DASHLANE

2024 GLOBAL PASSWORD HEALTH SCORE REPORT

Global password security health trends in 2024

What Dashlane's Password Health score tells us about the state of cybersecurity, authentication, and passwords worldwide in 2024.

INTRODUCTION

The Global Password Health Score Report

The evolution of credential security

In 2022, Dashlane published the first-ever deep-dive look at global password health. New for this year's report, we analyzed enterprise-specific password hygiene with data from over 23,000 businesses protected by Dashlane. We found that while enterprise users have stronger password health than consumers, there's a pervasive number of credentials not protected by single sign-on (SSO). We also examined which industries have the best and worst password health.

Since we published our first report, Dashlane users worldwide have seen their Password Health scores trend upward each year, underscoring that knowledge equals power when it comes to security. Progress in security often happens gradually, and with passkeys and other passwordless technology still in the early stages of adoption, compromised and unsecure credentials remain a risk that organizations will have to continue to manage for years to come.

SECTION 1

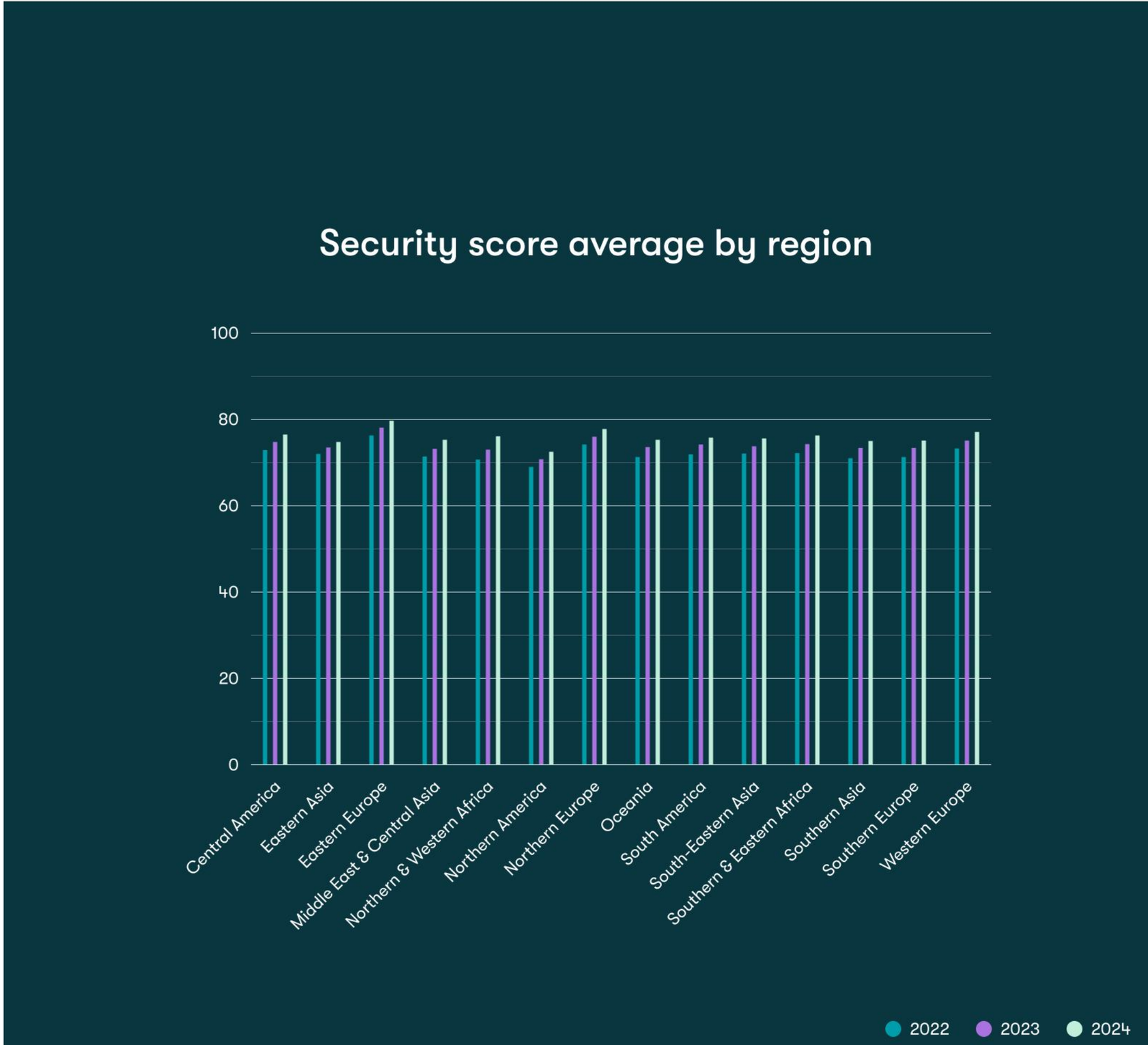
How password health changed by region from 2022–2024

Password health for Dashlane users across the world has improved over the last year, yet unsafe credential handling persists. These are our top findings by region and across industries.

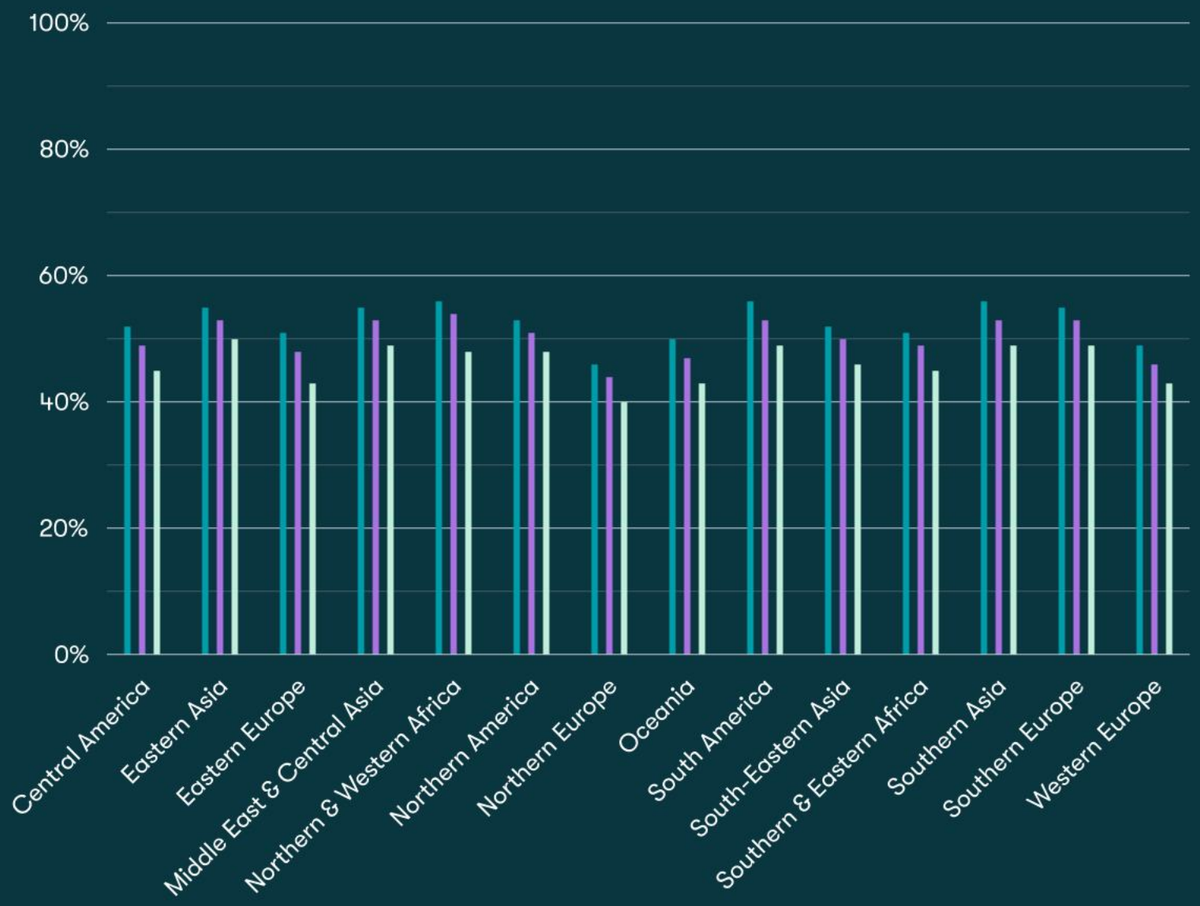
Password health improves globally

Looking across regions, the average Password Health Score in 2024 was between 72.6 (Northern America) and 79.8 (Eastern Europe). While each region fell within the “Needs Improvement” range (a score between 60-90), all regions improved their scores between 2-4% in the past year. This is due to the continued decrease in reused and compromised passwords globally. These steady improvements can significantly reduce risk for users and their employers, especially from opportunistic, wide-net phishing attacks that take advantage of weak, reused, or compromised credentials.

“The cyber health of an organization requires employees to be aware and careful,” said Robin Koetje, Vice President of Information Technology of boutique hotel brand Staypineapple. “The Password Health score makes it easy for our employees to find and fix weak and reused passwords.”



Share of reused passwords by region



Share of compromised passwords by region

2022 2023 2024

As the data shows, the share of compromised passwords decreased globally, yet the share of reused passwords remains between 40-50% worldwide, representing poor security hygiene. The share of weak passwords has trended upwards across all regions.

Lowest security score:
Northern America

Northern America had the lowest security score at 72.6, due to having the highest percentage of compromised passwords (15%) and among the highest percentage in reused passwords (48%). Northern America is a corporate hub and is more likely to have high-value returns, so is more often targeted by attackers.

Strongest passwords:
Eastern Europe

Eastern Europe had the strongest average Password Health score at 79.8, with a 10% fastest reduction rate of compromised passwords.

Compromised passwords:
Northern and Western Africa

Northern and Western Africa had the lowest percentage of compromised passwords (9%), and had the highest reduction rate in reused passwords (11%).

SECTION 2

A look at password health across organizations

New to the report in 2024: We've added enterprise and industry stats, which provide differentiating trends and allow us to dive deeper into global password security patterns.

Industry comparisons & how password health impacts them

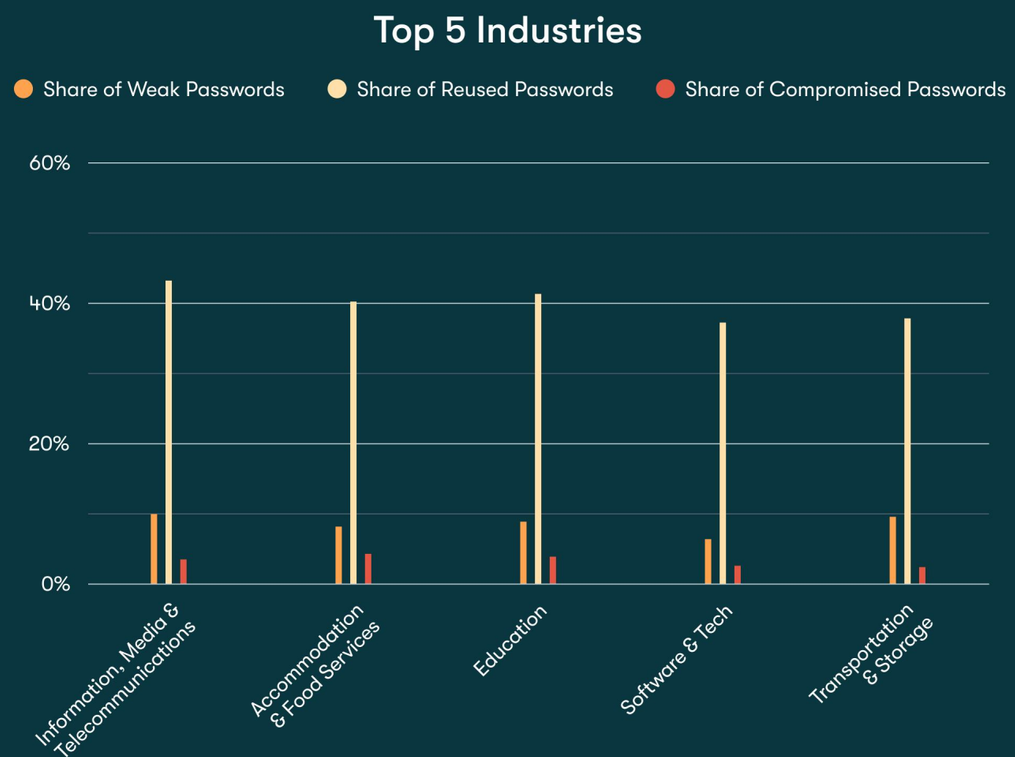
Top 5 Industries with the highest security scores in 2024

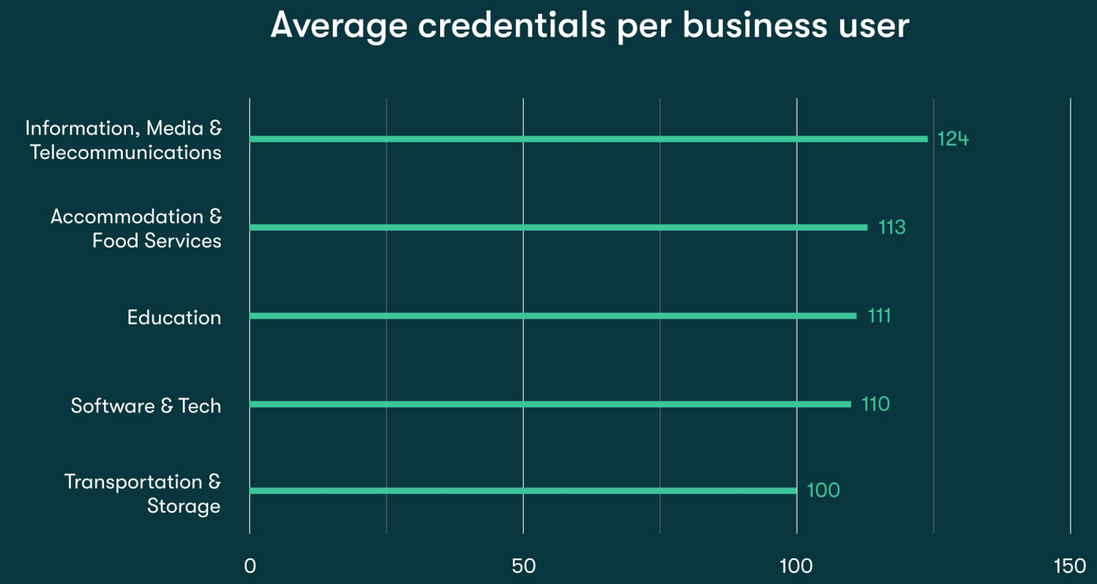
1. Software & Tech
2. Information, Media & Telecommunications
3. Education
4. Transportation & Storage
5. Accommodation & Food Services

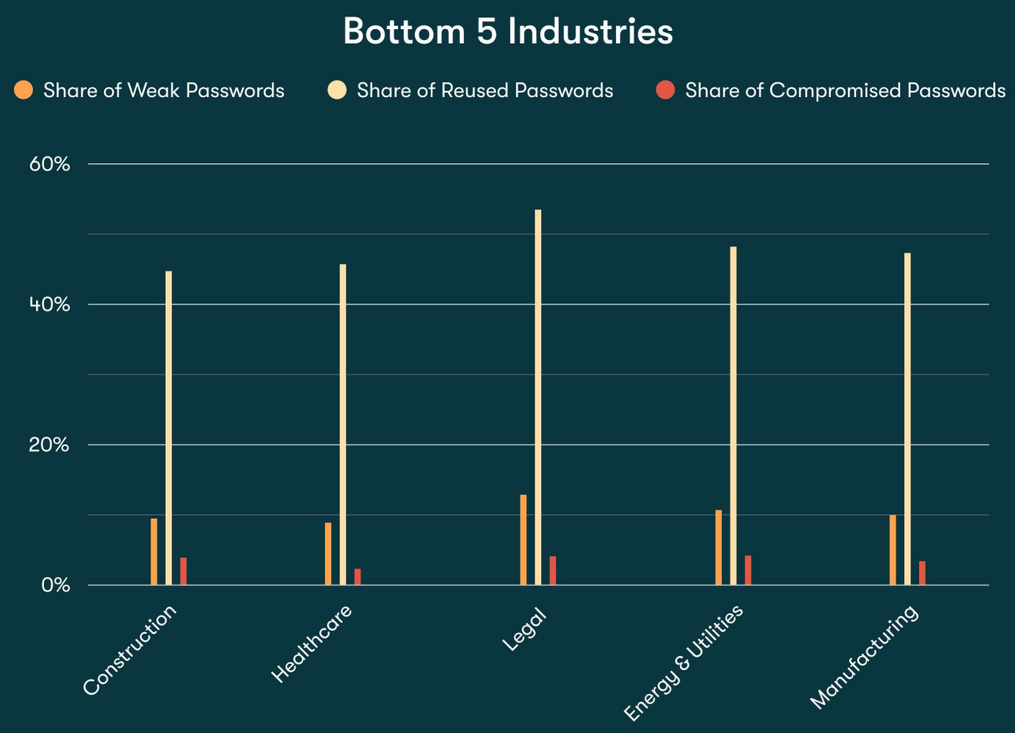
It comes as no surprise that industries that are famously “online” and SaaS-fluent—and likely much savvier and well-informed about cybersecurity risks—are paying more attention to their security scores. These characteristics are especially true for industries such as Software & Tech, Information, Media & Telecommunications and Education.

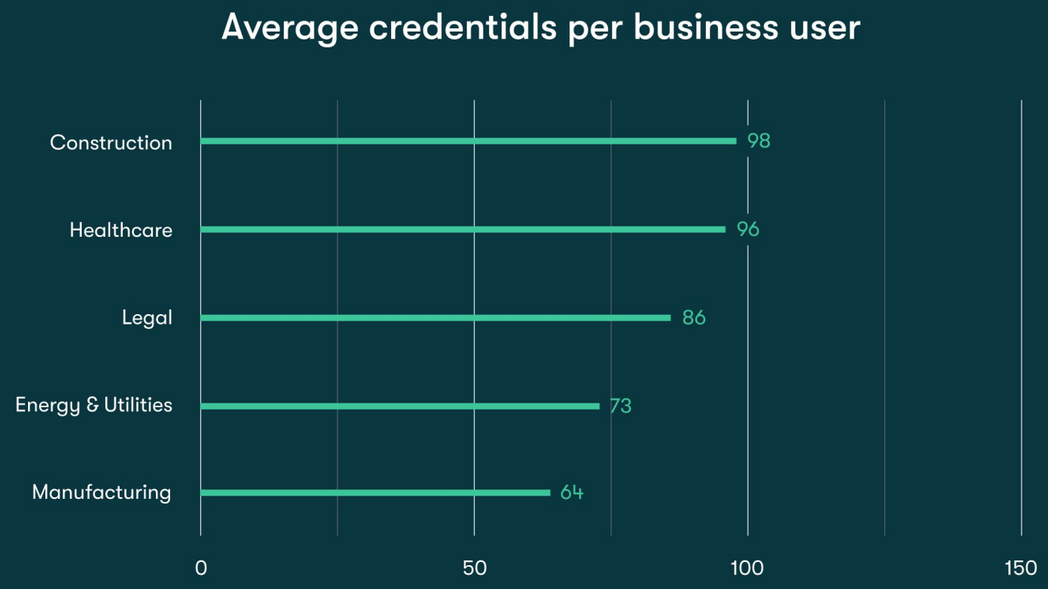
What stands out about Education is how far it has come in regard to digital security. Securing its faculty and students’ data while also educating students on cyber best practices is no easy task, especially considering that the Education industry is one of the most targeted for ransomware. If a school district or student were to get breached, a cybercriminal could exploit extensive amounts of sensitive data about minors.

Transportation & Storage and Accommodation & Food Services often have a different cyber perspective due to heavy reliance on supply chain operations. A cyberattack could physically halt production and operations in these industries.









Industries with the lowest security scores in 2024

1. Legal
2. Manufacturing
3. Construction
4. Healthcare
5. Energy & Utilities

As we introduce our findings for the industries with the lowest security scores, we are able to share insights into each. For example, the Legal industry is not traditionally known for its technological sophistication or being quick to adapt to the rapidly changing online landscape. They can often find themselves lagging behind.

What Manufacturing, Construction, Energy, and Utilities all have in common is that their work takes place in physical locations offline. With employees in these industries traveling away from a home office base and corporate policies requiring password changes every 90 days, despite NIST guidance to the contrary, reused passwords are common, as are shared logins.

With Healthcare being one of the most highly targeted industries for cyberattacks as well as one of the most highly regulated industries under HIPAA, healthcare workers are subject to much more stringent security policies than most. However, sometimes, this has the opposite effect: Employees may assume these regulatory and security requirements are enough to keep them safe, so they might not rely on third parties for security protection as heavily. If they don't use security tools like password managers, they could be missing a critical step in patient and staff protection of highly sensitive data.

If healthcare workers don't use security tools like password managers, they could be missing a critical step in patient and staff protection of highly sensitive data.

Dashlane found the average number of credentials per business user varies greatly when comparing organizations of different sizes.

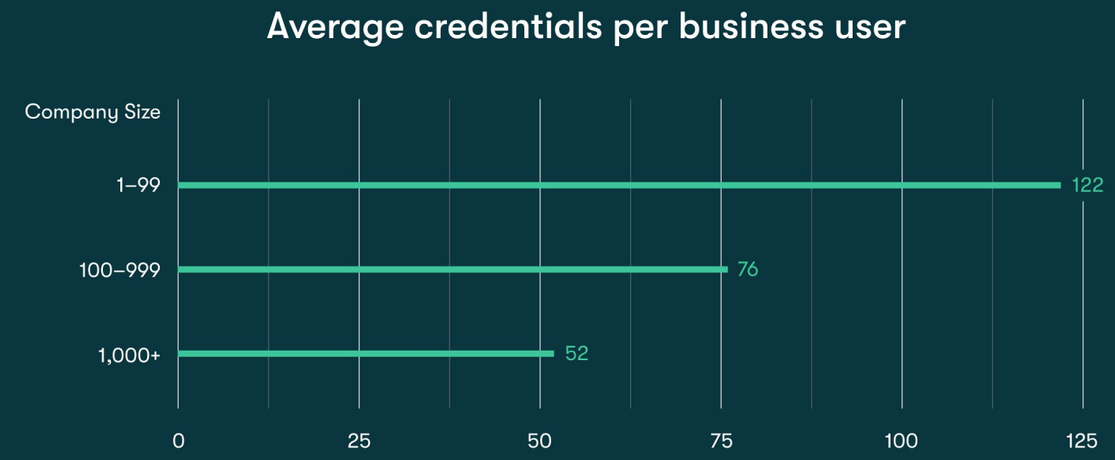
Small businesses had the greatest average number of credentials per user (122), followed by a precipitous drop for midsize businesses (76) and large enterprises (53). While midsize and large businesses often have a more mature identity security stack that includes SSO, it's also common for them to have legacy apps and services that may be slow to offer (or never offer) an SSO option. Even with SSO, the number of credentials in the enterprise represents a significant risk for the organization if not properly secured.

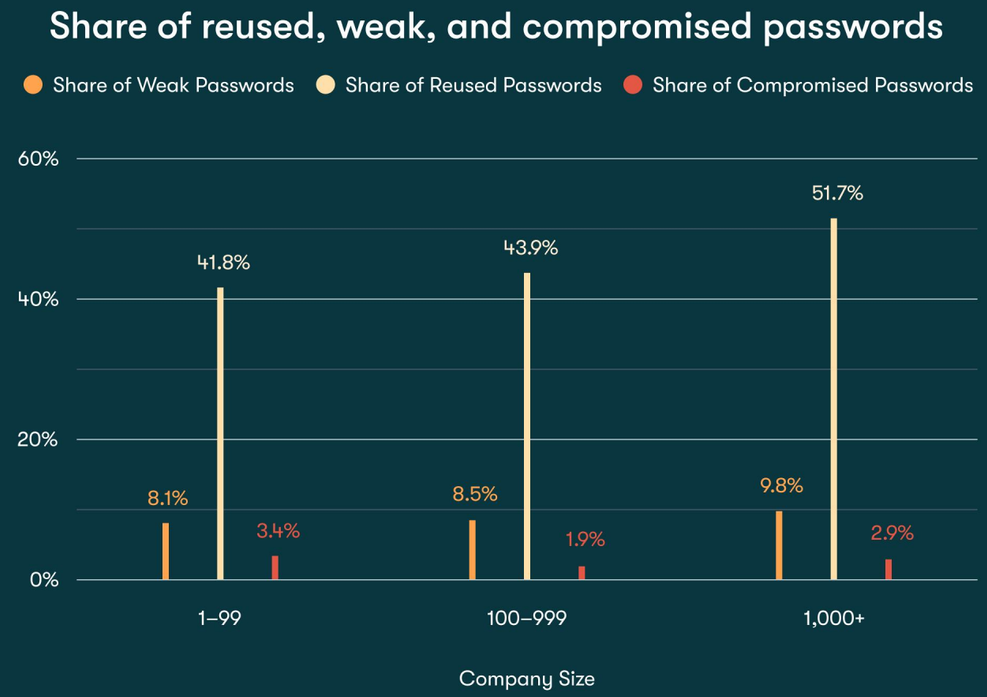
As cited in a CISA report, small and midsize businesses often lack the technical knowledge or financial resources to implement SSO. Vendors are known to charge an "SSO tax" for SSO integrations, which often puts the control out of reach from a cost perspective.

According to John Bennett, Chief Executive Officer at Dashlane, many small and midsize businesses also lack the underlying identity infrastructure, whether that's Active Directory or another identity provider, to implement SSO.

"Betting on SSO as a way to protect organizations is not enough," said Bennett. "A landscape of constantly sprouting new products and services—even with an uptick of new businesses jumpstarting with widely available LLMs—means it's unlikely that a company will be able to manage 100% of its services with SSO at any given time."

Rounding out our look at credential hygiene differences by organization size, midsize businesses (100-999 employees) had the lowest share of compromised passwords (1.9%) compared to small businesses (3.4%) and enterprises (2.9%). More than company size, cybersecurity budgets and policies affect password health.





SECTION 3

How we conducted our research

To illustrate the state of password health in 2024, we collected anonymous usage data from both personal and business accounts, incorporating hundreds of billions of data points.

What factors into your score?

Dashlane's unique algorithm, the Password Health score, identifies weak, reused, and compromised passwords in user vaults for a snapshot of overall password health.

Pro tip

To boost your score, make sure passwords are hard to crack by using our Password Generator with the zxcvbn algorithm, which measures password strength and suggests improvements.

What your score means

Scores of 90 and above are ideal. For scores between 60 and 90, update weak or compromised passwords. Scores below 60 require immediate attention to ensure your online security.

Pro tip

Passwords you don't control, such as smartphone codes, can be stored securely in a separate tab so they don't impact your score.

Data by region

Password Health scores for each region are based on the average and median scores for Dashlane users within that region. We used anonymous data to compute regional scores.

Reducing bias

All countries in the world have been included and grouped into key regions. We created distinct regions that each have a high enough volume of Dashlane users to ensure a consistent breakdown of business and individual users for each region.

Why we use average scores

Our analysis looked at the median and average scores and the distribution of security scores across regions. The average score gives the most meaningful overview of global password health.

Reused and weak passwords are similar globally

However, the amount of compromised passwords varies greatly by region, contributing to the differences we observed in each region.

“Good password hygiene is a critical part of strengthening users against credential-based threats and hardening enterprises from breach.”

—John Bennett, CEO, Dashlane

SECTION 4

Checklist for improving your password health

Ready to boost your password health? Here are five steps to take toward better online security.

Adopt the right credential manager

Gartner® recommends organizations use a workforce password management solution. Solutions like Dashlane help businesses understand and improve password health and security.

Update reused or compromised passwords

Dashlane will notify you of reused, weak, or compromised passwords in your vault. Instantly update or create new strong, unique passwords with our Password Generator.

Create a culture of security

A strong security culture involves every member of an organization. Share the importance of protecting sensitive data and provide tools so employees can be part of the solution.

Simplify security with the right tools

Eliminate compliance risks by securely storing sensitive data in a credential manager like Dashlane, which is GDPR and CCPA-compliant and offers enterprise-grade protection.

Enable multi-factor authentication

Additional proofs of identity, such as facial recognition and fingerprint ID, make logins more secure and significantly reduce the likelihood of account compromise.

Consider transitioning to passwordless

Passkeys and passwordless logins simplify authentication and help protect against phishing attacks. Dashlane was the first credential manager to release passwordless login.

Gartner, “Innovation Insight: Workforce Password Management Tools,” Nayara Sangiorgio, 18 March 2024. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

About Dashlane

Dashlane is the universally loved credential manager that secures access and proactively protects against breaches. Over 23,000 brands worldwide, including Sephora, Air France, and Forrester, trust Dashlane for industry-leading innovations that keep them ahead of evolving threats. We pair patented, enterprise-grade security with consumer-grade design in a top-rated platform, empowering everyone to be part of the credential security solution.

Visit dashlane.com/blog for more resources, digital security tips, and Dashlane product news.

dashlane.com

Privacy & Security

Dashlane employs zero-knowledge architecture in our platform.

We do not and cannot know what information users store on the Services ("Secured Data").

No "personal data" was collected for use in this report. As outlined in our Privacy Policy, Dashlane defines "personal data" as information that, either alone or when combined with other information we hold, identifies an individual, such as name, mailing address, email address, IP address, or telephone number.

All data collected for this report is anonymized and aggregated using IP address information without the last four digits to determine users' location.

Anonymous data means data that, alone or combined with other information available to us or a third party with whom the data is shared, does not permit the identification of an individual.

To get your organization's Password Health score, visit dashlane.com for a free demo.

Regional key

#1 | 79.8 | Eastern Europe:
Bulgaria, Poland, Czechia, Ukraine, Moldova, Slovakia, Russian Federation, Romania, Hungary, and Belarus.

#2 | 77.9 | Northern Europe:
Estonia, Denmark, Guernsey, United Kingdom of Great Britain and Northern Ireland, Isle of Man, Sweden, Iceland, Latvia, Jersey, Faroe Islands, Lithuania, Ireland, Finland, Norway, Svalbard and Jan Mayen, and Åland Islands.

#3 | 77.2 | Western Europe:
Germany, France, Netherlands, Monaco, Switzerland, Belgium, Luxembourg, Austria, and Liechtenstein.

#4 | 76.6 | Central America:
Costa Rica, Dominican Republic, Puerto Rico, Barbados, Martinique, Montserrat, Bonaire, Sint Eustatius and Saba, El Salvador, Belize, Saint Lucia, Cayman Islands, Anguilla, Guadeloupe, Panama, Virgin Islands (U.S.), Curaçao, Cuba, Saint Vincent and the Grenadines, Grenada, Bahamas, Honduras, Haiti, Trinidad and Tobago, Aruba, Jamaica, Saint Martin, Sint Maarten (Dutch part), Dominica, Mexico, Nicaragua, Guatemala, Antigua and Barbuda, Virgin Islands (British), Saint Barthélemy, Turks and Caicos Islands, Saint Kitts, and Nevis.

#5 | 76.4 | Southern & Eastern Africa:
Zimbabwe, Réunion, Seychelles, Somalia, Kenya, Namibia, Mozambique, Zambia, Malawi, Eritrea, Mauritius, Madagascar, Comoros, South Sudan, Swaziland, Tanzania, United Republic of Botswana, Rwanda, Djibouti, Burundi, South Africa, Ethiopia, Mayotte, Lesotho, and Uganda.

#6 | 76.2 | Northern & Western Africa:
Morocco, Côte d'Ivoire, Libya, Senegal, Sierra Leone, Mali, Guinea-Bissau, Gabon, Cabo Verde, Ghana, Burkina Faso, Egypt, Congo (Democratic Republic of the), Angola, Equatorial Guinea, Sudan, Tunisia, Togo, Congo, Algeria, Nigeria, Niger, Benin, Guinea, Gambia, Western Sahara, Cameroon, Mauritania, Saint Helena, Ascension and Tristan da Cunha, Liberia, Central African Republic, Chad, Sao Tome, and Principe.

#7 | 75.9 | South America:
Guyana, Falkland Islands (Malvinas), Argentina, Venezuela (Bolivarian Republic of), Colombia, Ecuador, French Guiana, Suriname, Bolivia (Plurinational State of), Brazil, Chile, Uruguay, Paraguay, and Peru.

#8 | 75.7 | South-Eastern Asia:
Philippines, Vietnam, Thailand, Brunei Darussalam, Lao People's Democratic Republic, Malaysia, Cambodia, Myanmar, Singapore, and Indonesia.

#9 | 75.4 | Middle East & Central Asia:
Turkey, Oman, Uzbekistan, Kuwait, Kazakhstan, Azerbaijan, Yemen, Bahrain, Turkmenistan, Israel, United Arab Emirates, Armenia, Palestine State of Tajikistan, Cyprus, Jordan, Georgia, Qatar, Kyrgyzstan, Iraq, Syrian Arab Republic, Saudi Arabia, and Lebanon.

#10 | 75.4 | Oceania:
French Polynesia, Fiji, Samoa, New Zealand, Tuvalu, Vanuatu, Northern Mariana Islands, Micronesia, Nauru, Pitcairn, New Caledonia, Wallis and Futuna, Solomon Islands, Tonga, Guam, Papua New Guinea, Tokelau, Cook Islands, Marshall Islands, Australia, American Samoa, and Palau.

#11 | 75.2 | Southern Europe:
Portugal, Italy, Slovenia, Gibraltar, Greece, Croatia, Macedonia, Spain, Malta, Andorra, Bosnia and Herzegovina, San Marino, Serbia, Montenegro, Holy See, and Albania.

#12 | 75.1 | Southern Asia:
India, Iran (Islamic Republic of), Nepal, Maldives, Afghanistan, Sri Lanka, Pakistan, Bhutan, and Bangladesh.

#13 | 74.9 | Eastern Asia:
China, Japan, Korea (Republic of), Macao, Korea (Democratic People's Republic of), Hong Kong, Taiwan, Province of China, and Mongolia.

#14 | 72.6 | Northern America:
Canada, Bermuda, Greenland, Saint Pierre and Miquelon, and United States of America.