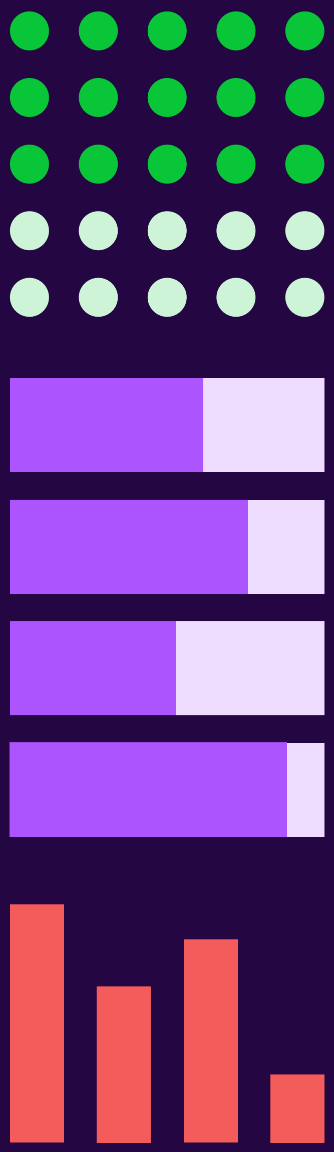
AUSTRALIA

The State of Trust Report 2024



Vanta

Table of contents

Introduction

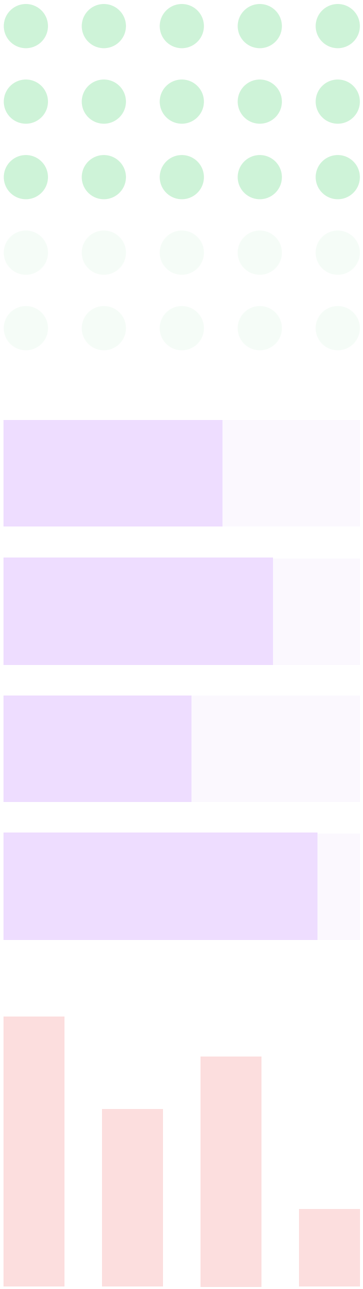
Trust is critical to the success of every business. But building, scaling and demonstrating trust is getting harder for Australian organisations.

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 (with 500 of the respondents from Australia), our research found that more than half (58%) of Australian organisations say that security risks for their business have never been higher.

But as risks increase, so do the opportunities. Automation and AI can significantly minimise the manual security and compliance tasks that prevent security teams from focusing on mission-critical work. According to our research, in Australia just 10% of a company's IT budget is dedicated to security – but in an ideal world, leaders say it would be 14%.

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



Key findings - Australia

58%

of Australian organisations think that security risks for their organisation have never been higher.

#1

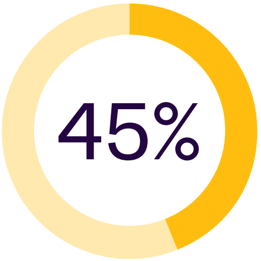
Cybersecurity threats are the number one concern for Australian businesses in 2024, higher than financial and operational risk.

9 working weeks

are being spent on compliance tasks in 2024.

5 working weeks

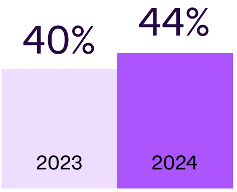
a year could be saved if security and compliance tasks were automated.



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

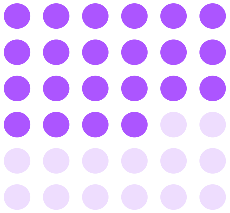
5 hours

IT decision makers in Australia spend an average of 5 hours per week – the equivalent of 6 working weeks a year – assessing and reviewing vendor risk.



Nearly half

of Australian organisations believe good security practices drive customer trust for their business, an increase of 4% from 2023.

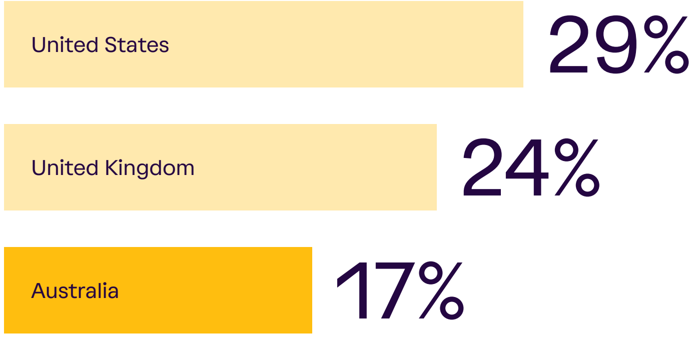


Nearly two-thirds

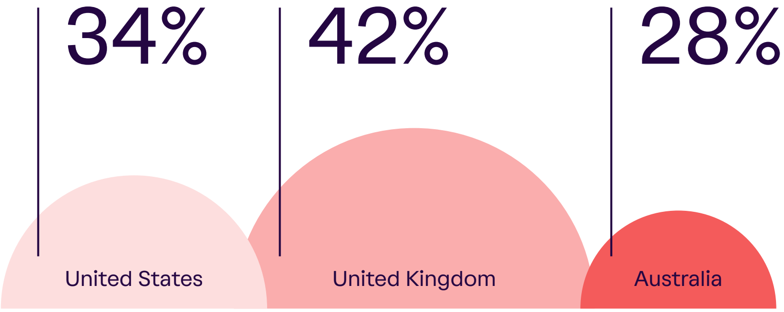
(62%) of Australian organisations say that customers, investors and suppliers increasingly require demonstration of compliance.

Australia vs other countries

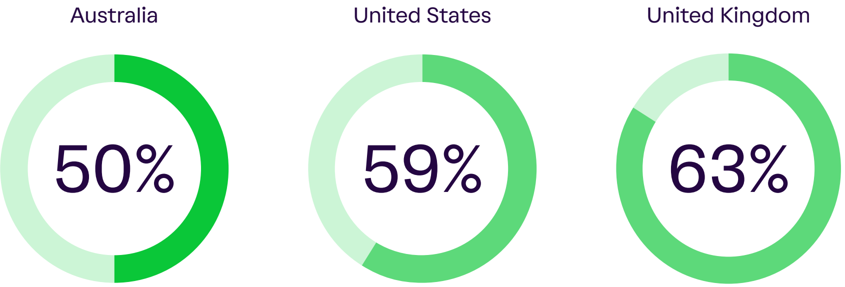
Companies in Australia have the least insight into vendor risk, with only 17% having "strong" visibility.



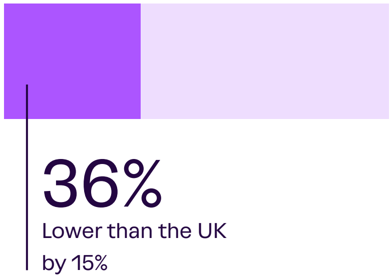
Only 28% of companies in Australia have, or are in the process of putting, a company AI policy in place – lower than all other countries.



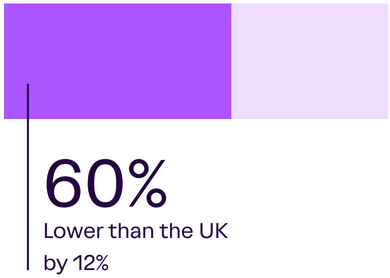
In Australia, 50% of organisations have a dedicated team to oversee AI security and compliance – lower than all other countries.



Organisations in Australia are the least likely to have increased their investment in automation for security operations.



Only 60% of Australian organisations have a formal policy for assessing and managing third-party risk.



1.

The state of trust today

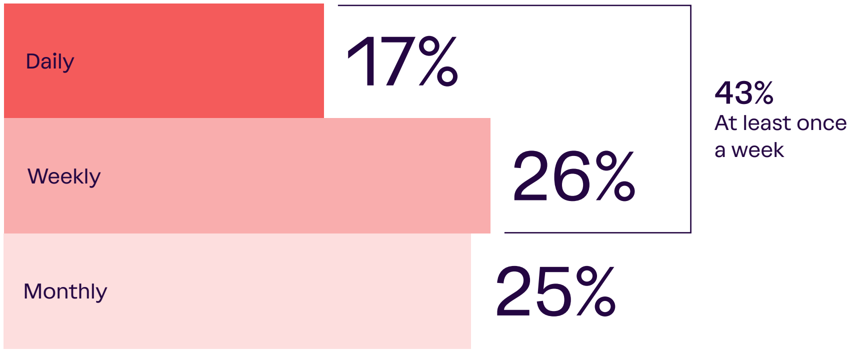
The security landscape — compounded by third-party risk and AI — has never been more challenging

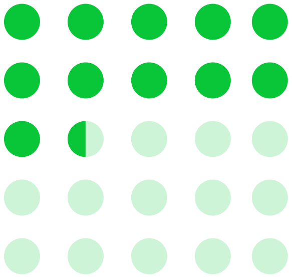
Cybersecurity threats are the number one concern for businesses in 2024, higher than financial and operational risk. And more than half (58%) of Australian organisations say that security risks have never been higher, with 43% of Australian organisations detecting and responding to cybersecurity threats at least once a week.

Further complicating security is vendor risk – almost half (45%) of Australian organisations say that a vendor of theirs has experienced a data breach since they started working together.

At the same time, almost half (49%) of Australian organisations have concerns around the use of AI and the risks it poses for the security of the organisation.

Frequency of detecting and responding to cybersecurity threats





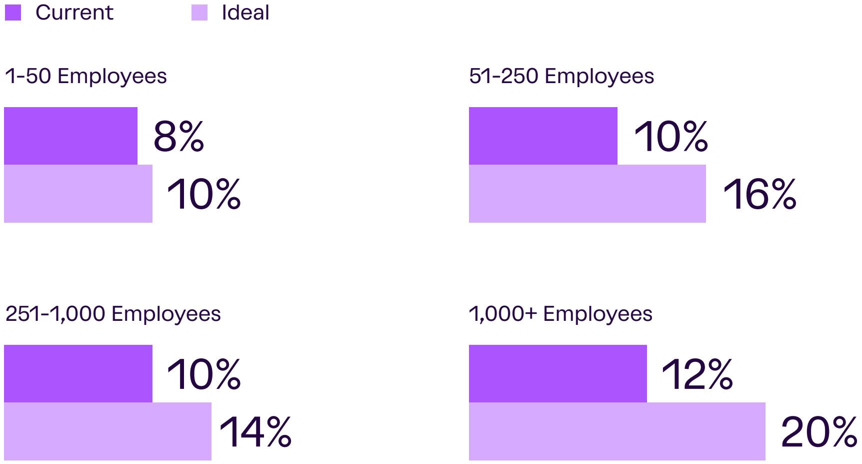
45%

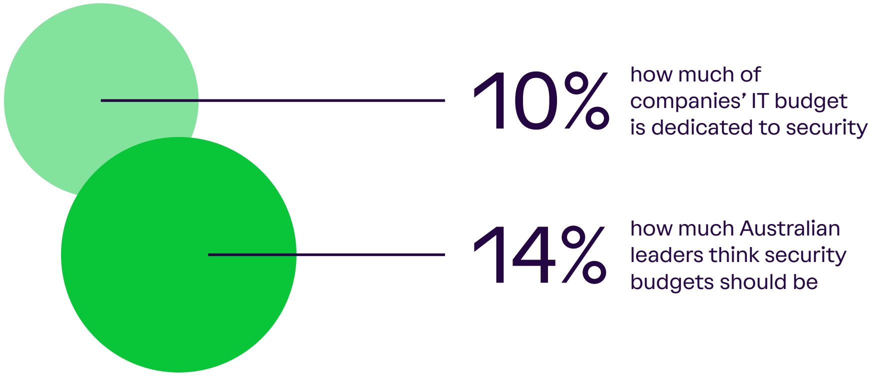
of Australian organisations have had a vendor experience a data breach since they started working with them.

“Trust is difficult to regain once lost… It’s easier to get and maintain compliance while your company is still small.”

Inian Parameshwaran, Software Engineer
Supabase

Current and ideal security budget percentage climbs with organisation size





10% how much of companies' IT budget is dedicated to security

14% how much Australian leaders think security budgets should be

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

Despite increasing security risks, just 10% of a company's IT budget in Australia is dedicated to security – but in an ideal world, leaders say it would be 14%.

The larger the organisation, the more of its IT budget is spent on security. However, for Australian organisations with over 1,000 employees, leaders say that 20% of their organisation'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 (12%) Australian organisations have decreased their investment in hiring cybersecurity staff – an ongoing consequence of a tough economy, budget constraints and talent shortages.

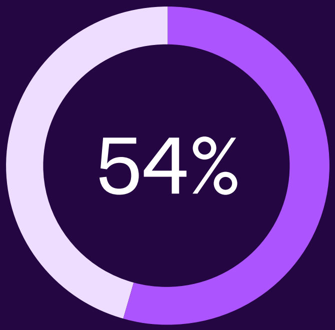
While threats are increasing, businesses are also facing growing security expectations. Nearly two-thirds (62%) of Australian organisations say that customers, investors and suppliers are increasingly requiring proof of compliance. To establish and deepen trust with customers, businesses need to prioritise security resourcing.

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 (54%) of Australian businesses plan to invest more in security around the use of AI within their organisation in the next year. And over the last 18 months, cyber risks and threats have gone up, with Australian businesses experiencing more phishing attacks (32%), a rise in AI-based malware (29%) and more compliance violations (24%).

AI governance and risk management, however, are still relatively nascent. Only 26% of Australian organisations currently conduct, or are in the process of conducting, regular AI risk assessments. When it comes to formal policies for governing AI usage, only 28% of Australian organisations have or are in the process of putting a company AI policy in place despite the increased use of AI tools – lower than all other countries.

Building trust in AI



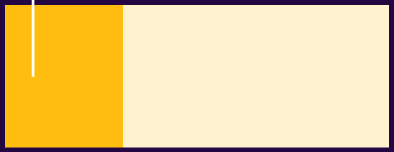
of Australian organisations plan to invest more in AI security in the next 12 months

26%

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

28%

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



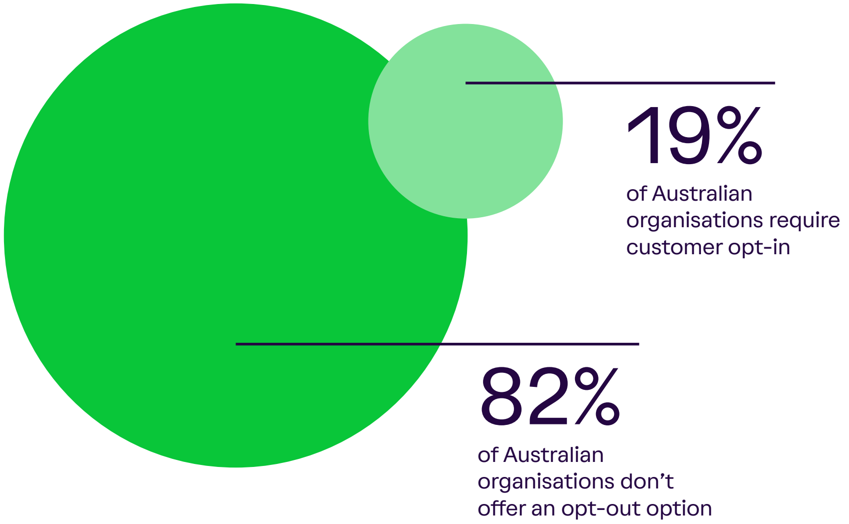
Protecting customer trust in a AI world

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

Almost a quarter of Australian organisations (22%) use a mix of customer and synthetic data to train AI models, while 24% use anonymized customer data. Further, while 19% of Australian organisations require opt-in from customers to use their data for AI training, 82% of companies don't offer an opt-out option.

While the future of AI is far from set, Australian organisations 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

Australian organisations are spending an average of 9 working weeks on achieving compliance in 2024. And 5% of respondents are spending over 21 hours each week – over 25 working weeks a year – on security compliance. This is the least amount of time spent on compliance out of the countries surveyed.

When it comes to security program management across Australian organisations, IT decision makers spend an average of 4.6 hours per week – 5.6 working weeks a year – assessing and reviewing vendor risk.

Time spent on manual compliance is staying the same

9

working weeks

a year in 2023 and 2024

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

4.6 hours a week = **5.6** working weeks a year

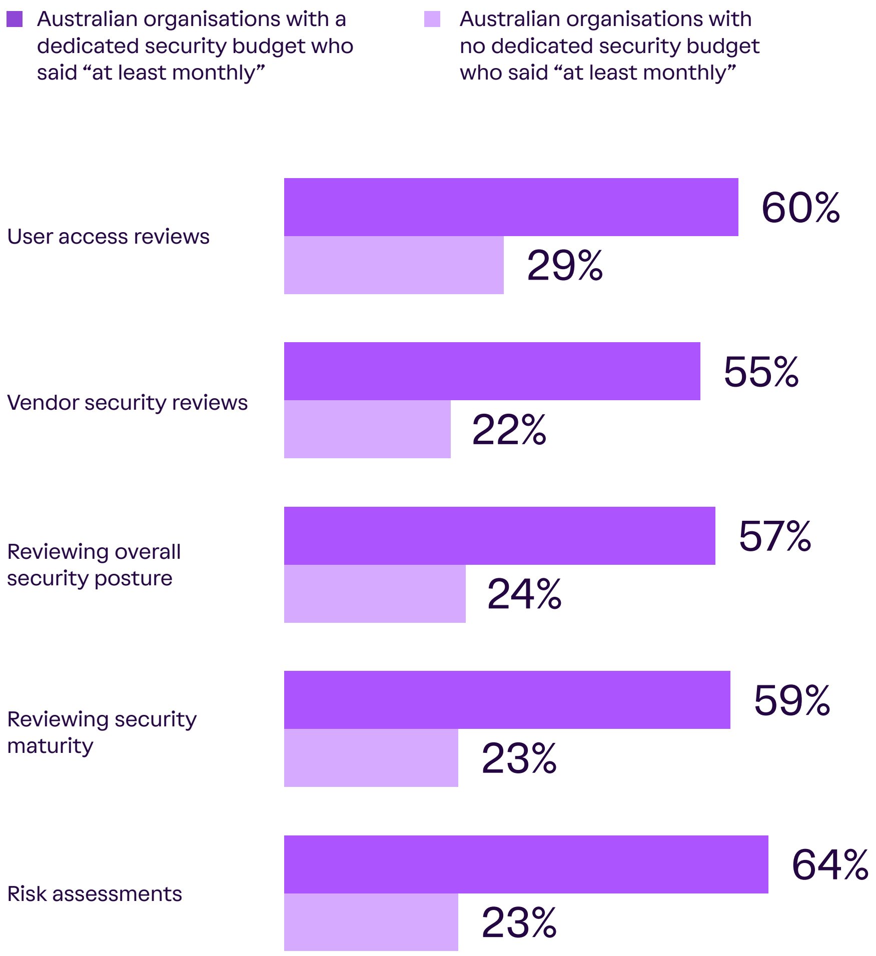
> “In previous years, it would take four quite senior people 15 hours each to get all the evidence together and go back and forth with the auditor. But last September, we got an auditor who could work in Vanta, and it took me just five hours to pull everything together on my own.”

Nathan Miller, Head of Information Security & Compliance

Dovetail

There is also a significant gap in the frequency of foundational security activities depending on whether Australian organisations 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, Australian security professionals could save 8% of the working week. In 2024, Australian organisations estimate that they could save more time through automation than they did in 2023.

Automation is of growing importance to security teams, with 36% of Australian organisations saying that their investment in automation for security operations has increased over the past year. And more than half (56%) say that automating manual work is a priority for their security and compliance strategy.

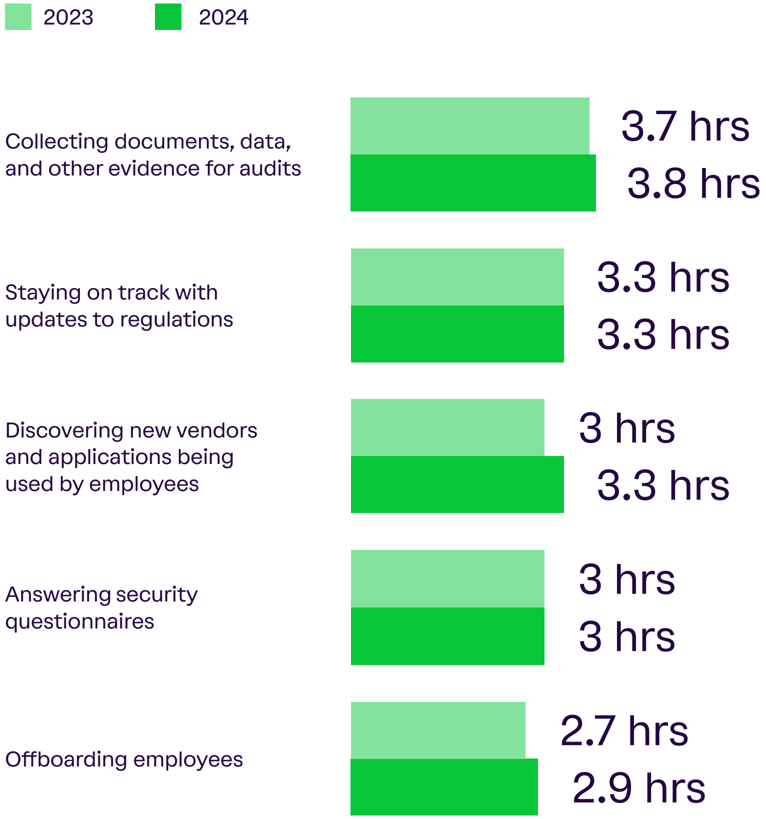
On average, security teams in Australia could save between 2-4 hours a week by automating activities like user access reviews, employee management and answering security questionnaires – allowing them to focus on strategic security initiatives.

While 63% of Australian IT decision makers say that their company could save time and money through automation, just 54% 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 34% of respondents in Australia agreeing that good security practices bring peace of mind.

More than half

of Australian organisations 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.

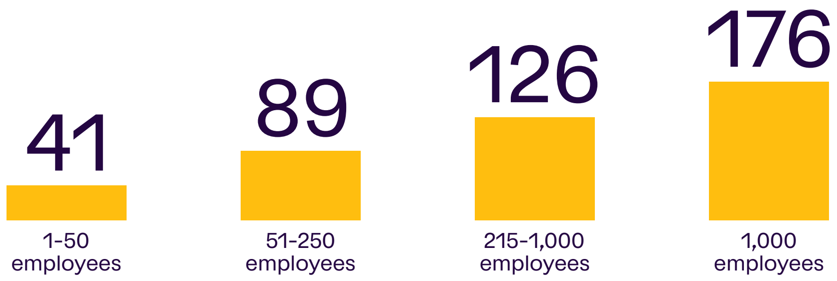
Trust and third-party risk

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 fifth (17%) of Australian organisations rate their visibility into vendor risk as "very strong" — lower than all other countries. With almost half (46%) of Australian organisations 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



> "Using different tools for vendor risk management and compliance led to a patchwork approach to vendor security, which required more work on my part to consolidate notes and findings on each vendor. It definitely prevented me from working as efficiently as I wanted to."

Cameron Perry, Staff Site Reliability Engineer

Kapiche

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

The majority of Australian organisations (64%) feel confident that their vendors comply with relevant industry standards and regulations. But breaches are still prevalent, and regardless of their security maturity, 45% of Australian businesses say that a vendor of theirs has had a data breach since they started working with them or using their products.

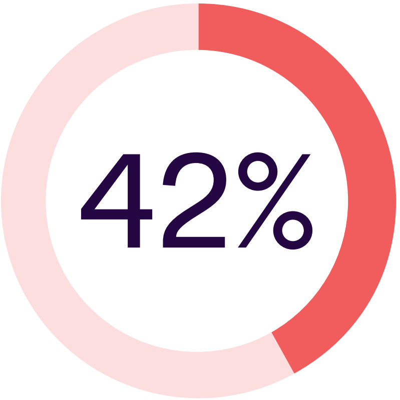
These types of breaches have a serious impact on customer trust, with 60% agreeing that third-party breaches negatively impact their organisation's reputation. More than 2 in 5 (42%) Australian businesses say they've terminated a vendor relationship due to security concerns.

To maintain and scale trust — both across their own Australian organisations 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.

AI can transform vendor risk management and security reviews

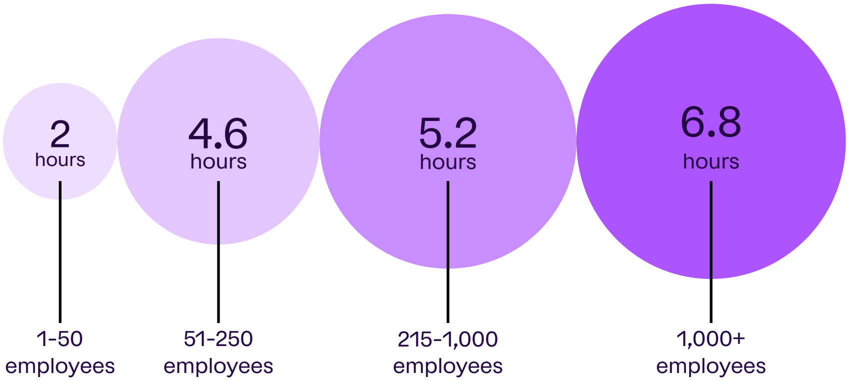
On average, Australian organisations spend 4.4 hours per working week — the equivalent of over 5 working weeks a year — on vendor security reviews and risk assessments. But Australian organisations now see even more potential in AI to streamline vendor risk reviews and onboarding than they did last year — up from 35% in 2023 to 42% in 2024.

IT and business leaders in Australia say the most transformative areas for AI are streamlining vendor risk reviews and onboarding (42%), improving the accuracy of security questionnaires (37%), eliminating manual work (37%) and reducing the need for large teams (26%).



More than 2 in 5 businesses saying they have terminated a vendor relationship due to security concerns

Hours per week spent on vendor security reviews in Australia by organisation size



4.

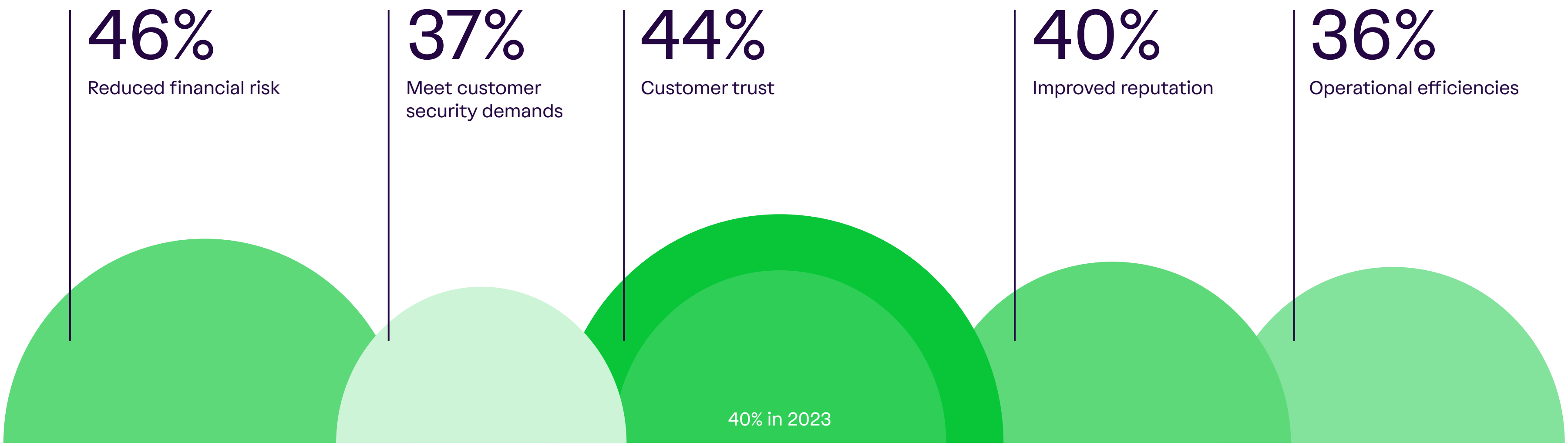
Good security is good business

Demonstrating trust continues to drive business value

As the security expectations of customers grow, Australian leaders continue to recognise the business value of investing in security — and demonstrating it. Close to two-thirds (62%) of Australian organisations say that customers, investors and suppliers increasingly require demonstration of compliance.

Nearly half (46%) of Australian organisations recognise that good security practices lead to reduced financial risks and 44% of Australian organisations believe good security practices drive customer trust for their business (up 4% from last year).

The value of good security practices



“Having industry-recognised certification enables us to build trust and make the deal that little bit easier to close.”

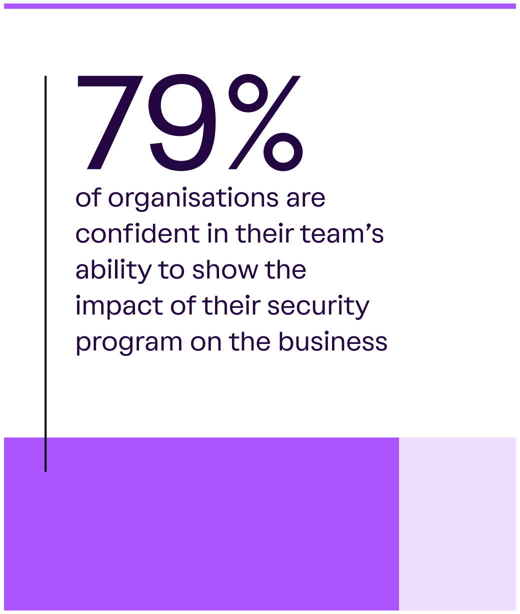
Prue Burns, Head of Legal & Data Security
Josef

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

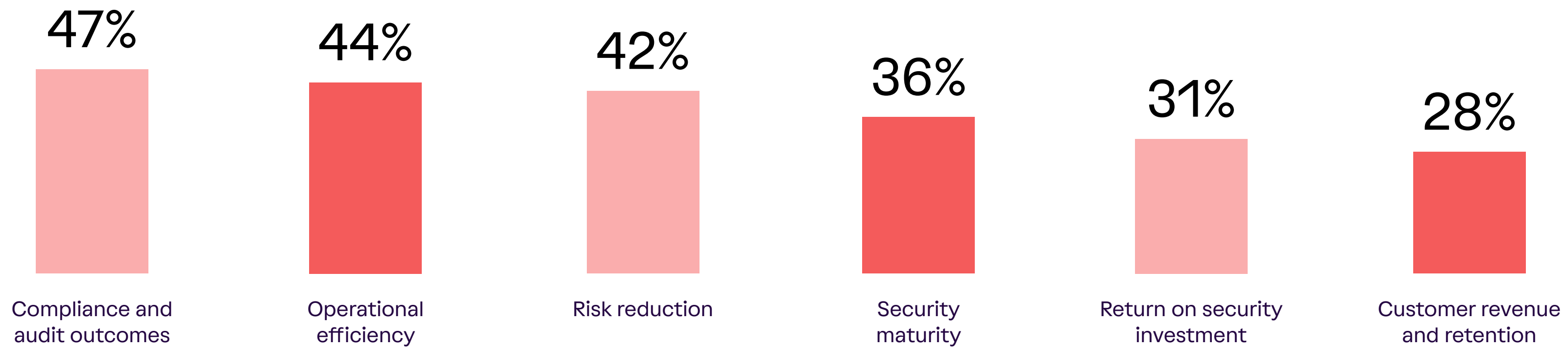
An overwhelming 79% of Australian organisations are confident in their team's ability to show the impact of their security program on the business. Further, more than 4 in 5(83%) Australian organisations quantify and measure the impact of their program in some capacity.

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

While teams are quantifying and measuring impact, only 31% 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 centralise visibility across their security program.



How Australian organisations are measuring a security program's impact



Conclusion: Go beyond the standard with trust management

For Australian organisations of all sizes, building and scaling trust is difficult. Greater reliance on third-party vendors and the growing usage of AI technologies mean that security leaders face an increasingly complex threat landscape while also navigating resource constraints.

But the tools available today only make this work more challenging. Teams are stuck with solutions that rely on screenshots and spreadsheets 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 a holistic trust management strategy, Australian organisations can not only reduce risk, but also build customer confidence and accelerate revenue growth.

Here are three ways that Australian organisations 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 centralised 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 organisation. It also reflects your network of vendors, partners and business ecosystem. Raise the bar for your security by building a bespoke standard of trust that centralises visibility and allows you to define what good security looks like for those that do business with you.

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 behaviours and attitudes of 2,500 business and IT leaders across Australia, the UK and U.S. Year-over-year comparisons for relevant questions were calculated using only the Australia, UK and U.S. datasets from The State of Trust Report 2023.

About Vanta

Vanta is the leading trust management platform that helps organisations 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