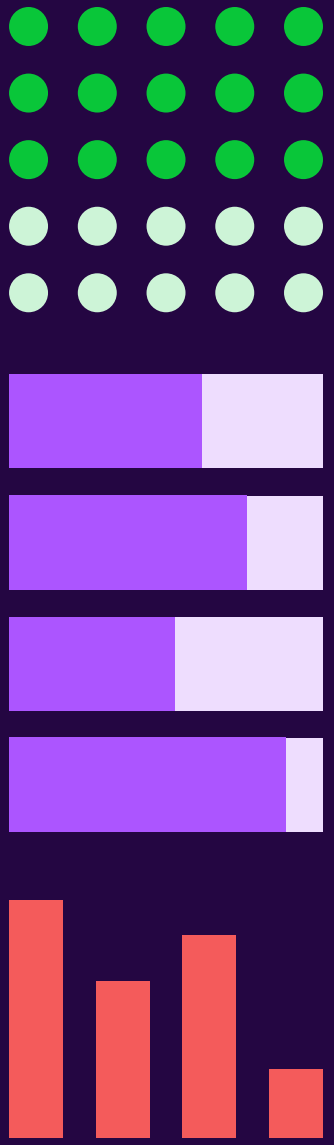
The State of Trust Report 2024



Vanta

Table of contents

Introduction

Trust is critical to the success of every business. But building, scaling, and demonstrating trust is getting harder for organizations.

To meet customer expectations, security leaders and their teams must address complex threats, a growing compliance burden, and increasing risk from their third-party vendor footprint. The rapid adoption of AI technologies only adds to the challenge, requiring more oversight and governance.

Vanta's second annual State of Trust Report uncovers key trends across these areas of security, compliance, and the future of trust. Based on a survey of 2,500 IT and business leaders in the U.S., UK, and Australia, our research found that more than half (55%) of organizations say that security risks for their business have never been higher.

But as risks increase, so do the opportunities. Automation and AI can significantly minimize the manual security and compliance tasks that prevent security teams from focusing on mission-critical work. According to our research, just 11% of a company's IT budget is dedicated to security—but in an ideal world, leaders say it should be 17%.

This is where automation and AI can play a transformative role in unlocking efficiencies for security teams and ultimately, business value for organizations.

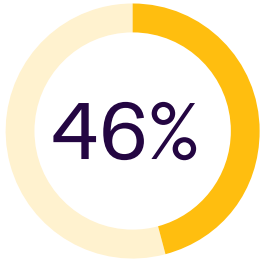
Key findings

55%
of businesses think that security risks for their organization have never been higher.

53%
of organizations say cybersecurity threats are their number one concern, higher than financial and operational risk.

11 working weeks
a year are spent on compliance tasks, increasing by a week since last year.

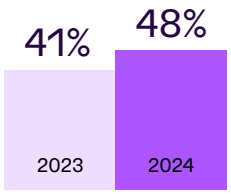
5 working weeks
a year could be saved by automating security and compliace tasks.



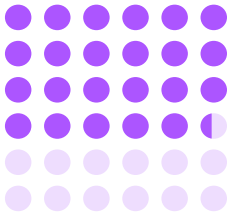
of organizations say that a vendor of theirs has experienced a data breach since they started working together.

6.5 hours

IT decision makers spend an average of 6.5 hours per week assessing and reviewing vendor risk.



Nearly half
believe good security practices drive customer trust for their business, an increase of 7% from 2023.



Nearly two-thirds
(65%) of organizations say that customers, investors, and suppliers increasingly require demonstration of compliance.

1.

The state of trust today

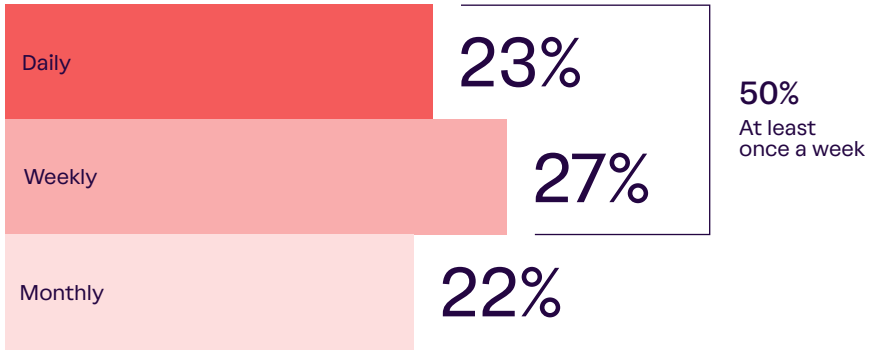
The security landscape—compounded by third-party risk and AI—has never been more challenging

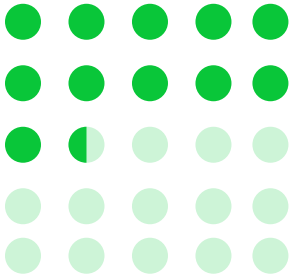
Cybersecurity threats are the number one concern for businesses in 2024, higher than financial and operational risk. And more than half (55%) of organizations say that security risks have never been higher, with 50% of organizations detecting and responding to cybersecurity threats at least once a week.

Further complicating security is vendor risk—almost half (46%) of organizations say that a vendor of theirs has experienced a data breach since they started working together.

At the same time, more than half (51%) of organizations have concerns around the use of AI and the risks it poses for the security of the organization.

Frequency of detecting and responding to cybersecurity threats

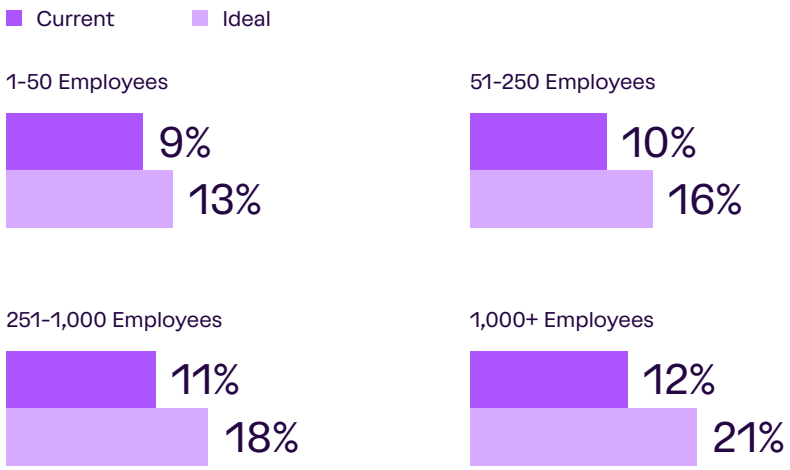


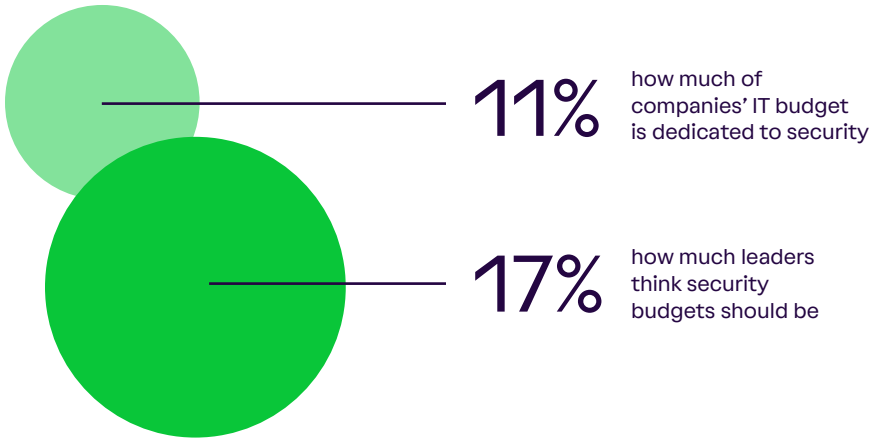


46%

of organizations have had a vendor experience a data breach since they started working together

Current and ideal security budget percentage climbs with organization size





Security budgets and investment are not where leaders think they should be, especially in larger organizations

Despite increasing security risks, just 11% of a company's IT budget is dedicated to security—but in an ideal world, leaders say it should be 17%.

The larger the organization, the more of its IT budget is spent on security. However, for organizations with over 1,000 employees, leaders say that 21% of their organization's security budget would ideally be dedicated to security when it is currently just 12%.

Compounding this challenge is the fact that over 1 in 10 (11%) organizations have decreased their investment in hiring cybersecurity staff—an ongoing consequence of a tough economy, budget constraints, and talent shortages.

While threats are increasing, businesses are also facing growing security expectations. Nearly two-thirds (65%) of organizations say that customers, investors, and suppliers are increasingly requiring proof of compliance. To establish and deepen trust with customers, businesses need to prioritize security resourcing.

“Security doesn’t need to be complex. It needs to scale the business, be a business enabler, and it needs to be there at the very beginning. Without it, it’s only a matter of time before there’s a serious issue.”

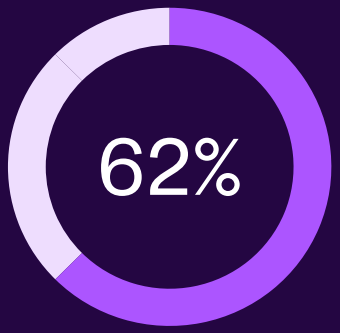
Leo Cunningham, Former CISO
Flo Health

As AI adoption accelerates, governance and risk management stall

At the same time that AI is becoming increasingly common in the tech stack, security concerns are also on the rise. A majority (62%) of businesses plan to invest more in security around the use of AI within their organization in the next year. And over the last 18 months, cyber risks and threats have gone up, with businesses experiencing more phishing attacks (33%), a rise in AI-based malware (32%), and more compliance violations (27%).

AI governance and risk management, however, are still relatively nascent. Only 2 in 5 (37%) organizations currently conduct, or are in the process of conducting, regular AI risk assessments. When it comes to formal policies for governing AI usage, only 36% of organizations have, or are in the process of putting, a company AI policy in place despite the increased use of AI tools. This rises as high as 42% in the UK, but falls as low as 28% in Australia.

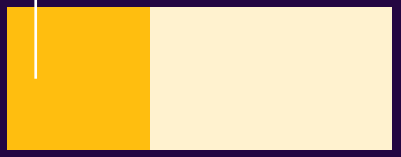
Building trust in AI



of organizations plan to invest more in AI security in the next 12 months

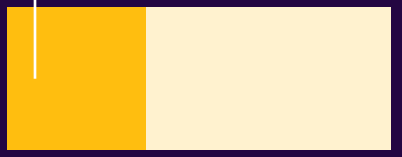
37%

of organizations have conducted, or are in the process of conducting, regular AI risk assessments



36%

of organizations have, or are in the process of putting, a company AI policy in place



“Being an AI company requires us to build an even deeper level of trust because this technology is largely unknown. We need our customers to see us as a trusted partner to help them implement this.”

Peadar Coyle, CTO and Co-Founder
AudioStack

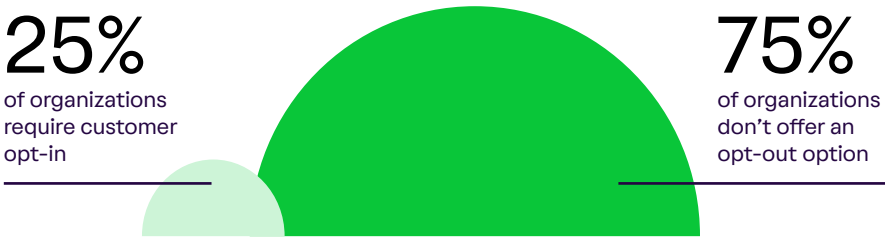
Protecting customer trust in a AI world

Building and maintaining trust is even more critical as organizations accelerate their usage of AI to develop and deliver new products. This means committing to safe and ethical AI practices and prioritizing transparency, particularly when it comes to training AI models.

Almost one-third of organizations (31%) use a mix of customer and synthetic data to train AI models, while 27% use anonymized customer data. Further, while 25% of organizations require opt-in from customers to use their data for AI training, over 75% of companies don’t offer an opt-out option.

While the future of AI is far from set, organizations can maintain trust by giving customers control over their data through an informed consent model. This vigilance should extend to third parties too, and companies should require a formal data processing agreement (DPA) stipulating that vendors not use customer data to train their AI models.

Training AI with customer data



2.

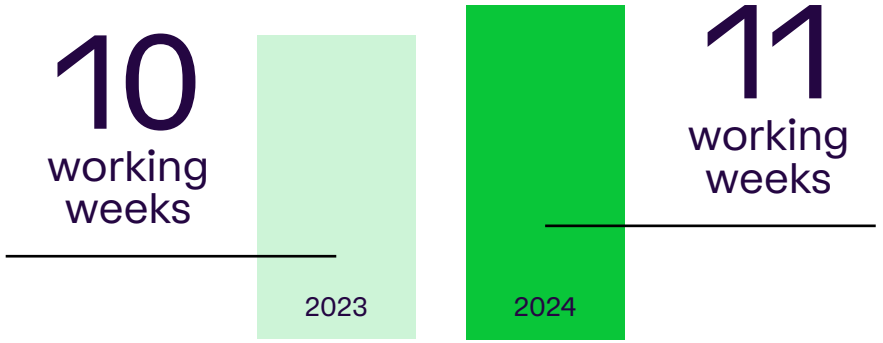
Easing the compliance burden

The compliance burden has never been higher

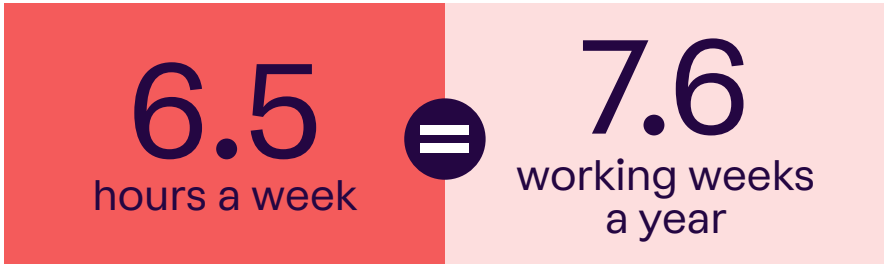
Time spent on compliance tasks increased to 11 working weeks in 2024—up from 10 working weeks in 2023. And 1 in 10 (9%) respondents are spending over 21 hours each week—25 working weeks a year—on security compliance. Meanwhile, organizations in the UK spend the most time on compliance out of all regions—12 working weeks a year (an increase of two hours a week compared to 2023).

When it comes to security program management across organizations, IT decision makers spend an average of 6.5 hours per week—7.6 working weeks a year—assessing and reviewing vendor risk.

Time spent on manual compliance per year is going up



The average time IT decision makers spend on assessing and reviewing vendor risk



“We don’t have time for manual work such as tracking in spreadsheets, sending emails, creating documentation for auditors and vendor management. In order for us to successfully mitigate risk and focus on what’s important for the business, these tasks need to take up less than 10% of my team’s time.”

Michael Hensley, Head of Information Security and HIPAA Security Officer

Modern Health

There is also a significant gap in the frequency of foundational security activities depending on whether organizations have a dedicated security budget.

How budgets impact the frequency of security activities

Security and compliance automation frees up time and improves efficiency for security teams

The scale of activities required for compliance is extensive. But with automation, security professionals could save 10% of the working week. In 2024, organizations estimate that they could save more time through automation than they did in 2023.

Automation is of growing importance to security teams, with 44% of organizations saying that their investment in automation for security operations has increased over the past year. And 6 in 10 (59%) say that automating manual work is a priority for their security and compliance strategy.

On average, security teams could save between 3-5 hours a week by automating activities like user access reviews, employee management, and answering security questionnaires—allowing them to focus on strategic security initiatives.

While 72% of IT decision makers say that their company could save time and money through automation, just 57% of business decision makers say the same. Leaders from the frontlines of security can help bridge this gap by getting buy-in for automation that reduces time-consuming processes. Automation not only benefits the business but also improves employee wellbeing, with 39% of respondents agreeing that good security practices bring peace of mind.

6 in 10

of organizations say that the automation of manual work is a priority for their security and compliance strategy

Estimated hours saved through automation per working week

3.

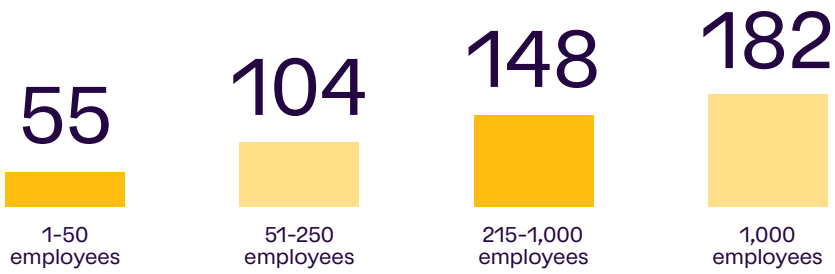
Trust and third-party risk

Third-party risk increases as companies scale

Managing vendor risk is a challenge for any business, and this only becomes more difficult as a company scales. The larger the business, the more vendors they have—and the bigger the associated risk.

At the same time, less than a quarter (24%) of organizations rate their visibility into vendor risk as "very strong." With almost half (48%) of organizations saying that a vendor they work with has previously experienced a breach, businesses need to implement a proactive approach that reduces risk and enables continuous visibility into their third-party landscape.

The average number of vendors according to organization size



"We have an ever-growing and ever-changing list of vendors, and we need to stay on top of them while having finite resources. Vanta's Vendor Risk Management helps me stay on top of all of our vendors and see at a glance which ones need an updated review."

Quentin Berdugo, Chief Information Security Officer
Pigment

Confidence in vendor compliance is high, but third-party breaches undermine overall security and trust

The majority of organizations (69%) feel confident that their vendors comply with relevant industry standards and regulations. But breaches are still prevalent, and regardless of their security maturity, 46% of businesses say that a vendor of theirs has had a data breach since they started working with them or using their products.

These types of breaches have a serious impact on customer trust, with 62% agreeing that third-party breaches negatively impact their organization's reputation. One in two (50%) businesses say they've terminated a vendor relationship due to security concerns.

To maintain and scale trust—both across their own organizations and their third-party vendors—forward-thinking leaders need to go beyond the standard of point-in-time checks towards a holistic and continuous approach to monitoring.

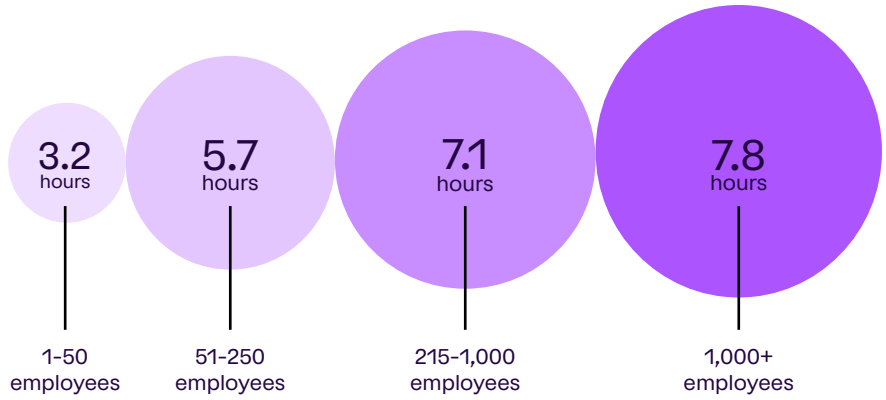
One in two businesses say they have terminated a vendor relationship due to security concerns

AI can transform vendor risk management and security reviews

On average, organizations spend 6 hours per working week—the equivalent of 7 working weeks a year—on vendor security reviews and risk assessments. But organizations now see even more potential in AI to streamline vendor risk reviews and onboarding than they did last year—up from 35% in 2023 to 42% in 2024.

IT and business leaders say the most transformative areas for AI are improving the accuracy of security questionnaires (43%), streamlining vendor risk reviews and onboarding (42%), eliminating manual work (38%), and reducing the need for large teams (30%).

Hours per week spent on vendor security reviews by organization size



4.

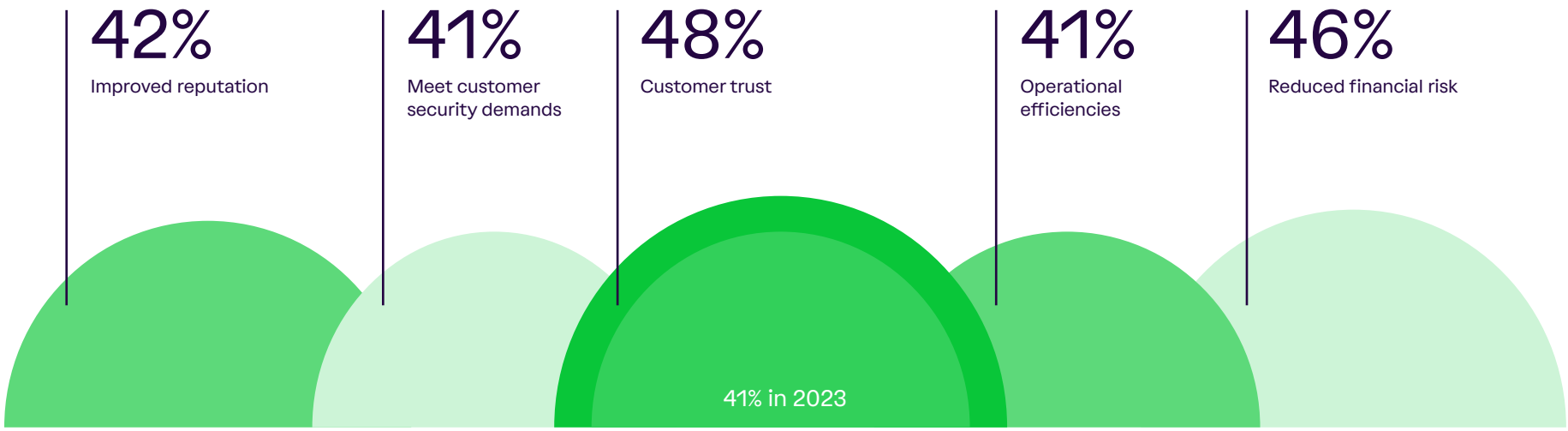
Good security is good business

Demonstrating trust continues to drive business value

As the security expectations of customers grow, leaders continue to recognize the business value of investing in security—and demonstrating it. Close to two-thirds (65%) of organizations say that customers, investors, and suppliers increasingly require demonstration of compliance.

Nearly half (48%) of organizations believe good security practices drive customer trust for their business (up 7% from last year), and 46% recognize that good security practices lead to reduced financial risks.

The value of good security practices



“Our big opportunity as a compliance team is looking at every compliance activity as a sales activity.”

Leah Bosé, Senior Privacy Compliance Manager
ZoomInfo

Confidence in reporting on security program outcomes is high, but measuring the ROI of trust is more challenging

An overwhelming 85% of organizations are confident in their team's ability to show the impact of their security program on the business. Further, 9 in 10 (89%) quantify and measure the impact of their program in some capacity.

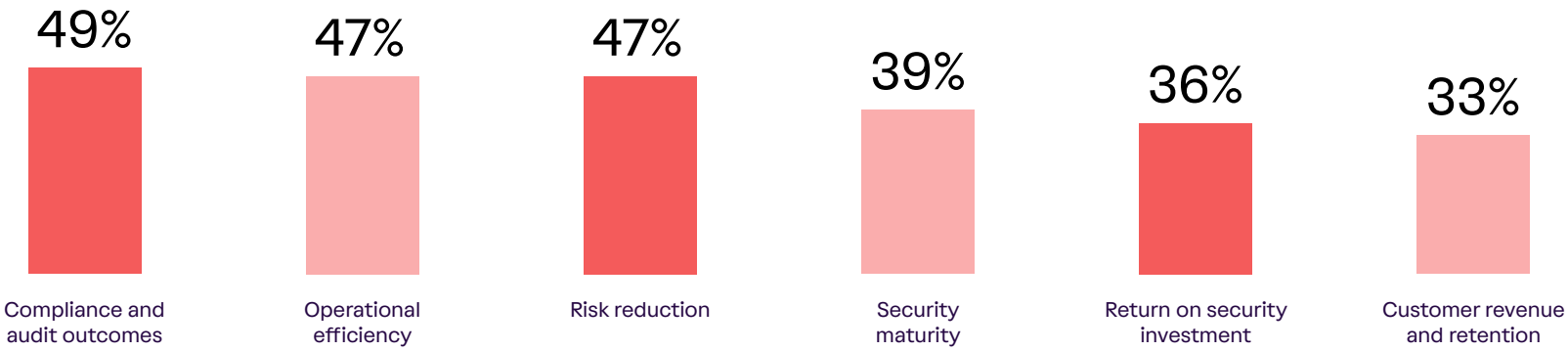
The top three ways that organizations measure impact are: compliance and audit outcomes, operational efficiency, and risk reduction.

While teams are quantifying and measuring impact, only 36% are measuring actual ROI. And even fewer are tracking the security program's impact on customer revenue and retention. With increasing pressure on security teams to demonstrate measurable impact—in addition to reduced risk—leaders need actionable reporting capabilities that centralize visibility across their security program.

83%

of organizations are confident in their team's ability to show the impact of their security program on the business

How organizations are measuring a security program's impact



Conclusion: Go beyond the standard with trust management

For organizations of all sizes, building and scaling trust is difficult. With more reliance on third-party vendors and increased use of AI technologies, security leaders face a more complex threat landscape while managing resource constraints.

But the tools available today only make this work more challenging. Teams are stuck with screenshots and spreadsheets or legacy solutions that rely on manual updates and only provide point-in-time visibility into their security posture.

To keep pace with where the future of trust is headed, security leaders need to go beyond the standard way of doing things. They need to make trust continuous, collaborative, and automated across every part of their business. With trust management, organizations can not only reduce risk, but also build customer confidence and accelerate revenue growth.

Here are three ways that organizations can start to make this shift:

01

Build a trust program powered by automation

The tools you use to manage your trust program should help rather than hold you back. Implement trust management platforms that automate key workflows, continuously monitor your security and compliance, and provide centralized visibility and insights across your program.

02

Demonstrate trust in real time

Go beyond point-in-time compliance certifications and create opportunities to proactively demonstrate and maintain trust with customers. This looks like showcasing your security controls through a public Trust Center and instantly and accurately responding to security questionnaires with the help of AI.

03

Strengthen your entire trust network

Trust isn't just a reflection of your organization. It also reflects your network of vendors and partners. Raise the bar by establishing your own standard for trust in your organization. Create custom controls based on your definition of what good security looks like for those that do business with you to strengthen trust across your ecosystem.

Methodology

In July and August 2024, 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 Research co-designed the questionnaire and surveyed the behaviors and attitudes of 2,500 business and IT leaders across the U.S., UK, and Australia. Year-over-year comparisons for relevant questions were calculated using only the U.S., UK, and Australia datasets from The State of Trust Report 2023.

About Vanta

Vanta is the leading trust management platform that helps organizations of all sizes automate compliance, manage risk, and prove trust. Thousands of companies including Atlassian, Omni Hotels, Quora, and ZoomInfo rely on Vanta to build, maintain and demonstrate trust—all in a way that's continuous and transparent. Founded in 2018, Vanta has customers in 58 countries with offices in Dublin, London, New York, San Francisco and Sydney.

For more information, visit www.vanta.com.

Vanta