Kiteworks

REPORT

Kiteworks Data Security and Compliance Risk 2025 MFT Survey Report

www.kiteworks.com

Table of Contents

Executive Summary

Despite claiming mature security programs, organizations are failing at managed file transfer (MFT) protection. The data is stark: 59% suffered MFT security incidents in the past year while basic vulnerabilities remain unaddressed. Government agencies encrypt only 8% of their stored data. Healthcare—handling our most sensitive information—protects just 11%. Even well-resourced mid-market companies show the highest breach rates at 32%.

This failure stems from a critical misalignment in risk priorities. Organizations consistently choose moderate security stances—ranking foundational controls like patching as merely “very important” rather than “extremely critical.” This measured approach proves insufficient against actual threat landscapes.

This isn’t about sophisticated zero-day attacks or nation-state actors. Our inaugural Data Security and Compliance Risk: MFT Survey Report reveals that most incidents exploit fundamental gaps: unencrypted data sitting in storage, security tools that can’t see file transfers, and fragmented systems that create blind spots. Emerging threats compound these vulnerabilities: 26% have already experienced AI-related data incidents while 30% permit uncontrolled AI tool usage with sensitive files.

Three Gaps That Matter Most

The survey identifies three critical failures that separate the 59% experiencing incidents from the 39% who remain secure:

Encryption Gap: Organizations obsess over encrypting data in motion (76% have end-to-end encryption) while ignoring data at rest. Only 42% protect stored data with AES-256, leaving the majority vulnerable where attackers strike—in file storage, backups, and temporary directories.

Visibility Gap: 63% of organizations haven't connected their MFT systems to security monitoring. Their SOC teams watch network traffic and endpoint activity while file transfers—often containing the most sensitive data—operate in darkness.

Complexity Gap: 62% maintain separate systems for email security, file sharing, and web forms. This fragmentation doesn't just waste resources; it creates the inconsistencies and blind spots that attackers exploit.

59% experienced incidents in the past year

62% operate MFT in a silo

58% do not use AES-256 for MFT data at rest

63% do not have SIEM/SOC integration with their MFT

26% do not test their MFT incident response plans

28% do not thoroughly vet vendors

33% have not adopted ABAC

42% do not conduct quarterly security reviews

73% do not use CDR

87% have <90% of MFT jobs automated (only 13% reach 90% to 100%)

Figure 1: 10 Stats That Matter.

Progress Without Impact

Organizations are busy but not effective. The survey shows genuine effort in several areas:

Access Evolution: 67% have implemented attribute-based access control, and 58% conduct quarterly reviews

Vendor Scrutiny: 72% thoroughly evaluate vendor security—yet incidents persist

Emerging Awareness: 48% have begun addressing AI-related risks, yet 26% have already experienced AI-related incidents while 30% permit uncontrolled AI usage with sensitive files

But activity doesn't equal security. The disconnect between effort and outcomes points to a fundamental problem: Organizations are adding advanced capabilities while leaving foundational vulnerabilities exposed.

This disconnect stems from organizations' preference for moderate risk stances—ranking critical controls like patching as merely "very important" (3.71 priority score) rather than "extremely critical" (3.05). This measured approach fails to match actual threat severity.

Industry Highlights

Industry highlights reveal the real-world impact:

Healthcare: Achieves 100% end-to-end encryption—an admirable accomplishment—yet protects only 11% of data at rest. Result: 44% incident rate with the highest breach percentage at 11%.

Government: Strong policy frameworks meet weak implementation. Despite federal mandates, only 8% encrypt stored data. Half of respondents reported MFT security incidents in the past year.

Financial Services: The exception that proves the rule. Balanced implementation across all controls yields a 25% incident rate—still concerning but half the average.

Education: Broad security gaps drive a 57% incident rate. While reporting no breaches in the survey, high rates of unauthorized access (29%) and availability issues (29%) suggest detection gaps rather than strong prevention.

Why Size Doesn't Equal MFT Security

Conventional wisdom suggests larger organizations have better security. The data disagrees:

Mid-market companies (5,000–10,000 employees):

Highest breach rate at 32% despite 75% testing incident response

Largest enterprises (>20,000 employees):

Achieve only 10% breach rate but through maturity, not just resources

Small organizations (<5,000 employees):

Resource constraints force focus, sometimes achieving better outcomes than mid-market peers

The Lesson:

MFT security isn't about size or spending—it's about addressing the right vulnerabilities.

Your Starting Point

The path from the vulnerable 59% to the secure 39% doesn't require perfection. It requires closing three specific gaps:

1. **Encrypt Your Stored MFT Data:** If you're among the 58% without AES-256 at rest, this is your highest-risk exposure. Every day of delay is another day attackers could access years of accumulated files.
2. **Connect Your Security Tools:** If you're in the 63% without SIEM integration for MFT, your security team is partially blind. Modern MFT platforms can connect in hours, not months.
3. **Simplify Your Data Exchange Architecture:** If you're part of the 62% with fragmented systems, each additional platform multiplies your risk. Unification isn't just about efficiency—it's about survival.

Section 1: Critical Security Gaps That Demand Immediate Action

The survey identifies three critical security gaps affecting most organizations: insufficient encryption at rest, lack of security monitoring integration, and the disconnect between incident response planning and outcomes.

1.1 Encryption Gap That Leaves Data Exposed

The survey reveals a significant gap in encryption practices:

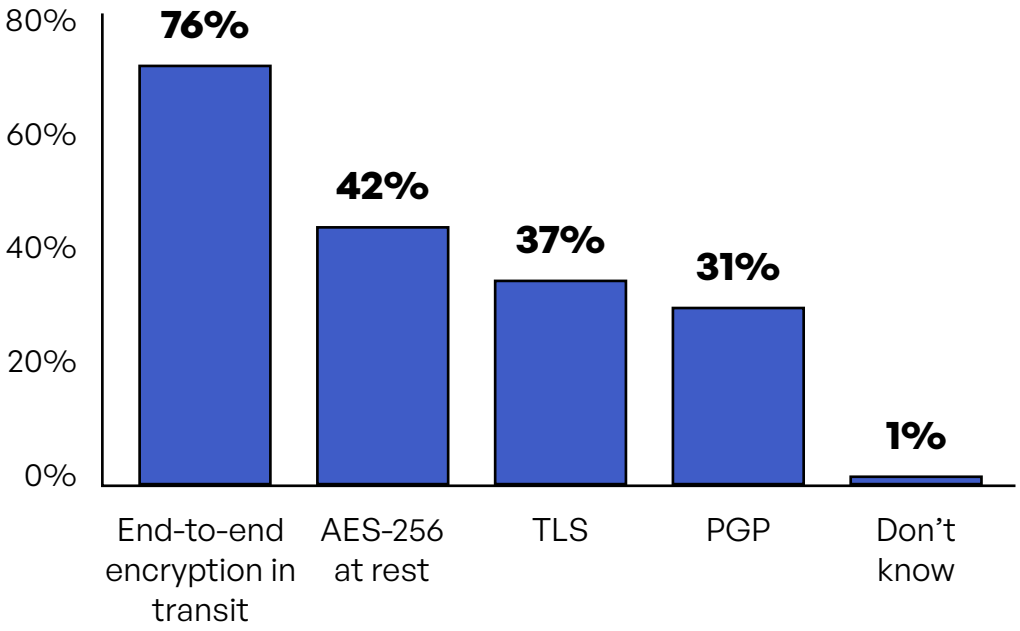


Figure 2: MFT Encryption Methods in Use.

While 76% of organizations implement end-to-end encryption for data in transit, only 42% use AES-256 for data at rest. This 34 percentage point gap means the majority leave data vulnerable when stored.

Industry-specific findings reveal concerning patterns:

Industry	End-to-End Encryption in Transit	AES-256 at Rest
Government	75%	8%
Healthcare	100%	11%
Financial Services	75%	27%
Education	71%	29%
Manufacturing	67%	44%
Technology	60%	46%

Figure 3: Encryption Methods by Industry.

The data makes it clear that while most organizations are confident securing files in transit, they are far less consistent about protecting data at rest. The resulting encryption gap—often 30 points or more—represents a blind spot that adversaries can exploit, particularly in sectors like Government and Healthcare where exposure risks are highest. Closing this gap requires prioritizing AES-256 at rest alongside existing transit protections, ensuring end-to-end coverage across the full file life cycle.

1.2 Integration Blind Spot Creating Security Silos

Security integration remains a major gap:

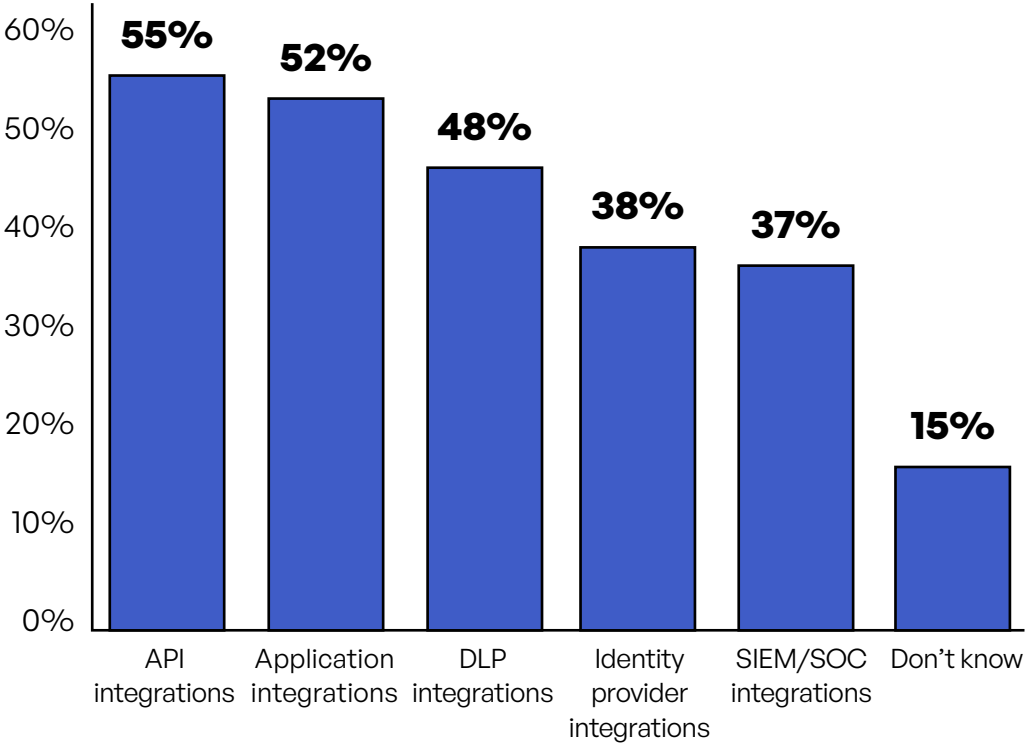


Figure 4: Integration Capabilities.

Only 37% of organizations have integrated MFT with SIEM/SOC platforms. This means 63% cannot correlate MFT events with broader security monitoring, creating a significant blind spot.

Integration Type	Have It	Don't Have It	Impact of Gap
SIEM/SOC	37%	63%	Cannot detect correlated attacks
Identity Provider	38%	62%	Inconsistent access control
DLP	48%	52%	Data loss prevention gaps
Applications	52%	48%	Manual processes required
APIs	55%	45%	Limited automation capability

Figure 5: Integration Gaps by Capability.

The survey highlights a critical integration gap: Most organizations have some level of API or application integration, yet fewer than four in ten connect MFT into their SIEM or identity provider. This leaves file transfer events siloed from broader security visibility and undermines unified access enforcement. The result is a patchwork approach—automation works in pockets, but blind spots persist where MFT data flows fall outside central monitoring. Closing these gaps is essential to prevent attackers from exploiting unmanaged channels.

1.3 Testing-Reality Disconnect

The survey reveals a troubling gap between incident response planning and actual outcomes:

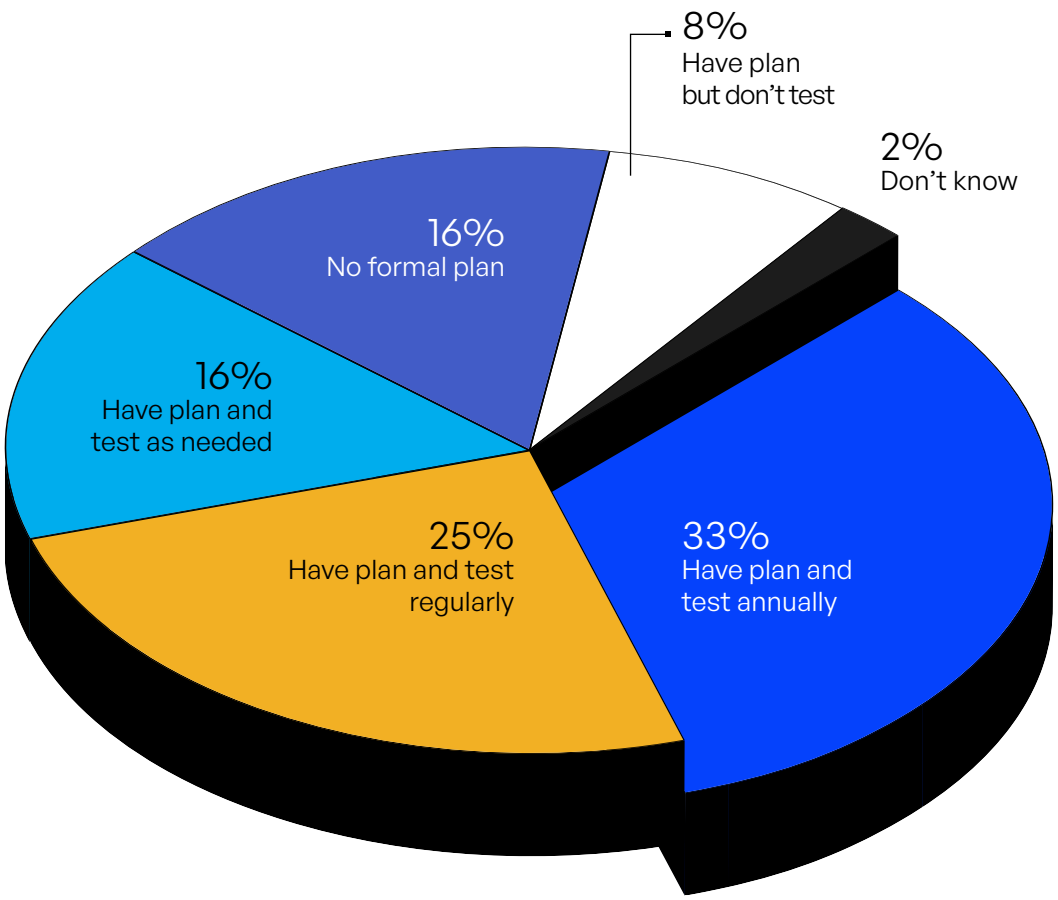


Figure 6: Incident Response Plan Status.

The incident response data exposes security theater at its worst. While 82% claim to have IR plans and 74% say they test them, only 25% test regularly—the minimum frequency for maintaining readiness. The remaining organizations either test annually (33%), which becomes outdated within months, or "as needed" (16%), which typically means after an incident occurs. This explains the paradox of high testing rates coexisting with a 59% incident rate.

The most dangerous group may be those testing annually or sporadically. They believe they're prepared, creating false confidence that prevents recognition of vulnerabilities. This illusion of preparedness likely explains why mid-market companies show the highest testing rates (75%) yet suffer the most breaches (32%). Real IR readiness requires regular testing with MFT-specific scenarios, prompt remediation of findings, and measuring actual recovery capability—not just process completion. The 39% avoiding incidents understand this difference between checking boxes and achieving resilience.

Despite high testing rates, incident rates remain significant:

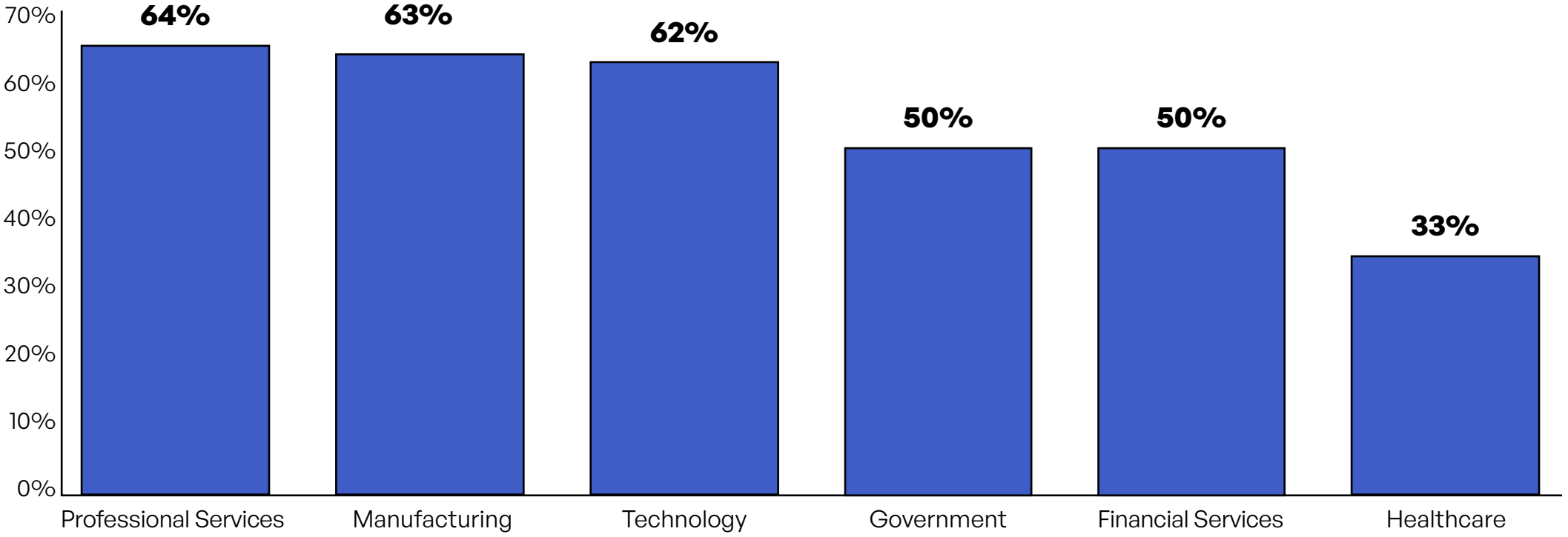


Figure 7: Incidents Experienced by Industry.

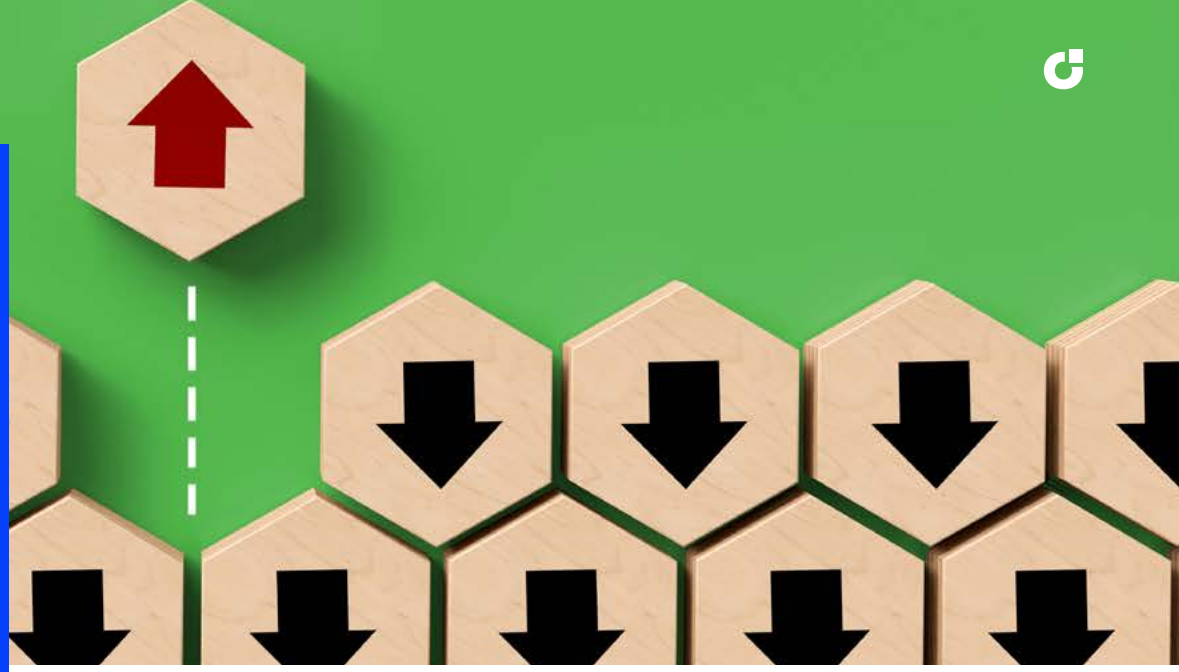
The data shows that even organizations with regular testing experience breaches:

Organization Size	Test Regularly	Breach Rate
1,000–1,500 Employees	67%	16%
5,000–10,000 Employees	75%	32% (highest)
10,000–20,000 Employees	72%	19%
Over 20,000 Employees	80%	10% (lowest)

Figure 8: IR Testing vs. Breach Rate by Organization Size.

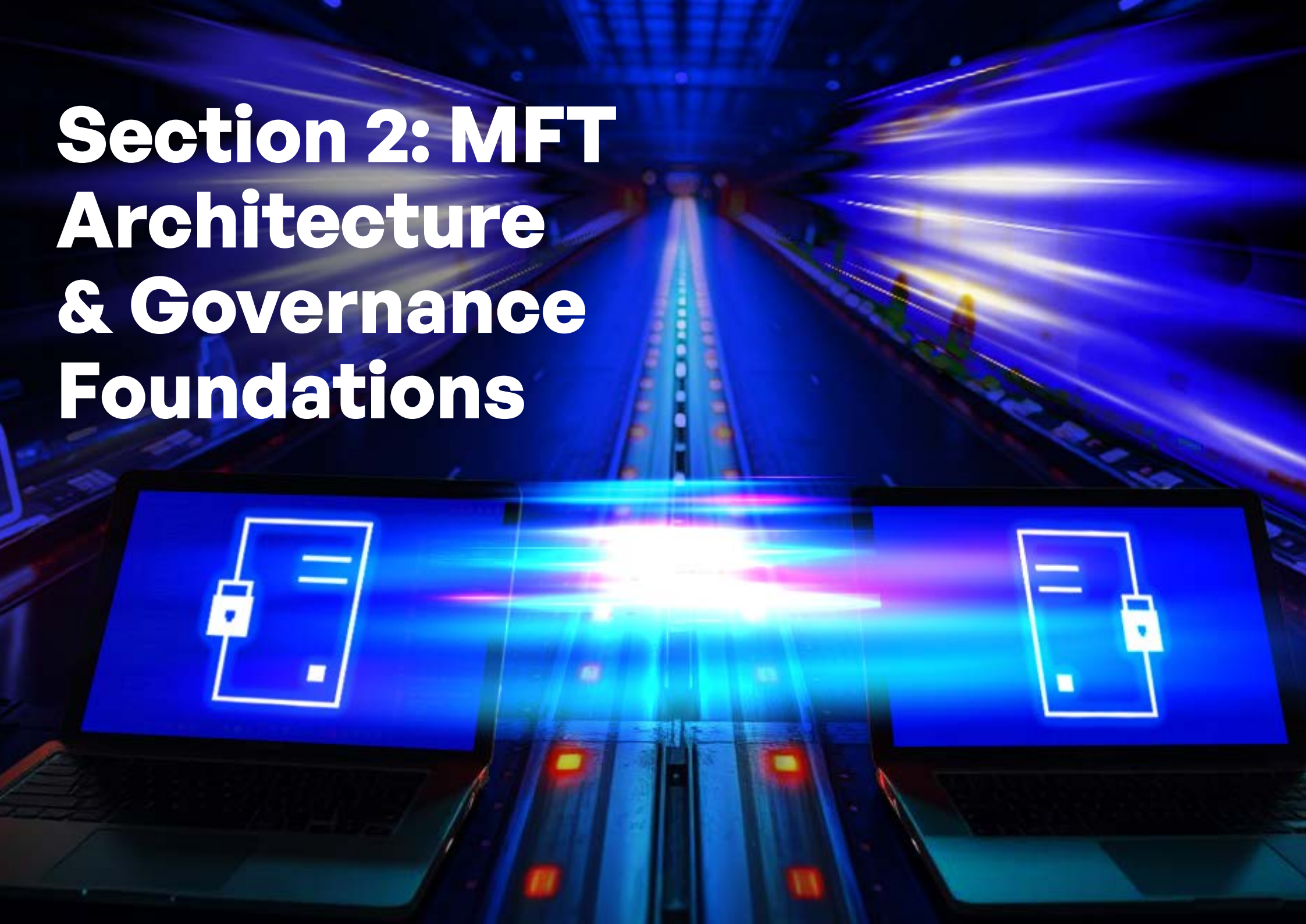
Incident Response Testing

Largest organizations achieve the lowest breach rate (10%)—with incident testing playing an important role.



The data reveals a troubling disconnect between incident response preparation and real-world outcomes that challenges conventional security wisdom. While organizations across all sectors invest heavily in IR testing—with rates ranging from 67%–80%—actual incident rates tell a starkly different story. **Government** (50%) leads in incident rates, suggesting that current testing methodologies fail to address the actual threats these organizations face. Even more concerning, the correlation between testing frequency and breach prevention appears almost inverse for mid-sized organizations, where 75% test regularly yet suffer the highest breach rate at 32%—double the rate of smaller organizations that test less frequently.

This paradox points to a fundamental flaw in how organizations approach incident response: They're testing for compliance rather than resilience. The **largest organizations** (>20,000 employees) achieve the lowest breach rate at 10%, not simply because 80% test regularly but because their testing likely incorporates real-world scenarios, cross-functional coordination, and meaningful metrics beyond checkbox completion. The message is clear—incident response testing without addressing underlying vulnerabilities like encryption gaps, fragmented systems, and lack of security tool integration merely creates false confidence. Organizations must shift from performative testing to comprehensive security programs that close fundamental gaps while building genuine response capabilities, recognizing that even the best incident response plan cannot compensate for absent preventive controls.



Section 2: MFT Architecture & Governance Foundations

Architecture and governance decisions create the foundation for MFT security. The survey reveals how fragmentation, access control maturity, and automation levels impact security outcomes.

2.1 Hidden Cost of Fragmentation

The majority (62%) operate fragmented data exchange systems across MFT, email, file sharing, and web forms. This fragmentation creates multiple challenges:

Inconsistent security policies across systems

Multiple points of vulnerability

Complex audit and compliance processes

Difficult incident investigation across systems

Aspect	Unified (38%)	Fragmented (62%)
Architecture	Single platform	Multiple systems
Policy Management	Consistent	Varies by system
Audit Trail	Consolidated	Scattered
User Experience	Single interface	Multiple logins
Integration Points	Fewer required	Multiple needed

Figure 9: Platform Fragmentation Impact.

2.2 Access Control Evolution

Access decisions increasingly rely on richer logic: **ABAC (67%)** leads, followed by **RBAC (45%)**, **context-aware (45%)**, and **least-privilege (37%)**. ABAC's momentum reflects the need to evaluate user, resource, and environmental attributes in regulated and high-variance workflows. Industries differ in emphasis, but the direction is consistent: broader context, finer granularity.

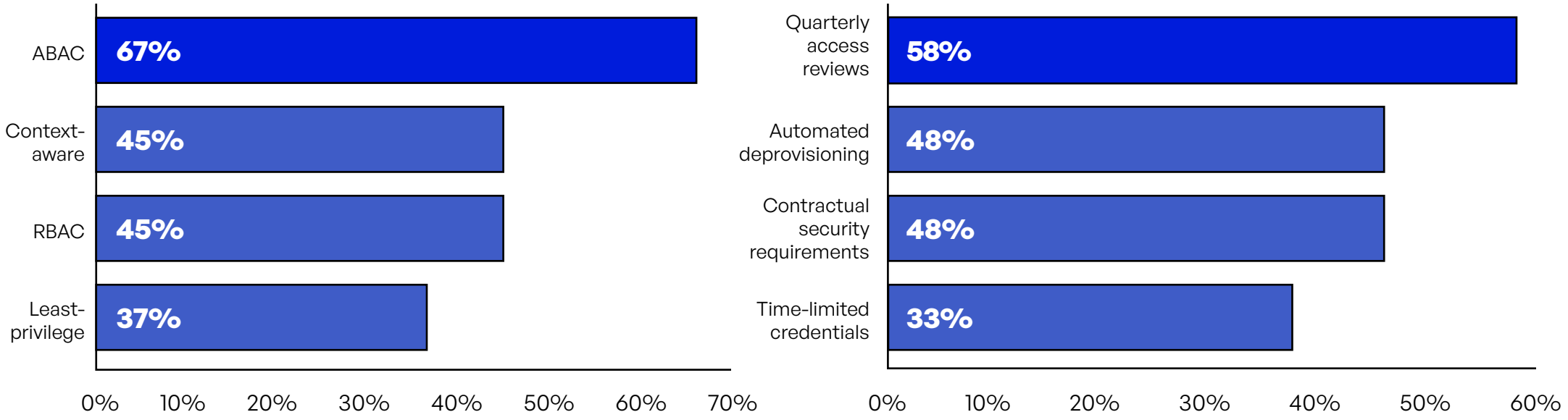


Figure 10: Access Control Models.

The numbers reveal a troubling pattern: Organizations invest in sophisticated access models while neglecting foundational practices. While **67% have adopted ABAC**—a significant shift from traditional role-based controls—this means **33% still lack attribute-based capabilities entirely.** More concerning, only **37% enforce least-privilege access**, leaving nearly two-thirds (63%) with excessive permissions that attackers exploit.

Governance practices show similar gaps. Although **58% conduct quarterly access reviews**, the remaining **42% allow stale permissions to accumulate indefinitely**—a direct path to insider threats that account for 27% of incidents. The automation picture is equally mixed: **48% automate deprovisioning**, but half still rely on error-prone manual processes. Most critically, only **33% use time-limited credentials**, meaning two-thirds of organizations let access persist without expiration—a practice that turns every departed employee into a potential vulnerability.

2.3 Governance Practices by Industry

Decision logic is only effective if access is right sized over time. 58% perform quarterly access reviews, 48% automate deprovisioning, 48% enforce contractual security requirements, and 33% use time-limited credentials. Gaps here correlate with higher incident exposure due to stale privileges and lingering accounts.

Industry	ABAC	Quarterly Reviews	Automated Deprovisioning	Time-Limited Credentials	Key Insights
Financial Services	65%	60%	52%	45%	Balanced adoption across controls supports the lowest incident rate (25%).
Government	62%	55%	47%	40%	Moderate governance overall but paired with weakest AES-256 encryption (8%).
Healthcare	61%	56%	44%	30%	Strong transit encryption (100%), but only 11% AES-256 at rest creates risk.
Manufacturing	59%	50%	41%	28%	Lags in automation and maturity; governance practices inconsistent.
Technology	63%	57%	49%	36%	Fair adoption, but fragmentation undermines governance effectiveness.
Professional Services	55%	52%	39%	27%	Governance inconsistent, with resource constraints limiting adoption.
Legal	53%	49%	33%	22%	Trailing adoption rates across all controls; slow governance maturity.
Life Sciences	60%	54%	42%	31%	Reasonable ABAC uptake but weak on automated offboarding and reviews.

Figure 11: Industry Access Control Maturity.

The correlation is clear: Organizations with mature governance practices experience fewer incidents. Financial Services' balanced approach yields the lowest incident rate at 25%, less than half the 59% average. The 39% avoiding incidents don't just implement ABAC or conduct reviews—they do both, creating defense in-depth that works.

2.4 Automated File Transfer Imperative

Automation Band	Insights
<30% automated	Heavy reliance on manual transfers, logging, and compliance reporting.
30%–49% automated	Basic scheduling automated, but governance and monitoring still manual.
50%–69% automated	Core transfers automated with MFT, but deprovisioning, evidence capture, or error handling often ad hoc.
70%–89% automated	Majority of jobs automated using MFT, including some integrations (SIEM, DLP, IDP). Plateau point for most.
90%–100% automated	Nearly all file transfer jobs automated end-to-end, including governance, compliance, and incident response triggers.

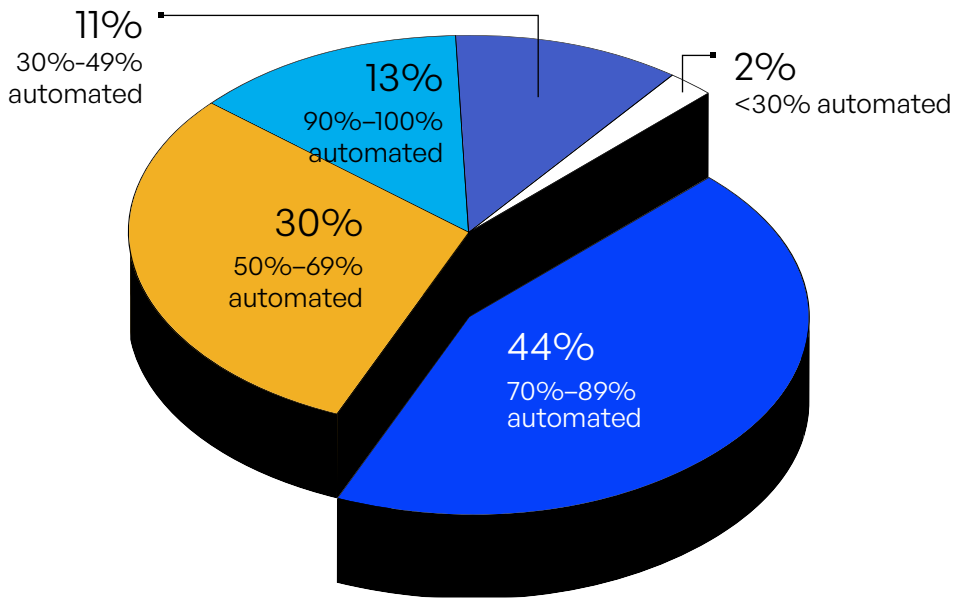


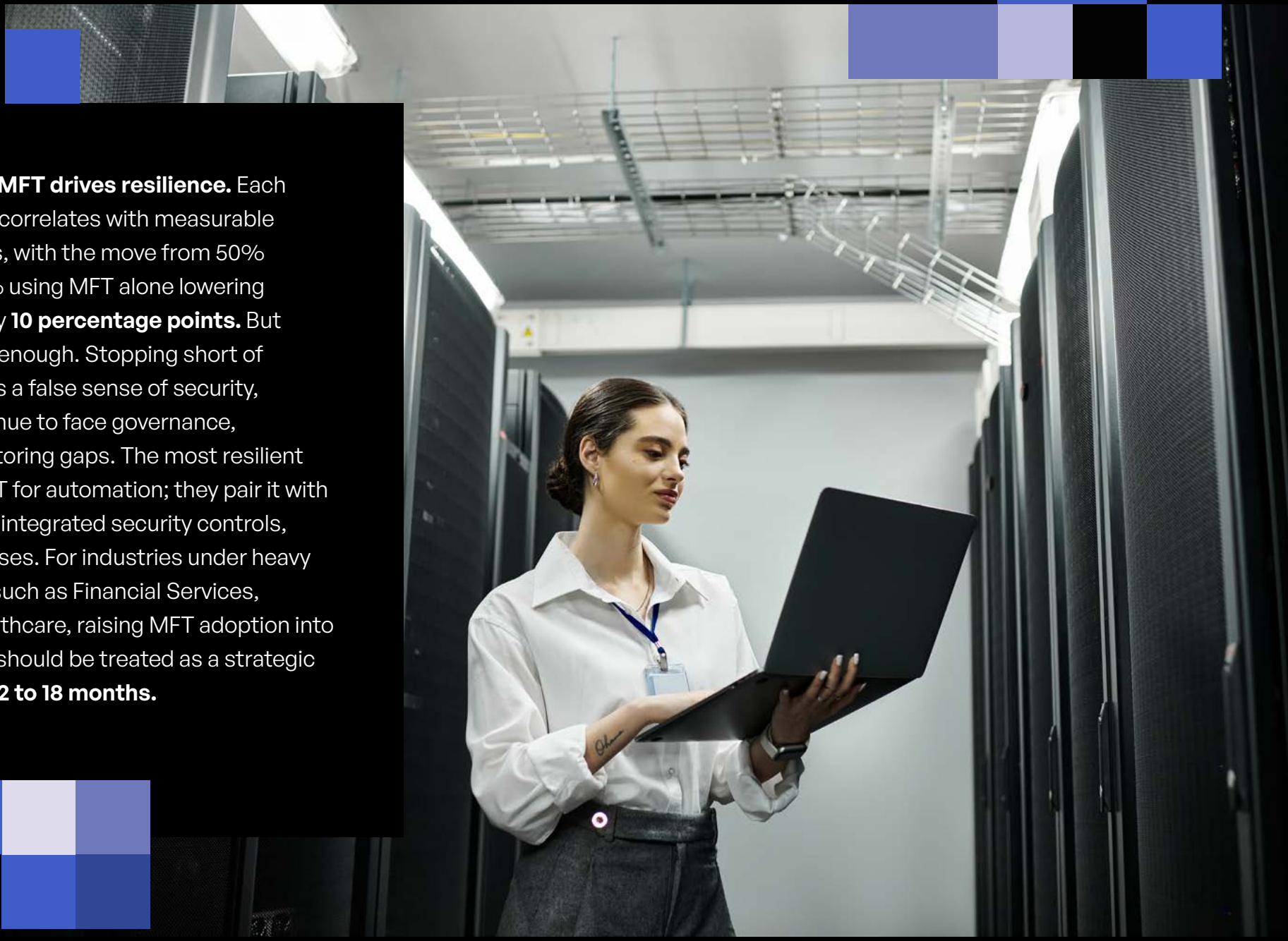
Figure 12: Distribution of Manual File Transfer vs. MFT (automated).

Most organizations plateau in the 50%–89% automation band, where routine transfers and scheduling are covered but advanced workflows such as automated evidence capture, error handling, and security integrations remain manual. This creates diminishing returns, as partial automation still leaves gaps attackers can exploit. By contrast, the 13% of organizations that achieve full automation at the 90%–100% level report the lowest incident rates—just 29%—because they treat automation as a strategic control rather than simply an efficiency measure.

Industry patterns reinforce this divide: Financial Services and Technology have pushed automation further, often using MFT 70%–89% or higher, which aligns with their lower breach rates. Government and Education, however, frequently stall with MFT in the 50%–69% band due to legacy infrastructure. The maturity assessment underscores this gap, showing that many organizations remain stuck at basic or ad hoc levels, where even partial automation fails to deliver results without integration into SIEM, DLP, or identity systems.

Automated MFT vs. Manual File Transfer	Average Incident Rate
<50% using MFT	71% reported an incident
50%–69% using MFT	61% reported an incident
70%–89% using MFT	52% reported an incident
90%–100% using MFT	29% reported an incident

Figure 13: MFT vs. Incident Response Rates.



The takeaway is clear: **MFT drives resilience.** Each step up in automation correlates with measurable reductions in incidents, with the move from 50% to 69% to 70% to 89% using MFT alone lowering incident rates by nearly **10 percentage points.** But partial progress is not enough. Stopping short of full automation creates a false sense of security, as organizations continue to face governance, compliance, and monitoring gaps. The most resilient 13% don't just use MFT for automation; they pair it with strong encryption and integrated security controls, creating layered defenses. For industries under heavy compliance pressure such as Financial Services, Government, and Healthcare, raising MFT adoption into the 90%–100% range should be treated as a strategic priority over the **next 12 to 18 months.**

Section 3: MFT Third-Party & Supply Chain Risks

Third-party risks and content inspection capabilities represent critical components of MFT security that many organizations overlook.

3.1 Vendor Assessment: Beyond the Checkbox

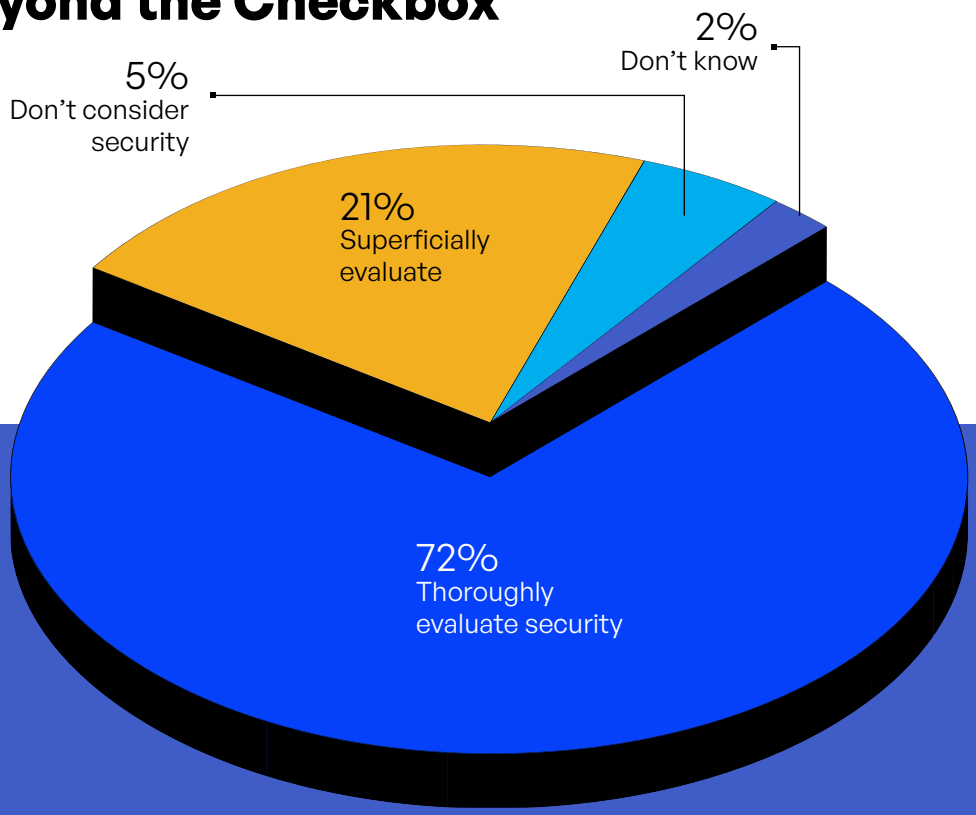


Figure 14: Vendor Security Evaluation Depth.

Third-party risk management and content inspection remain weak links in MFT security. While 72% of organizations report thoroughly evaluating vendors, the 59% incident rate shows that "checkbox diligence" often fails to uncover deeper vulnerabilities. A further 21% admit only superficial evaluation, 5% ignore vendor security altogether, and 2% are unsure. This gap highlights that vendor reviews alone cannot guarantee resilience—organizations must pair them with advanced content inspection and continuous assurance. Without deeper controls, third-party oversight remains a compliance exercise rather than a true defense against breaches.

3.2 Content Inspection: The Advanced Threat Gap

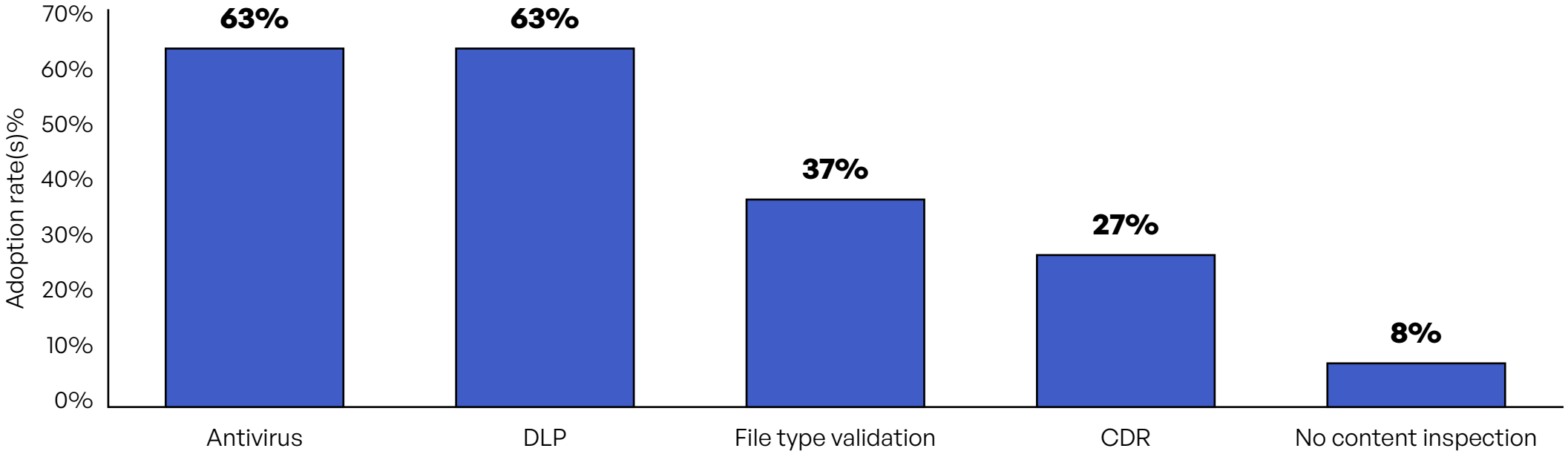


Figure 15: Adoption Rate for Data Security Inspection Capabilities.

Organizations show progress in basic data security safeguards, but gaps remain that directly affect data privacy. Most rely on antivirus **(63%)** and DLP **(63%)** to meet baseline protections, yet only **37%** rely on file type validation and only **27%** deploy advanced safeguards that ensure sensitive information is stripped of hidden risks before sharing. Even the largest enterprises report just 35% adoption of these stronger controls, while half of the smallest organizations operate with only basic or no safeguards at all. Mid-size firms demonstrate more balanced adoption, but across the board, overreliance on legacy measures leaves sensitive files exposed. Until stronger data security and privacy controls are consistently applied, organizations risk unauthorized exposure of sensitive information and compliance failures.

Organization Size (Employees)	Advanced Controls	Basic Controls
>20,000	18%	32%
10,001–19,999	29%	29%
5,001–10,000	20%	37%
Under 5,000	24%	25%

Figure 16: Advanced MFT Security Per Organization Size.

3.3 MFT Data Types

Data Type	Rank 1	Rank 2	Rank 3	Total Answers
PII	39%	9%	11%	58%
PHI	10%	10%	7%	26%
PCI	11%	12%	9%	33%
Intellectual property	10%	11%	9%	30%
Financial records	11%	22%	14%	46%
B2B transaction data	12%	12%	13%	36%
Confidential corporate communications	3%	9%	18%	30%
Customer data subject to privacy regulations	4%	13%	15%	33%

Figure 17: Rankings of MFT Data Types.

The table highlights that personally identifiable information (PII) clearly dominates as the top-ranked data type of concern, with nearly **39%** ranking it first and **58%** including it among their top three priorities. This reflects the growing emphasis on data privacy regulations worldwide, as protecting PII is foundational for compliance and risk management. Financial records also stand out, with **46%** of responses including them among the top three—underscoring the critical role of safeguarding sensitive financial information against fraud, theft, and regulatory penalties. PCI and customer data subject to privacy regulations also draw significant attention, reinforcing that compliance-driven categories remain front and center.

Beyond regulatory-driven concerns, business-critical data categories such as B2B transaction data **(36%)** and intellectual property **(30%)** also score strongly. This indicates that organizations are increasingly balancing compliance obligations with strategic protection of competitive assets. Interestingly, confidential corporate communications scored lower in first-place rankings (just 3%) but still appeared in nearly **30%** of top three mentions, suggesting that while not seen as the most urgent risk, it is a growing area of sensitivity. Together, the results suggest that organizations are taking a broad, multi-dimensional view of data protection—prioritizing regulatory requirements while recognizing the operational and competitive risks of unmanaged business data.

3.4 Real-World Impact

The data still shows a tight link between control maturity and outcomes: The 39% of organizations reporting no incidents have consistently higher adoption of advanced safeguards, while those with breaches (20%) or unauthorized access (27%) typically lack comprehensive protections. Availability issues (12%) signal how partial or poorly tuned controls can strain systems.

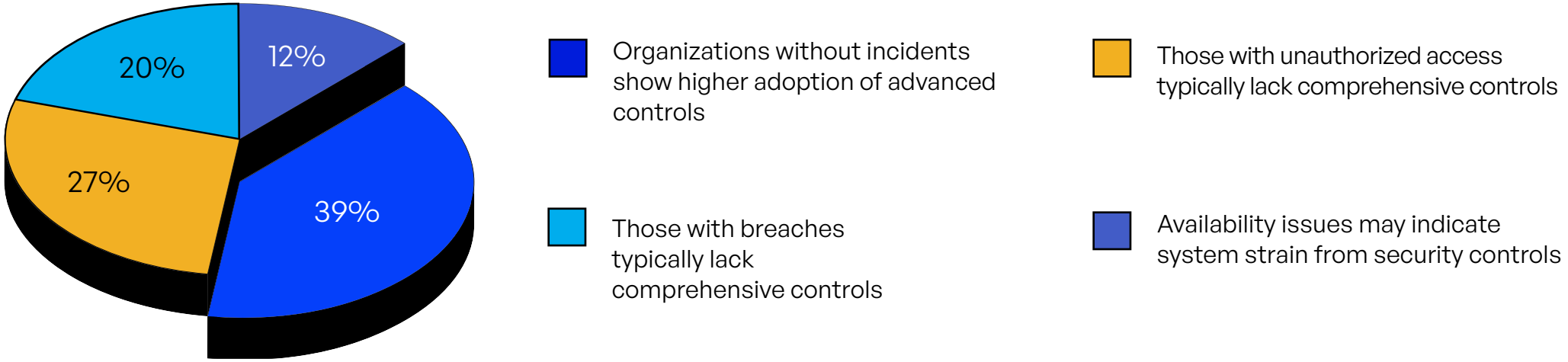
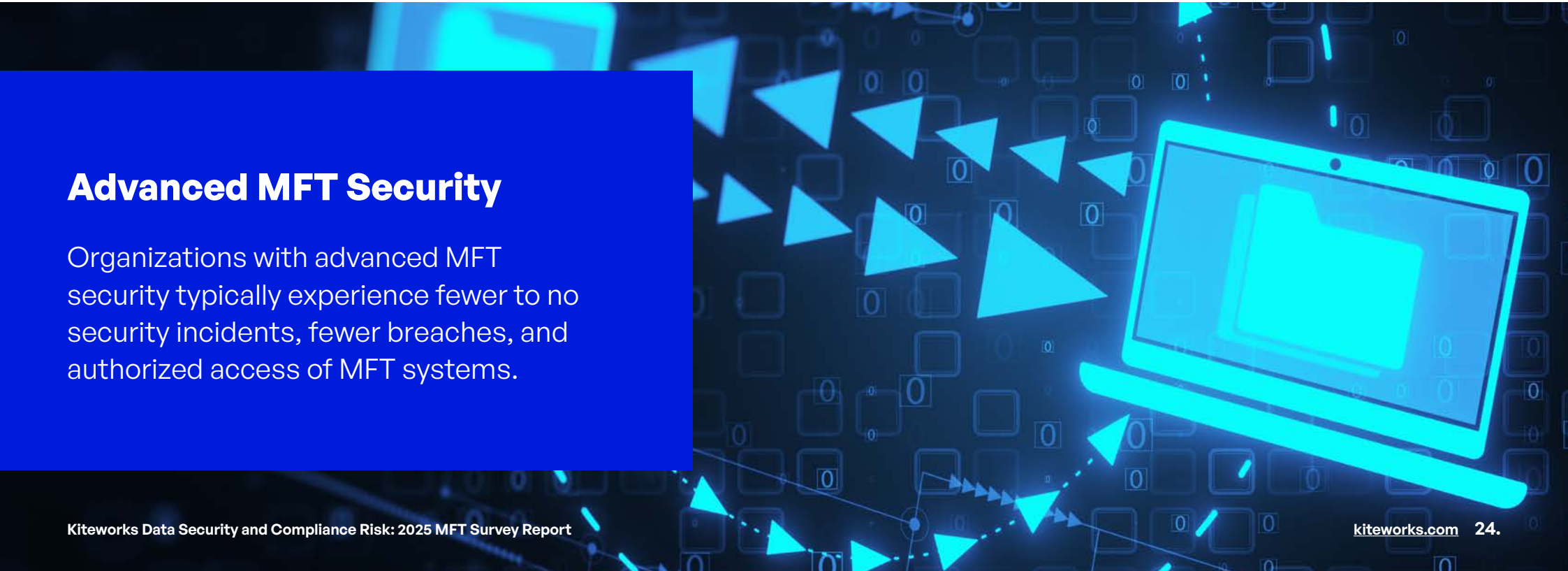


Figure 18: Advanced Security and Data Incidents.

By industry, **Professional Services (64%)**, **Manufacturing (63%),** and **Technology (62%)** now show the highest total incident rates in our sample, driven largely by unauthorized access (≈27%–33%) with meaningful availability issues in the first two. **Government (50%)** and **Financial Services (50%)** have similar overall incident rates but very different profiles—Government splits evenly between breaches (25%) and unauthorized access (25%), whereas Financial Services is more balanced across breach (≈14%), unauthorized (≈18%), and availability (≈18%). **Healthcare** reports a lower total incident rate (33%) but a comparatively high breach share (≈22%), consistent with weak encryption at rest. Together, these results reinforce that resilience isn't about isolated safeguards; it comes from layered, well-integrated defenses that both prevent attacks and maintain operational stability.

Industry	Total Incidents	Unauthorized Access	Availability Issues	Breaches	Key Insights
Technology	62%	28%	10%	24%	Mixed profile: notable breaches and access attempts; strengthen at-rest encryption and unified monitoring.
Manufacturing	63%	33%	19%	11%	OT/IT mix shows up as higher access + availability issues; integration and automation gaps likely.
Financial Services	50%	18%	18%	14%	Balanced adoption, but incidents still split across breach and ops issues—continue SIEM + encryption focus.
Government	50%	25%	0%	25%	Policy strong, technical controls uneven; weakest at-rest encryption drives breach exposure.
Healthcare	33%	11%	0%	22%	Over-indexed on transit encryption; at-rest encryption shortfall elevates breach risk.
Professional Services	64%	27%	18%	18%	Governance inconsistency and manual off-boarding show up as higher incidents.

Figure 19: Incident Patterns Across Industries.



Advanced MFT Security

Organizations with advanced MFT security typically experience fewer to no security incidents, fewer breaches, and authorized access of MFT systems.

Section 4: Compliance & Emerging Regulations

Organizations face an increasingly complex compliance landscape for MFT systems. Our survey shows that while 54% of organizations cite GDPR compliance, many lack the fundamental security controls these frameworks require. The disconnect between compliance claims and security reality creates significant risk.

This section examines compliance framework adoption, the emerging challenge of data sovereignty, and how organizations are beginning to address AI-related governance.

4.1 Compliance Landscape

The survey reveals organizations managing multiple regulatory frameworks simultaneously:

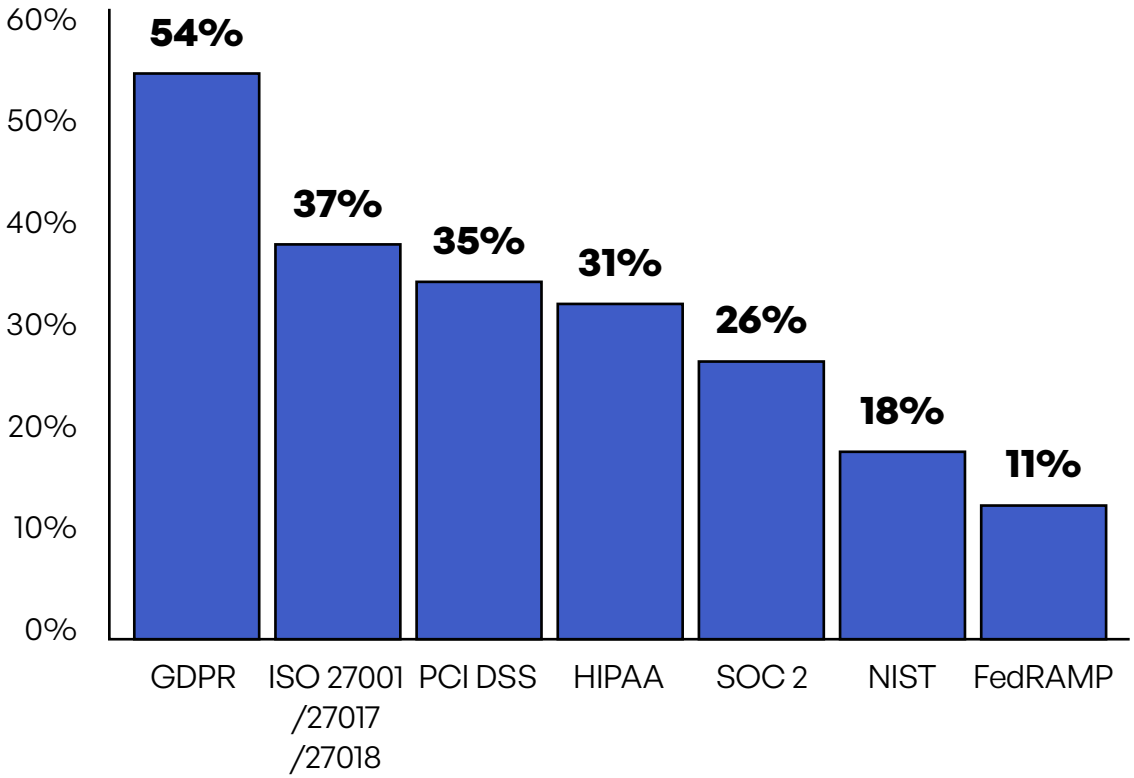


Figure 20: Compliance Framework Adoption.

Adoption Patterns Per Industry

The adoption patterns vary significantly by industry. **Healthcare shows high HIPAA adoption** as expected, while **Financial Services** organizations report **compliance with multiple frameworks. Government agencies** show **adoption of federal frameworks** like NIST and FedRAMP.

However, framework adoption doesn't guarantee adequate security implementation. The survey data reveals concerning gaps:

Industry-Specific Implementation Gaps

The survey data reveals striking gaps between compliance claims and technical implementation across industries.

Healthcare organizations achieve 100% end-to-end encryption adoption, yet only 11% implement AES-256 at rest—the second lowest of any industry. This imbalance is especially concerning given HIPAA's emphasis on protecting patient data. Healthcare also reports a 44% incident rate, including an 11% breach rate, showing how compliance without comprehensive security leaves vulnerabilities exposed.

Government agencies present an even sharper policy-practice disconnect. Despite broad adoption of frameworks like NIST and FedRAMP, only 8% implement AES-256 encryption at rest—the weakest adoption of any sector. Their 50% incident rate, with 25% experiencing unauthorized access attempts, reflects the risks created by this implementation gap.

Financial Services stands out as an exception, demonstrating more balanced alignment between compliance frameworks and technical controls. This consistency likely contributes to its relatively low incident rate of 25%, the best outcome among surveyed industries.

Education struggles with both governance and resilience. With 57% reporting incidents, including 29% unauthorized access attempts and 29% availability issues, the sector shows broad security gaps. While some institutions adopt time-limited credentials, weak deprovisioning and inconsistent technical implementation suggest that detection gaps may mask actual breaches.

4.2 Data Sovereignty: The Next Compliance Frontier

Data sovereignty has become a critical consideration for global MFT operations. The survey examines how organizations address data residency and cross-border transfer requirements:

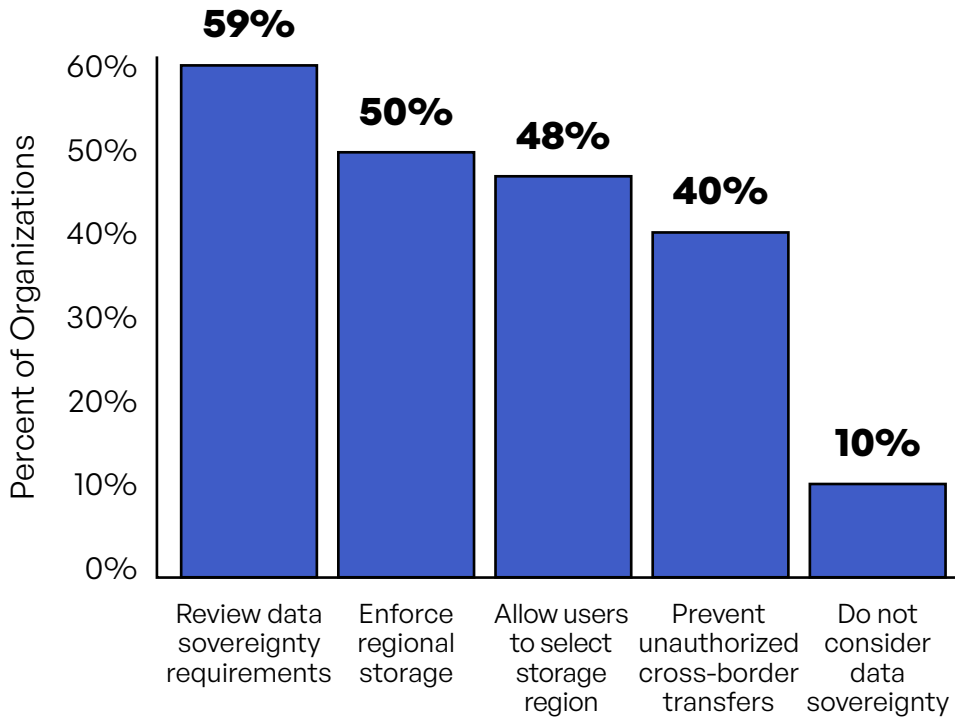


Figure 21: Data Sovereignty Practices.

The 9 percentage point gap between those who review requirements (59%) and those who enforce regional storage (50%) indicates implementation challenges. Organizations understand the requirements but struggle to enforce them technically.

4.3 Bridging the Compliance-Implementation Gap

The survey highlights three pressing challenges that prevent organizations from turning compliance into effective security.

Multiple Framework Requirements. Most organizations must juggle several frameworks simultaneously—GDPR (54%), ISO 27001/17/18 (37%), PCI DSS (35%), and others. Each framework imposes specific MFT requirements, from encryption and access control to logging and sovereignty, forcing organizations to maintain overlapping obligations.

Implementation Gaps. The most troubling finding is the gulf between stated compliance and technical reality. While 54% of organizations claim GDPR compliance, only 42% encrypt data at rest with AES-256. Similarly, 59% review sovereignty requirements, but just 50% enforce regional storage. These gaps show how policies may be documented yet remain unenforced, exposing organizations to both operational risk and regulatory penalties.

Emerging Requirements. AI governance is quickly becoming a compliance frontier. Nearly half (48%) conduct regular AI risk reviews, yet only 44% implement automated controls. Alarmingly, 12% report no AI risk management at all—leaving them exposed as AI adoption accelerates and regulators sharpen their focus on algorithmic accountability.

From Checkbox to Reality. The data suggests that compliance cannot remain a box-ticking exercise. Organizations must translate frameworks into operational controls—encrypting data, enforcing sovereignty, automating governance—if they want to reduce incident rates. The correlation is clear: Where technical implementation lags, incidents rise.

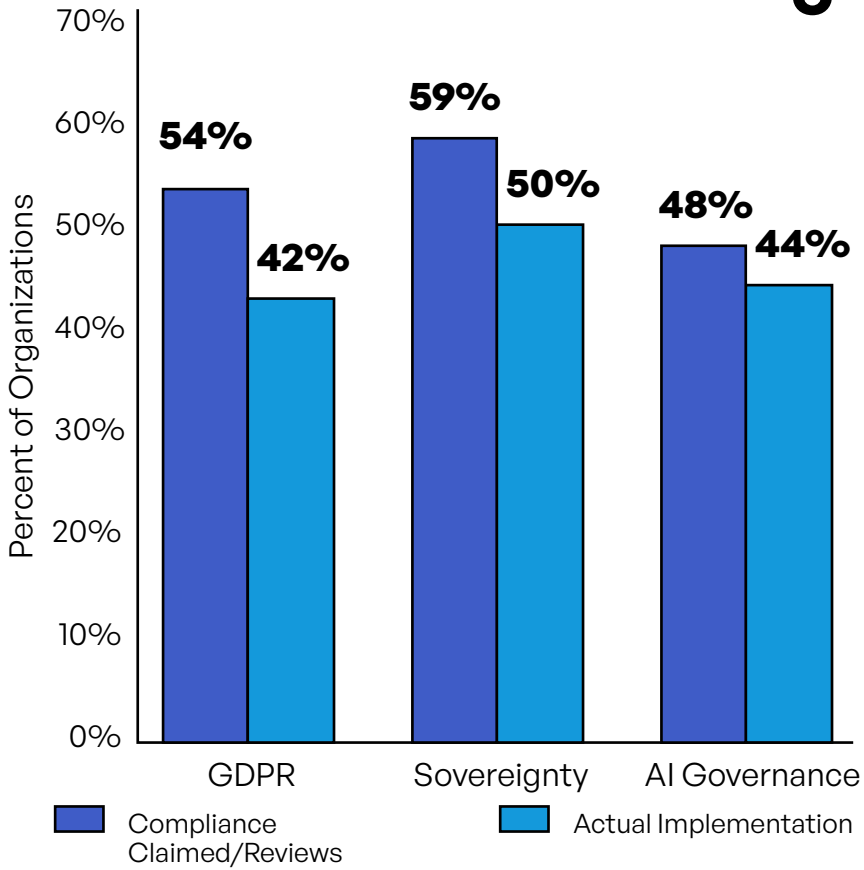


Figure 22: Compliance vs. Implementation Gaps.

Key Takeaway: A persistent gap exists between compliance claims and security reality. With **54%** claiming GDPR compliance but only **42%** implementing encryption at rest, and with half failing to enforce sovereignty or automate AI governance, organizations face both security and regulatory risks. True compliance requires more than framework adoption—it demands practical, enforced, and verifiable controls.

Section 5: Industry Benchmarks & Peer Comparison

The survey data reveals distinct patterns across industries and organization sizes. Understanding where your organization stands relative to peers provides context for prioritization and realistic goal setting.

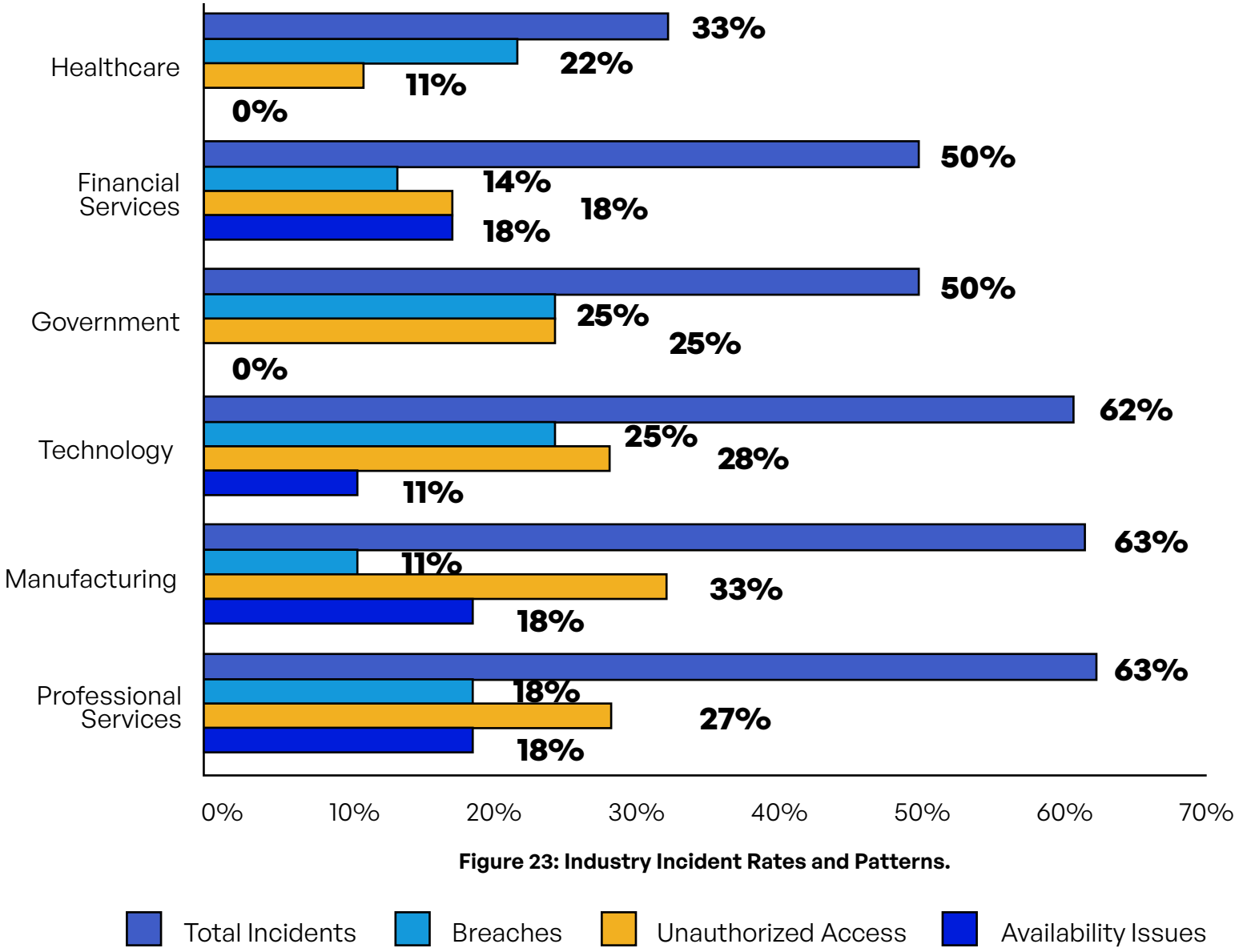


Figure 23: Industry Incident Rates and Patterns.

Each industry faces unique challenges reflected in their security implementations and outcomes. The data shows no industry has achieved comprehensive protection, though some fare significantly better than others.

Healthcare Industry Scorecard

Healthcare presents a striking paradox in MFT security. While leading all industries with **44%** cloud-only deployment and achieving 100% end-to-end encryption adoption, healthcare organizations show the worst performance in data-at-rest protection with only 11% using AES-256. This gap proves costly—44% of healthcare organizations experienced security incidents, including an **11%** breach rate, tied for the highest across all sectors. The disconnect stems from Healthcare's interpretation of HIPAA requirements, which designate encryption as "addressable" rather than required. Organizations have focused on visible controls like transit encryption while neglecting stored data protection. Combined with fragmented systems across clinical, administrative, and research functions, Healthcare's strong cloud adoption hasn't translated into resilience.

Financial Services Industry Scorecard

Financial Services demonstrates what balanced security implementation can achieve. With the lowest incident rate at **25%** and the lowest breach rate at just **8%,** the sector shows how comprehensive approaches pay off. Financial organizations don't lead in any single control but maintain consistent implementation across multiple dimensions—encryption, access management, vendor vetting, and compliance frameworks. Its success comes despite facing the heaviest regulatory burden, averaging multiple simultaneous compliance requirements including GDPR, PCI DSS, and SOC 2. Rather than treating each framework separately, leading institutions build unified control sets that satisfy multiple requirements simultaneously. Remaining challenges center on completing SIEM integration and expanding advanced threat protections like CDR.

Government Industry Scorecard

Government agencies exemplify the gap between policy and practice. While showing strong adoption of federal frameworks and sovereignty enforcement (**67%** enforce regional storage), government organizations demonstrate the weakest technical implementation with only **8%** using AES-256 encryption at rest. The result is a **50%** incident rate, with **25%** experiencing unauthorized access attempts—evidence of persistent targeting by threat actors. This policy-practice disconnect reflects systemic challenges in government IT: legacy constraints, complex procurement processes, and budget cycles that favor visible initiatives over foundational security. The strong sovereignty enforcement shows government can implement controls when mandated, but voluntary best practices like comprehensive encryption continue to lag.

Education Industry Scorecard

Education faces broad security challenges, with a **57%** incident rate split between unauthorized access **(29%)** and availability issues **(29%)**. Notably, Education reported no breaches in the survey, though this may reflect detection gaps rather than strong prevention. The sector shows inconsistent control adoption—some institutions demonstrate advanced capabilities while others lack basic protections. Resource constraints drive many of these gaps. With diverse user populations including students, faculty, and researchers, combined with limited IT budgets and legacy systems, Education struggles to implement consistent controls. The high rate of availability issues suggests that when controls are deployed, they may strain already limited infrastructure.

Technology Industry Scorecard

Technology reports 62% total incidents, split across **24%** breaches, **28%** unauthorized access, and **10%** availability issues. Strengths include higher automation and stronger integration than most sectors, but gaps in encryption at rest and consistent access governance still create exposure—particularly to breach and access attempts. Rapid platform adoption can also introduce fragmentation, so unification and SIEM/SOC coverage remain priorities.

5.1 Size-Based Maturity Patterns

Organization size profoundly impacts security approaches, available resources, and outcomes, though the relationship proves non-linear. The survey reveals that bigger doesn't always mean better when it comes to MFT security.

Organization Size	Key Characteristics	Breach Rate	Notable Strengths	Key Challenges
<1,000	Constrained resources, limited staff	15%	Simpler infrastructure, potential to benefit from unified platforms	Reliance on basic inspection (AV only), little advanced protection
1,000–5,000	Transitioning to formalized security	16%	70% DLP adoption, structured governance starting	Balancing growth with security investment
5,000–10,000	Mid-market, most at risk	32% (highest)	High IR testing (75%), leading AI governance automation	Breach rate remains highest due to scaling complexity and gaps in basics
10,000–20,000	Large, stable but slow to adapt	19%	Strong traditional controls, resources available	Integration complexity, organizational inertia
>20,000	Very large, most mature	10% (lowest)	80% conduct regular IR testing, lowest breach rates	Legacy systems, slow adoption of new frameworks

Figure 24: Security Maturity by Organization Size.

Organizations under 1,000 employees operate with constrained resources that force focused approaches. Half show only basic or no content inspection, relying on antivirus without advanced protections. Yet their smaller attack surface and simpler infrastructure can work to their advantage if basic controls are properly implemented. These organizations often lack dedicated security staff, making unified platforms and automation particularly valuable.

The 1,000–5,000 employee range marks the beginning of security formalization. These organizations achieve **70%** DLP adoption—strong for their size—and begin implementing structured governance. Their **16%** breach rate sits near the survey average, suggesting they're managing the transition to formal security reasonably well. The key challenge becomes balancing continued growth with security investment.

Mid-market organizations from 5,000–10,000 employees face the most challenging dynamics. Despite showing the highest IR testing rate at **75%,** they suffer the highest breach rate at **32%.** This seeming contradiction reveals the complexity of their position—large enough to attract sophisticated attackers but still building mature security capabilities. They lead in AI governance automation, showing innovation capacity, but struggle with the basics. The transition period as they scale creates vulnerabilities faster than controls can address them.

Large organizations between 10,000–20,000 employees show more stable patterns with a **19%** breach rate. They've implemented strong traditional controls but show slower adoption of emerging frameworks. Integration complexity becomes their primary challenge as dozens of systems must work together. These organizations have the resources for comprehensive security but struggle with organizational inertia.

The largest organizations over 20,000 employees achieve the lowest breach rate at **10%** through mature security programs and dedicated resources. With **80%** conducting regular IR testing, they demonstrate security discipline. However, they lag in adopting new technologies and frameworks, constrained by legacy systems and complex change management processes. Their challenge becomes maintaining security while modernizing infrastructure.

Largest organizations experienced the fewest breaches—**10%**—vs. mid-market organizations that experienced the highest at **32%.**

5.2 Success Pattern Analysis

Examining the 39% of organizations reporting no security incidents reveals actionable patterns any organization can follow. These incident-free organizations don't share a single profile but demonstrate consistent practices that differentiate them from the vulnerable majority.

Control Area	All Orgs (Average)	Incident-Free (39%)	With Incidents (59%)	Key Insights
Unified MFT Platform	38%	Much higher	Lower	Architecture simplicity drives consistency
SIEM/SOC Integration	37%	Higher adoption	Lagging	Eliminates monitoring blind spots
Automation ≥70%	~44%	Majority	Plateau at 50%–70%	Push past plateau for resilience
CDR Adoption	27%	Higher adoption	Low	Advanced file security differentiator
Encryption (in transit and at rest)	~76%/42%	Both implemented	Gaps remain	Comprehensive protection required

Figure 25: Controls Adoption—Incident-Free vs. Others.

Architecture emerges as a foundational differentiator. While only **38%** of all organizations have unified MFT platforms, incident-free organizations show significantly higher adoption. Unification reduces complexity, enables consistent policy enforcement, and simplifies security monitoring. The correlation between architectural simplicity and security outcomes proves stronger than any single security control.

Integration capabilities separate successful organizations from those experiencing incidents. Organizations with SIEM/SOC integration detect and respond to threats faster, while those operating in silos miss attack patterns. The incident-free cohort shows higher rates of integration across all categories—SIEM/SOC, DLP, identity providers, and applications. They've eliminated the blind spots that attackers exploit.

Automation levels strongly predict security outcomes. Organizations achieving **70%** or higher automation show markedly lower incident rates. Automation ensures consistent policy application, reduces human error, and enables rapid response. The incident-free organizations cluster in the higher automation bands, having pushed past the common plateau at **50%–70%** automation.

Automation of File Transfer

Organizations with higher rates **(70% or more)** of MFT adoption show a remarkedly lower rate of security incidents.

Only 38% of organizations have unified MFT platforms, which ratchets up security and compliance risks.

Advanced threat protection separates leaders from laggards. While overall CDR adoption sits at only **27%,** incident-free organizations show significantly higher implementation. They recognize that traditional antivirus and DLP cannot catch modern file-based attacks and have invested in content disarm and reconstruction capabilities.

The survey data reveals that no single control guarantees security. Instead, incident-free organizations implement multiple controls comprehensively. They encrypt data both in transit and at rest, integrate security monitoring, automate operations, and protect against advanced threats. This layered approach creates defense in-depth that proves difficult for attackers to penetrate.

Financial Services exemplifies this comprehensive approach, achieving the lowest incident rate through balanced implementation rather than excellence in any single area. It doesn't lead in encryption, integration, or automation individually but maintains solid implementation across all dimensions. This consistency, rather than sporadic excellence, drives its superior outcomes.

5.3 Learning From Leaders and Laggards

The survey data demolishes several security myths. Organization size doesn't guarantee security—mid-market companies with significant resources show the highest breach rates. Industry doesn't determine destiny—Healthcare's advanced cloud adoption coexists with critical encryption gaps. Testing doesn't equal protection—high IR testing rates don't prevent incidents without addressing fundamental gaps.

Instead, the data points to architectural decisions and comprehensive implementation as the true differentiators. Organizations achieving security success share common traits regardless of industry or size: **unified platforms** that reduce complexity, **comprehensive encryption** protecting data throughout its life cycle, **integrated security monitoring** that eliminates blind spots, **advanced threat protection** addressing modern attacks, and **automated operations** ensuring consistency.

The path forward varies by starting point. Healthcare must close its encryption gap while maintaining cloud momentum. Government needs technical implementation to match policy frameworks. Education requires basic control implementation before advancing. Financial Services should complete integration while maintaining balanced approaches.

Size-based strategies differ as well. Smaller organizations benefit most from unification and automation that multiply limited resources. Mid-market companies must stabilize basics while scaling. Large enterprises need modernization strategies that work within complex environments.

Yet the destination remains consistent: comprehensive, integrated, automated MFT security. The **39%** of organizations avoiding incidents prove this goal achievable. The question becomes not whether to pursue comprehensive security, but how quickly organizations can close their specific gaps before joining the **59%** experiencing incidents.

Industry Gaps

High adoption rates of cloud deployments but low encryption rates in Healthcare highlight a significant MFT security risk.

Section 6: Your Action Plan

The survey data provides clear direction for improving MFT security, but knowing where to start can be overwhelming. This section translates insights into practical action plans tailored by organization size and current maturity level.

6.1 Data Breach Patterns and Impact

Data breaches are less common than unauthorized access or availability issues but remain the most severe outcome. Across all respondents, 20% reported experiencing a data breach in the past 12 months, underscoring that while other incident types disrupt operations, breaches carry direct compliance, financial, and reputational consequences.

Breaches by Industry

Breach prevalence varies widely across sectors. **Government (16%)** and **Healthcare (11%)** stand out with the highest rates, despite both being subject to strict regulatory regimes. In Government, the breach rate reflects a persistent gap between policy frameworks and technical implementation, with only 8% using AES-256 encryption at rest. Healthcare's breach exposure stems from overreliance on in-transit encryption while neglecting at-rest protection, combined with fragmented systems across clinical and administrative functions. **Manufacturing (9%)** also reports elevated breach activity, reflecting the complexity of securing both IT and operational technology systems. **Technology firms (7%)** perform somewhat better, aided by greater automation and modern infrastructure. **Financial Services (8%)** leads the way, achieving the lowest breach rate of any major sector. Its strength lies not in excelling at any single control, but in maintaining consistent implementation across encryption, access governance, vendor diligence, and compliance frameworks.

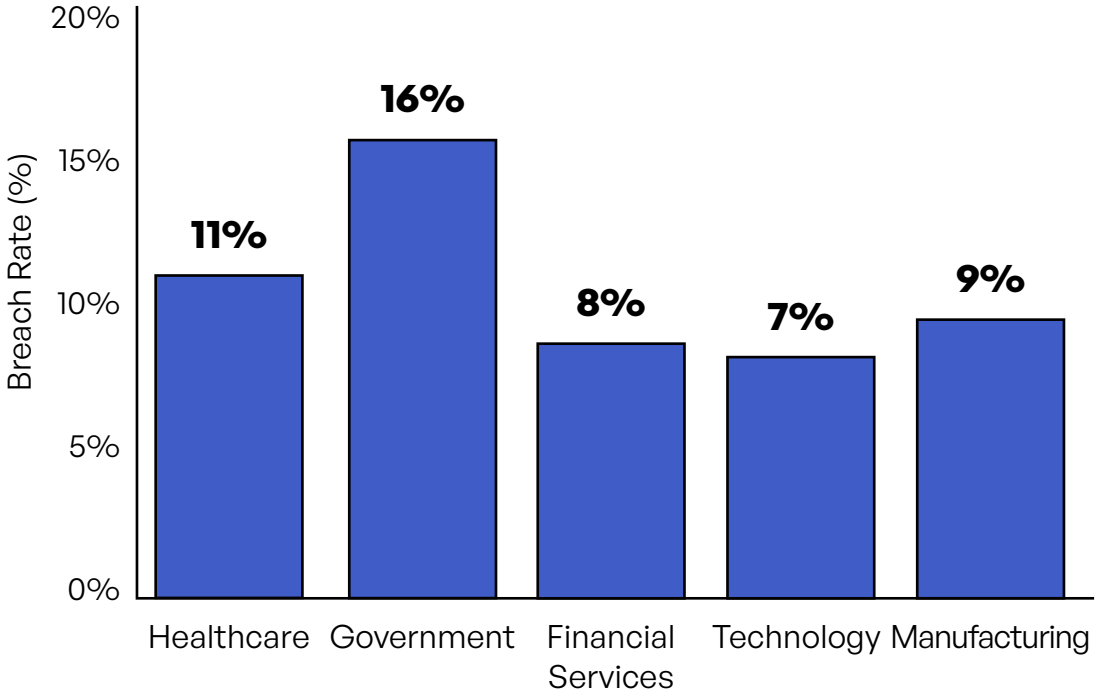


Figure 26: Data Breach Rates by Select Industries.

Breaches by Organization Size

Breach rates also reveal a non-linear relationship with organization size. **Mid-market organizations (5,000–10,000 employees)** suffer the highest breach rate at **32%**, despite being among the most diligent in incident response testing (75% test regularly). These organizations are large enough to attract sophisticated attackers but are still building security maturity, creating a dangerous mismatch between scale and resilience. In contrast, the **largest enterprises (>20,000 employees)** record the lowest breach rate at **10%**, benefiting from mature programs and deeper resources. Organizations in the **1,000–5,000 band** average **16%**, while those under 1,000 show a similar 15%, reflecting resource constraints but simpler infrastructures. **Large firms (10,000–20,000 employees)** fall in the middle at **19%**, with integration complexity as their main barrier.

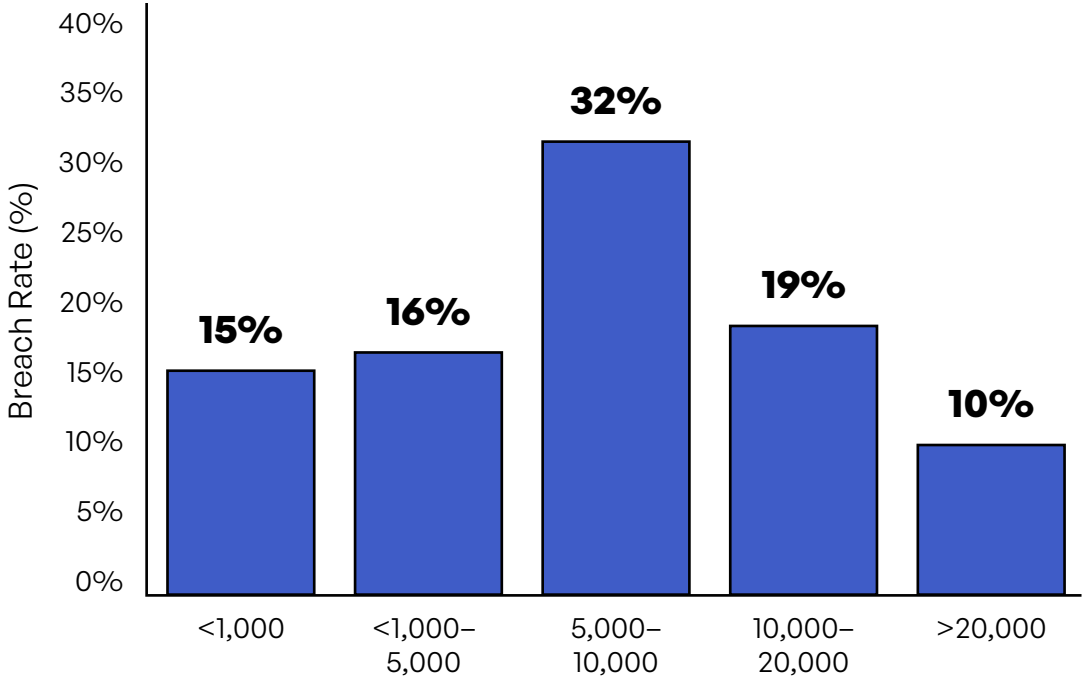
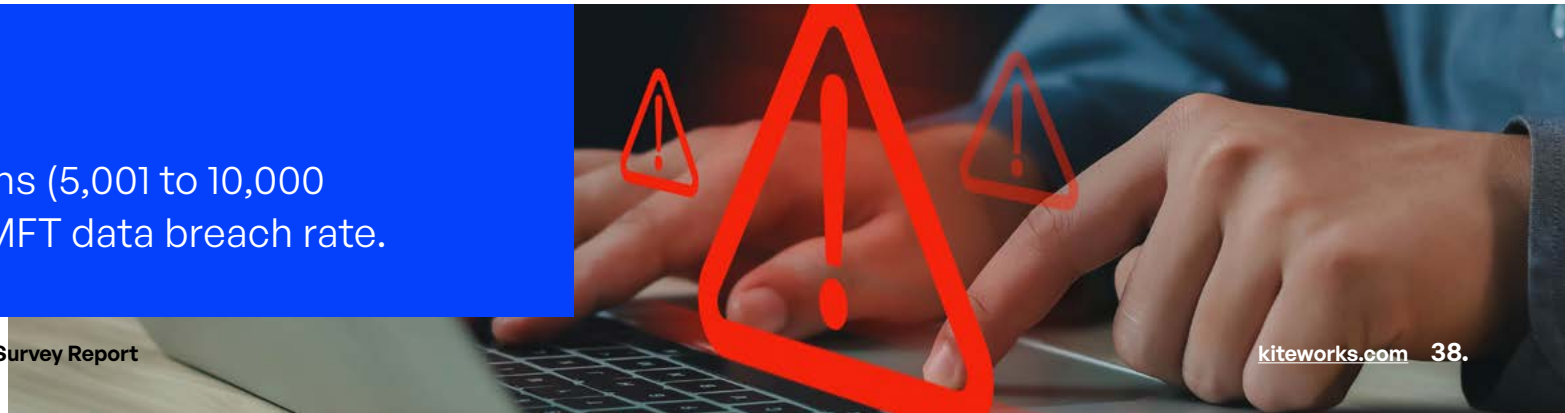


Figure 27: Breach Rates by Organization Size.

The data makes clear that **breach prevention depends less on compliance claims and more on consistent technical enforcement.** Industries with weak encryption at rest or fragmented governance continue to face the highest breach exposure. Mid-sized organizations represent the riskiest cohort, as they attract more attacks while still scaling their capabilities. And vendor choice matters: Platforms with incomplete integration or dated architectures correlate with higher breach rates. To reduce breach likelihood, organizations must prioritize end-to-end encryption, SIEM/SOC integration, and higher levels of automation, while applying rigorous vendor diligence to ensure controls perform as advertised.

Mid-Market Risk

32% of mid-market organizations (5,001 to 10,000 employees) suffer the highest MFT data breach rate.



6.2 Quick Wins vs. Strategic Initiatives

The survey data enables clear distinction between immediate improvements and longer-term transformations. Both matter, but sequencing determines success.

Immediate Impact Actions

Encryption represents the highest-impact quick win. With **58%** lacking AES-256 at rest while **76%** have end-to-end encryption in motion, most organizations can extend existing encryption to storage with minimal architectural change. The survey shows Government at only 8% and Healthcare at 11% adoption—these sectors could dramatically improve security posture through this single change.

Integration offers another high-impact opportunity. The **63%** without SIEM/SOC integration operate blindly, missing attack patterns visible through correlation. Modern MFT platforms include SIEM connectors that can be enabled in hours, not weeks. Even basic integration marking file transfer events improves detection capabilities.

Access control improvements show immediate benefits. The **42%** not conducting quarterly reviews and 52% without automated deprovisioning leave obvious vulnerabilities. Implementing automated deprovisioning prevents the insider threats that account for 27% of incidents. Time-limited credentials, used by only **33%,** prevent credential accumulation that attackers exploit.

CDR Adoption and Data Protection

CDR is an important signal for MFT security maturity, but only **27%** of survey respondents indicated they have it implemented.

Strategic Transformations

Platform unification addresses the **62%** fragmentation rate but requires careful planning. The survey shows unified organizations achieve better outcomes across all metrics—fewer incidents, easier compliance, lower operational costs. However, unification projects typically span 12 to 18 months and require business process reengineering alongside technical implementation.

Advanced threat protection through CDR adoption remains low at **27%,** despite effectiveness against modern attacks. Implementation requires new technology adoption, workflow modification for file reconstruction, and user education about modified files. Organizations pursuing CDR must plan for these changes beyond just purchasing technology.

Automation advancement shows clear correlation with positive outcomes, yet only **13%** achieve **90%–100%** automation. Moving from the typical **50%–70%** range to higher automation requires different approaches—orchestration platforms, infrastructure as code, and cultural shifts toward automation-first thinking. The investment pays off through consistency, speed, and freed human resources for strategic work.

Initiative	Implementation Time	Breakeven Point	2-Year Value
AES-256 at Rest	1–3 months	Immediate	Incident prevention
SIEM Integration	2–4 weeks	3 months	Faster detection
Access Automation	2–3 months	6 months	Efficiency + security
Platform Unification	12–18 months	18–24 months	TCO reduction
CDR Deployment	3–6 months	12 months	Advanced protection
90%+ Using MFT	6–12 months	12–18 months	Operational excellence

Figure 28: ROI Timeline for Key Initiatives.

6.3 Risk Calibration Disconnect: Why “Very Important” Isn’t Important Enough

MFT patching criticality rankings (Figure 29) reveal a concerning disconnect between security priorities and outcomes that exemplifies the report’s central theme of “progress without impact.” Organizations rank patching as “very important” (3.71 priority score) rather than “extremely critical” (3.05), suggesting a preference for moderate risk positions over urgent security postures. This measured approach contradicts the harsh reality that 59% experienced incidents in the past year despite widespread security investments, indicating that treating foundational controls like patching as merely “important” may be insufficient for effective risk management.

Rank	Answer	1 Rank	2 Rank	3 Rank	4 Rank	5 Rank	Priority Score
1	Very important	34%	31%	13%	17%	5%	3.71
2	Moderately important	14%	22%	47%	10%	7%	3.24
3	Extremely critical	25%	18%	17%	16%	24%	3.05
4	Somewhat important	12%	21%	14%	40%	13%	2.80
5	Not important	15%	8%	10%	16%	51%	2.21

Figure 29. How Critical Is Continuous Security Patching for Your MFT Deployment.

Organizations show a strong commitment to data sovereignty (Figure 30), with 59% regularly updating MFT practices to reflect evolving localization laws and 50% enforcing strict geographic storage to meet regional regulations. Nearly half (48%) leverage solution capabilities to restrict or select data storage locations according to customer or regulatory needs, while 40% have explicit cross-border transfer controls. However, the 16% grappling with operational complexity and the 10% that ignore sovereignty requirements highlight persistent implementation challenges, especially for global and cloud-centric operations. This distribution underscores that, although data sovereignty is widely recognized as critical, translating policies into robust, scalable controls remains a key barrier to achieving comprehensive MFT compliance.

Your Organization's MFT Approach to Data Sovereignty	Percentage
We regularly review and update our MFT practices to stay compliant with evolving data sovereignty and localization laws	59%
We ensure that data is stored and processed only in specific geographic regions to comply with local laws and regulations	50%
Our MFT solution allows us to select or restrict data storage locations based on customer or regulatory requirements	48%
We have implemented controls to prevent cross-border data transfers unless explicitly approved	40%
We face challenges in meeting data sovereignty requirements due to the complexity of global operations or cloud adoption	16%
We do not consider data sovereignty or data residency requirements when configuring file transfers	10%

Figure 30. MFT Approach to Data Sovereignty.

Organizations overwhelmingly recognize AI-related data security risks in MFT yet struggle to enforce technical controls, revealing a pronounced policy-practice gap (Figure 31. Nearly half (48%) regularly update risk management practices for emerging AI threats, and 44% have automated controls such as DLP or access restrictions. However, only 40% enforce policies restricting AI tool use manually, 30% permit uncontrolled AI usage, and 26% have experienced AI-related incidents—indicating detection rather than prevention. The fact that 12% still do not assess AI risks at all underscores that while strategic awareness is widespread, many organizations lack the operational or technical maturity to translate policies into effective safeguards, exposing sensitive data to misuse in AI-enabled file transfers.

Your Organization's MFT Approach to AI Data Security	Percentage
We regularly review and update our risk management practices to address emerging AI security threats in MFT	48%
Automated technical controls (such as DLP scanning or access restrictions) are in place to monitor and prevent unauthorized use of AI tools	44%
We have policies restricting the use of AI tools with sensitive files, but enforcement is primarily manual (e.g., training, audits)	40%
Employees are permitted to use AI tools with MFT data, but there are no formal policies or controls in place	30%
We have experienced or investigated incidents involving data exposure or misuse related to AI tools in our MFT environment	26%
We do not currently assess or manage AI-related data security risks in our MFT processes	12%

Figure 31. MFT Approach to Data Security.

Assessing MFT Security Data

Looking across these three critical MFT security areas, a concerning pattern emerges that exemplifies the report's central theme of "progress without impact." Organizations consistently position themselves in a moderate risk stance—ranking security patching as merely "very important" rather than "extremely critical" (3.71 vs. 3.05 priority score), implementing geographic data controls while 16% struggle with complexity, and recognizing AI threats while 30% still permit uncontrolled usage. This measured approach appears fundamentally misaligned with the harsh reality of a 59% incident rate despite widespread security investments. The data reveals a systemic policy-practice disconnect where strategic awareness fails to translate into operational execution: Organizations update practices for compliance (59% for sovereignty, 48% for AI risks) yet struggle with basic implementation, demonstrating stronger maturity in traditional regulatory areas like geographic storage controls (50% enforcement) while faltering with emerging AI threats where 26% have already experienced incidents.

The correlation between high activity levels and persistent vulnerabilities suggests that successful MFT security requires not just more controls or policies, but a fundamental recalibration of risk assessment frameworks. Organizations achieving better outcomes, like Financial Services with its 25% incident rate, likely maintain more stringent prioritization rather than defaulting to "moderate importance" across critical controls. The fact that 10%-12% of organizations still ignore fundamental requirements entirely, combined with the preference for "very important" over "extremely critical" rankings for essential controls like patching, indicates many organizations may be intellectually acknowledging risks while maintaining operationally insufficient security postures. This misalignment between measured approaches and actual threat landscapes appears to be a root cause of the persistent gap between security activity and effectiveness, suggesting that organizations need to move beyond balanced, moderate positions to treat foundational security elements with the genuine criticality their risk profiles demand.

The survey's most important lesson about measurement: Perfection isn't the goal—progress is. The 39% of incident-free organizations didn't achieve that status overnight but through consistent improvement. They closed critical gaps, implemented comprehensive controls, and maintained vigilance against evolving threats.

6.4 From Insight to Action

The survey data reveals that security outcomes aren't predetermined by industry, size, or current state—they're determined by focused action on critical gaps. Financial Services achieves a 25% incident rate through balanced controls. Healthcare reaches 100% end-to-end encryption despite resource constraints. Even the largest organizations achieve 10% breach rates through mature programs.

Start with your biggest vulnerability. Without encryption at rest? That's your priority. Missing SIEM integration? Connect those systems. Operating fragmented architectures? Begin consolidation planning. The survey proves what's possible when organizations move beyond moderate risk stances to treat foundational controls with appropriate urgency.

Key Takeaway: The survey data enables precise action planning: close your encryption gaps, integrate your security monitoring, and unify your architecture. Organizations addressing these three areas see dramatic improvement in security outcomes. The path from vulnerable to resilient is clear—execution determines success.

From Security Theater to Real Protection

The report reveals a stark reality in managed file transfer security across organizations. The most critical finding is that 59% of organizations experienced security incidents in the past year, despite many claiming mature security programs. This failure stems from fundamental gaps rather than sophisticated attacks.

Four critical vulnerabilities emerge from the data. *First,* the encryption gap shows that while 76% encrypt data in transit, only 42% protect data at rest with AES-256 encryption. This disparity is particularly severe in Government (8%) and Healthcare (11%), leaving stored data vulnerable where attackers most often strike. *Second,* 63% of organizations haven't integrated their MFT systems with security monitoring platforms, creating significant blind spots in threat detection. *Third,* 62% operate fragmented systems across email, file sharing, and web forms, multiplying vulnerabilities and complicating security management. *Finally,* emerging threats compound these vulnerabilities, with 26% already experiencing AI-related data incidents while 30% permit uncontrolled AI tool usage with sensitive files.

Industry patterns reveal concerning disconnects between compliance claims and implementation. Healthcare achieved 100% end-to-end encryption in motion yet protects only 11% of data at rest, resulting in the highest breach rate at **11%.** Government agencies show the weakest implementation despite strong policy frameworks. Financial Services demonstrates that balanced, comprehensive approaches work—achieving the lowest incident rate at **25%** through consistent implementation across all security dimensions.

Organization size presents another crucial insight. Mid-market companies (5,000–10,000 employees) face the highest breach risk at 32%, as they're large enough to attract sophisticated attacks while still building security capabilities. The largest enterprises achieve only 10% breach rates through mature programs.

The path forward is clear: Organizations must close the encryption gap, integrate security monitoring, and unify fragmented architectures. Success comes not from perfection but from addressing these fundamental vulnerabilities systematically. The 39% of organizations avoiding incidents prove that comprehensive MFT security is achievable through focused action on critical gaps rather than advanced capabilities alone.

Fourfold Mandate

Organizations must close the encryption gap, integrate security monitoring, unify fragmented architectures, and proactively manage AI data security risks.

Survey Methodology

Legal Disclaimer

The information provided in this report is for general informational purposes only and should not be construed as professional advice. Kiteworks and Centiment make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability of the information contained in this report. Any reliance you place on such information is strictly at your own risk. None of the sponsoring or contributing organizations shall be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or profits arising out of, or in connection with, the use of this report. Readers should consult with qualified legal counsel and cybersecurity professionals when addressing specific compliance requirements.

The data in this report was analyzed using AI and the content was generated with AI assistance. While AI enhances analytical capabilities, it can occasionally produce errors or biased information that should be considered when reviewing these findings.

About Centiment

Centiment is a market research firm specializing in data collection and analysis for the cybersecurity and technology sectors. The company delivers actionable insights through customized survey design, targeted respondent recruitment, and sophisticated analytics. Centiment's proprietary research platform ensures exceptional data quality through AI-driven verification and expert human oversight. The company serves Fortune 500 enterprises, technology vendors, and government agencies, providing intelligence for strategic decisions in evolving markets. Headquartered in Denver, Centiment conducts research globally to help organizations understand complex technology landscapes and cybersecurity trends.

Kiteworks

October 2025

www.kiteworks.com