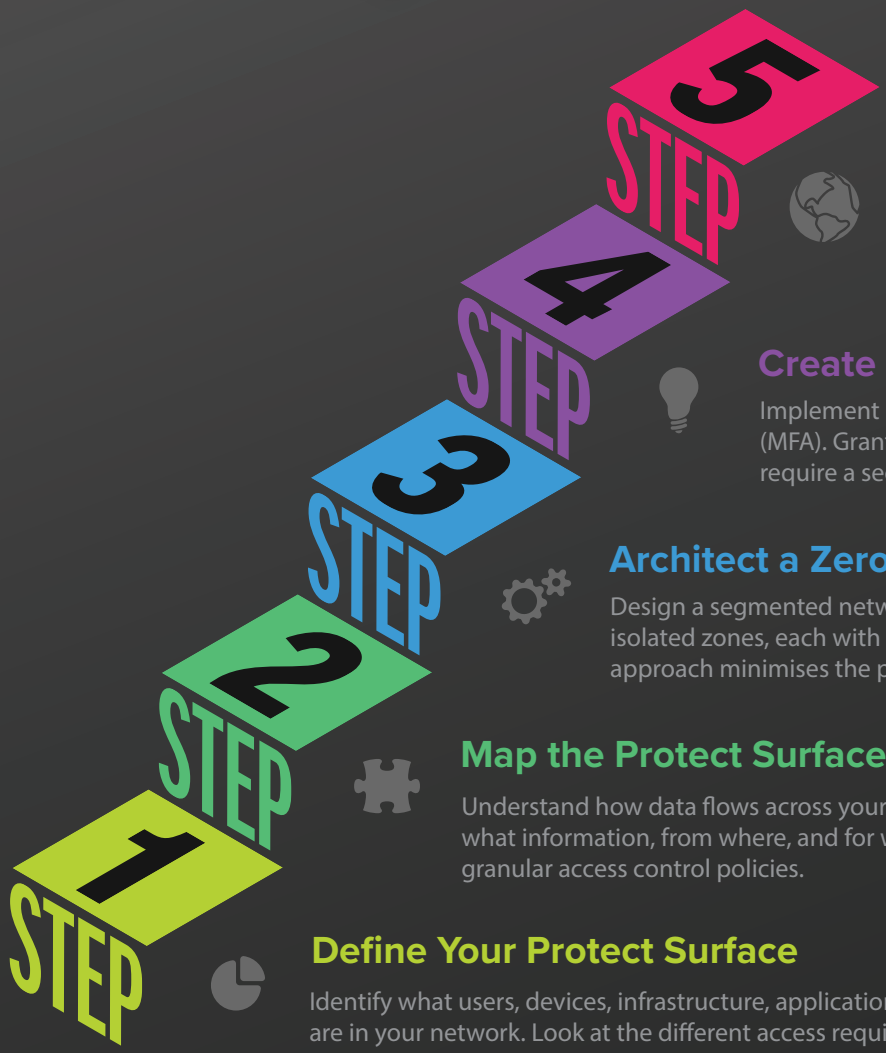
Five Steps Towards a Zero Trust Model



Monitor & Maintain the Network

Continuously monitor for potential threats with tools and automated responses to isolate and contain breaches. Regularly review and refine policies for optimal security.

Create a Zero Trust Policy

Implement least privilege and multi-factor authentication (MFA). Grant users only the minimum access needed and require a secondary verification factor beyond passwords.

Architect a Zero Trust Network

Design a segmented network architecture. Divide your network into isolated zones, each with specific resources and access controls. This approach minimises the potential impact of a security breach.

Map the Protect Surface Transaction Flows

Understand how data flows across your network – who accesses what information, from where, and for what purpose. This informs granular access control policies.

Define Your Protect Surface

Identify what users, devices, infrastructure, applications, data, and services are in your network. Look at the different access requirements of user groups and key individuals to help prioritise how Zero Trust is rolled out.

ZERO TRUST FOR:

USERS | APPLICATIONS | INFRASTRUCTURE

Identity **Device/Workload** **Access** **Transaction**

Need help planning and implementing Zero Trust?

Experienced network and security specialists are on hand to help you achieve Zero Trust. Benefit from the dynamic vSOC Connect Console, giving you full visibility of your project management.

SPEAK TO AN EXPERT

01423 425 498 dataconnect.co.uk moreinfo@dataconnect.co.uk

DATACONNECT
CYBER SECURITY - CONSULTANCY | SERVICES | TECHNOLOGY