FORRESTER®

Closing The Resilience Gap

How Professional Services Turn AI Complexity Into Operational Agility

The rapid proliferation of AI is increasing system complexity and expanding the attack surface, making digital disruptions more frequent, faster moving, and more consequential for enterprises. But what's changing most is where and how those disruptions originate. Failures are no longer isolated within a single system or team — instead, they emerge across interconnected AI-driven infrastructure environments that span internal hardware, third-party providers, and AI-driven data pipelines.[1]

In this new reality where agentic AI is infiltrating every workflow, each action is now simultaneously a network routing decision, a security trust decision, and a telemetry event, which only adds to the fragility and pressure on digital systems. AI-driven failures, security breaches, or data integrity issues can trigger immediate downstream impacts on revenue, customer trust, regulatory compliance, and brand reputation. What begins as a technical issue can quickly escalate into a business crisis. This shift is redefining digital resilience from a technical priority into an urgent, enterprisewide imperative for modern infrastructure.

While modern AI-powered support can go beyond break-fix and provide visibility and insights to prevent issues, professional services play a critical mitigating role by:

- Helping organizations design resilient, AI-enabled architectures.
- Embed governance and guardrails into AI systems.
- Operationalize rapid detection, response, and recovery.

A FORRESTER CONSULTING THOUGHT LEADERSHIP PAPER COMMISSIONED BY CISCO, MAY 2026



Without these proactive interventions, organizations risk compounding localized failures into cascading outages, flawed decision-making, and long-term strategic setbacks.

In our study of 718 IT decision-makers with responsibility over their organization's IT infrastructure professional services, we found that scaling AI without also scaling infrastructure resilience is one of the most underestimated risks enterprises face today.

KEY FINDINGS

Skills gaps are creating immediate exposure as threats accelerate. Nearly half of respondents (46%) report shortages in resilience, security, and recovery skills for complex AI infrastructure at the exact moment cyberattacks are becoming more sophisticated and AI is expanding the attack surface. This mismatch has exposed organizations, underscoring the urgency of strengthening resilience through new knowledge, tools, and operating models.

Resilience is breaking down at the seams between systems — not within them. The biggest challenge is no longer a single vulnerability but the inability to see and manage across environments. Forty six percent of respondents struggle to ensure data accessibility and visibility across owned and third party infrastructure, while 42% lack end to end observability. At the same time, 41% cite highly interconnected systems that amplify the risk of cascading failure where one disruption rapidly spreads across the ecosystem.

Legacy infrastructure is intensifying risk at scale. Forty six percent of respondents say their infrastructure cannot meet modern performance or security needs, while 42% report an increasing attack surface. These legacy constraints make it harder to monitor, secure, and recover systems just as the complexity of AI driven environments accelerates.

Building the right resilience stack requires both modernization and expertise. By modernizing IT infrastructure, strengthening observability, and augmenting internal capabilities with professional services, enterprises can reduce detection times, improve recovery outcomes, and build resilience that keeps pace with AI driven complexity.

Skills Shortages And Infrastructure Visibility Issues Compound Growing Complexity Within Legacy Infrastructures

As AI reshapes enterprise environments, resilience challenges are becoming less about isolated weaknesses and more about systemic complexity. Organizations are not just defending individual assets; they are also trying to manage dynamic ecosystems of interconnected technologies, data flows, and dependencies that they no longer fully control.

46%

of respondents cite skills shortages in resilience, security, and recovery at the same time cyberattacks are becoming more sophisticated.

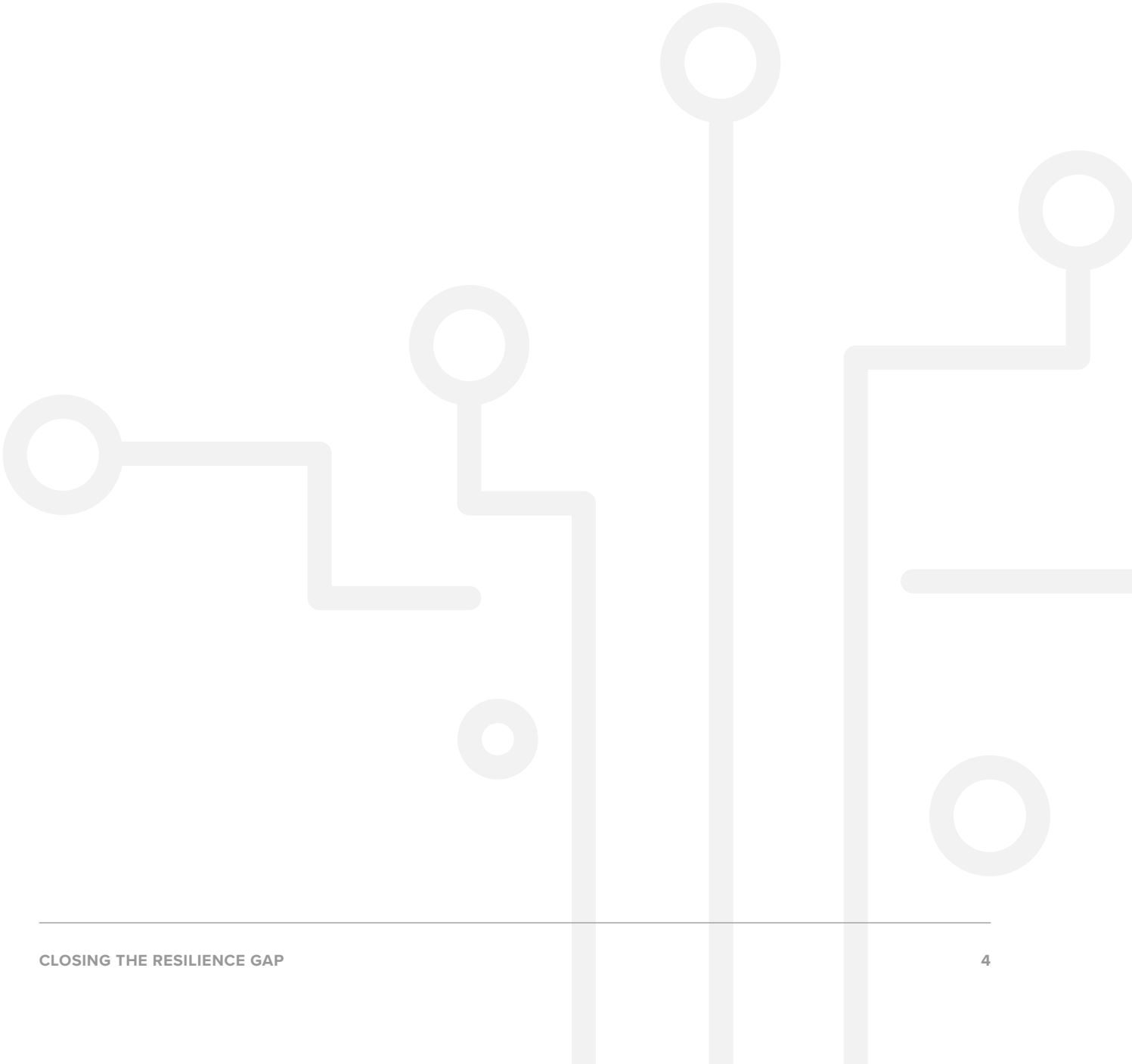


- **Increasing complexity of both cyberattacks and the security landscape leaves organizations exposed.** One of the top challenges reported by 46% of respondents is the shortage of skills in resilience, security, and recovery. At the same time, cyberattacks are becoming more adaptive and sophisticated, leveraging automation and AI to exploit vulnerabilities faster. As the attack surface expands, IT teams are under pressure to defend more systems with fewer specialized resources, creating a widening gap between threat sophistication and defensive capability.

- **Infrastructure must evolve to support an interconnected, high risk environment.** Even highly skilled teams cannot overcome the limitations of outdated systems. Forty six percent of respondents report that aging infrastructure cannot meet modern performance or security requirements. This is compounded by the rise of highly interconnected systems, which 41% say increase the risk of cascading failures. In these environments, a disruption in one component can propagate rapidly, turning minor issues into widespread incidents.

- **Resilience is constrained by what organizations cannot see.** Visibility has emerged as a foundational challenge. Respondents report difficulty

maintaining observability and monitoring across environments (42%), alongside challenges ensuring data accessibility and visibility across both owned and third party infrastructure (46%). AI amplifies this problem by increasing the number of integrations, data pipelines, and external dependencies. As a result, failures often originate in areas outside direct control — making them harder to detect and contain.



The Resilience Gap Is Widening, But Professional Services Can Help Close It

In the AI era, resilience is no longer something organizations can build and manage entirely on their own. It has become an ecosystem challenge, requiring coordination across technologies, teams, and partners. This is where professional services are shifting from a supporting role to a strategic necessity. Building a resilient infrastructure foundation now means designing systems that can adapt continuously, embedding governance into AI workflows and aligning IT, security, and business teams around shared resilience objectives. Organizations that invest in these capabilities today will be better positioned to innovate with confidence in an increasingly volatile environment.

- **Modern organizations require resilient, AI-ready architecture and design.** Respondents recognize that their current environments are struggling to keep pace, but many lack the expertise to independently address these challenges. Professional services are seen as a critical enabler for strengthening resilience. Respondents expect these engagements to enhance cyber resilience (44%) and improve infrastructure architecture and design. Importantly, they also expect better observability and monitoring across both owned and unowned systems (34%), a reflection of the need to manage beyond traditional boundaries (see Figure 1).

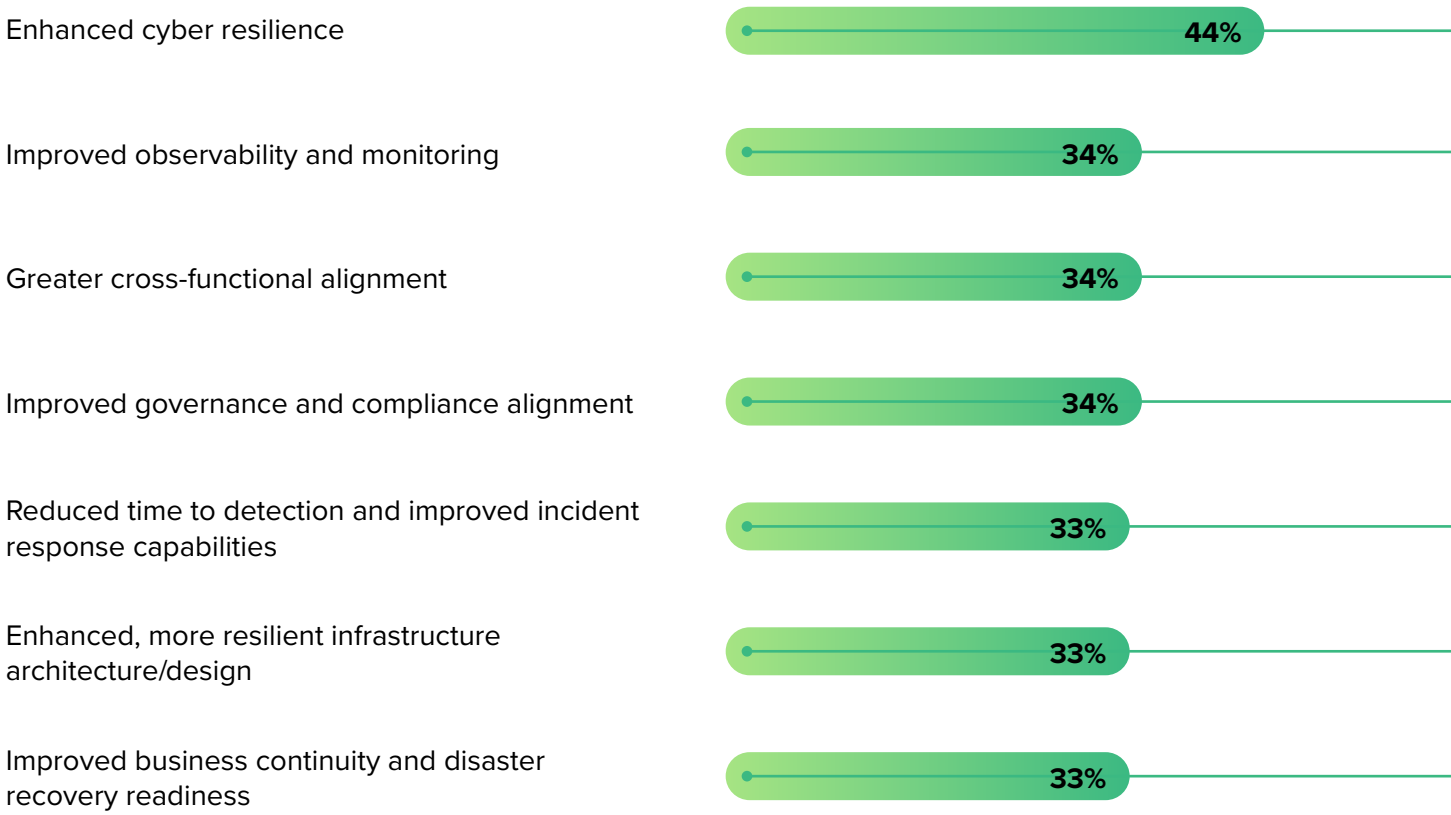
- **Resilience is broader than cybersecurity — and demands cross-functional alignment.** While security remains essential, respondents' expectations reveal a broader definition of resilience. They anticipate improvements in business continuity and disaster recovery (33%), as well as faster detection and incident response capabilities (33%). Beyond technical improvements, organizations expect professional services to drive greater alignment across IT, security, and business teams (34%), as well as to strengthen governance and compliance alignment (34%). These outcomes highlight that resilience is as much about coordination and decision-making as it is about defense.

- **Organizations are embedding professional services in long-term resilience strategies.** Rather than serving as short-term problem solvers, external partners are increasingly viewed as ongoing contributors to resilience maturity. As organizations upskill their workforce and adapt to evolving risks, they expect professional services to support continuous improvement, helping them navigate infrastructure complexity, adopt new technologies responsibly, and maintain alignment across stakeholders.

FIGURE 1

Expected Benefits From Engaging With Professional Services To Aid In Increasing Digital Resilience

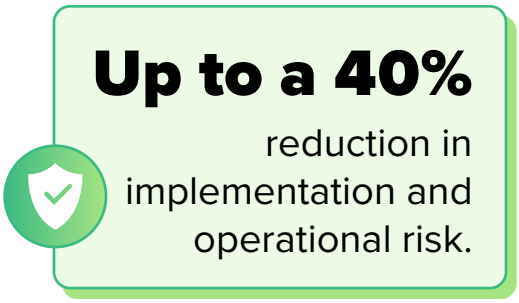
(Showing ranked top five)



Note: Showing top seven responses
Base: 718 IT decision-makers at global enterprises with responsibility over their organization's professional services for IT infrastructure strategy
Source: Forrester's Q1 2026 AI-Enabled IT Professional Services Survey [E-66761]

The Stakes

The consequences of failing to adapt resilience strategies to the AI era are significant and increasingly visible. Organizations that continue operating with limited visibility, outdated infrastructure, and insufficient expertise are more likely to experience disruptions that escalate quickly and spread widely. By contrast, those that invest in modern infrastructure and the right expertise can achieve measurable benefits.



The most common expectations among IT decision-makers include:

- Up to a 40% reduction in implementation and operational risk.
- Up to 30% cost savings.
- Up to a 30% reduction in time to market.

These outcomes reflect not just improved resilience but also improved agility and competitiveness.

Ultimately, resilience in the AI era is no longer a perimeter that organizations build around themselves — it is a distributed capability that spans systems, partners, and processes and must be actively engineered across the entire technology ecosystem. The defining challenge is no longer whether organizations can protect individual systems but whether they can see, manage, and recover across the complex web of those systems and the infrastructure they form. Those that succeed will treat resilience not as a defensive afterthought but as a foundational design principle that is built into their infrastructure, their operations, and their professional services partnerships from the start.

Appendix A: Methodology

Summary Of Results From The Cisco-Commissioned Thought Leadership Study, "The Cost Of Inaction: Why Leaders Must Modernize IT Infrastructure With Professional Services To Maximize AI Investments."

Cisco commissioned this study to understand evolving enterprise use of professional services for IT, especially AI-enabled professional services.

To achieve these objectives, Forrester conducted an online survey with 718 IT decision-makers at global enterprises with responsibility over their organization's professional services for IT infrastructure strategy.

To read the full results of this study, please refer to the Thought Leadership Paper commissioned by Cisco titled, "The Cost Of Inaction: Why Leaders Must Modernize IT Infrastructure With Professional Services To Maximize AI Investments."

Project Team:
Madeline Harrell,
Senior Market Impact Consultant

Contributing Research:
Forrester's Technology Architecture And Delivery research group

Appendix B: Endnotes

[1] Source: The CIO's Guide To AI Readiness, Forrester Research, Inc., January 23, 2026.

ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute their specific priorities using a unique engagement model that ensures lasting impact. For more information, visit forrester.com/consulting.

© Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. [E-66761]