VERIDIUM
TRUSTED DIGITAL IDENTITY

PASSWORDS ARE THE WEAK LINK

Biometrics are the Path Forward for Enterprise Security

White Paper

PASSWORDSS ARE THE WEAK LINK

BIOMETRICS ARE THE PATH FORWARD FOR ENTERPRISE SECURITY

It cannot be stated often or strongly enough – data breaches are one of the biggest threats organizations face today.

The number of confirmed data breaches grew by 14.5 percent from 2016 to 2017 to reach 2,216, while the number of incidents that could result in compromised data increased 26 percent to exceed 53,000.

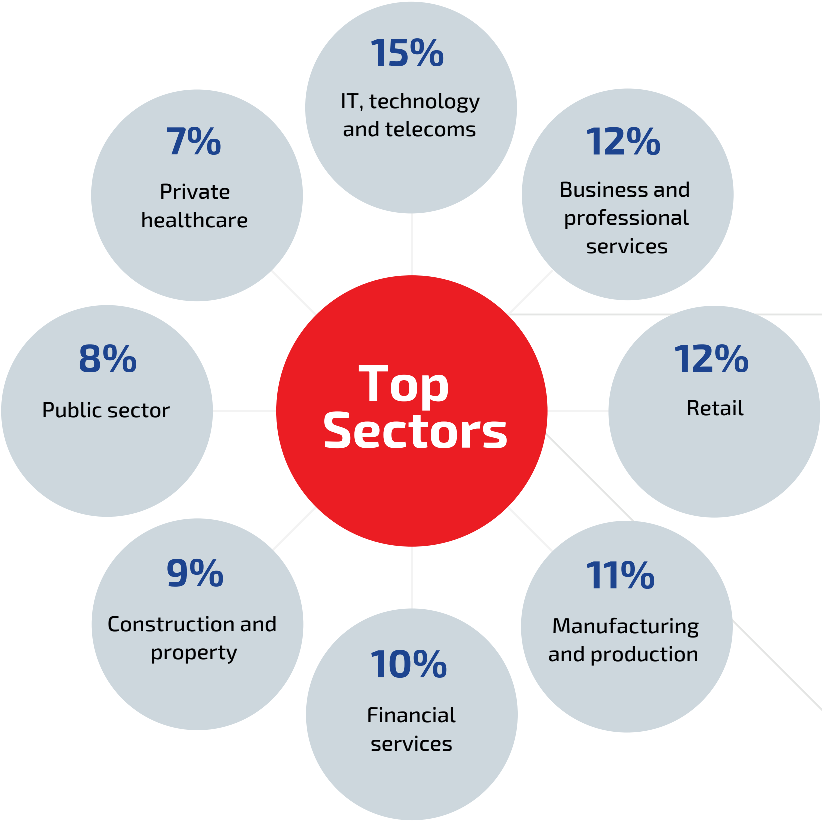
You have implemented hardware tokens for two-factor authentication, one-time passwords, and pushed employee security training initiatives. But hackers are always one step ahead of the technology and, try as you might, it seems impossible to get end users to embrace best practices.

The findings of a new Vanson Bourne survey of 200 senior IT decision makers in the United States, commissioned by Veridium, confirm that passwords remain the weak link in enterprise security.

The survey also highlights the benefits of biometric authentication to help organizations improve security at a lower total cost of ownership with increased employee satisfaction. Find out what IT professionals are saying about the pitfalls of passwords and the steps they are taking to better protect their data with biometric authentication.

DEMOGRAPHICS

200 Senior IT Decision Makers in the United States



Top Sectors

15% IT, technology and telecoms

12% Business and professional services

12% Retail

11% Manufacturing and production

10% Financial services

9% Construction and property

8% Public sector

7% Private healthcare

IT BUDGET

$10–$50 million	: **20%**
$50–$250 million	: **22%**
> $250 million	: **17%**
< $1 million	: **10%**
$1–$5 million	: **16%**
$5–$10 million	: **15%**

THE RISE OF DATA BREACHES

Overall, 59 percent of respondents say their organization has experienced a data breach, 53 percent within the last five years.

All of those who have experience a breach have implemented additional security measures to prevent another from happening in the future.

Sixty-three percent are, or plan to, implement biometric authentication.

59% of organizations have experienced a data breach

63% are, or plan to, implement biometric authentication

Only 34 percent are very confident that passwords alone can protect their data, while 73 percent believe a combination of passwords and biometrics is better, and 71 percent look to traditional multi-factor authentication solutions.

34% **are very confident that passwords can protect their data**

Overall, 99 percent are still using passwords within their organization, though 65 percent have deployed some form of biometric authentication.

65% **have deployed biometric authentication**

The upcoming GDPR compliance deadline also plays a major role in respondents' approach to managing and securing data, with 89 percent says it impacts their decisions, and half saying it has a significant impact. Interestingly, the ratio of respondents concerned with the GDPR increases as their IT budgets do, with 79 percent of respondents from organizations with an IT budget of more than $250 million reporting "significant impact".

89% **say GDPR impacts their decisions**

WHERE PASSWORDS FAIL

The biggest problem with passwords is that end users will always look for ways to get around best practices if they find them cumbersome or inconvenient. According to respondents:

- 90 percent of employees reuse the same password but add or change a number or special character
- 53 percent of employees store their passwords in a browser or password manager
- 41 percent write their passwords down
- 32 percent use "common" passwords like "password123"
- 17 percent said their employees don't bypass their policies

The average length of time between required password changes, one of the main strategies companies use to try to improve security, was three months.

However, on average, 35 percent of help desk calls are for password resets, across all respondents.

This costs organizations $76 per reset, on average, and the number of calls and average cost both rise in correlation with an organization's IT budget.

In order to stem the tide of data breaches and the threat that passwords pose, organizations spend, on average, 22 percent of their annual IT budget on multi-factor authentication. This is expected to rise to 33 percent over the next three years.

Additionally, 81 percent of respondents believe that biometric authentication will perform better than passwords alone, and 39 percent believe it to be more secure than traditional MFA.

MOVING FORWARD WITH BIOMETRICS

Overall, 94 percent of survey respondents already use, or plan to use, biometrics in the next 24 months, with 17 percent planning to implement within 12 months.

There are many reasons for these swift deployment initiatives.

Fifty-three percent say it's because passwords alone aren't enough, 49 percent say it's because stronger authentication is needed for today's more complex threat landscape, and 46 percent say it's to reduce data breaches and fraudulent transactions.

The majority of respondents (97 percent) say they already see, or expect to see, major benefits from using biometric authentication, such as:
Overall better security (63 percent), increased workforce productivity (54 percent), and better accessibility (50 percent).

However, there are still some concerns over adopting biometrics. 42 percent of IT decision makers said they are worried about integration with their existing systems, 41 percent noted employee skepticism as a worry, and 38 percent are concerned with privacy.

But the benefits outweigh these worries, as 62 percent report they are using, or will use, biometric authentication for high privileged access, 62 percent for on-premise login, and 58 percent for remote access control.

In order to ensure security and privacy, respondents were also asked which biometric identifier they think is most secure.

Overwhelmingly, 45 percent said fingerprint recognition, followed by iris recognition (28 percent), face (21 percent), and finally voice (5 percent).

They were also asked what they think the most secure way to store biometric data is, with 43 percent saying on a server, 28 using a distributed data model (stored split between multiple locations), and 24 percent saying on the device.

Ultimately, 86 percent of respondents agree that biometrics is the most secure authentication method for both enterprises and consumers to use.

CONCLUSION

Without question, the survey indicates that senior IT decision makers view biometric authentication as the most secure authentication method for employees and consumers.

This is driven by a genuine lack of confidence that passwords alone can safeguard data sufficiently and a strong desire to make authentication as user-friendly as possible.

To effectively deploy biometric authentication in an enterprise environment, you need a platform that is scalable, extendable, configurable to meet your security needs, and that effectively protects your end users' biometric data.

The VeridiumID platform provides back-end server software and a mobile app that plug seamlessly into many enterprise environments.

Replace passwords, PINs, and tokens with single-step multi-factor biometric authentication in Microsoft Active Directory, Azure AD, Citrix, WSO2, and VPNs that use RADIUS protocols.

VERIDIUM
TRUSTED DIGITAL IDENTITY
Passwordless Authentication
Innovative Ideas,
Inspiring Technologies,
Integrated Identity Platform.
VERIDIUM
TRUSTED DIGITAL IDENTITY
VeridiumID Passwordless Authentication.
The VeridiumID software-only platform has a front-end mobile SDK. So it introduces a variety of explicit and implicit biometric authenticators in your own applications.

VERIDIUM
TRUSTED DIGITAL IDENTITY

London

119 Marylebone Rd
North West House
London NW1 5PU
United Kingdom
+44 1753 208780

Oxford

The Magdalen Centre
Robert Robinson Avenue
Oxford Science Park
Oxford OX4 4GA
United Kingdom

New York

1325 Avenue of the Americas
28th Floor New York 10019
United States of America
+1-857-228-7805

Romania

Bucharest
Buzesti Street 71

Press Contact

info@veridiumid.com
+1-857-228-7805

www.VeridiumID.com