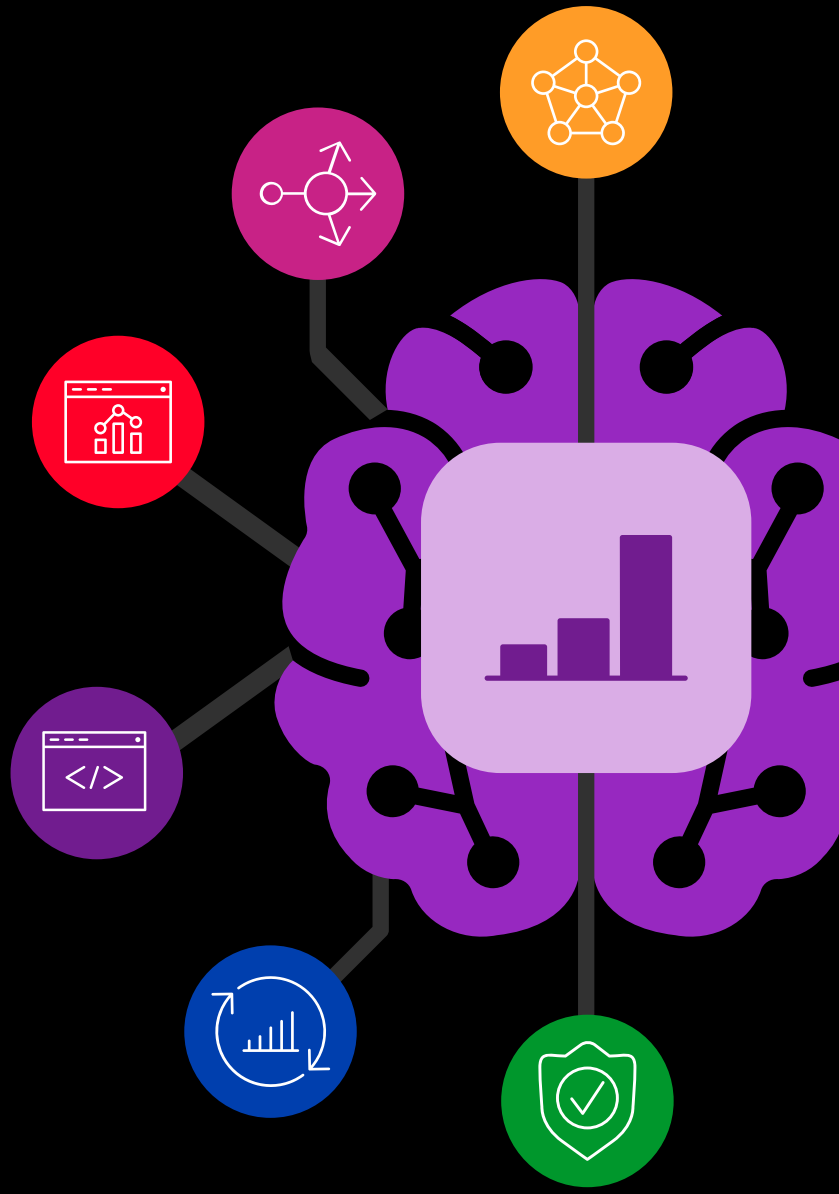
2024

Digital Enterprise Maturity Index Report

The Impact of Generative AI



Contents

Introduction

The past year has demonstrated, quite publicly, the folly of failing to modernize one's enterprise architecture. From outages to breaches, headlines often proclaimed the consequences of failing to modernize for everyone to see.

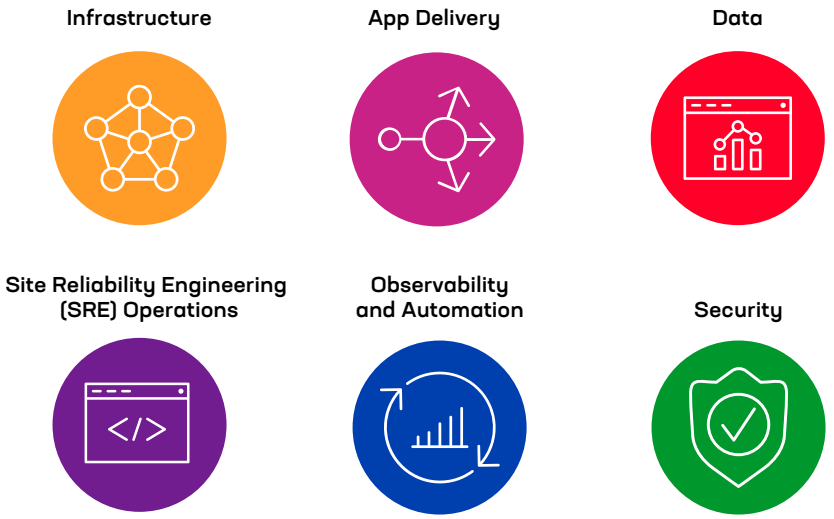
If the spectacle of outages and breaches did not spur digital *dawdlers* to action, perhaps the arrival of generative AI will. In the era of AI, the entire digital transformation journey to modernize has one goal: to establish an adaptable enterprise architecture capable of harnessing the power of AI—both generative and predictive. Generative AI has provided the clarity organizations need to recognize how valuable AI will be to becoming a digital business. Many organizations are now clearly signaling their intention to finish their transformational journey.

To achieve that, organizations need an architecture that can absorb and incorporate new technologies at the rate with which they emerge. Generative AI is only the tip of the iceberg. There will be change, and it will be rapid and unpredictable. A modern, flexible enterprise architecture is the way to ensure the ability to do just that.

There are six key capabilities that underpin such an enterprise architecture. Realizing these capabilities requires organizations to modernize entrenched practices and approaches to support the needs of a digital enterprise.

"Organizations need an architecture that can absorb and incorporate new technologies at the rate with which they emerge."

We've previously described this transformation in our book, Enterprise Architecture for Digital Business and dug deeper into the six technical capabilities needed to accelerate the journey:



To help enterprises, we use a model based on these technical capabilities to measure their readiness to thrive as a digital business. These measures span the use of core tools, technologies, and adoption of practices critical to the six key capabilities identified in our book.

Today, we're thrilled to deliver the results of that analysis in the second annual Digital Enterprise Maturity Index.

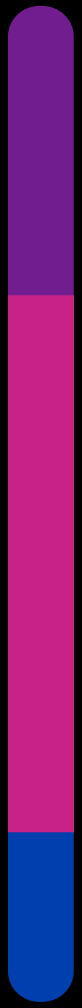
The State of Digital Transformation in 2024

The past year has brought plenty of reasons for organizations to accelerate digital transformation efforts. Between the arrival of generative AI and the increasing number of high-profile outages and breaches due to aging enterprise architectures, it was no surprise to see that most organizations are now *dabbling* in enterprise architecture modernization. Some organizations made significant progress, with nearly one in four joining the ranks of *doers* this year. A dwindling percentage of organizations continue to *dawdle*, with little progress on their journey.

The impact of these accelerated transformation efforts can be seen in the average number of apps and APIs organizations manage on their journey. Digital *dabblers* and *doers* have a significantly higher number of APIs under management than *dawdlers*. Organizations *dabbling* in digital transformation tend to be in a phase of digital expansion, which focuses on delivering digital services and modernizing IT. Organizations in this phase build seamless digital experiences for their users. While these experiences present as a single application, they are delivered by a workflow stitched together from multiple applications that are connected using APIs.

This is the result of modernization. When we asked how organizations planned to modernize applications back in 2021, 61% told us they were "adding a layer of APIs to enable modern user interfaces" as a method of modernization. In 2022 that number was 45%. And then in 2023 46% of respondents told us they were moving to SaaS to **replace** traditional apps, and 59% were going to **replace** with modern equivalents, which inherently increases the number of APIs. As a result, organizations that are invested in digital transformation will arrive at their destination with many more APIs than apps due to modernization.

Digital Enterprise Maturity Index



29%

Doers are considered those with scores in the top 20%.

54%

Dabblers are considered those with scores in the middle 60%.

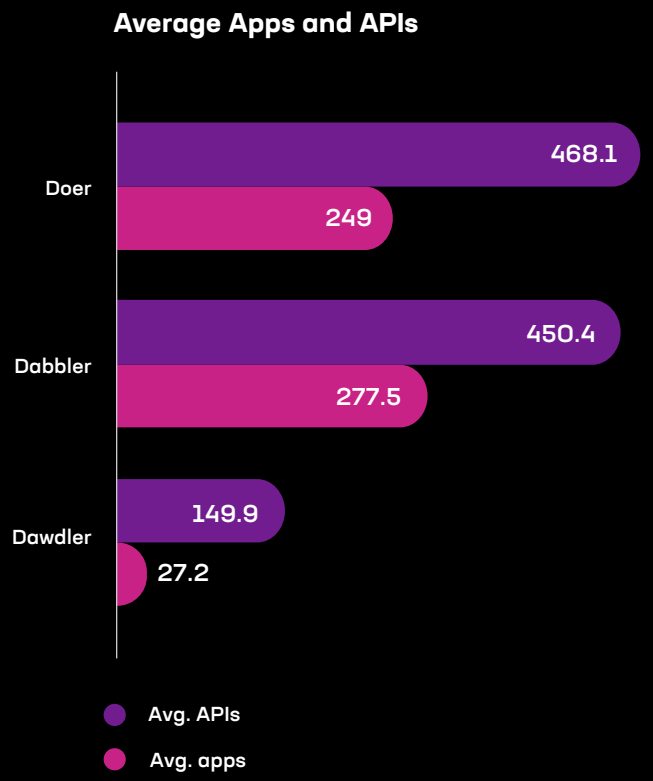
17%

Dawdlers are considered those with scores in the bottom 20%.

Evidence of digital maturity is seen not just in the ratio of apps to APIs, but in how distributed those apps are across core, cloud, and edge. A modernized infrastructure can support a more distributed portfolio of applications and the delivery and security services needed to protect them.

We see this in the number of organizations who are operating hybrid apps; that is, applications whose components are in at least two distinct environments. Most commonly, elements of an application will be deployed both on-premises and in the public cloud, but organizations also might distribute components of applications across two different public cloud providers or use edge computing to deliver some portion of their services. Because hybrid applications are by nature distributed, a higher degree of digital maturity is required to operate them. While only 10% of *dawdlers* operate hybrid apps, 82% of *doers*, well, do. Even a slight majority of *dabblers*—51%—operate hybrid apps today.

The relationship between the ability to operate hybrid apps and digital business can be seen in the ability to leverage AI. The data is clear that AI models, LLMs, and apps will be hybrid, with components deployed in the best environment based on cost, performance, and security.



On average, as organizations mature, the number of APIs they manage far outpaces their number of apps.

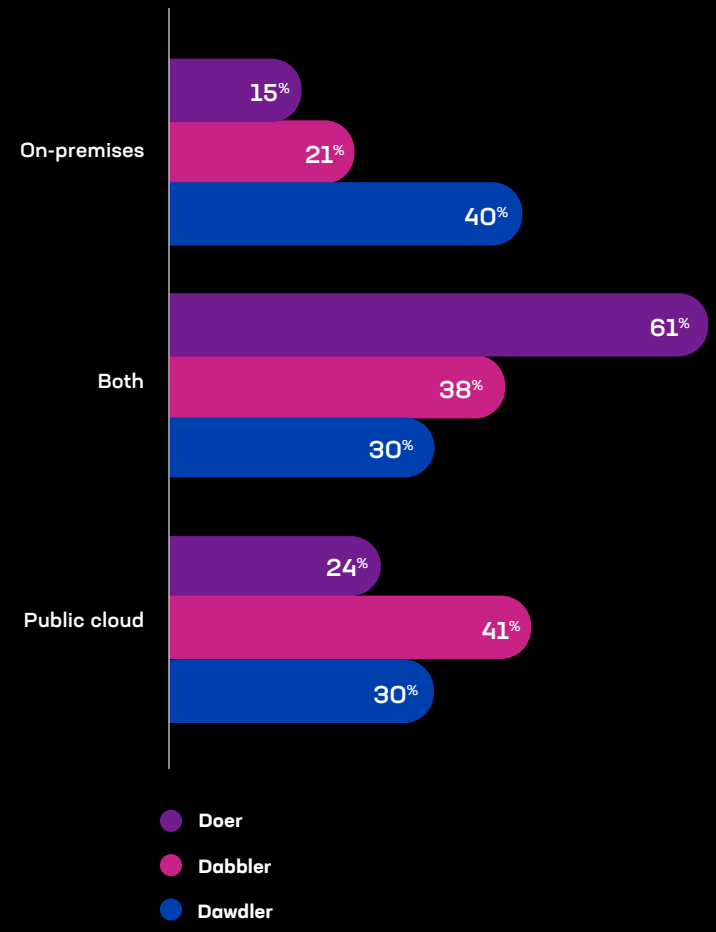
AI application deployment plans exhibit a similar distribution, with *dabblers* and *doers* demonstrating a preference for on-premises over public cloud. As organizations mature digitally, they establish larger data lakes with increasingly valuable data, so the slight shift toward on-premises is understandable given the security and privacy needs of more sensitive data, particularly when AI—a still nascent and immature technology—is involved.

Supporting all this digital activity and data requires maturation—through modernization—of the enterprise architecture. To understand how organizations are faring today, we return to the six key—and core—technical capabilities organizations need to develop to successfully become a digital business.

"AI is fueling an organization's ability to realize the promise of digital transformation. New AI powered apps will create insights faster. This speed, coupled with the depth of the analysis, will increase productivity and drive revenue growth. Everyone can see the potential for employee productivity gains today, but in the future, as accuracy increases and trust matures, AI's potential to streamline, automate, expedite, and create will reach into every business function."

Cindy Borovick, F5 Market and Competitive Strategy Director

Where Organizations Plan to Deploy AI Engines



Key Capability: Infrastructure

"With the emergence of artificial intelligence as a key strategic initiative within many digital businesses, the importance of maintaining a close relationship to (and deep understanding of) the infrastructure components underlying these AI-backed applications is more important than ever before. The measured application of hardware acceleration and the ability to rapidly distribute models to where they perform their tasks on data can mean the difference between success and failure of AI workloads."

Joel Moses, F5 CTO Systems and Distinguished Engineer

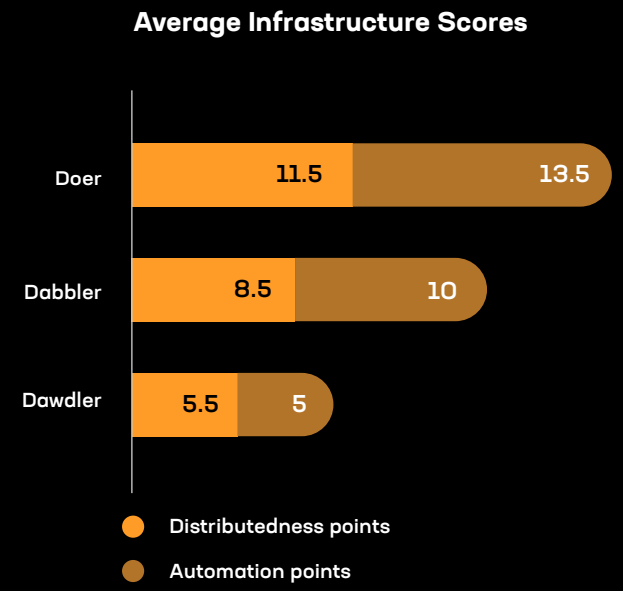
Enterprise Architecture for Digital Business

The Top Three Digital Doers

With respect to infrastructure capabilities, the top three industries for digital *doers* are:

1. Telecommunications
2. Government/public sector
3. Education

Given that the focus of the telecommunications industry is to provide connectivity across the globe, it is no surprise to see them leading digital maturity of infrastructure. Education, though highly distributed, is perhaps surprising today until one recalls that the forerunner of the public Internet was largely made possible because of universities.



A top score for infrastructure is 30 points, with each measure contributing 15 possible points.

Measures

Distributedness: A digital business must be able to use and incorporate infrastructure across core, cloud, and edge locations.

Automation: A digital business must be able to react—both expanding and contracting—by scaling and securing apps across infrastructure with minimal human intervention.

Infrastructure Distributedness

When it comes to operating digital services in a hybrid IT model, it is imperative that the underlying infrastructure—network and application—can also operate in that model. That means stretching infrastructure from on-premises to public cloud and out to the edge. We call the ability to operate infrastructure in this way *distributedness.*

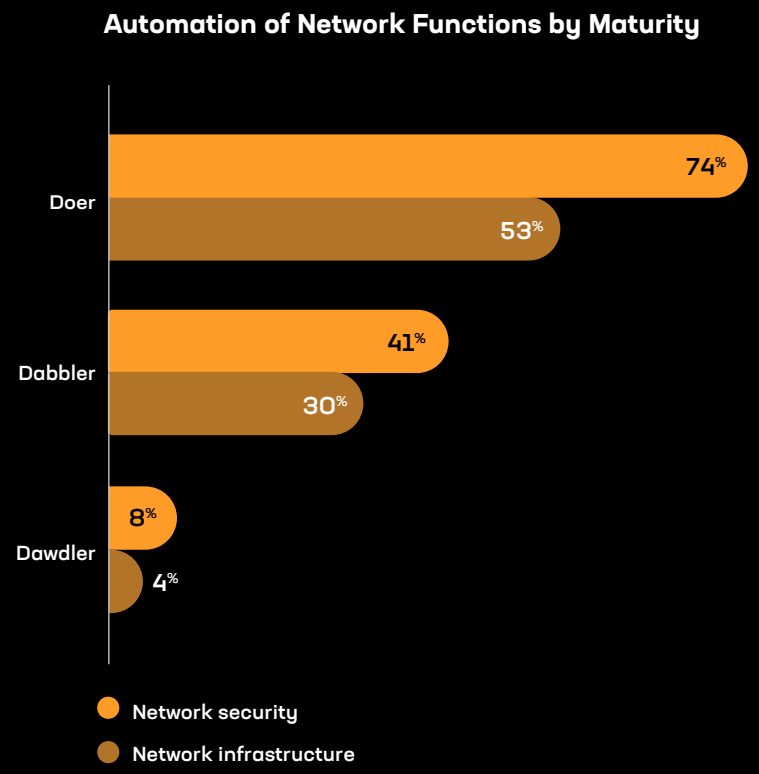
This is not an easy task. Operating distributed infrastructure means rising to the challenge of complexity introduced by different frameworks, APIs, and consoles. This complexity has plagued organizations for nearly a decade, with little relief in sight. And yet we see *doers* executing, despite the complexity, to achieve impressive maturity in distributedness of their infrastructure.

That's a good sign, given the findings with respect to AI and where organizations tell us they plan to deploy its engines (LLMs, models) and applications. AI will cement hybrid IT as the standard operating model. That puts a lot of pressure on organizations to modernize infrastructure and ensure seamless connectivity from core to cloud to the edge.

Infrastructure Automation

As infrastructure grows to support a healthy portfolio of digital services, operations must also grow and leverage tools and technologies to remain efficient while scaling up to maintain performance and security expectations. Maturity is indicated by the ability to leverage automation to operate network and network security infrastructure. It is no surprise to find that the *doers* are much further ahead in automating both network security and infrastructure.

What's more interesting than maturity of automation—which fell out as we'd expect it to—is why organizations aren't automating more. What's holding back *dawdlers* and *dabblers* from joining the *doers*?



This is where it gets interesting. For *dawdlers*, both budget and lack of prioritization keep them from automation network infrastructure. But for *dabblers*, it's budget and complexity of tools; namely, tools that don't inter-operate with each other. *Doers* aren't without struggles; they cite variety of vendors as the primary reason they aren't automating even more.

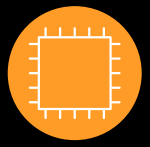
For network security automation, the story is very different. Budget isn't the biggest problem for *dawdlers* and *dabblers*—the biggest challenge for them is skillsets. *Doers*, however, point to a lack of budget and once again cite problems with managing too many vendors as key limitations.

None of this is surprising. Security is one of the best-funded functions in organizations today, but budget can't address vendor quantity or fix tools that don't play well together. It can, however, address skills deficits by funding training and certifications. This points to a lack of interest in investing in existing talent through upskilling efforts as a strategic blocker to maturing in infrastructure automation. *Doers* have clearly addressed the skillset deficit—less than 10% point to gaps in skills as a blocker to automation—and are now faced with challenges controlled by external forces.

These challenges are mirrored in the challenges faced by those operating apps across multiple clouds, with complexity of tools and APIs topping the list. This makes the trend toward platform approaches understandable, especially when that platform provides a single API and interface to a broad set of security and delivery services and explains the rise of multicloud networking as a rapidly growing market.

The Impact of Generative AI on Infrastructure

One might think the impact of generative AI on infrastructure is minimal, but that would be shortsighted. The earliest impacts of generative AI have been on infrastructure and on system infrastructure.



(GPU) Graphic Processing Unit
Used to accelerate the processing of complex math related to cryptography and graphics.

(DPU) Data Processing Unit
Used to accelerate processing of data at the circuit board level.

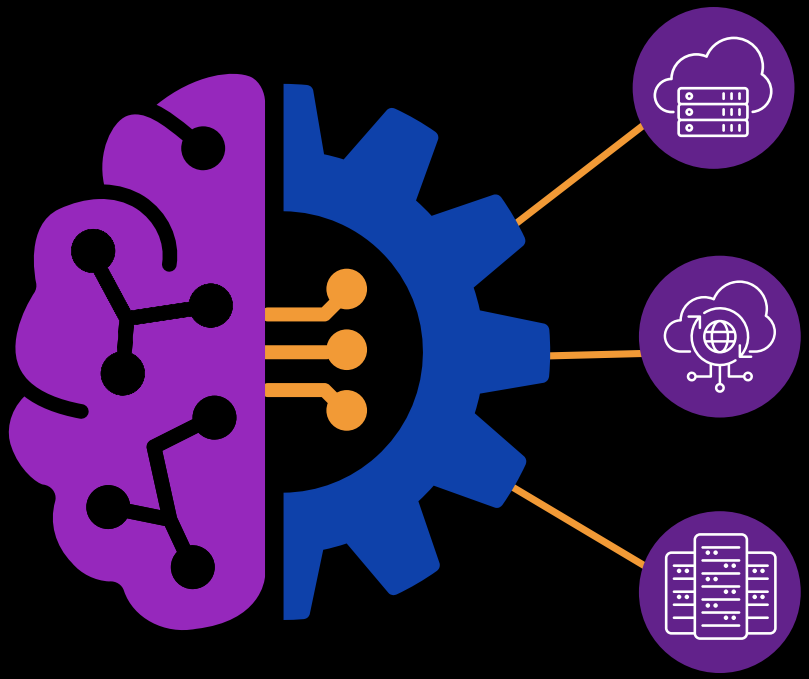
(NPU) Network Processing Unit
Used to accelerate processing of network traffic.

(LPU) Language Processing Unit
Used to accelerate semantic processing of natural language for analysis and generation by large language models (LLM).

We saw the emergence of an infrastructure renaissance nearly two years ago when Moore's Law was declared dead and GPUs took over where CPUs left off. The explosive growth of specialized processing units—from GPUs to DPUs to NPUs and, this year, to LPUs—is fueled by the underlying need for blazing fast computation of the complex mathematical equations required for cryptography, modern gaming, and all forms of AI.

Generative AI has further driven demand for greater bandwidth, owing to its reliance on natural language (verbose plain text) as both input and output. This, in turn, is fueling advancements in networking at both the system and enterprise level.

If that weren't enough, the predominate architecture for deploying generative AI and the applications that leverage it will be hybrid; that is, deployed both on-premises and across public clouds. This is what makes the distributedness of the enterprise infrastructure such a critical foundation for digital business. Organizations able to operate with a high degree of distributedness will be better placed to harness the power of AI through advanced system resources (hardware) wherever it is located.



Key Capability: Observability and Automation

The Top Three Digital Doers

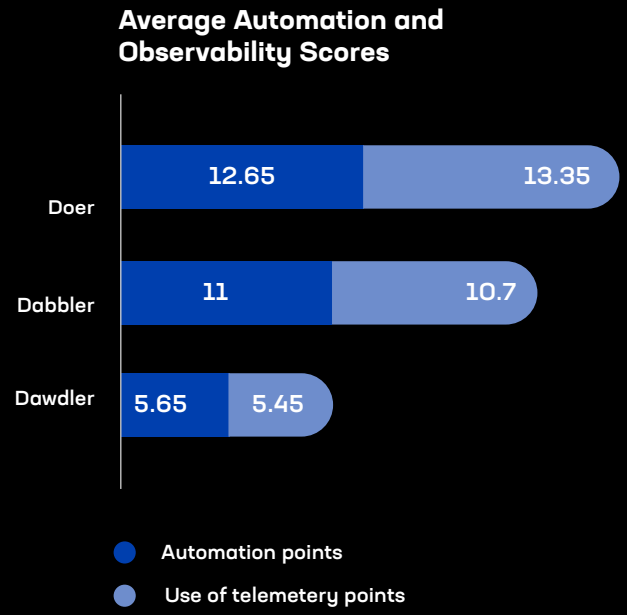
With respect to observability and automation capabilities, the top three industries for digital *doers* are:

1. Government/public sector
2. Healthcare
3. Education, technology

To see healthcare leading maturity in observability and automation is no surprise. Of all the industries that exist, healthcare—like manufacturing—has long relied on observability and automation at the device level. No doubt this industry is able to apply lessons learned to software to achieve an impressive level of maturity in observing and automating a broad set of operations despite the challenge of a highly distributed estate.

Automation Capability

The speed and scale of operations an organization can achieve are directly attributable to the maturity of its automation capability. The speed with which changes can be made (whether deploying or decommissioning applications and services) and the number of applications and services that can be supported are determined by how often human intervention is required. Requiring even one approval for a system to initiate a change introduces operational latency that drags down time to change—and resolution—and creates challenges at scale.



A top score for automation and observability is 30 points, with each measure contributing 15 possible points.

Measures

Automation capability: A digital business must employ automation that is driven by data with minimal human intervention.

Use of telemetry: A digital business must use the telemetry it collects to its fullest extent, moving beyond simple binary status to insights and, ultimately, automation.

Thus, the maturity of an organization's automation capability relies on how much—or little—manual intervention is required.

Clearly, digital *doers* are quite mature in their automation capability, more likely to leverage scripts and more often relying on systems to execute changes automatically. This general capability is applied to a variety of operational systems including network security and infrastructure, app and API security, as well as app infrastructure and delivery services.

Not everything is automated today, but that's not for a lack of desire on the part of digitally savvy organizations. What has been holding them back are capabilities around generation and analysis; capabilities that are just now being made possible by AI.

Indeed, regardless of level of digital maturity, the use of generative AI to automatically adjust and deploy security and delivery policies was ranked the most valuable. Only improving the efficacy of security services came close to matching the value placed on leveraging generative AI for automation.

Use of Telemetry

To achieve autonomous operations—indeed, to achieve a state of automated operations—requires a robust data set about the performance, health, and security of infrastructure, services, and applications. That information comes from telemetry. Telemetry is simply a specific type of data; we use the word "telemetry" to distinguish it from more traditional types of transactional data such as customer profiles, accounts, products, and sales.

How an organization leverages telemetry speaks to their level of operational maturity and readiness to operate as a digital business. Organizations just starting out on their digital transformation journey are not likely to have a robust data practice in place, nor the tools and technologies needed to analyze and act on that data. But *dabblers* and *doers* have all three and are using it to drive operational efficiencies unachievable without the use of technology.

Levels of Automation

None
Fully manual operations. Human operators use CLI and GUI to create configurations and push policies to adjust delivery and security services.

- 48% of Dawdlers
- 8% of Dabblers
- 5% of Doers

Scripted
Human operators use scripts to make minor configuration changes and push policies that adjust delivery and security services.

- 36% of Dawdlers
- 55% of Dabblers
- 37% of Doers

Automated
Systems execute scripts based on conditions to make minor configuration changes and push policies that adjust delivery and security services.

- 16% of Dawdlers
- 37% of Dabblers
- 59% of Doers

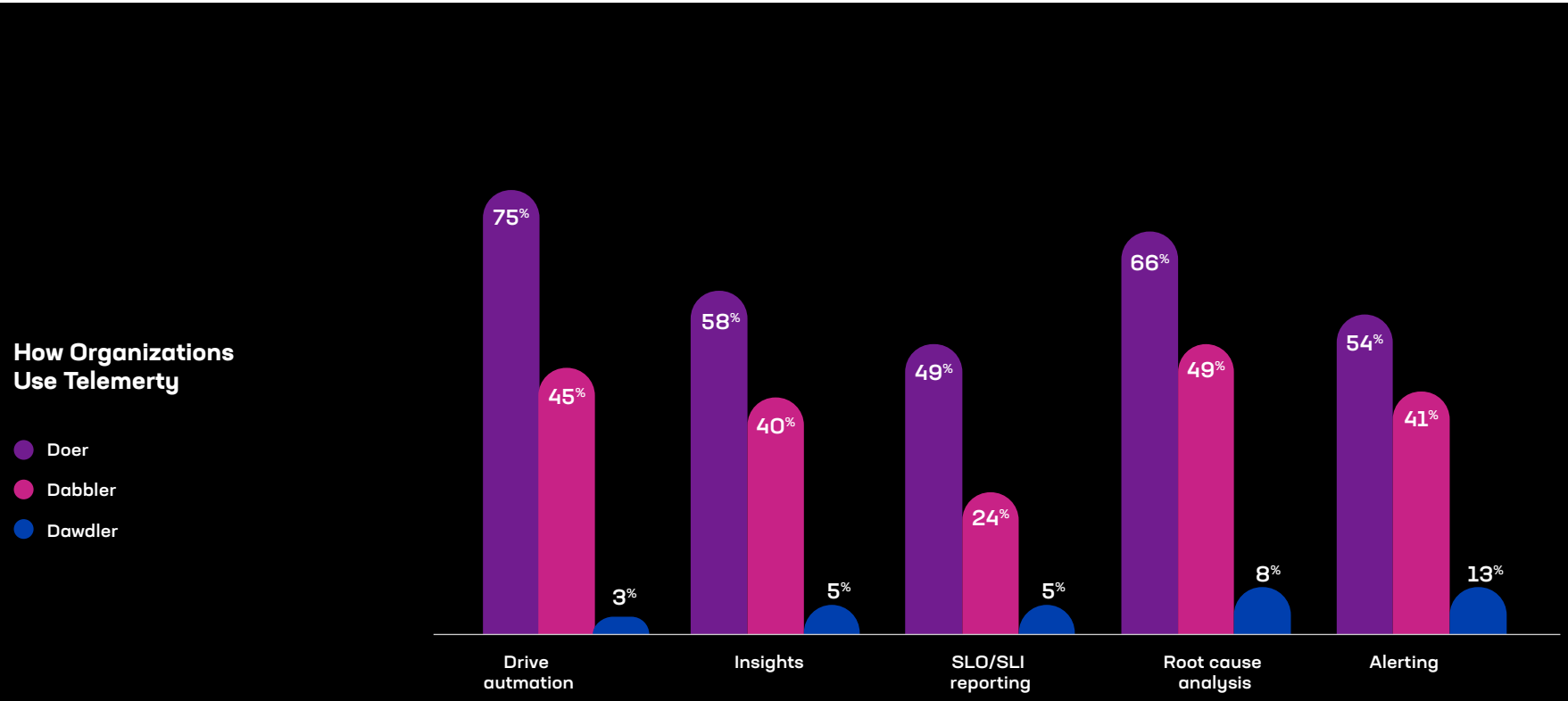
Autonomous
Systems generate and deploy configurations and policies that meet defined SLOs automatically based on conditions.

We organize maturity of telemetry use starting at its most basic utility: alerting. From there, organizations tend to move through different stages of use as their maturity grows. From root cause analysis to SLO/SLI reporting, then onto the generation of insights and, finally, using telemetry to drive automation. The most mature organizations use telemetry in every way far more than *dawdlers*, who are least likely to employ telemetry for any use beyond alerting.

The Impact of Generative AI on Observability and Automation

Prior to the introduction of generative AI, the use of AI to analyze telemetry was limited to predictive models. Generally, commercial security services put predictive AI to good use extracting insights from telemetry, while use in other domains remained mostly nascent.

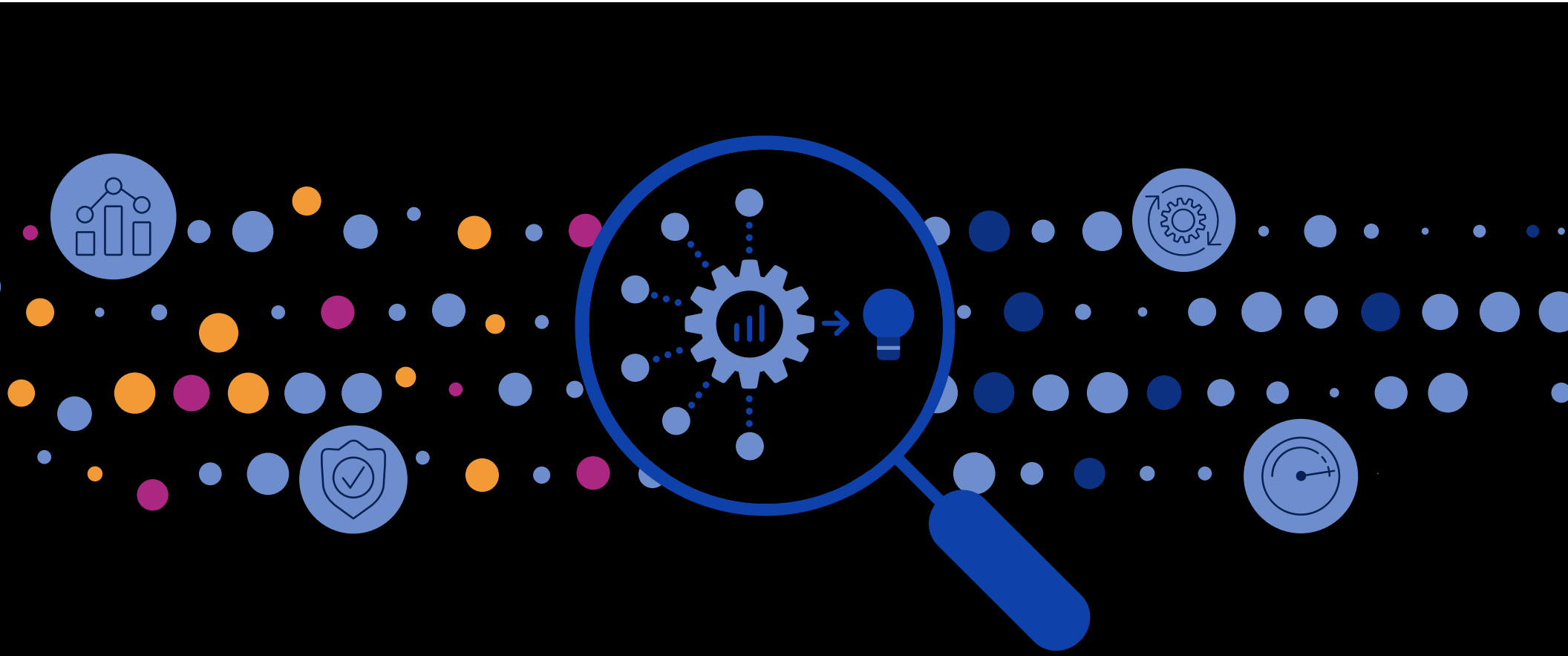
The ability to use generative AI to assist in complex data analysis may ignite a spark in this domain. Prior to generative AI, depth of analysis and value of insights derived from telemetry were limited to either (a) predictive AI or (b) highly skilled data analysis experts. Generative AI opens the door to more complex analysis by generating code and queries for a variety of systems that could then be used to drive automation or produce actionable insights.



This potential has reignited an interest in autonomous operations; that is, AIOps. This level of automation moves beyond minor changes and adjustments and assigns more operational responsibilities to systems based on the ability of AI—both generative and predictive—to extract insights from telemetry and act on them to generate and deploy the appropriate configurations and policies to meet established service level objectives (SLOs).

No organization is operating at this level…yet. We anticipate that as organizations grow and learn to harness the power of AI, they will advance their maturity even further and, one assumes, reap the benefits organizations realize today from mature automation practices. Across every benefit of automation—consistency, cost savings, and efficiency—organizations reap greater return on their investment as their automation practices mature.

Organizations whose automation maturity is “automated” saw the biggest benefits: 53% enjoy greater consistency, 71% saw cost savings, and 80% report greater operational efficiencies.



Key Capability: Data

"Data governance practices are increasingly important due to the demand to employ Generative AI to deliver business value. Operational data silos continue to proliferate, so data governance practices provide the single source of truth for how to manage operational data for the organization, even if multiple data platforms and a mesh of pipelines between them exist."

James Hendergart, F5 Director, Development Operations

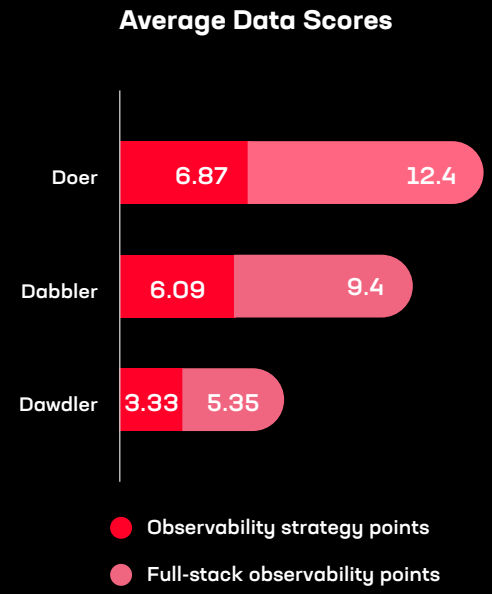
Enterprise Architecture for Digital Business

The Top Three Digital Doers

With respect to the maturity of data practices, the top three industries for digital *doers* were:

1. Technology
2. Cloud service providers
3. Manufacturing

No surprises in the top three digital *doer* list with respect to data capabilities. Technology and cloud services are relatively young industries that are not held back by legacy data stores and practices. Manufacturing, though a long-lived industry, has always been an early adopter of automation and modernization. Manufacturing organizations lag behind their technology-driven counterparts, but nonetheless have achieved significant digital maturity.



A top score for data is 24 points, with observability strategy contributing 9 points and full-stack observability status contributing 15 possible points.

Measures

Full-stack observability: A digital business needs to monitor its health as indicated by the digital signals generated from the entire IT stack.

Observability strategy: A digital business must be able to interpret those signals within the context of desired business outcomes.

Full-Stack Observability

Observability is a term used almost exclusively within IT to describe the capability to observe a system in its entirety. This means that the data collected is operational; that is, it is the telemetry generated by network, system, and application infrastructure, application services, and the applications themselves.

This data is different in frequency and volume than traditional enterprise data sources. But there are similarities, in that data from different sources is often interrelated. Like customer data, telemetry spans the entire application stack—from infrastructure to app services to APIs. But those components are not mutually exclusive, and the relationship between them is what ultimately uncovers insights and exposes the source of incidents.

Missing one piece of telemetry can be the difference between downtime and degradation, between an outage and operational continuity. This is why achieving full-stack observability is critical for organizations to become a digital business. AI and analytics cannot fill in the gaps; the data must come from operational reality to serve the business and meet expected outcomes. So it was no surprise to see that *doers* have largely achieved full-stack observability, while *dawdlers* are still struggling to do so.

Simply achieving full-stack observability does not guarantee an organization will be able to wring insights from it. Indeed, when we dig into the challenges with extracting insights from that data, no one is immune. Half (50%) of *dawdlers* struggle because they lack full-stack observability, while half (51%) of *dabblers* and a majority (58%) of *doers* are both challenged by data silos that keep critical telemetry locked up in disparate solutions. This is why the observability strategy is directly tied to the digital maturity of an organization.

Observability Strategy

Full-stack observability depends largely on the ability to make connections between disparate data across the stack. That can be enabled or impeded by an organization's strategy with respect to how that data is stored.

Ultimately, an observability strategy can determine whether you end up with a data lake or a data swamp. The difference is important. After all, it's expected that the insights drawn from observability will eventually drive automation that impacts business and operational outcomes. Getting it right is of the utmost importance.

It was no surprise that 65% of *dawdlers* have no strategy at all. Still, it is an improvement over the 72% of *dawdlers* who had no strategy in place in 2023.

More *doers* than *dabblers* have adopted a single data lake approach to managing telemetry, which aligns with plans shared last year around consolidation. Last year, nearly half (45%) of *doer* said they planned to consolidate on a single data lake; only 35% have reached that goal this year. Given challenges with integration, interoperation, and tool sprawl affecting every domain, we anticipate that the number of organizations hoping to achieve the goal of consolidation will continue to outpace the number that are able to do so. For decades, enterprises have leveraged data warehouses to extract business insights from customer data. It's no surprise to see a similar approach for telemetry.

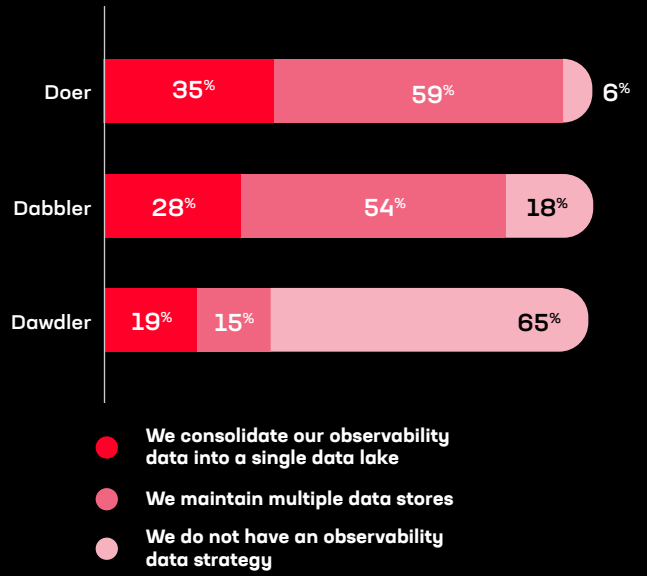
The Impact of Generative AI on Data

Of all the domains in the enterprise architecture, data is the one most impacted by AI today. The power of generative AI, after all, lies in its ability to generate data. While most of that data will wind up discarded, some will be used—as code, queries, and historical conversations that unearthed insights.

Generative AI is built on data. While the predominant use of generative AI is via established (foundational) models which have already consumed vast quantities of data, it is also true that most organizations are already adopting retrieval augmented generation (RAG) techniques that enable greater precision of answers than a general LLM can provide alone. It is the use of RAG, which relies on additional sources of data, that is dramatically impacting this domain, changing established application architecture patterns and, by extension, every other enterprise domain.

The generation, collection, processing, and governance of all this data—from operations to business use cases—is driving new practices, approaches, and pipelines into the enterprise. This is, indeed, a new frontier for most organizations that will need exploration and careful navigation to ensure the data domain will mature at a rate that allows the continued maturation of other domains in a digital business—which are, after all, dependent on data.

Observability Strategies by Digital Maturity



Key Capability: App Delivery

"App delivery and security have become key capabilities due to the increasing importance of digital services on every business. But while the deployment and distribution of these services is normalized,the ability to operate them at scale by harnessing automation has not. Generative AI promises to accelerate automation of app delivery and turn the ability of digital business to scale exponentially."

Lori MacVittie, F5 Chief Evangelist and Distinguished Engineer

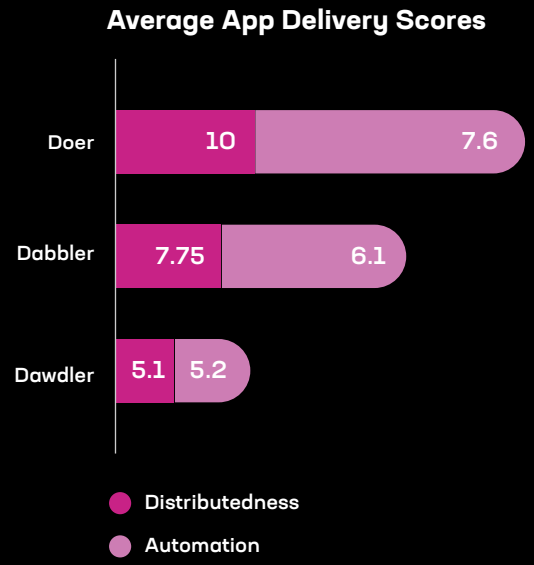
Enterprise Architecture for Digital Business

The Top Three Digital Doers

With respect to maturity of app delivery, the top three industries for digital *doers* were:

1. Healthcare
2. Education
3. Energy/natural resources

This is somewhat surprising as there were less than 3% of digital *doers* in each of these industries, overall. However, given the distributed nature of these types of organizations, we suspect the ability to distribute resources is not what is holding them back from digital maturity, but rather struggles with maturing other capabilities.



A top score for app delivery is 30 points, with each measure contributing 15 possible points.

Measures

Distributedness: A digital business must be able to deploy app delivery and security services where applications, employees, and consumers need them.

Automation: A digital business must be able to respond to changing conditions to maintain performance, availability, and security of digital services with minimal human intervention.

Distributedness

It is no surprise that app delivery distributedness maps closely to the distributedness of infrastructure. After all, both domains exist to deliver and secure applications—which are increasingly distributed across core, cloud, and edge.

The ability to distribute the services responsible for scale, speed, and security of applications and APIs is critical, and contributes to the average 93% deployment rate for each of thirty different application services. This rate has increased dramatically, with growth driven by acceleration of digital transformation caused by the global pandemic. With billions now relying on digital services for work, play, and financial management, the security and availability of applications and APIs is inarguably important.

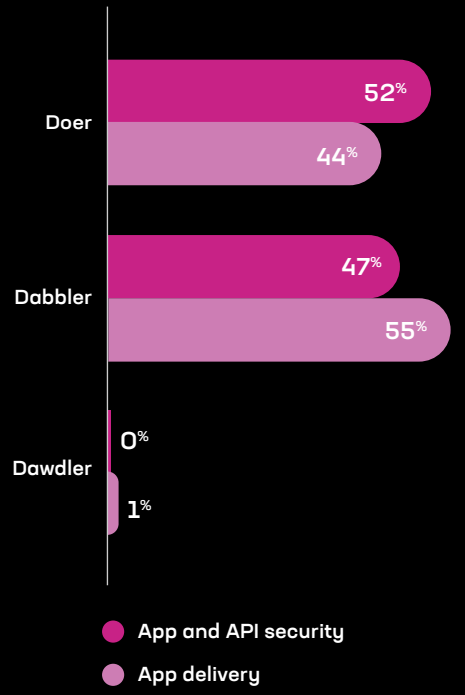
The impact of distributedness can be seen in the enterprise portfolio strategy, which looks at plans for applications and their deployment. *Doers* are five times more likely than *dawdlers* to plan on modernizing applications with the intention of enabling portability across public cloud providers. Mobility of workloads—whether to improve performance or reduce costs—is a desired capability that comes with digital maturity, which relies heavily on the distributedness of app delivery and supporting infrastructure.

Automation

Automation of app delivery and security services is the capability that all organizations—from *dawdlers* to *dabblers* to *doers*—can improve. This capability remains the least mature across all measures, with app and API security seeing slightly better rates of automation than their counterpart, app delivery.

Overall, about 40% of respondents have automated app and API security functions and a mere 23% have automated app delivery. For those who have not automated, the reasons cited vary little based on maturity. For 48% of *dawdlers* and 38% of *dabblers*, skillsets are holding them back. For 51% of *doers* and 38% of *dabblers*, budget gets in the way. But close behind budget for *doers* is complexity; that is, 49% cite a lack of interoperability and 49% point out there are too many tools and APIs. This picture repeats for app delivery automation, with complexity rising as a blocker for both *dabblers* and *doers*.

App Delivery and Security Automation



Of the 40% who have automated app and API security and delivery, most are dabblers and doers.

We suspect there is a correlation between complexity, skillsets, and budgets, as app delivery and security are rarely standardized across the enterprise. A heterogeneous set of tools, technologies, and services are used—each with their own unique consoles, APIs, and dashboards. Thus, it is costly for an enterprise to acquire a bench of experts, which contributes to anemic automation capabilities even in the most mature digital organizations. However, generative AI has now entered the room and breathed new life into the potential for achieving this capability.

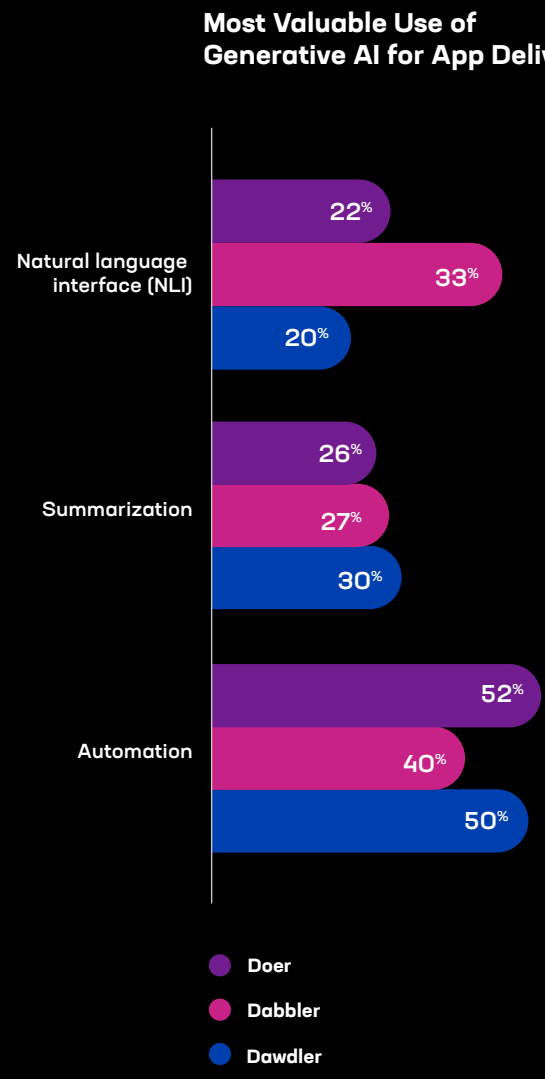
The Impact of Generative AI on App Delivery

While generative AI is likely to have significant impacts across every business, there is no architectural domain more likely to benefit from its arrival than app delivery and security.

As the complexity of scaling, optimizing, and securing applications and APIs in a hybrid IT estate continues to grow, there is an urgent need for automation to help scale operations to meet what is highly dynamic demand. In addition to its obvious use as a natural language interface (NLI) to complex operational data sets, generative AI has the potential to generate configurations specific to app delivery and security solutions far faster than any human operator.

But generation still assumes some way to put them in place, and generative AI does not disappoint. With emergent agent-based capabilities, generative AI promises the ability to not only generate configurations and policies but deploy them by leveraging the APIs that app delivery and security solutions have been providing for years.

This use of generative AI was rated the most valuable in general. Digging deeper, those who **haven't automated app delivery functions**—whether *dabbler* or *doer*—tagged automation capabilities of generative AI as most valuable whether their blocker was budget, skillsets, or complexity. While leveraging generative AI to summarize performance and metrics for executives and board members is considered less valuable, it still handily beat out using generative AI as a natural language interface to operational data.



Key Capability: SRE Operations

The Top Three Digital Doers

With respect to maturity of SRE operations, the top three industries for digital *doers* were:

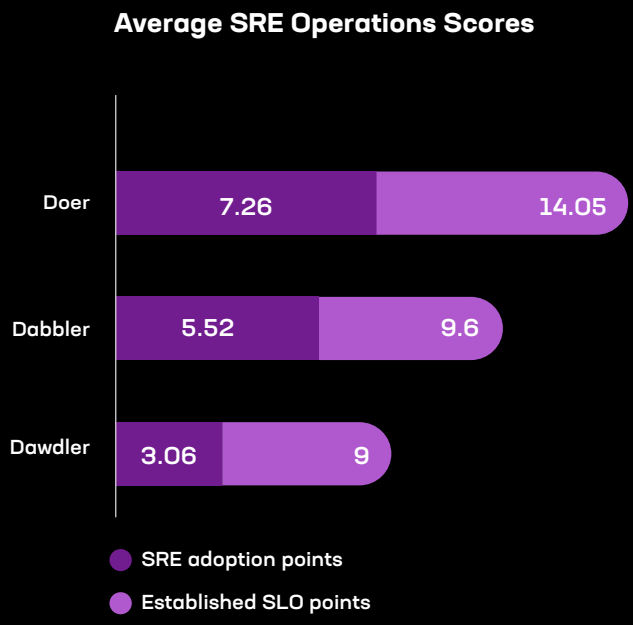
1. Telecommunications
2. Cloud service providers
3. Government/public sector

While we were not surprised to see telecom or cloud service providers leading *doers* in maturity of SRE operations, we were surprised to see government/public sector demonstrate such a high degree of maturity. Perhaps we shouldn't be, given that government and public sector organizations today are just as distributed and reliant on scalable operational practices as telecom and cloud service providers.

SRE Adoption

Adopting SRE operations is more than just changing people's titles in an org chart. SRE operations fundamentally operates on a different set of principles that drive toward achieving business outcomes rather than avoiding operational incidents. That means implementing practices that support reducing mean time to resolution (MTTR) and availability of services rather than trying to hit an unattainable uptime metric.

We've seen SRE adoption explode over the past few years, with more organizations already or planning to adopt its practices. It is no surprise that nearly all *doers* (97%) have adopted or are planning to adopt SRE practices, while a strong majority (86%) of *dawdlers* have not. The benefits go beyond operations and impact a broad set of capabilities across the entire organization.



A top score for SRE operations is 24 points, with SRE adoption contributing 9 possible points, and established SLOs 15 possible points.

Measures

SRE adoption: A digital business needs to adopt SRE operational approaches to scale its capacity and ability to operate digital services.

Established SLOs: A digital business aligns its operational goals with business outcomes.

More than half (60%) of all organizations can operate hybrid applications. That is, multiple components of a single application are deployed in different locations. A single app might have a data source on-premises, a front end in the public cloud, and other services deployed at the edge. Hybrid apps allow organizations to optimize deployment for performance and cost. With plans for AI engines and applications to be hybrid, the ability to operate hybrid apps becomes a key indicator for AI readiness.

That capability is tied to the adoption of SRE operations. Nearly all organizations running hybrid apps have adopted SRE operations. The 8% of *dabblers* who do so without adopting SRE are outliers, as the majority are staunchly in the adopted or planning to adopt SRE operations categories.

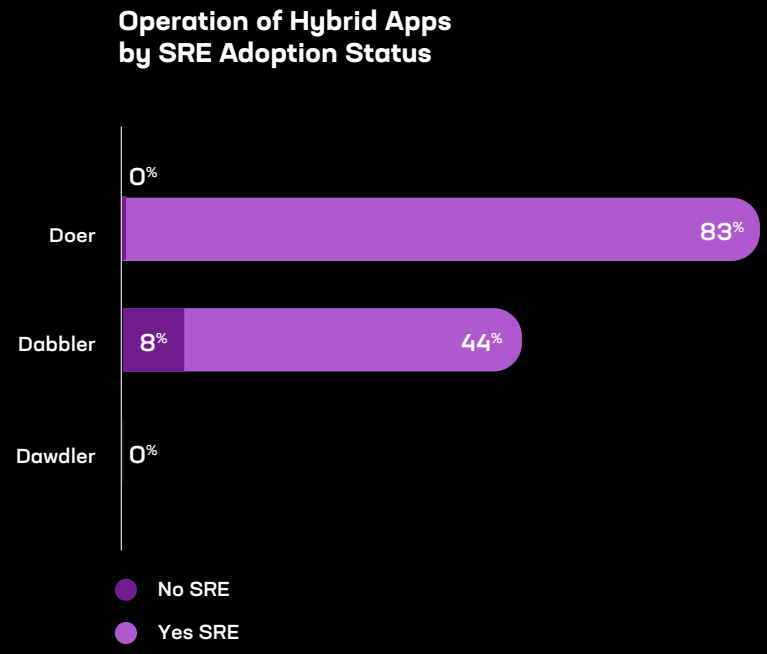
Unfortunately, simply adopting a new operational approach isn't enough. There must be clearly defined and measurable objectives toward which the practices can be used.

Established SLOs

Service level objectives (SLOs) are markedly different from their predecessors—service level agreements (SLAs)—in that organizations strive to achieve objectives that are aligned with business outcomes rather than purely operational metrics. Operations teams measure at a much more granular level using service level indicators (SLIs) to help guide their processes toward quicker identification of root causes and faster resolution of incidents. This approach shifts the focus toward achieving a goal rather than avoiding a penalty and allows for continuous improvement in processes. In turn, these shifts lead to a healthier operational organization that is better able to support dynamic and distributed environments.

Doers, almost universally, have established SLOs (92%) compared to zero percent of *dawdlers*. The establishment of SLOs has impacts on other domains, particularly that of observability, data, and how operations teams use telemetry. Two-thirds (67%) of *doers* with established SLOs use telemetry to drive automation, while only 15% of *dabblers* can say the same.

Conversely, the ability to establish and work toward SLOs is heavily influenced by the availability of full-stack observability. Nearly half (47%) of the *doers* with established SLOs have also achieved full-stack observability, compared with a mere 1.5% of *doers* who have established SLOs but not achieved full-stack observability.



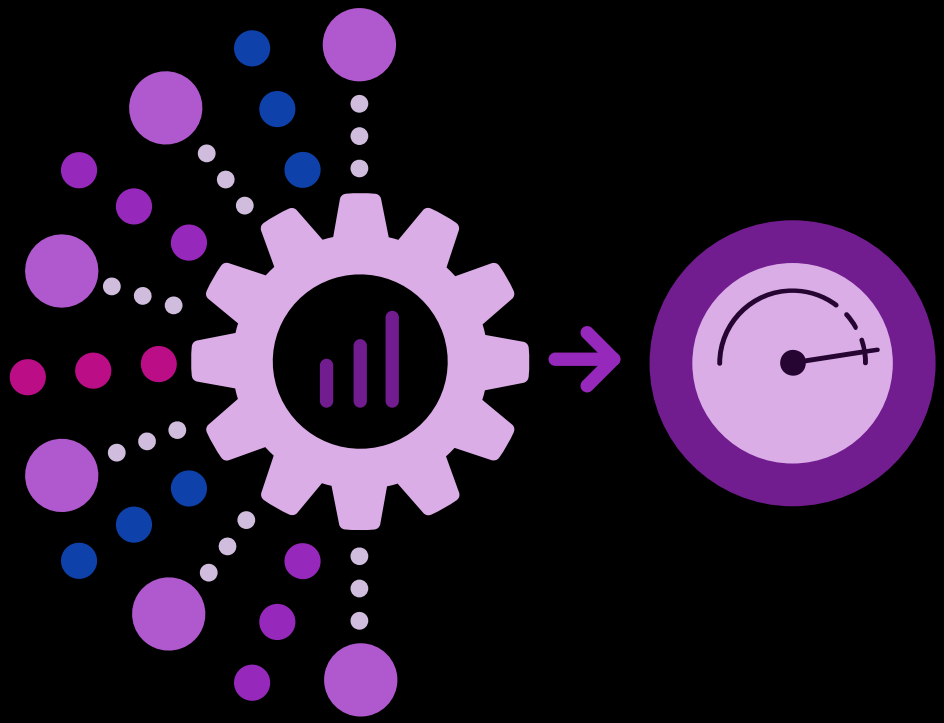
The mature digital business is not only an amalgam of technology and business, but also an interwoven set of technical capabilities that produce the ability to harness AI in all its forms.

The Impact of Generative AI on SRE Operations

Of all the domains in an enterprise architecture, few will be as impacted by AI as operations. While productivity currently gets top billing because of generative AI's ability to summarize and generate natural language content, it is its ability to generate code and queries that will advance what is known as AIOps.

AIOps is generally defined as the use of AI to drive and optimize operations. From analysis of the volumetric data generated by observability (telemetry) to acting autonomously on discovered insights, AI in both predictive and generative forms will join forces as hypermodal AI to deliver unparalleled advances in automation of operations. This, in turn, will enable businesses to scale and secure applications, APIs, and data in ways that previously were impossible to achieve.

When we examine the value assigned to generative AI with respect to app delivery—the domain with the lowest automation rates—we find that *doers* are nearly twice as likely as *dabblers* to see the value of applying AI toward automating the generation and deployment of operational polices. Across the board, as digital maturity grows, so does the interest in using generative AI to automate technical capabilities. Digital *doers* view AI as a force multiplier of all technical capabilities and will ultimately benefit from it while *dawdlers* continue to struggle to find use cases and applications.



Key Capability: Security

"AI will have a profound impact on cybersecurity, enabling everyone, not just an elite few, to gain access to a technology that radically improves productivity while simultaneously exposing a new class of threats and concerns. Viewed from the threat landscape lens, the ability to launch sophisticated attacks will no longer be the purview of nation-states and well-funded hacking syndicates but will be open to anyone with modest prompt engineering skills."

Ken Arora, F5 Distinguished Engineer and Strategic Architect

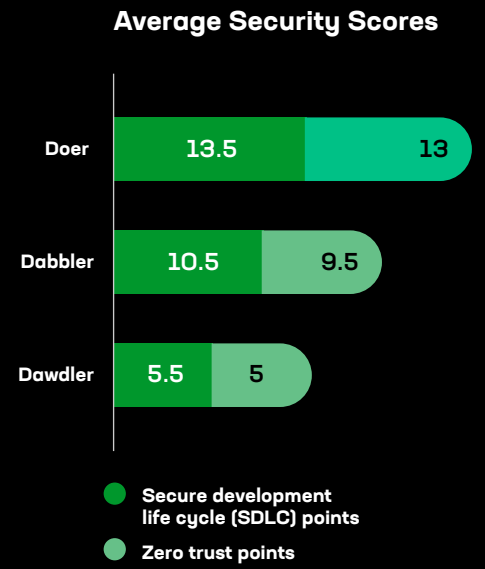
Enterprise Architecture for Digital Business

The Top Three Digital Doers

With respect to maturity of the security domain, the top three industries for digital *doers* were:

1. Government/public sector
2. Cloud service providers
3. Telecommunications

It is no surprise that one of the sources of regulation and standards—governments—leads all industries in security maturity. That telecom and cloud service providers are also excelling at security is a comforting finding, as so much of our data—corporate and personal—is stored, processed, and transferred via these industries. To be fair, among individual organizations, some of the top *dawdlers* are also government and public sector, which is to say that no industry has a lock on digital maturity when it comes to security.



A top score for security is 30 points, with each measure contributing 15 possible points.

Measures

SDLC adoption: A digital business depends on its software and services, making their security a priority.

Zero trust adoption: A digital business approaches security as risk management, employing an approach that supports continual assessment and centers on identity.

SDLC Adoption

Security of software starts—or should start—before the first line of code is written. The SDLC—secure development life cycle—starts with planning a piece of software and extends to the end of its life. The adoption of this approach provides a consistent foundation upon which software is designed, developed, tested, and ultimately, maintained. Thus, it is a pillar of modern security whose adoption indicates digital maturity.

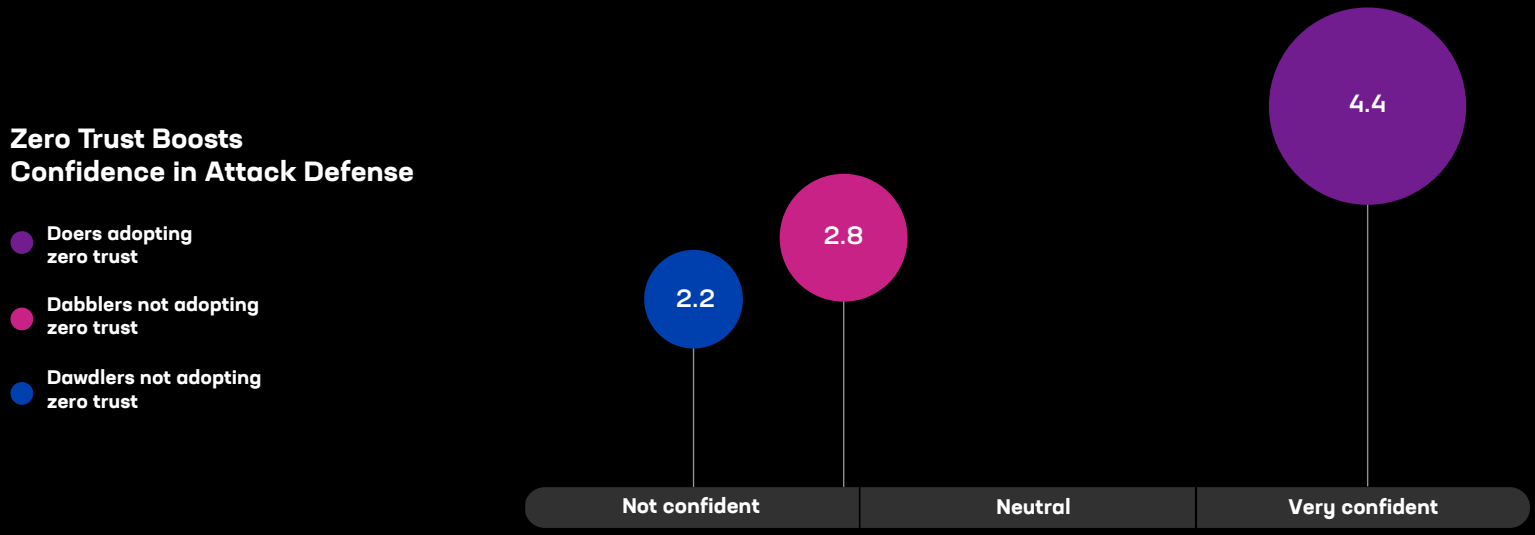
Adhering to secure development practices nets intangible benefits for the business, such as the confidence to withstand an attack on applications or APIs. Even *dawdlers* who have adopted SDLC report greater confidence (3.3 of 5) than their non-adopting counterparts (2.8 of 5). And *doers* are even more confident when adopting SDLC, reporting an impressive average confidence of 4.4 out of 5.

Zero Trust Adoption

Not all that confidence comes from adopting the SDLC. Some of it comes from putting zero trust principles into practice. We see the same pattern of confidence across *dawdlers* and *doers* with respect to adoption of zero trust. Adoption correlates with higher confidence, and *doers* have an even greater confidence than their *dawdling* counterparts.

The adoption of zero trust relies heavily on the maturity of other domains. Distributedness of app delivery and infrastructure, observability, and data maturity all contribute to the ability to put zero trust into practice by ensuring visibility and the capability to act on insights using distributed tools and technologies.

Zero Trust Boosts Confidence in Attack Defense



Confidence to withstand an application or API layer attack. Confidence rated as (1) no confidence to (5) great confidence.

The Impact of Generative AI on Security

Security, whether enforcement, monitoring, or operations, was one of the first domains to benefit from predictive AI and is rapidly becoming the first to enjoy benefits from generative AI.

The ability of predictive AI to uncover patterns and anomalies indicative of a potential attack combined with the ability to automatically generate the appropriate actions to counter that attack promises to improve the efficacy of both security solutions and operations. This is particularly encouraging given that efficacy and automation are the two top use cases for generative AI in the realm of security.

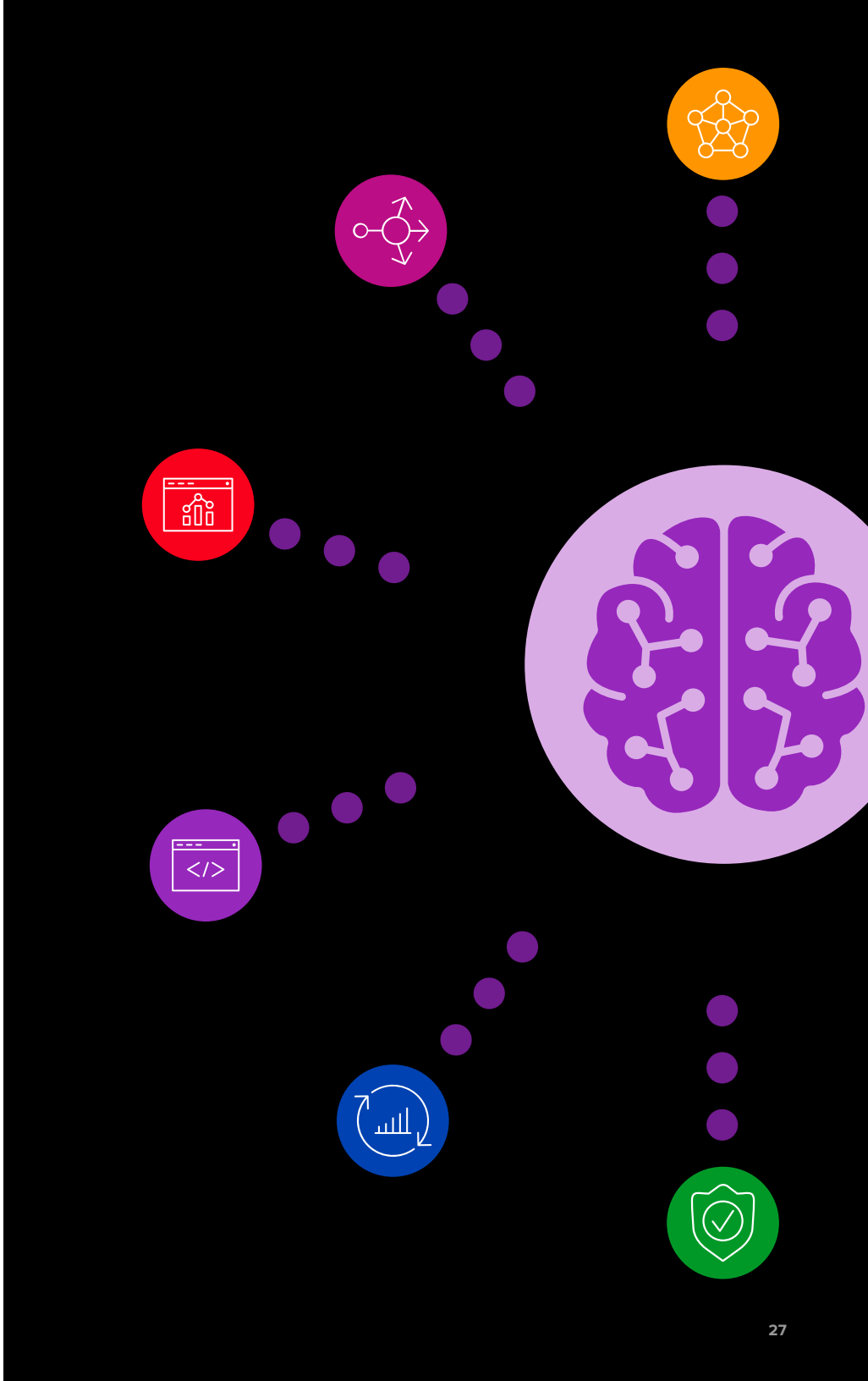
This is also one of the few areas where all enterprises, regardless of digital maturity, agree. While *doers* were more likely to value generative AI as a tool to achieve autonomous security, even *dawdlers* reported slightly more value for this use case over improving efficacy.

Technology is already shifting to incorporate generative AI into security services and solutions, with platforms adding automation to improve efficacy of operations. We anticipate significant progress in the next two to three years with respect to AI and its integration with security.

Conclusion

Digital maturity is difficult to measure. The expansive nature of today's enterprise organizations prevents a "lift and shift" approach to the modernization required to achieve digital maturity. We see organizations making progress in multiple domains, including those that have been introduced as necessary to maintaining momentum on the digital transformation journey.

While there has been significant maturing in the past year, we expect that will pale to the advancements in the coming years thanks to the introduction of generative AI and the steady march of modernization.



About the Report

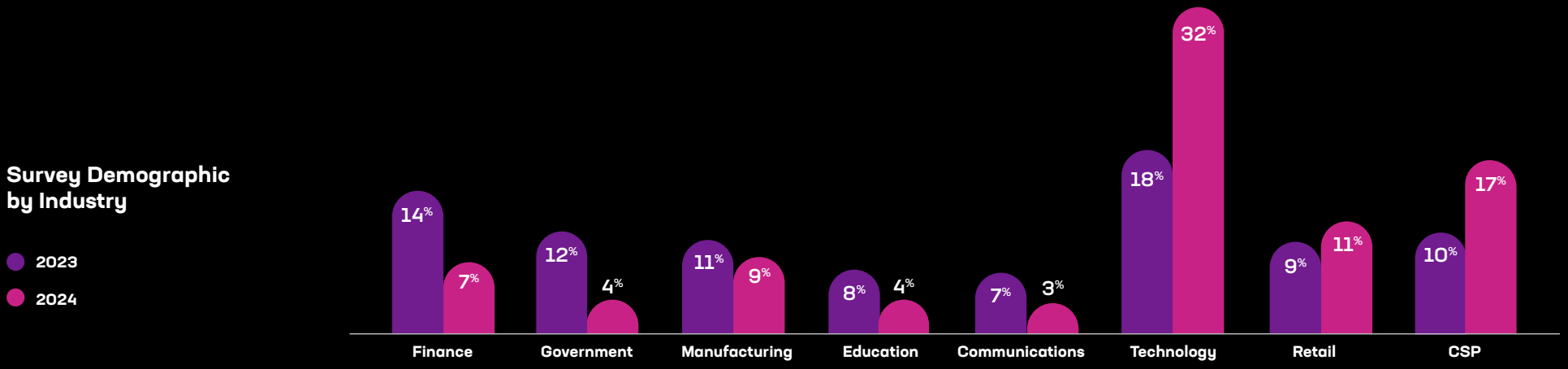
We analyzed 713 responses selected from our annual State of Application Strategy research based on completeness of answers to the key questions that make up our digital maturity model.

Just about one-third of respondents hail from the technology industry. There is good representation from retail, manufacturing, and financial services.

Respondents represent a global sample, with just about a third from each major region: NA, EMEA, and APCJ.

Similarly, grouping by annual revenue nets a fairly even distribution across large (27%), medium (32%), and smaller enterprises (32%).

Survey Demographic by Industry



ABOUT F5

F5 is a multicloud application security and delivery company committed to bringing a better digital world to life. F5 partners with the world's largest, most advanced organizations to secure every app—on premises, in the cloud, or at the edge. F5 enables businesses to continuously stay ahead of threats while delivering exceptional, secure digital experiences for their customers.

For more information, go to F5.com. (NASDAQ: FFIV)