WHATS YOUR SECURE SCORE?

THE FIRST STEP IN PROTECTING YOUR ORGANISATIONS MICROSOFT 365 TENANT

STEVE BARKER

OVERVIEW

EXECUTIVE SUMMARY

Microsoft 365 provides your organisation with an ever-growing selection of tools and services which let staff communicate and collaborate regardless of location or the device they use. This freedom boosts productivity yet it also introduces new risks to your data, intellectual property and privacy.

In this eBook we explore Microsoft 365's 'Secure Score'. This is a feature of the platform that helps you focus on critical security tasks by assigning a 'score' to your current settings and identifies ways to improve your protection level.

The Challenge of Microsoft 365 Security

How will you keep your Microsoft 365 tenant secure? This is a deceptively simple-sounding question – and providing a neat, clear-cut answer is far from easy.

The cloud represents many opportunities for businesses – more ways to communicate, the ability to collaborate from anywhere and new styles of working. However, while Microsoft invests over $1 billion dollars per year in keeping its platform safe, the cloud continues to pose a risk to business data and identities.

Broadly speaking, the cloud is much more secure than the kinds of defences that businesses could implement on their own platforms. Nevertheless, achieving security in the cloud requires new skills, strategies and mindsets. And this learning curve is critical - one recent survey found that almost a third of security professionals worry that the level of cloud security expertise at their organisations is either ‘novice’ or ‘not very competent’.

When it comes to Microsoft 365, all organisations that open a tenant receive an ‘out-of-the-box’ level of security to begin with. These generic settings then need to be adapted to address your organisation’s risk posture – an approach that is acceptable for one organisation may feel highly risky to another and unnecessarily restrictive to a third.

If your organisation is planning to move to Microsoft 365 or has already moved but has not yet refined its security status, this eBook aims to help. You will learn how to leverage the Microsoft ‘Secure Score’ – a feature of the platform which assesses your current level of security, and identify the things you can do to improve it.

What’s Your Appetite for Risk?

Different organisations have different tolerance to risk when it comes to Intellectual Property and personal data. Recognising this, Microsoft allows companies to configure their tenants to be as restricted or open as they wish. That said, most businesses will want to take a medium to high-risk approach to their security - especially in the era of GDPR where breaches of customer data could result in enormous fines and/or reputational damage.

With Microsoft 365 you have the option of ‘locking down’ your environment – only allowing people to view documents and folders after passing multiple layers of security and restricting what they can do on the tenant. However, this hyper-secure approach negates many of the benefits of the cloud – such as the ability to view documents on a personal device while on the go or to create a simple collaboration platform with partner organisations.

Finding the right balance is about weighing up risk vs functionality, adaptation, understanding business needs and end user experience.

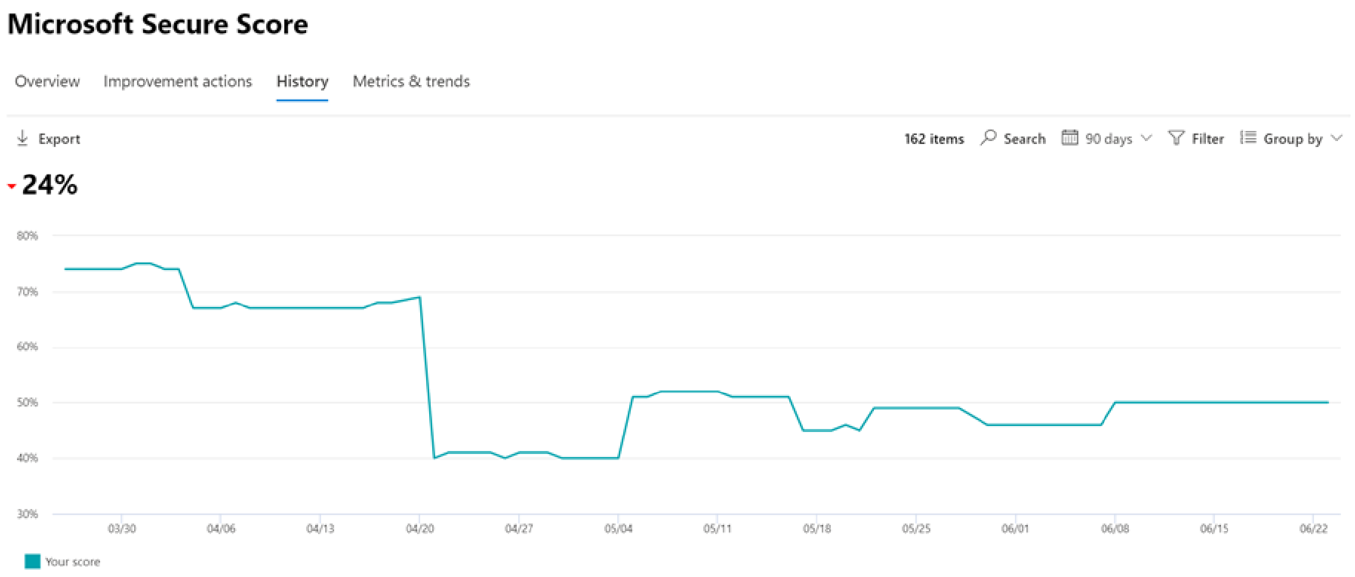
Secure Score—a convenient way of assessing your protection level

Imagine you are at a board meeting. Your CEO has just congratulated you on the migration to Microsoft 365, but is now asking about how secure the platform really is – she has heard that companies can still have data breaches in the cloud.

In the on-premises IT model, you might have told her about the security protocols you were enforcing or your firewall's status. Unfortunately, security is very different in the cloud. The kinds of threats you are facing are new, and you do not effectively have control over a firewall since your data and applications are in the cloud.

And this is where Secure Score is helpful. You could use the score to demonstrate to the CEO exactly which actions have been taken, how your score is improving, and even show how you are doing compared to your company's peers. By presenting an historical view of your score over time, you can demonstrate continual improvement and a pro-active approach to Microsoft 365 security.

Track your Secure Score over time



Microsoft Secure Score

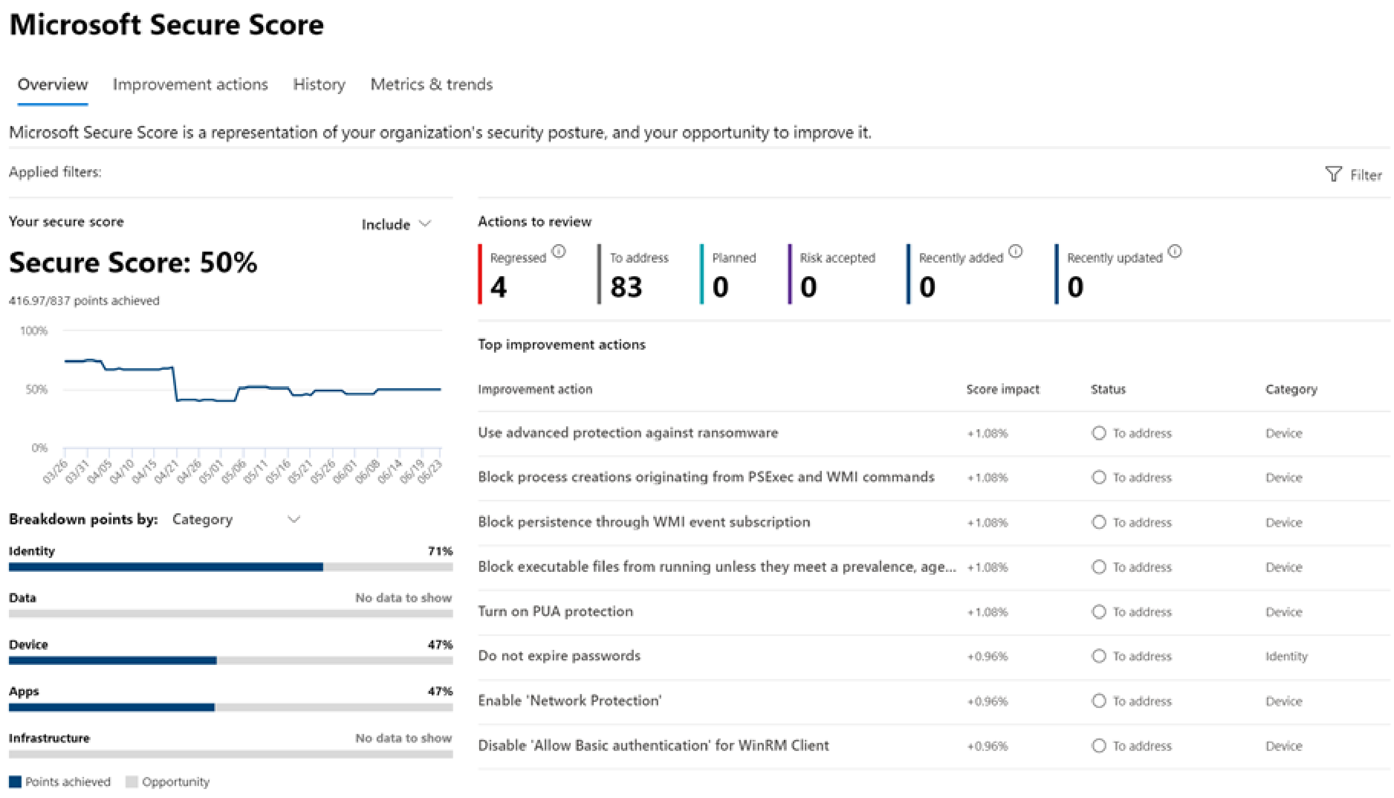
162 items

90 days

24%

What is Microsoft Secure Score?

Secure Score overview chart example



Microsoft Secure Score

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Applied filters:

Your secure score

Secure Score: 50%

416.97/837 points achieved

Breakdown points by: Category

Identity	71%
Data	No data to show
Device	47%
Apps	47%
Infrastructure	No data to show

■ Points achieved □ Opportunity

Actions to review

Regressed	To address	Planned	Risk accepted	Recently added	Recently updated
4	83	0	0	0	0

Top improvement actions

Improvement action	Score impact	Status	Category
Use advanced protection against ransomware	+1.08%	○ To address	Device
Block process creations originating from PSExec and WMI commands	+1.08%	○ To address	Device
Block persistence through WMI event subscription	+1.08%	○ To address	Device
Block executable files from running unless they meet a prevalence, age...	+1.08%	○ To address	Device
Turn on PUA protection	+1.08%	○ To address	Device
Do not expire passwords	+0.96%	○ To address	Identity
Enable 'Network Protection'	+0.96%	○ To address	Device
Disable 'Allow Basic authentication' for WinRM Client	+0.96%	○ To address	Device

Secure Score is a measurement of your company's security posture – the higher the score, the more security actions you have taken. Microsoft provides an extensive list of recommendations that any company can implement to improve their score and make their tenant safer. It can be viewed by logging into the admin dashboard in Microsoft 365's security centre.

Secure Score covers various areas of the Microsoft 365 and Azure suites which help administrators control security aspects of their environment, and includes:

- **Identity management**
- **Devices (smartphones, laptops, printers etc.)**
- **Document and email control**
- **Analytics (identifying breaches and suspicious activity)**

Because Microsoft provides so many security tools and settings it can be overwhelming to know where to begin. Secure Score is designed to simplify the task of managing the many variables related to IT security in the cloud by providing a straightforward list of tasks to action.

How does Secure Score help you?

There are several benefits to using Secure Score as part of your Microsoft 365 governance strategy:

- **Improves overall security**

  Secure Score's rating system improves organisations efforts to manage data and protect the privacy of customers and employees.

- **Informs your strategy**

  Microsoft 365 provides an almost unlimited number of variations when it comes to configuring your security posture. This can be confusing, so Secure Score helps identify the ones which are most relevant to your strategy so you can prioritise them.

- **Compare your score with peers**

  Secure Score lets you compare your security posture against industry peers. Microsoft 365 is used by hundreds of thousands of businesses—meaning Microsoft can use anonymised data to tell you how your posture compares to companies of a similar size and industry.

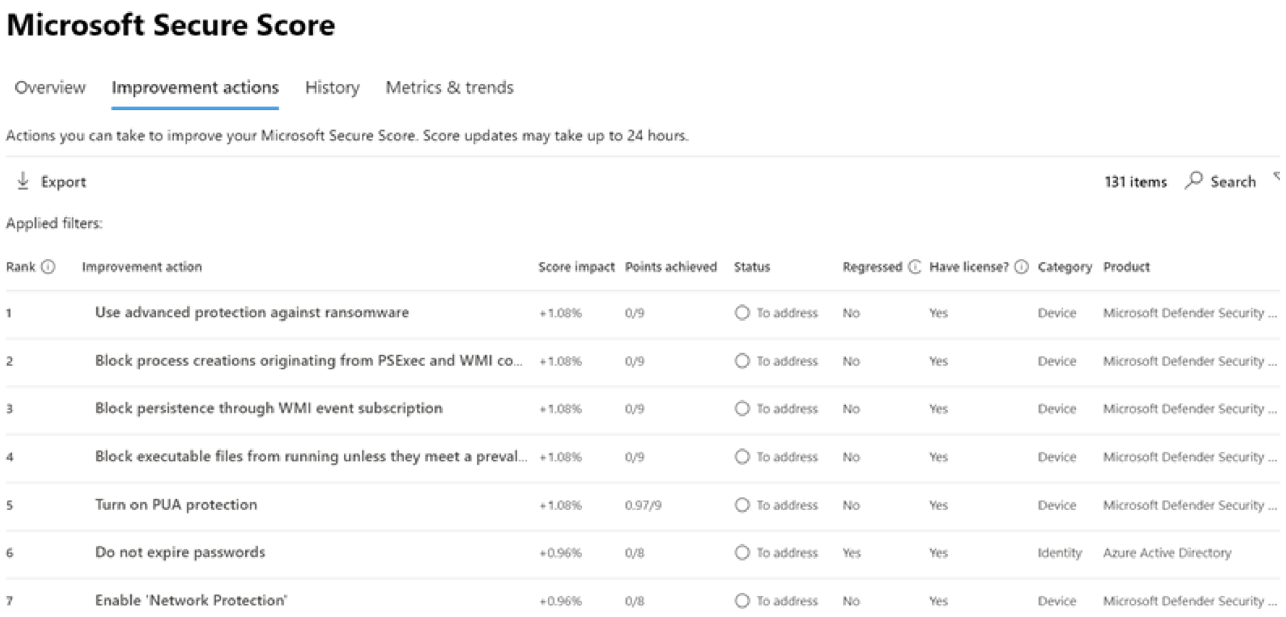
- **A metric everyone can understand**

  From your CEO to external auditors to end users, Secure Score provides an easy-to-understand metric for security. This communicates your current stance and helps non-technical users under stand why you are making changes. It also provides an auditable 'log' of actions taken.

- **Demonstrate improvement**

  Your Secure Score can be tracked over time to inform stakeholders of the continual improvement of your security improvement strategy.

Example of improvement actions



Microsoft Secure Score

Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

Applied filters:

Rank	Improvement action	Score impact	Points achieved	Status	Regressed	Have license?	Category	Product
1	Use advanced protection against ransomware	+1.08%	0/9	○ To address	No	Yes	Device	Microsoft Defender Security ...
2	Block process creations originating from PSExec and WMI co...	+1.08%	0/9	○ To address	No	Yes	Device	Microsoft Defender Security ...
3	Block persistence through WMI event subscription	+1.08%	0/9	○ To address	No	Yes	Device	Microsoft Defender Security ...
4	Block executable files from running unless they meet a preval...	+1.08%	0/9	○ To address	No	Yes	Device	Microsoft Defender Security ...
5	Turn on PUA protection	+1.08%	0.97/9	○ To address	No	Yes	Device	Microsoft Defender Security ...
6	Do not expire passwords	+0.96%	0/8	○ To address	Yes	Yes	Identity	Azure Active Directory
7	Enable 'Network Protection'	+0.96%	0/8	○ To address	No	Yes	Device	Microsoft Defender Security ...

How should you use the Secure Score?

Because Microsoft provides a series of simple instructions on how to improve your score, it is tempting to use the tool as a 'box ticking' exercise. However, this misses the point!

Instead, administrators, business users and the leadership team need to develop a strategy to make best use of the tool. At FITTS, we recommend you start by:

- **Gaining a picture of how your organisation works**

  How do you manage user identity? Do you know how employees use data held in the cloud? Are they accessing content on personal smartphones? Where do they do it, and what for? To begin using Secure Score, you first need an accurate view of how your organisation uses its information - this then informs your security strategy.

- **Assessing your risks**

  Use internal and publicly available data to assess the threat level to organisations of your type. Secure Score also tells you how other organisations in your sector are protecting themselves.

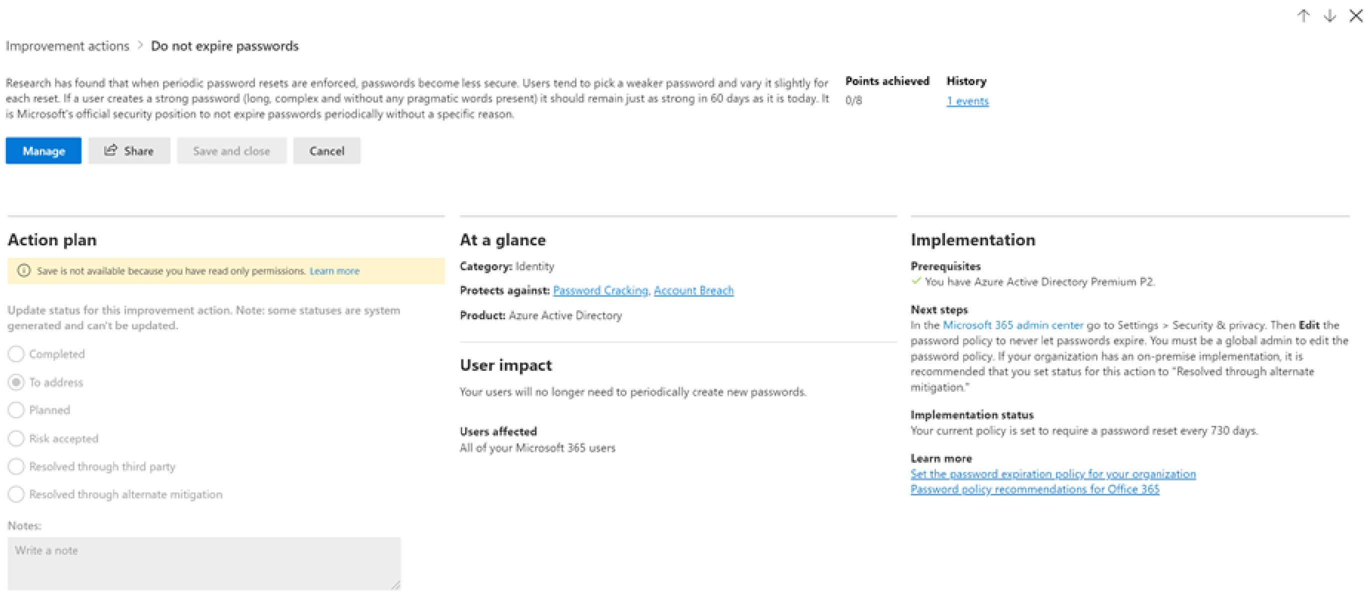
- **Defining limits and setting a strategy**

  Next, you will need to define what kinds of security limits you are comfortable with and prioritise the configurations that apply to your business. For example, a company whose salespeople often travel will need to permit remote access on mobile, but if none of your teams need content out side the business, this can be switched off.

- **Configuring your security settings**

  You are now in a position to use the Secure Score to begin changing settings in Microsoft 365 or Azure Active Directory in line with your strategy.

Simple 'action plan' on how to improve



Improvement actions > Do not expire passwords

Research has found that when periodic password resets are enforced, passwords become less secure. Users tend to pick a weaker password and vary it slightly for each reset. If a user creates a strong password (long, complex and without any pragmatic words present) it should remain just as strong in 60 days as it is today. It is Microsoft's official security position to not expire passwords periodically without a specific reason.

Points achieved
0/8

History
1 events

Action plan

Save is not available because you have read only permissions. Learn more

Update status for this improvement action. Note: some statuses are system generated and can't be updated.

○ Completed
● To address
○ Planned
○ Risk accepted
○ Resolved through third party
○ Resolved through alternate mitigation

Notes:
Write a note

At a glance

Category: Identity

Protects against: Password Cracking, Account Breach

Product: Azure Active Directory

User impact

Your users will no longer need to periodically create new passwords.

Users affected
All of your Microsoft 365 users

Implementation

Prerequisites
✓ You have Azure Active Directory Premium P2.

Next steps
In the Microsoft 365 admin center go to Settings > Security & privacy. Then **Edit** the password policy to never let passwords expire. You must be a global admin to edit the password policy. If your organization has an on-premise implementation, it is recommended that you set status for this action to "Resolved through alternate mitigation."

Implementation status
Your current policy is set to require a password reset every 730 days.

Learn more
Set the password expiration policy for your organization
Password policy recommendations for Office 365

Identity: a quick win for Secure Score at any organisation

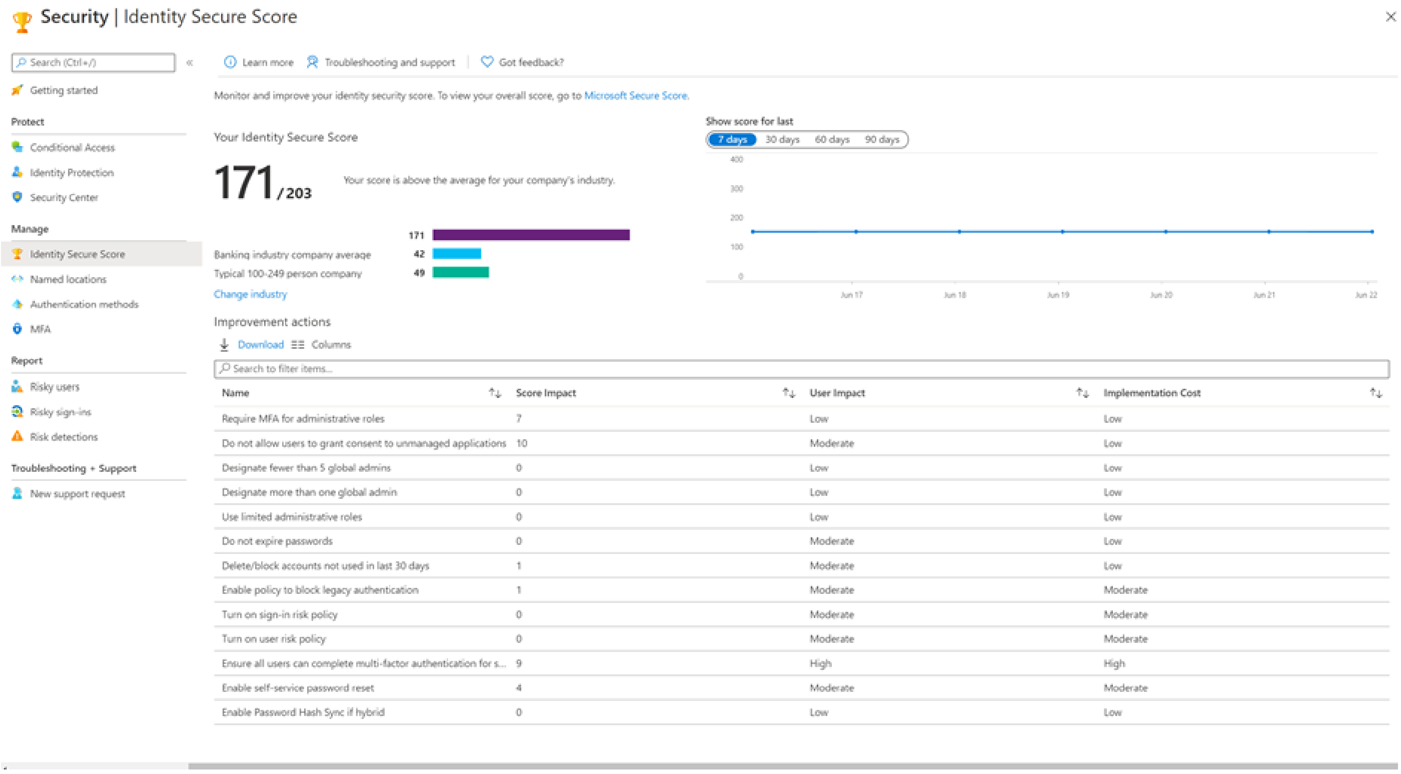
Every organisation is different and will have unique requirements with regards to security. That said, a great place to start for any business is identity management – this is perhaps the area which is most targeted by cybercrime and the quickest way to boost your defences

Configuring a robust Identity strategy can be a challenge. Typically, organisations work with employees, partners, consultants, vendors and a number of other identities which may need access to company resources. A zero-trust model must be considered since, as an organisation, you may not have full visibility of the individuals accessing your environment. However, there are some fundamental improvements you can make in any situation:

- Multifactor authentication should be turned on for all users
- Minimise the number of administrators
- Ensure user identities match up with Active Directory
- Monitor Leavers of the organisation and remove user accounts
- Review 3rd party access and regularly enforce strict password protocols

Any organisation that introduces these identity 'quick wins' will immediately outperform their peers when it comes to security.

Identity Secure Score example view



Monitor and improve your identity security score. To view your overall score, go to Microsoft Secure Score.

Your Identity Secure Score

171 / 203

Your score is above the average for your company's industry.

	171
Banking industry company average	42
Typical 100-249 person company	49

Improvement actions

Name	Score Impact	User Impact	Implementation Cost
Require MFA for administrative roles	7	Low	Low
Do not allow users to grant consent to unmanaged applications	10	Moderate	Low
Designate fewer than 5 global admins	0	Low	Low
Designate more than one global admin	0	Low	Low
Use limited administrative roles	0	Low	Low
Do not expire passwords	0	Moderate	Low
Delete/block accounts not used in last 30 days	1	Moderate	Low
Enable policy to block legacy authentication	1	Moderate	Moderate
Turn on sign-in risk policy	0	Moderate	Moderate
Turn on user risk policy	0	Moderate	Moderate
Ensure all users can complete multi-factor authentication for s...	9	High	High
Enable self-service password reset	4	Moderate	Moderate
Enable Password Hash Sync if hybrid	0	Low	Low

CASE STUDY

How Secure Score helped one engineering firm level up

Since 2018, FITTS has been working with a multinational renewable energy business. The firm had already migrated to Microsoft 365 but had left the security settings that come 'out of the box' with any Microsoft 365 deployment.

Unfortunately, the company had experienced a data breach – sensitive documents had been sent outside of the organisation by email. The firm knew that their security posture needed to be 'beefed up' but were unsure where to begin.

The very first thing FITTS' team did was to check the company's Secure Score. As suspected, this was at 'rock bottom' – indeed their score was at -1. To remediate this problem, our project team:

- Conducted interviews and focus groups to understand the company's needs and activities
- Assessed their security risk
- Identified 'low hanging fruit' which immediately enhanced security
- From the interviews and planning stage, we knew the company had specific security requirements - such as a security classification convention for all documents and a method for managing content on users' devices.
- These measures were rolled out using a communications plan which got end users 'on board' with the change

As a result of the project:

- In less than 4 months, the firm's Secure Score reached 97 – a huge improvement from a starting point of -1
- Security is now configured to their specific needs, risks and activities
- Their score is significantly higher than the average for their sector
- User acceptance of multi factor authentication is high
- End users now have a better understanding of risk

More than a boxing ticking exercise

In this eBook, we have seen how Microsoft's Secure Score is a valuable tool for helping organisations improve their security posture. With Microsoft 365 and Azure Active Directory, Microsoft has given its customers a huge variety of settings which let customers configure the platform to their needs.

However, the Secure Score should not be thought of as a 'box ticking' exercise. It is perfectly possible to improve a business's Secure Score yet remain exposed to major threats. It is a valuable starting point, but building on Secure Score to truly protect your business assets requires a tailor-made plan which fits security around your needs.

FITTS helps large and medium-sized businesses to improve their security posture in Microsoft 365 and we use the Secure Score as a key benchmark in all our engagements. Because every business is unique, we first get to know you before configuring security to ensure that it meets your specific needs and context.

To help you understand your current security posture, FITTS is offering a free, no-obligation Microsoft 365 security assessment using Secure Score.

Book your assessment here, or contact us today

THE AUTHOR

Steve Barker

Steve Barker has been working in the IT industry for over 20 years and over that time has developed a unique balance of understanding business challenges and solution architecture. Trusted as an innovator in the Microsoft cloud technology field, Steve has a proven track record in helping business understand complex and challenging scenarios and generating value from technical innovation.

ABOUT FITTS

We're more than just a run-of-the-mill IT consultancy or digital transformer. We combine powerful technology with tailor-made service to deliver game-changing results. For each and every client, we'll rigorously assess and analyse entire operational systems to deliver the best possible solution, with cross-sector knowledge and niche expertise. It's why we've been recognized as a Microsoft Gold partner.

To learn more about FITTS visit: fitts.io

http://fitts.io | hello@fitts.io | +44(0) 203 855 0750