Vanta

France State of Trust Report

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

Table of Contents

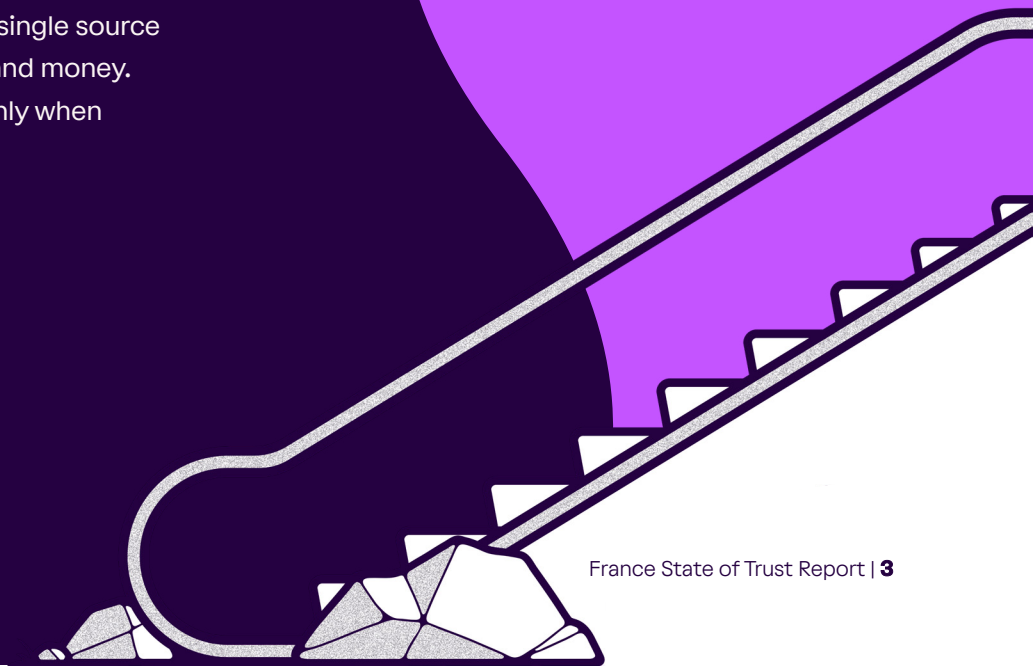
Foreword

French 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 fuelling an urgent need for companies to improve — and prove — their security posture.

Vanta's State of Trust Report (France edition) reveals that three quarters (76%) of French businesses say they need to improve security and compliance measures, with nearly one in four (22%) rating their organisation'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 regulatory landscape and growing compliance time-suck it entails as the EU and other regions continue to evolve their security governance frameworks. In an environment where customers increasingly want more proof of a company's security practices, organisations 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, centralising security programme 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.



Key Findings - France

76%

Three quarters

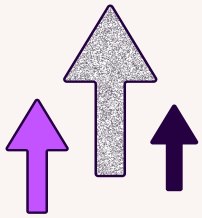
of business and IT leaders say their business requires improved security and compliance measures - the highest of all countries surveyed.

Only 9%

of IT budgets are dedicated to security.

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

2.5 hours per week



74%

Nearly 3 in 4 say a better security and compliance strategy would positively impact their business through greater efficiency.

76%

More than three quarters

of businesses say that customers, investors and suppliers are increasingly looking for proof of security and compliance.

44%

Respondents say the biggest transformation potential of AI will be streamlining vendor risk reviews and onboarding.

73%

Almost three-quarters of businesses are already or planning to use AI/ML to detect high risk actions.

Respondents spend on average 7.3 hours each week on security compliance. That's 350 hours — over working nine weeks — per year.

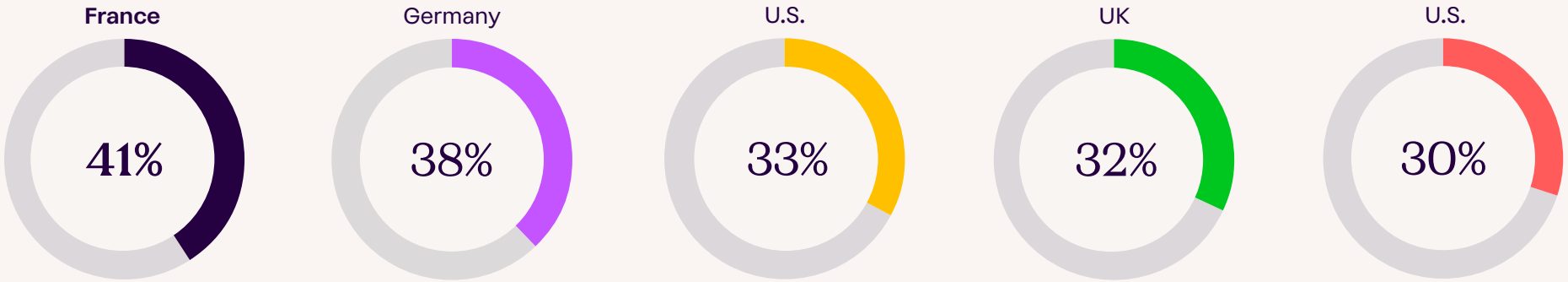
7.3 hours per week

KEY FINDINGS

France vs other countries

French leaders are most likely to say that phishing and social engineering against staff is their biggest security concern, at **41%.**

Other countries: U.S., 30%; UK, 32%; Australia, 33%; and Germany, 38%.



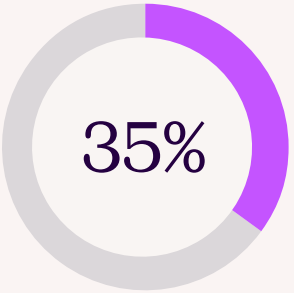
The most common way of proving security to customers in **France** is by providing an internal audit report **(43%).**

The U.S. and Australia also came in at 43% while the UK came in at the low end of the scale at 37%.

Fewer than half **(46%)** of **French** leaders state they have a strong visibility into risk compared to the UK and Australia at 42%.

The U.S., by contrast, was at 52%.

French leaders are the most likely to say that lack of staffing **(35%)** is a barrier to maintaining a robust security programme.



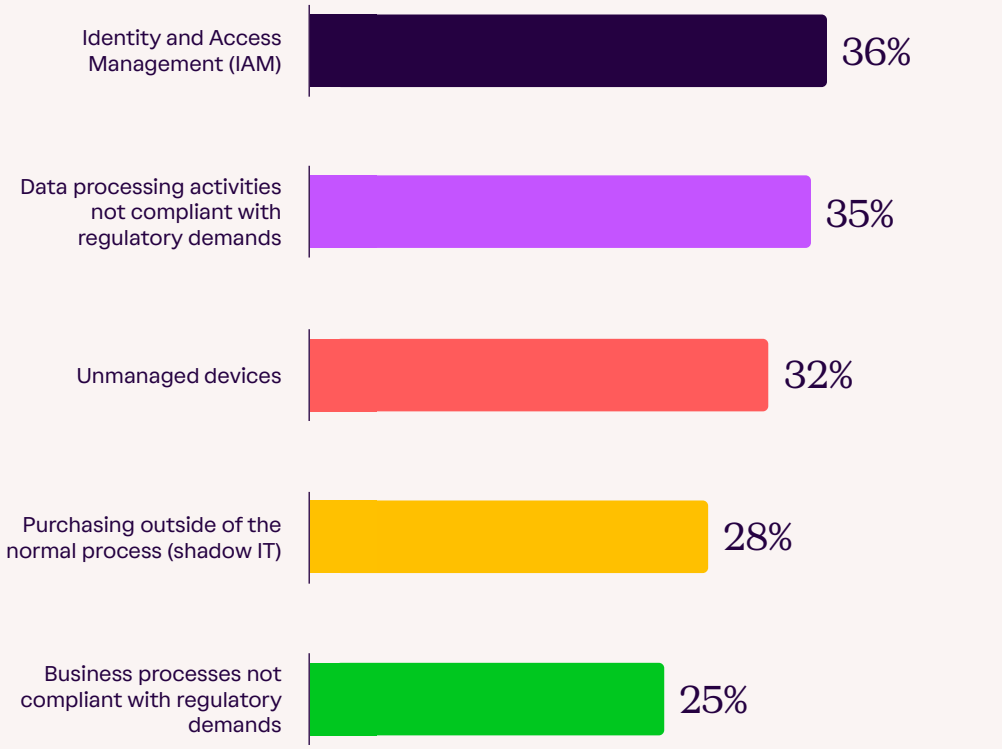
The security improvement imperative

The State of Trust survey of 2,500 global IT and business decision-makers (with 500 respondents from France) reveals an urgent need for businesses to improve security.

Over three quarters (76%) of French respondents believe their business needs to improve both security and compliance measures - the highest of all markets.

According to a recent report from the French National Cyber Security Agency (ANSSI)[1], the main victims of ransomware in France "remain micro-businesses, SMEs and intermediate-sized enterprises", accounting for 40% of reported attacks. Yet, for French companies of all sizes, limited risk visibility and blind spots accelerate this need to improve security and compliance. Fewer than half (46%) organisations rate their risk visibility as strong. Meanwhile, identity and access management (36%) and data processing activities not compliant with regulatory demands (35%) are the two biggest blind spots for organisations.

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



1 - https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-002.pdf

Security as a selling point

Over three quarters (76%) 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 43% provide internal audit reports (compared to 41% globally), 36% third-party audits (slightly below the global average of 37%), and 36% complete security questionnaires (matching the global average), one in eight (aligned with the global average at 12%) admit they don't or can't provide evidence when asked. This means French companies are falling at the very first hurdle, costing potential revenue and growth opportunities.

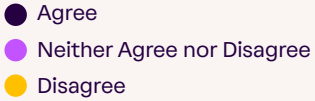
According to respondents, the biggest barriers to proving and demonstrating security externally are a lack of staffing (35%) and too many tools to manage security (29%).

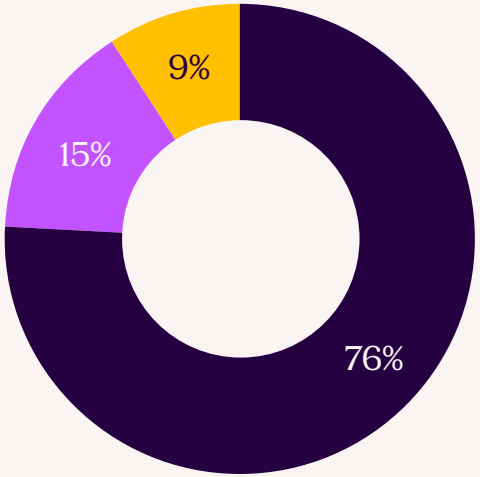
This comes at a time when 45% of French organisations surveyed say they have already, or plan to reduce IT staff. Almost a third of leaders (31%) say that their overall IT budgets have shrunk as they continue navigating the economic downturn, while 60% have either already downsized IT security budgets or are planning to.

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

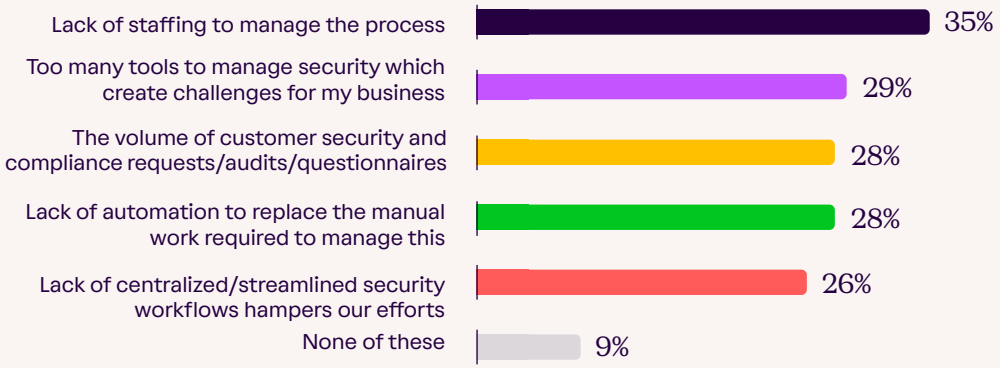
To what extent do you agree or disagree with the following statement regarding your security and compliance strategy?

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





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



Compliance deprioritized

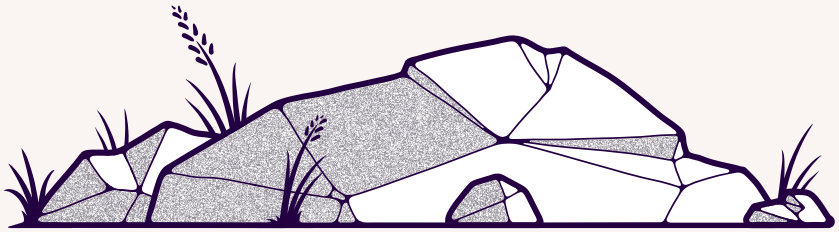
Given these trends, it's not surprising that respondents admit they're not prioritising compliance due to the time and financial investment. But failure to comply ultimately costs these companies potential revenue and growth opportunities, particularly in expanding to new markets.

Time is being plunged into businesses' efforts to meet and maintain the demands of compliance. Respondents spend an average of 7.3 hours per week (9 working weeks per year) on compliance.

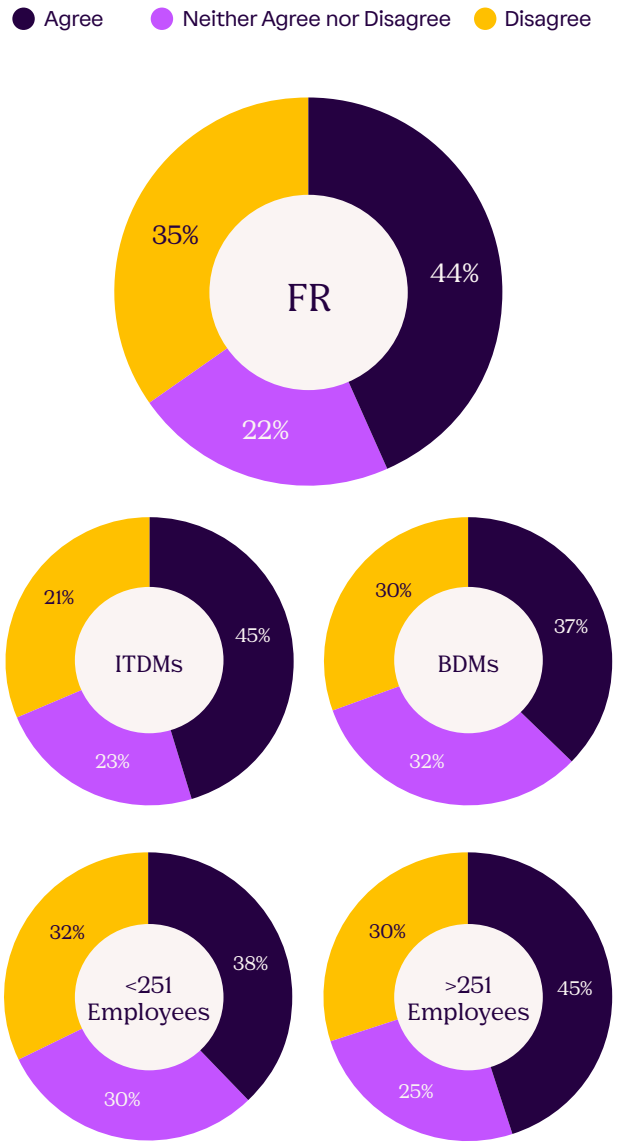
Exacerbating this time-suck, more than half (64%) of respondents say that remaining compliant with different international regulations like HIPAA and GDPR is becoming increasingly difficult.

Nearly half (44%) of businesses have deprioritised compliance due to the time it takes, with 44% admitting that it's due to the required investment.

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



"My business... has deprioritized compliance due to the investment it requires."



Keeping up with French regulations

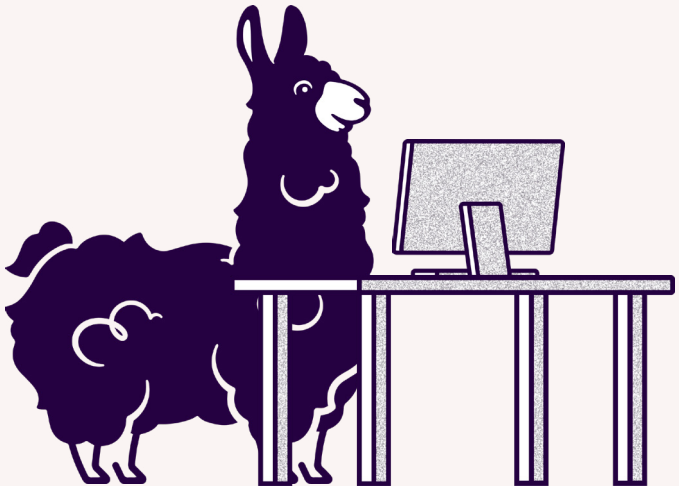
French specific regulation includes the EU's General Data Protection Regulation (GDPR), which states that personal data must be processed securely using appropriate technical and organisational measures. The EU's Networks and Information Systems (NIS2) Directive also passed its revisions in November 2022 considerably expanding the range of affected organisations in France.

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.

French businesses recognise the opportunity. 73% of French respondents already or plan to use AI/ML to detect high risk actions. However, over half (52%) are concerned that secure data management is becoming more challenging with AI adoption. And 45% say that using Generative AI could erode customer trust.

As a result, 57% of businesses say regulating AI would make them more comfortable investing in it.



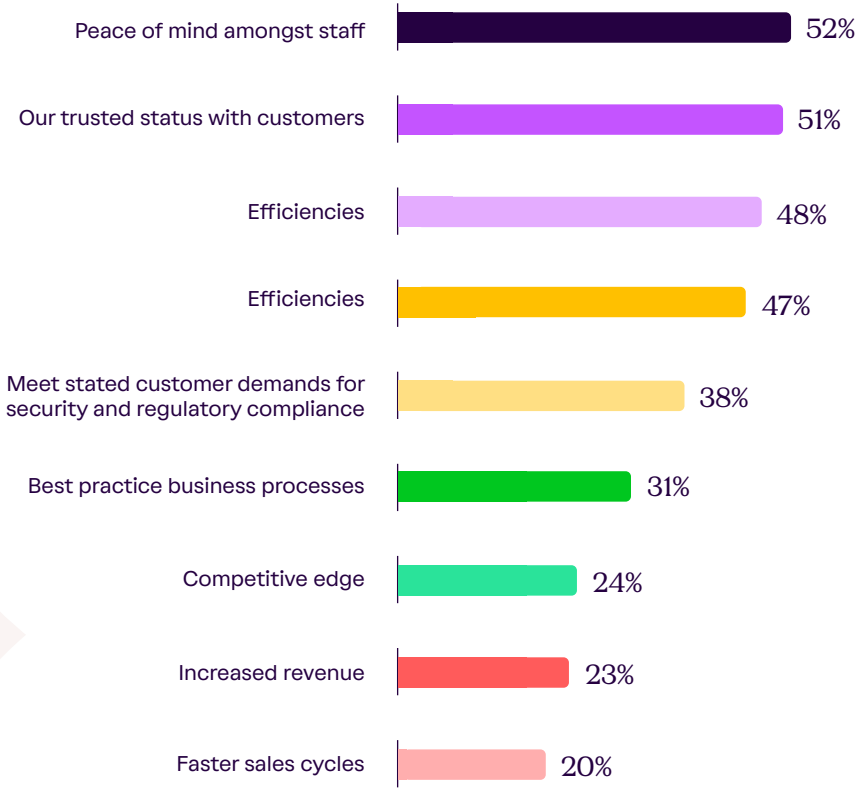
PART TWO

The trust managment tipping point

According to CERT-FR, the French national and governmental Computer Emergency Response Team, which is part of the National Cybersecurity Agency (ANSSI), “many of the incidents observed and reported to ANSSI in 2022[2] were prompted by the exploitation of vulnerabilities with available patches by vendors and were the subject of advisories or alerts.”

Given current trends, the business case for better security is plain to see. Ultimately, it improves efficiency and boosts the bottom line. Three in four (75%) of French leaders say that a better security and compliance strategy positively impacts their businesses thanks to stronger customer trust, while three in four (74%) agree that a better security and compliance strategy would make them more efficient. For 47%, one of the biggest value-drivers of good security practices is improved reputation.

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



2 - https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-002.pdf

PART TWO

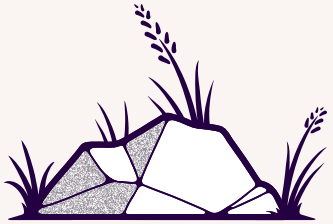
Streamlining security and compliance through automation

Improving and proving security doesn't need to be a heavy lift. In fact, 66% of respondents believe that time and money could be saved by automating compliance with different regulations and frameworks.

Automation brings trust and transparency to life, and companies are taking notice. 77% of businesses have increased or plan to increase their use of automation.

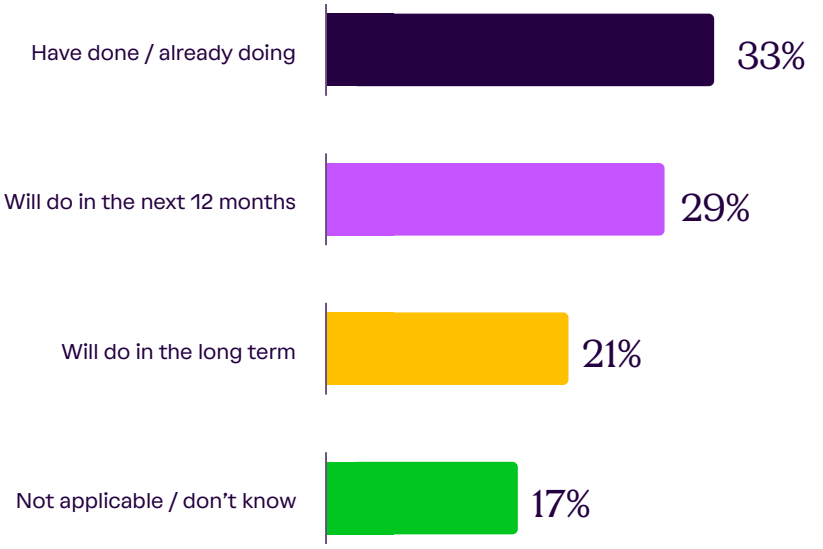
This is true for compliance as well as overall security management. On average, respondents believe they could save at least two hours per week — over 2.5 working weeks a year — if security and compliance tasks were automated.

Two thirds (67%) agree that their business is more likely to consider automating security compliance when scaling to different markets. And one crucial way to do that is through use of a trust management platform.



Thinking about your security and compliance strategy, what steps or measures will your business take in the near future to de-risk?

"Work with vendors to automate compliance."



PART TWO

Accelerating security workflows and transforming trust with AI

While AI offers both new opportunities and new risks, when done right, it can dramatically accelerate security workflows, enabling teams to focus on strengthening their security posture and building customer trust.

Respondents in France think AI can be transformative to streamlining vendor risk reviews and onboarding (44%), improving the accuracy of security questionnaires (43%), reducing the need for large teams (37%), and eliminating manual work (33%).

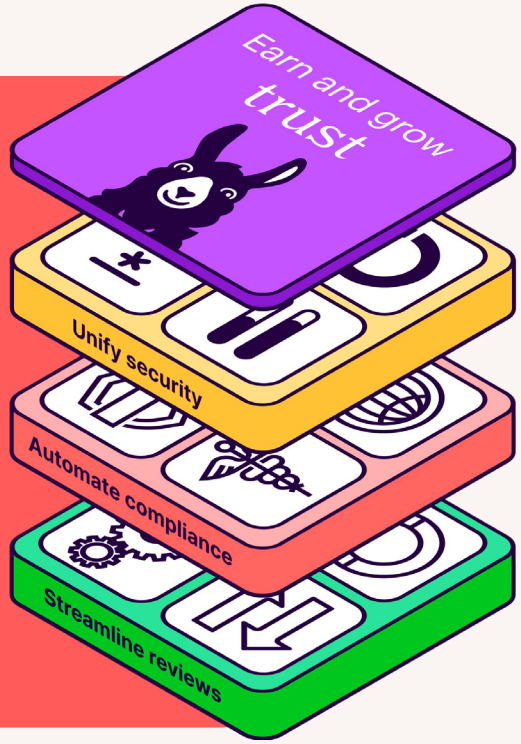
Whether that's saving time, budget or staffing resources, AI can help you do more with less: time-consuming tasks can be handed off to AI. But in a climate of growing cyber-threats, and AI tools presenting a new risk surface, it is essential to prioritise transparency and trust when deploying AI.

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 instil confidence in both prospects and customers.

A trust management platform provides a single source of truth for centralising 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 assessmentsto 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

Conclusion

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

Organisations 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, centralising security processes, automating compliance, and accelerating security reviews can turn trust into a truly 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

- **Centralise:** With over half of French leaders facing low levels of risk visibility, establish a central source of truth to unify your security and compliance programmes.
- **Invest:** France is the second most likely country surveyed to say that lack of IT budget is a barrier to maintaining a robust security programme. Security underpins growth - invest to unlock opportunities.
- **Transparency:** Over a third of French firms demonstrate security through questionnaires. They can streamline workflows by showcasing security measures through audits, continuous monitoring, and a public Trust Centre.
- **Automate:** French leaders are most likely to say that their businesses require improved security and compliance measures. Automation is the quickest path to ensuring security and compliance standards are met quickly and without manual effort.

Research 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 behaviours and attitudes of 2,500 business and IT leaders across Australia, France, Germany, the UK, and U.S. The local data in this report comes from 500 French organisations.

About Vanta

Vanta is the leading trust management platform that helps simplify and centralise security for organisations 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. Founded in 2018, Vanta has customers in 58 countries with offices in Dublin, New York, San Francisco and Sydney.

For more information, visit www.vanta.com