Remediate by nccgroup

An NCC Group Publication

The most common blockers to avoid when entering transformation projects with a hybrid estate

Lloyd Brough, Technical Associate Director at NCC Group

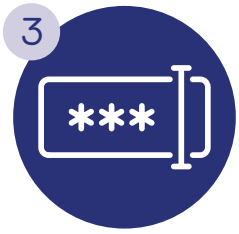
Hybrid estates are going to be here for a while, and there are some really good reasons to maintain your own estate whilst adopting cloud services. However, the move to hybrid has shifted the perimeter and the front-line of cyber defences has moved.

If you're using On-Prem directories to store computers, identities, groups and other items, integrating those directories with Azure provides a common identity for accessing both cloud and On-Prem resources. Admins can use conditional access based on application resource, device and user identity, network location and multi-factor authentication (MFA). However, we are still seeing some issues that could be avoided.

The top three issues that our Security Improvement & Remediation Team has observed after an incident response or proactive security review are as follows:

Insecure cloud configuration

Legacy perimeters



Password quality problems

Insecure cloud configuration

The importance of maintaining a secure external perimeter and securing the blurred lines between cloud surface and On-Prem is key. It seems too obvious to mention, but it is critical that all externally facing services for corporate services; whether they are cloud or On-Prem, are protected by MFA.

With that in mind, here are four key steps to secure cloud configuration:

- **Set up and mandate MFA** across the board for all users who require remote access. Ensure that all users have completed this process in a timely manner: in certain situations, attackers can exploit users with a poor or breached password to set up MFA themselves.

  Be aware that sometimes conditional access may prevent MFA setup from occurring e.g. if a user always uses a Virtual Private Network to enter into the corporate network. During the migration process it may be useful to consider changing conditional access to force MFA for all criteria.

- **Turn off legacy authentication** for all domains. Legacy email protocols do not support MFA, making it possible for attackers to easily bypass MFA using these legacy applications: 99% of credential password sprays use legacy protocols. Critically, a phishing attack from internal 'trusted' users is much more likely to succeed.

  Often, we hear concerns about a board member's old iPad or something similar, so turn audit mode on first to find out if there are any users actively using legacy authentication.

- **Set up and use conditional access** to ensure that MFA is mandated for circumstances which require it based on your policy. The modern security perimeter now extends beyond an organisation's network to include user access and devices, so this approach will ensure that they can only be accessed by devices that meet your standards for security and compliance.

- **Audit and review On-Prem LAN security:** once modern cloud implementations are in place, it is often the case that 'legacy' aspects are neglected. This is true of external facing services and also internal networks; where examples such as relatively open network shares become an unused treasure trove for attackers.

Legacy perimeters

IT teams rarely have total clarity about the state of their estate due to the changes that organisations typically undergo throughout their lifetime. These include transformation projects, mergers and acquisitions, growth spurts and difficult times where people had to develop workarounds to ensure the organisation's survival. Amid all of this activity, legacy applications and systems often get left behind without being decommissioned properly.

However, these legacy systems affect the perimeter of your IT estate: threat actors monitor outdated products for vulnerabilities that can be exploited to gain access to your network, so it's important that you action the three steps below as a minimum to prevent legacy items from delaying transformation projects.

Segment your network

by isolating legacy systems from the internet and your other systems internally, using MFA, firewalls and other tactics to prevent threat actors from using them as a jumping off point to your network. If you can decommission legacy items, this should be actioned as soon as possible.

Patch properly

by creating a clear list of your assets and their current status, and ensuring that they are kept up to date with the latest patches. This will enable you to identify when a legacy system becomes outdated and isolate it properly.

Assess and address supplier risk:

we've seen multiple attacks where threat actors have compromised legacy systems in a supplier to infiltrate that organisation's customers, so conduct due diligence and ensure that your third-parties are adhering to the same security standards as you.

Password quality problems

Successful corporate password and identity access management (IAM) requires a layered approach to secure the many facets that comprise an enterprise environment and the same is true for cloud services. MFA aspects should be considered an extra layer in this layered approach.

Again, there are five actions that organisations can take here:

- **Implement fine-grained password policies** to ensure administrative accounts are subject to more stringent password complexity and account lockout policies. In Active Directory, the domain functional level must be Windows Server 2008 or greater.
- **Use password blacklists** to block the use of common passwords such as 'Password1' and [MonthYear]. This can be implemented through third-party solutions or through Microsoft Azure's Active Directory Password Protection.
- **Harness managed service accounts or privileged access management** where possible, to enforce random and complex 100+ character passwords that are managed automatically by Active Directory or a third party tool. If this is not feasible, service accounts should use 25+ character passwords.
- **Enable MFA** on all internally sensitive systems and external facing portals, whether via text message or mobile application. Disable push notifications to prevent a user inadvertently approving a login request.
- **Separate administrative accounts** for all users who perform a privileged function, ideally performed from a privileged access workstation. The separate administrative account should not have email or internet access.

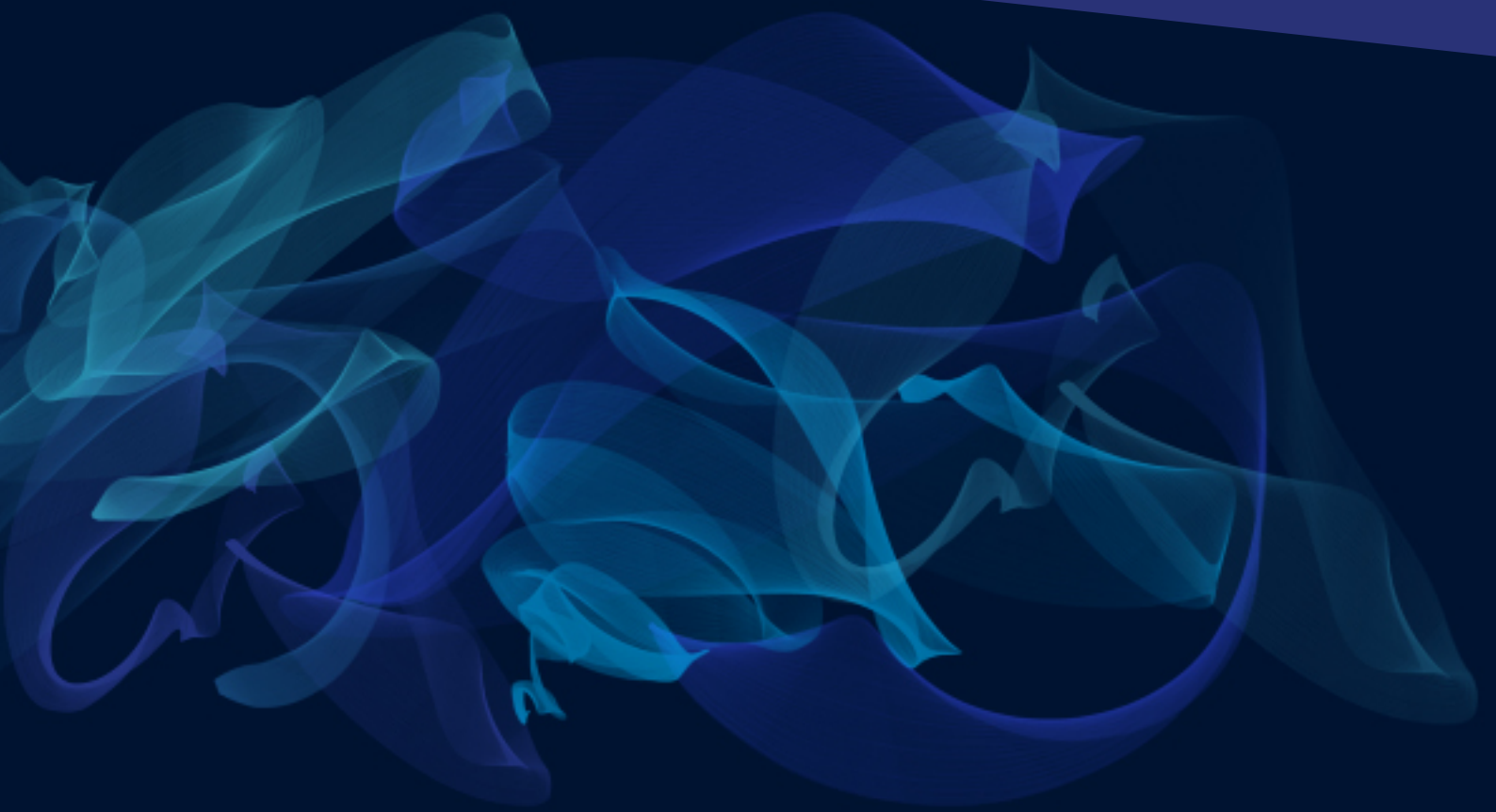
Innovate with confidence

As with all transformation projects, hybrid estates can present a number of cyber security pitfalls for organisations. However, by focusing on securing their cloud configuration, legacy perimeters and improving the IAM, MFA and quality of passwords across the business on an ongoing basis, organisations can innovate with confidence and reduce security risk in the short, medium and long-term.

To discuss how we can help you remove the blockers to digital transformation, speak to our team:

+44 (0)161 209 5111
response@nccgroup.com
www.nccgroup.com

Remediate by nccgroup



About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience and global footprint, it is best placed to help businesses assess, develop and manage the evolving cyber risks they face.

To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

+44 (0)161 209 5111
response@nccgroup.com
www.nccgroup.com