secureframe

Cybersecurity and Compliance

2026 Benchmark Report

Table of Contents

Executive Summary 02

Inside the Data: Key Cybersecurity Benchmarks and Insights

1. Cybersecurity is a priority, but remains undersourced 03
2. Budgets are growing, but so is pressure 04
3. The burden of manual compliance 04
4. AI as both a threat and an essential tool 05
5. Compliance is now a competitive advantage 06
6. Proactive transparency as the new standard for trust 07
7. The cost of non-compliance 08
8. Multi-framework compliance as a maturity marker 08
9. Small teams shouldering big expectations 09

About the Survey: Full Data & Methodology 11

About Secureframe 17

Executive Summary

Cybersecurity has never been more central to business strategy, yet many organizations are still working to build the operational muscle to support it. Many cybersecurity and leaders are operating with small teams, cautious budgets, and legacy processes that were not designed for the speed or complexity of modern threats.

The responses from more than 250 organizations reflect this reality. Nearly everyone agrees cybersecurity is essential, but more than half have one or fewer full time staff dedicated to it. Budgets are rising, but not quickly enough to match the speed and scale of today's risks or the growing list of compliance expectations.

Key Takeaways

- 93% of companies say cybersecurity is a top or major organizational priority
- Nearly half of companies (47%) say a lack of compliance certification has delayed sales cycles
- 70% rely on security questionnaires and RFPs to prove their security posture
- 23% say the manual work of audit preparation is their biggest challenge heading into 2026
- 33% are already using AI for compliance or security operations

At the same time, the landscape is shifting in meaningful ways. AI is reshaping both the threat environment and the tools defenders rely on. Manual, repetitive work continues to drain time and resources. And compliance, long viewed as a checkbox, is becoming a meaningful way to signal trust and maturity to customers.

These findings point to a shift toward greater efficiency and clarity as organizations look for ways to reduce manual effort, improve visibility, and keep pace with growing cybersecurity demands. The survey data that follows shows how these pressures are playing out inside real organizations, and what they mean for the future of security and compliance.

My hope is that these insights provide clarity and guidance as you shape your own security and compliance roadmap for 2026 and beyond.

Shrav Mehta

Shrav Mehta
Founder & CEO

Inside the data: Key cybersecurity benchmarks and insights

The survey findings that follow offer a closer look at how these dynamics are playing out inside real organizations. Each takeaway reflects both the data itself and the broader patterns shaping how teams manage cybersecurity today. Together, these insights provide a clearer view of where the industry stands, where it is strained, and where it is headed as companies work to balance rising expectations with limited time, talent, and resources.

1. Cybersecurity is a priority, but remains undersourced

Over the past decade, cybersecurity has shifted from a behind-the-scenes IT function to a consistent topic in boardrooms. That shift is nearly universal. 93% of respondents described cybersecurity as either a top priority or one of the top priorities for their organization.

Yet many teams remain significantly understaffed. **More than half** of the companies surveyed have one or fewer full-time cybersecurity professionals, and **nearly a third** have none at all. In smaller organizations, especially those under 100 employees, security is still distributed informally across IT, engineering, and leadership teams.

This gap between urgency and capacity creates a growing risk exposure. As compliance requirements expand and attack surfaces become more complex, companies that treat cybersecurity as a shared responsibility often struggle to maintain clear ownership. Smaller organizations in particular will need automation and managed services to support their programs. The next phase of cybersecurity maturity will be defined not by headcount, but by how effectively organizations use technology to scale the impact of the teams they already have.

Survey Highlights

- 93% say cybersecurity is a top or major priority
- 58% have one or fewer full-time cybersecurity staff
- 27% have no dedicated staff and distribute security work across other roles

2. Budgets are growing, but so is pressure

The staffing challenge is closely tied to budgets that have not kept pace with rising expectations. Nearly two-thirds of organizations increased their cybersecurity and compliance spending in 2025, yet most still invest **less than 15%** of their annual budget in these areas. For many companies, this leaves little room for additional hiring or program expansion.

Organizations are trying to meet rising expectations with limited resources. This creates a widening divide between well-funded enterprises and smaller businesses that must choose between advancing security maturity and supporting growth. Over time, the ability to achieve more with existing budgets will become a key differentiator. The future of cybersecurity spending will depend less on total dollars allocated and more on how efficiently teams convert those dollars into measurable improvement.

Survey Highlights

- 66% increased cybersecurity budgets this year
- 75% spend 15% or less of their total annual budget on security and compliance
- Most smaller organizations operate with under $5 million in revenue

3. The burden of manual compliance is at a breaking point

As AI raises the stakes, manual work remains one of the biggest obstacles limiting security teams. Nearly a quarter of respondents said the most significant challenge they face heading into 2026 is the manual work of preparing for internal and external audits. Many also struggle to maintain continuous compliance and keep up with evolving framework requirements.

Teams spend an **average of eight hours per week** on compliance tasks, often duplicating work across frameworks. With staffing and budgets limited, this level of manual effort is unsustainable.

Survey Highlights

- 23% say manual audit preparation is their biggest challenge
- 8 hours per week spent on compliance and audit tasks on average
- 3–6 months is the typical time to achieve compliance with a new framework

Organizations are looking to automation to centralize evidence, map controls more efficiently, and maintain real-time compliance visibility. This shift away from point-in-time preparation and toward continuous readiness is already underway. Teams that adopt automation early will gain significant advantages in efficiency, accuracy, and audit preparedness.

Survey highlights

55%

cited AI-powered attacks as a top concern for 2026

33%

are already using AI or generative AI tools for compliance or security operations

Common AI use cases include **evidence validation**, **risk assessments**, and **policy generation**.

4. AI is both a threat and an essential tool

As organizations navigate rising expectations around security and compliance, another force is reshaping the landscape even more rapidly: artificial intelligence. AI is introducing a new layer of both opportunity and risk that teams must account for as they plan for the year ahead.

AI-powered attacks were the second most concerning threat for 2026, just behind phishing. Respondents reported growing concern about deepfakes, automated social engineering, and malware that adapts faster than traditional defenses.

At the same time, many organizations have begun using AI to support security and compliance. **A third of respondents** already use AI or generative AI to streamline evidence collection, support risk assessments, or assist with policy creation.

AI has become a source of both pressure and possibility. Organizations that use it responsibly, pairing automation with strong oversight, will gain a competitive edge in both readiness and resilience. Those that do not risk falling further behind as threats evolve.

5. Compliance has evolved from checkbox to competitive advantage

Survey Highlights

- 61% needed compliance to secure contracts
- 40% used compliance to reach enterprise buyers
- 32% pursued it to satisfy investors or partners

As internal processes strain under growing workloads, the consequences extend beyond operations and into the customer experience and revenue performance.

While compliance once functioned primarily as a risk management exercise, today it is a meaningful way to win trust and enable revenue. **61% of respondents** said achieving compliance was required to win or renew contracts, and 40% reported pursuing certification specifically to reach enterprise customers. Investors and partners are also raising expectations, with nearly a third of respondents citing external pressure as a driver.

Compliance now sits at the intersection of trust, growth, and competitive positioning. Organizations that achieve and maintain rigorous certifications signal their reliability and maturity to the market. As buyers increasingly demand verifiable proof of security, compliance has become inseparable from the sales process. Automation, transparency, and continuous validation will play a growing role in helping organizations meet both audit requirements and customer expectations.

> "Our research confirms what forward-thinking security leaders already know: reactive compliance approaches are exponentially more expensive than proactive programs."

Shrav Mehta
Founder & CEO
Secureframe

6. Proactive transparency is the new standard for trust

Even as compliance grows in importance, a striking majority of organizations still rely on reactive methods to prove their security posture. Our data shows that **nearly 70% of companies** rely on questionnaires and RFPs to demonstrate assurance, and **nearly 60%** use static audit reports like SOC 2, all of which require significant manual effort and provide limited visibility into ongoing security practices. They are also repetitive, time-consuming, and often disconnected from an organization's day-to-day security practices.

This reactive approach slows procurement cycles and places a heavy burden on small security teams. It also limits visibility for customers, who increasingly expect real-time, verifiable insight into how their vendors manage risk.

A minority of organizations are shifting toward more proactive methods, such as trust centers or customer-facing portals that consolidate certifications, policies, penetration testing summaries, and continuous monitoring data. These efforts show a higher level of maturity by making security transparent and accessible.

Survey highlights

About
70%
of companies rely on completing security questionnaires and RFPs.

Approx.
60%
share a third-party audit report such as SOC 2.

Only
20%
provide proactive visibility through internal attestations, dashboards, or trust centers

Nearly half (47%) said a lack of certification or proof of compliance has delayed sales or damaged customer relationships.

> "Companies now have to prove compliance across remote teams, personal devices, and decentralized environments, presenting a monitoring burden that's nearly impossible to manage manually."
>
> Chintan Parikh
> VP of Engineering, Secureframe

7. The cost of non-compliance is lost revenue and slower growth

The business impact of these gaps is significant. Buyers increasingly equate compliance with credibility, which means the absence of verifiable proof has direct revenue consequences. **Almost half of respondents** said that lacking a compliance certification has slowed down or jeopardized sales, and more than one-third reported losing revenue or competitive bids as a result.

For prospects, a lack of compliance often signals heightened risk or operational immaturity, and in more regulated sectors, it can prevent a vendor from entering the conversation at all. Organizations that can demonstrably prove their security posture accelerate buying decisions and reduce friction during vendor evaluation, turning compliance into a growth enabler rather than a cost center.

Survey Highlights

- 46% of organizations say that lacking a compliance certification has delayed sales cycles
- 38% reported lost revenue or competitive bids
- 24% experienced strained customer relationships due to insufficient proof of compliance
- 14% said non-compliance hurt their ability to raise funding or satisfy investors

8. Multi-framework compliance is a maturity marker

A single certification such as SOC 2 may meet immediate customer expectations, but growing organizations often require a broader compliance posture. **52% of surveyed companies** are compliant with more than one framework, and the number increases significantly with company size and revenue.

Larger and more mature organizations tend to maintain certifications across SOC 2, ISO 27001, HIPAA, PCI DSS, and NIST frameworks. This evolution reflects both regulatory pressure and the need to demonstrate trustworthiness across different markets and industries.

Managing multiple frameworks introduces operational complexity. Without automation, organizations risk repetitive work, misalignment across frameworks, and compliance fatigue. Centralized evidence management, control mapping, and continuous monitoring become essential as companies take on additional requirements.

Survey Highlights

- 52% of surveyed companies are compliant with more than one framework
- Organizations with over 500 employees maintain an average of 3.1 frameworks, compared with 1.6 frameworks for companies with fewer than 100 employees
- Companies earning more than $100 million in annual revenue manage an average of 3.2 frameworks, nearly twice as many as those below $25 million
- SOC 2 remains the most common starting point, followed by ISO 27001, HIPAA, PCI DSS, and NIST 800-53 as companies grow in complexity

9. Small teams are shouldering big expectations

Teams responsible for cybersecurity and compliance are operating under increasing pressure, regardless of company size. Even in organizations with mature programs and established security functions, the day-to-day work of safeguarding systems, responding to threats, and maintaining compliance often falls on a core group of people juggling multiple roles.

Despite these constraints, security and compliance teams are adopting a wide range of modern tools and practices. 91% use MFA or password management, and 67% have implemented vulnerability scanning or patch management tools. Many organizations have implemented SIEM platforms, and a growing number are integrating GRC automation to reduce repetitive work and improve consistency across frameworks.

This combination of high expectations and lean teams represents a significant opportunity for scalable and accessible compliance tools. As frameworks proliferate and customers demand greater visibility, tools that streamline security operations for small and midsize businesses will play a critical role in shaping the next phase of cybersecurity maturity.

Survey Highlights

- 91% use MFA or password management, and 67% use vulnerability scanning or patch management tools
- 67% use vulnerability scanning or patch management tools

The path to sustainable security and compliance

The findings in this report demonstrate a clear inflection point for cybersecurity and compliance programs: security teams are working hard to meet rising expectations while carrying more responsibilities than ever. Manual work, limited resources, and growing complexity continue to create friction.

The shift happening now is not just about emerging threats. It's about finding ways to make security work sustainable. Efficiency, automation, and clearer visibility are quickly becoming essential. They help teams shift time away from manual evidence collection toward strengthening their overall posture and building the customer trust that now shapes buying decisions.

For organizations looking to build a stronger and more scalable compliance program, Secureframe can streamline the path forward. Our platform gives teams a simpler and more scalable way to manage compliance, centralize evidence, and stay continuously audit-ready. If you want to see how automation can reduce your workload and support a stronger security program, explore Secureframe through a personalized demo.

About the survey:
Full data and methodology

This report is based on a survey conducted by UserEvidence from October 22–31, 2025, targeting members of Secureframe's internal customer community across multiple industries and company sizes. A total of 255 responses were collected from security, compliance, and IT professionals.

Respondents represented organizations ranging from early-stage startups to large enterprises and spanned key sectors including technology, financial services, healthcare, and professional services. Questions covered cybersecurity priorities, budgets, staffing, implemented frameworks, top challenges, and the perceived business impact of compliance. Data was analyzed in aggregate to identify cross-industry trends and maturity patterns.

Cybersecurity priority and resource allocation

Business Importance of Cybersecurity

- Top priority: 35%
- One of the top priorities: 58%
- Important, but not a priority: 7%

93% of companies consider cybersecurity a top or major priority.

Budget Allocation

- Less than 10%: 43%
- 10 to 15%: 32%
- 15 to 30%: 23%
- More than 30%: 3%

Average annual spend on cybersecurity and compliance: 13.71%

Year-over-year change

- Increased somewhat: 42%
- Stayed the same: 30%
- Increased significantly: 19%
- Decreased: 3%

Ownership of Cybersecurity and Compliance

- CTO: 26%
- CISO or Head of Cybersecurity: 23%
- Head of IT: 16%
- Head of Engineering: 14%
- Other: 14%
- CEO or COO: 7%

Security Staffing Levels

- None, with no plans to hire: 27%
- None, but plan to hire within the next year: 10%
- One full-time employee: 31%
- Two to five: 26%
- More than five: 5%

Security and Compliance Technologies in Use

- Multi-factor authentication or password managers: 91%
- Vulnerability scanning and patch management: 68%
- Endpoint protection (EDR or XDR): 55%
- SIEM: 41%
- AI-powered security tools: 39%
- Generative AI for security or compliance tasks: 33%
- GRC automation solution: 23%

Threat landscape and security motivation

Top Cybersecurity Threats for 2026

- Phishing: 65%
- AI-powered attacks: 55%
- Insider threats and human error: 53%
- Business Email Compromise (BEC): 45%
- Supply chain and vendor risk: 44%
- Ransomware: 41%
- DoS/DDoS attacks: 32%
- Other: 2%

Primary Motivation for Maintaining Strong Security

- Protecting customers: 60%
- Achieving or maintaining compliance certifications: 20%
- Protecting intellectual property and internal assets: 11%
- Supporting sales and revenue: 8%
- Other: 1%

How Organizations Prove Their Security Posture

- Sharing a third-party audit report: 73%
- Completing security questionnaires and RFPs: 70%
- Sharing internal audit or self-attestation: 36%
- Sharing a security dashboard or trust page: 31%
- None of the above: 4%
- Other: 2%

Top Challenges Heading Into 2026

- Manual audit preparation: 23%
- Demonstrating compliance to customers or partners: 20%
- Understanding the threat landscape: 15%
- Monitoring systems and controls to maintain compliance: 15%
- Interpreting framework requirements: 12%
- Navigating framework changes: 8%
- Determining which frameworks apply: 7%
- Other: 1%

Compliance effort and outcomes

Weekly Time Spent on Compliance and Security Tasks

- Fewer than 5 hours: 36%
- 5 to 10 hours: 37%
- 10 to 20 hours: 18%
- 20 to 40 hours: 6%
- More than 40 hours: 3%

Time Required to Achieve a New Framework

- 1 to 3 months: 35%
- 3 to 6 months: 37%
- 6 to 9 months: 14%
- 9 to 12 months: 9%
- More than 12 months: 5%

Business Challenges Caused by Lack of Certification

- Delayed sales cycles: 47%
- Lost revenue or competitive bids: 38%
- Increased risk exposure: 40%
- Strained customer relationships: 24%
- Difficulty raising funding: 14%
- None: 15%
- Other: 4%

Motivations for Achieving Compliance
(Respondents selected up to two)

- Strengthen internal security posture and prevent incidents: 62%
- Required to win or renew contracts: 62%
- Fulfill industry, regulatory, or legal requirements: 48%
- Move upmarket or attract enterprise clients: 40%
- Satisfy partners or investors: 33%

Framework adoption and maturity

Frameworks Achieved or In Progress

- SOC 2: 90%
- ISO 27001: 28%
- HIPAA: 23%
- PCI DSS: 15%
- FedRAMP: 4%
- CMMC or NIST 800 171: 3%
- Other: 7%

Multi-Framework Adoption

- One framework: 46%
- Two frameworks: 31%
- Three frameworks: 17%
- Four or more frameworks: 4%

Average Number of Frameworks by Industry

- Aerospace and Robotics: 3.0
- Transportation: 3.0
- Non-Profit: 3.0
- Manufacturing and Industrial: 2.5
- Retail and E-commerce: 2.5
- Government and Public Sector: 2.25
- Healthcare: 2.10

Annual Revenue	Average Number of Frameworks
Less than $5 million	1.6
$5 to $25 million	1.7
$25 to $100 million	1.9
More than $100 million	3.2

Company demographics

Employee Count

- 1 to 50 employees: 57%
- 50 to 100: 20%
- 100 to 200: 10%
- 200 to 500: 8%
- More than 500: 6%

Annual Revenue

- Less than $5 million: 50%
- $5 to $25 million: 31%
- $25 to $100 million: 12%
- More than $100 million: 6%

Industry Representation

- Software and Tech: 79%
- Financial Services: 17%
- Healthcare: 11%
- Professional Services and Consulting: 11%
- Manufacturing and Industrial: 4%
- Government and Public Sector: 2%
- Retail and E-commerce: 1%
- Other: 6%

Regions Served

- North America: 85%
- Europe: 21%
- Latin America: 8%
- Asia Pacific: 12%
- Middle East and Africa: 4%
- Global: 16%

secureframe

Build trust. Unlock growth.

The leading, all-in-one automated security and privacy compliance platform

AUTOMATED EVIDENCE COLLECTION

Our 200+ integrations help you gather information from your existing tech stack automatically.

PREBUILT POLICIES

We provide standard templates for policies, procedures, and system security plans written by former federal auditors that can be edited to meet your specific needs.

ROLE-BASED ACCESS CONTROL

Security officers maintain control over the data that users have access to using role-based settings.

REPORTS AND DASHBOARDS

Get a clear view into your security posture and status, and see how you're progressing towards compliance.

AUTOMATED TESTS

View, assign, filter and export tests on a single page, and easily access all active and inactive tests from the Test Library.

CLOUD REMEDIATION WITH COMPLY AI

Secureframe helps fix failing cloud tests with step-by-step guidance and generative AI to provide infrastructure-as-code fixes.

IN-PLATFORM TRAINING

Secureframe delivers proprietary employee training for frameworks and in-platform tracking to help you stay compliant.

ACCESS TO COMPLIANCE EXPERTS

30+ dedicated compliance experts and former auditors help guide you through the process and recertifications.

TAILORED AUDITOR EXPERIENCE

We make it easy for auditors to review evidence and get through an audit quickly.

TAILOR YOUR COMPLIANCE PROGRAM

Create custom frameworks, controls, and tests that best fit your unique business needs.

TRUST CENTER

Showcase your security posture and remove friction from the end-to-end security review process.

QUESTIONNAIRE AUTOMATION

Save hundreds of hours answering RFPs and security questionnaires with Secureframe's ML-powered Questionnaire Automation.

TRUSTED BY TODAY'S LEADING COMPANIES

ramp · Teamable · Rand McNally · Magellan Jets · smartcar · Doodle · stream · wellfound: formerly AngelList Talent · lyra · GENERALI · The Salvation Army · Security Scorecard

"Secureframe is a very user-friendly platform and has a great UI/UX. I can confidently say that the platform is so easy and it has everything you need to make getting SOC 2 [compliance] fast."

Thomas Mirmotahari
CEO and Co-Founder, PerkUp

Ready to automate your compliance?

Reach out to sales@secureframe.com or visit secureframe.com to learn more.