



Service Description Multi-factor Authentication 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 struggle with inconsistent or weak identity authentication controls, particularly across diverse user groups, device types, and access scenarios. Legacy MFA configurations like SMS, limited MFA adoption, and poor alignment between security requirements and user experience increase the risk of account compromise while creating friction for users and administrators.

Quorum Cyber's Solution

Quorum Cyber delivers a structured Entra ID Multi-Factor Authentication (MFA) engagement to strengthen identity security while maintaining usability.

Discovery

- Review of existing Entra ID MFA configuration, scope, and coverage
- Requirements gathering for all user types, including corporate users, BYOD users, non-smartphone users, temporary access scenarios, and privileged accounts
- Assessment of access conditions across device ownership and location combinations

Design

- Creation of a tailored MFA authentication model aligned to user groups and risk profiles
- Definition of supported authentication methods, prerequisites, and technical limitations
- Identification of security risks and operational considerations
- Development of a phased roadmap for MFA strengthening and adoption
- Support for internal documentation and governance requirements

Deployment

- Scoping and preparation for implementation based on the agreed design and roadmap
- Alignment of technical controls with Entra ID conditional access and authentication policies

Handover

- Delivery of clear design documentation and implementation scope
- Knowledge transfer to internal teams to support confident rollout and ongoing management

Differentiators

- Security-first design that balances strong authentication with real-world usability
- Deep expertise in Entra ID, conditional access, and modern authentication methods
- User-centric approach that accounts for complex access scenarios and edge cases
- Risk-driven authentication design rather than one-size-fits-all MFA
- Clear, actionable roadmaps that support phased adoption and maturity growth

Service Features

- Review and optimisation of existing Entra ID MFA configurations
- User group-based authentication modelling
- Addresses configuration for standard users, privileged, administrative, and break glass accounts
- Temporary access and exception handling considerations
- Risk and limitation analysis for authentication options
- High-level design documentation and implementation scoping

Service Benefits

- Stronger protection against credential theft and account compromise
- Reduced MFA fatigue and administrative overhead
- Clear visibility of authentication posture
- Faster, more confident deployment of modern identity security controls
- Alignment with Zero Trust and modern identity security best practices