A1TECHNOLOGIES

Microsoft Passwordless Security

Reduces Chances of Being Compromised by up to 99.9%

Microsoft

Microsoft see 10 million username/password attacks every single day. If your organisation is still relying on password protection, and drastically fending off such onslaught, then we feel for you. We also truly hope your security defences are both solid and sound. The hacker is changing tactics, and savvy organisations know that getting hacked and compromised is a case of when rather than if. However, since implementing passwordless security, Microsoft report a reduction in risk of up to 99.9%.

Increasing organisational password complexity or frequency of changes is no solution. Such policies only increase support calls and further alienate users. Sadly, it is users who, unwittingly or otherwise, are key contributors to your organisation's security weakness. Indeed, to such an extent that one speaker at the ***2019 Gartner IAM Conference*** commented:

> ***"Hackers don't break-in, they log in."*** - Bowron, 2020

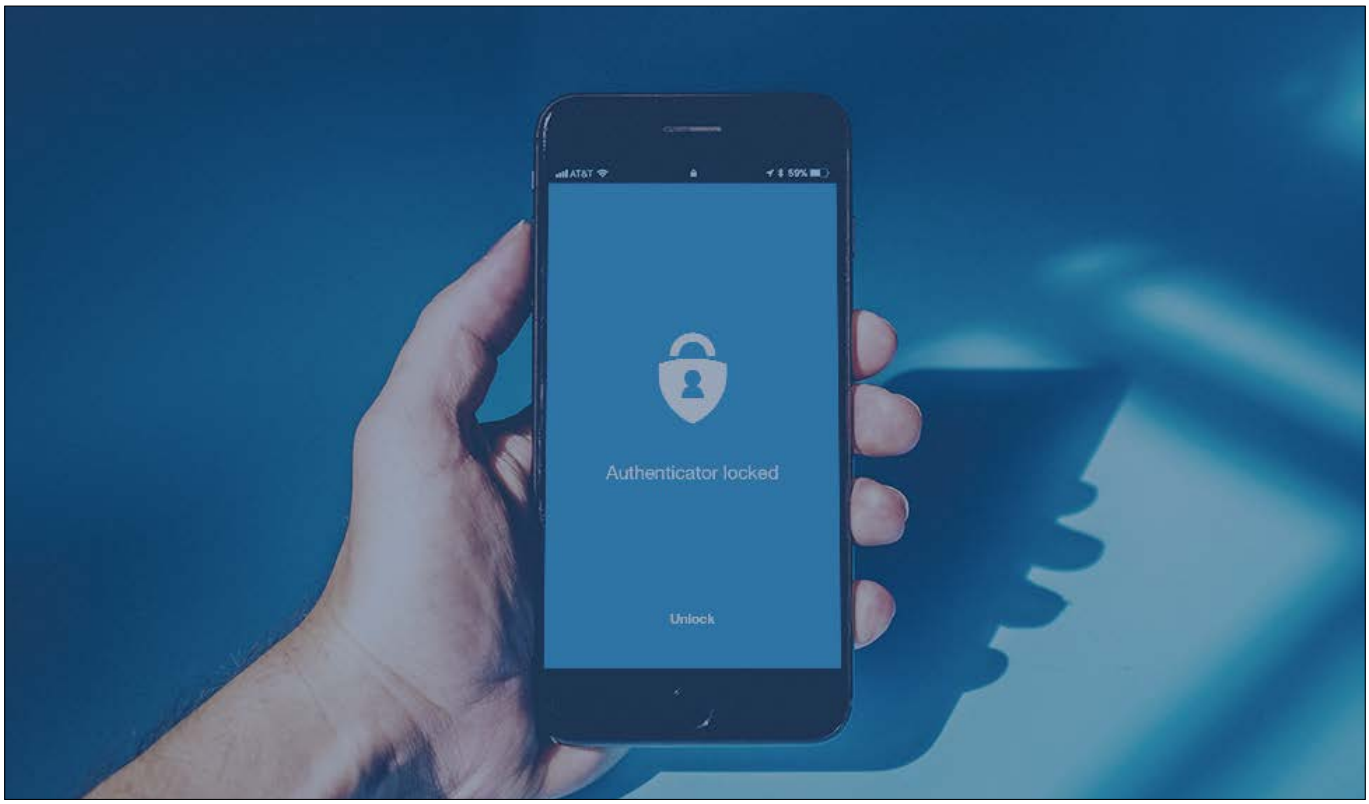
It is up to the organisation to take control

Password protection merely perpetuates a false sense of security. One which contains so many loopholes and backdoors that your organisation may have already been hacked. If not, then every negligent day that such practices remain unchecked shunts your company ever closer to that one unrecoverable breach:

> ***"60% of small to medium sized businesses that suffer a significant cyberattack never recover and go out of business..."*** - Koulopoulos, 2017

Despite user education and awareness about organisational security, they remain a major risk. Indeed, Edward Fulton's statement that "Given a choice between dancing pigs and security, users will pick dancing pigs every time" is, arguably, as valid today as it was the day it was spoken.

Given such behaviour and practices present such risks, and radical change is not even on the radar let alone on the horizon, the only real solution is for organisations to act. In doing so, they remove the weakest link, eliminate all loopholes, and bolster their defence. That is exactly what Microsoft and passwordless security are doing.



Why are Microsoft moving toward passwordless security?

The cost of using outdated and insecure password systems outweighs benefits (Microsoft, 2018, p. 3). Such systems rarely deter hackers and, despite attempts to educate users to the risks, problems are prevalent:

> *"...the biggest surprise is that even though people are aware of the major cyberattacks and increases in costly data breaches, it's still not translating to better password security practices."* - Vijayan, 2018

Reduce your chances of being compromised by up to 99.9%

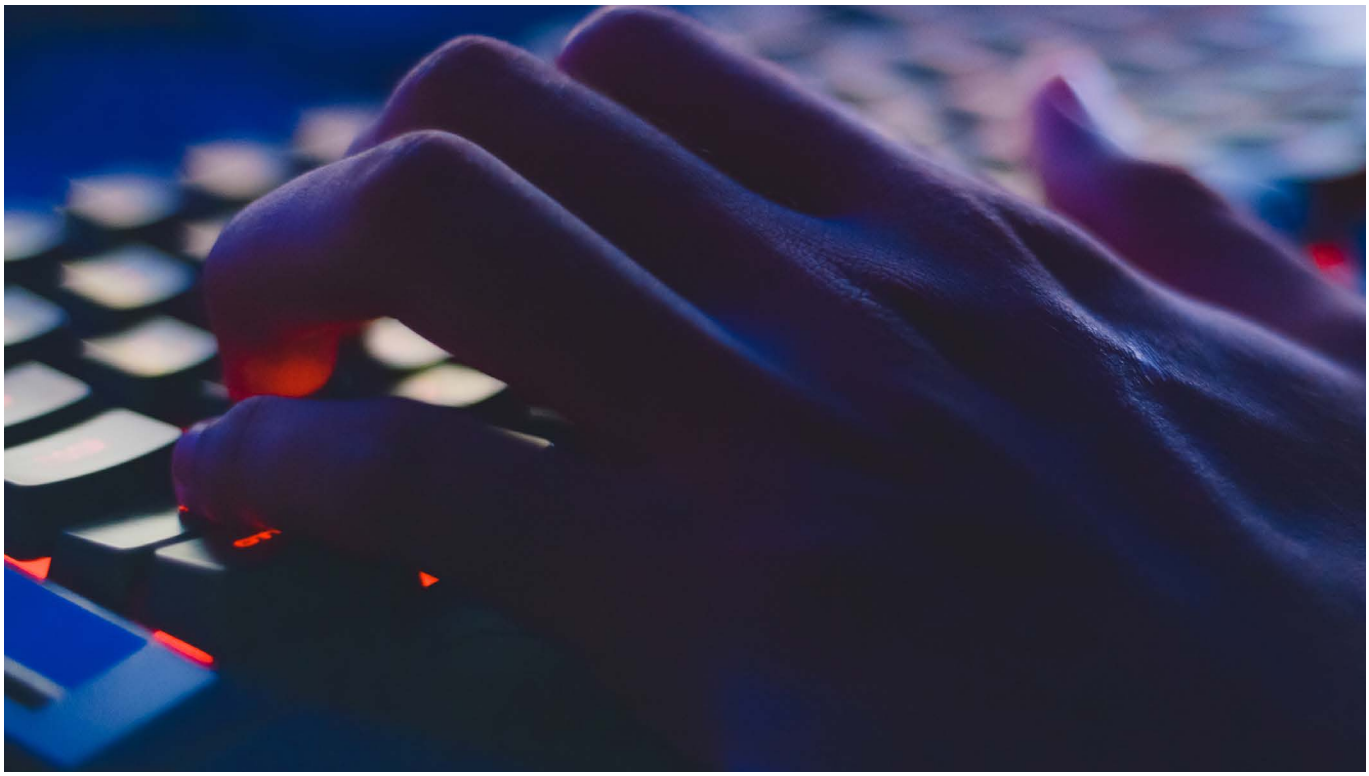
By eliminating passwords, you systematically remove both cause and problem. Indeed, research has shown that by implementing passwordless security/Multi-factor Authentication (MFA), the chance of being compromised can be reduced by up to 99.9% (Microsoft 2018 Security Research).

Moreover, that is not the only benefit. According to Okta (2019), organisations can also avoid what happens when a user forgets their password:

- **37%** are locked out of their account.
- **37%** cannot access something they need.
- **19%** delay work.

Following their own implementation of passwordless authentication, Microsoft experienced significant savings:

> *"When Microsoft switched to passwordless, the support cost of managing passwords internally went down by 80%."* - Joy Chik, CVP in Microsoft's Identity Division



Additional passwordless security benefits

Other benefits include:

- **Improved user experience —** fewer passwords to remember or update, less stress, streamlined and faster logins, improved productivity, self-service password resets, etc.
- **Enhanced security —** user practices such as sharing or reusing passwords are sub-standard and are, according to Verizon, attributable to 81% of breaches (2019).
- **Cost reduction —** for many organisations, password resets account for between 30%-50% of IT help desk tickets (Forrester, 2018); for Microsoft, this was 80%.
- **Better control and visibility —** simplified user management, better and easier to manage policies, centralized and granular control, etc.
- **Less downtime —** quicker authentication means faster logins, less delayed work, less frustrations, improved support capabilities, etc.

"Turning on passwordless makes management much simpler, it reduces the cost; it makes the adoption of what's basically MFA more secure and with a better user experience." - Joy Chik

As of May 2020, in addition to the over 150 million Microsoft consumer and enterprise accounts that were using passwordless authentication, so were over 90% of Microsoft's 150,000+ employees.

How does Microsoft's passwordless security work?

Passwordless protection uses a form of Multi-Factor Authentication (MFA) that uses secure alternatives to achieve your organisation's 'desired security outcome'. This outcome will, typically, consist of a combination of secure login, user-friendliness, minimal support burden, organisational policies, etc. Passwordless protection requires at least two verification methods, secured via a cryptographic key pair, that establish you are who you say you are and can therefore permit access. Verification methods are based on something you know, have, and are.

Microsoft's verification methods

Microsoft uses the following 3 verification methods for passwordless protection:

- **Windows Hello for Business –** a biometric authentication feature that uses fingerprint matching and facial recognition to guard against spoofing ***(something you are).***
- **Microsoft Authenticator –** this uses similar biometrics data to Windows Hello. The authenticator typically generates a PIN or receives a push notification that users then used to verify they physically have the device ***(something you know—the code—and have—the device).***
- **FIDO2 security keys –** strong encryption and authentication via high-security, portable, public-key cryptography-type devices which allow e password replacement with either a personal or an organisational security key ***(something you have).***

All 3 methods use the same cryptographic authentication pattern to generate and authenticate credentials to securely validate and verify your identity.

Note: Microsoft Edge is an additional component that contains a Web Authentication API enabling you to authenticate from your browser using Windows Hello or FIDO2 security key compatible apps.

Example

In its simplest form, logging in with MFA requires you to authenticate using 2 verification methods. This could be a password, or a passcode combined with a PIN number generated on the authentication app you have on your device. Even guessing or hacking your password will not permit entry and, given the minimal chances of guessing the random authentication number.

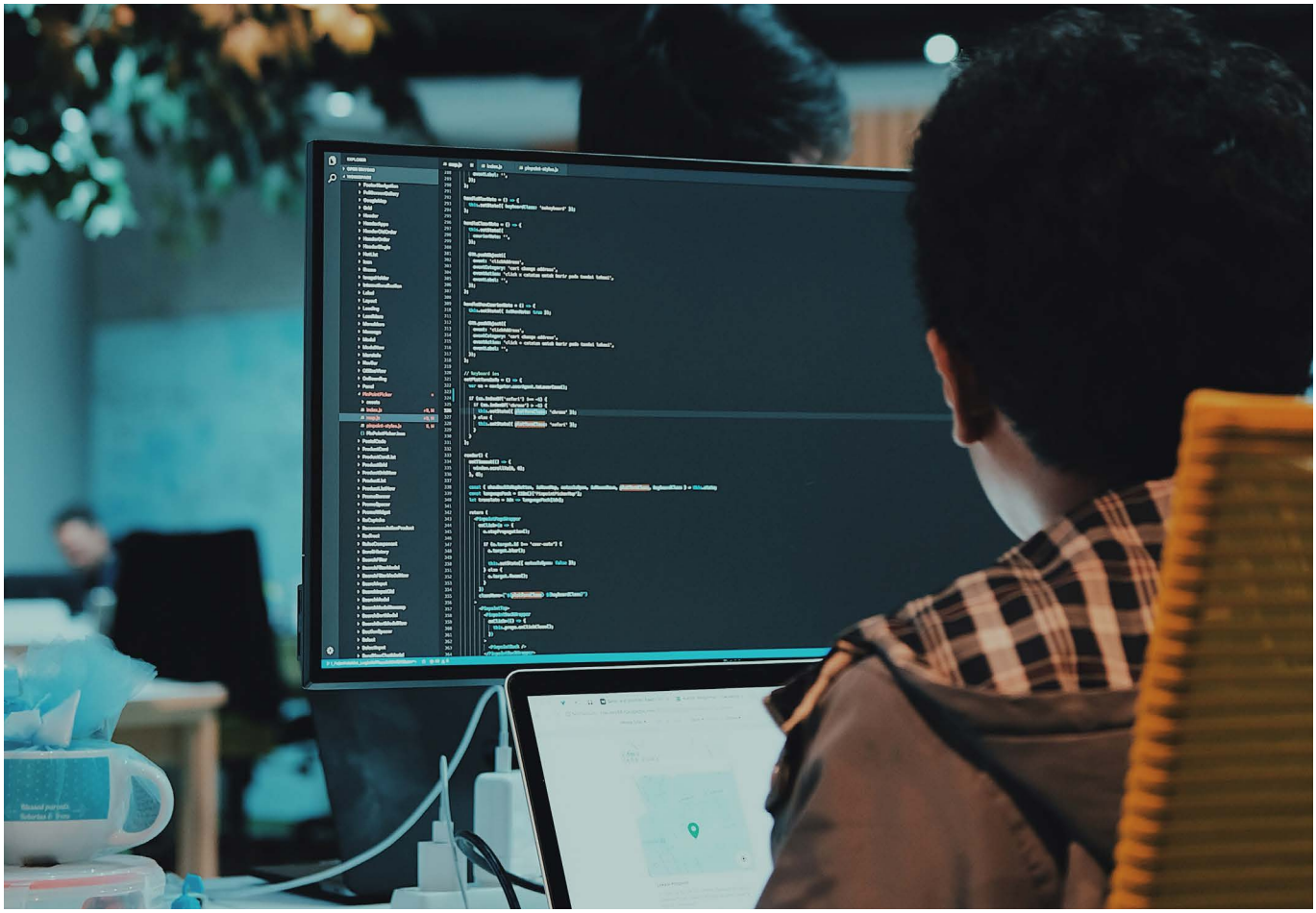
> *"Over nine in 10 respondents (92%) believe that delivering a passwordless experience for end-users is the future for their organisation."* - LastPass, 2020

Next Steps

If you have any questions about the article you have just read or want additional information, then ***click here to contact us.***

For further reading, we recommend:

- **Managed Cloud Services** – A1 Technologies have deep experience with Azure and can help answer all your questions.
- **IT Consultants & Professional Services** – a team of expert IT consultants, we have years of experience helping to design, deploy, and maintain reliable and innovative IT solutions.
- **Case studies** — real-life results of how we have helped organisations like yours achieve great successes.



Bibliography

- Bowron, R. (2020, January 29). ***5 Final Thoughts on Gartner IAM 2019.*** Retrieved November 25, 2020, from idenhaus: https://www.idenhaus.com/5-more-takeaways-gartner-iam-2019
- Forrester. (2018). ***Best Practices: Selecting, Deploying, And Managing Enterprise Password Managers: Solutions Reduce The Risk Of Breaches From Compromised Credentials.*** Cambridge, MA: Forrester. Retrieved December 3, 2019, from https://keepersecurity.com/assets/pdf/Keeper-White-Paper-Forrester-Report.pdf
- Koulopoulos, T. (2017, May 11). ***60 Percent of Companies Fail in 6 Months Because of This.*** Retrieved November 25, 2020, from Inc.com: https://www.inc.com/thomas-koulopoulos/the-biggest-risk-to-your-business-cant-be-eliminated-heres-how-you-can-survive-i.html
- LastPass. (2020). ***From Passwords to Passwordless.*** NK: LastPass.
- Microsoft. (2017, December 26). ***What's the solution to the growing problem of passwords? You, says Microsoft.*** Retrieved November 27, 2020, from Microsoft: https://news.microsoft.com/features/whats-solution-growing-problem-passwords-says-microsoft/
- Microsoft 2018 Security Research. (2018, January 29). ***Five steps to securing your identity infrastructure.*** Retrieved November 23, 2020, from Microsoft: https://docs.microsoft.com/en-us/azure/security/azure-ad-secure-steps
- Microsoft. (2018, November 12). ***The end of passwords.*** Retrieved November 25, 2020, from Microsoft: https://www.microsoft.com/en/security/business/identity/passwordless?market=af
- Okta. (2019, June). ***The Passwordless Future.*** Retrieved November 23, 2020, from Okta: https://www.okta.com/resources/whitepaper-passwordless-future
- Verizon. (2019). ***2019 Data Breach Investigations Report.*** Retrieved August 22, 2019, from https://enterprise.verizon.com/resources/reports/dbir/
- Vijayan, J. (2018, May 1st). ***Password Reuse Abounds, New Survey Shows.*** Retrieved November 25, 2020, from Dark Reading: https://www.darkreading.com/informationweek-home/password-reuse-abounds-new-survey-shows/d/d-id/1331689

A1 TECHNOLOGIES

A1 Technologies is an Australian IT Consultancy and Managed Service Provider (MSP) specialising in delivering robust, responsive, and secure IT and Technology solutions to businesses Australia-wide.

If you need help deploying, managing, or optimising any part of your technology infrastructure, feel free to reach out, we would love to hear from you.

Get in Touch

Contact: Rob Rattray, Sales Director
P: 1300 287 910 | **E:** rob@a1t.com.au