A1TECHNOLOGIES

Enhanced Organisational Security, Improved User Experiences

and $8,000,000 Cost Savings to Boot

Microsoft

This is a follow-on article to the article '**Microsoft Passwordless Security Reduces Chances of Being Compromised by Up to 99.9%**' where we looked at why Microsoft are moving towards passwordless security for Azure AD. In this article we will look at the following topics:

- The cost to the organisation
- Organisational password-related security issues
- How passwordless authentication will impact your business/IT environment
- Microsoft's Passwordless Authentication Methods
- Recommendations for adopting a passwordless strategy

"By 2022, Gartner predicts 60% of large and global enterprises, and 90% of mid-size enterprises, will implement passwordless methods in more than 50% of use cases."- Omale, 2019

The cost to the organisation

Password protection–usernames and passwords–is weak, inefficient, and expensive. Given that the number of passwords each user must manage is growing—some say each user has approximately 200 passwords; others say this figure is conservative—organisation's actual figures around loss of productivity and support costs varies. However, in terms of both expectations and risk, it is a major problem.

"The problem is to ask humans to memorize and manage hundreds of them."
- Emmanuel Schalit, CEO, Dashlane

For Microsoft, their figures are stark. Prior to rolling out passwordless authentication, they estimated the following costs:

- $6 million/year in **Soft Costs –** productivity lost from users who cannot login
- $3 million/year in **Hard Costs —** support desk costs for helping those users.
- Since implementing passwordless, **both have been reduced by 87%** (to a combined total of just over $1 million USD).

"When Microsoft switched to passwordless, the support cost of managing passwords internally went down by 80%." - Joy Chick, CVP, Microsoft Identity Division

Not only a massive reduction in costs, but also delivering intangible extra such as extra time, labour, and expense incurred by the hacker. If your organisation is deliberating the switch to passwordless protection, the following will also interest you.

Organisational password-related security issues

In their 2018 report, Forrester highlighted 5 on-going password-related security issues that organisations must address: (Forrester, 2018)

- **High support costs –** many organisations allocated $1 million+ annually to manage password-related support tasks. Much to organisation's chagrin, increasing password complexity and frequency of changes proved counterproductive

> *"The starting point is to move beyond the assumption that an ever-growing security team is the best way to respond to increasing security risk."* - Gartner, 2020

- **Increased security risks for legacy apps and systems –** disparate systems and a lack of consolidated sign-on exposes the organisation to undue risk. According to Okta's 2019 report, 34% of users use the same passwords for multiple accounts (The Passwordless Future).
- **Increased risk of insider attacks –** with 34% of users reusing passwords for multiple accounts and 26% of users writing passwords down on paper, the organisation is wide open to exploitation and malicious intent (Okta, 2019).

> *"81% of hacking related breaches used either stolen or weak passwords"* - Verizon, 2019

- **Lost end user productivity –** Microsoft's soft and hard costs amounted to over $9 million annually.
- **High compliance costs –** tracking and managing access across disparate networks is not only problematic and time-consuming but the way users manage it of risk to the organisation.

> *"While the average cost of compliance is $5.47 million… the average cost for organisations that experience non-compliance problems is $14.82 million."* - Globalscape, 2017

However, by moving to passwordless authentication/security, Microsoft aim to eliminate these issues.

How passwordless authentication will impact your business/IT environment

Eliminating such opportunities and reducing the elements of poor or insecure user practices offers several key benefits to both your business/IT environment and the organisation:

- **Enhanced security –** switching to passwordless Multi-Factor Authentication (MFA) has been proven to reduce the odds of being compromised by 99.9% (Microsoft 2018 Security Research, 2020).
- **Balanced convenience –** easy to use, convenient sign in, combined with speed, simplicity, and self-service management benefits both user experience and organisational security risk.
- **Reduced support burden –** empowering users with their own login security and password reset functionality eases the support burden allowing them to focus on more business-critical tasks.
- **Flexible, manageable, and scalable –** when MFA is used with other security systems, such as Single-Sign-On (SSO) and company security and access policies, this is not only easier to manage, but is both more flexible to change and scalable.

- **Maximum efficiency –** eliminating the number of lockouts, the reliance on support to permit access, and the delays therein minimizes downtime, hassle, and removes obstructions to work

This is further correlated by AT&T's 2020 survey which discovered that,

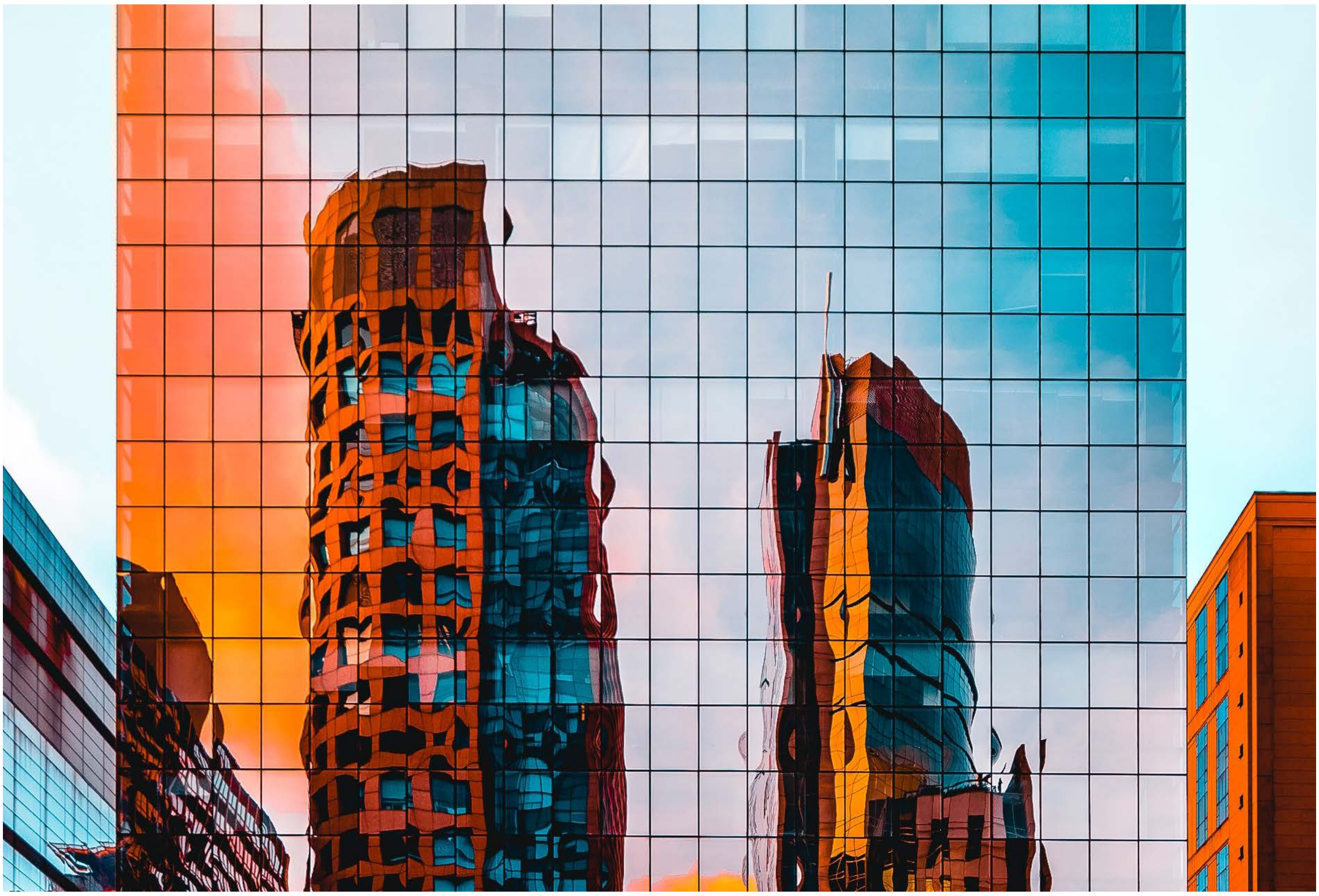
> *"Despite their successes, "leading" organisations understand that security is a journey and not a destination... and strive for continuous improvement. So, while "leading" organisations spend more on security, they report stronger return on investment (ROI) on security investments."*
> - AT&T Cybersecurity, 2020

Microsoft's Passwordless Authentication Methods

- **Windows Hello –** strong 2-factor MFA on PC's and mobile devices that authenticates via a user biometric credential or a device-specific PI. *(prerequisites)*
- **Windows Authenticator –** using similar technology, the authenticator app enables any iOS or Android phone as a verifiable credential. *(prerequisites)*
- **FIDO2 Security keys –** a passwordless authentication method tied to a physical device such as a USB drive, Bluetooth, etc. *(prerequisites)*

Note: Though not a passwordless authentication method, Windows Edge is also used as it permits browser authentication via supported apps that use Windows Hello and external FIDO2 devices.

> *"Windows Hello for Business is personal, simple, and provides a brilliant user experience with high security. Our people love logging on with their fingerprint or face."*
> - Peter Scott, Director of Dynamic IT, British Telecom Technology



Recommendations for adopting a passwordless strategy

If your organisation already uses Microsoft technologies, then the transition is straightforward. From their **website,** Microsoft recommend you follow these 4 steps:

1. **Understand password risks** - they recommend auditing your environment for risky passwords to help raise user awareness in why eliminating passwords is critical as well as to helping them understand how much easier passwordless authentication is.
2. **Enable self-service reset** – users performing their own password reset without any support or admin involvement not only empowers them, but it also provides valuable additional insights and control from an administration perspective.
3. **Try password alternatives** – passwordless authentication is both convenient and secure. The increased numbers of apps that require 2-factor MFA show that usage is becoming more widespread, and this step raises awareness around what your organisation requires for its own deployment.
4. **Reduce prompts** – Conditional access determines the context of each login, including whether access is internally on a computer or externally on a device. This aids in analysing risk, understanding threats, and providing exactly the right user' access and permissions.

When used in conjunction with organisational security and access policies, this helps increase productivity, control risk, address compliance and governance issues, and manage costs.

"Don't let perfection stand in the way of progress. Every step toward passwordless is a step toward improving your security posture." - Bret Arsenault, CISO for Microsoft

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:

- **Microsoft Passwordless Security Reduces Chances of Being Compromised by Up to 99.9%** – an overview of the benefits of passwordless security
- **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

- AT&T Cybersecurity. (2020, March). ***The Relationship Between Security Maturity and Business Enablement.*** Retrieved November 27, 2020, from AT&T Cybersecurity: https://cybersecurity.att.com/resource-center/white-papers/security-maturity-and-business-enablement
- 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
- Gartner. (2020). ***Rethink the Security & Risk Strategy. Stamford: Gartner.*** Retrieved from https://www.gartner.com/en/publications/rethink-security-risk-strategy-ebook
- Globalscape. (2017, December). ***The True Cost of Compliance With Data Protection Regulations.*** Retrieved November 27, 2020, from Globalscape: The True Cost of Compliance With Data Protection Regulations
- Microsoft 2018 Security Research. (2020, 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
- Okta. (2019, June). ***The Passwordless Future.*** Retrieved November 23, 2020, from Okta: https://www.okta.com/resources/whitepaper-passwordless-future
- Omale, G. (2019, March 6). ***Embrace a Passwordless Approach to Improve Security.*** Retrieved November 30, 2020, from Gartner: https://www.gartner.com/smarterwithgartner/embrace-a-passwordless-approach-to-improve-security
- Verizon. (2019). ***2019 Data Breach Investigations Report.*** Retrieved August 22, 2019, from https://enterprise.verizon.com/resources/reports/dbir/

A1TECHNOLOGIES

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