Azure Security Defaults

VS

Conditional Access

Tiberium

Azure Security Defaults

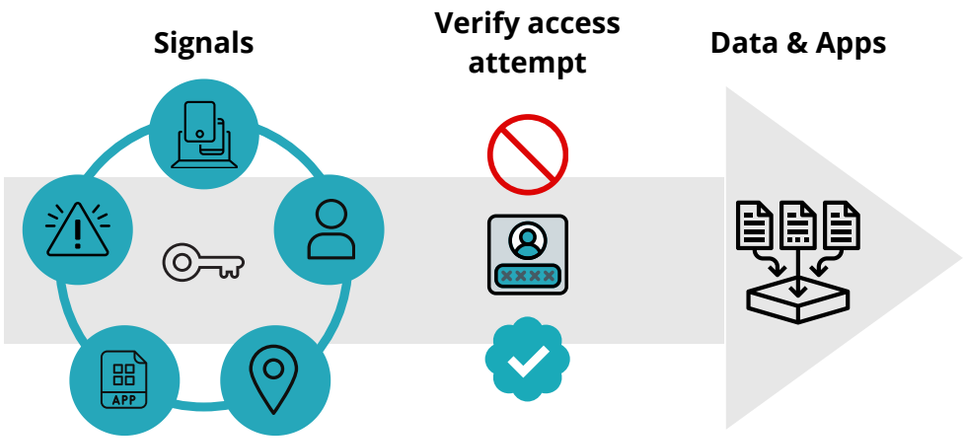
Pre-configured security settings that improve the protection of your organisation

But... how?

- Azure AD Multi-Factor Authentication registration for all users
- Multi-factor authentication enforcement for administrators
- Privileged activities protection e.g. Access to Azure Portal
- Multi-factor authentication requests when necessary
- Blocking of legacy authentication protocols used by attackers

Conditional Access

An Azure Active Directory tool that combines signals (IP, user, application, device, location, etc.) to make decisions (limit, allow or block access & require MFA) and enforce organisational policies



Azure Security Defaults are for you if...

- you want to improve your security but don't know how
- you use the free tier of Azure Active Directory licensing

Conditional Access is for you if...

- you have complex security requirements
- you have Azure Active Directory Premium licenses

A big tick is... **Tiberium FROST**

FROST is the best option as it includes **REACT** and **RESPONSE** options using automation. The **FROST** bot checks your security settings and applies best practices, then alerts you if something goes wrong!

With FROST we enable either Security Default or Conditional access to massively improve your Microsoft Security Score.

Find out more