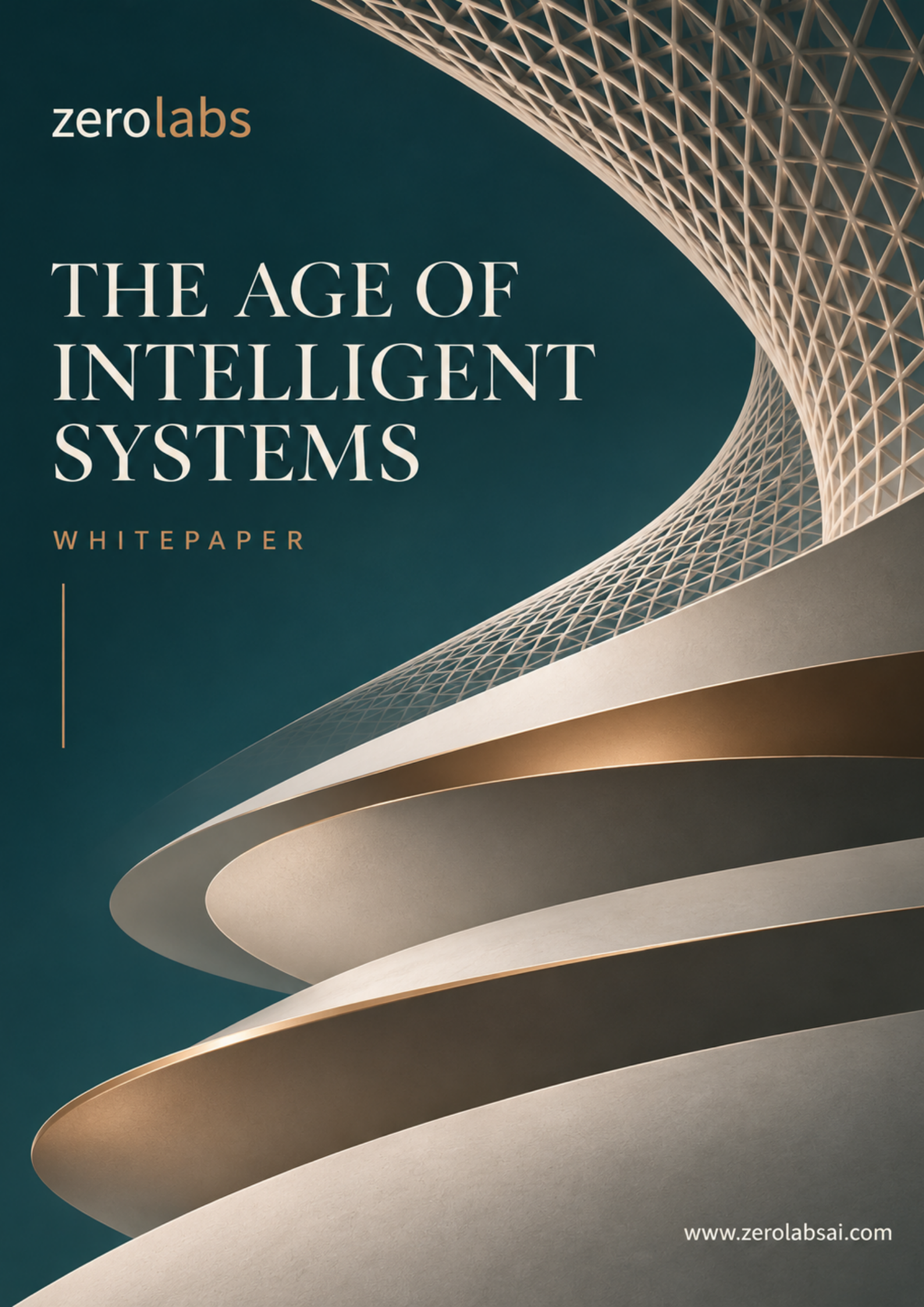
zerolabs

THE AGE OF INTELLIGENT SYSTEMS

WHITEPAPER



www.zerolabsai.com

READING GUIDE

Inside this white paper

This illustrated edition follows the research manuscript published on the Zero Labs White Paper page. Research figures, comparisons, and diagrams include the source limitations and evidence qualifications.

01 / FOREWORD	The Next Technology Challenge May Be Our Ability to Keep Up
02 / EXECUTIVE SUMMARY	The Enterprise Software Adaptation Gap
03 / CHAPTER 01	The Hidden Economics of Enterprise Software
04 / CHAPTER 02	The Cost of Changing What Already Exists
05 / CHAPTER 03	The Cost of Delayed Adaptation
06 / CHAPTER 04	Why Artificial Intelligence Changes the Context
07 / CHAPTER 05	An Existing Economic Burden, Not a Hypothetical Market
08 / RESEARCH CONCLUSION	The Problem Is Not a Lack of Technology
09 / REFERENCE NOTES	Sources & Methodological Notes

Publication status: This is a foundational research manuscript (v0.2). Its figures and source interpretations remain subject to final editorial, methodological, copyright and citation verification. These charts visualize cited source data, not additional research.

01 / FOREWORD

The Next Technology Challenge May Be Our Ability to Keep Up

Technology has always evolved alongside the needs of business.

Companies introduce new systems to improve productivity, reduce operating costs, increase reliability, meet regulatory requirements, and respond to changing markets.

Over time, those systems become fundamental to the organization's operations.

They manage financial transactions, customer relationships, production processes, supply chains, employee services, and the information businesses depend upon to make decisions.

But technology investments do not end when systems become operational.

Applications must be maintained. Infrastructure must be updated. Dependencies change. Security vulnerabilities emerge. Business requirements evolve. Regulatory expectations shift. Customers demand new capabilities.

And every new system must coexist with the technologies that came before it.

The result is a continuing financial and operational responsibility that is rarely visible to customers but is fundamental to how modern enterprises function.

Artificial intelligence is changing the environment in which this responsibility must be managed.

In only a few years, AI has progressed from specialized analytical applications toward systems capable of assisting with increasingly complex knowledge work, software development, design, and operational activities.

Businesses are gaining access to capabilities that previously required considerable expertise, investment, or development effort.

Yet an important question remains.

If technological capabilities are advancing rapidly, can the software ecosystems supporting established businesses evolve at a comparable pace?

Existing research suggests that many organizations face considerable difficulty maintaining this balance.

Technical debt consumes technology budgets. Modernization programs encounter delays and cost overruns. Security remediation requires continuing engineering effort. Organizations struggle to connect new technological investments with measurable business outcomes.

These are not problems created exclusively by artificial intelligence.

They existed long before the emergence of modern generative AI.

What has changed is the pace at which new technological capabilities are becoming available—and the potential consequences of being unable to adopt them effectively.

This paper investigates a challenge we call the Enterprise Software Adaptation Gap.

It examines the financial and operational pressures associated with maintaining existing technology while responding to new business requirements.

Our purpose is to understand the scale of the problem, the economic forces behind it, and why it deserves greater attention as businesses enter the age of intelligent systems.

Before considering new approaches, we must first understand what organizations are struggling to accomplish, what those difficulties cost, and why existing investments have not eliminated them.

02 / EXECUTIVE SUMMARY

The Enterprise Software Adaptation Gap

RESEARCH AT A GLANCE

$545B - $720B

Worldwide application services

2025 market baseline to 2029 forecast; broad industry category.

GARTNER [1]

80% / 20%

Run versus change

Budget allocation for studied heavy IT sustainers, not all enterprises.

MCKINSEY / SERVICEWARE [3]

$1.52T

Accumulated US technical debt

Historical 2022 modeled stock; not yearly spending or addressable market.

CISQ [7]

43 days

Median vulnerability remediation

Studied known-exploited vulnerabilities; not a universal benchmark.

VERIZON DBIR 2026 [6]

These statistics concern different markets, samples, years and methods. They are not additive.

Technology investment is growing. So is the challenge of sustaining and changing existing systems.

Modern enterprises depend on increasingly complex portfolios of applications, infrastructure, data platforms, and technology services.

These investments are essential to daily operations. However, they also create continuing obligations that compete for financial resources and engineering capacity.

The challenge is not simply deciding which technologies to adopt.

It is maintaining reliable operations while continuously adapting existing systems to changing business conditions.

We define the Enterprise Software Adaptation Gap as:

The difference between the technological changes an organization needs to deliver and its practical capacity to implement, secure, verify, and sustain those changes within acceptable time, cost, and risk constraints.

This is a proposed research construct rather than an established industry measurement.

Three interconnected economic pressures

1. **The cost of maintaining existing technology**

Organizations allocate significant resources to operating applications, maintaining infrastructure, addressing technical debt, complying with requirements, and supporting established business processes.

These commitments can constrain the resources available for developing new capabilities.

2. **The cost of changing existing technology**

Application modernization, system integration, software upgrades, testing, and business-process changes require coordination across interconnected environments.

As dependencies accumulate, individual changes may become increasingly difficult to evaluate and implement safely.

3. **The cost of delayed adaptation**

When important changes cannot be completed promptly, organizations may face prolonged security exposure, operational inefficiencies, deferred improvements, and missed business opportunities.

The consequences can extend beyond technology budgets into broader business performance.

What existing research indicates

Gartner's 2025 forecast estimated the worldwide application services market at $545 billion, growing to $720 billion by 2029. This represents an established expenditure category, although not all of that spending relates to the adaptation problems examined here.[1]

McKinsey's research has documented how technical debt diverts funding from new-product development. Its more recent 2026 analysis shows the continuing difficulty of balancing expenditure on existing operations against investments in new capabilities.[2][3]

Enterprise modernization surveys published in 2026 report substantial budget overruns, delayed initiatives, and incomplete understanding of application dependencies.[4][5]

Cybersecurity research demonstrates that software vulnerabilities remain an important route for attackers and that remediation requires substantial time.[6]

These findings arise from different studies, geographies, and methodologies. They should be interpreted as complementary evidence of related problems—not combined into a single estimate.

The central research proposition

The ability to introduce new technology is advancing, but the economic and operational burden of maintaining and changing existing enterprise systems remains significant.

The research that follows investigates whether this burden is becoming a more important constraint on organizational competitiveness.

It also examines the conditions under which businesses can improve their capacity to change without compromising reliability, security, financial discipline, or accountability.

03 / CHAPTER 01

The Hidden Economics of Enterprise Software

Every application creates an ongoing obligation.

An enterprise application is not a one-time purchase or development activity.

Whether created internally or acquired from a third-party provider, it becomes part of an operating environment requiring continuing attention.

Its dependencies must remain supported. Its data must remain accessible and protected. Its integrations must continue functioning. Changes must be tested. Vulnerabilities must be addressed. Users must be supported.

The larger the technology estate becomes, the more these responsibilities must be coordinated.

A business may operate modern cloud applications alongside software developed decades earlier.

Some systems may be governed by specialized internal teams. Others may depend on external service providers, proprietary platforms, or technologies for which experienced personnel have become difficult to recruit.

Replacing these systems is not always economically or operationally practical.

Many continue to perform essential functions, even when their underlying technology is no longer modern.

This creates a recurring financial decision.

How much should an organization spend maintaining what already works, and how much should it invest in what the business needs next?

The run-versus-change dilemma

TECHNOLOGY BUDGET ALLOCATION: RUN VERSUS CHANGE

Two categories from McKinsey / Serviceware analysis of 17 enterprises (2026).



Descriptive patterns from the studied group; not an industry-wide average or a recommended budget allocation.

McKinsey and Serviceware examined technology expenditure across 17 global enterprises in research published in March 2026.

Their analysis distinguished two broad categories:

Run expenditure — spending required to sustain existing technology operations, including applications, infrastructure, cybersecurity, compliance, and cloud platforms.

Change expenditure — investments in modernization, new application capabilities, data platforms, analytics, and AI.

The researchers identified materially different allocation patterns across their studied companies.

In the reported archetypes, organizations categorized as heavy IT sustainers allocated approximately 80% of their technology budgets to run activities and 20% to change.

Organizations categorized as deliberate modernizers allocated approximately 63% to run and 37% to change.[3]

These are descriptive patterns from a small sample, not universal benchmarks or recommended ratios for every industry.

Nevertheless, the analysis illustrates a fundamental economic tension.

Spending is required to preserve the value of existing technology. But that same spending competes with investment in the organization's future capabilities.

Technical debt and the price of complexity

Technical debt is commonly understood as the future work and cost associated with software design, architecture, or implementation decisions that make subsequent changes more difficult.

Not all technical debt is inherently harmful. It can arise from reasonable decisions made under time, cost, and business constraints.

However, unmanaged debt can increase maintenance effort and make future development less predictable.

In a McKinsey survey of 50 CIOs at financial-services and technology companies with annual revenues exceeding $1 billion, respondents reported that 10–20% of technology budgets intended for new products were diverted toward technical-debt issues.[2]

Separately, the Consortium for Information & Software Quality estimated accumulated software technical debt in the United States at approximately $1.52 trillion in 2022.[7]

That figure represents a modeled historical stock of remediation obligations, not annual enterprise spending or a current market valuation.

Together, these findings illustrate how past software decisions can impose financial constraints on future development.

The economic question

What proportion of enterprise technology expenditure is devoted to preserving existing systems rather than creating new capabilities?

And how does that allocation change as software portfolios grow more complex?

These questions matter because the economic burden of existing technology is not limited to maintenance invoices.

It also includes engineering time, postponed improvements, dependency on specialized expertise, and the difficulty of redirecting resources toward emerging business needs.

04 / CHAPTER 02

The Cost of Changing What Already Exists

Modernization is not simply replacing old technology.

Businesses modernize applications for many reasons.

They may need to introduce new customer experiences, improve operational efficiency, integrate acquisitions, meet regulatory requirements, reduce infrastructure dependencies, or support new products.

In each case, the business objective may be straightforward.

The engineering work required to achieve it may not be.

A seemingly limited change can involve multiple applications, databases, interfaces, security controls, and operational teams.

Undocumented dependencies may only become visible once implementation has begun.

Compatibility problems can emerge during testing. Critical business processes may restrict deployment windows. Changes may require review by security, compliance, operations, and business stakeholders.

These constraints can make modernization expensive even when the technology being introduced is well understood.

Evidence of modernization difficulty

MODERNIZATION SURVEY INDICATORS

48%

Behind modernization goals

Share of organizations surveyed.

KYNDRYL 2026 [5]

9%

Fully mapped dependencies

Business-critical apps and dependencies.

KYNDRYL 2026 [5]

71%

Exceeded modernization budgets

Surveyed decision-makers at large organizations.

ENSONO 2026 [4]

61%

Paused, scaled back or abandoned

Modernization initiatives in the surveyed group.

ENSONO 2026 [4]

The Kyndryl and Ensono findings are from different samples; these percentages are not global enterprise estimates.

Kyndryl's 2026 State of Modernization study reported that 48% of surveyed organizations were behind their modernization goals.

Only 9% reported having fully mapped their business-critical applications and dependencies.

The surveyed enterprises operated an average of 383 business-critical applications.[5]

These findings suggest that some enterprises face difficulty understanding the full extent of the technology environments they must change.

Without reliable information about application relationships, modernization becomes harder to plan, estimate, and execute.

Ensono's 2026 State of IT Modernization research provides complementary financial evidence.

Among 500 technology and business decision-makers surveyed at large organizations in the United States and United Kingdom:

• 71% reported exceeding modernization budgets. • 61% reported pausing, scaling back, or abandoning modernization initiatives. • 97% reported that talent shortages had increased costs.[4]

These are survey findings from a defined enterprise population, not globally representative rates. The source is also a modernization services provider, a factor that should be considered when interpreting its findings.

Even with those limitations, the research supports the existence of meaningful challenges in modernization delivery.

Why changes become difficult

Several factors can combine to increase the cost and duration of enterprise software change:

Dependencies. Applications exchange data and rely on services whose behavior may be affected by modifications elsewhere.

Incomplete documentation. Teams may lack reliable records of business rules, interfaces, historical decisions, and operating assumptions.

Legacy constraints. Older systems can remain business-critical while requiring specialized expertise or compatibility safeguards.

Testing requirements. Changes must be verified against expected behavior, particularly when failures can interrupt important operations.

Operational approvals. Security, regulatory, financial, and business responsibilities can require multiple reviews before changes are released.

Limited engineering capacity. Teams must divide their attention between support obligations, incidents, planned improvements, and new projects.

The resulting difficulty is not simply a shortage of programming effort.

It is a coordination challenge involving technology, knowledge, people, and business responsibility.

The economic question

What does it actually cost an enterprise to deliver a verified application change?

The answer requires more than measuring coding time.

It should include discovery, dependency assessment, implementation, testing, rework, approval, deployment, and post-release verification.

This distinction becomes increasingly important when evaluating the impact of new software development technologies.

05 / CHAPTER 03

The Cost of Delayed Adaptation

Some technology changes cannot be postponed without consequence.

Not every delayed software improvement creates immediate financial harm.

Some changes are optional. Others can be deferred without materially affecting business performance.

However, some changes are time-sensitive.

A newly disclosed vulnerability may require urgent remediation.

A regulatory change may establish a fixed compliance deadline.

A failing integration may interrupt transactions.

An outdated application may prevent the launch of an important business capability.

In these circumstances, the organization's ability to implement verified changes becomes a matter of operational and financial risk.

Vulnerability remediation as a measurable example

THE REMEDIATION CHALLENGE

31%

Vulnerability exploitation

Share of initial access in studied breaches.

VERIZON DBIR 2026 [6]

43 days

Median vulnerability resolution

Studied critical vulnerabilities.

VERIZON DBIR 2026 [6]

These represent different study populations and do not measure the probability of a breach at any particular company.

The 2026 Verizon Data Breach Investigations Report found that vulnerability exploitation accounted for approximately 31% of initial-access methods in its analyzed breaches.

Its reported median time to fully resolve the studied critical vulnerabilities was 43 days.[6]

These statistics describe different analytical populations and should not be treated as direct measures of the probability that a particular enterprise will suffer a breach.

They nevertheless illustrate two relevant realities.

Software vulnerabilities remain important security exposures, and remediation can require considerable time.

Discovering a weakness is not equivalent to correcting it.

Depending on the affected asset, remediation may require configuration changes, vendor updates, dependency upgrades, code modifications, testing, and controlled deployment.

Some vulnerabilities require changes to application software. Others involve operating systems, network equipment, vendor-controlled components, or infrastructure.

Their resolution may depend on entirely different technical teams and operational authorities.

The financial consequence of security incidents

IBM's 2026 Cost of a Data Breach Report estimated a global average cost of approximately $4.99 million per breach in its studied population.[8]

These costs include factors such as business interruption, response activities, investigation, customer impact, and recovery.

This figure is not the annual expected security loss of an average company, nor can it be directly attributed to delays in application patching.

It demonstrates the potential financial consequences of certain security failures.

A stronger understanding of the adaptation problem requires examining how long organizations take to resolve known issues, why those issues remain open, and which constraints prevent timely correction.

Delayed business change

Security is not the only area where time matters.

A company may need to update pricing logic, support a new distribution channel, change an approval process, integrate a strategic partner, or adapt its systems to a revised operating model.

When software changes are delayed, the business may be forced to continue using less efficient processes or postpone planned initiatives.

The financial impact is not always visible in technology accounting.

It may appear as additional manual work, slower customer service, deferred revenue opportunities, higher operating expenses, or continued dependency on unsuitable systems.

These costs require case-specific measurement. They cannot be inferred solely from the length of an engineering backlog.

The economic question

What is the cost of a delayed software change?

The answer depends on the business process affected, the importance of the change, the duration of the delay, and the risks involved.

A central objective of this research is to distinguish measurable losses from hypothetical opportunity costs.

06 / CHAPTER 04

Why Artificial Intelligence Changes the Context

The problem existed before AI. The competitive environment is changing around it.

Enterprise software maintenance, technical debt, integration complexity, and modernization delays are longstanding challenges.

Artificial intelligence did not create them.

However, AI may change the relative importance of these challenges as organizations gain access to more powerful development, analytical, and operational capabilities.

Stanford University's 2026 AI Index reports organizational AI adoption reaching 88%, alongside rapid advances in selected technical capabilities.[9]

This indicates broad adoption, but does not mean that 88% of organizations have successfully transformed their business processes or achieved positive financial returns.

The distinction matters.

Adopting a capability is not the same as incorporating it effectively into an operating business.

Individual productivity and organizational performance

AI-assisted tools can reduce the effort required for certain tasks.

Yet an improvement in one activity does not necessarily produce a proportional improvement in the entire business process.

Software development provides a useful illustration.

Generating an initial implementation is only one part of delivering a production change.

The work may also require understanding an existing codebase, reviewing dependencies, testing behavior, validating security, obtaining approval, and coordinating release.

Google's 2025 DORA research emphasizes that AI-assisted development can amplify existing organizational strengths and weaknesses. The benefits of new tools therefore depend partly on the systems and practices in which they are used.[10]

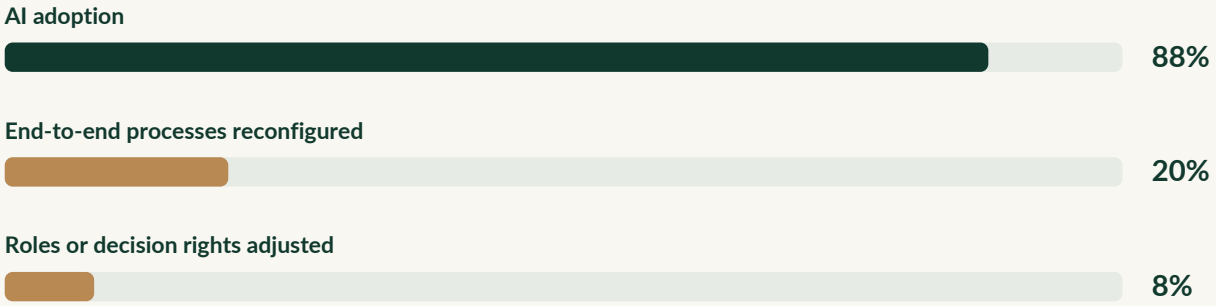
The significance is not that faster coding has no value.

It is that enterprise-level value must be measured through completed and reliable outcomes rather than isolated task speed.

Organizational readiness

AI ADOPTION VERSUS ORGANIZATIONAL TRANSFORMATION

Independent studies describe different stages of adoption; percentages are not directly comparable.



Stanford global adoption data and APAC organizational redesign data have different samples and definitions; visual comparison is illustrative, not a measured conversion funnel.

The World Economic Forum and Accenture's June 2026 research examined how organizations across Asia are adapting their operations to AI.

The report found that only 20% of surveyed APAC organizations had reconfigured end-to-end processes around AI, while 8% had adjusted job roles or decision responsibilities accordingly.[11]

Separately, appliedAI's 2026 maturity assessment placed approximately 59.7% of its 187 assessed European organizations at the experimentation level.

The researchers explicitly cautioned that the sample was not statistically representative.[12]

These studies describe different populations, but both suggest that meaningful operational adaptation can lag behind interest in and deployment of new technology.

New capabilities can create new obligations

AI adoption can introduce additional requirements for data access, integration, evaluation, security, operating controls, maintenance, and continuing improvement.

Avnet's January 2026 survey of 1,200 engineers found that 54% identified continuous learning and maintenance among their leading operational challenges when integrating AI into products.[13]

This is a measure of respondents' concerns, not a quantified increase in maintenance expenditure.

Nevertheless, it reinforces a wider question.

If new technologies create new operating responsibilities while existing systems remain in place, what happens to an organization's long-term technology cost structure?

The strategic question

AI may increase the range of capabilities available to enterprises.

But organizations will benefit differently depending on their ability to integrate those capabilities into existing systems, redesign operations, manage risk, and sustain improvements.

The economic opportunity is therefore linked not only to the pace of technological invention, but also to the capacity of businesses to adapt.

07 / CHAPTER 05

An Existing Economic Burden, Not a Hypothetical Market

Enterprises already pay to maintain and change software.

The commercial relevance of this research does not depend on creating a new spending category.

Organizations already purchase application development services, infrastructure management, system integration, modernization assistance, software maintenance, quality assurance, and cybersecurity services.

Gartner's 2025 application-services forecast estimated worldwide spending of $545 billion, with an anticipated increase to $720 billion by 2029.[1]

This figure is useful evidence that organizations already commit substantial budgets to application-related services.

It is not, however, a measure of the Enterprise Software Adaptation Gap.

The application-services category covers activities beyond the specific problems examined in this paper, and the forecast should not be interpreted as a market opportunity available to any particular company.

Who carries the financial responsibility?

The cost of maintaining and adapting software is distributed across enterprise functions.

Chief Information Officers manage technology investment, operational reliability, modernization priorities, and overall technology expenditure.

Chief Technology Officers and engineering leaders are responsible for software development capability, technology architecture, delivery performance, and engineering quality.

Chief Information Security Officers oversee security risk, vulnerability management, compliance obligations, and coordination with teams responsible for remediation.

Business and operational leaders experience the consequences of technology limitations through delayed improvements, inefficient workflows, customer friction, or constrained commercial initiatives.

These responsibilities vary by organizational structure.

Nevertheless, they indicate why enterprise software adaptation is not simply a technical issue.

It affects financial allocation, operational resilience, business strategy, and executive accountability.

Three distinct forms of expenditure

WORLDWIDE APPLICATION SERVICES: FORECAST

Gartner 2025 baseline and projected 2029 spending, USD billions.



This is a broad application-services spending forecast; it does not represent Zero Labs TAM, current revenue, or available market share.

For analytical purposes, this paper will separate:

Committed operational expenditure: Recurring spending required to maintain existing systems and services.

Planned change expenditure: Budgets allocated to modernization, new features, integration, compliance changes, and other improvements.

Realized costs of failures and delay: Documented losses associated with outages, incidents, project overruns, prolonged remediation, or delayed business outcomes.

Separating these categories is essential.

A projected market size cannot be added to an estimate of technical debt. A historical breach-cost estimate cannot be treated as annual maintenance spending. An expected productivity gain cannot be recognized as realized financial savings.

Each measure answers a different question.

Why this distinction matters

Investors evaluating a technology business need to understand more than whether a problem is interesting.

They need to know whether organizations recognize the problem, allocate money toward addressing it, and continue requiring that work over time.

The evidence reviewed so far establishes the existence of substantial application-services spending and recurring operational challenges.

More precise estimates of expenditure by enterprise size, industry, and problem category remain subjects for further research.

08 / RESEARCH CONCLUSION

The Problem Is Not a Lack of Technology

It is the continuing difficulty of adapting the technology businesses already depend on.

Our research begins with an observation.

Enterprise technology environments accumulate over many years.

Applications become interconnected. Business processes become dependent upon them. Technical decisions create future obligations. Security and regulatory requirements change. Modernization becomes increasingly difficult to separate from the need for uninterrupted operations.

At the same time, new technological capabilities continue to emerge.

Artificial intelligence is accelerating this dynamic by expanding what can be developed, analyzed, and automated.

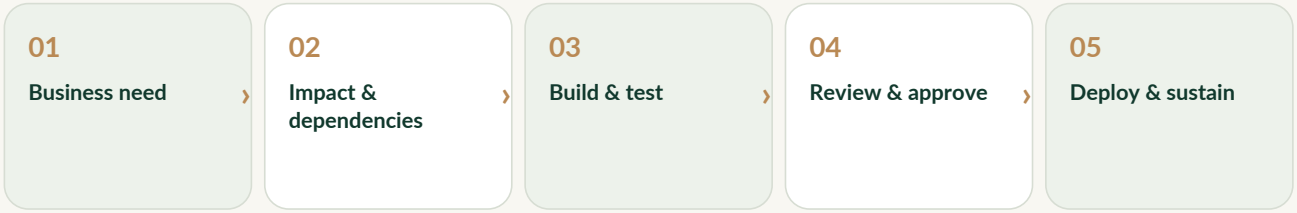
The opportunity for businesses may be substantial.

But so may the challenge of adapting existing environments to take advantage of it.

What the evidence supports

SOFTWARE ADAPTATION IS MORE THAN CODING

A conceptual enterprise change workflow—not a measured industry benchmark.



Enterprise outcomes require requirements, engineering, validation, governance, and ongoing operations—not code generation alone.

The research examined in these opening chapters supports five preliminary conclusions.

First, enterprise application operation and change represent substantial existing expenditure.

Organizations already purchase services to maintain, integrate, modernize, and develop software.

Second, technical debt and legacy complexity create measurable resource constraints.

Published studies document budget diversion, dependency challenges, and difficulties completing modernization initiatives.

Third, the process of changing enterprise software extends beyond software creation.

Reliable delivery involves understanding dependencies, implementation, testing, verification, authorization, and operational coordination.

Fourth, delayed changes can produce material business consequences.

Security exposure, modernization overruns, operational disruptions, and deferred business improvements represent distinct forms of financial and operational risk.

Fifth, increasing technological capability does not automatically eliminate organizational constraints.

AI adoption and task-level productivity improvements do not guarantee enterprise-wide operating or financial benefits.

What remains to be established

This paper does not yet establish that the Enterprise Software Adaptation Gap is widening across all industries.

Nor does it establish a single globally applicable financial cost.

Those claims require longitudinal data that connect technology demand, software change volume, expenditure, delivery capacity, and realized business outcomes.

The next stage of research will investigate these relationships more directly.

The principal research questions

1. How much do enterprises spend annually maintaining and changing existing application portfolios?

2. What portion of that expenditure is associated with technical debt, integration complexity, modernization, and operational support?

3. Which factors most frequently delay the delivery of verified software changes?

4. What are the measurable financial consequences of those delays?

5. How do these costs and constraints vary by industry, organization size, application portfolio, and technology maturity?

6. As AI capabilities advance, do enterprises experience lower adaptation costs, greater technological complexity, or a combination of both?

7. What measurable improvements would materially change the economics of enterprise software maintenance and adaptation?

The central proposition

The next phase of business transformation will require more than access to increasingly powerful technology. It will require the capacity to maintain, secure, and continually adapt the systems upon which organizations depend.

Understanding the economics of that challenge is the purpose of this research.

Before evaluating any proposed solution, the evidence must establish where the burden is greatest, what organizations already spend, and which outcomes they would value enough to purchase.

09 / REFERENCE NOTES

Sources & Methodological Notes

The following references support this initial manuscript. Figures are identified according to their source methodology and should be checked again during final publication review.

[1] Gartner (2025). Forecast Analysis: Application Services, Worldwide. Published July 18, 2025. Market forecast, not observed future spending. https://www.gartner.com/en/documents/6743834

[2] McKinsey & Company (2020). Tech debt: Reclaiming tech equity. Survey of 50 CIOs at large financial-services and technology companies. https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/tech-debt-reclaiming-tech-equity

[3] McKinsey & Company and Serviceware (2026). Recalibrating technology budgets for the AI era. Published March 30, 2026. Analysis of 17 global enterprises. https://www.mckinsey.com/capabilities/mckinsey-technology/our-insights/recalibrating-technolog y-budgets-for-the-ai-era

[4] Ensono (2026). The State of IT Modernization 2026: Enterprise Reality Check. Survey of 500 decision-makers in large U.S. and U.K. organizations.

https://www.ensono.com/insights-and-news/white-papers/your-legacy-systems-arent-the-proble m/

[5] Kyndryl (2026). State of Modernization Report. Enterprise modernization survey; application portfolio, dependency visibility, and modernization progress. https://www.kyndryl.com/au/en/insights/research/enterprise-modernization-report

[6] Verizon (2026). 2026 Data Breach Investigations Report. Security incident analysis and vulnerability-remediation findings. https://www.verizon.com/business/resources/reports/dbir/

[7] Consortium for Information & Software Quality (2022). The Cost of Poor Software Quality in the U.S.: A 2022 Report. Historical modeled estimates, including accumulated technical debt. https://www.it-cisq.org/the-cost-of-poor-quality-software-in-the-us-a-2022-report/

[8] IBM and Ponemon Institute (2026). Cost of a Data Breach Report 2026. Observational research on breach-related costs. https://www.ibm.com/reports/data-breach

[9] Stanford Institute for Human-Centered Artificial Intelligence (2026). AI Index Report 2026. Technical performance, adoption, economics, governance, and broader AI impacts. https://hai.stanford.edu/ai-index

[10] Google Cloud / DORA (2025). State of AI-assisted Software Development. Research on AI, software delivery, and organizational performance. https://dora.dev/research/2025/dora-report/

[11] World Economic Forum and Accenture (2026). Asia's Human-led AI Opportunity: A Framework for Transformation. June 2026. See particularly pages 6 and 11. Source document: WEF_Human_Centric_AI_Transformation_in_Asia_2026.pdf

[12] appliedAI Initiative (2026). AI Maturity 2026: The Year Agents Redefine Value Creation. March 2026. See page 10. The authors explicitly identify limitations in statistical representativeness. Source document: appliedAI-Whitepaper-AI-Maturity-2026-EN.pdf

[13] Avnet Insights (2026). The Reality of Artificial Intelligence: Engineers Get Behind AI, Despite the Challenges. January 2026. Global engineer survey; see pages 2, 8 and 9. Source document: the-reality-of-artificial-intelligence-whitepaper.pdf

10 / PUBLICATION NOTES

Research Integrity & Publication Notes

Source classification: Industry-spending forecasts, company-sponsored surveys, academic research, observational studies, and modeled economic estimates must remain distinct.

Statistical limitations: Survey findings apply to their sampled populations and should not be extrapolated to all enterprises without justification.

Causation: Evidence that modernization problems and AI adoption occur together does not establish that AI causes those problems.

Market sizing: Existing application-services expenditure cannot be presented as a directly addressable market for a particular product.

Future outlook: Claims about developments between 2027 and 2031 must be labeled as scenarios, assumptions, or projections.

Commercial neutrality: This portion of the paper establishes the enterprise problem. Product proposals, commercial models, and claimed solution benefits are outside its present scope.

Publication status: Research manuscript v0.2. Figures and source interpretations remain subject to final editorial, methodological, copyright, and citation verification.