Vanta

State of Trust Report 2023

Uncovering global trends in security, compliance, and the future of trust

Table of Contents

Foreword

Businesses today are navigating an unprecedented security landscape. The expansion of attack surfaces in a post-pandemic hybrid world, combined with shrinking teams and budgets and the rapid rise of Generative AI, are fueling an urgent need for companies to improve — and prove — their security posture.

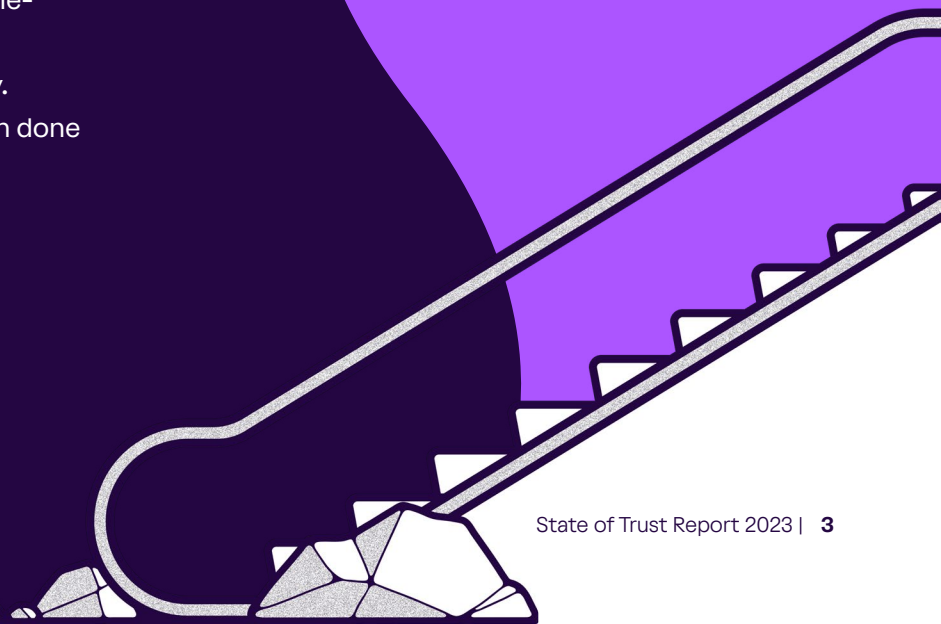
Backdoor deployments are on the rise while ransomware continues to grow as the second highest form of attack on companies, according to IBM.[1] In the last year alone, Verizon found that corporate email compromises nearly doubled to more than 50% of social engineering incidents.[2]

Vanta's State of Trust Report reveals that over two-thirds of businesses say they need to improve security and compliance measures, with almost one in four rating their organization's security and compliance strategy as merely reactive.

With rising risk and shrinking resources, the message is clear: **businesses need new methods to improve their security**. Compounding the urgency is the ever-evolving global regulatory landscape and growing compliance time-suck it entails. In an environment where customers increasingly want more proof of a company's security practices, organizations are at an impasse. **So, what's the solution?**

As we'll uncover, automation can accelerate security and compliance when deployed as part of a broader, proactive trust management strategy. Focusing on trust management — automating time-consuming compliance tasks, centralizing security program management with a single source of truth, and streamlining security reviews — can unlock significant savings of both time and money. Supercharging these capabilities with AI will further disrupt the security status quo, but only when done responsibly and transparently.

Let's dive in.



1 - https://www.ibm.com/reports/threat-intelligence
2 - https://www.verizon.com/business/resources/reports/dbir/2023/results-and-analysis-intro/

Key Findings

67%

Over two thirds

of business and IT leaders say their organization needs to improve security and compliance measures.

Only 9%

of IT budgets are dedicated to security.

Respondents say they could save at least two hours each week – over 2.5 working weeks a year – if security and compliance tasks were automated.

2 hours per week

24%

rate their businesses' security and compliance strategy as merely "reactive."

60%

have either reduced IT budgets in the economic downturn – or are planning to.

70%

Seven in ten say a better security and compliance strategy would positively impact their business through higher customer trust.

Fewer than half

of organizations rate their risk visibility as strong.

Respondents spend on average 7.5 hours per week on security compliance. That's 360 hours — more than nine working weeks — per year.

7.5 hours per week

The biggest barriers

to proving security externally are a lack of staffing (33%) and of automation to replace manual work (32%).

PART ONE

The security improvement imperative

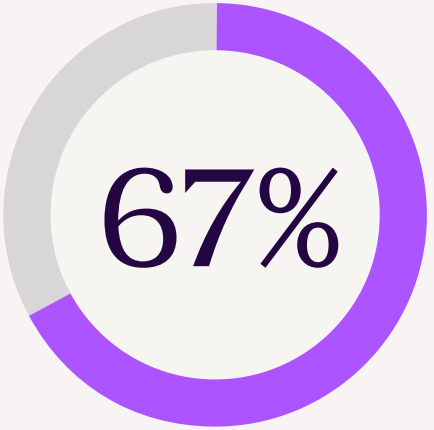
The State of Trust Report surveyed 2,500 IT and business decision-makers across Australia, France, Germany, the UK and U.S. and reveals the urgent need for businesses to improve security.

When diving into the regional variations, the numbers illustrate large differences around the world.

In France, the concern rises to 76% – the highest of all countries surveyed – while it dips to 55% in Germany.

Responses also vary greatly by role. 73% of IT decision-makers say their business needs to improve security and compliance measures, compared to only 61% of business decision-makers.

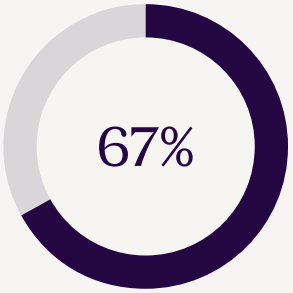
Over two-thirds of all respondents believe their business needs to improve both security and compliance measures.



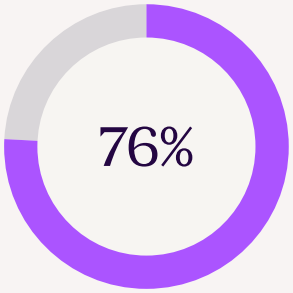
To what extent do you agree with the following statements regarding your security and compliance strategy?

"My business requires security and compliance improvement measures."

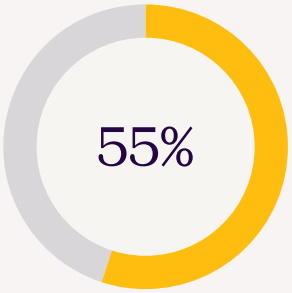
Australia



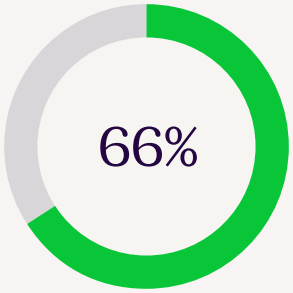
France



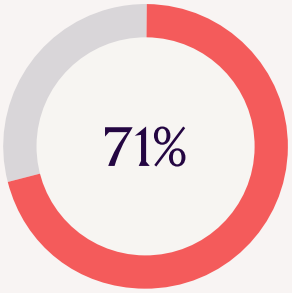
Germany



United Kingdom



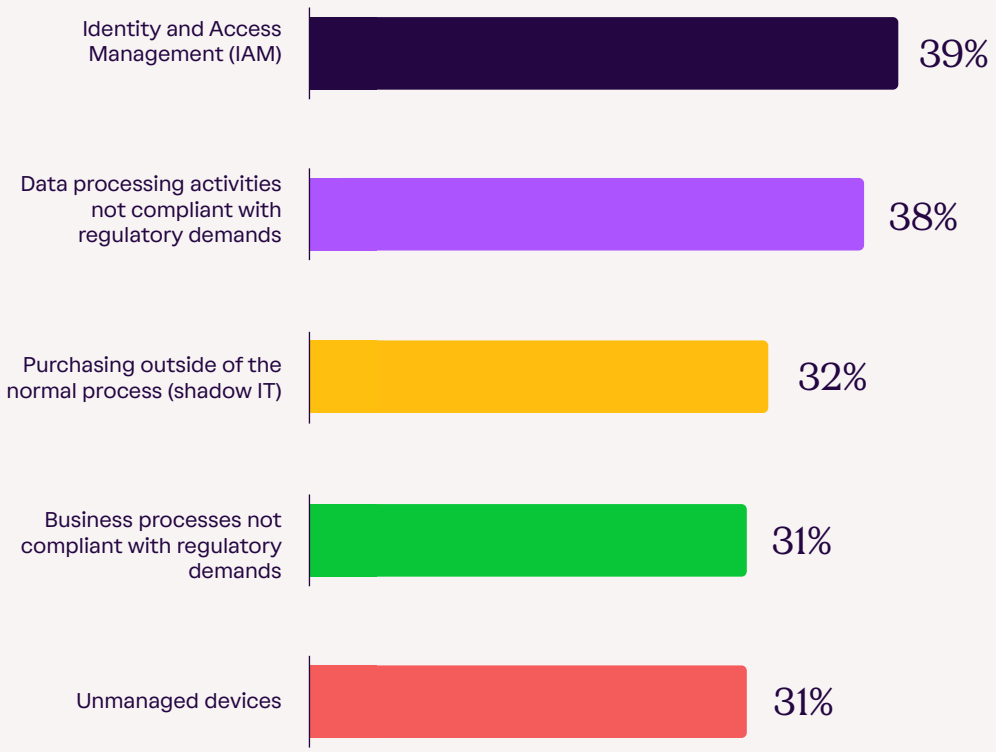
United States

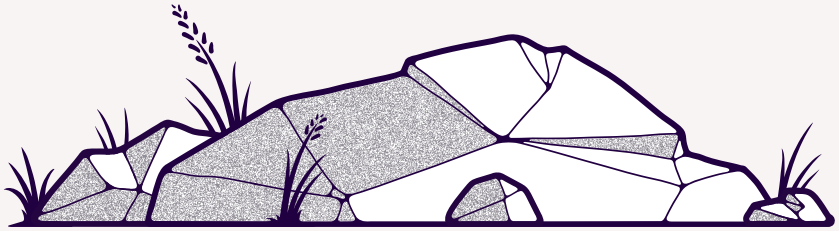


For companies of all sizes, limited risk visibility and blind spots accelerate the need to improve security and compliance. Only 4 in 10 organizations rate their risk visibility as strong. Meanwhile, identity and access management and data processing that doesn't comply with regulations are the two biggest blind spots for organizations.

In the UK, keeping up to date with evolving regulation spikes to 37%, the highest of all regions, but dips in Germany to 26%.

What are your organization's biggest IT security and compliance blind spots?





Security as a selling point

To gain customer trust and land deals, transparency is a must. Two-thirds (66%) say that customers, investors and suppliers are increasingly looking for proof of security and compliance.

But companies are struggling to maintain and demonstrate their security posture, even in the face of growing customer demand.

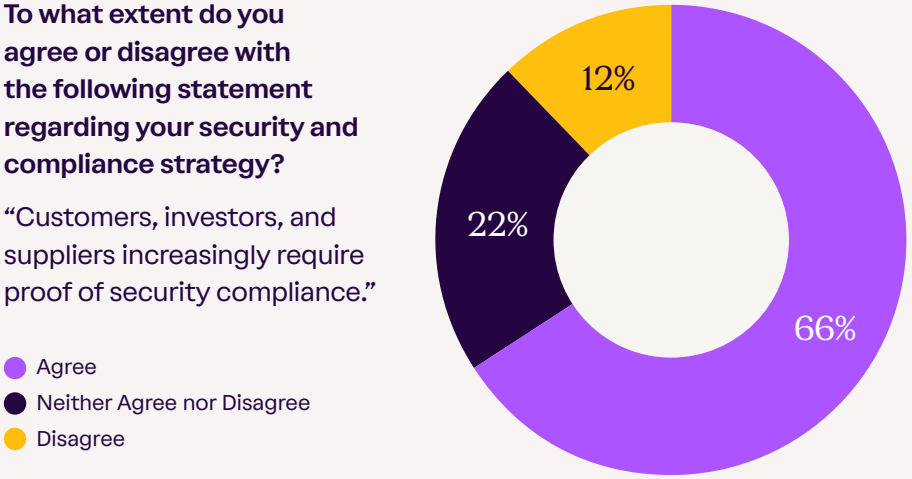
While 41% provide internal reports, 37% third-party audits, and 36% complete security questionnaires, one in eight (12%) companies surveyed admit they don't or can't provide evidence when asked. This number is lowest in the U.S. (10%), but increases to 16% in Australia, the highest of any country surveyed. This means companies around the world are falling at the very first hurdle, costing them potential revenue and growth opportunities in new markets.

"Our users trust us to provide a safe place to share information and connect on our platform. Through our partnership with Vanta, we're able to demonstrate our security posture and scale up our compliance program."

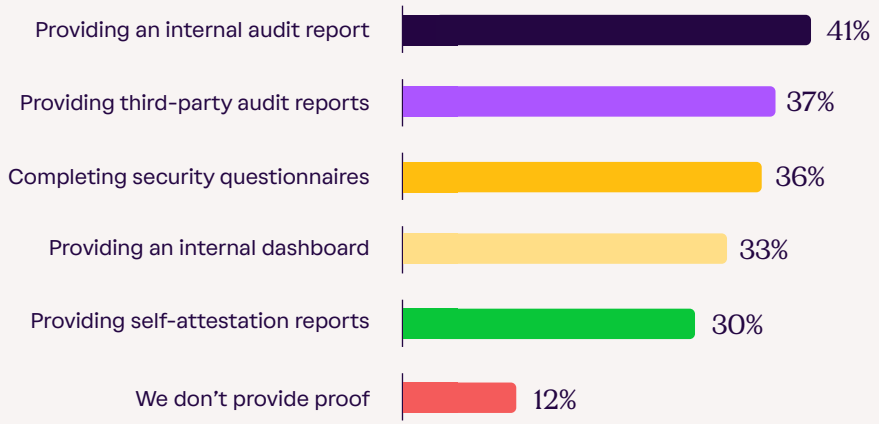
Spencer Chan, Staff Software Engineer
Quora

To what extent do you agree or disagree with the following statement regarding your security and compliance strategy?

"Customers, investors, and suppliers increasingly require proof of security compliance."



How do you demonstrate security to customers or third parties when they ask for proof?



The challenge:
Scaling security as resources stall

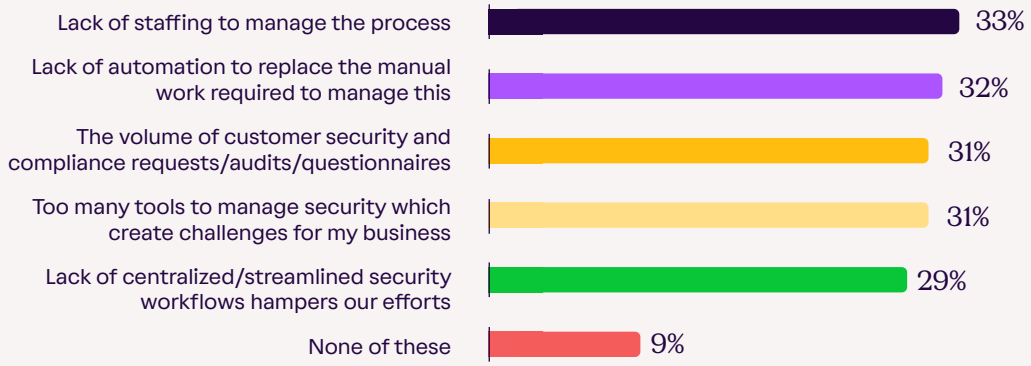
In spite of the clear consensus that global companies need to improve their security, shrinking budgets and staffing resources are making it difficult.

According to respondents, the biggest barriers to proving and demonstrating security externally are a lack of staffing and automation to replace manual work.

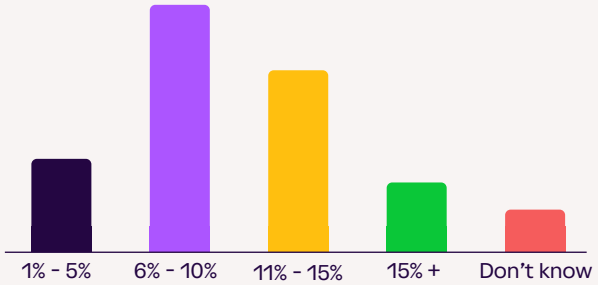
This comes at a time when one in four (24%) businesses surveyed say they have reduced IT staff. And it's not just team size that's decreasing. One in three leaders (33%) say that their overall IT budgets are shrinking as they continue navigating the economic downturn while 60% have either already downsized IT budgets or are planning to.

On average, only 9% of IT budgets are dedicated to security, further exacerbating resource constraints.

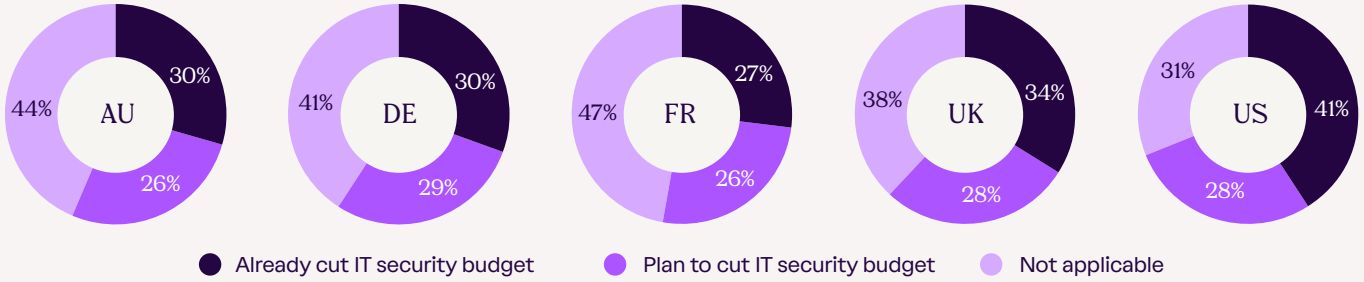
What are your biggest barriers to proving and demonstrating security externally?



How much of your company's IT budget is dedicated to security?



When asked if decision-makers have already, or are planning to reduce their IT security budget, respondents said:



Compliance deprioritized

Given these trends, it's not surprising that respondents admit they're not prioritizing compliance due to the time and financial investment.

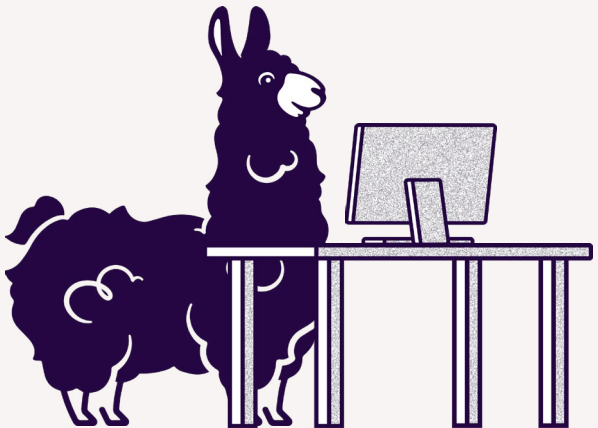
For businesses trying to meet and maintain the demands of compliance, time is being plunged into these efforts. Respondents spend an average of 7.5 hours per week (more than 9 working weeks) on compliance.

Exacerbating this time-suck, more than half (55%) of respondents say that remaining compliant with different national regulations is becoming increasingly difficult.

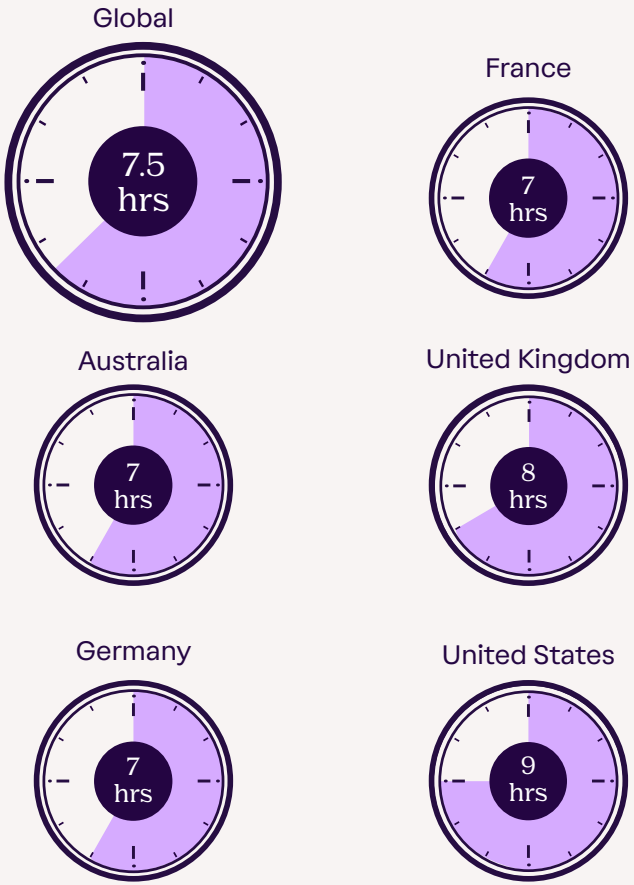
Consequently, nearly half (43%) of businesses have deprioritized compliance due to the time it takes, while 41% admit it's due to the required financial investment.

For organizations with complex operations and global employees, compliance needs grow exponentially as they scale. Nearly half (45%) of companies with over 250 employees say they're not prioritizing compliance due to required financial investment, compared to 38% of smaller organizations.

Increasingly, new means to automate compliance are transforming the way companies demonstrate trust.



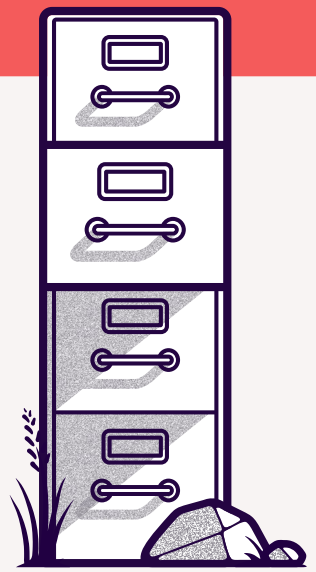
Thinking about an average working week, how much time have you spent on achieving compliance and/or staying compliant by you (or the team responsible)?



Risk management:
An eye on visibility

Risk management remains an ongoing challenge for many. In fact, half (50%) of businesses are still managing risk surfaces manually. This increases to 54% in the UK, the highest of any country surveyed, compared to 45% in the U.S.

The smaller the business, the bigger the problem. Only 35% of businesses with fewer than 251 employees believe they have strong visibility of their risk surfaces compared to a healthier 56% for larger companies.



Enter AI

AI has enormous potential to reduce the repetitive, manual work needed to achieve compliance and prove security. By automating tedious tasks that teams have no choice but to perform manually, businesses have more time to focus on strategic work.

Businesses worldwide recognize the opportunity: 77% already or plan to use AI/ML to detect high risk actions, unsecured cloud storage, unassigned compliance responsibilities, or unrevoked access privileges.

However, over half (54%) are concerned that secure data management is becoming more challenging with AI adoption. And more than half (51%) say that using Generative AI could erode customer trust.

Without proper guardrails, the industry recognizes the inherent risk to using Generative AI, including limited transparency into decision-making due to the vast number of weighted data points that large language models (LLMs) use.

"Human-driven compliance is so slow that it will stifle your innovation and time-to-market. When it comes to compliance, automation is king. The platforms and tools we're using to build our product generate more than enough evidence to prove security. You don't need humans to do unnecessary work to prove your company is trustworthy."

Diego Susa, Head of Engineering
Unleash

PART TWO

The trust managment tipping point

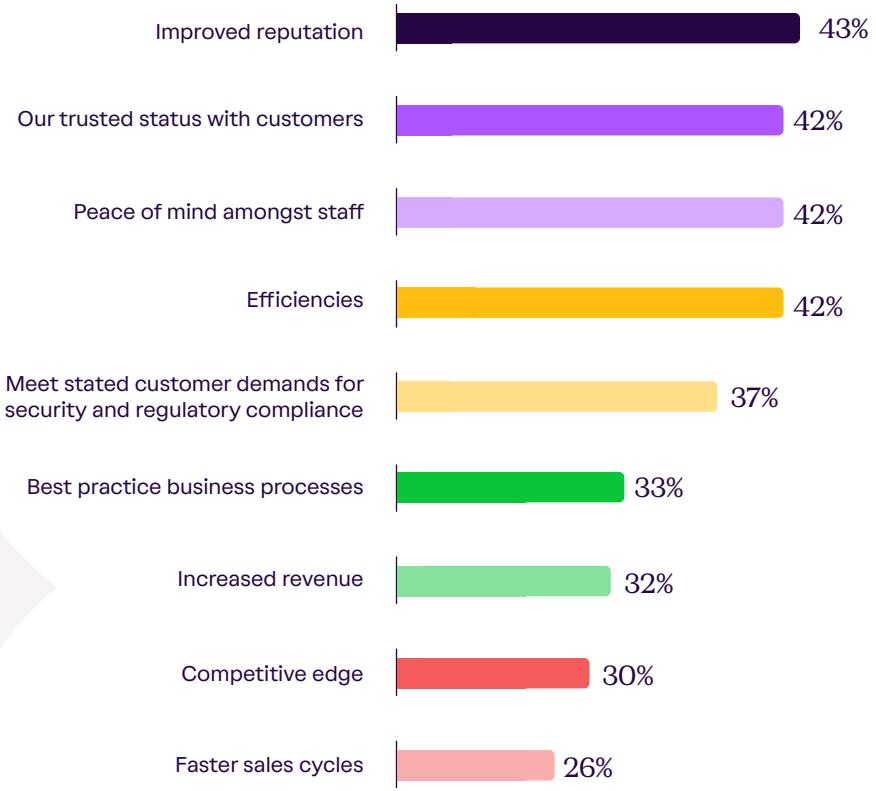
The business case for better security is plain to see. Ultimately, it improves efficiency and boosts the bottom line. Seven out of ten of leaders say that a better security and compliance strategy positively impacts their businesses thanks to stronger customer trust, while nearly three in four (72%) respondents agree that a better security and compliance strategy would make them more efficient.

For 43% of respondents, the biggest value-driver of good security practices is improved reputation.

> "People like to conduct business with companies they trust, and compliance is a key component in building that trust. Pursuing compliance visibly and proactively can significantly raise the trust profile of a business while increasing brand strength."

IDC, IDC PlanScape: Future IT Strategies to Ensure and Manage Compliance Ecosystems, Doc #US49536422, August 2022

Thinking about good security practices, what value do they drive for your business?



PART TWO

Streamlining security and compliance through automation

Improving and proving security doesn't need to be a heavy lift. In fact, 63% of respondents believe that time and money could be saved by automating compliance with different regulations and frameworks. This rises to 67% in the U.S., the highest of any country surveyed.

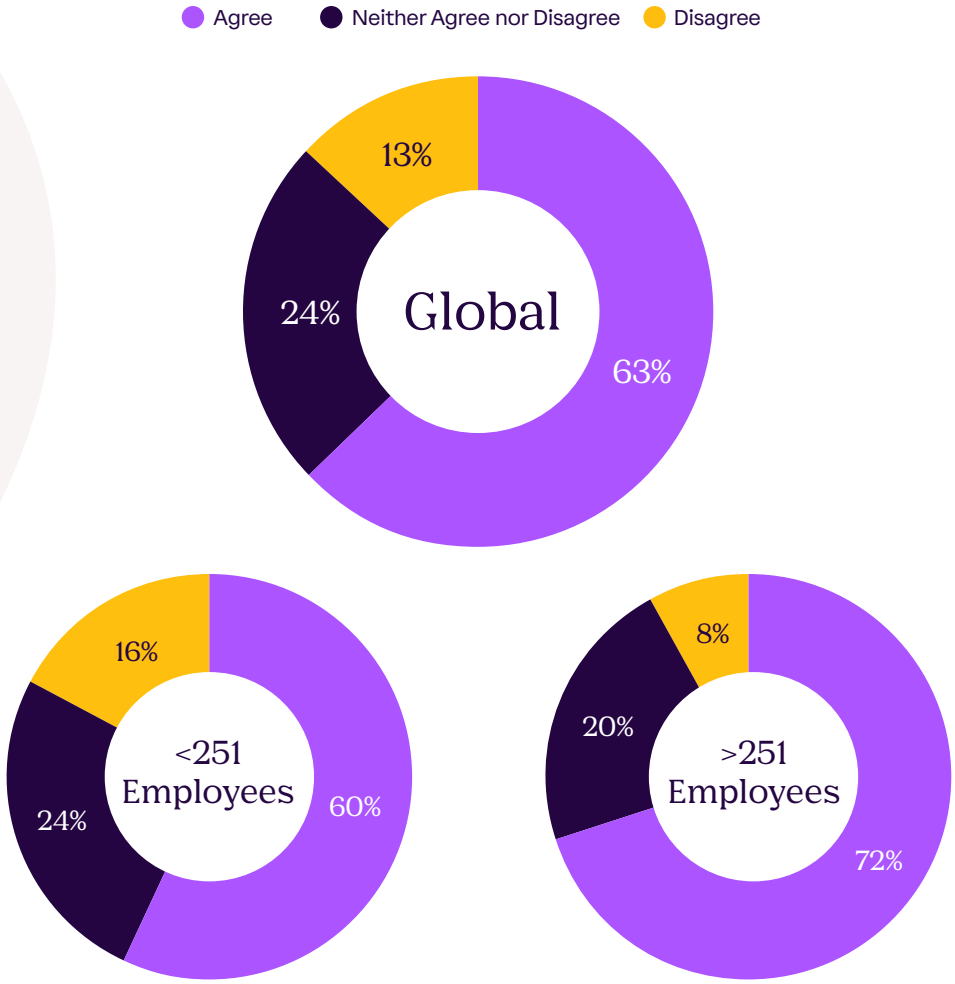
IT decision-makers are in on the time and money-saving secret. Two-thirds (68%) agree automation will save these resources compared to 58% of business decision-making counterparts, a 10% difference.

Automation brings trust and transparency to life, and companies are taking notice. Over 8 in 10 (83%) of businesses have increased or plan to increase their use of automation, in particular for reducing manual work (42%) and streamlining vendor risk reviews and onboarding (37%).

This is true for compliance as well as overall security management. On average, respondents believe they could save at least two hours per week — over 2.5 working weeks a year — if security and compliance tasks were automated.

Three-fifths (60%) agree that their business is more likely to consider automating security compliance when scaling to different markets, rising to 67% for French respondents.

"My company could save time and money on complying with regulations and frameworks through automation."

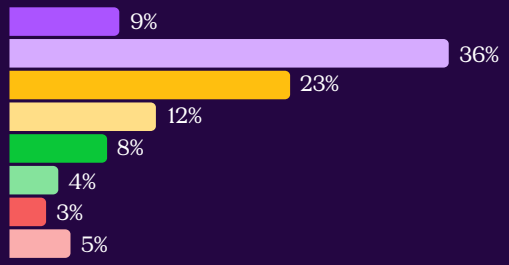


How much time per week do you think you could save on the following security and compliance tasks through automation?

0 hours | 1-2 hours | 3-4 hours | 5-6 hours | 7-8 hours | 9-15 hours | 16+ hours | Not sure

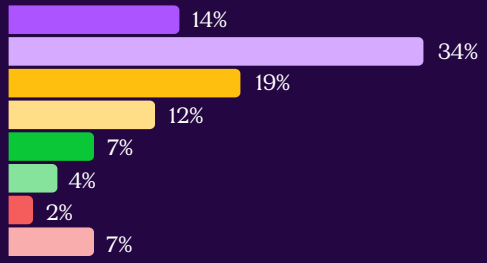
Updating documents and evidence for audits

Median: 3 hours | **% of working week:** 7%



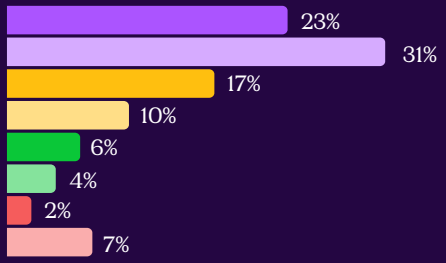
Reviewing and scoring vendor risk

Median: 3 hours | **% of working week:** 7%



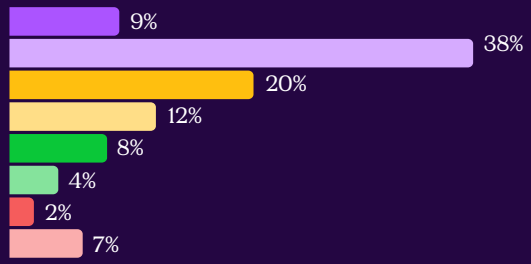
Offboarding employees

Median: 2 hours | **% of working week:** 6%



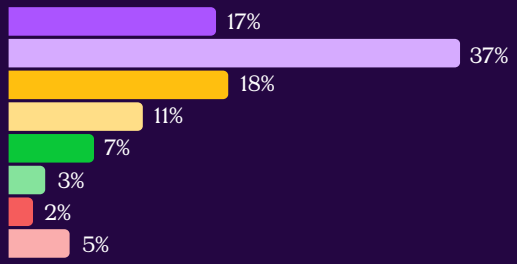
Staying on track with updates to regulations

Median: 3 hours | **% of working week:** 7%



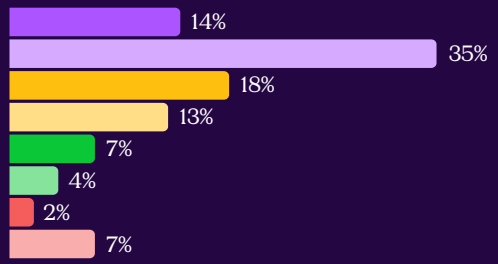
Answering security questionnaires

Median: 3 hours | **% of working week:** 7%



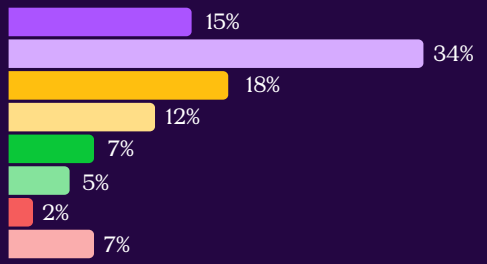
Navigating different market regulations

Median: 3 hours | **% of working week:** 7%



Discovering new vendors & applications being used by employees

Median: 3 hours | **% of working week:** 7%



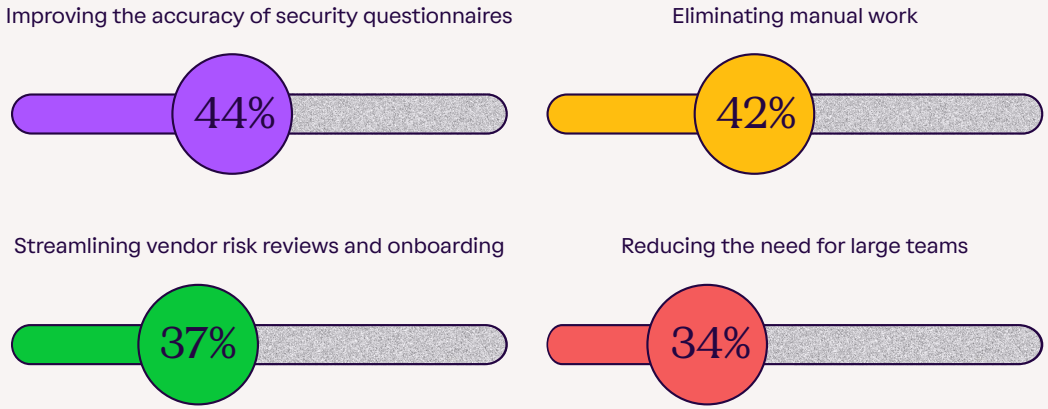
Accelerating security workflows and transforming trust with AI

AI can dramatically accelerate workflows, enabling teams to focus on strengthening their security posture and building customer trust.

Respondents think AI can be transformative to improving the accuracy of security questionnaires (44%), eliminating manual work (42%), streamlining vendor risk reviews and onboarding (37%), and reducing the need for large teams (34%).

Whether saving time, budget or staffing resources, AI can help you do more with less: time-consuming tasks can be handed off to AI-powered trust management platforms. But in a climate of growing cyber-threats, and AI tools presenting a new risk surface, it's essential to prioritize transparency and trust when deploying AI.

Where do you think AI can be most transformative for security teams?

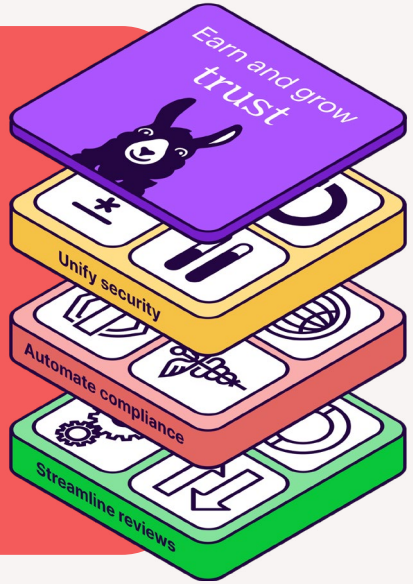


What is trust management?

Trust management[3] is a holistic approach to defining, managing, maturing, and proving your security and compliance commitments. It's a concerted and intentional effort to both become more secure and communicate that security to instill confidence in prospects and customers.

A trust management platform is a single source of truth for centralizing and accelerating these efforts. Key capabilities of a trust management platform include unified security program management, automated compliance, and streamlined security reviews.

With a trust management platform, businesses of all sizes are able to move from point-in-time assessments to real-time visibility of their security posture, enabling them to increase efficiency, reduce risk, and demonstrate trust continuously.



3 - https://www.vanta.com/resources/what-is-a-trust-management-platform

Vanta's AI principles

The following AI principles outline how we plan to steward the safe and effective deployment of AI. These principles have been developed in line with the NIST AI Risk Management Framework[4] and seek to move Vanta iteratively toward further alignment with the framework and its intentions. All AI projects at Vanta follow these principles, from conception to launch — and beyond.

Do no harm

All usage of AI at Vanta must first and foremost seek to do no harm to its customers or to Vanta. Reasonable attempts should be made to predict any and all potential cases of harm posed by a project.

Security and privacy by design

Every AI project and ongoing effort must incorporate security and privacy by design from day 0 and at every substantive change. Evidence must be shown.

Impact of incorrectness

Projects must commit to and have practical, achievable plans to assess the likelihoods and impacts of incorrectness and design human-in-the-loop review processes where necessary.

Explainability and transparency

Reasonable efforts are taken to ensure the explainability of results and provide transparency into the process by which they were derived.

Data control and risk

A clear understanding of the data being used by AI is established and guardrails are in place to control the scope of data access. A plan is established for the risks posed by such access as well as the resulting outputs.

4 - https://www.nist.gov/itl/ai-risk-management-framework

Conclusion

Improving and proving security is harder than ever. The risk of attacks is rising, and AI has added another layer of complexity for IT and business leaders to navigate. In today's challenging economic climate, companies have been forced to reduce the resources and budget to solve these very problems.

Organizations are being slowed down by manual tasks and face increased risk as they mature. Without the ability to prove their security efforts, companies can't scale, leaving themselves vulnerable to falling behind competitors.

The tipping point for trust management is here.

Supercharged by AI, trust management is critical to reducing the tedious and repetitive security tasks that pull teams away from their most strategic work. For companies at the forefront of this disruption, centralizing security processes, automating compliance, and accelerating security reviews can turn trust into a marketable advantage. By closing the loop on the security lifecycle from compliance through continuous monitoring and communication, businesses can transform how they build trust and ultimately unlock growth.

Trust management essentials

- **Centralize:** Establish a single source of truth to unify your security and compliance programs.
- **Automate:** Use automation and AI to reduce manual work, like collecting evidence and completing security questionnaires.
- **Differentiate:** Use security as a competitive advantage during sales conversations.
- **Assess:** Review vendor security regularly to ensure they uphold your commitments.
- **Demonstrate:** Proactively show customers your security posture through audits, continuous monitoring, and a public Trust Center.

Methodology

In September 2023, quantitative research conducted by Sapio Research was commissioned by Vanta to understand the challenges and opportunities businesses are facing when it comes to security and trust management. Vanta and Sapio co-designed the questionnaire and surveyed the behaviors and attitudes of 2,500 business and IT leaders across Australia, France, Germany, the UK, and U.S.

About Vanta

Vanta is the leading trust management platform that helps simplify and centralize security for organizations of all sizes. Thousands of companies including Atlassian, Autodesk, Chili Piper, Flo Health and Quora rely on Vanta to build, maintain and demonstrate their trust — all in a way that's real-time and transparent.

For more information, visit www.vanta.com