

The 2018 Global Password Security Report

Understanding password hygiene in businesses worldwide –
and how your company stacks up

LastPass... | enterprise
by LogMeIn

What's Inside

► INTRODUCTION

Businesses need a password security benchmark.....	3
Defining benchmark scores.....	4
Methodology.....	5
Announcing the LastPass Password Security Benchmark.....	6

► EXPLORE THE DATA

Password security is harder for big companies.....	7
Which industry is getting password security right?.....	9
Which countries have security locked down?.....	11
A closer look at password strength.....	13
Password security improves rapidly in the first year.....	17
The state of multifactor authentication.....	18
The state of password sharing.....	21
Websites that are gaining and losing popularity in the workplace...	22
Employees are mixing work and personal.....	23

► CONCLUSION

Use the benchmark to chart a better course.....	24
---	----

► TAKE ACTION

Becoming a top performer.....	25
-------------------------------	----

Businesses need a password security benchmark

Passwords have long been a challenge to cybersecurity in the workplace, and attacks continue to grow in number and complexity every year. Despite these threats, businesses have struggled to quantify their own level of password risk. They lack proof of their policies' effectiveness. They're missing visibility into their employees' behaviors. And they can't verify how they compare to others of similar size, industry or location.

Until now. In this report, we're not only revealing true password behaviors in the workplace but creating a benchmark that businesses can use to measure progress when investing in password security. By showing averages for companies big and small, we aim to help IT professionals understand where they rank and how to improve their company's password security.

Defining benchmark scores

There are two scores analyzed in this report:

The LastPass Password Strength Score and the LastPass Security Score. Both are calculated as a part of the LastPass Security Challenge, a built-in password-auditing tool available for all LastPass users. For business accounts, this data is also reported to LastPass admins for insight into password hygiene at the employee level.

The LastPass Password Strength Score evaluates the combined, averaged password strength of all passwords stored in the user’s vault. Factors include the length, complexity and reuse of passwords.

The LastPass Security Score is calculated using the following criteria:

- The number of duplicate passwords
- The number of sites marked “vulnerable” (due to publicly disclosed data breaches)
- The number of weak passwords
- The average strength of each password
- The strength of shared passwords
- The multifactor authentication score

This total score tells businesses not only how strong individual passwords are but how well those passwords are protected.

For both scores, LastPass defines the values as the following:



0 to 39: Poor



40 to 64: Fair



65 to 89: Good



90 to 100: Exceptional

Methodology

We anonymized and aggregated data from more than 43,000 organizations that use LastPass as their business password manager.

Much like our 2017 report, The LastPass Password Expos , this report represents organizations of all types and sizes across nearly every industry. Compared to last year, the data set has grown significantly and allows us to draw a more precise picture of password management. Though the data only reflects LastPass users, we've broadened our conclusions for the IT community at large.

► INTRODUCTION

Announcing the LastPass Password Security Benchmark

Our finding: In analyzing 43,000 businesses using LastPass, across companies of all sizes and industries, the benchmark average Security Score is 52.

What does this score tell us? Even as more businesses invest in password management, most are performing middle of the road for password security. While a score of 52 is fair, it shows a need for more effective policies and training so organizations can surpass the benchmark.

An average global Security Score of 52 also means that most businesses still have work to do in overcoming weak, reused, old and potentially compromised credentials. Many passwords could be stronger, and every one is a potential entryway to the business that should be protected and managed.

Read on to find out more about how your company's own security and password behaviors compare with organizations around the world.



is the **Average Security Score** across 43,000 businesses using LastPass.

► EXPLORE THE DATA

Password security is harder for big companies

The bigger the company, the lower its Security Score on average. Organizations with 25 or fewer employees have the highest average Security Score of 50, and the average drops as the company size increases – up to a point. Once a company hits 500 employees, the average Security Score holds steady at 46.

It seems that organizations of over 500 people, whether 1,000 or 10,000, face similar challenges in improving password hygiene. More employees bring more passwords and unsanctioned apps, as well as extra opportunities for dangerous password behaviors. In larger organizations, it’s simply more challenging for IT to hold all employees to password security standards.



Organizations over 500 people face challenges in improving password hygiene.



► EXPLORE THE DATA

Size is no excuse.

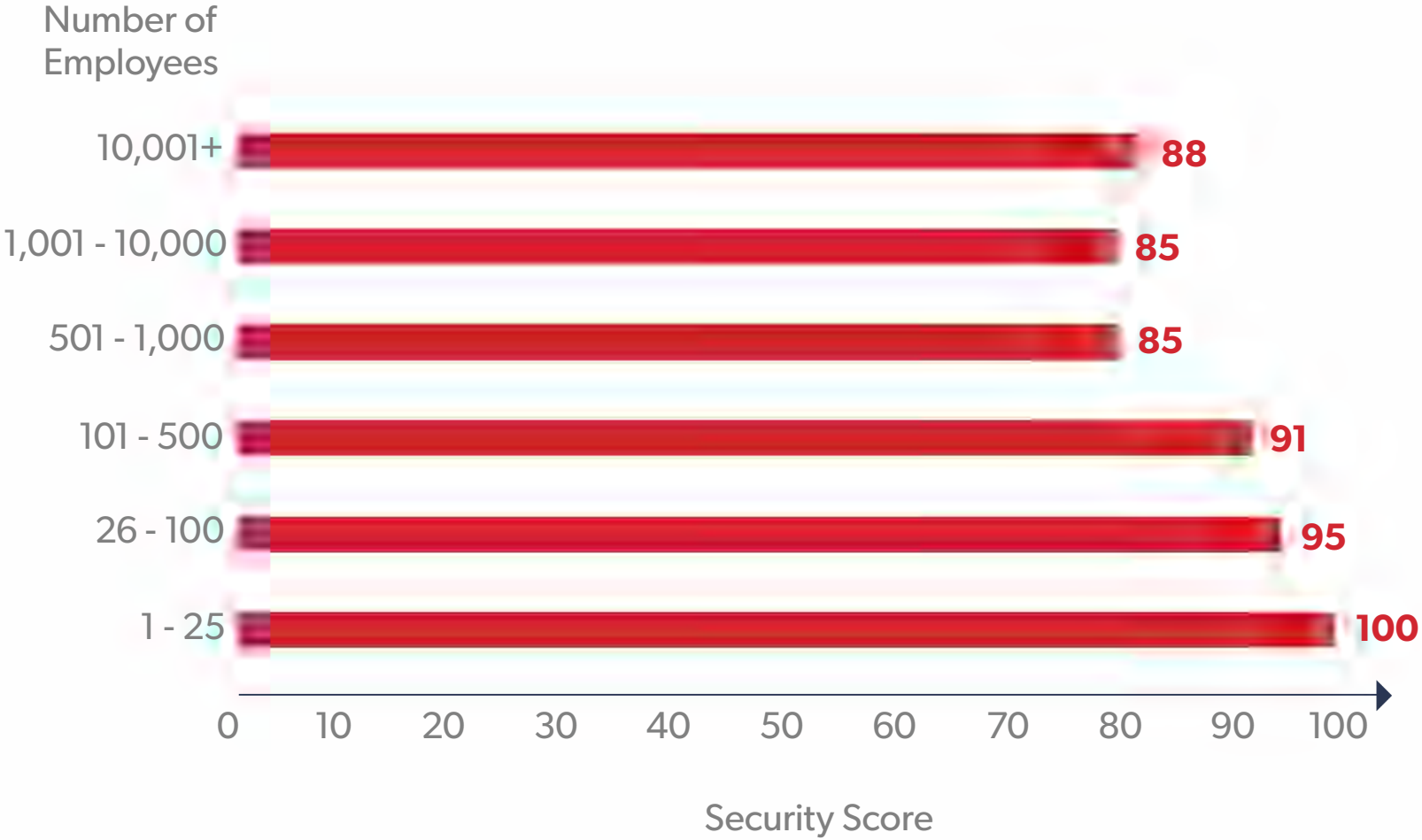
However, large businesses shouldn't let those challenges become excuses. When looking at top performers, it's encouraging to see that even large companies can achieve exceptional scores of 85 and 88. Size is merely a factor IT professionals need to account for.

Unsurprisingly, smaller companies are also more likely to achieve exceptional Security Scores. For companies with 25 employees or fewer, the highest is a perfect 100. For companies with 25 to 100 employees, the highest Security Score is also an enviable 95. That means these companies have near-perfect passwords and multifactor authentication for all employees.



88 is an exceptional security score for a large company.

**Top Security Score
by Company Size**



► EXPLORE THE DATA

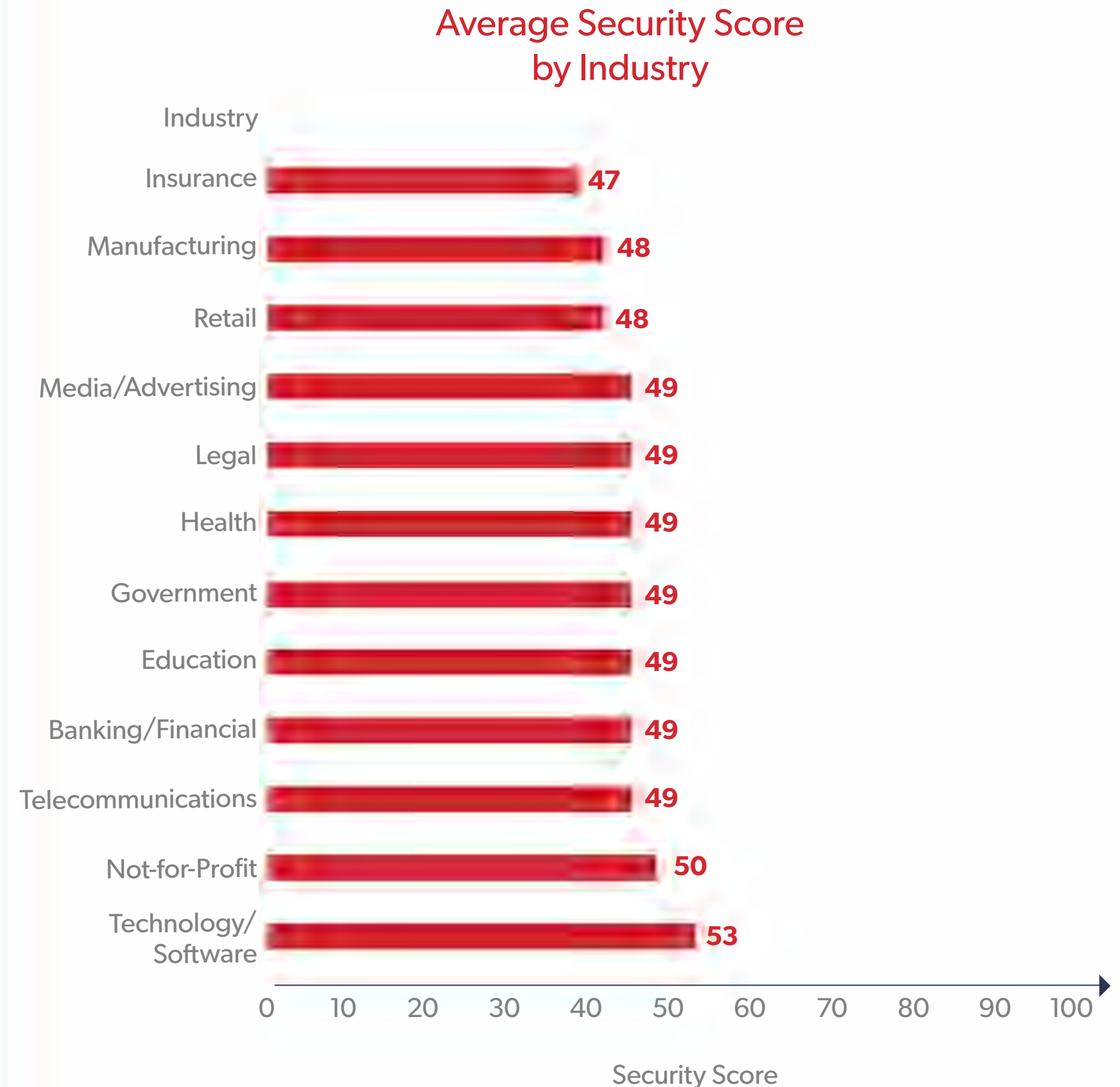
Which industry is getting password security right?

We wanted to see how various industries manage password security. The highest average Security Scores are in Technology (53), with Not-for-Profits (50) a close follower. Retail (48) and Insurance (47) trail the pack, while most others fall comfortably in between the leaders and laggards.

Since many Technology companies need to comply with privacy and data laws, it's not surprising they lead the pack. What is surprising, though, is that heavily-regulated industries like Banking, Health, Insurance and Government are not achieving comparable (or even superior) average Security Scores. And given that those industries – in particular Health – are more frequently targeted by attackers, we would expect to see higher commitments to password security.



53 Technology is the industry with the highest average security score.



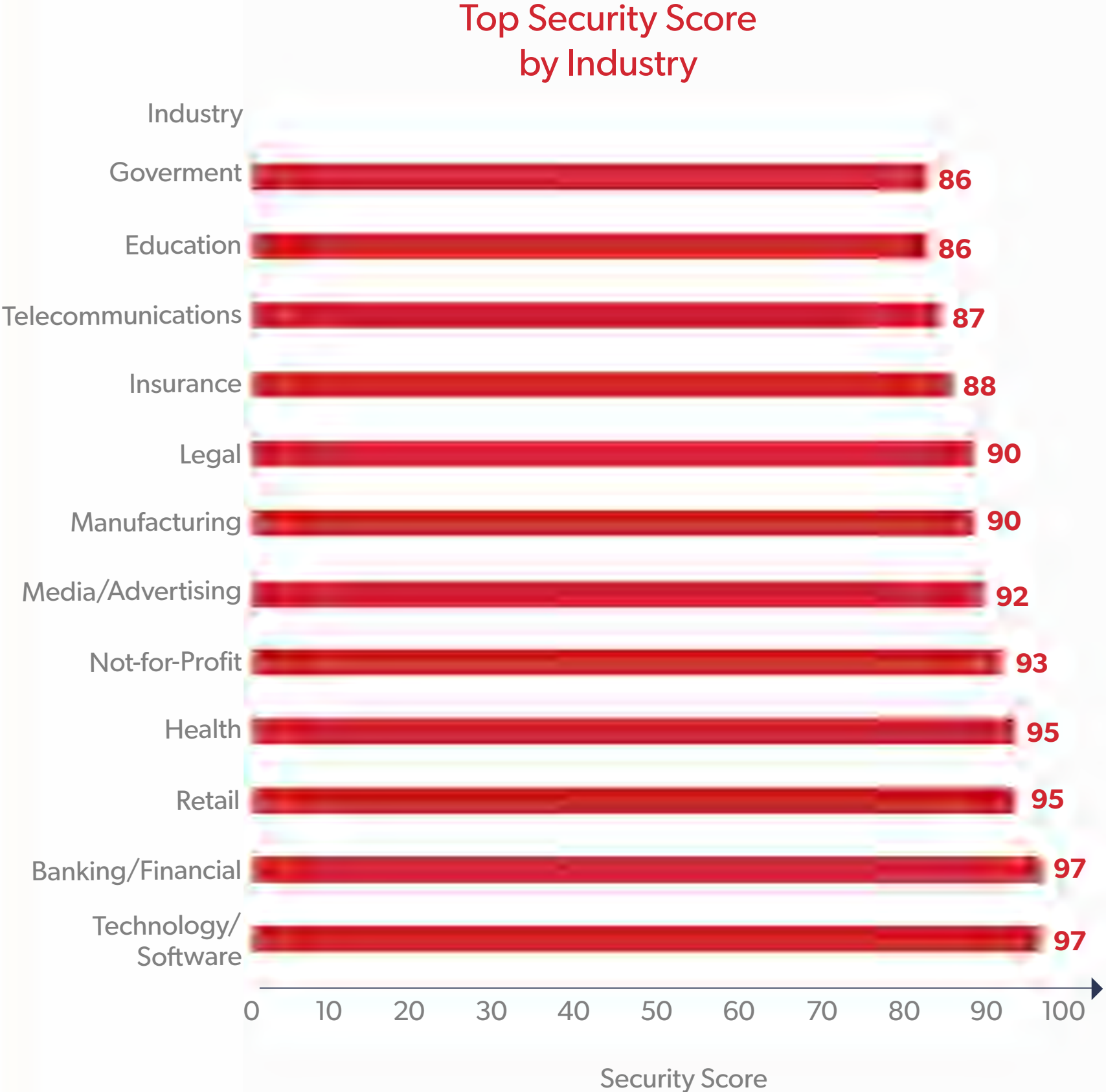
► EXPLORE THE DATA

Trends aren't the end.

However, industry trends need not be a predictor of overall password success. We see the highest Security Score, an exceptional 97, in Technology and Banking companies. Others in those two industries have some tough competition.

Interestingly, top performers in both Health and Retail achieve an excellent Security Score of 95, despite lower Security Scores for their industries on average. The leaders in Health and Retail outpace Government and Education by about 10 points, indicating that even the best in the latter two sectors have work to do if they want to take the lead.

It's promising to see that businesses across all industries are achieving exceptional scores.



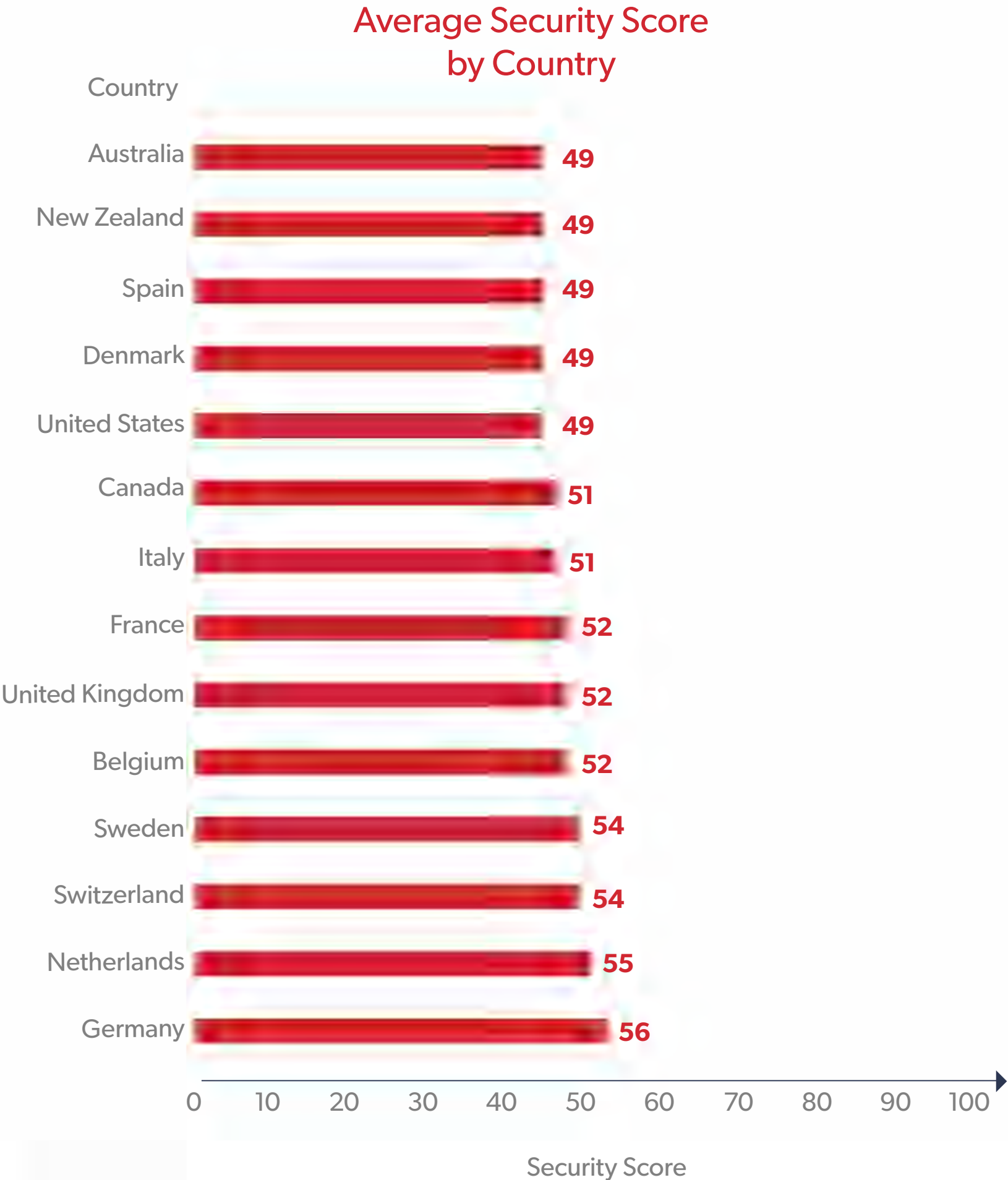
► EXPLORE THE DATA

Which countries have security locked down?

When it comes to average Security Scores for countries, it's no surprise that Germany ranks highest at 56, followed closely by the Netherlands at 55, which puts them above the global average of 52. With a reputation for security and the adoption of standards like the General Data Protection Regulation (GDPR), it's understandable why they lead the pack.



52 is the average global security score.



► EXPLORE THE DATA

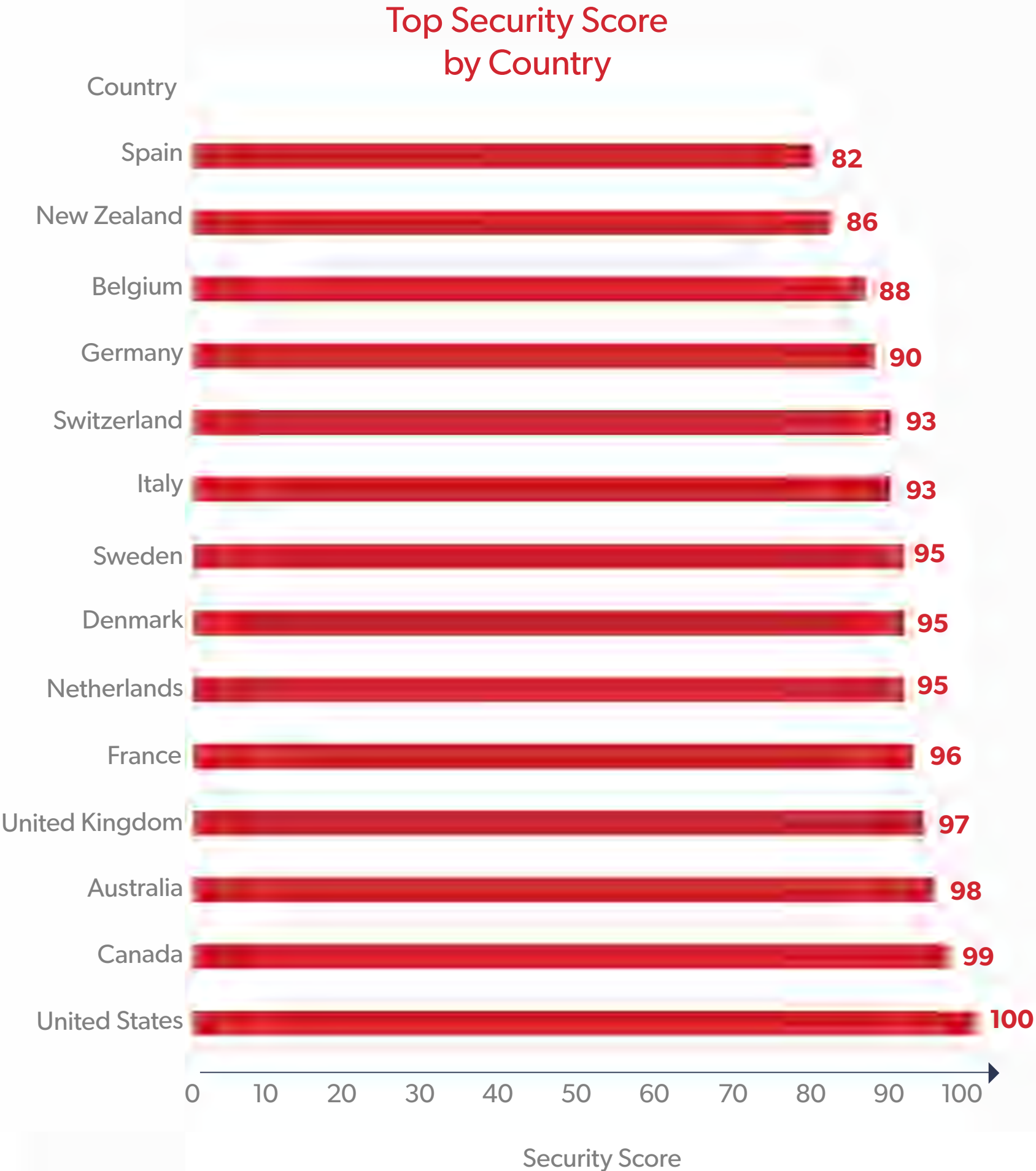
Even perfect needs practice.

But when it comes to top performers, the United States outpaces other countries with a perfect Security Score of 100, followed very closely by Canada and Australia at 99 and 98, respectively. Businesses in those countries have managed to eliminate poor passwords and standardize on multifactor authentication for added security.

What is surprising, however, is that on average the United States falls ten points behind Germany. Even though the United States has strong top performers, overall the country has work to do.



100 is a perfect security score.

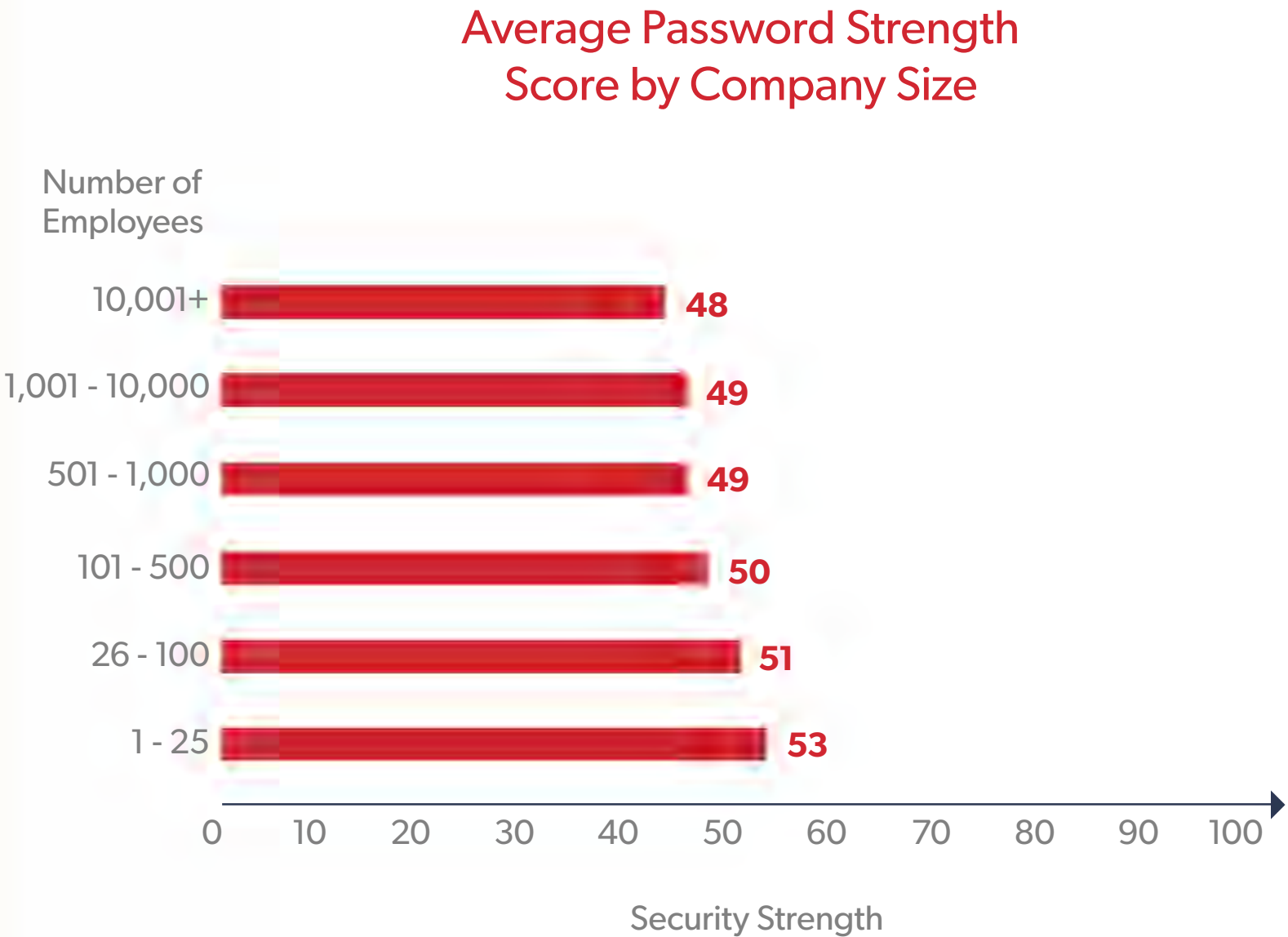


► EXPLORE THE DATA

A closer look at password strength

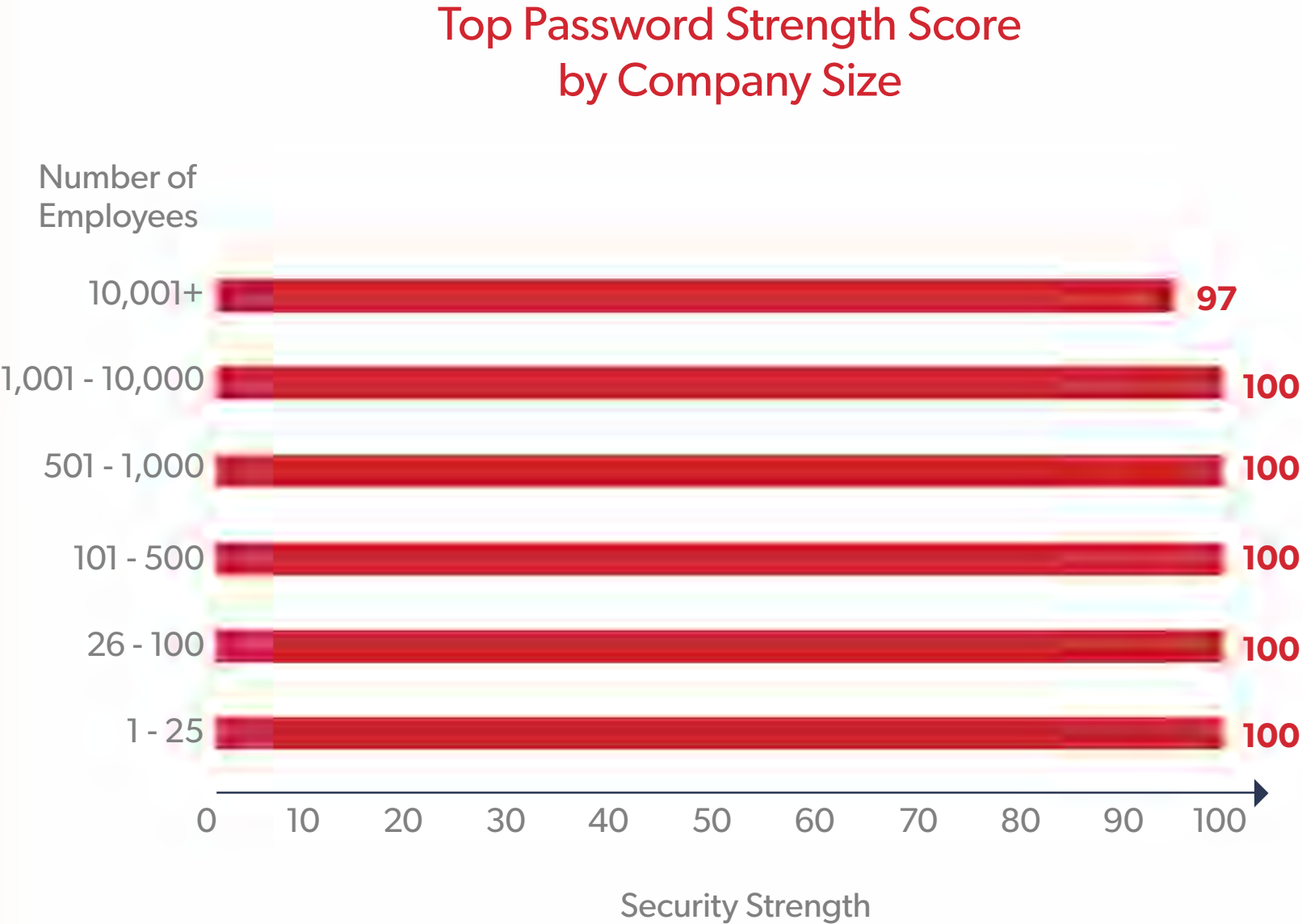
Overall, Password Strength Scores follow the trends for Security Scores: As companies get bigger, on average their Password Strength Score goes down.

For businesses with fewer than 25 employees, the average total Password Strength Score is 53. At more than 10,000 employees, the average score drops to 48. Again, we can infer that the larger the organization, the more difficult it is to address challenges like budgets, competing priorities, bureaucratic red tape or scaling training initiatives. Smaller companies, despite fewer resources, seem to achieve better results.



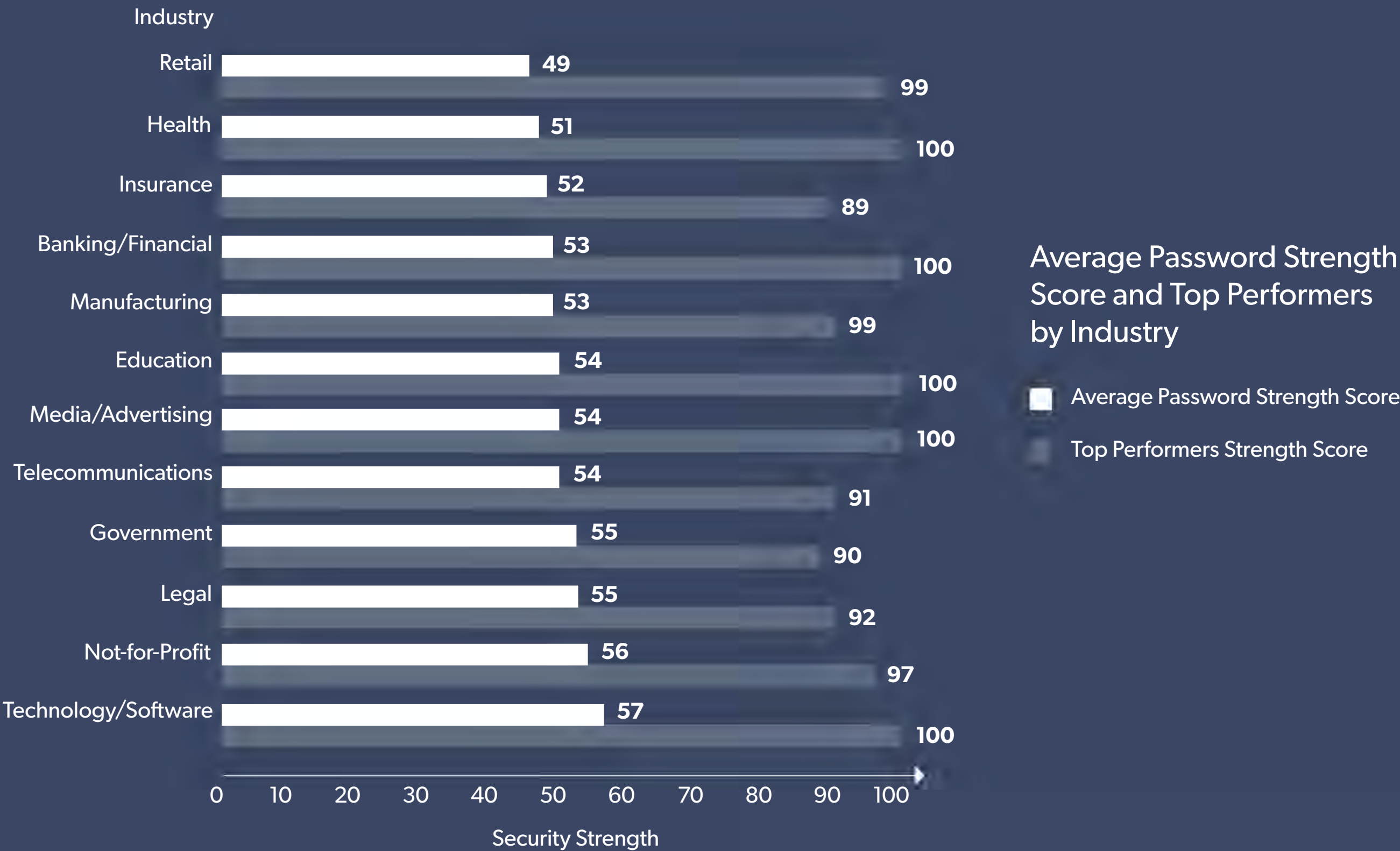
► EXPLORE THE DATA

Surprisingly, companies of nearly every size achieved a perfect Password Strength Score of 100. While the top performers in large organizations with 10,000 employees rank lower, it's not by much – just three points. Though an increase in size may present challenges, it doesn't prevent high scores. Companies of all sizes are forging ahead and surpassing the averages to achieve stronger password security.



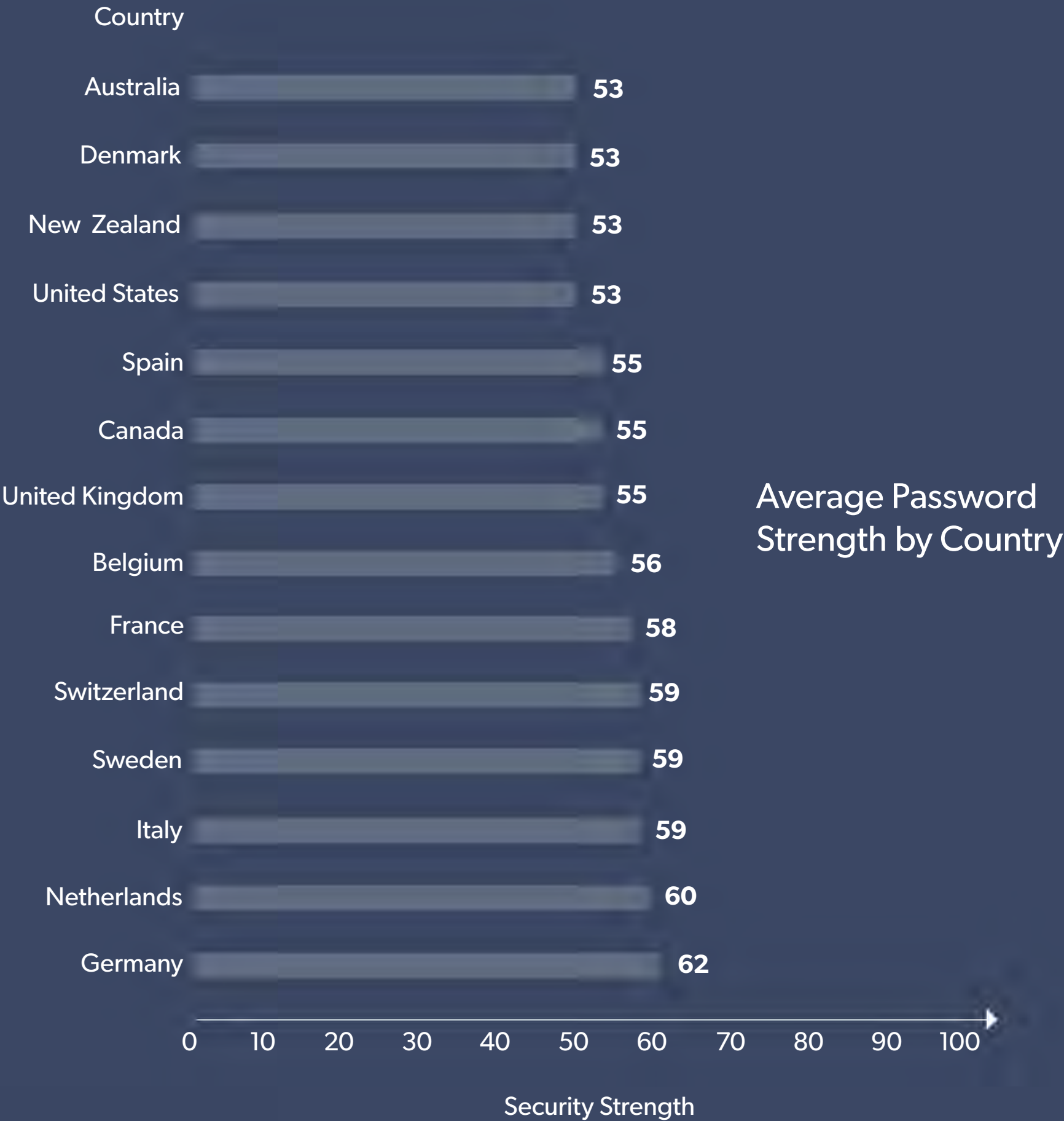
► EXPLORE THE DATA

For average Password Strength scores, we again see that Technology (57) takes the lead, followed closely by Not-for-Profit (56), Legal (55) and Government (55). Though there isn't great variability across industries it's clear that some industries are more likely to achieve greater password strength.



► EXPLORE THE DATA

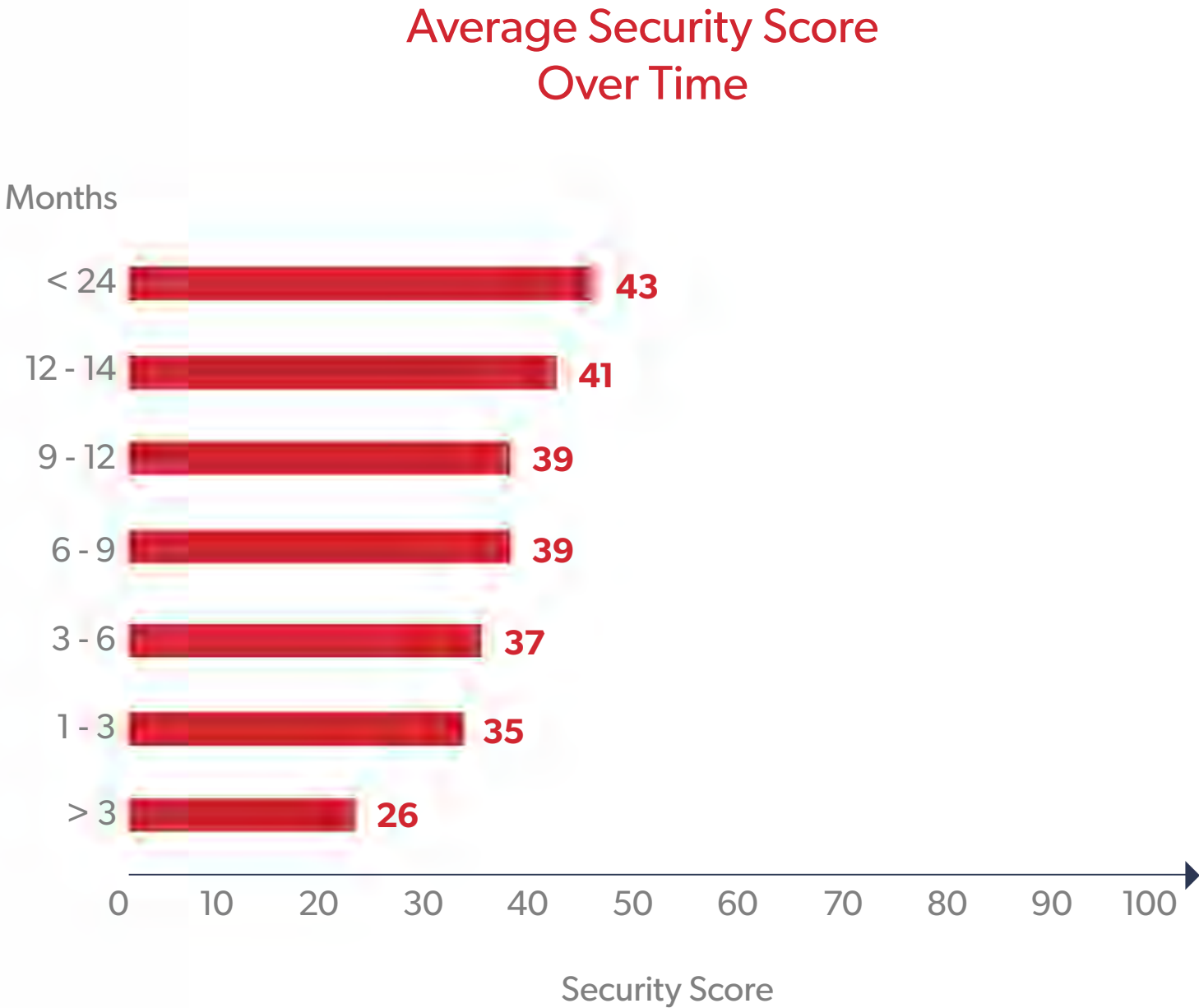
We also see interesting trends for geographic locations. German companies are easily leading the pack with an average Password Strength Score of 62. Close followers include the Netherlands (60), Switzerland (59) Sweden (59) and France (58). Denmark, the United States, New Zealand and Australia all trail at 53. Again, European countries live up to their reputation of being more security-conscious, while businesses in North America and Australasia lag behind.



► EXPLORE THE DATA

Password security improves rapidly in the first year

Investing in password management helps companies rapidly improve their password security. Despite starting with an average score of 26, companies rolling out a password manager gain, on average, nearly 15 Security Score points in the first year. And scores continue to improve in the years that follow, indicating that even as employees join and leave the company, IT teams are able to make significant progress in password security.



► EXPLORE THE DATA

The state of multifactor authentication

Multifactor authentication remains an industry best practice for preventing unauthorized account access. Our analysis this year found that, overall, 45% of businesses are using multifactor authentication. This is a significant increase from last year's 24.5%. Encouragingly, more businesses are augmenting account security with methods beyond the password. We applaud IT professionals for the strides they've made.

Small companies are strong users of multifactor authentication. Of companies that have turned on multifactor authentication, 41% have 25 or fewer employees. As the company grows larger, usage generally decreases, with a noticeable dip down to 3% for companies with more than 10,000 employees.

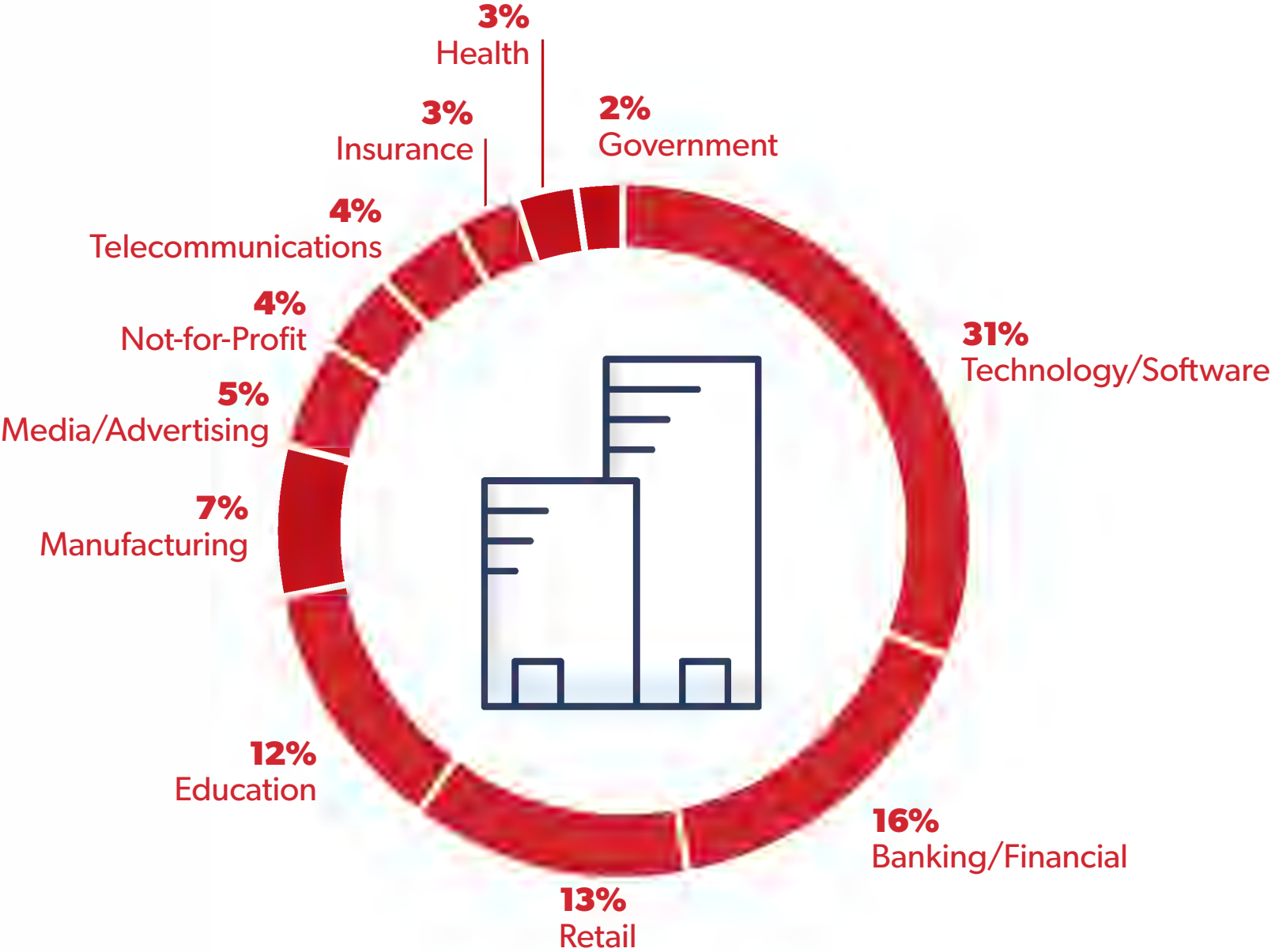
Breakdown by Company Size for Businesses Using Multifactor Authentication



► EXPLORE THE DATA

Maintaining the trend of being a security leader, Technology outperforms all others in multifactor authentication. Of companies that have turned it on, 31% are in Technology. Other industries with notable usage include Banking (16%), Retail (13%) and Education (12%). To our surprise, Health trails at 3% despite its heavy regulations.

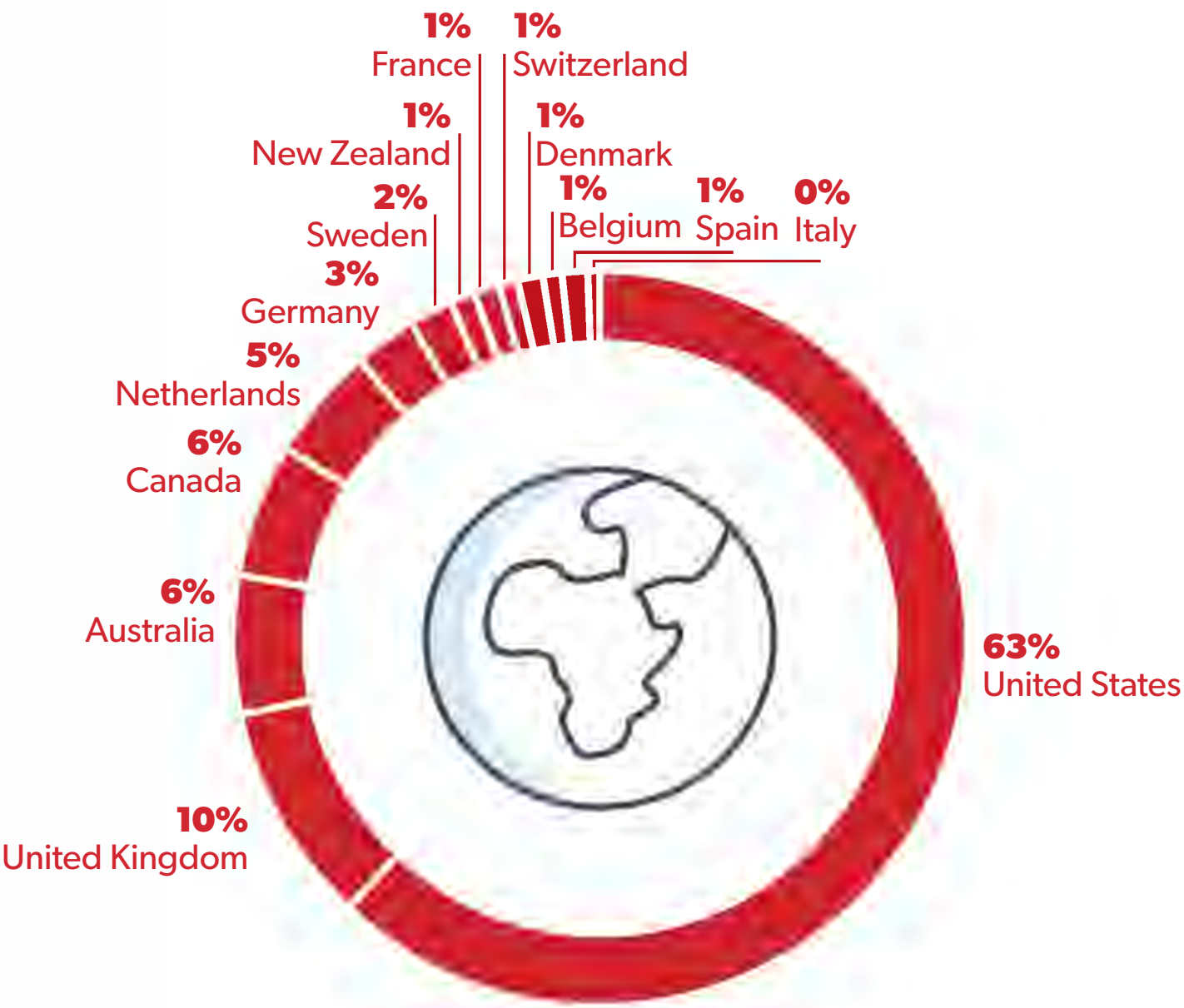
Breakdown by Industry for Companies Using Multifactor Authentication



► EXPLORE THE DATA

The United States shines when it comes to multifactor authentication. Of companies with multifactor authentication enabled, about 63% are in the U.S. Given it ranks lower for both the Security Score and Password Strength Score, we're surprised to see usage so high. On the other hand, Germany, which leads both scores on average, accounts for less than 3% of the companies that have multifactor authentication enabled. Despite the growing usage of multifactor authentication as a whole, some countries have not as readily adopted this security trend.

Breakdown by Country for Companies Using Multifactor Authentication

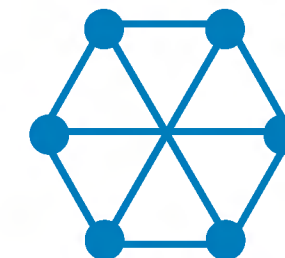


► EXPLORE THE DATA

The state of password sharing

We found that, on average, any given employee now shares about six passwords with coworkers. This is a slight increase from last year's Password Exposé, which found that, on average, an employee shares four passwords.

Password sharing remains frustrating for employees and IT admins alike. Employees resort to weak-but-memorable passwords and insecure sharing methods so they can simply get their work done. IT, however, knows these passwords are a potential backdoor into the business. As teams become more distributed and technology-dependent, the ability to protect, track and audit shared passwords is more important than ever. Employees don't need to stop sharing – they just need a secure way to do so.



6 passwords are shared by the average employee.

► EXPLORE THE DATA

Websites that are gaining and losing popularity in the workplace

When it comes to the websites employees are storing most in LastPass, we see a few trends emerge compared to last year. Newcomers to the top 30 websites include Microsoft’s O365 portal office, pharmaceutical tracking platform Tracelink, eSignature service DocuSign, single sign-on provider Okta, web conferencing tool Zoom and ecommerce platform Myshopify. In turn, we’ve seen Netflix, Yahoo, Box, Verizonwireless and Ebay all drop, at least temporarily, from the list.

2017

- Adobe.com
- ADP.com
- Amazon.com
- Americanexpress.com
- Apple.com
- Atlassian.com
- Atlassian.net
- Box.com
- Chase.com
- Dropbox.com
- Ebay.com
- Facebook.com
- GitHub.com
- Godaddy.com
- Google.com
- Instagram.com
- Intuit.com
- LinkedIn.com
- Live.com
- Mailchimp.com
- Microsoftonline.com
- Netflix.com
- PayPal.com
- Salesforce.com
- Slack.com
- Trello.com
- Twitter.com
- Verizonwireless.com
- Yahoo.com
- Zendesk.com



Losing popularity



Gaining popularity

2018

- Adobe.com
- ADP.com
- Amazon.com
- Americanexpress.com
- Apple.com
- Atlassian.com
- Chase.com
- DocuSign.com
- Dropbox.com
- Facebook.com
- GitHub.com
- Godaddy.com
- Google.com
- Instagram.com
- Intuit.com
- LinkedIn.com
- Live.com
- Mailchimp.com
- Microsoftonline.com
- Myshopify.com
- Office.com
- Okta.com
- PayPal.com
- Salesforce.com
- Slack.com
- Tracelink.com
- Trello.com
- Twitter.com
- Zendesk.com
- Zoom.us

► EXPLORE THE DATA

Employees are mixing work and personal

Though we would like to believe that any poor personal security habits don't carry over into the workplace, we know that's not reality. Most often, employees own the passwords for these services – even after they leave a company. It's hard to know whether these sites are being used for business or personal purposes, but the IT professional should take action either way.



43% of the top 30 domains employees use are also popular consumer apps.



50% of people do not create different passwords for personal and work accounts.

► CONCLUSION

Use the benchmark to chart a better course

It's critical that IT leaders change the way they think about passwords. The benchmark scores in this report provide businesses everywhere a way to measure their own password security, while the top performers give IT teams a goal to move towards.

Visibility is fundamental for this process. You can't measure your security unless you have a system that gives you these insights. That means for businesses that want to go beyond the averages, a password manager is a must.

Solving the password problem improves security, productivity, brand perception, employee satisfaction and even your customer experience. The organizations that can rapidly and effectively address their password challenges are well positioned to safely navigate their business into the future.



► TAKE ACTION

Becoming a top performer

The top performers highlighted in this report shared similar strategies for password security:



Deploy a business password manager.

The right solution can help you:

- Randomize every password
- Apply role-based permissions to passwords
- Achieve accountability for shared credentials
- Add protection with multifactor authentication
- Revoke credentials after employees leave



Create (and execute) an adoption plan.

Getting started is simple with the right steps:

- Communicate password policies and best practices
- Make the password manager part of security training
- Ensure all new hires are trained and onboarded
- Share the tool, how to use it and where to go for questions



Monitor progress with reporting tools.

A password solution like LastPass lets you identify:

- Weak and reused passwords
- Poor security and password strength scores
- Account inactivity

► Use this report to create your own benchmark and measure progress over time. Periodic readouts, targeted follow-ups to struggling employees and ongoing training will ensure success. By embracing a new approach to password management, any business can achieve the strong password security they know is important.

See how simple security can
be with a password manager.

lastpass.com/business

LastPass... | enterprise
by LogMeIn