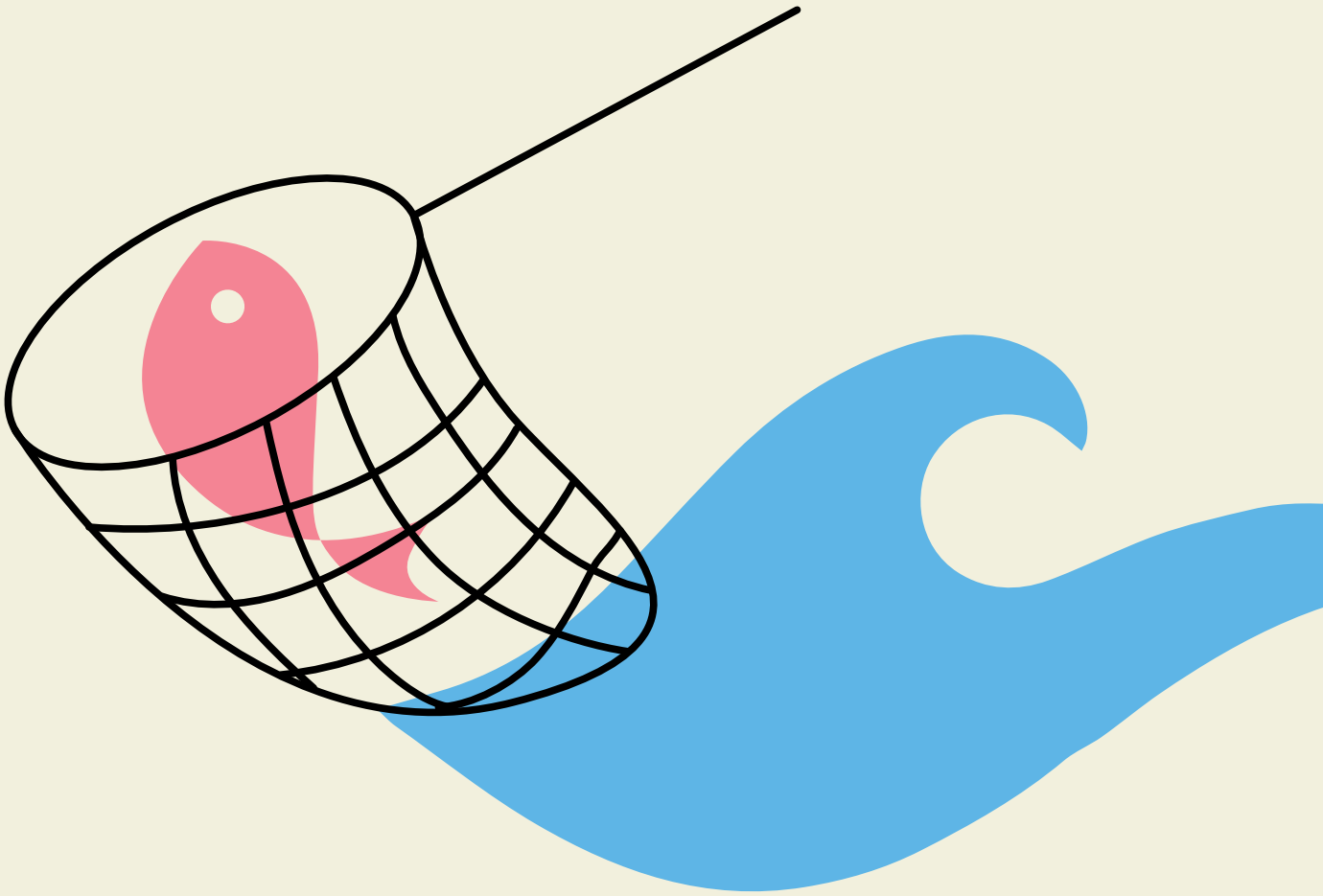
azured

From minnows to whale sharks

Why securing Microsoft 365 should be top priority for all businesses.



In the UK alone there are, on average, three companies who fall victim to a cyberattack every day of the year*. As we all know, it's hard enough trying to run a business — especially at the moment — without the additional worry that your company could be the latest victim of a ransomware attack. Once only a concern for large corporations, cybercriminals have now cast their nets wider; hauling in both minnows and whale sharks.

We are all exposed to the next generation of cybercriminals

Traditionally cybercrime was targeted at large organisations due to the level of effort and skill it took criminals to find a way into the organisation, find data and then steal or encrypt it. Smaller companies slipped under the radar, proving not worth the effort.

This has changed dramatically in the last twelve months. Attackers no longer need the skills to conduct a sophisticated attack by themselves. As a terrifying example, login credentials for organisations are traded online for only a few pounds each. Cybercriminals operating illegal 'Ransomware as a Service' businesses help run the whole attack, including providing the decryption methods and handling the ransom payment, for a share of the profits.

Low-level cybercriminals can now easily perform ransomware attacks, meaning smaller companies with less security are very much in the crosshairs.

Businesses of all sizes must take cybersecurity seriously. If not, they risk potentially irreparable damage through financial loss, destruction of reputation and the inability to trade.

> 'Ransomware as a Service' businesses handle the decryption and the ransom payment for a share of the profits

* IT Governance, 2020 cyber security statistics, January 2021

azured

Protecting small businesses against enormous threat

Microsoft 365 gives us an incredible service for very little investment. Microsoft has recently unlocked features previously unavailable to the SMB sector, allowing businesses to collaborate like never before. You may have experienced this when using Teams and document collaboration during the recent lockdowns, tools that have made remote-working not only possible, but seamless. Productivity increases exponentially when you're able to access your company's data from anywhere on the planet.

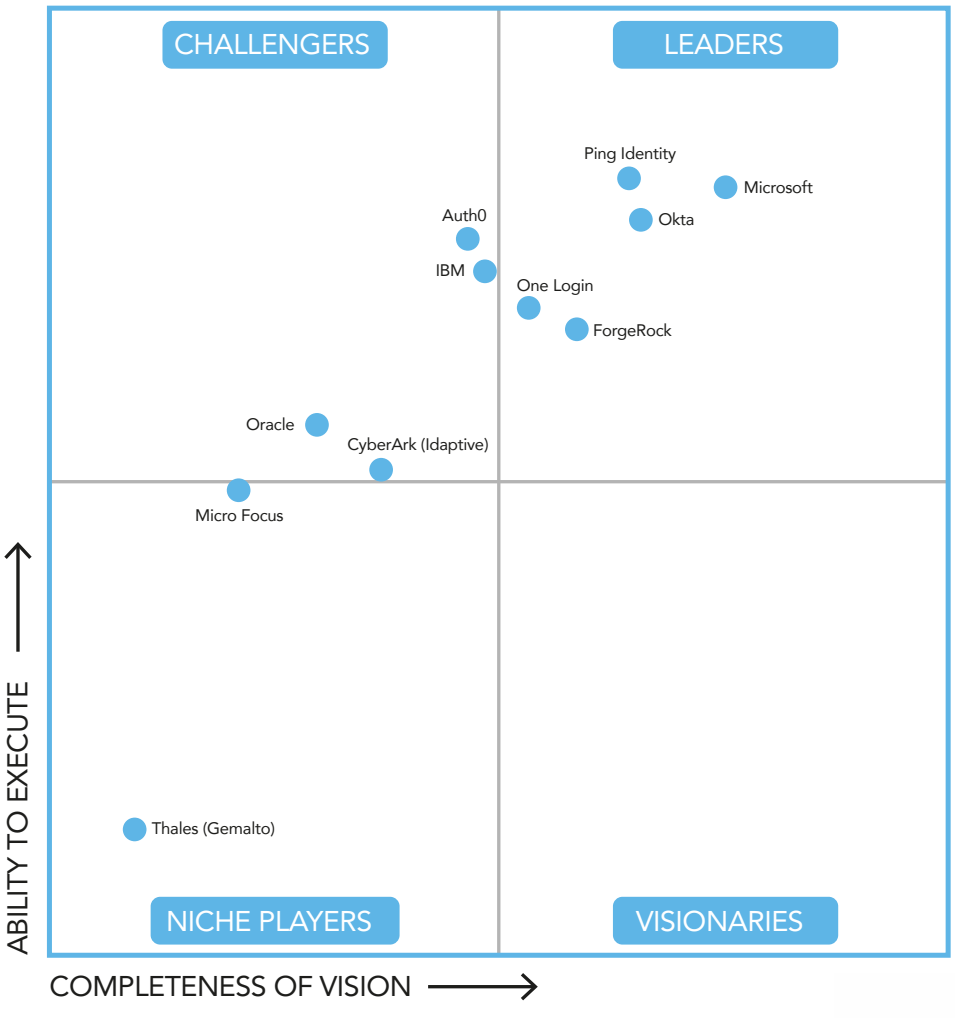
But this level of accessibility causes a significant problem. Cybercriminals can also attempt to access your environment from anywhere on the planet. Companies must adopt a zero-trust approach to protect themselves.

Cloud security typically starts with Identity and Access Management, which is the method used to authenticate into cloud services, usually in the form of an email address and password. This is often the most straightforward service to breach as cybercriminals can use various methods to steal a staff member's username and password.

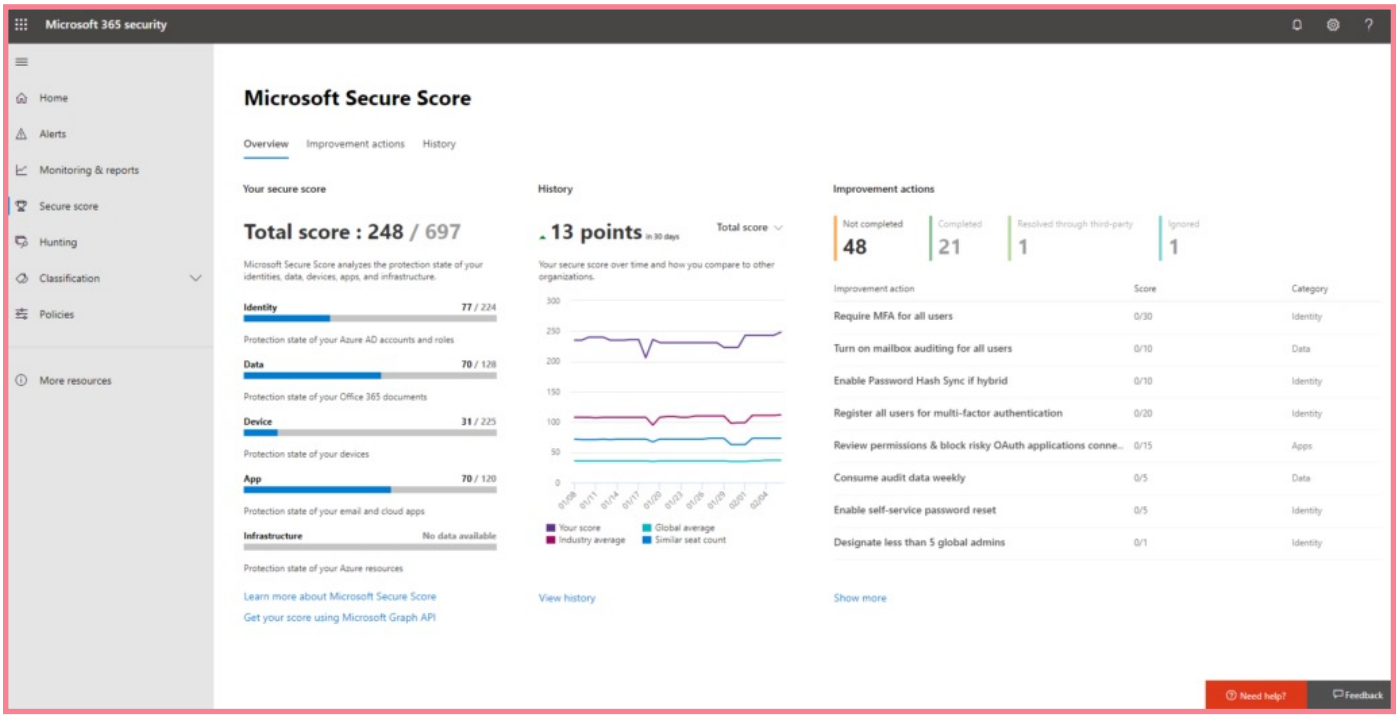
Over the past few years, Gartner has ranked Microsoft as a leader in five different security areas, including Identity and Access Management.

Using Microsoft 365 gives you the foundation you need to deliver exceptional security around Identity and Access Management. Implementing Microsoft 365 correctly can increase the security of your cloud-based services no end.

Productivity increases exponentially when you're able to access your company's data from anywhere on the planet.



azured



Example Secure Score dashboard

Scoring highly for security: Microsoft Secure Score

Recognising the sudden growth in cyberattacks, Microsoft engineered an invaluable benchmarking system to help companies reduce their risk of attack. Back in 2020, they released Microsoft Secure Score. Secure Score marks your organisation out of 100 for various security elements — including Identity and Access Management, devices, data, apps and infrastructure — providing you with multiple sub-scores each contributing to the overall score for your security. As you configure your environment your score either increases or decreases, based on your real-time security posture.

Using these scores gives an organisation a straightforward way to understand, monitor and improve the security of their Microsoft 365 environment.

The Secure Score console is divided into various sections, giving you easily digestible and actionable information about:

- Your current score
- Your score history
- A list of actions to review which can increase your score
- A comparison against other organisations

You can start now by going to **https://security.microsoft.com** and signing in to access your own secure score.

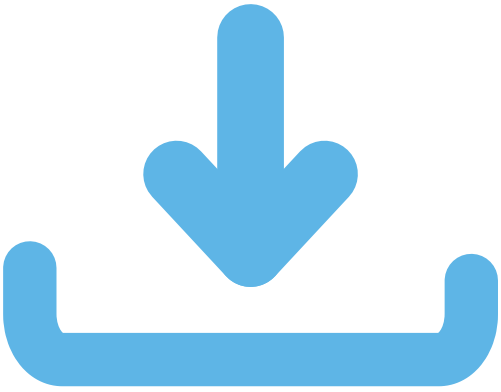
The dashboard will suggest the actions you need to take to improve your score and, ultimately, your organisation's security.

As a starter for ten, here are some pointers that will almost certainly improve that score:

- Insist all staff use the strongest level of Multifactor Authentication (MFA) available
- Block legacy authentication methods from the environment; legacy authentication doesn't support MFA, meaning it can be bypassed
- Reduce administrative rights on all standard accounts

Secure Score marks your organisation out of 100 for various security elements — including Identity and Access Management, devices, data, apps and infrastructure

azured



And always backup your data

Data backup is not featured on Secure Score, but it's critical, so we had to mention it. You can never be 100% protected from ransomware (that's a fact), so backup must always be front of mind. Having good backups can make the difference between your company continuing to operate or going bust.

Imagine logging on tomorrow and every document, database and file in your organisation being encrypted. Now think of the consequences of not being able to recover that data.

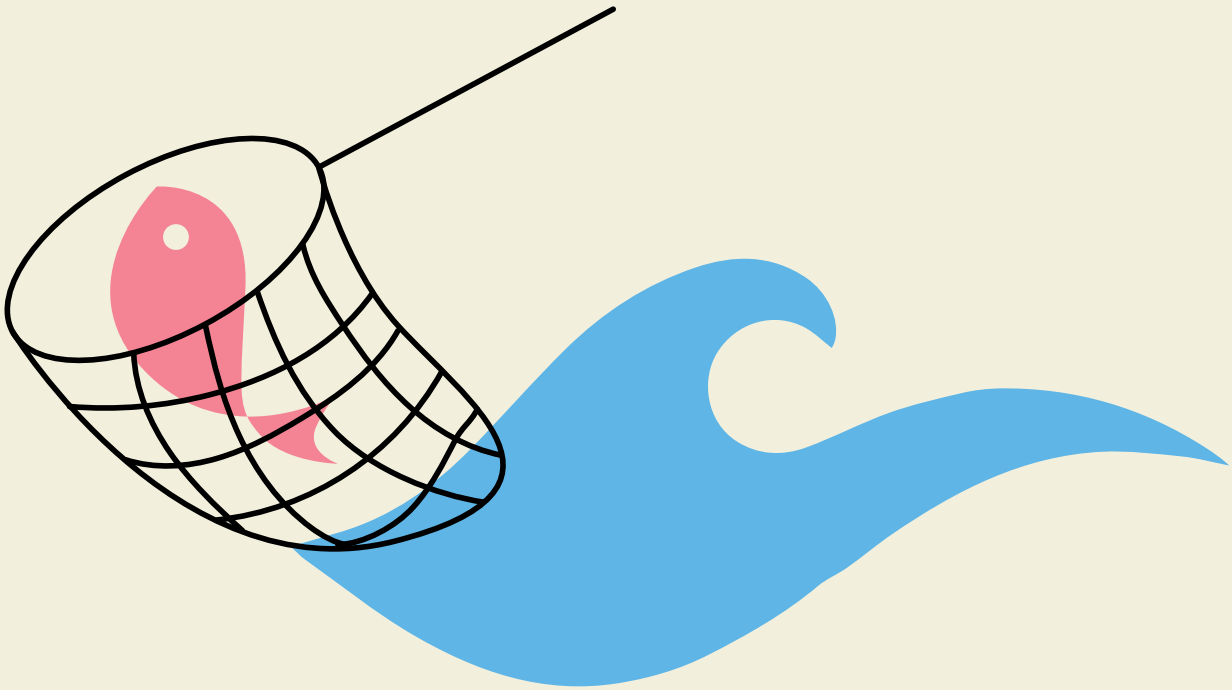
If you're not backing up your data effectively, we urge you to start now!

Conclusion

Microsoft 365 is an essential service for organisations of all sizes, but it must be appropriately secured, and data must be protected. This guide is not an exhaustive list of how to secure your environment but is designed to give you some general information about where to make a start. If you are not familiar with the techniques discussed above, we recommend getting some advice from a professional consultancy.

Book in a cloud security assessment with Azured and if we can't find any vulnerabilities, it's free! Schedule a quick call or drop us a line at: hello@azureduk.com to find out more.

azured



azured

Azured UK Ltd
www.azureduk.com
hello@azureduk.com