Digital Core Index—Security Maturity Scores



# Cost of cyberattacks

Cybersecurity remains the top global business risk, affecting customer trust, business growth and corporate value.

**Breaches not only increase financial costs but also have significant reputational consequences—79% of cybersecurity professionals rank reputation as their top concern during an attack[11].**

As organizations prepare to invest more in security services, prioritizing investments that align with growth strategies is a critical challenge. While 96% of CEOs view cybersecurity as essential for growth, 74% remain concerned about minimizing damage from potential cyberattacks[12]. Furthermore, cybersecurity has become a key element of corporate ESG (Environmental, Social and and Governance) evaluations, influencing ratings, transactions and mergers and acquisitions, with publicly traded companies seeing an average 7.5% stock drop after a data breach[13].

The urgency of these concerns is underscored by the rapidly evolving threat landscape.

Security professionals and executives alike recognize the rising dangers:

- Seventy-five percent of security professionals report an increase in cyber-attacks over the past year[14], and 56% of executives believe that generative AI gives attackers a clear advantage[15].
- Since the launch of ChatGPT, phishing attacks have surged by 1,265%[16] and deepfake attempts using generative AI have skyrocketed by 3,000% year-over-year in 2023[17].
- Accenture's Cyber Intelligence (ACI) researchers have also noted a 223% rise in the trade of deepfake-related tools on dark web forums between Q1 2023 and Q1 2024[18]. Moreover, cloud environment intrusions have surged 75% from 2022 to 2023, as threat actors exploit unique cloud features to initiate attacks[19].

The gravity of these concerns is reflected in several recent high-profile incidents:

- A Greater China multinational suffered a $25 million loss as the result of a sophisticated deepfake scam. The scammers digitally recreated the company's chief financial officer along with other employees on a conference call instructing colleagues to transfer money[20].
- A vulnerability in an Asian airline's software led to a massive data breach, exposing 6.5 terabytes of data including the personal details of flight crews. The breach stemmed from a misconfigured Amazon Web Services bucket. Safety detectives found 23 million files, including sensitive flight charts, navigation data and plain-text passwords[21].
- In May 2023, a global automobile company reported a data breach affecting about 260,000 customers due to a misconfigured cloud environment. Data from customers in Japan, Asia and Oceania was exposed. The automobile company swiftly blocked external access and initiated an investigation across all cloud environments[22].

These three incidents highlight mounting security challenges as the threat landscape continues to evolve. But organizations' security policies and behaviors amid the rush to reinvention also contribute significantly to the growing security challenge.

79%

of cybersecurity professionals rank reputation as their top concern during an attack[11].

# Closing the security gap

To close the gap in security maturity within the digital core and achieve reinvention readiness, companies should engage three strategic levers.

# Lever 01

## Streamline security to lower costs and optimize investments

**Rationalizing security eliminates redundancies, driving down costs, streamlining processes and optimizing investments. Efficient, integrated solutions lead to better resource allocation and a stronger security posture.**

## Actions to take:

### Consolidate vendors and tools

Consolidate cybersecurity products to streamline your toolsets and reduce complexity. This will help you to achieve better security outcomes such as faster threat detection and improved incident response times.

Achieving this requires a thorough evaluation of existing security solutions to integrate them into a unified, streamlined system that eliminates redundancies and enhances overall security. By harnessing the capabilities of generative AI, you can unlock new levels of efficiency and effectiveness in your security operations. For example, generative AI can combine the functionalities of various security tools—such as intrusion detection, threat intelligence and incident response—into a single, cohesive system.

### Adopt integrated platforms over standalone tools

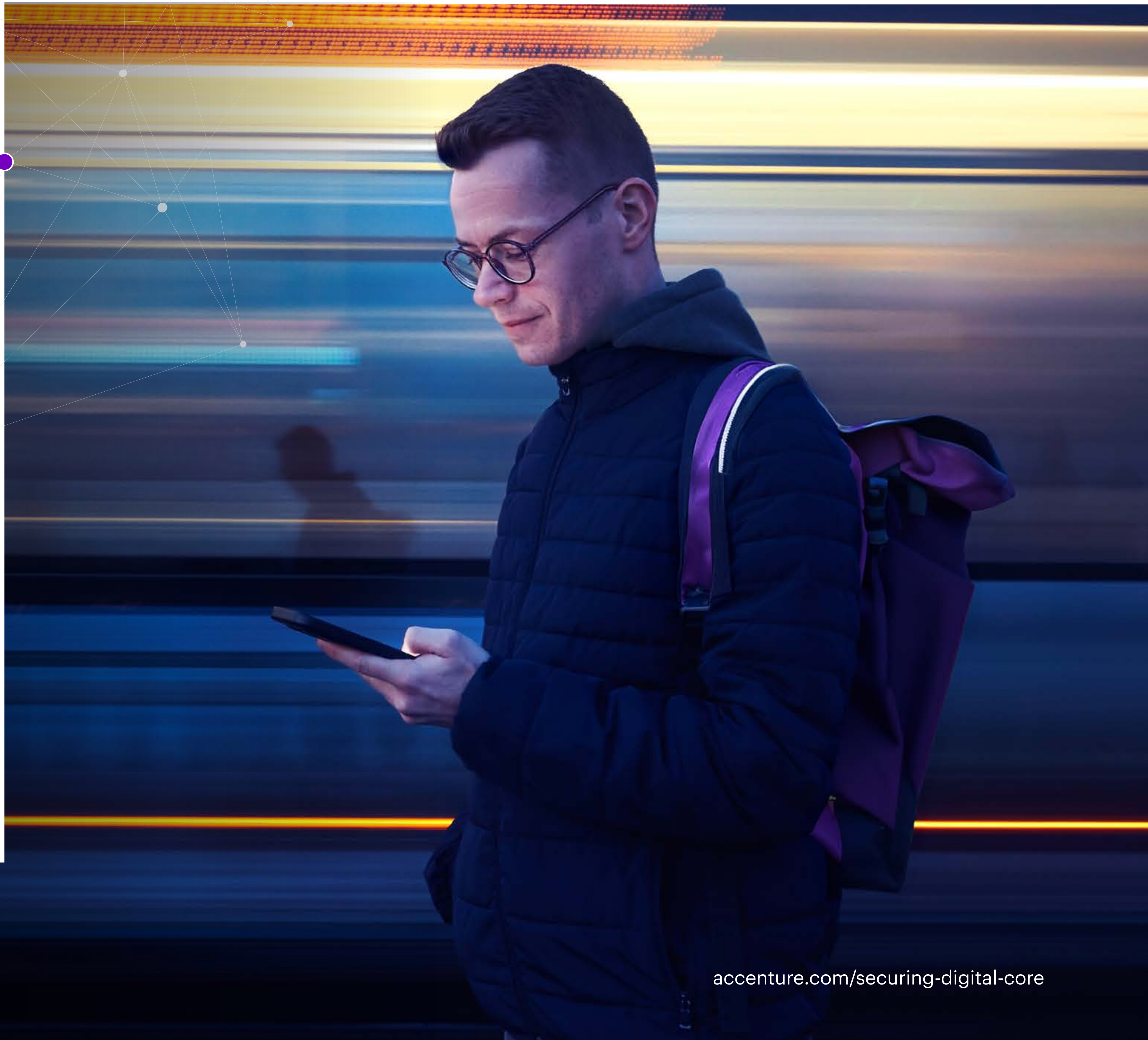
Invest in integrated platforms instead of relying on isolated, standalone tools to simplify management and fortify your organization's defense against emerging threats. Consolidated platforms not only streamline operations but also enable real-time intelligence sharing, which is vital for preventing zero-day threats. By integrating diverse data points, dashboards and user experiences, these platforms offer security teams a holistic view of their organization's risk posture. This unified approach empowers teams to identify and mitigate threats more swiftly and efficiently. Moreover, the centralization of data and tools helps reduce the risk of oversight and improves the ability to correlate events across different systems, leading to a more robust and resilient security strategy.

### Retire legacy tools and invest in best-of-their-kind solutions

Upgrade to modern tools to streamline management and optimize resource allocation. Start by transitioning away from legacy tools that no longer align with modern business processes to accelerate your organization's security transformation. This strategic shift will not only reduce complexity but also eliminate redundancies, thereby significantly enhancing your overall security posture. Direct your resources toward advanced technologies that provide robust protection against contemporary threats.

Case study

## Zero Trust journey for a public transport organization



A public transportation organization needed to enhance its cybersecurity, by introducing Zero Trust principles across its hybrid cloud environment. By assessing the cybersecurity program, identifying gaps and defining a Zero Trust vision, Accenture cocreated a practical plan and developed a strategic project catalog, prioritizing key projects such as a cybersecurity mesh for identity and certificate management. The end result was reduced business disruption risk and increased estate visibility from 10% to 90%+, connected teams across silos with redefined roles and governance and cost reductions, including an optimized investment strategy, added automation and consolidated software licenses.

# Lever 02

## Modernize and integrate security with the business

**Creating a reinvention-ready digital core requires rethinking and revisiting security while also investing in innovation and remediating technical debt. Organizations cannot afford to prioritize rapid growth at the expense of security. Ensuring robust security involves not only updating measures for new innovations but also addressing legacy systems with dedicated security programs or modernization.**

**A holistic approach to security is essential. Many security processes extend beyond the typical security functions and need to be modernized alongside the business to achieve resilience. An agile security program will enable organizations to respond swiftly to attacks, ensure seamless operations and reduce costs.**

## Actions to take:

### Embed security into the entire cloud native application protection (CNAPP) ecosystem

Leverage proprietary templates, predefined scripts, playbooks and technology integrations to ensure robust security in both brownfield and greenfield client environments. Rapidly migrating security operations to the cloud enables organizations to access advanced tools and pre-built assets, modernizing their security infrastructure. For instance, by implementing IaC, security scanning and automated continuous integration and continuous delivery/deployment (CI/CD) pipelines, security configurations can be standardized and integrated early in the development lifecycle. Generative AI can further enhance cloud security by providing Terraform IaC templates with embedded security parameters, simplifying the creation of secure and compliant infrastructure while reducing configuration errors. Additionally, securing your generative AI cloud service provider (CSP) environments is crucial to safely deploy unique AI services like OpenAI on Azure, Google GCP Gemini and AWS Bedrock. These strategic moves ensure security is agile, scalable and capable of meeting the demands of a dynamic threat landscape.

### Secure data and AI

To combat evolving threats in AI environments, you need the support of all key departments, including legal, regulatory, human resources and operations. This can be achieved by forming cross-functional teams to oversee AI adoption, audits and security, while establishing clear policies and controls. AI security should be incorporated into governance, risk and compliance (GRC) frameworks. Organizations should define AI governance principles based on their specific business needs and assign shared responsibilities across legal and compliance functions. Collaboration with governments and industry peers can help shape forward-looking cybersecurity policies.

Having a unified security foundation with a common data model and integrated operations ensures seamless AI integration.

With AI models proliferating, AI firewalls customized to fit organizational policies provide a strong first line of defense, securing interactions, preventing data leakage and blocking malicious or unauthorized uses. But AI firewalls alone aren’t enough. A full defensive strategy must include secure architecture, data protection, access controls and continuous monitoring to prevent vulnerabilities in areas like orchestration layers, RAG databases and APIs. Securing the entire AI stack, including the data layer, the foundational model, AI applications, as well as identity access and controls, is vital.

Additionally, incorporating enriched risk context—such as through red teaming or adversarial testing—enhances security by rigorously testing AI models against real-world attack scenarios, uncovering weaknesses and building more robust defenses. This approach ensures that risk assessments evolve in step with the rapidly changing security landscape. To further enhance AI security, automation plays a key role in streamlining defense mechanisms, allowing organizations to respond swiftly to AI-related threats at scale. Security maturity scores in our Digital Core Index show that leading organizations are 15 index points ahead of the rest in Automation of Security (Figure 3).

### Secure Cyber-Physical Systems

Cyber-Physical Systems (CPS) are crucial for creating value, and any disruptions can lead to halted production or mission failures. As connectivity increases, so does organizations’ vulnerability to ransomware and malware attacks. Identify and secure all CPS and conduct regular vulnerability assessments. Only 39% of organizations we surveyed have the capability to detect Information Technology and Operational Technology incidents in real time[23]. According to our Digital Core Index, industry leaders excel in CPS security, outperforming their peers by 18 index points[24].

### Implement Zero Trust principles

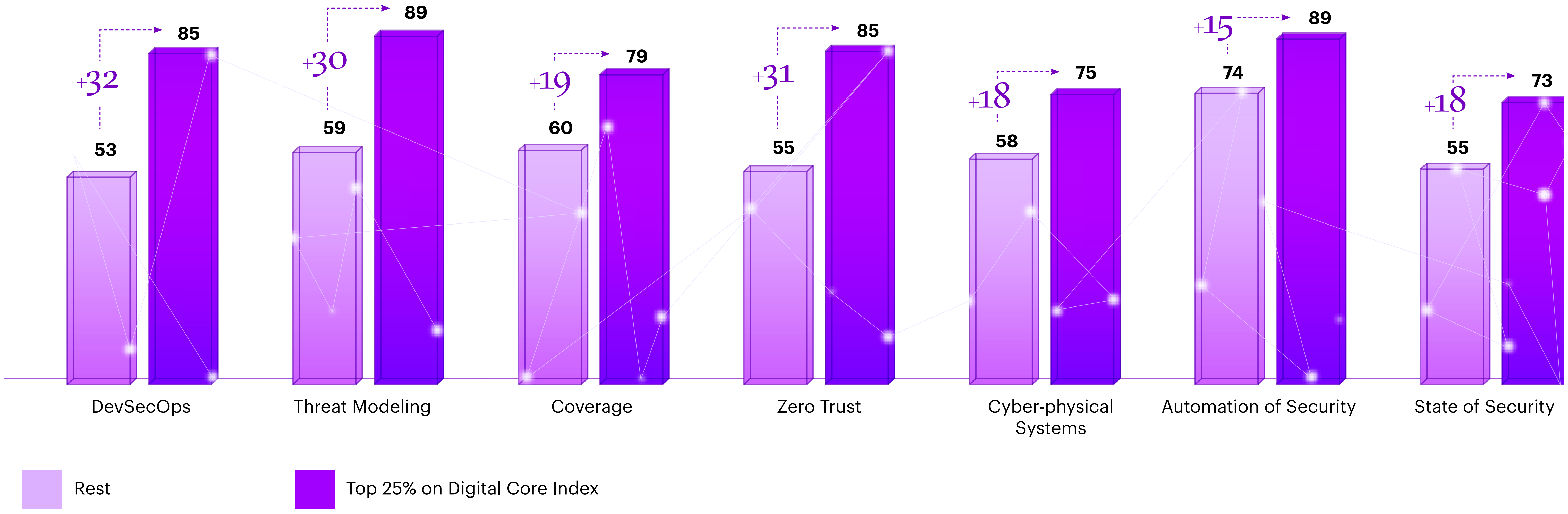
Zero Trust fundamentally redefines traditional security models by enhancing how organizations connect to modernized applications. This approach treats every access attempt as potentially unauthorized, irrespective of the user's identity or network location. According to the Digital Core Index, organizations that lead in Zero Trust practices score 31 points higher than their peers.

For Zero Trust networks, start with Secure Access Service Edge (SASE). SASE improves how clients connect to modernized applications versus traditional VPNs that have access to everything on the network. It integrates networking and security into a unified cloud service as organizations transition security to the cloud. This consolidation reduces complexity, boosts agility and secures multi-cloud Software Defined-Wide Area Network (SD-WAN) architectures.

### Build cyber resilience to strengthen digital trust

Move beyond traditional methods and leverage data and AI for proactive threat preparation, prediction and defense. A critical component of this strategy is implementing advanced Identity and Access Management (IAM) practices, a framework of policies and technologies to ensure the right users have the appropriate access to technology resources. An example is passwordless authentication. Passwordless solutions enhance security by eliminating the risks associated with password theft and misuse, ensuring only verified users can access sensitive systems and data. When combined with proactive threat detection, automated incident response and advanced security measures, these IAM innovations significantly bolster cyber resilience and reinforce customer trust and loyalty. Security maturity scores on the Digital Core Index show that leaders outperform the rest by 30 and 18 index points respectively in terms of Threat Modeling and State of Security.

## Figure 3: Security maturity scores



Case study

## Comprehensive cloud, identity and managed security services transformation for a global products manufacturer

As part of its digital transformation, a global products manufacturer engaged Accenture Security to transition business applications and data to the cloud while improving their IT security posture. Accenture's approach involved accelerating secure-by-design cloud transformation, improving visibility, and reducing cyber risks. Within eight weeks, Accenture remediated the client's AWS cloud environment and protected sensitive data in an enterprise data lake by automating identity controls and governance. Additionally, the client's security operations were significantly improved through enhanced detection, incident response capabilities and alignment with the MITRE ATT&CK Framework. Key outcomes included the remediation of >360,000 vulnerabilities, reducing false positive alerts by >85%, and increasing visibility from minimal to ~90%. The onboarding time for new application teams was reduced from two weeks to 48 hours, allowing for secure global collaboration. Finally, client teams were upskilled to manage critical security controls independently.

## Lever 03

# Scale through automation and Cybersecurity-as-a-Service

**The growing talent and skills shortage is a significant hurdle in modernizing security. To address this challenge, businesses should leverage AI and CSaaS to evolve and scale their security programs.**

71%

of tasks performed by information security analysts can be automated or augmented using generative AI[25].

## Actions to take:

### Scale with automation

As AI-powered threats become more sophisticated, traditional security solutions are becoming inadequate. Adopt AI-driven defense technologies and utilize automated tools for threat testing such as red teaming and penetration testing. These are especially critical as AI regulations advance. Leading platform organizations and hyperscalers are already rolling out AI-based security features. For example, Accenture's Managed Detection and Response (MxDR) service, powered by Google Cloud's AI, integrates seamlessly with a variety of security environments and cloud platforms.

### Augment and automate security with generative AI

Transform manual security tasks by integrating generative AI into your operations. Our analysis reveals that 71% of tasks performed by information security analysts can be either automated (28%) or augmented (43%) using generative AI. This approach not only increases efficiency but also elevates your security posture. Leading organizations in our Digital Core Index scored 89 index points, or 15 points higher than the others on average.

### Adopt Cybersecurity-as-a-Service

CSaaS is essential for digital transformation, providing scalable, expert-managed security solutions that adapt to the ever-changing threat landscape. Outsource security management to concentrate on innovation while reducing the complexity and costs associated with maintaining multiple security tools and personnel. This model not only strengthens overall security but also ensures compliance and cost efficiency, making it a key enabler of success in the digital era.

Case study

## Retail organization leverages CSaaS to improve business outcome

When a retail chain transitioned to a standalone public company, it needed to completely revamp its IT operations. Accenture helped support the retailer's information security team by implementing and managing the company's security operations, including its threat intelligence function and a Security Operations Center (SOC). Today, Accenture provides a comprehensive suite of services—including data protection, identity management, network security, vulnerability management and security awareness. The retailer now benefits from enhanced cyber resilience and secure, better business outcomes.

# Getting started

In today’s digital age, effective security isn't just a safeguard, it's a strategic enabler that can differentiate your market presence. It fosters an environment rich in trust, resilience and adaptability, enabling organizations to securely evolve their digital core to capture new opportunities and sharpen their competitive edge.

## Start securing your digital core by asking these crucial questions to identify vulnerabilities and drive action.

Questions every company should ask themselves:

### Streamline

- How many security tools are used to manage our security posture?
- Do we still rely on legacy security tools to guard against cyber threats?

### Modernize

- Has our organization's cybersecurity been re-platformed to the cloud with assets designed to accelerate the deployment and configuration of security tools?
- Is our cybersecurity program sufficiently mature and agile to effectively address modern-day threats?

### Scale and evolve

- Is our organization leveraging AI to scale security through automation?
- Are we using CSaaS expertise to evolve our security operations?

# References

1. Reinventing with a Digital Core | Accenture
2. Security Leaders Peer Report | Panaseer
3. 2024 Cybersecurity Workforce Study | ISC2 Research
4. Reinvention in the age of generative AI| Accenture
5. Reinventing with a Digital Core Survey 2024 | Accenture
6. Guardian of Trust Survey 2024 | Accenture
7. Cyber Resilient CEO: Cyber-Resilient CEO | Cybersecurity | Accenture
8. The Invisible $1.52 Trillion Problem: Clunky Old Software |The Wall Street Journal
9. Security Leaders Peer Report | Panaseer
10. 2024 Cybersecurity Workforce Study | ISC2 Research
11. State of Cybersecurity 2023 Report | ISACA
12. Cyber Resilient CEO: Cyber-Resilient CEO | Cybersecurity | Accenture
13. The Devastating Business Impacts of a Cyber Breach | Harvard Business Review
14. Voice of SecOPs 2023| DeepInstinct
15. World Economic Forum Cybersecurity Outlook 2024| WEF and Accenture
16. The State of Phishing 2023 | SlashNext
17. Identity Fraud Report 2024 | Onfido
18. Beyond the illusion—unmasking the real threats of deepfakes | Accenture
19. Global Threat Report 2024 | Crowdstrike
20. Deepfake scammer walks off with $25 million in first-of-its-kind AI heist | Ars Technica
21. Pegasus Airline breach sees 6.5TB of data left in unsecured AWS bucket | TechMonitor
22. Cloud misconfiguration causes massive data breach at Toyota Motor | Chief Security Officer
23. Reinventing with a Digital Core Survey 2024 | Accenture
24. Reinventing with a Digital Core Survey 2024 | Accenture
25. Research Modelling and Analysis | Accenture

# About the research

## Quantitative Executives Survey

Data used to inform this point of view was based on security-related data from our Reinventing with a Digital Core research.

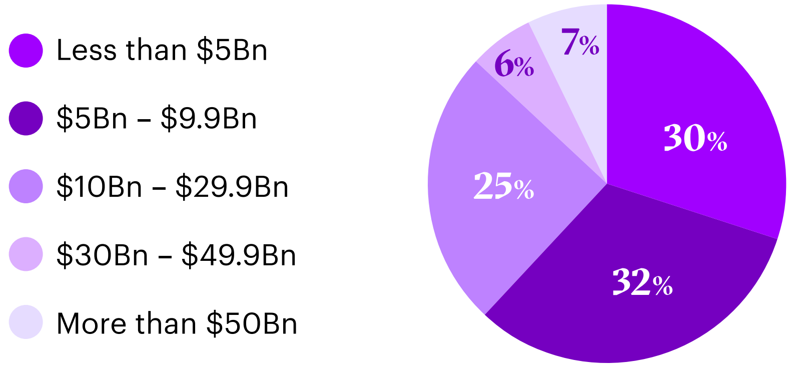
1,500 executives global

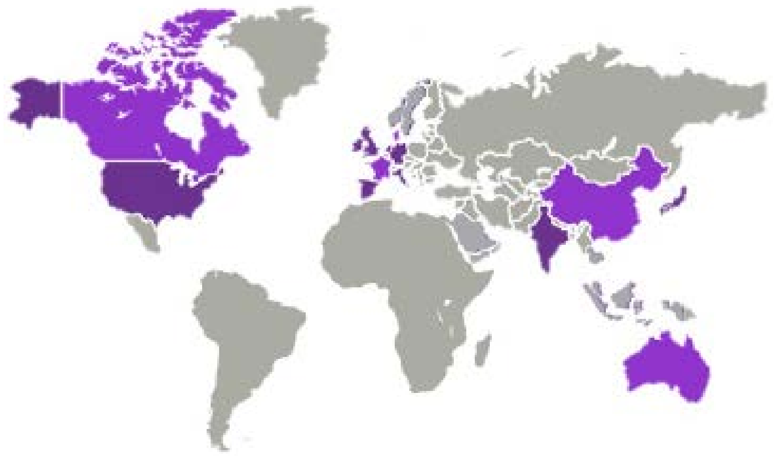
52% completed tech transformation

19 industries

C-Level only

### Company Size





### Industry Coverage

**Financial Services**
Banking (83)
Capital Markets (45)
Insurance (86)

**Media & Technology**
Media & Communications (80)
High Tech (82)
Software & Platforms (86)

**Resources**
Utilities (83)
Energy
(Oil & Gas included) (83)
Chemicals (84)
Natural Resources (81)

**Health & Public Service**
Healthcare (78)
Public Services (40)

**Products**
Retail (115)
Consumer goods & services (113)
Airline, Travel, Transport (80)
Aerospace & Defense (41)
Industrial Equipment (80)
Life Sciences & Pharmaceuticals (79)
Automotive (81)

### 10 Countries

Australia (50)
Canada (70)
China (80)
Germany (130)
France (90)
India (80)
Italy (50)
Japan (100)
United Kingdom (130)
United States (720)

## The security component of the Digital Core Index

We built a composite indicator (an index) to measure the strength of a company’s digital core capability based on 39 assessment questions (out of which 7 focused on Security). We applied a two-step aggregation process corresponding to the digital core component definitions and normalized the overall score on a 0-100 scale, where 100 means maximal strength across all components while 0 means absence of it. As a next step, we created three groups of organizations based on overall Digital Core Index score distribution. The top group corresponds to the top quartile of the Digital Core Index which we refer to as leaders. We then we compared the security maturity score across components between the leaders and the rest of the group. The index represents the aggregate strength of their digital core as the average of each component's capability. Capability points represent the relative sophistication of a given technology. Gaps represent technology modernization activities needed to achieve the next level of capability. The greater the gap, the more time and investment required to achieve a target level of capability and unlock the associated value.

## Authors

**Paolo Dal Cin**

Global Lead –
Accenture Security

**Rex Thexton**

Chief Technology Officer –
Accenture Security

**Andrew Winkelmann**

CTO of Cyber Protection
Team – Accenture Security

**Yusof Seedat**

Global Research Lead –
Accenture Security

## Acknowledgements

Research Lead:
**Manav Saxena**

Research team:
**Gargi Chakrabarty, Arlene Lehman, Shachi Jain**

Marketing team:
**Mark Klinge, Kamilla Giedrojc, Eileen Moynihan, Ewa Szkudlarek**

**The authors would like to extend a special thanks to John Delmare, Muthu Raja Sankar, Ganesh Devarajan and Sadhana Joliet for the insights and contributions to this research.**

## About Accenture

Accenture is a leading global professional services company that helps the world's leading businesses, governments and other organizations build their digital core, optimize their operations, accelerate revenue growth and enhance citizen services—creating tangible value at speed and scale. We are a talent and innovation led company with 738,000 people serving clients in more than 120 countries. Technology is at the core of change today, and we are one of the world's leaders in helping drive that change, with strong ecosystem relationships. We combine our strength in technology with unmatched industry experience, functional expertise and global delivery capability. We are uniquely able to deliver tangible outcomes because of our broad range of services, solutions and assets across Strategy & Consulting, Technology, Operations, Industry X and Accenture Song. These capabilities, together with our culture of shared success and commitment to creating 360° value, enable us to help our clients succeed and build trusted, lasting relationships. We measure our success by the 360° value we create for our clients, each other, our shareholders, partners and communities.

Visit us at www.accenture.com

## About Accenture Research

Accenture Research creates thought leadership about the most pressing business issues organizations face. Combining innovative research techniques, such as data-science-led analysis, with a deep understanding of industry and technology, our team of 300 researchers in 20 countries publish hundreds of reports, articles and points of view every year. Our thought-provoking research developed with world leading organizations helps our clients embrace change, create value and deliver on the power of technology and human ingenuity. For more information, visit Accenture Research on www.accenture.com/research.

Disclaimer: The material in this document reflects information available at the point in time at which this document was prepared as indicated by the date in the document properties, however the global situation is rapidly evolving and the position may change. This content is provided for general information purposes only, does not take into account the reader's specific circumstances, and is not intended to be used in place of consultation with our professional advisors. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals. 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.

Some images included in this document have been generated using artificial intelligence technology.