Three ways to implement Zero Trust into your organisation

daisy. COMMUNICATIONS

In the rapidly evolving landscape modern organisations operate in, a fresh and adaptable security model, such as Zero Trust, is essential to navigate the complexities of the contemporary environment, accommodate the hybrid workplace, and ensure the protection of people, devices, applications, and data.

By embracing Zero Trust, organisations can confidently address the challenges posed by the dynamic nature of today's digital ecosystem, bolstering their resilience and fortifying their defences against emerging security threats.

Never trust, always verify

- Fully authenticate, authorise, and encrypt every access request.
- Consider user, device, location, service, data, and network information.

Limit user access

- Apply the principle of least privilege.
- Grant access on an as-needed basis for specific tasks.

Assume breach, monitor constantly

- Embrace a security culture assuming active cyberattacks.
- Continuously monitor the environment to protect against real-time threats.

The six dimensions of Zero Trust security:

1. Verify identities with Multi-Factor Authentication.
2. Allow only managed and compliant devices.
3. Protect data from accidental and malicious leaks.
4. Harden application security to reduce risks.
5. Secure private data centres and public cloud infrastructures.
6. Constantly assess security posture and respond to threats.

Find out how Daisy Communications can implement Zero Trust into your organisation.

› Contact Daisy Communications now