



SMARSH'S 2026 AI TRENDS STUDY

The Future Belongs to Enterprises That Operationalize Communications Data

Protect It. Govern It. Innovate With It.

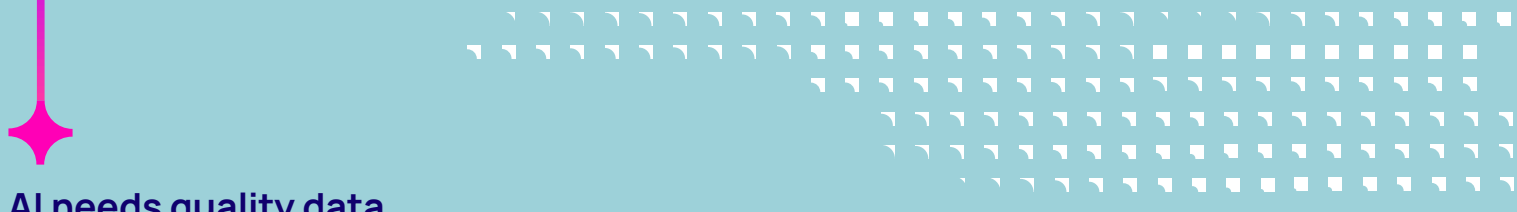
Every competitive advantage in the AI era begins with a single question; can you trust, govern, and operationalize the data hidden inside your organization's conversations? The answer will shape how organizations navigate the 5 trends redefining the future of AI, governance, and communications data.





For decades, communications data was treated as a regulatory obligation. Organizations captured emails, messages, calls, and collaboration data primarily to satisfy recordkeeping requirements, support investigations, and respond to audits.

Today, communications data has become one of the most valuable and underutilized assets in the enterprise. Every customer interaction, employee conversation, collaboration thread, and market signal leaves a digital footprint inside communications systems.



AI needs quality data

Most organizations were not built to operationalize communications data at enterprise scale. Governance frameworks continue to lag behind AI deployment. Communications data remains fragmented across systems, while security and compliance teams struggle to keep pace with increasingly interconnected environments. At the same time, many organizations still view compliance as a defensive function rather than a strategic enabler of innovation.

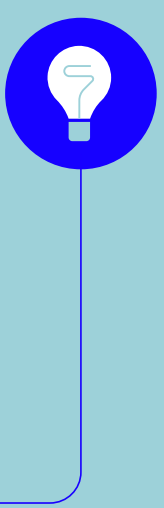
According to Smarsh's 2026 AI Trends Study conducted by FTI Consulting, enterprises are rapidly investing in AI, data modernization, and governance initiatives. Yet the research reveals significant gaps between the pace of technology adoption and enterprise readiness to govern, secure, and maximize the value of these investments.

The findings point to five trends shaping the future of enterprise communications data. AI adoption is accelerating faster than governance. Organizations continue to leave valuable insights trapped within communications archives. Risk is increasingly emerging across interconnected systems, data flows, and AI-driven environments. Security and compliance are evolving from reactive oversight to continuous assurance. And governance itself is becoming a strategic function—one that helps organizations innovate responsibly while managing risk at scale.

The organizations that address these challenges will be best positioned to unlock AI safely, strengthen resilience, and turn communications data into a source of competitive advantage.

Competitive advantage starts with communications data

The future belongs to enterprises that operationalize communications data. Those that can govern it, protect it, and innovate with it will be best positioned to unlock AI safely, manage risk effectively, and create new sources of intelligence across the business.



About the FTI Research Survey

FTI Consulting conducted a survey of 114 decision makers and leaders involved in digital communications monitoring and archiving solutions across enterprise, corporate, and public sector organizations in the United States. The survey was conducted online between March 12–31, 2026. This report represents insights from 47 enterprise-level decision makers working in the financial services, insurance, or banking sectors.

FTI Consulting is an independent global business advisory firm dedicated to helping organizations manage change, mitigate risk and resolve disputes: financial, legal, operational, political and regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centers throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities.

© 2026 FTI Consulting, Inc. All rights reserved. fticonsulting.com

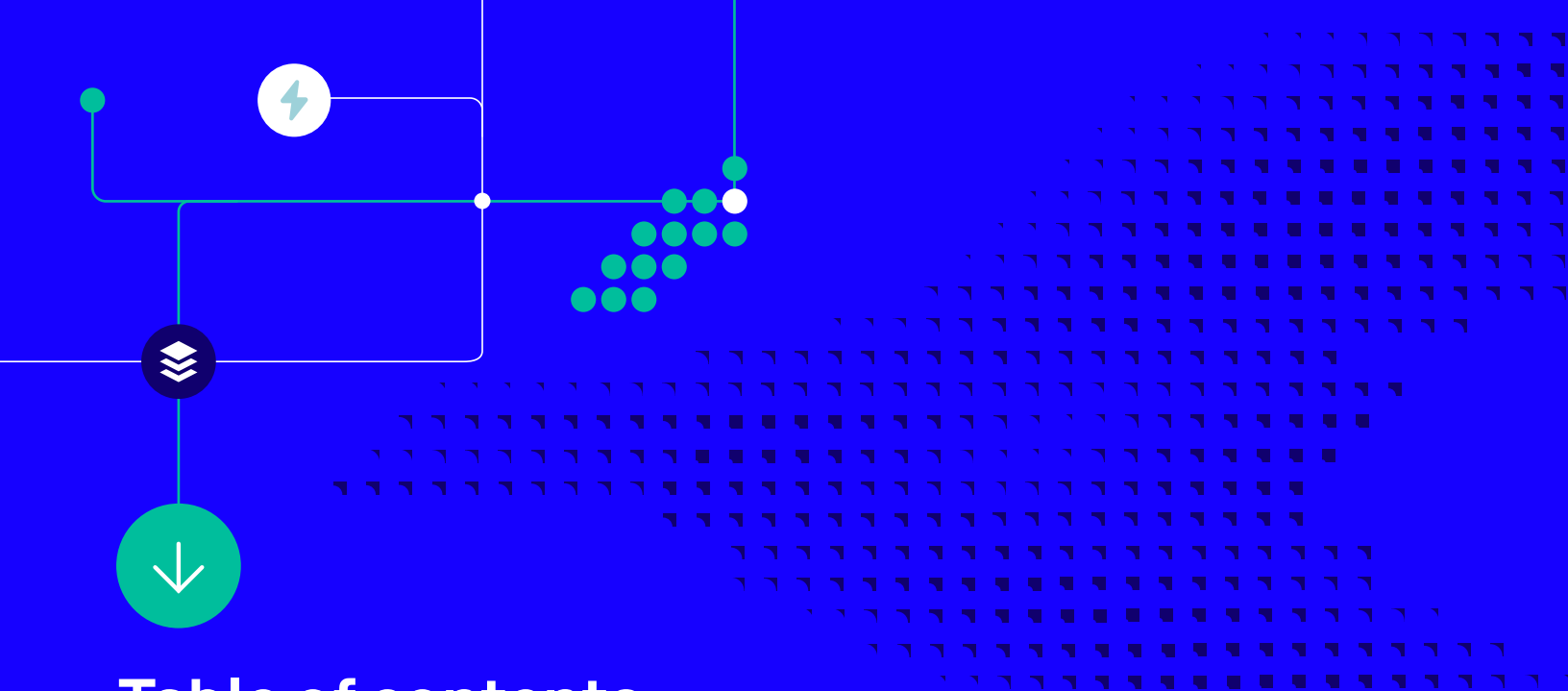


Table of contents

TREND #1

AI adoption is outpacing governance

PAGE 5

TREND #2

Organizations are leaving data value on the table

PAGE 8

TREND #3

Risk no longer lives inside a single system

PAGE 12

TREND #4

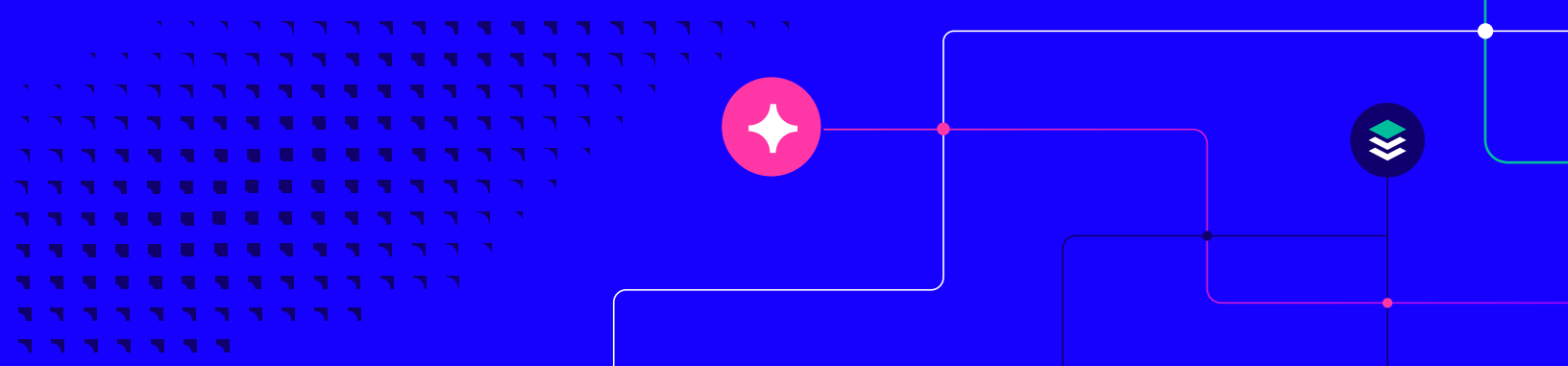
Security and compliance are becoming proactive

PAGE 15

TREND #5

Governance is becoming a strategic orchestrator

PAGE 17

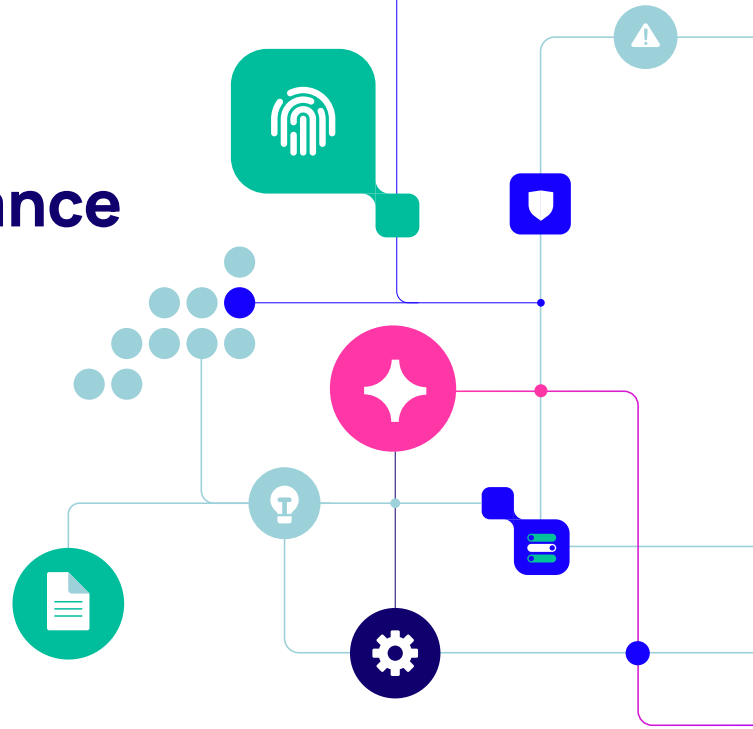




AI adoption is outpacing governance

Enterprise AI adoption has entered a new phase. What began as experimentation has become operational deployment.

According to the research, 55% of enterprises are actively deploying AI tools across their organizations. Yet only 26% report that their governance frameworks are fully aligned with the pace of implementation. Another 57% say governance is keeping pace, but gaps remain.



CURRENT APPROACH TO AI ADOPTION

Actively deploying AI tools

55%

Piloting in select areas

36%

Prioritizing governance before deployment

9%

No meaningful adoption

0%

GOVERNANCE ALIGNMENT WITH AI IMPLEMENTATION SPEED

Fully aligned

26%

Keeping pace but gaps exist

57%

Lagging behind

15%

No governance framework

0%



The result is a widening governance gap. Organizations are deploying AI faster than they can govern it.



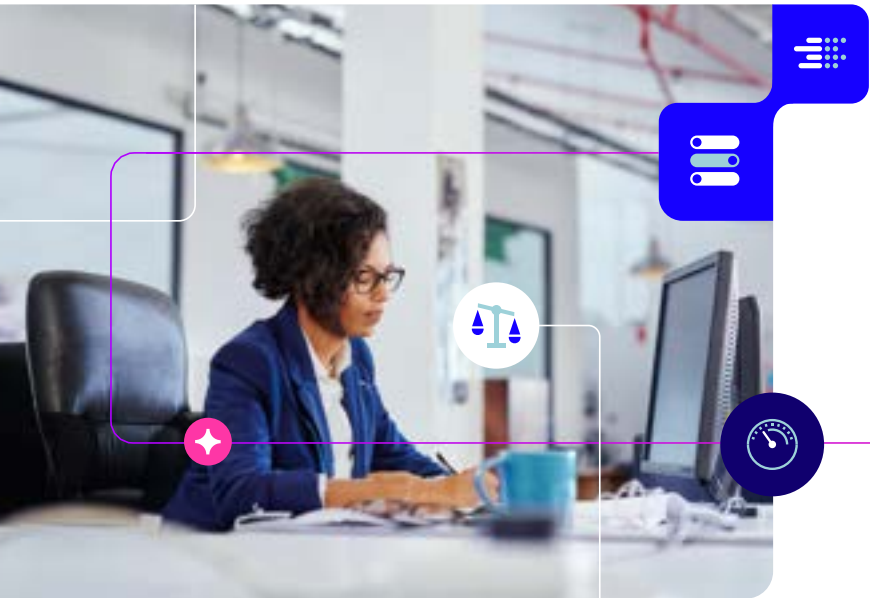
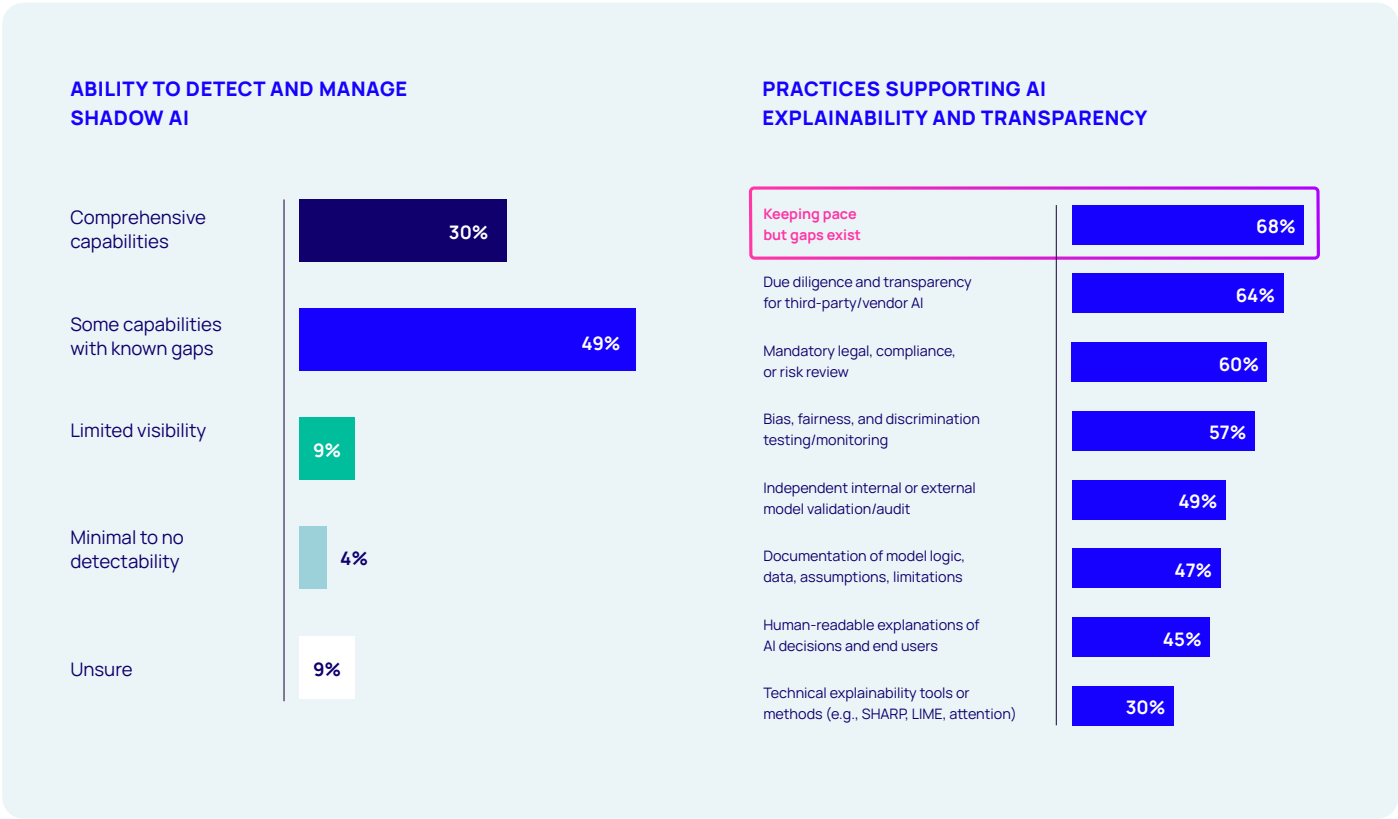
"With continuing AI adoption, individual employees will seek to upskill on their own to adapt. For some organizations, this may lead to increased risks to data privacy, data protection, and corporate governance through shadow IT apps, uneducated use, and hallucinated outcomes that result in liability implications."

JONATHAN ROBERTS
SENIOR DIRECTOR, RISK & COMPLIANCE, FTI TECHNOLOGY

Shadow AI creates new blind spots

Employees are increasingly using generative AI tools outside approved workflows, often without visibility from compliance, legal, risk, or security teams. This rise of “shadow AI”, or unapproved use of generative AI tools by employees, is a key concern.

The study found that only 30% of enterprises report comprehensive capabilities to detect and manage shadow AI. Nearly half report only partial visibility with known governance gaps. This means a significant portion of enterprise AI activity is either invisible or only partially visible to governance teams.



For regulated organizations, this challenge should feel familiar.

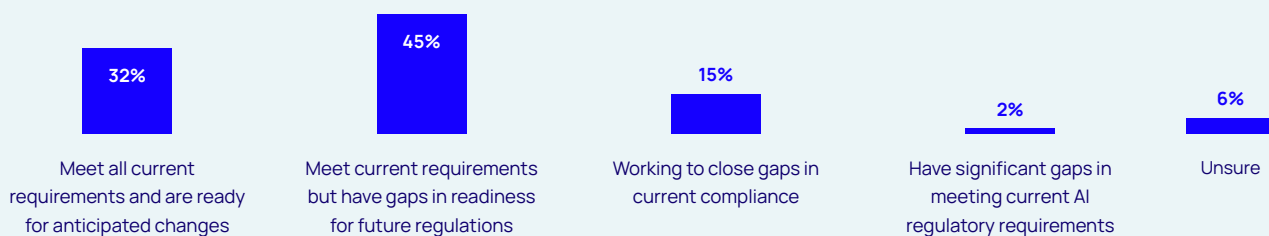
The rise of shadow AI mirrors the off-channel communications problem that resulted in billions of dollars in regulatory enforcement actions across regulated organizations. Existing compliance obligations apply the moment AI enters your workflow. You cannot defer governance and hope to remediate later. Your compliance responsibilities are immediate and unconditional.

AI communications governance raises the stakes beyond recordkeeping

Regulatory records involve more than just communication. They include all artifacts that convey value or risk to the business. Record-keeping answers two key questions: Did we preserve what happened, and how can we reconstruct what happened if we didn't preserve the record?

Beyond meeting written regulatory obligations, risk governance asks whether we understand what could go wrong, and what did we do to reduce the risk. The fact that GenAI can generate outputs that are wrong, biased, leaky, or autonomous raises the risk threshold beyond recordkeeping to issues like IP leakage, data privacy exposures, and cybersecurity threats.

PREPAREDNESS FOR AI-RELATED REGULATORY REQUIREMENTS



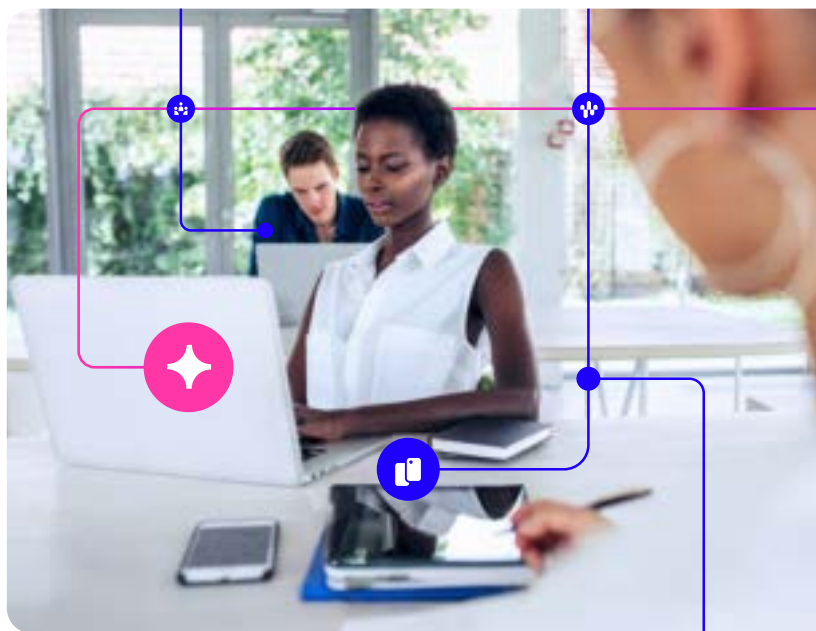
Research shows that most regulated firms' controls are still evolving, with most organizations reporting partial detection and only some enterprises having full visibility. Due diligence, employee training, and mandatory legal and compliance reviews are the most widely adopted practices today.

Regulators view AI governance as a risk issue, not just a record-keeping one, and they don't wait for governance frameworks to catch up. As soon as AI becomes part of a regulated workflow, existing obligations for record-keeping, supervision, privacy, surveillance, and risk management apply.



The implication is clear:

The next generation of enterprise governance needs to provide comprehensive visibility across both human and AI-generated communications.



"AI-based surveillance will become a standard component in communications monitoring programs, making voice and video communications easier to search and helping teams interpret emojis, slang and code words that employees might use to bypass standard risk alerts. In essence, AI will evolve into a standardized tool within communications surveillance programs."

JOHN GOFF

MANAGING DIRECTOR, INFORMATION GOVERNANCE, PRIVACY & SECURITY, FTI TECHNOLOGY

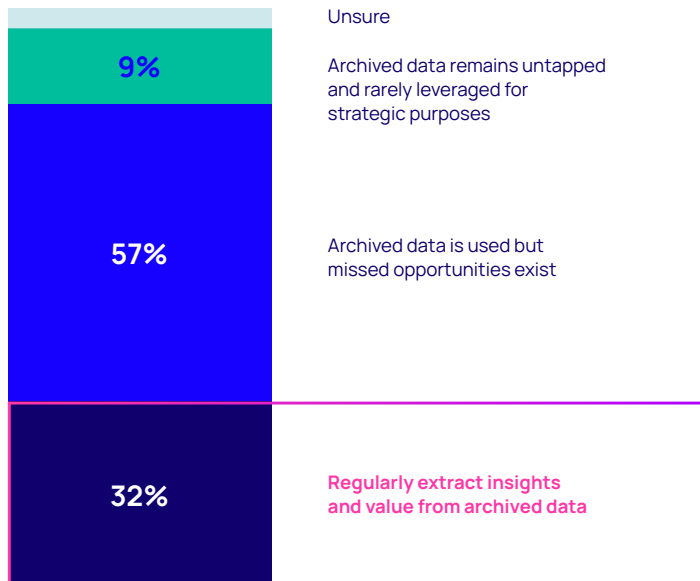


Organizations are leaving data value on the table

For years, organizations have viewed archived communications as evidence. A vault where data was stored. Necessary for regulatory requirements. Today, they are beginning to recognize it as intelligence.

FTI research reveals that only 32% of enterprises regularly extract business insights from archived communications data. Meanwhile, 57% report that they use archived data but are missing significant opportunities to derive value from it.

STRATEGIC USE OF ARCHIVED DATA



As Goutam Nadella,
Smash Chief Strategy Officer notes:

"As AI initiatives scale, organizations struggle to leverage their data due to foundational challenges around data quality, lineage, enrichment, and access controls. Trusted data from an intelligent data cloud is becoming essential not only for compliance, but for responsible AI adoption and operational resilience."

From evidence to enterprise intelligence.

The enterprises that will win in the AI era view their communications archives not as compliance overhead, but as strategic intelligence infrastructure. This requires three things: modernizing your archive, integrating with analytics platforms, and establishing governance that enables both oversight and innovation.

The FTI survey results confirm this shift and found that enterprise investment priorities include:

62%

Investing in AI and machine learning for insights

53%

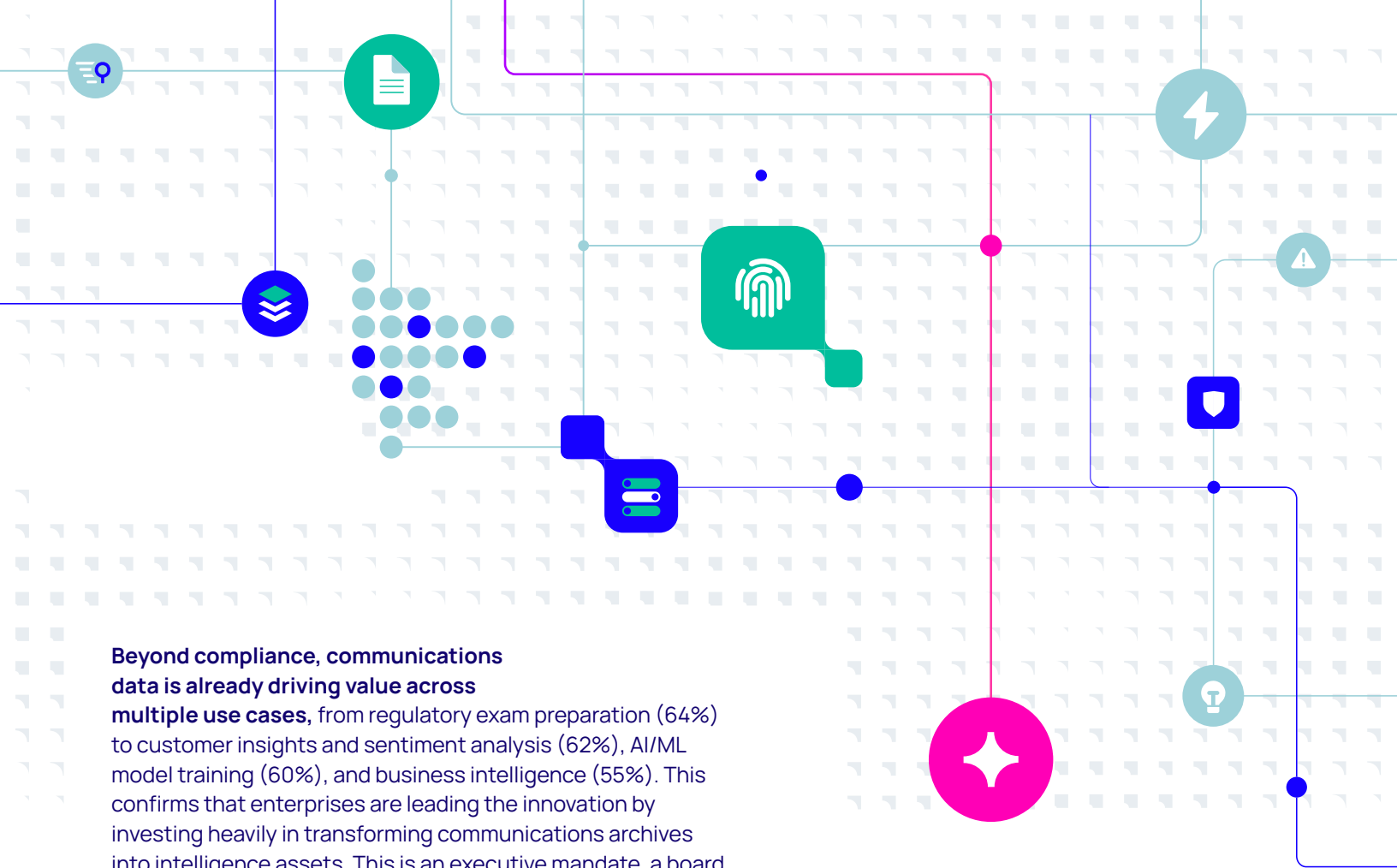
Investing in data quality and enrichment

51%

investing in archive modernization

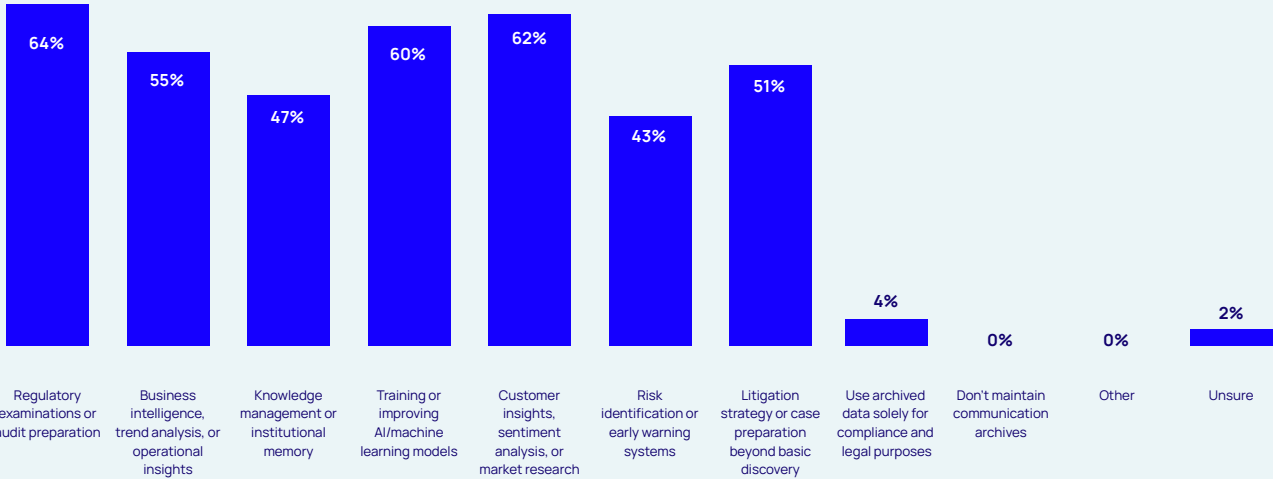
47%

Investing in unstructured data analytics

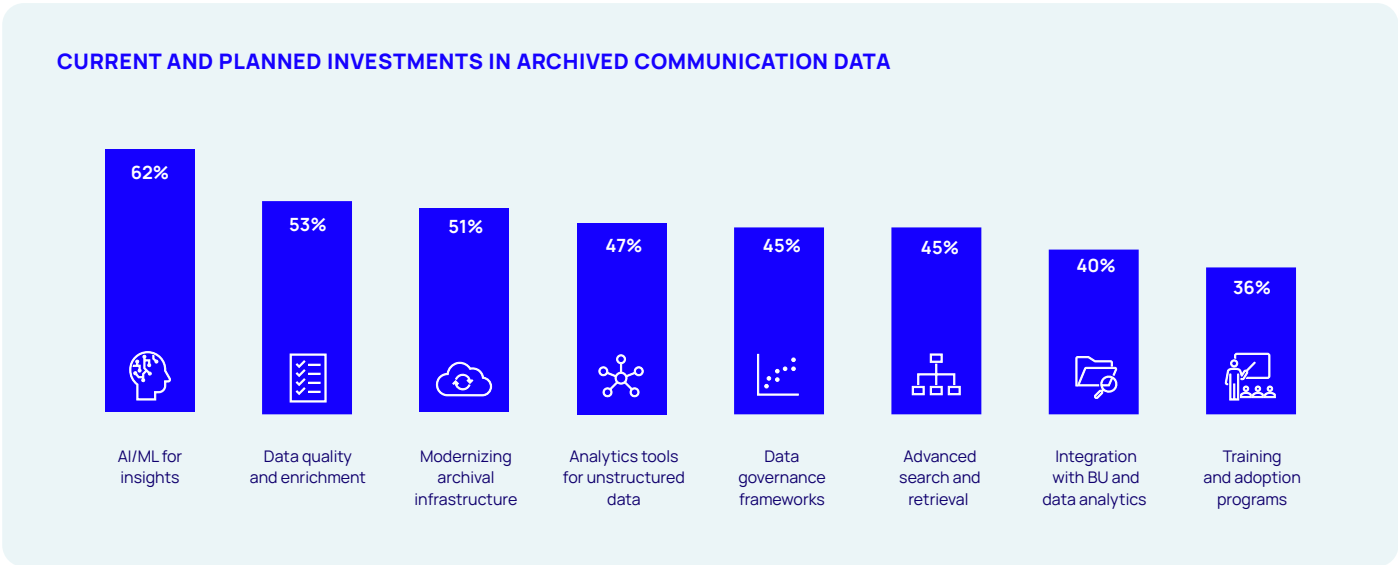


Beyond compliance, communications data is already driving value across multiple use cases, from regulatory exam preparation (64%) to customer insights and sentiment analysis (62%), AI/ML model training (60%), and business intelligence (55%). This confirms that enterprises are leading the innovation by investing heavily in transforming communications archives into intelligence assets. This is an executive mandate, a board room priority and a business imperative to get right.

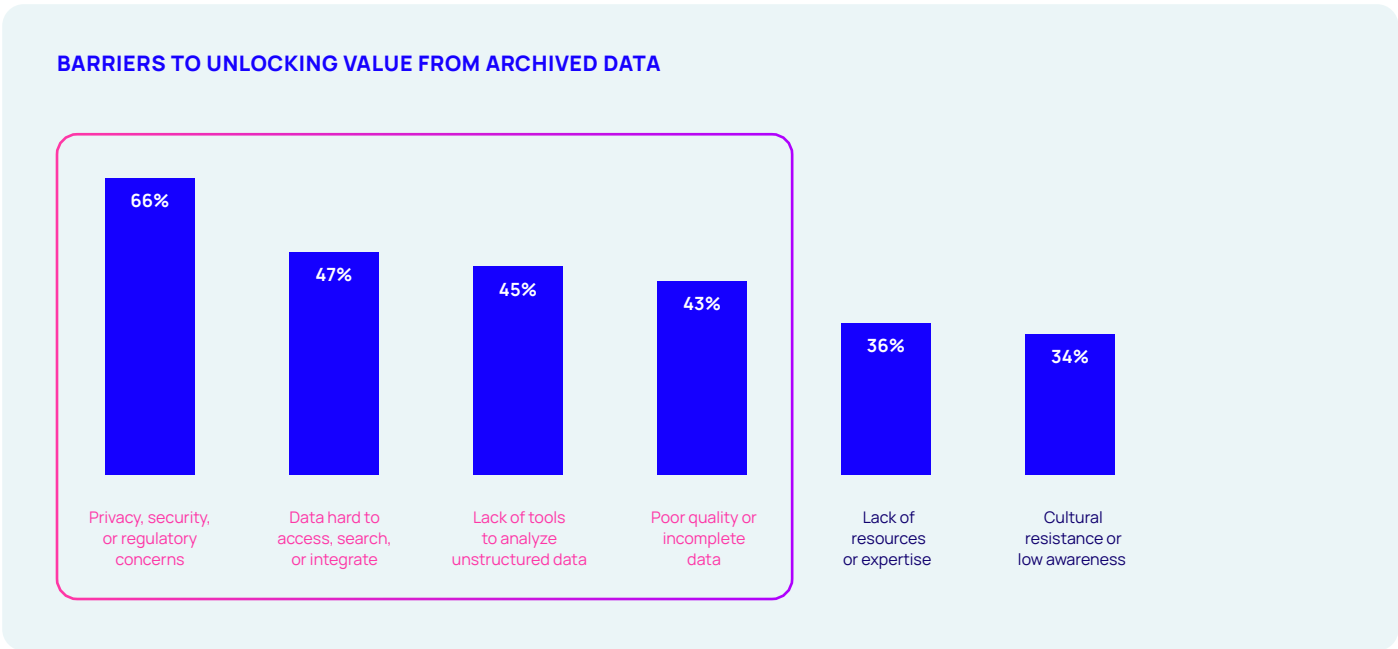
ENTERPRISE USES OF ARCHIVED COMMUNICATIONS DATA



Not surprisingly, most enterprises are leveraging communications data for rapid preparation for regulatory examinations. This will be highly beneficial for most enterprises, specifically in the time savings and reduction of manual workstreams. But perhaps more noteworthy, close second is customer insights and sentiment analysis. What's striking is that most of the use cases are exhibiting high numbers, with AI/ML training at 60% and business intelligence, trend analysis or operational insights at 55%. The implication here is that just over half have invested in modernizing their systems from competitive advantage.



What's standing in the way of value?



The barriers are well understood but solvable. It's no surprise that privacy, security, and regulatory concerns top the list (66%), followed by access and search limitations, lack of purpose-built tools, and poor data quality. Organizations with solutions specifically designed for compliance and security, like Smarsh, significantly reduce these barriers.

Competitive advantage is hiding in the archive.

The archive is no longer just where organizations store information. It is an intelligence asset. Organizations that unlock this value will gain significant competitive advantage.

The new use cases beyond compliance fall into four main categories:

1

Sentiment Analysis:

Understand what's happening with customers, markets, and employees in real-time. Extract market signals that inform strategic decisions. Gain visibility into employee culture and customer drivers.

2

Proactive Intelligence:

Move from reactive compliance to proactive risk detection. Identify anomalies in communication patterns that precede fraud, misconduct, or systemic risk before damage occurs.

3

Power Investigations:

Reduce investigation cycles from weeks to hours. Leverage AI to surface relevant evidence from unstructured communications automatically—not just email and Teams, but all channels.

4

Rapid Answers and Productivity Engines:

Automate documentation, summarization, and escalation workflows. Build custom insights, reports, and dashboards. Work smarter with intelligent access to governed communications data.



The implication is clear:

Communications data is becoming the foundation for AI initiatives, investigations, operational intelligence, and strategic decision-making. The organizations that unlock this value will separate from competitors still treating communications data solely as a compliance requirement. Communications data is now a competitive advantage.





Risk no longer lives inside a single system.

Enterprise technology environments have become increasingly interconnected. AI agents interact with applications. Applications connect through APIs. Employees collaborate across dozens of communications platforms. Data moves continuously between internal systems, cloud environments, vendors, and external partners. As a result, enterprise risk has fundamentally changed.

Risk no longer resides within individual systems. It resides in the connections between them.

APPROACHES TO TRACKING AI AND SYSTEM INTEGRATIONS

Centralized, continuously updated inventory of all connections

43%

Track individual integrations but lack enterprise-wide visibility

36%

Track major integrations, smaller connections are often missed

17%

Reactive discovery or no systematic tracking

0%

Unsure

4%

THIRD-PARTY AI AND DATA GOVERNANCE PRACTICES

Vendors must meet specific AI governance standards

49%

Assess vendors against industry standards

26%

Minimal oversight through contracts/attestations or basic due diligence

13%

Governance varies or no third-party integrations

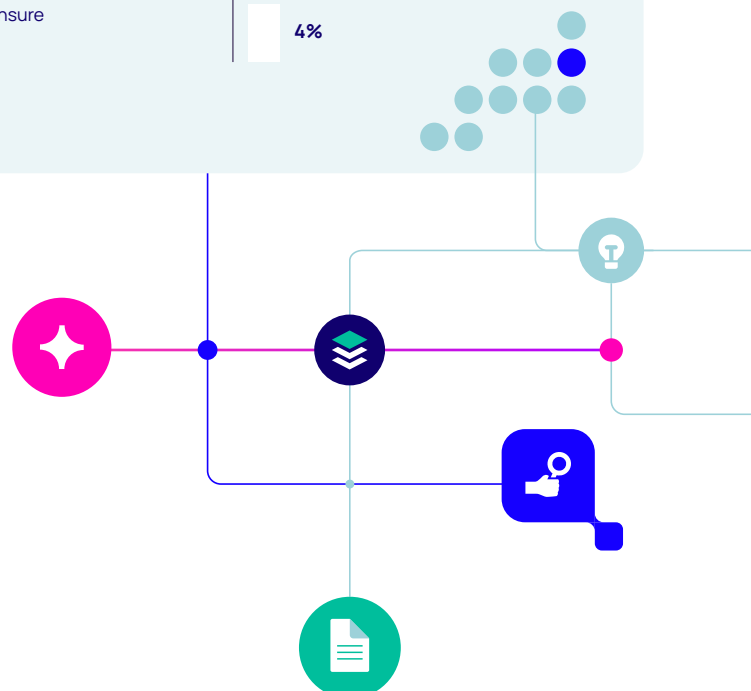
8%

Unsure

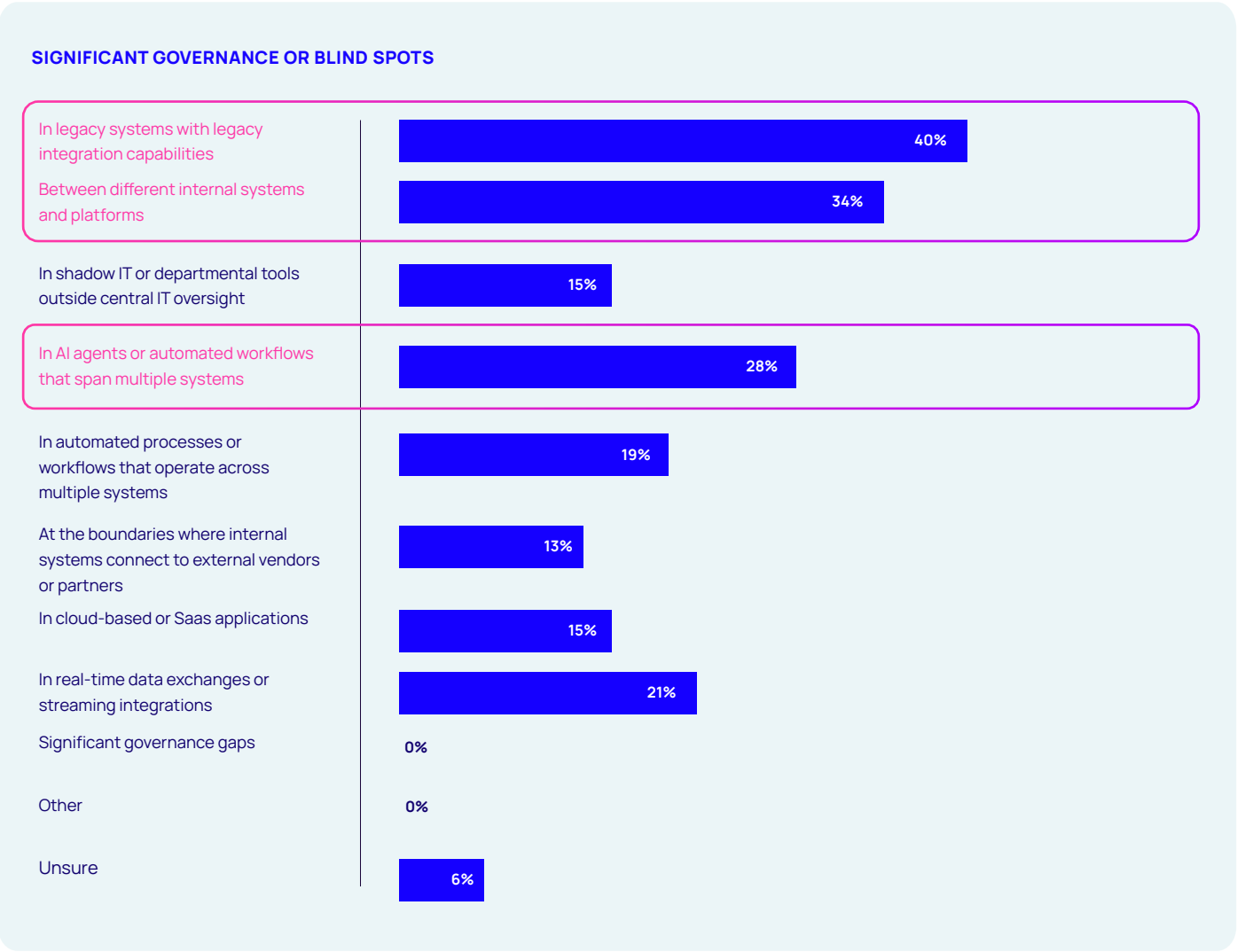
4%

The research found that only 43% of enterprises maintain a centralized, continuously updated inventory of AI agents, APIs, and third-party integrations. Meanwhile, 36% track integrations individually but lack enterprise-wide visibility.

→ This fragmentation creates dangerous blind spots.



Governance gaps



These findings reveal a critical challenge.

Most governance programs were designed for discrete applications. Today's risks emerge from interconnected ecosystems.

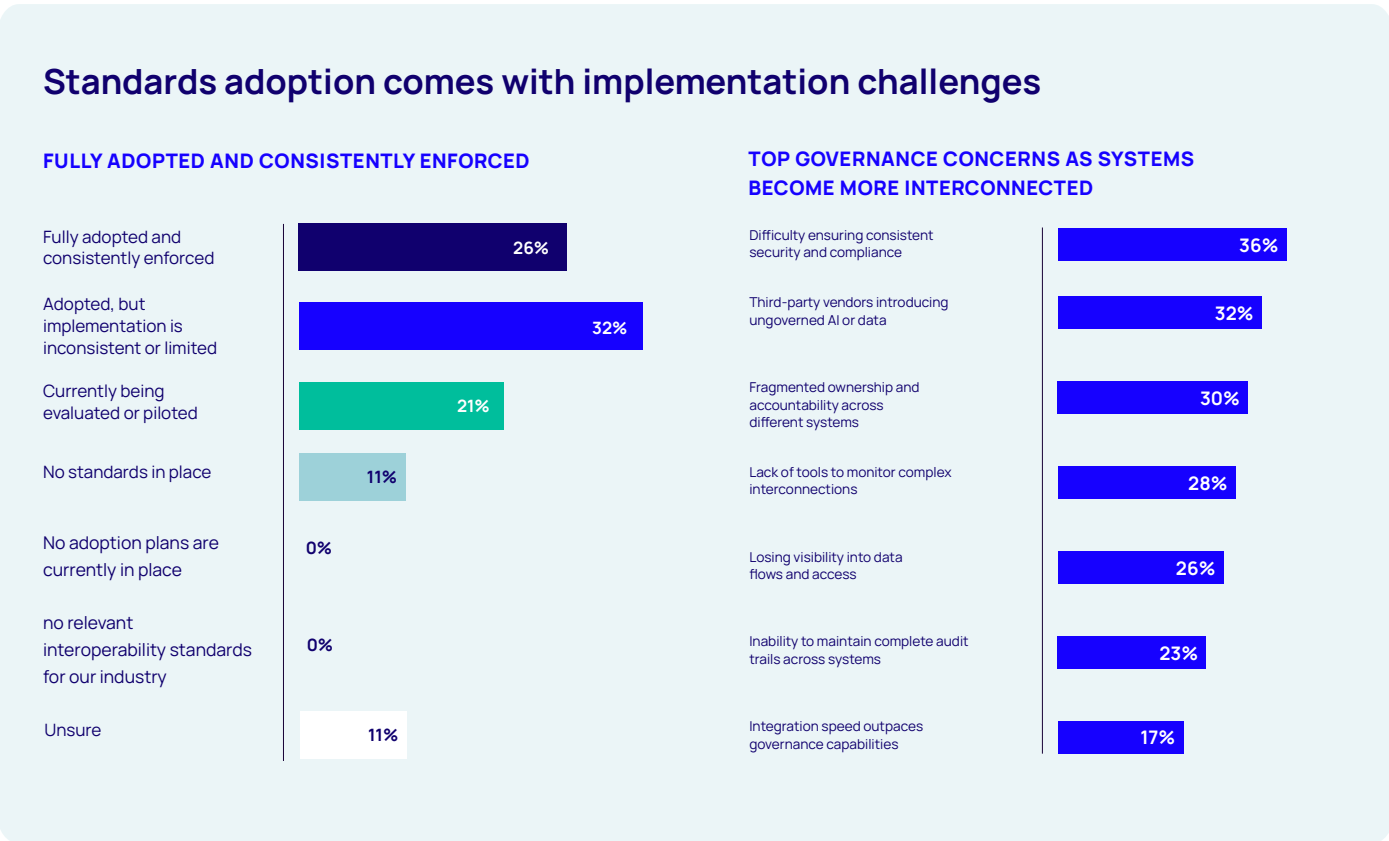
Legacy architectures and siloed systems were not built for AI-driven environments where data moves continuously across workflows, agents, platforms, and external services.

Organizations need governance models that extend beyond applications and into the relationships between systems.

Because increasingly, the risk is in the seams. The connections that integrate data across workstreams, tools, and systems.

Interoperability standards have low adoption

Not surprisingly, the adoption of interoperability standards is low. With only 26% of enterprises indicating standards are fully adopted and consistently enforced; most enterprises face inconsistent implementation or lack of clear standards. That should raise alarms.

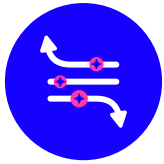


Govern data flows not just endpoints

In regulated industries, the intersection of systems, data, and workflows is both the attack surface and the governance frontier. Communications flow through multiple channels including email, chat, trading platforms, workflow engines, API connections to counterparty systems. A single message about a trade might appear as structured data in one system, unstructured text in another, and as a chat record in a third.

Your compliance function needs to see all three instances connected. Your security function needs to understand the risk implications of that connection. Your governance model needs to enforce consistent controls across all three. At the same time, global privacy and sovereignty requirements, including the EU AI Act, DORA, China GenAI Measures, Korea AI Basic Act, Brazil AI Bill, UK AI Framework, SEC/FINRA and other fragmented international regulations, are adding new layers of operational complexity.

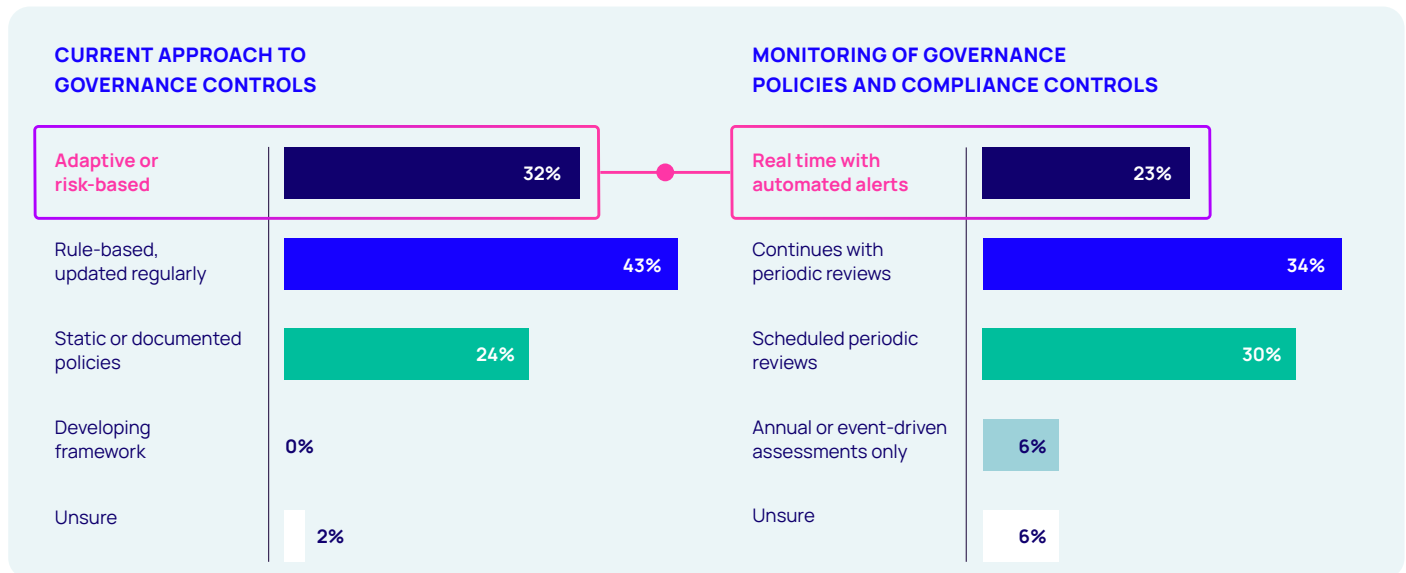
 **The implication is clear:**
Govern the data flows, connections and workflows, not just endpoints.



Security and compliance are becoming proactive.

Traditional compliance models were designed around periodic review. Or reactive response to a regulatory inquiry. But today, the modern risk environments of the Enterprise require continuous assurance.

- ✓ AI systems evolve constantly.
- ✓ Data flows change dynamically.
- ✓ Threat actors move faster than annual assessments.
- ✓ Regulatory expectations continue to expand.
- ✓ Static controls cannot keep pace.



One third of enterprise respondents report using adaptive, risk-based governance controls. However, significant challenges remain:

36%

struggle to maintain consistent security and compliance across interconnected systems

28%

express concerns about ungoverned third-party AI and data environments

30%

say expanding monitoring capabilities is a top governance priority

32%

lack consistency in how controls are applied across teams or situations

77%

lack real-time monitoring

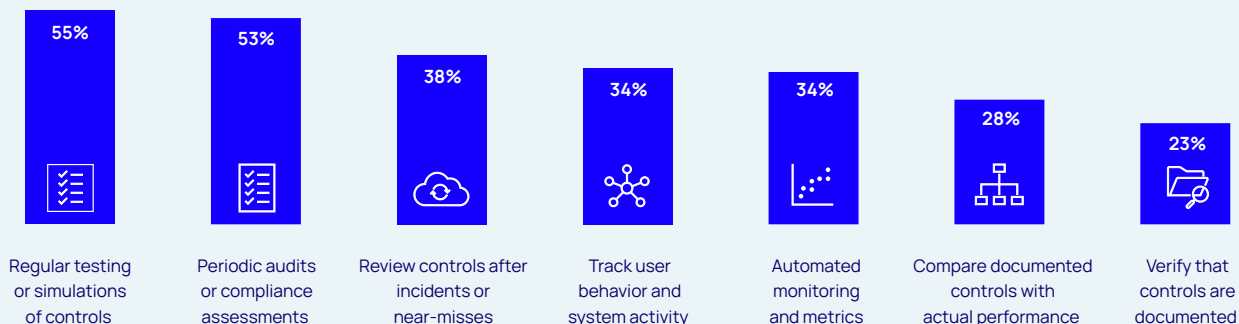
30%

only rely on scheduled periodic reviews (e.g., weekly, monthly, quarterly)

Assessing governance control effectiveness

Enterprises increasingly recognize that the best approach to resilience depends on proactive and continuous oversight. More than half conduct regular testing, simulations, and audits to validate controls. This aligns with the trend to shift from baseline compliance to governance models that can continuously identify vulnerabilities, adapt policies in real time, and maintain oversight in rapidly changing environments. But the reality of that change is not easy.

APPROACHES TO ASSESSING GOVERNANCE CONTROL EFFECTIVENESS



Alarmingly, 38% shared they only review controls after incidents or near-misses. 32% report lacking tools to monitor complex interconnections. Only 28% compare documented controls with performance and 23% verify that controls are documented.



“Now is more important than ever to shift to a proactive approach to your security and governance controls. Prioritize systems that integrate detection, testing, and controls into their foundation, automate in real-time and proactively monitor and report. As data, AI and digital communications continue to grow at exponential rates, this will only escalate and grow more complex. Now is the time to solve this.”

GOUTAM NADELLA
SMARSH CHIEF STRATEGY OFFICER

Static control model evolution

These findings point toward an important shift. Security, resilience, and defensibility are no longer compliance checkboxes. They are operational requirements. The old static control model is insufficient in today's new data environment. Organizations are moving away from reactive governance and toward adaptive assurance models capable of evolving alongside changing risks.



The bottom line:

Reactive governance cannot manage real-time enterprise risk. Security and Resilience in 2026 require continuous assurance to manage real-time enterprise risk. It will require always-on security, governance and resiliency.



Governance is becoming a strategic orchestrator

Historically, compliance functioned as a checkpoint. Its primary responsibility was enforcing policy and responding to regulatory requirements. Today, leading organizations are elevating governance into strategic business capability. AI is forcing organizations to rethink governance entirely. Information governance is no longer a back-office activity. It is becoming a strategic enabler of responsible innovation.

COMPLIANCE ROLE IN BUSINESS AND TECHNOLOGY INITIATIVES

Actively shaping and early-stage decision support

47%

Planning-stage risk review And alignment

23%

Risk oversight with limited Early involvement

11%

Policy enforcement and Issue response

17%

Unsure

2%

The research shows this progress is already well underway, with almost half sharing that compliance actively shapes early-stage business and technology decisions.

While compliance influence varies across organizations, a majority of Enterprise decision makers report that it plays a leading or active role in several key business decisions. Nearly 60% cite strategic planning and priority-setting, 62% cite vendor selection and third-party risk decisions, and more than half cite technology selection and the design of new products, services, and business processes.

COMPLIANCE FUNCTION INVOLVEMENT IN KEY ACTIVITIES

% LEADING OR ACTIVE ROLE

Vendor selection and third-party risk decisions

62%

Selection of new technologies or platforms

62%

Strategic planning and priority-setting

60%

Design of new products, services, or business processes

51%

Budget allocation for technology or innovation initiatives

40%

EXECUTIVE PERCEPTION OF THE COMPLIANCE FUNCTION

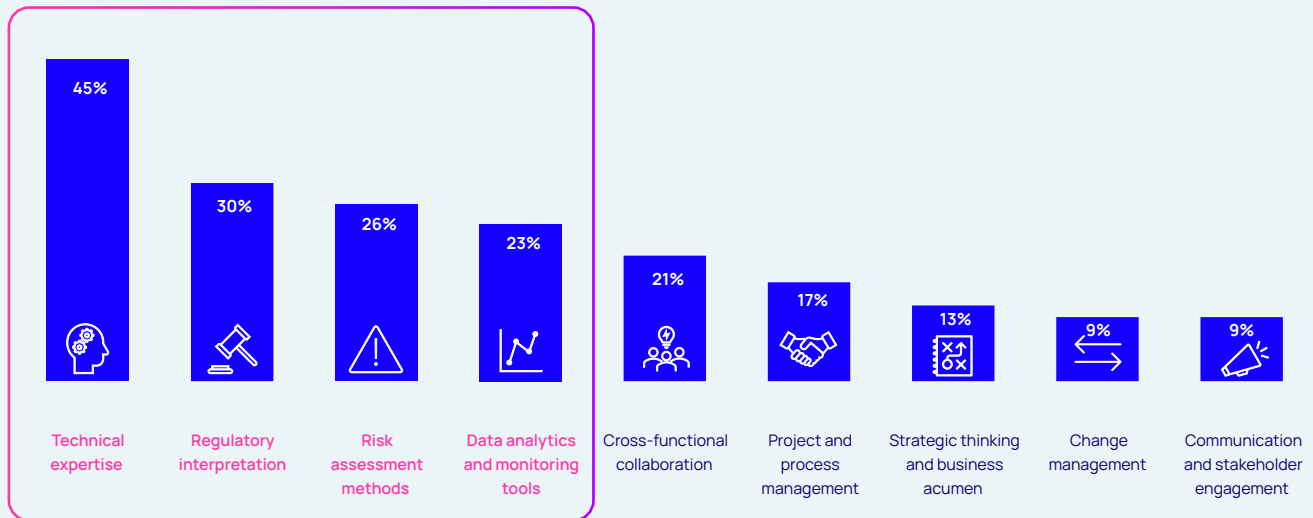


These findings point to a positive shift.

Conversely, 58% of executives still overlook the strategic value of the compliance function and only 32% value them as a strategic partner. This implies that not only are they overlooking their value but also missing the opportunity for strategic partnership, to evolve the function to be a strategic enabler of responsible innovation.

Opportunities to strengthen compliance

BIGGEST OPPORTUNITIES TO STRENGTHEN COMPLIANCE TEAMS



There is some real opportunity to elevate the role of compliance to govern emerging technologies and complex risks. Nearly half shared that technical expertise, especially data science, AI/ML and cybersecurity skills would help strengthen the compliance function, while 30% also highlighted challenges in interpreting and applying regulations to rapidly evolving technologies. AI has been a notable example of that gap.

Evolution of compliance itself

Ultimately, AI is forcing the industry to rethink governance models altogether. Information governance is no longer a back-office function; it is becoming a strategic enabler of responsible AI adoption. Organizations that can establish trusted data foundations, defensible oversight, and scalable governance frameworks will be best positioned to innovate confidently while meeting growing regulatory expectations. The most successful organizations will establish governance models that unite compliance, security, risk management, data governance, and AI oversight.



In this future, compliance becomes something much larger than regulatory oversight. It becomes the enterprise control tower.

Perhaps this is the most important shift revealed in the research is the evolving role of compliance itself.



“To keep pace with the rapid pace of technology disruption, compliance departments should have a baseline level of modernized compliance workflows and governance, risk and compliance platforms in place. These will serve as the foundation for further technological transformation. Without the basics of policies, GRC capabilities and supporting technology platforms, it will be difficult for compliance teams to approach generative AI in an effective manner.”

MELANIE STANDISH
SENIOR DIRECTOR, RISK & COMPLIANCE, FTI TECHNOLOGY

Operationalizing communications data with Smarsh

The five trends explored throughout this research are clear. AI is creating both a new category of communications risk and a new opportunity to unlock enterprise intelligence. Organizations need a trusted platform capable of capturing, governing, protecting, and activating communications data at enterprise scale. Addressing these challenges requires a foundation built for the AI era.

The Smarsh Communications Intelligence Platform helps organizations operationalize communications data throughout its lifecycle. By unifying capture, preservation, governance, supervision, and analytics together into a single intelligent environment.

Built for the AI-era, the platform provides a trusted foundation for compliance, surveillance, investigations, discovery, AI initiatives, and operational intelligence. As communications data becomes the engine behind governance, resilience and innovation, organizations that can govern and activate it effectively will be best positioned to compete, adapt, and lead in the years ahead.



Capture every conversation

Smarsh captures communications across email, Microsoft Teams, Slack, Zoom, mobile messaging, social channels, voice communications, and emerging AI interactions. Organizations gain a complete and defensible record of communications activity while preserving context, fidelity, and regulatory requirements.



Build a trusted communications archive

The Smarsh archive centralizes communications data in a hyperscalable cloud environment designed for regulated enterprises. The platform creates a trusted source of truth that supports compliance, investigations, supervision, retention management, and AI-ready data strategies.



Detect risk earlier with AI-driven surveillance

Smarsh combines domain-specific AI with advanced surveillance capabilities to identify misconduct, policy violations, market abuse concerns, and emerging risks. Agentic AI workflows reduce false positives, prioritize meaningful alerts, and help compliance teams focus on what matters most.



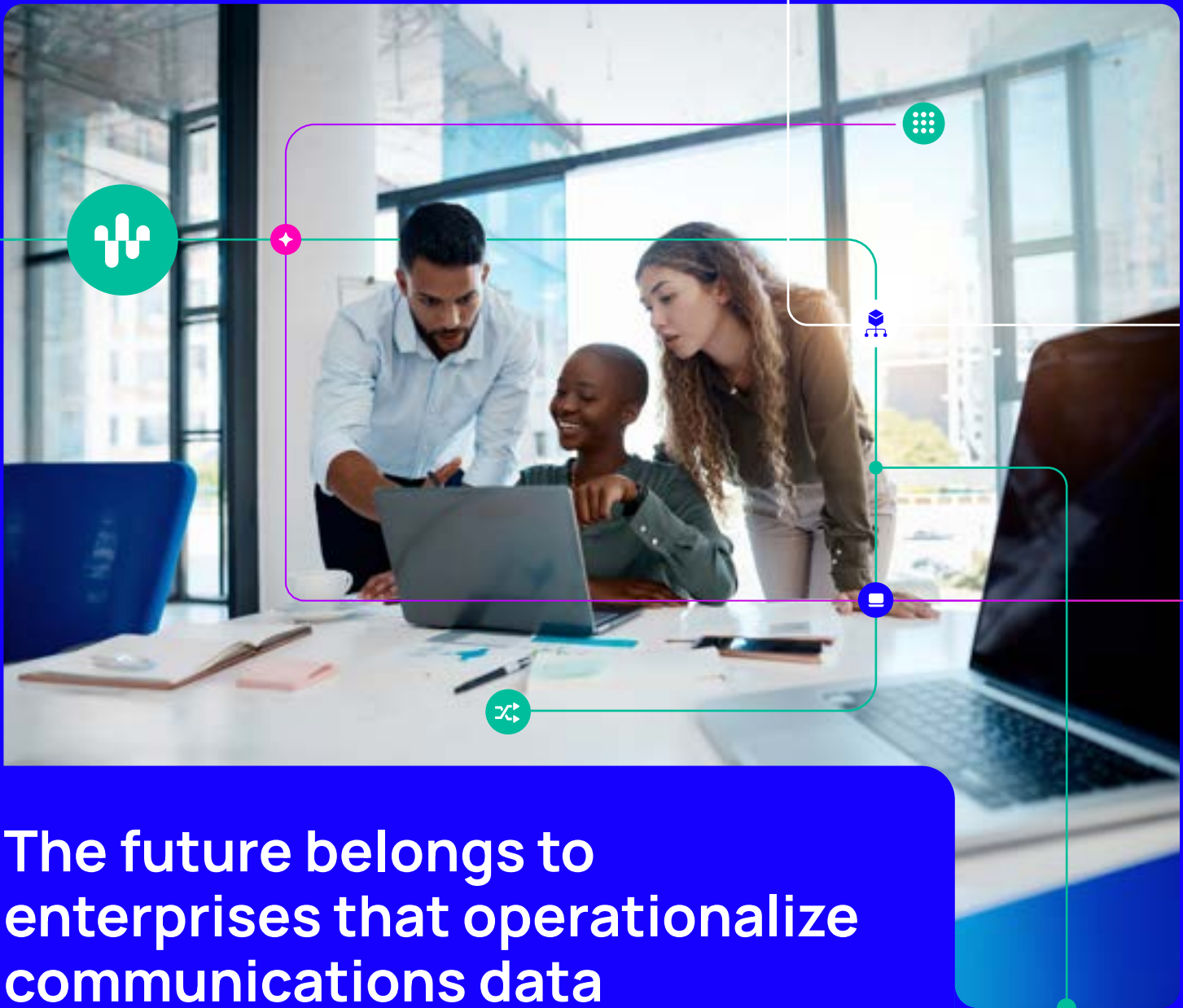
Accelerate discovery and investigations

Smarsh Discovery streamlines legal and regulatory response through intelligent search, contextual review, automated prioritization, and defensible workflows. Organizations can reduce review costs while accelerating access to critical evidence.



Unlock voice intelligence

Voice remains one of the richest sources of customer and operational insight. Smarsh Voice Intelligence captures, preserves, and analyzes conversations across calling, conferencing, and contact center platforms, helping organizations understand risk, customer sentiment, and business outcomes.



The future belongs to enterprises that operationalize communications data

The next generation of enterprise advantage will not be built solely on AI. It will be built on trusted data.

Organizations that can govern communications data, protect it, and activate it responsibly will unlock new levels of intelligence, resilience, and innovation.

The future belongs to enterprises that operationalize communications data.

Smarsh helps make that future possible.

Govern every conversation. Understand every risk.
Activate communications data for enterprise intelligence.

Smarsh Communications Intelligence Platform.

