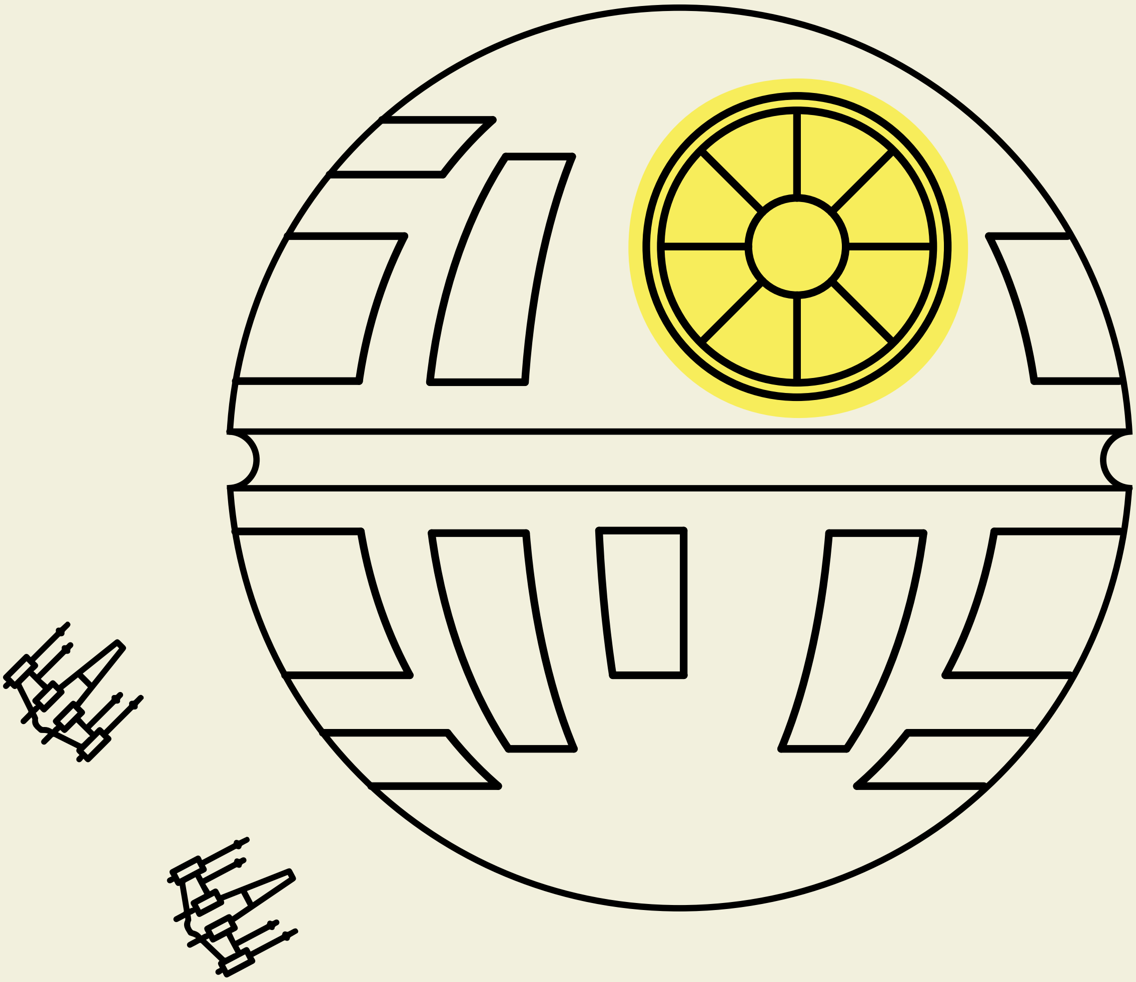
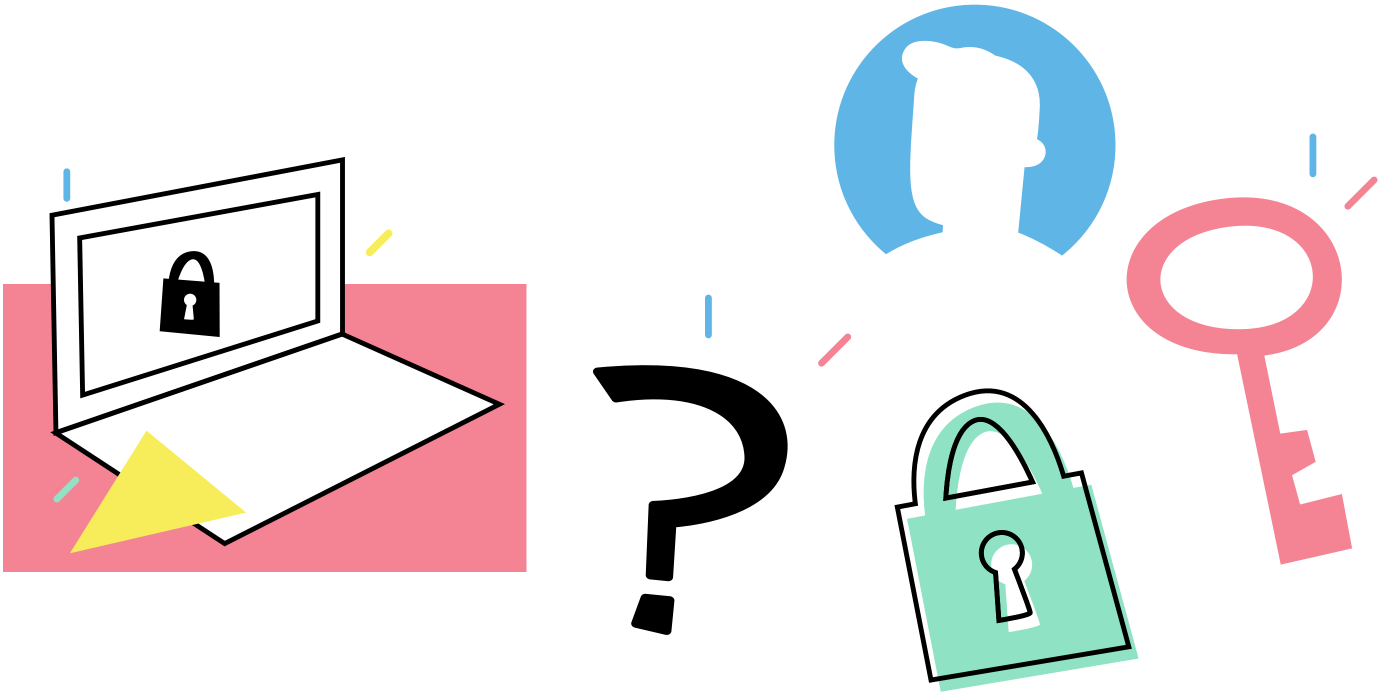
How to avoid the fate of the Death Star

The Azured Guide to Identity and Access Management



The Azured Guide to Identity and Access Management



Remember the days when every prince in Nigeria was giving away his inheritance? While these scams might seem painfully obvious, there's a reason why they've become so prolific. Every now and again, someone will take the bait.

The same logic applies to IT security. It only takes one ill-advised click to bring down an entire operation and with 83 per cent of breached businesses subject to phishing attacks, the odds are rarely in your favour. In fact, the cybercrime business has never been more profitable. Nefarious actors can even access Ransomware as a Service and vanish into the murky depths of the dark web before you've had the chance to switch on the lights.

But enough of the scaremongering. You came here looking for solutions. And that's exactly what cloud Identity and Access Management (IAM) can offer. The real trick is knowing how, and where, to implement it.

If you're already using Azure and you don't have insight into vulnerabilities across your entire stack, then now's the time to seek them out. Don't go the way of the Death Star. Use our handy guide to identify your weak points and give your Microsoft Secure Score a much-needed boost.

It only takes one ill-advised click to bring down an entire operation.

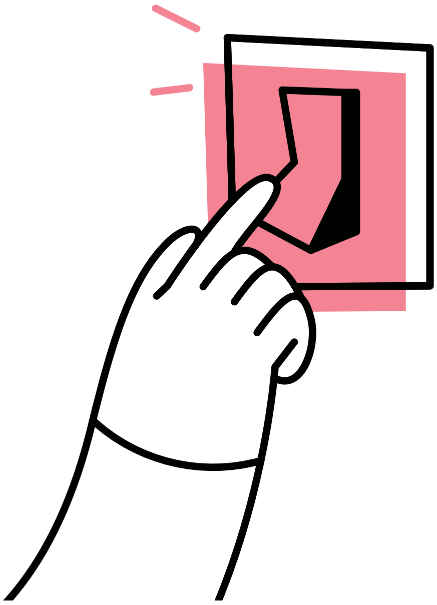
What on earth is Microsoft Secure Score?

If you're asking this question, then the chances are you need it. Microsoft Secure Score allows you to measure the strength of your Azure security, tighten any areas that need tightening, and track your progress across your entire cloud environment. Your overall Secure Score is calculated by tallying up the performance scores of several different products in the Microsoft Suite. A crucial subset of these markers is Identity Secure Score performance, which is the focus of this paper.

This free tool from Microsoft will also give you suggestions for improving your score, and you can then choose which of Microsoft's recommendations you want to follow to make improvements. Not every recommendation will work for your environment; there will always be a trade-off between security and usability. It's no good having the most secure laptop in the world if you can't actually use it. It just depends how much risk you're willing to accept.

Here are a few ways you can beef up your defence without sacrificing that sweet, sweet user experience.

> There will always be a trade-off between security and usability.

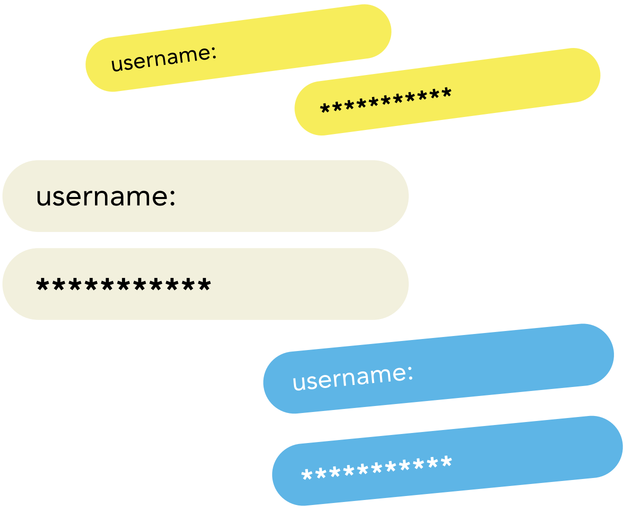


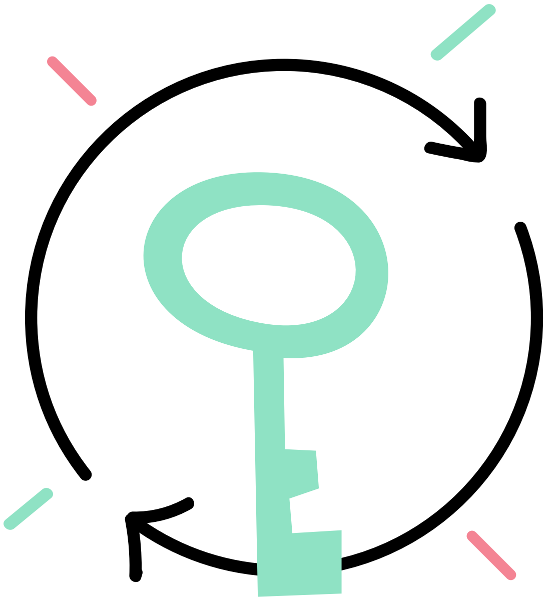
Turn on Multi-Factor Authentication

Relying on passwords alone is like storing your life savings under your mattress. For example, 34 per cent of employees admit to sharing their passwords with co-workers.

In the age of the cloud, Multi-Factor Authentication (MFA) is the big, angry Doberman behind the rusty perimeter fence. Every time an employee logs into an application from a new location or device, they'll be asked to confirm their identity using something personal to them, like their phone or thumbprint.

Setting up these defences throughout your organisation is the crucial bit. You need to know that every user is jumping through the right hoops at the right time. In Azure Active Directory, you can do this using Conditional Access policies, which you can make as granular and specific as you like. For example, you might want to trigger the MFA process every time a member of your finance team requests access to an invoice or purchase order. This way, you'll know that anyone who compromises their credentials will gain nothing more valuable than their favourite pet's name.





Switch to Single Sign-On

How many of your employees use the same password for multiple work accounts (let alone their personal accounts)? Well, if they're anything like the average Joe, then it's probable that more than half are guilty of this crime. But before you send them all an angry memo, think about why this is happening.

A typical business now deploys around 130 apps – which means a whole heap of numbers, letters and special characters to conjure up on command. Couple this with the regularity at which these apps come and go and you can start to sympathise a little more.

Fortunately, there's now a way to escape this alphabet soup. With Single Sign-On (SSO), users can access multiple applications with a single set of credentials. While this might sound like a riskier approach, when configured properly, SSO can lead to quicker and more secure software provisioning.

Federated authentication, for example, allows you to authenticate an SSO request using tokens sent between your on-premise Active Directory (if you have one), Azure Active Directory, and an end user's browser. As long as these have been set up correctly, you can even send the tokens via different protocols (e.g. OpenID Connect and OAuth).

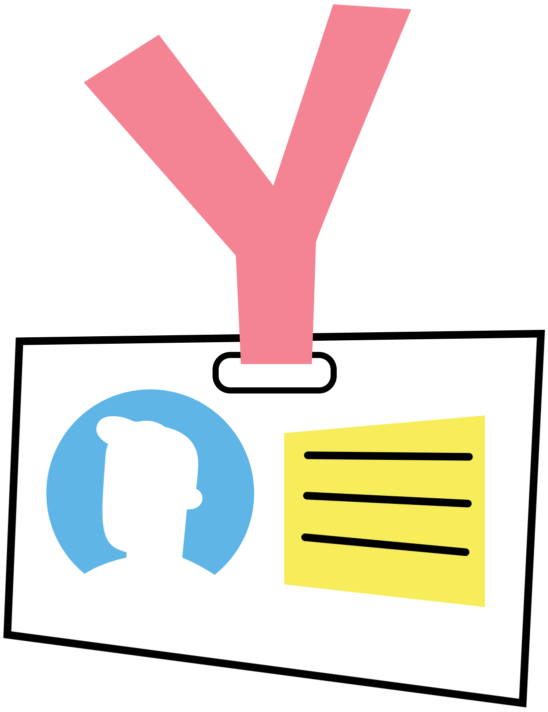
> With Single Sign-On, users can access multiple applications with a single set of credentials.

Consider Self-Service Password Reset

Ever locked yourself out of your car? Embarrassing, isn't it? You probably remember sitting in the cold, waiting for the locksmith to arrive and wondering where it all went so wrong. Well, for many employees, that's how it feels each time they forget their password. In fact, 60 per cent of them say they've been unable to work due to password-related issues.

It's a real headache for your technical team, too. According to Gartner, 20-50 per cent of helpdesk calls are for simple password resets. That's a lot of time and money spent on the same repetitive task. Imagine if you had that left over in your budget at the end of each month; you might finally be able to upgrade that wheezy Linux server.

It's for exactly this reason that Self-Service Password Reset (SSPR) exists. Built into Azure Active Directory, the technology makes it possible for users to reset both expired and non-expired passwords without the need to contact an administrator or helpdesk. While 'DIY IT' can often end in a sticky mess, SSPR uses several measures (like MFA) to ensure the process is secure. Typically, 95 per cent of password change requests are mitigated by using SSPR.



Roll out Privileged ID Management

With the average employee now able to access more than 10.8 million shared files, it's no wonder firms are looking for ways to limit unauthorised activity. But you can't give what you don't have and that's exactly why the principle of least privilege is so prevalent in modern cloud computing.

But it's not quite as simple as setting a blanket, catch-all policy. Employees want access to different resources at different times, and it's hard to know who legitimately needs their hand in the cookie jar. What's 'tight-fitting' to one person is restrictive to another and potentially a straitjacket to your business as a whole.

Privileged Identity Management (PIM) helps to reduce the risk of unauthorised access, without compromising on flexibility and autonomy. Employees get access to sensitive documents for just long enough to complete their task before that privilege is revoked.

Only the Privileged Role Administrator and the Global Administrator have overall control of these assignments, so you never end up in a situation where non-privileged users have continuous access to a protected resource.

> Rather than blocking access at every turn, consider where you can introduce self-remediation options.

Make the most of Identity Protection

Striking the right balance between fluid user experience and robust security might feel like an eternal struggle. But you don't have to be a Shaolin monk to maintain a strong and durable posture. Rather than blocking access at every turn, consider where you can introduce self-remediation options.

Maybe you can relax your user risk policy by setting up Self-Service Password Resets. Or streamline sign-ins by triggering Multi-Factor Authentication. At the end of the day, it's up to you what level of risk you're willing to accept. But it certainly doesn't need to be uncalculated.

While rising threats such as password sprays are often difficult to spot, automating the detection of these identity-based attacks makes it possible to mitigate them at the first attempt. Each day, Microsoft uses machine learning to analyse 6.5 trillion signals to identify and protect you from potential threats. And you can monitor them all in Azure Identity Protection.

By feeding the data from Identity Protection into other Identity and Access Management tools – such as Conditional Access – you can make more informed policy decisions and determine the risk level associated with each unfamiliar action.

To err is human

Social Engineering. We're going to hearing this term a lot in 2022 (almost as much as "you're on mute"). And those companies that understand that all cyberattacks have a social engineering element, and how to mitigate this, will be the ones that are more likely to stay one step ahead of hackers.

So, what exactly is social engineering?
It's the means by which hackers get access to your network, services, identity platform, apps, infrastructure (the list goes on...) by manipulating the single most variable and therefore most vulnerable asset in your organisation... your people.

Even phishing attacks are a form of social engineering. Their success or failure depends on whether Geoff in Accounts clicks on that link in the email that ostensibly looks as if it's come from Janet in Sales.

Social engineering methods include everything from paying or persuading your staff to plug a USB key into your system to swiping a staff member's pass card and physically installing hardware, or watching over a remote-worker's shoulder and noting their password as they happily tap away in the local Costa.

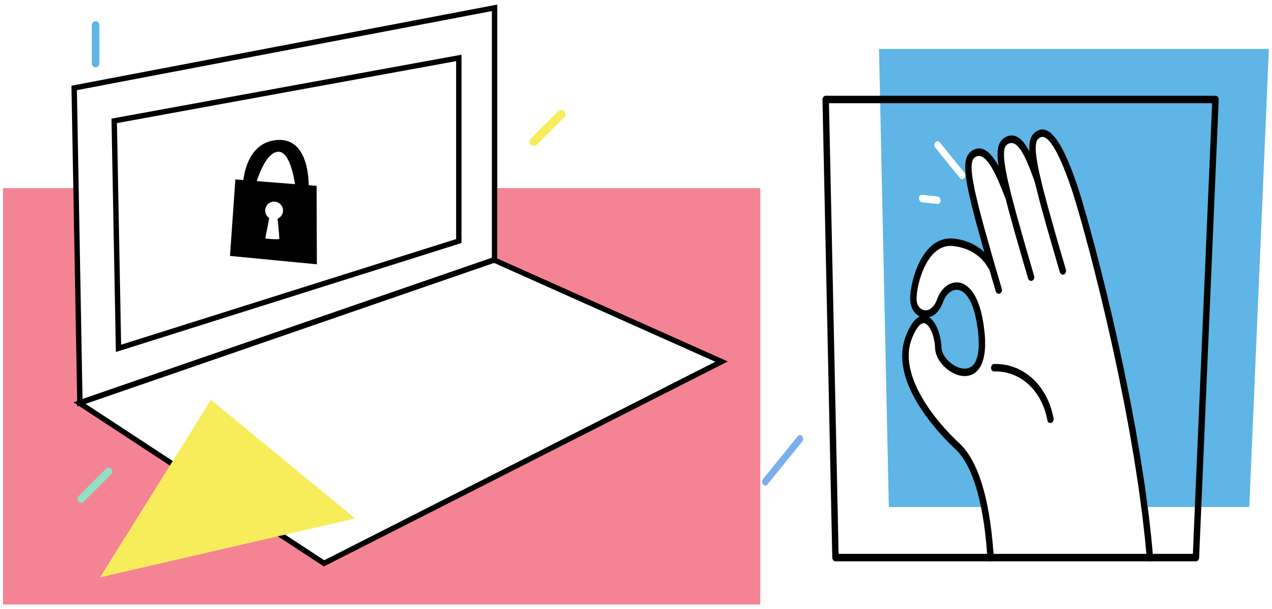
In a recent survey 48 per cent of employees in just one organisation who found a (planted) USB from an unknown source on their desk, plugged it into their device – no questions asked.

Once a nefarious actor has access to your infrastructure they're home and dry, in fact you probably won't know they're there until the damage is done.

The only way of dealing with social engineering-led attacks is to prevent them in the first place, by educating your staff and ensuring they know what to do if they suspect something.

The first few hours after an attack are absolutely critical to the recovery of your business. While ensuring you've got the right technology in place is the larger part of being adequately protected, you also need to underpin this with a cyber security action plan and staff training, giving your staff a step by step guide to what they should do in the event of an attack.

> Once a nefarious actor has access to your infrastructure, they're home and dry.



Keep it secret, keep it safe

The sad truth is that more than 60 per cent of businesses go bust after experiencing a data breach. It's simply not enough to stand up a firewall and pray for good weather – especially when the traditional IT perimeter has evaporated under the bright sun of remote working and cloud-hosted apps. Even when you think you've prevented a threat, it can already be too late.

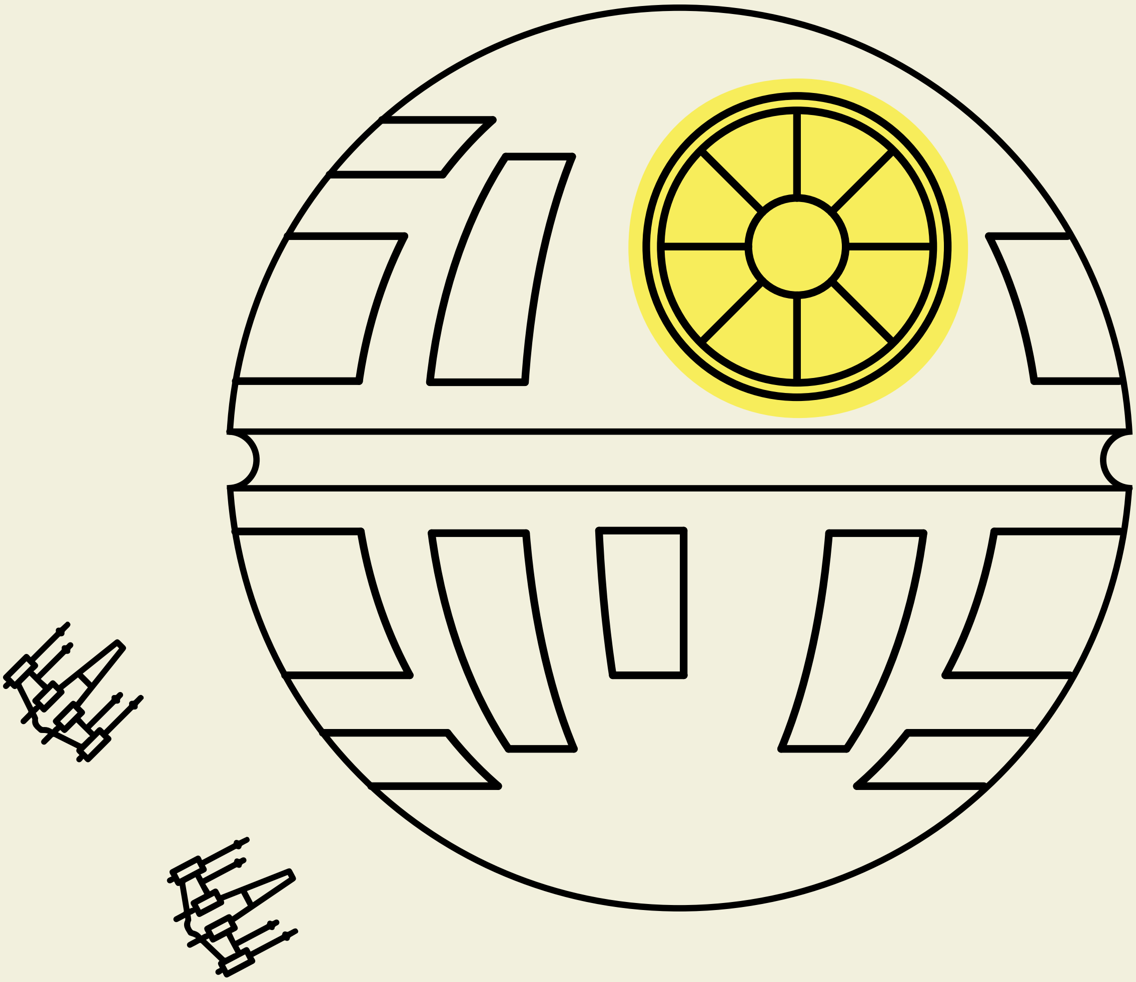
Hackers aren't afraid to play the long game. In fact, the majority will wait weeks or even months to launch an attack, with many looking for opportune moments such as employee away days or board meetings to make their move.

For this reason, the right cloud IAM infrastructure can make or break your security and compliance strategy. Don't let complacency kill your drive. Get tested – and if your Microsoft Secure Score is lower than expected, call in the experts to ensure that extra level of protection.

In conclusion, if you only take away these five points to action, we'll be happy chappies (and chappesses):

1. Employ the right technology to assist with prevention and detection
2. Create a cybersecurity action plan
3. Invest in training for staff
4. Get yourself some cyber insurance
5. If in doubt, call in the specialists

For more information on Identity and Access Management **book a call** with one of our friendly cloud security wizards.



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