Cubit
TECHNOLOGY

Zero Trust

Zero Trust is a security concept that assumes that all users, devices, and applications inside or outside an organisation's network are potentially malicious and should not be automatically trusted. In other words, Zero Trust assumes that no user or device can be trusted by default, and that access to resources should be granted on a need-to-know basis.

To implement a Zero Trust model, organisations need to adopt a range of security controls and technologies that enforce strong authentication, authorization, and access controls. These controls may include

- **Multi-factor authentication**
- **Network segmentation**
- **Micro-segmentation**
- **Least privilege access**
- **Continuous monitoring**

Zero Trust can help organisations improve their security posture by:

- **Reducing the risk of insider threats**
- **Minimizing the impact of external attacks**
- **Improving visibility and control over their digital assets**

By adopting a Zero Trust approach, organizations can also reduce their compliance risk by ensuring that they have proper controls in place to protect sensitive data.

The Microsoft MDM platform and endpoint software, called Intune, enforces predefined security policies ensuring all devices are in compliance before the device is able to access any data. The software also provides segmentation of personal & company data which is especially useful when a device isn’t company owned. The separation of data allows just the company data to be deleted without affecting any personal data if a device is lost or stolen or in the event of a bad leaver.