Quorum Cyber

Service Description Conditional Access G Cloud 15

+44 333 444 0041
quorumcyber.com
Verdant, 2 Redheughs Rigg, Edinburgh, United Kingdom, EH12 9DQ

Table of Contents

Service Overview 3
Background 3
Quorum Cyber's Solution 3
Differentiators 3
Service Features 4
Service Benefits 5

Service Overview

Background

Organisations often face challenges when using Conditional Access (CA) in complex, high-risk environments. Configured correctly CA can help us prevent unauthorised access to our valuable applications and data, providing an added layer of protection on top of authentication methods. Misconfigured or inconsistently applied policies can introduce security gaps, create unnecessary friction for users, or lead to over-use of broad exclusions that weaken Zero Trust objectives. Mistakes with policies can result in service disruption, user lockouts, or unintended access paths, particularly where legacy applications, multiple identity types, and operational constraints coexist. Over time, environments can suffer from policy sprawl, limited documentation, and configuration drift from best practice, making it difficult to understand intent, demonstrate compliance, or respond effectively to changes in threat landscape, regulation, or organisational need.

Quorum Cyber's Solution

Quorum Cyber provide professional services for CA no matter where you are in your implementation journey:

- New deployments: Quorum Cyber's Security Consultants assess your environment and challenges, design best-practice CA policies aligned to your security and compliance goals, and support their safe implementation by carefully evaluating user impact before deployment.
- Reviews: CA reviews provide the benefit of restoring clarity, effectiveness, and confidence in how controls are protecting an organisation. They identify gaps, misconfigurations, and exclusions that may expose sensitive systems or data, while also highlighting overly restrictive policies that negatively impact users and operations.
- Ongoing support: Quorum Cyber offer two ways of providing ongoing support for CA polices.
    - Our services team run quarterly reviews of your CA policies, providing recommendations for changes based on updated policy capabilities and changes to the threat environment.
    - Our separate Clarity Protect service provides SIEM services and configuration management of your Microsoft Defender environment, including Microsoft Entra CA polices. This can be useful for organisations with security teams who are already stretched for resources managing the environment, that having a trusted parter identify the most secure configuration and show you how to apply it across the Microsoft security stack becomes like an extension of your team.

Differentiators

- Our services combine specialist Microsoft CA skills with offensive security reviews to create a defence in depth offering, including testing for threats that your configuration may be susceptible to.
- Capabilities to design, build, deploy, and test your CA configuration.
- Managed services offering including CA policies where we define and show you how to configure in line with security best practice and evolving policy capabilities.
- We are a security services only company, and we see ourselves as your security partner to lift up your security capabilities.

Service Features

- Design, configure, and deploy new Microsoft Conditional Access policies.
- Review and make recommendations for existing Microsoft Conditional Access policies.
- Security test your Microsoft Conditional Access policy configuration from an external attacker and insider authenticated user perspective.
- Options for ongoing support and management.

Service Benefits

- **Reduced risk of unauthorised access** – Correctly designed and tested Conditional Access policies reduce the risk of account compromise and authorised access to sensitive applications and data.
- **Lower likelihood of service disruption and user lockouts** – Careful policy design, testing, and user impact assessment minimise the risk of outages and lockouts caused by misconfiguration.
- **Improved security without impacting the user experience** – Policies tuned to optimise security and usability.
- **Clear, defensible Zero Trust posture** – Rationalised and well documented polices reduce reliance on broad exclusions and help organisations demonstrate alignment to Zero Trust principles and security best practice.
- **Greater visibility and confidence in existing controls** – Reviews provide clarity around policy intent and effectiveness, allowing organisations to understand what is protecting them, where gaps exist, and what needs to change.
- **Improved audit and compliance readiness** – Reduced policy sprawl, clearer documentation, and alignment to best practice make it easier to provide evidence of the controls in place for regulatory compliance.