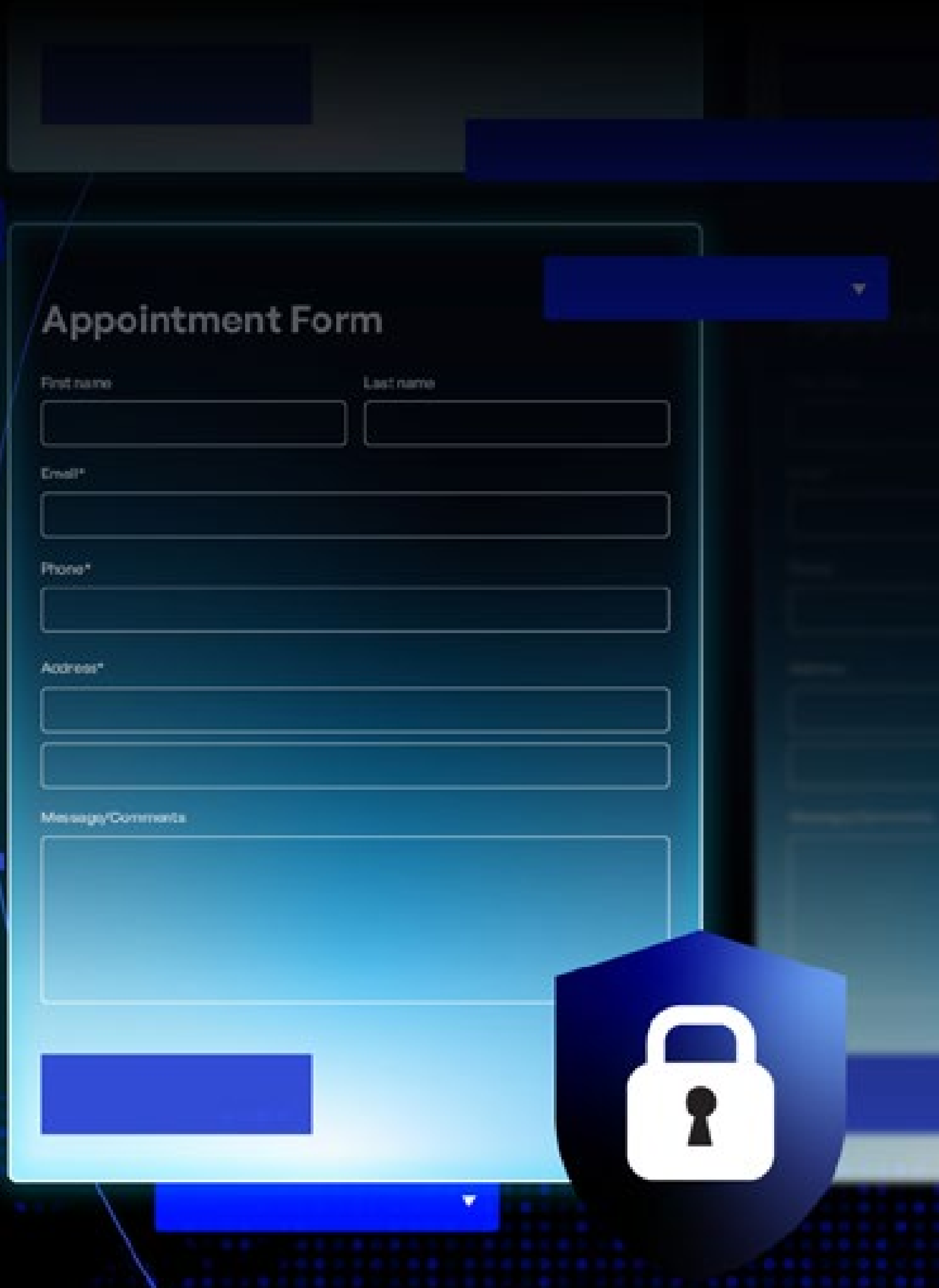
Kiteworks

REPORT

Data Security and Compliance Risk: 2025 Data Forms Survey Report

Stop Using Web Forms.
Start Using Secure Data Forms.



www.kiteworks.com

Contents.

Enter your full name:

Executive Summary

This report analyzes responses from **324 cybersecurity, risk, IT, and compliance professionals** on how organizations secure web forms and handle data sovereignty. The data shows a clear gap between confidence and reality. **48%** of organizations say they have advanced security. **88%** still experienced at least one web form-related security incident in the past two years.

Web forms now sit at the center of sensitive data collection. They capture financial records, health information, login credentials, and employee data. When forms are not properly secured, you **expose that data** at the point where it first enters your environment:

44% of respondents reported a confirmed data breach through form submissions

61% faced bot or automated attacks

47% faced SQL injection

39% faced cross-site scripting

These rates stay high even though most organizations report using web application firewalls, server-side validation, and parameterized queries.

Data sovereignty is now a requirement:

85% of respondents say data sovereignty is critical or very important

92% must comply with GDPR

58% must comply with PCI DSS

41% must comply with HIPAA, and in healthcare that figure reaches **97%**

Government, financial services, and healthcare also face their own sector rules. Because of this, organizations want clear control over where form data is stored and processed. They expect deployment options that let them keep data in specific regions and meet residency laws, not just general "cloud" hosting.

Spending and timelines reflect this urgency: Most organizations are planning form-security upgrades in the next six months and are already committing six-figure annual budgets to these projects.

Recent security incidents are the top driver behind project spending. New regulations, customer requirements, and board or executive mandates are close behind. Even with these budgets, **72%** still list budget constraints as a barrier because form security competes with other security initiatives. **58%** say they lack internal expertise, which slows deployment and leaves protection uneven across their forms.

Risk is not uniform. Some industry sectors are more exposed.

Financial services handle the broadest mix of sensitive data with the most complex regulatory stack. Almost all financial services respondents report GDPR and PCI DSS requirements, and **93%** say data sovereignty is critical or very important. They also report some of the highest adoption for ISO 27001, SOC 2 Type II, and PCI certification.

Healthcare collects protected health information on almost every form. It must satisfy HIPAA in the U.S. and GDPR where it handles European resident data. That combination raises the bar for encryption, audit trails, consent management, and strict data residency.

Government often requires FedRAMP, FIPS 140-3, and CMMC 2.0. **75%** of government respondents say data must stay within national borders. This creates a hard access barrier for vendors that cannot meet federal certification and residency expectations.

Patterns are consistent across organization size. Data sovereignty is a high priority in every size band, from 500 employees to over 20,000. Incident rates also stay high. Smaller organizations face the same regulatory and sovereignty pressures as large enterprises, but with fewer people and less time.

Decision-making is shared across roles. IT focuses on integration and deployment. Security teams look at depth of controls, coverage across all forms, and incident response. Risk teams consider financial impact and regulatory exposure. Compliance and legal teams validate alignment with frameworks and audit needs. If you want to win this buyer group, you need to show how your approach meets all four views without adding operational drag.

If you want to reduce risk from web forms, you have a focused set of actions:

1. **Bring all forms into scope**, including legacy, embedded, public, and mobile. Apply one security and compliance standard across them.
2. **Encrypt data** from submission through storage and processing. Use field-level encryption and tight access controls so only the right users and systems can see sensitive fields.
3. **Enforce data residency** with deployment options such as SaaS, hybrid, on-premises, private cloud, and government cloud that match regional and sector rules.
4. **Combine real-time detection with automated incident response** to shorten the time from alert to containment and reduce the chance that incidents become full breaches.
5. **Automate compliance evidence.** Capture logs, audit trails, configuration changes, and data flows in a way that maps to GDPR, PCI DSS, HIPAA, SOX, CMMC, and state privacy laws, so audits require less manual effort.
6. **Explain value in risk and effort terms.** Show how these steps lower breach probability, reduce audit workload, and shrink regulatory exposure, rather than just listing technical features.

Web forms are no longer simple front ends. They are core infrastructure for sensitive data intake. When you secure them consistently, you lower breach risk, improve your compliance standing, and reduce the chance that attackers use them as a quiet entry point into your environment.

Key Takeaways

88 % experienced web form security incidents

44 % suffered breaches via form submissions

85 % say data sovereignty is critical or very important

71 % plan implementation or upgrades within 6 months

83 % have annual budgets of $100k or more

Table 1: KPIs for Web (Data) Forms

Metric	Value	Definition
Incident prevalence	**88%**	Organizations that experienced at least one web form-related security incident in the past 24 months.
Breach via forms	**44%**	Organizations that suffered a confirmed data breach through form submissions.
Bot attacks	**61%**	Organizations targeted by automated or bot-driven attacks against web forms.
SQL injection	**47%**	Organizations that experienced SQL injection attempts or incidents.
Cross-site scripting (XSS)	**39%**	Organizations that encountered XSS attacks targeting form fields.
Data sovereignty rated “critical” or “very important”	**85%**	Organizations that require or strongly prefer geographic control over where form data is stored and processed.
GDPR applicability	**92%**	Organizations subject to GDPR requirements based on the data they collect.
Annual budget ≥$100k	**83%**	Organizations allocating at least $100,000 per year to web form security.
Implementation timeline ≤6 months	**71%**	Organizations planning to implement or upgrade form security controls within six months.
Automated incident response	**48%**	Organizations wthat use automated response workflows after detecting form-related threats.

SECTION 1

Threat Landscape: Data Breaches & Attacks

1.1 Incident Prevalence and Attack Vectors

Incidents are the norm, not the exception. Across the sample, **88%** of organizations had at least one web form-related security incident in the past 24 months. That includes attempted attacks, successful compromises, and confirmed data breaches.

The top attack types are:

61 %	Bot and automated attacks
47 %	SQL injection
44 %	Data breaches through form submissions
39 %	Cross-site scripting (XSS)
28 %	Session hijacking
21 %	Man-in-the-middle (MITM) attacks

These numbers sit alongside high adoption of common controls:

89 %	Web application firewalls (WAF)
92 %	Server-side validation
82 %	Parametized queries
76%	Input sanitation

The gap between control adoption and attack rates tells us three things:

1. **Coverage is uneven.** Controls exist at the platform level, but not every form uses them consistently, especially legacy, embedded, or department-owned forms.
2. **Attackers target weak points.** They aim at older forms, poorly maintained endpoints, and public-facing flows that sit outside central governance.
3. **Controls are not backed by strong response. 82%** have real-time detection, but only **48%** have automated response. Detection without response leaves a long window for attackers to work.

Bot and Automated Attacks

61% of organizations report bot or automated attacks against forms. These attacks:

- Flood login, registration, and contact forms with malicious traffic
- Probe for weak validation and rate limits
- Attempt credential stuffing, fake account creation, or spam injection

WAFs help, but many rules are tuned for traditional application attacks, not the volume and behavior patterns of modern bots. Where organizations lack rate limiting, device fingerprinting, or behavioral signals, bot attacks slip through.

SQL Injection and Input Abuse

47% of organizations report SQL injection. This happens even though most say they use server-side validation and parameterized queries. The likely reasons:

- Legacy forms still use string concatenation or weak validation
- Only some back-end services have adopted parameterized queries
- Third-party or embedded forms connect to systems that are not fully modernized

Input abuse extends beyond SQL:

39% report XSS, where attackers inject scripts into form fields that later execute in a user's browser

28% report session hijacking, often tied to weak session handling or insecure cookies

21% report MITM attacks, which show up where TLS is misconfigured or where endpoints lack certificate pinning, especially on mobile

Data Breaches Through Form Submissions

44% of organizations suffered a confirmed data breach through form submissions. That matters because of what these forms collect:

70% collect employee data

66% collect financial records

65% collect customer authentication credentials

Many collect government ID numbers, PHI, and payment card details

When attackers compromise a form flow, they often gain direct access to these data types without needing to pivot deeper into the network.

1.2 Business Impact Analysis

When respondents rank the impact of form-related incidents, five areas stand out.

1. Financial Loss

37% rank financial loss as a **catastrophic** impact. This aligns with external data showing multi-million-dollar breach costs. Financial loss includes:

- Incident response and forensics
- Legal and regulatory costs
- Customer notification and credit monitoring
- System remediation and hardening

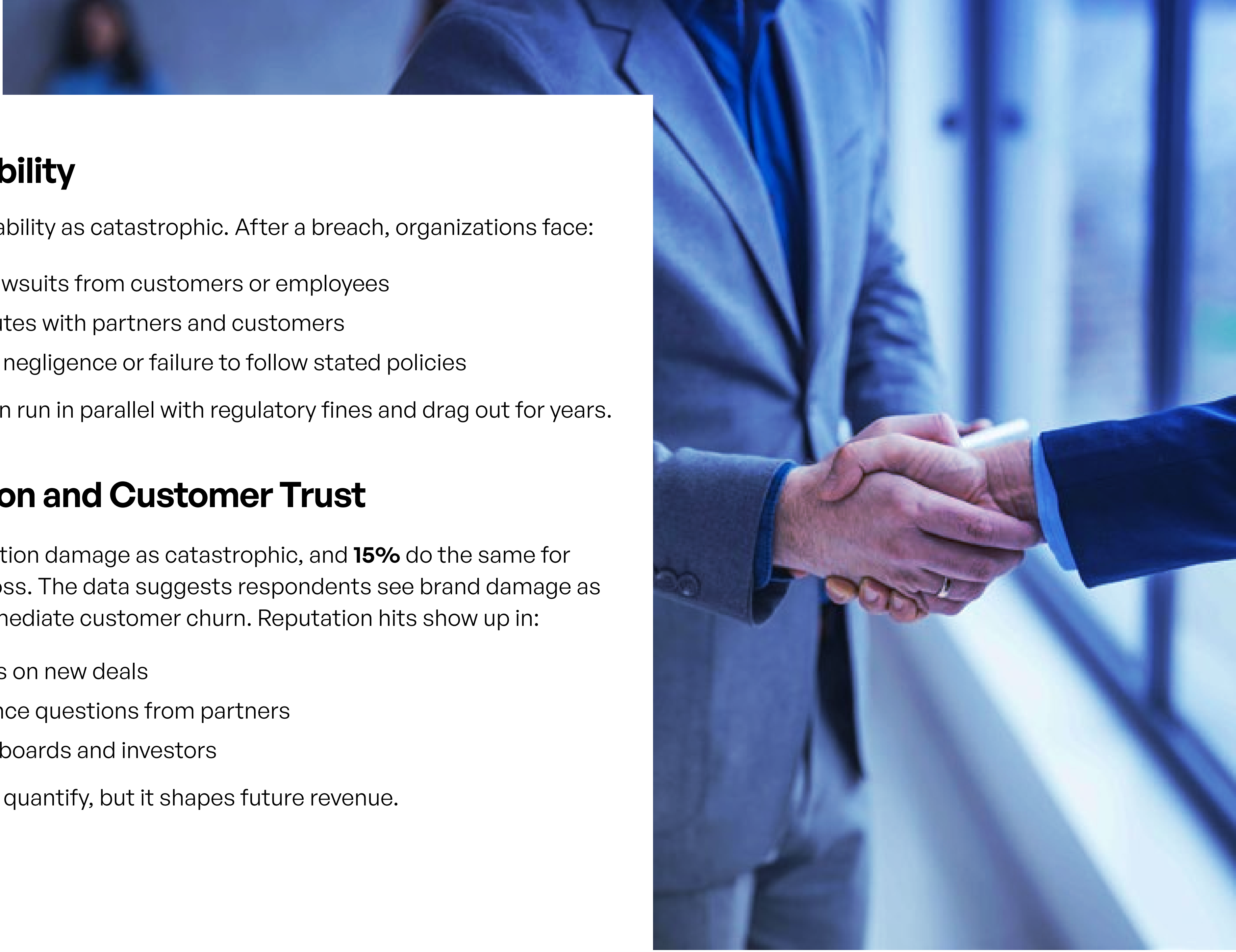
For boards and CFOs, this is the most visible damage.

2. Regulatory Penalties

26% rank regulatory penalties as catastrophic. With **92%** under GDPR, **58%** under PCI DSS, and **41%** under HIPAA (97% in healthcare), form-related breaches expose organizations to:

- Fines tied to global revenue (GDPR)
- Per-record penalties and PCI noncompliance costs
- Sector-specific sanctions or loss of certification

Because many forms collect regulated data, penalties are not a theoretical risk.



3. Legal Liability

23% rank legal liability as catastrophic. After a breach, organizations face:

- Class-action lawsuits from customers or employees
- Contract disputes with partners and customers
- Claims around negligence or failure to follow stated policies

These costs often run in parallel with regulatory fines and drag out for years.

4. Reputation and Customer Trust

20% rank reputation damage as catastrophic, and **15%** do the same for customer trust loss. The data suggests respondents see brand damage as broader than immediate customer churn. Reputation hits show up in:

- Lower win rates on new deals
- Tougher diligence questions from partners
- Pressure from boards and investors

Trust is harder to quantify, but it shapes future revenue.

5. Operational Disruption

Only **9%** rank operational disruption as catastrophic. **29%** say the impact is minimal. Most breaches do not shut the business down, but they do:

- Consume security, IT, and legal resources
- Delay projects and security initiatives
- Force unplanned system changes and manual workarounds

The sustained cost is more about ongoing monitoring, reporting, and compliance work than short-term outages.

Table 2: Impact Severity Distribution

Impact Dimension	Catastrophic	High	Medium	Low	None
Financial loss	**37%**	34%	**20%**	**7%**	2%
Regulatory penalties	**26%**	33%	**27%**	**10%**	4%
Legal liability	**23%**	32%	**30%**	**11%**	4%
Reputation damage	**20%**	31%	**32%**	**14%**	3%
Customer trust loss	**15%**	29%	**35%**	**17%**	4%
Operational disruption	**9%**	23%	**31%**	**29%**	8%

1.3 Industry-Specific Threat Profiles

The attack types are similar across industries, but some sectors are more attractive targets because of the data they collect and the regulations they face.

Financial Services

Financial services account for **36%** of the sample and show the highest risk profile:

90% collect financial records

85% collect employee data

83% handle payment card information

79% collect authentication credentials

They also face the tightest regulatory stack:

98% under GDPR

90% under PCI DSS

Finally, they also have high exposure to SOX and state privacy laws.

As a result, financial services organizations experience frequent targeting and high stakes when incidents occur. A single form breach can trigger both regulatory action and significant financial loss.

Healthcare

Healthcare represents about **10%** of the sample but carries unique risk:

- **97%** collect protected health information (PHI) through forms
- Nearly all must meet HIPAA, and **90%** must also meet GDPR

Healthcare forms often support patient intake, referrals, lab orders, insurance, and clinical workflows. A breach at the form layer exposes PHI and creates complex notification and remediation requirements. The mix of PHI, regulatory pressure, and often older infrastructure makes these organizations prime targets.

Government

Government respondents make up **5%** of the sample but operate under the strictest assurance requirements:

81 % collect government ID numbers

75 % require FedRAMP for cloud services

69 % require FIPS 140-3-validated cryptography

Not surprisingly, a significant number indicated they fall under CMMC 2.0 compliance requirements.

Here, form security is tied directly to national security and citizen trust. A form breach can expose sensitive citizen data, create attack paths into government systems, and undermine public confidence.

Other Sectors

Technology, manufacturing, energy, and professional services also collect high-value data (IP, credentials, trade secrets) and face a mix of GDPR, PCI, state laws, and industry-specific rules. Their risk is more distributed but still significant. Attackers treat them as attractive targets because they often act as suppliers or partners to more regulated sectors.

Table 3: High-Risk Data Types Per Industry

Data Type	Finance	Technology	Manufacturing	Healthcare	Government
Financial records	90%	62%	58%	40%	52%
Authentication credentials	79%	68%	61%	55%	64%
Protected health information (PHI)	8%	4%	3%	97%	6%
Government ID numbers	42%	34%	29%	38%	81%
Payment card data	83%	41%	36%	22%	30%

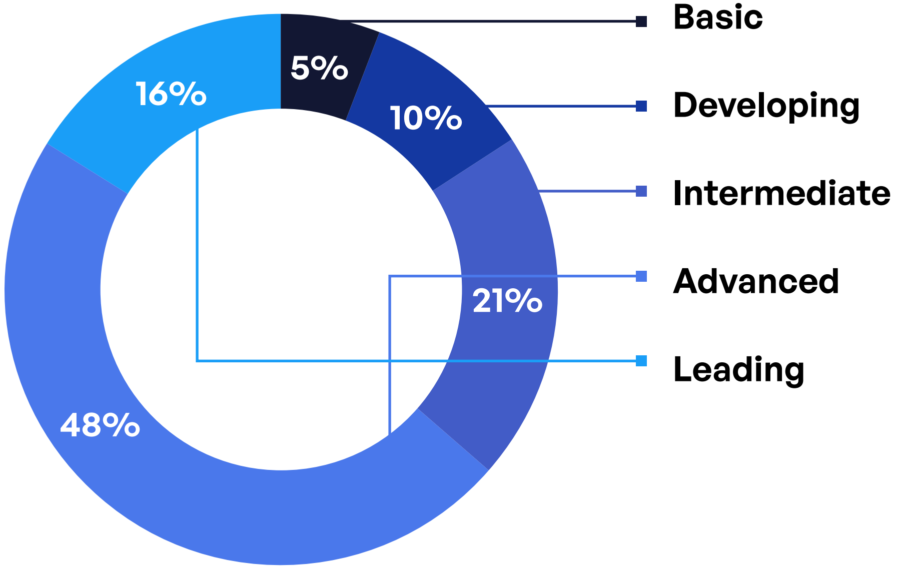
SECTION 2

Governance Controls & Tracking

This section looks at how organizations describe their security maturity, how that lines up with actual incident rates, and how well they monitor, validate, and control access to their web forms.

2.1 Security Maturity vs. Reality

Respondents place themselves high on the maturity curve:



Over **one-third** say they are at least “intermediate,” and nearly **two-thirds** indicate they are “advanced” or “leading.” Yet **88%** still report at least one form-related security incident in the last two years.

When you look at incidents by maturity band, the drop is modest:

Basic:	95% experienced incidents
Developing:	92%
Intermediate:	90%
Advanced:	87%
Leading:	83%

Higher maturity helps, but not nearly as much as the self-assessment labels suggest. Many organizations have deployed the right categories of controls but have not achieved consistent coverage across all forms, or they lack automation in detection and response.

Table 4: Security Maturity and Risk Ratio

Maturity Band	Incident Rate	Odds Ratio vs. Basic
Basic	95%	1.0
Developing	92%	0.7
Intermediate	90%	0.6
Advanced	87%	0.5
Leading	83%	0.4

These ratios show that "advanced" and "leading" programs do reduce risk compared to "basic," but nowhere near to the level their labels imply. Even in the "leading" group, more than four out of five organizations still experience form-related incidents.

2.2 Monitoring and Response Capabilities

Monitoring controls are widely deployed:

89 % Web application firewall (WAF)

82 % Real-time threat detection

76 % Security information and event management (SIEM)

69 % Regular security audits

61 % Penetration testing

The drop-off comes at **automated incident response,** which only **48%** have in place. So about **34%** have real-time detection but still rely on manual response, and **18%** have neither.

This creates a “detection without orchestration” gap. These organizations see attacks in near real time but still depend on tickets, emails, and manual handoffs to contain them. That delays containment and increases the chance that a probing attack turns into a breach.

In the data, organizations with both real-time detection and automated response report:

- Slightly lower overall incident rates
- Noticeably lower breach-through-forms rates
- Shorter time to contain incidents (based on qualitative responses where time-to-respond is not captured as a numeric metric)

Table 5: Detection Without Orchestration Gap

Cohort	Share of Organizations	Incident Rate	Breach via Forms
Real-time detection and automated response	48%	84%	40%
Real-time detection only (no automated response)	34%	90%	48%
No real-time detection	18%	95%	52%

The pattern is clear: detection helps but pairing it with automated response cuts both incident frequency and breach conversion.

2.3 Input Validation and Sanitization

Most organizations report strong validation practices:

92%	Server-side validation
82%	Parameterized queries
76%	Input sanitization
58%	Regular expression patterns
48%	Allowlist validation

Concerning responses:

30%	Client-side validation only
11%	Not sure which methods are used
4%	No validation implemented

Despite these adoption levels, **47%** still report SQL injection attacks, and **39%** report XSS. That suggests incomplete rollout, inconsistent use across all services, or weak validation rules.

Validation gaps are most visible in:

- Legacy forms that were built before current standards
- Public forms used for marketing or lead capture
- Embedded forms that pass data into older back-end systems
- Mobile flows where client-side logic is heavier and server checks are thinner

Here, “authorized” forms require user authentication (e.g., customer or employee logins), while “public” forms are accessible without authentication.

Table 6: Validation Adoption by Form Type

Validation Control	Public	Authorized	Mobile	Legacy
Server-side validation	78%	94%	86%	62%
Parameterized queries	69%	88%	78%	54%
Input sanitization	72%	82%	75%	57%
Regex-based validation	55%	63%	59%	41%
Allowlist validation	43%	52%	46%	35%
Client-side only	37%	18%	29%	42%

This table shows why SQLi and XSS are still common. The weakest validation appears on public and legacy forms, where attackers focus their efforts.

2.4 Authentication and Access Controls

Authentication controls on forms are strong overall:

89%	Multi-factor authentication (MFA)
61%	Username/ password only
41%	Risk-based authentication
9%	Public forms with no authentication
72%	Single sign-on (SSO)
48%	Biometric authentication
35%	Hardware security keys

These numbers suggest organizations are layering modern identity controls on top of many form flows, especially high-value ones. But password-only forms still exist in large numbers, and some public forms remain completely open.

Session hijacking rates illustrate the difference:

- Organizations that rely heavily on **password-only** or **no-auth** flows report the highest session hijacking rates.
- Those that combine **MFA, risk-based authentication,** and **hardware keys** report lower rates, especially on admin or high-value flows.
- Biometric authentication helps on mobile forms where users can authenticate frequently without friction.

Table 7: Authorization Control Presence vs. Session Hijacking Rate

Authorization Profile	Approximate Share of Organizations	Session Hijacking Rate
Password-only dominant (few or no MFA deployments)	15%	32%
Mixed (MFA present, but many password-only flows)	46%	28%
Strong auth (MFA + SSO; limited password-only)	30%	24%
Advanced (MFA + risk-based + hardware keys on sensitive flows)	9%	20%
Public/no-auth forms only (for specific low-risk use cases)	9%	35%

The pattern is straightforward: As organizations move from password-only toward layered, adaptive authentication, session hijacking rates fall. Where public or unauthenticated forms carry sensitive data, hijack rates are highest.

SECTION 3

Data Compliance & Privacy

This section looks at the regulatory frameworks with which organizations must comply, the challenges they face when managing those requirements, and the growing pressure around data sovereignty and security certifications.

3.1 Regulatory Framework Landscape

Most organizations operate under multiple overlapping regulations. The three with the widest reach are:

92 % GDPR

58 % PCI DSS

41 % HIPAA

Other frameworks follow:

37 % CCPA/CPRA

27 % SOX

30 % State-specific privacy laws

24 % International residency laws

21 % Industry-specific rules

14 % CMMC 2.0

But much higher in defense and government supply chains

This mix makes compliance a central factor in how organizations design, secure, and govern their web forms. With so much sensitive data entering through forms, compliance failures at the form level often become enterprise-wide problems.

Table 8: Security Framework Coverage

Framework	Percent of Organizations Required to Comply
GDPR	92%
PCI DSS	58%
HIPAA	41%
CCPA/CPRA	37%
SOX	27%
State laws	30%
Residency laws	24%
Industry-specific rules	21%
CMMC 2.0	14%

3.2 Compliance Challenges Ranking

When asked to rank their top compliance challenges, respondents show a clear order:

Data sovereignty and residency requirements (ranked #1 by 28%)

Maintaining audit trails and documentation (ranked #1 by 21%)

Data retention and deletion policies (ranked lowest overall)

User consent management

Cross-border data transfer compliance

The high ranking of sovereignty and audit trails reflects growing scrutiny from regulators, customers, and partners. Organizations face steep consequences when they cannot prove where data lives, who accessed it, or whether controls remained in place.

Table 9: Top Compliance Challenges (Ranked #1)

Challenge	Percent Ranking #1
Data sovereignty & residency	28%
Audit trails & documentation	21%
Consent management	19%
Cross-border transfers	17%
Retention & deletion	15%

3.3 Data Sovereignty Criticality

Data sovereignty has become one of the most important requirements in the entire survey:

85% say it is critical or very important

61% say it is strictly required for compliance

Only **1%** say it is not important.

Methodological note:

Unless otherwise stated, “critical” refers to respondents selecting the top response option critical only, while “critical or very important” refers to the combined share selecting *critical* or *very important.*

Across industries, government and financial services show the highest concentration of “critical” responses, reflecting the combination of regulatory pressure, national-security concerns, and the long-lived nature of the records they hold. Healthcare and public services follow closely behind, driven by patient privacy, safety concerns, and overlapping regional rules. Even in less heavily regulated sectors, sovereignty has moved from a “nice to have” to a gating requirement for form providers.

Government respondents stand out most clearly. **75%** rate data sovereignty as *critical* on its own, and **94%** rate it *critical* or *very important* overall, reflecting a strong bias toward in-country or government-cloud deployment models, strict control over encryption keys, and clear auditability of where data resides and how it moves between systems.

Data sovereignty expectations are also reinforced by the broader regulatory stack. In many cases, organizations cannot simply opt out of sovereign control requirements; they must demonstrate that citizen and customer data remains within approved jurisdictions, with appropriate controls for cross-border transfers, cloud providers, and subcontractors.

Different industries feel this pressure in different ways:

Government: 75% say sovereignty is critical (**94%** rate it "critical" or "very important" overall)

Financial Services: 69% critical, **24%** very important (**93%** combined)

Energy/Utilities: 70% critical

Healthcare: 61% critical

Technology: 65% critical

Manufacturing: 60% critical

The consistency across sectors and regions shows that residency and control over where data is stored is no longer a niche requirement. It influences architecture decisions, vendor selection, audit scope, and procurement timelines.

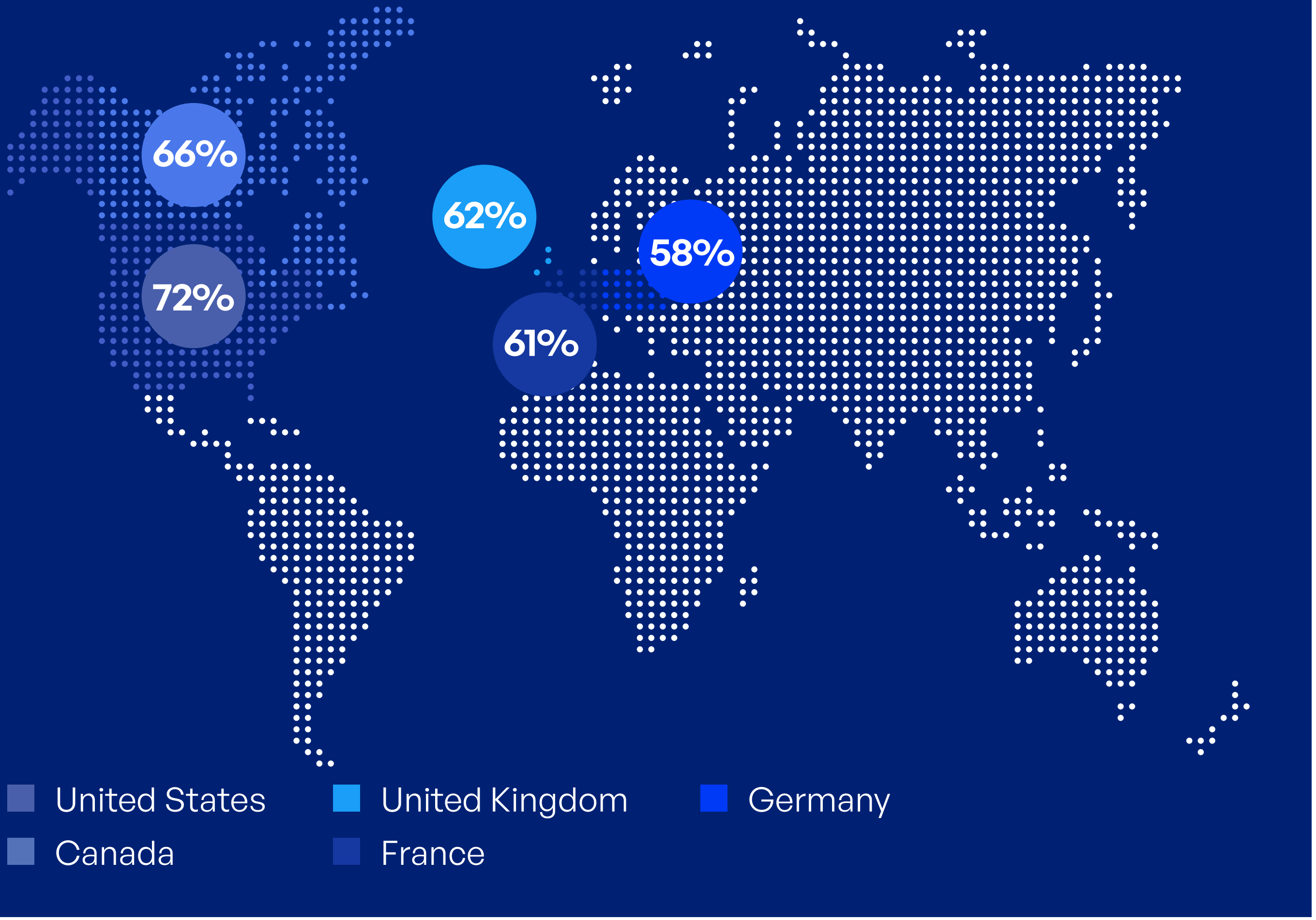
Table 10: Data Sovereignty Criticality by Industry

Industry	Critical	Very Important	Combined
Government	75%	19%	**94%**
Financial Services	69%	24%	**93%**
Energy/Utilities	70%	20%	**90%**
Healthcare	61%	22%	**83%**
Technology	65%	21%	**86%**
Manufacturing	60%	20%	**80%**

3.4 Industry Variations in Data Sovereignty

Building on the global picture in Section 3.3, sovereignty pressure intensifies in certain industries and regions, which in turn influences deployment and architecture decisions.

Regions with the highest sovereignty pressure (critical) are:



In contrast, Saudi Arabia and the UAE show lower "critical" ratings (50% to 56%) but still high combined "critical + very important" responses (83% to 86%). Their regulatory environments are still evolving but trending toward strict residency requirements.

This variation affects deployment choices:

86%	Cloud (SaaS)
65%	Hybrid
58%	On-premises
48%	Private cloud
24%	Government cloud

Key Takeaway: Most organizations need multiple deployment options to satisfy regional regulatory requirements and internal control policies.

3.5 Regional Differences in Form Risk and Compliance

While sovereignty is important everywhere, how it shows up in requirements differs by region. North American respondents report the highest density of overlapping privacy and sectoral regulations. European respondents show the most consistently "privacy-first" posture, with near-universal GDPR expectations. Respondents from countries in the Middle East report rapidly rising demands for sovereign-cloud and in-region storage, often codified through local or sectoral rules rather than a single omnibus regulation.

Table 11: Regional Differences in Data Sovereignty, Regulation, and Form Risk

Region	Example Countries	Data Sovereignty Signal	Dominant Regulatory Drivers	Form Risk & Compliance Profile
North America	United States, Canada	Very high: **~72% (U.S.)** and **66% (Canada)** rate sovereignty *critical*, with a further 21–24% calling it *very important* → >90% top two overall.	Mix of **GDPR** (for multinationals) plus **HIPAA, CCPA/CPRA, state privacy laws, PCI DSS, SOX,** and growing **CMMC 2.0** impact in the U.S.	Programs must reconcile EU-style privacy with sector-specific U.S. security mandates; form security is pulled in multiple directions at once.
Europe	U.K., Germany, France	High and broadly distributed across *critical* and *very important* (e.g., Germany **~58% critical, 26% very important).**	Near-universal **GDPR** (mid-90%+), strong **PCI DSS,** and SOX/ CCPA where applicable to global operations.	Most consistently "privacy-first"; sovereignty framed as both compliance obligation and competitive differentiator.
Middle East	Saudi Arabia, UAE	High but more mixed: e.g., Saudi respondents report around **50% critical, 33% very important.**	Lower explicit GDPR penetration, but rapidly increasing emphasis on **international data residency** and local laws; rising use of sovereign and government clouds.	Fast-moving shift toward "keep data in-region, under local control," with form projects increasingly tied to sovereign-cloud and residency guarantees.

North America: Multi-Regime Pressure

North American organizations live in a multi-regime world. U.S. and Canadian respondents must simultaneously account for:

- EU rules via **GDPR** (for multinationals and EU-facing services)
- Federal and state privacy laws such as **HIPAA** and **CCPA/CPRA**
- Sectoral and financial controls such as **PCI DSS** and **SOX**
- Emerging security and compliance mandates like **CMMC 2.0** for defense and contractor ecosystems

On data sovereignty, the signal is clear. In the United States, around **72%** of respondents rate data sovereignty as *critical* and a further ~21% as *very important*. In Canada, **66%** call it *critical*, with ~24% *very important*. In both countries, more than **90%** of respondents fall into the top two categories.

As a result, form modernization projects in North America are rarely driven by a single regulation. Instead, they must reconcile EU-style privacy baselines, sector-specific U.S. requirements, and state-level rules. This creates strong demand for:

- Flexible deployment and residency models
- Transparent audit trails for cross-border data flows
- Controls capable of satisfying both privacy and security auditors without duplicating infrastructure

Europe: Privacy-First, Compliance-Heavy

European respondents show the most consistently “privacy-first” posture in the dataset. Across the U.K., Germany, and France, **GDPR** is effectively universal, and is often paired with:

- **PCI DSS** for payment-related workflows
- SOX-style controls for listed entities and financial reporting
- Additional national or sectoral rules for healthcare, public services, and critical infrastructure

Data sovereignty expectations remain high but are more evenly distributed between *critical* and *very important*. For example, German respondents report around **58%** *critical* and ***26%*** *very important* for data sovereignty, yielding a strong top two signal without concentrating all demand at the very top of the scale.

In practice, this means European form programs:

- Treat privacy and sovereignty as default design constraints, not optional add-ons
- Put greater emphasis on data minimization, purpose limitation, and explicit consent
- Expect clear, documented controls for data transfers outside the EU/EEA and U.K.

Data sovereignty is framed not only as a regulatory obligation but also as a competitive factor—particularly for public-sector and financial institutions marketing “trusted” digital services.

Middle East: Sovereign-Cloud and Local Control

Respondents from Middle East countries such as Saudi Arabia and the UAE report sovereignty expectations that, while slightly less concentrated in the *critical* bucket, still skew heavily toward the top two response options. In Saudi Arabia, roughly ***50%*** rate sovereignty *critical* and ***33%*** *very important*—a strong signal even in the absence of a single omnibus regulation akin to GDPR.

The regulatory landscape here looks different:

- **GDPR** still applies for multinationals and EU-facing services, but less uniformly
- Local laws and sectoral rules increasingly emphasize **in-region storage** and **local control**
- Governments and regulators are promoting **sovereign-cloud** and government-cloud offerings, particularly for public-sector and critical services

As a result, modern form programs in the Middle East region are rapidly aligning with:

- Sovereign- or government-cloud deployment models
- Clear guarantees that sensitive citizen and customer data remain in-region
- Stronger controls over encryption keys, identity, and access, often tied to national-security and economic-sovereignty objectives

In short, Middle East respondents are moving quickly toward “keep data in-region, under local control.” The requirements may be less codified in a single framework than GDPR, but the direction of travel is unmistakable—and web and data forms are increasingly part of that sovereign-cloud strategy.

SECTION 4

Maturity of Advanced Security & Governance Programs

This section looks at how organizations implement high-assurance security controls, encryption standards, authentication maturity, continuous monitoring, and governance capabilities. These controls represent the “upper tier” of form security—features that go beyond basic hardening and directly support compliance, resilience, and risk reduction.

4.1 Federal and Government-Grade Security Requirements

Some certifications sit above standard enterprise expectations. They are often required in government, defense, or critical infrastructure environments.

FIPS 140-3

48% of respondents use FIPS 140-3-validated cryptographic modules. Adoption varies by sector:

69%	Government
59%	Financial Services
32%	Healthcare
27%	Technology

FIPS validation ensures that encryption modules meet U.S. federal requirements and are tested against tampering, side-channel attacks, and other cryptographic risks.

FedRAMP Authorization

30% of respondents require FedRAMP for form workflows. In government, that number jumps to **75%.**

This includes:

- FedRAMP Low and Moderate for general workloads
- FedRAMP High for law enforcement, emergency services, and other high sensitivity use cases

FedRAMP often determines which cloud services can be used at all, and forms part of procurement decisions.

CMMC 2.0

14% of respondents fall under CMMC 2.0 requirements. That number is highest in defense, aerospace, and manufacturing supply chains.

CMMC influences:

- How forms collect and store controlled unclassified information (CUI)
- Encryption and audit logging requirements
- Access controls and identity enforcement
- Vendor approval processes

Why These Standards Matter

Organizations subject to these frameworks face stricter audit cycles, stricter cryptographic requirements, and strict enforcement of data residency and access controls. These requirements also cascade down to contractors, suppliers, and partners.

4.2 Encryption Standards and Implementation

Encryption is a cornerstone of protecting data at rest and in transit. Adoption is high, but gaps remain.

Transport Layer Encryption

- **TLS 1.3:** 81%
- **TLS 1.2:** 48%
- Older TLS versions should not be in use for regulated workloads.

End-to-End Encryption

67% of organizations encrypt form data from submission through storage and processing. This prevents intermediaries—reverse proxies, load balancers, form plugins—from accessing plaintext data.

Encryption at Rest

- **AES-256:** 58% adopt strong encryption for stored form data.
- Some organizations rely on cluster-level encryption only, which leaves gaps around logs, backups, and field-level data.

Field-Level Encryption

41% encrypt individual form fields separately. This reduces the blast radius of compromise and supports principle of least privilege.

Concerning Patterns

- **9%** are unsure which encryption standards they use.
- **4%** report no encryption.

These are unacceptable gaps for organizations collecting credentials, financial records, or health information.

4.3 Security Capabilities Priority Ranking

Respondents rated advanced security capabilities by importance. The results show a divide between what organizations value and what they implement.

Ranked Most Important (Top 3):

1. **32%:** Military-grade encryption (FIPS 140-3)
2. **28%:** Data sovereignty controls
3. **Strongest #3 ranking:** Automated compliance monitoring

Ranked Least Important:

Enterprise integrations: lowest criticality

Audit trail automations: lowest #1 ranking

Real-time threat detection: seen as table stakes rather than a differentiator

Zero-trust architecture: low prioritization despite industry consensus

This mismatch is consistent across industries: Organizations value encryption and residency most, while underestimating the long-term value of automating compliance and audit workloads.

Table 12: Capability Priorities (Rank #1)

Capability	Rank #1 Responses
Military-grade encryption	32%
Data sovereignty controls	28%
Automated compliance monitoring	19%
Zero-trust architecture	12%
Multi-deployment options	6%
Real-time threat detection	3%
Audit trail automation	1%
Enterprise integrations	1%

4.4 Security Standards Criticality

Respondents rated specific standards on a six-point scale.

Rated "Critical":

23 %	FIPS 140-3
23 %	Certificate pinning (mobile)
18 %	Zero-trust architecture
16 %	MFA

Rated "Not Important":

24 % MFA

23 % Real-time threat monitoring

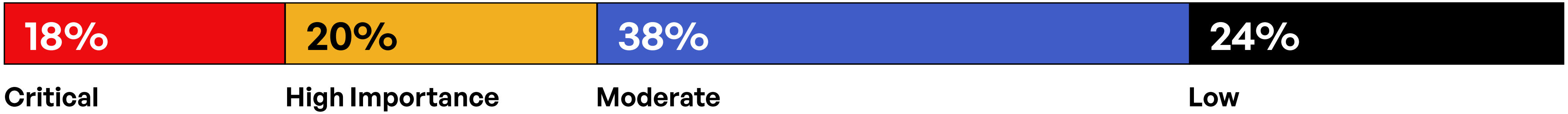
14 % Zero trust

These numbers show that:

- MFA and monitoring are widely adopted but not viewed as advanced differentiators.
- FIPS and mobile certificate pinning appeal to niche but important segments.
- Zero trust is poorly understood, poorly prioritized, or both.

4.5 Zero-Trust Architecture Adoption

Zero-trust adoption sits below what you see in other security domains:



The low “critical” rating contradicts broader industry guidance. Most organizations say they plan to adopt zero trust “in the future,” but do not list it as a current requirement for form infrastructure. As noted in Section 4.4, only **18%** rate zero-trust architecture as “critical,” and Table 11 shows just **12%** ranking it as their number one capability priority, reinforcing how far perception lags behind industry guidance.

Organizations that treat zero trust as a priority tend to:

- Have experienced form-related breaches
- Handle high-value data (financial, government IDs, PHI)
- Operate in cloud-first environments
- Support large remote workforces
- Serve regulated markets

Table 13: Integration Capabilities Ranked Critical

Integration Feature	Critical Rating
API flexibility	38%
Webhook support	27%
Security tool integrations	26%
Enterprise connectors	23%
Legacy compatibility	17%

SECTION 5

Operational Realities: Mobile, Budgets, Ownership, & Scale

This section covers patterns that cut across the entire dataset: mobile submissions, implementation strategy, investment levels, ownership, form usage scale, and the barriers that slow progress. These factors shape how organizations plan, deploy, and operate secure form infrastructure.

5.1 Mobile Security Considerations

Web forms are no longer used primarily on desktops. For many organizations, mobile is now the dominant entry point for sensitive data.

- **71%** of organizations receive **21%** to **60%** of all form submissions from mobile devices.
- **41%** fall in the **41% to 60%** range, making mobile their largest intake channel.

Despite this, mobile-specific security controls lag:

- **Certificate pinning:** Only **23%** rate it as critical.
- **Biometric authentication:** adopted by **48%** but rarely enforced on high-risk flows.
- **Mobile-specific TLS validation:** inconsistent across industries.

This mismatch shows that many organizations secure desktop workflows well but leave mobile flows under-protected. Attackers often target mobile-heavy forms—such as customer identity verification, password reset flows, benefits enrollment, and service portals—because they combine sensitive data with weaker client defenses.

5.2 Implementation Strategy and Timeline

Organizations are moving fast. **71%** plan to implement or upgrade form security in **six months or less:**

30 % within **3 months**

41 % within **3–6 months**

29 % beyond **6 months**

This pace is driven by:

82 % recent security incidents	**69 %** customer and partner demands
76 % new or expanding regulatory requirements	**61 %** board or executive directives

These numbers confirm that form security is no longer treated as a low-priority IT task. It is a compliance and risk-driven initiative with executive visibility.

Implementation Approaches

Respondents use three main approaches:

Hybrid rollout: 48%
Add new secure forms while maintaining some existing ones.

Pilot → scale: 30%
Test with one business unit, then expand.

Full replacement: 14%
Replace all forms with a unified platform.

Ad hoc upgrades: 8%
Fix forms individually, often without long-term governance.

The hybrid model dominates because most organizations operate hundreds or thousands of forms across many teams.

5.3 Investment and Budget Allocation

Organizations put significant budget into securing forms:

83% allocate at least **$100,000** per year

48% allocate **$250,000 or more**

21% exceed **$500,000** in annual spending

Financial services and technology companies represent the largest share of high-budget respondents, but even organizations with **500–999 employees** allocate six-figure budgets.

Budget constraints remain a challenge despite high spending:

72% list budget limitations as a barrier

48% cite technical complexity

58% cite lack of expertise

41% cite legacy system limitations

This shows that money exists, but stakeholders struggle to justify spend across competing security projects. Clear ROI, reduced audit workload, and faster response times are often the deciding factors.

5.4 Organizational Ownership and Decision-Making

Ownership for web forms is distributed:

85 %	IT	24 %	Operations	18 %	Marketing
26 %	Finance	22 %	HR	11 %	Sales

This spread highlights the challenge: Forms are built and maintained everywhere, but security is often centralized. Without governance, departments launch forms that do not meet security or compliance standards.

Decision-makers:

41%	Managers	30%	Directors	14%	VPs	9 %	C-Suite

Even in smaller organizations, decisions involve multi-role buying committees. Security, IT, privacy, risk, and legal often collaborate because form security touches all their domains.

5.5 Form Usage Patterns and Scale Requirements

Form volume varies widely:

35% of forms receive fewer than **10 submissions**

30% receive **11–100**

17% receive **101–500**

4% receive **5,000+**

The rest fall in mid-range buckets

Low submission volume does not mean low risk. Forms with fewer than 10 submissions often collect:

Financial records

Authentication credentials

Employee data

Government ID numbers

Attackers also target this “long tail” because:

- Security controls are often weaker
- Ownership is spread across departments
- Oversight is inconsistent

Sensitive data on low-volume forms is one of the clearest blind spots in the survey.

5.6 Barriers and Implementation Challenges

Respondents list several reasons that form security improvements are slow or uneven:

72%	Budget constraints
58 %	Lack of internal expertise
41%	Legacy system limitations
65%	Competing security policies
48 %	Technical complexity
35 %	Change management issues

These barriers reflect **two recurring themes:**

1. Many organizations want to improve form security but lack centralized governance.
2. Upgrading form security often requires touching older systems that are hard to modernize.

SECTION 6

Industry-Specific Deep Dives

This section highlights the industries with the strongest patterns in the dataset. Each industry shows distinct combinations of data sensitivity, regulatory pressure, attack exposure, and maturity gaps. These differences drive how organizations prioritize security, compliance, and sovereignty requirements in their form infrastructure.

6.1 Financial Services

Financial services face the highest overall risk because of the volume and sensitivity of data they collect and the regulatory environment they operate in.

Data Collected

90% collect financial records

85% collect employee data

83% collect payment card information

79% collect authentication credentials

78% collect PII across multiple workflows

Forms include onboarding, loan applications, KYC/AML flows, account updates, trading operations, and partner data exchanges.

Regulatory Requirements

98% must comply with GDPR

90% must comply with PCI DSS

62% with CCPA/CPRA

52% with SOX

41% with state-level privacy laws

Financial institutions also face internal audit requirements, vendor risk assessments, and third-party governance expectations.

Attack Landscape

- High targeting by bots, credential abuse, and SQL injection
- Attackers focus on authentication flows, payment forms, and identity verification portals
- Third-party and legacy forms are common weak points

Sovereignty and Certifications

- **93%** rate data sovereignty as critical or very important
- High adoption of ISO 27001, SOC 2 Type II, PCI DSS
- FIPS 140-3 adoption is higher than average because of cryptographic requirements in payment and trading systems

Key Takeaways

Financial services operate under the most intense regulatory scrutiny. Secure storage, encryption, auditability, and residency are non-negotiable. The sector leads in maturity on paper but still reports high attack and breach rates due to inconsistent coverage across older form flows.

6.2 Technology

Technology companies represent the second-largest segment. Their challenges stem from scale, speed, and global exposure.

Data Collected

- Mix of customer data, product telemetry, employee information, and authentication credentials
- Less likely to collect financial or PHI data, but heavily reliant on SaaS-based forms and distributed architectures

Regulatory Requirements

94% report GDPR applicability

72% report PCI applicability when handling payments

High exposure to state privacy laws and international data residency restrictions

Attack Landscape

- Frequent bot attacks on login and sign-up flows
- SQL injection and XSS remain common due to rapid release cycles and legacy forms embedded in older systems
- Heavy mobile usage increases risk when certificate pinning or mobile-specific controls are not implemented

Sovereignty and Certifications

- **86%** rate sovereignty as critical or very important
- ISO 27001 and SOC 2 Type II adoption are high
- Lower adoption of FIPS but growing interest in zero trust and API-based controls

Key Takeaways

Tech companies lead in automation and modern architectures, but rapid development cycles and decentralized teams increase the risk of inconsistent form security practices.

6.3 Manufacturing

Manufacturers face a unique mix of IT and OT (operational technology) challenges.

Data Collected

- Employee data
- Customer account information
- Supplier and partner data
- Less financial or PHI data, but high-value intellectual property

Regulatory Requirements

- GDPR, PCI DSS for supplier payments, and industry-specific requirements depending on sector (automotive, electronics, industrial equipment)
- Growing exposure to export controls and supply-chain compliance initiatives

Attack Landscape

- High exposure to bots and SQL injection
- Attackers often target supplier portals, warranty registration forms, RMA forms, and embedded forms on legacy portals
- Legacy systems remain a primary weak spot

Sovereignty and Certifications

- **80%** rate sovereignty as critical or very important
- ISO 27001 adoption is strong, but SOC 2 Type II adoption varies
- Zero-trust adoption remains lower than in other sectors

Key Takeaways

Manufacturers have broad attack surfaces because their forms span suppliers, customers, and internal operations. Legacy infrastructure and decentralized ownership are the core risks.

6.4 Healthcare

Healthcare handles the most sensitive data in the dataset, making even minor security gaps costly.

Data Collected

- **97%** collect PHI through forms
- Patient intake, lab orders, telehealth, insurance details, and referral workflows
- Authentication credentials and financial data for billing and insurance claims

Regulatory Requirements

- **HIPAA** (nearly 100% of healthcare respondents)
- **GDPR** when treating EU residents or managing global research
- State-level health privacy restrictions
- Increasing federal scrutiny on patient data portability and interoperability

Attack Landscape

- High rates of XSS and credential attacks
- PHI flows make forms a prime target for fraud, insurance abuse, or identity theft
- Legacy clinical systems and third-party portals are common weaknesses

Sovereignty and Certifications

- **83%** rate sovereignty as critical or very important
- HIPAA attestation is widespread
- FIPS adoption is growing, especially for encrypted storage and secure messaging
- FedRAMP matters for public-sector healthcare and research programs

Key Takeaways

Healthcare forms have some of the strictest compliance requirements and highest breach costs. Many organizations struggle because form infrastructure spans EHR systems, patient portals, third-party clinical systems, and older custom workflows.

6.5 Government

Government agencies and public-sector organizations face the strictest requirements in the dataset and must balance overlapping mandates for security, residency, and auditability—often on top of legacy systems.

Data Collected

- **81%** collect government ID numbers
- High-value workflows: applications, benefit enrollment, permitting, procurement, and citizen service portals
- Sensitive records on citizens, employees, and contractors

Regulatory Requirements (see also Section 4.1)

- FedRAMP authorizations (75% of government respondents)
- FIPS 140-3 validated cryptography (69%)
- CMMC 2.0 for defense and contractor environments
- Local and national data residency laws
- Strict audit, logging, and incident reporting requirements

Attack Landscape

- High targeting from both criminal and state-aligned actors
- Frequent bot attacks, credential harvesting, and injection attempts
- Legacy platforms and slow modernization cycles increase exposure

Sovereignty and Certifications

- 4% rate data sovereignty as critical or very important
- Government-cloud and sovereign-cloud adoption are significantly higher than in other industries
- Zero-trust mandates drive shifts toward identity-first architectures
- Encryption, key management, and audit expectations exceed those in commercial sectors

Key Takeaways

Government workloads require capabilities that many commercial form tools cannot provide. Vendors without FedRAMP, FIPS 140-3 alignment, data residency guarantees, and zero-trust controls are effectively excluded from this segment.

6.6 Comparative Industry Summary Table

Table 14: Industry Comparison

Metric	Financial Services	Technology	Manufacturing	Healthcare	Government
Incident prevalence	90%	87%	85%	89%	90%
Breach via forms	45%	43%	42%	44%	43%
Sovereignty critical/ very important	93%	86%	80%	83%	94%
PHI collection	8%	4%	3%	97%	6%
Financial records collection	90%	62%	58%	40%	52%
Payment card data	83%	41%	36%	22%	30%
Government ID collection	42%	34%	29%	38%	81%
Key certifications	ISO/SOC/PCI	ISO/SOC	ISO	HIPAA/ISO	FedRAMP/FIPS

6.7 Industry Takeaways

Financial Services

Most mature controls but highest data value and strongest regulatory pressure; attackers target credential and payment flows.

Technology

Fast-moving, global, API-driven; gaps come from decentralized teams and rapid release cycles.

Manufacturing

Broad and distributed attack surface across suppliers, operations, and legacy systems.

Healthcare

Highest data sensitivity; form security failures have immediate regulatory, financial, and patient trust impact.

Government

Strictest requirements; many vendors simply cannot enter this market without FedRAMP, FIPS, and sovereignty controls.

SECTION 7

Market Insights & Strategic Recommendations

This section combines the key market insights from the survey with clear, actionable recommendations. It explains how organizations segment into distinct buying groups, where today's form-security solutions fall short, and what steps teams should take to close those gaps. The goal is to give security, compliance, and IT leaders a practical roadmap based on the actual pain points and priorities revealed in the data.

7.1 Market Segmentation

Four distinct market segments emerge from the data. Each segment has different regulatory drivers, deployment needs, and security expectations.

1. High-Security Segment (Government + Financial Services)

These organizations face the strongest regulatory requirements and the highest data sensitivity.

They require:

- FedRAMP
- FIPS 140-3
- CMMC 2.0
- PCI DSS
- Region-specific data residency
- Immutable audit trails
- End-to-end encryption

This segment is inaccessible to vendors without government-grade certifications and residency guarantees.

2. Regulated Industries (Healthcare, Life Sciences, Legal)

These organizations handle PHI, legal data, patient information, or sensitive financial data.

They prioritize:

- HIPAA readiness
- GDPR and PCI DSS coverage
- Audit trail automation
- Encryption at rest and in transit
- Role-based and policy-based access controls

3. Enterprise Segment (Technology, Manufacturing, Professional Services)

These organizations run global operations, hybrid or multi-cloud architectures, and high volumes of internal and customer-facing forms.

They care most about:

- API-first integration
- Deployment flexibility
- Data residency
- Workflow automation
- Modern identity and authentication

The biggest challenge in this segment is inconsistent controls across hundreds or thousands of forms.

4. Mid-Market (500–999 employees)

Mid-market security and compliance needs mirror enterprise requirements but with fewer resources. They care most about:

They need:

- Fast deployment
- Clear compliance defaults
- Simplified configuration
- Automation to reduce manual work
- Cloud-first but residency-aware options

7.2 Important Requirements

Survey data reveals several areas where organizations need capabilities that many form vendors either **do not support** or **cannot support.**

1. Data Sovereignty Controls (the Biggest Gap)

85% say sovereignty is critical or very important.

Most form tools cannot enforce:

- Region-specific storage
- Data isolation
- Sovereign or government cloud deployments
- Preventing cross-region replication

Vendors lacking residency controls will fail to meet the needs of high-security and regulated industries.

2. Encryption Strength (FIPS 140-3)

32% rank military-grade encryption as their top priority.

Nearly half of organizations require FIPS-validated cryptography.

Most form tools rely on generic cloud encryption rather than validated modules

3. Compliance Automation

Organizations struggle with:

- Audit trails
- Control documentation
- Evidence generation
- Cross-framework mapping

VMost form platforms provide logs but not audit-ready evidence. Automation here offers immediate ROI.

Identity, Zero Trust, and Session Control

Most vendors still rely on username/password authentication rather than:

- MFA
- Risk-based authentication
- Hardware keys
- Granular session controls

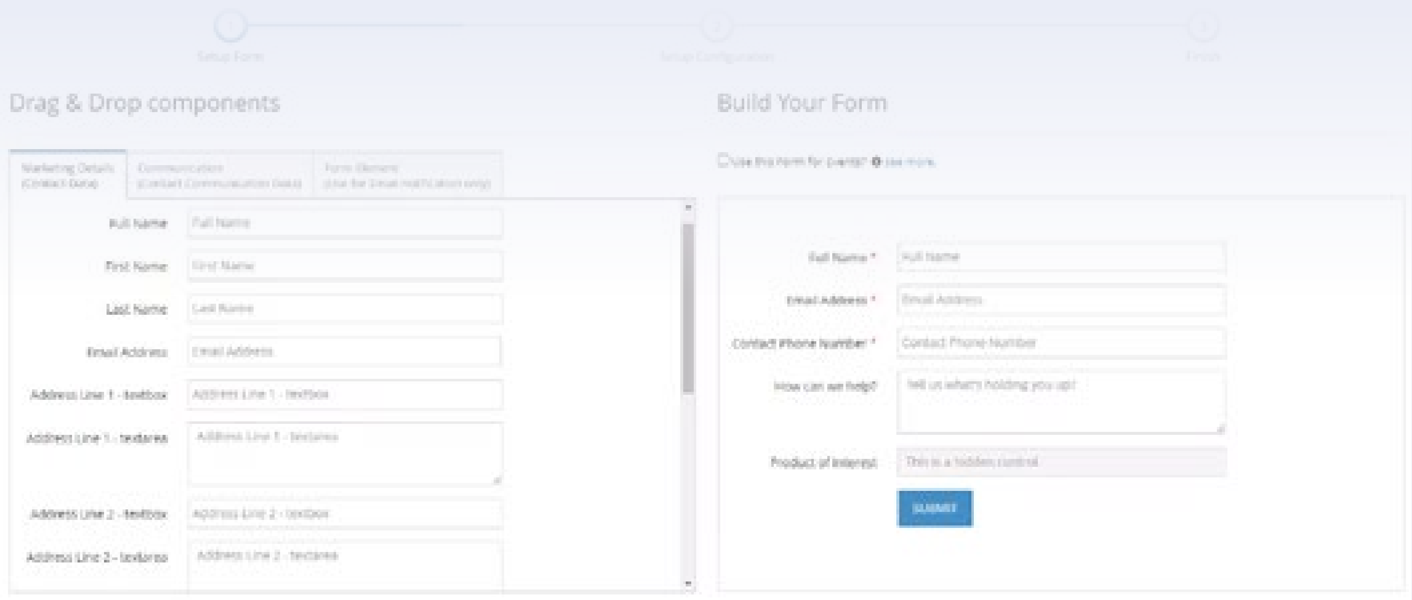
Attackers exploit these weaker flows. This under-prioritization mirrors the survey findings in Sections 5.4 and 5.5, where only **18%** classify zero-trust architecture as “critical” and overall adoption skews toward “moderate” or “low” importance rather than a core requirement for form infrastructure.

Full Governance Across All Forms

One of the largest unsolved problems is the “long tail” of forms:

- Legacy forms
- Embedded forms
- Third-party/vendor forms
- Mobile-heavy flows
- Department-built forms

Current tools secure only the forms created inside their platform. Organizations want coverage across their *entire* environment.



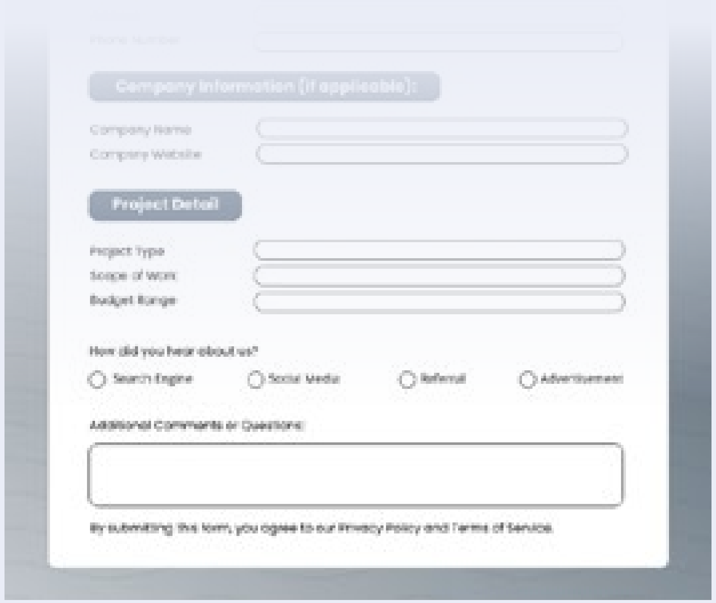
Drag & Drop components

Full Name	Full Name
First Name	First Name
Last Name	Last Name
Email Address	Email Address
Address Line 1 - textbox	Address Line 1 - textbox
Address Line 1 - textarea	Address Line 1 - textarea
Address Line 2 - textbox	Address Line 2 - textbox
Address Line 2 - textarea	Address Line 2 - textarea

Build Your Form

Full Name *	Full Name
Email Address *	Email Address
Contact Phone Number *	Contact Phone Number
How can we help?	Tell us what's holding you up!
Product of Interest	This is a hidden control

Setup Form
Setup Configuration
Finish
Marketing Details (Contact Data)
Communication (Contact Communication Data)
Form Element (Use for Email notification only)
SUBMIT



Company Information (if applicable):

Company Name

Company Website

Project Detail

Project Type

Scope of Work

Budget Range

How did you hear about us?

○ Search Engine ○ Social Media ○ Referral ○ Advertisement

Additional Comments or Questions:

By submitting this form, you agree to our Privacy Policy and Terms of Service.

7.3 Key Market Opportunity Signals

Three consistent themes emerge across industries, sizes, and regions.

1. Maturity does not equal protection.

Even “advanced” organizations report high incident and breach rates.

They need solutions that:

- Detect inconsistencies across forms
- Enforce uniform controls
- Automate response
- Reduce manual governance

2. Compliance pressure is rising.

GDPR, HIPAA, PCI DSS, state privacy laws, and residency rules are stacking—not shrinking.

Organizations want:

- Automated evidence
- Continuous compliance monitoring
- Residency enforcement
- Encryption assurances

3. Residency and sovereignty are deal-breakers.

Multi-deployment, multi-region isolation, and sovereignty controls are now core buying criteria.

7.4 Strategic Recommendations

Based on the combined insights from maturity patterns, attack data, regulatory exposure, and deployment requirements, the following actions offer the highest impact.

1. Centralize Governance Across All Forms

You should:

- Inventory every form across all teams and systems
- Require standardized validation, encryption, and logging
- Review and retire insecure or redundant forms
- Enforce a single governance model

Most breaches occur in forms that sit outside formal oversight. (This is especially important for the long tail of low-volume forms described in Section 5.5.)

2. Enforce Strong Encryption End-to-End

You should:

- Require TLS 1.3 for all form flows
- Encrypt data from submission through processing
- Use AES-256 for stored data
- Apply field-level encryption for high-risk fields
- Verify FIPS 140-3 compliance where required

Weak encryption or inconsistent coverage contributes directly to breach severity.

3. Automate Compliance Evidence

Manual compliance slows teams and increases risk.

You should:

- Monitor form configurations continuously
- Capture audit logs for access, changes, and data handling
- Generate evidence mapped to frameworks automatically
- Detect and flag drift from policy in real time

This lowers audit preparation time and reduces audit failures.

4. Close the Detection-to-Response Gap

You should:

- Pair real-time detection with automated response
- Integrate with SIEM/SOAR for containment workflows
- Reduce human handoffs
- Test and validate response playbooks

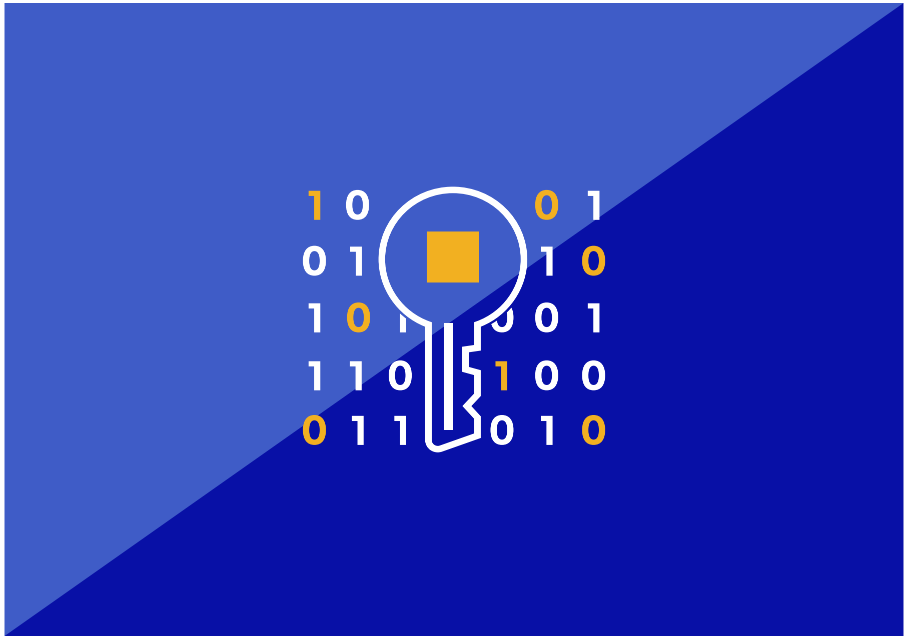
Detection without automation slows containment and increases breach conversion.

5. Strengthen Identity and Authentication Controls

You should:

- Enforce MFA on all high-risk forms
- Use SSO to centralize authentication
- Add risk-based and device-aware authentication
- Use hardware keys for privileged access
- Require biometrics on mobile flows

These steps significantly reduce session hijacking and credential abuse.



6. Modernize or Replace Legacy Forms

You should:

- Rebuild forms tied to unsupported systems
- Replace outdated validation logic
- Migrate high-value workflows to governed platforms
- Create a life-cycle process for form retirement

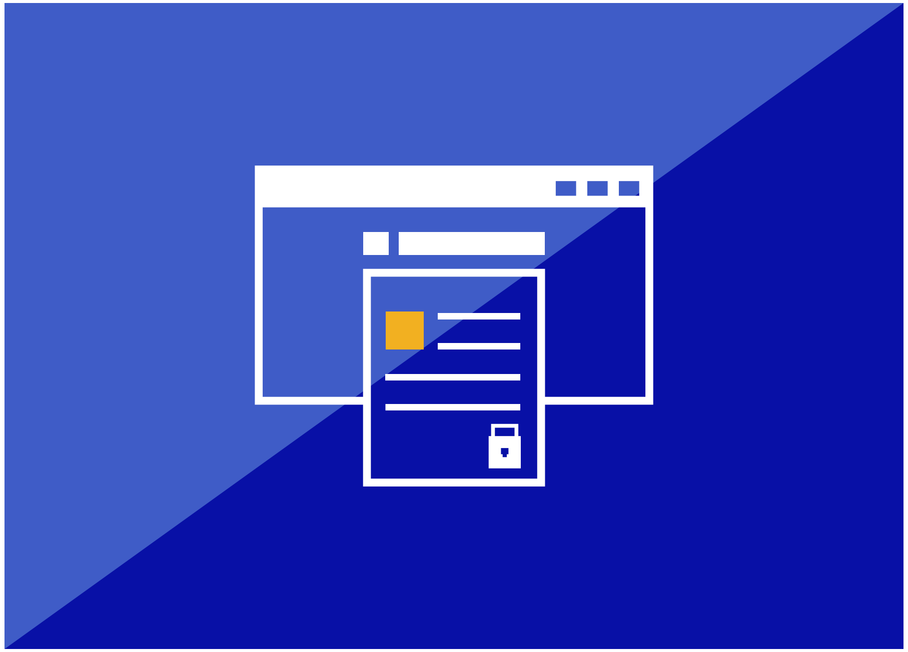
Legacy forms represent outsized security and compliance risk.

7. Enforce Data Residency and Deployment Controls

You should:

- Deploy forms in compliant regions
- Validate where backups, logs, and analytics data live
- Use cloud, hybrid, on-premises, or government cloud as needed
- Prevent cross-region replication unless explicitly allowed

Residency failures are a major source of audit findings.

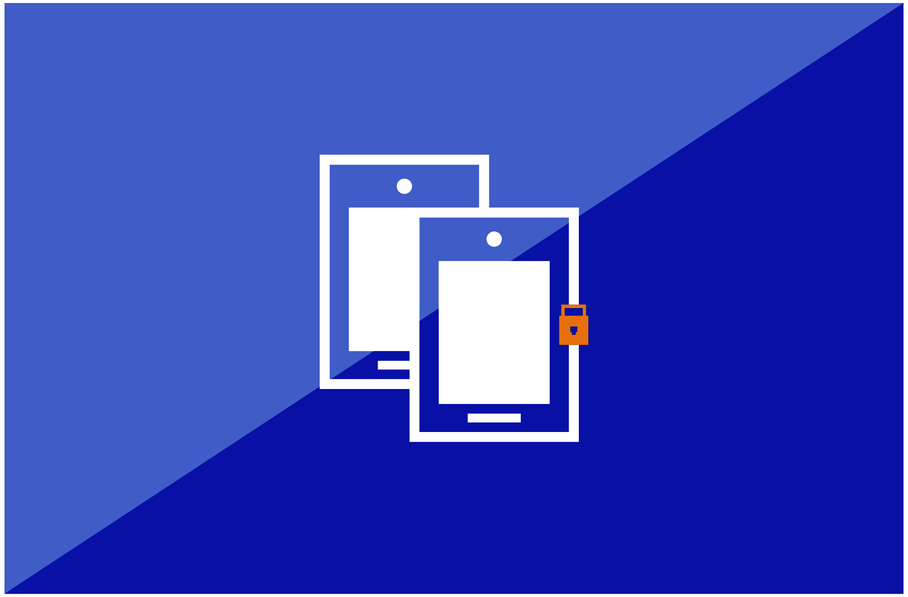


8. Strengthen Mobile Security

You should:

- Enable certificate pinning
- Enforce biometric authentication
- Validate strict TLS handling
- Monitor mobile threat signals

Mobile is now a primary data intake channel and must be secured accordingly.



9. Build a Sustainable Governance Operating Model

You should:

- Assign ownership for form governance
- Standardize templates, controls, and processes
- Review all new forms before deployment
- Run regular audits across all business units

This ensures security and compliance do not degrade over time.

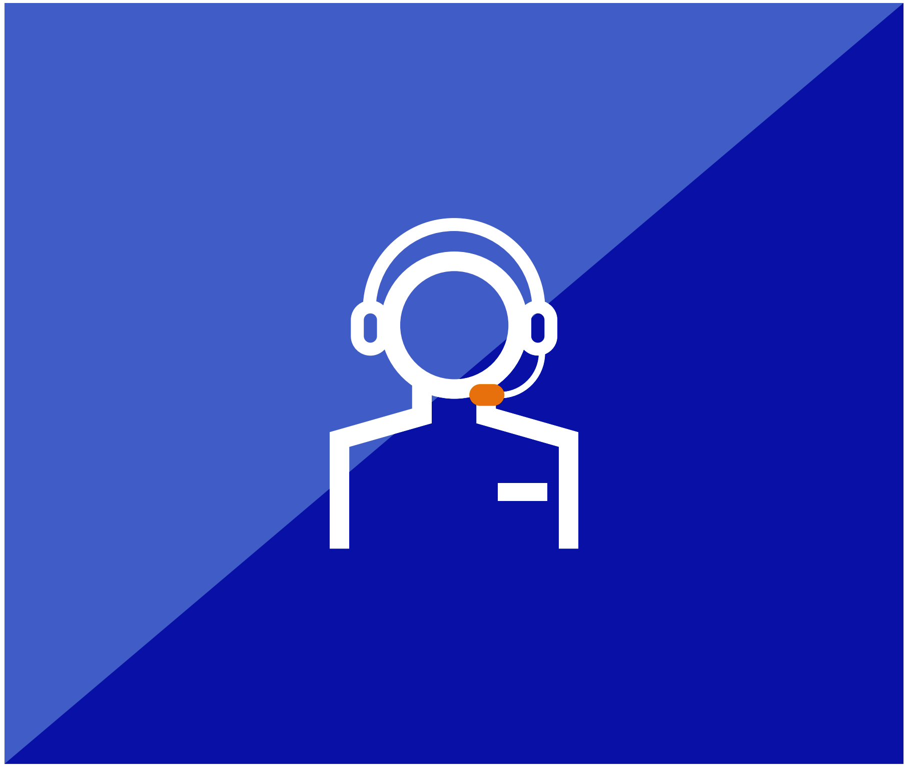
10. Prove ROI to Maintain Executive Support

Executives need measurable outcomes.

Track improvements in:

- Incident frequency
- Breach conversion rates
- Audit workload
- Response times
- Manual hours saved
- Deployment time for new form

ROI drives continued investment.



Appendix

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.

Sampling and Data Collection

A total of **324 cybersecurity, risk, compliance, and IT professionals** completed the survey. All respondents were required to work full time, use or manage web forms in their role, and have knowledge of their organization's security and compliance posture. Respondents were drawn from a balanced mix of industries, regions, and organization sizes.

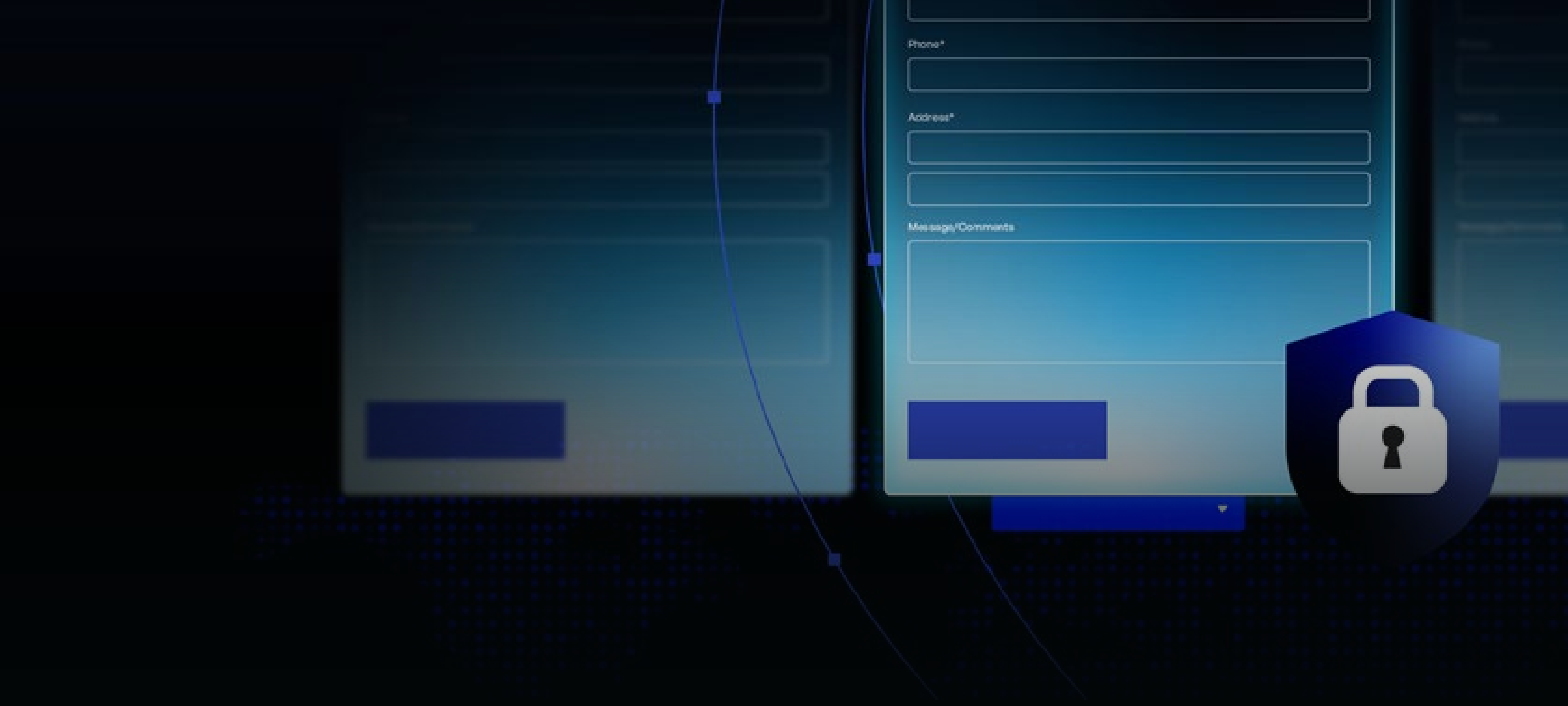
Table 15: Demographics of Respondents

Category	Segment	Percent
Industry	Financial Services	36%
	Technology	24%
	Manufacturing	15%
	Healthcare	10%
	Government	5%
	Other	10%
Region	United States	35%
	Canada	13%
	United Kingdom	16%
	Germany	10%
	France	9%
	Middle East	17%
Organization Size	500–999 employees	14%
	1,000–4,999 employees	37%
	5,000–9,999 employees	21%
	10,000–19,999 employees	16%
	20,000+ employees	12%

Category	Segment	Percent
Job Function	IT/Technology	61%
	Cybersecurity/Privacy	22%
	Risk Management	9%
	Compliance/Legal	8%
Seniority	Manager	41%
	Director	30%
	VP	14%
	C-Suite	9%
	Other	6%

Table 16: Certification Adoption

Certification	Adoption
ISO 27001	89%
SOC 2 Type II	82%
PCI DSS	72%
GDPR certification framework (e.g., ISO 27701)	61%
FIPS 140-3	48%
HIPAA attestation	41%
FedRAMP	30%



December 2025

www.kiteworks.com