Account Guard Advanced MFA

rocket IT

Credentials are targets

36% of data breaches involve phishing. One credentials are harvested they often go up for sale on the Dark Web. Unwanted account access is now a risk.

Humans make mistakes

90% of data breaches involve human error. Cyber criminals also continuously try to breach popular services to gain access to their credential vault.

Strong MFA is vital

It is vital to protect your business users against unauthorised access. Using either a smartphone app, txt message with the access code, or a voice call to authorise system access is paramount .

MFA addresses modern threats.

Using MFA as a 2nd requirement to access an application is like having a deadlock on your house.

Authentication using only a username and password is single-factor authentication.

MFA raises the bar for security by requiring a user to offer 2 out of 3 factors to verify their identity:

- Something you know
(e.g. username and password)

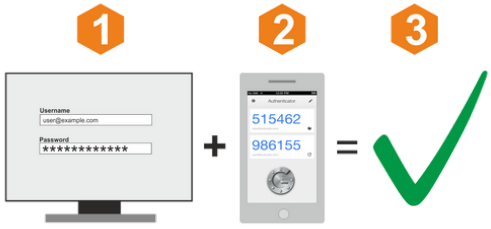
- Something you have
(e.g. A smartphone app software token)

- Something you are
e.g. biometric – fingerprint, facial recognition

The bar is simply too low with passwords. Even legacy MFA methods, such as SMS or mobile authentication, have all been proven to be highly vulnerable to phishing. MFA is the modern and effective approach to keeping your hard work, brand image, and business protected.

Benefits-at-a-glance

- Reduces fraud and identify theft
- No client software needed
- Minimises password recall
- Define access policies (i.e location based)
- Simple "Approve / Deny" process
- Reduces support costs
- Achieves compliance



Have a question? Let's chat...

Whether you're interested to learn more about key features, pricing or anything else, we're here to help.

Reach out to us today

Call: +64 0800 485 644

Email: security@rocketit.co.nz

Website: rocketit.co.nz

Service	Overview
Policy & Control	Enable your team to define and enforce rules on who can access what applications, under what conditions. Define access policies by user group and per application to increase security without compromising end-user experience.
Device Insights	Decentralization of device management and the rise of BYOD (Bring Your Own Device) can leave administrators wondering how users are accessing resources. The Device Insight dashboards show which OS platforms, devices, and browsers connect to your Duo protected applications and services. See at a glance how many systems have out of date or vulnerable software.
Endpoints	Review operating system, browser, and third-party plugin version information for end user devices accessing Advanced MFA. Enable self-remediation to notify users to update browsers and plugins. Prevent access to your protected applications from clients with outdated software. All without installing additional agents or monitors.
Trust Monitor	Surface and monitor anomalous authentication behavior. Create a custom risk profile to focus on applications, users, or locations that matter most. Examine detailed risk factors for events to determine which are actionable for your organization.

Why advanced MFA?

The bar is simply too low with a login name and password alone. Conditional Access MFA is the modern and effective approach to keeping your hard work, brand image, and business protected from un-authorised login requests.

In order to gain access to an advanced MFA protected account, the user must meet all the imposed conditions (OS Version, Browser Name, Country of Access etc) before MFA will allow the user to use gain access to an application.

This makes an advanced MFA authentication system extremely secure. This method of MFA is also a popular choice from Remote Desktop Access where you want account logins or applications secured with MFA.

Access Controls

With extensive access policies, you can limit access to your applications based on your company's unique security needs. Manage permissions by user group and flag trusted devices to minimize friction for your employees, while reducing security risk.

Have a question? Let's chat...

Whether you're interested to learn more about key features, pricing or anything else, we're here to help.

Reach out to us today

Call: +64 0800 485 644

Email: security@rocketit.co.nz

Website: rocketit.co.nz