



# A telco approach to Zero Trust

Dave Harcourt

Chief Security Authority & BT Fellow



# BT Group



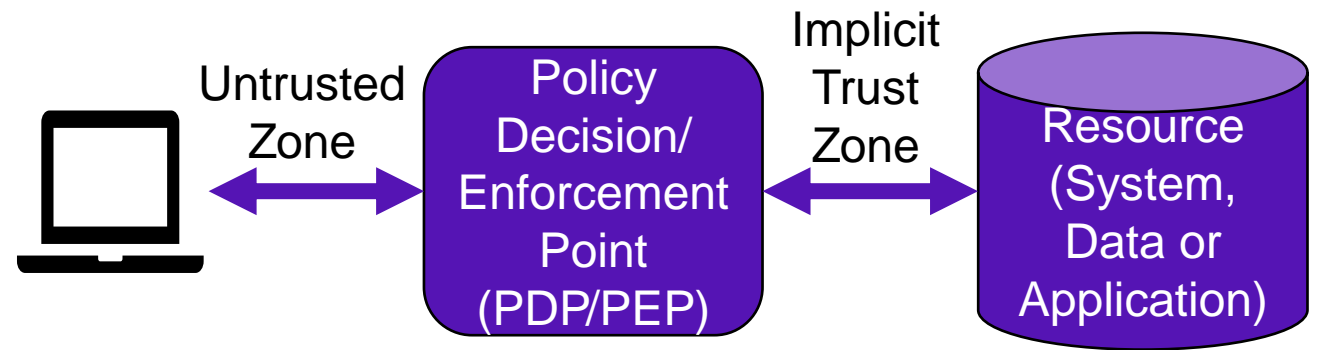
# What do we mean by Zero Trust?

Zero Trust is a class of architecture. Most simply it is a just formal statement that any access to IT resources must be subject to an identity-based access-control policy.

NIST define a reference architecture which is an acceptable starting point. The abstract model here is simplified but can be applied to a broad range of environments.

The architectural goal is to reduce the scope of the implicit trust zone, in other words to put the PDP logically close to the object that is being protected.

Zero trust depends on strong, mutual authentication and strong encryption of traffic in the untrusted zone.



From NIST Special Publication 800-207

# Zero Trust Principles

NCSC, Microsoft and others have defined a range of Zero Trust principles. At their core they all focus on a common set, which I'll summarise as:

**Verify explicitly** – authenticate and authorise based on identity, location, device health, service, data classification

**Least privilege** – Just-In-Time and Just-Enough-Access using risk based policies and data protection

**Don't trust networks** – including your own! A shift from network based security measures

**Focus monitoring on endpoint** – users, devices and services

**Assume breach** – minimise blast radius and reduce lateral movement

**Simplicity** – if it's easier to understand the security wrap, it's easier to have confidence in its effectiveness

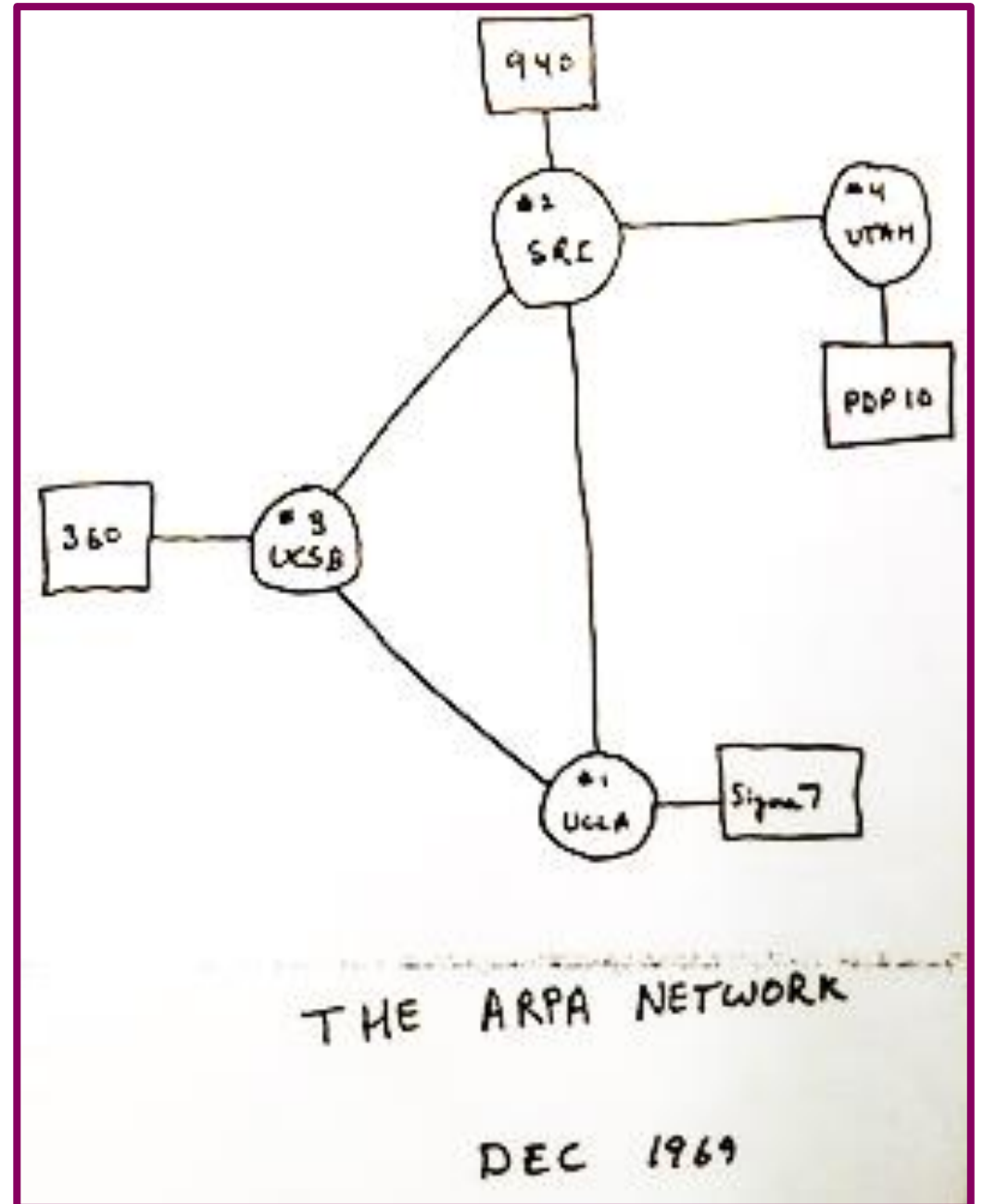
# Why move to Zero Trust?

A little history of the internet...

ARPANet was the genesis for the internet as we know it today

Availability was the core of its design principles, not security

The internet as we know it today wasn't perceived when ARPANet was originally conceived



# Why move to Zero Trust?

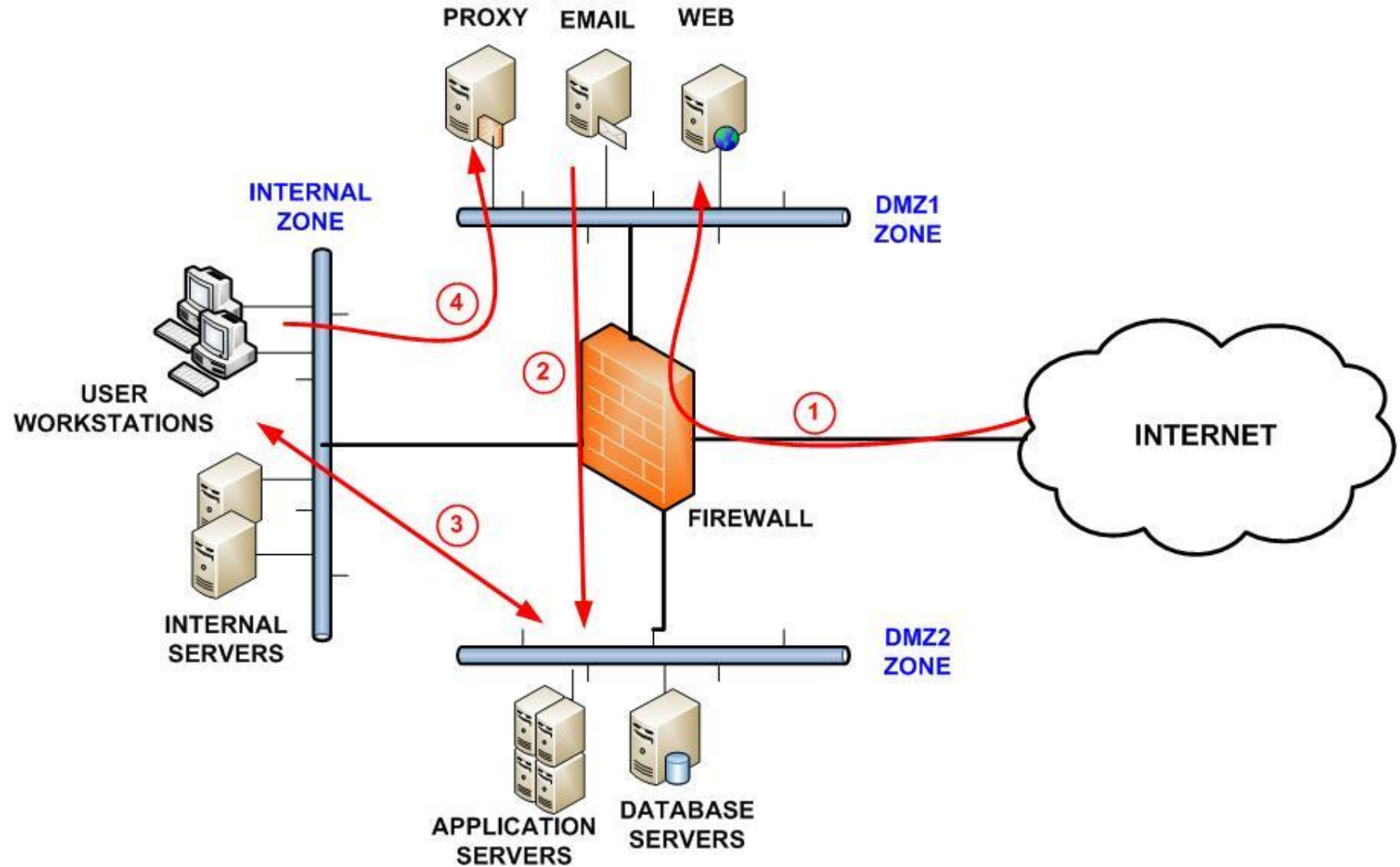
## Adding in a little security

Private Networks implemented Firewall perimeters to keep secure from wider internet threats as the internet grew.

Internet = Untrusted

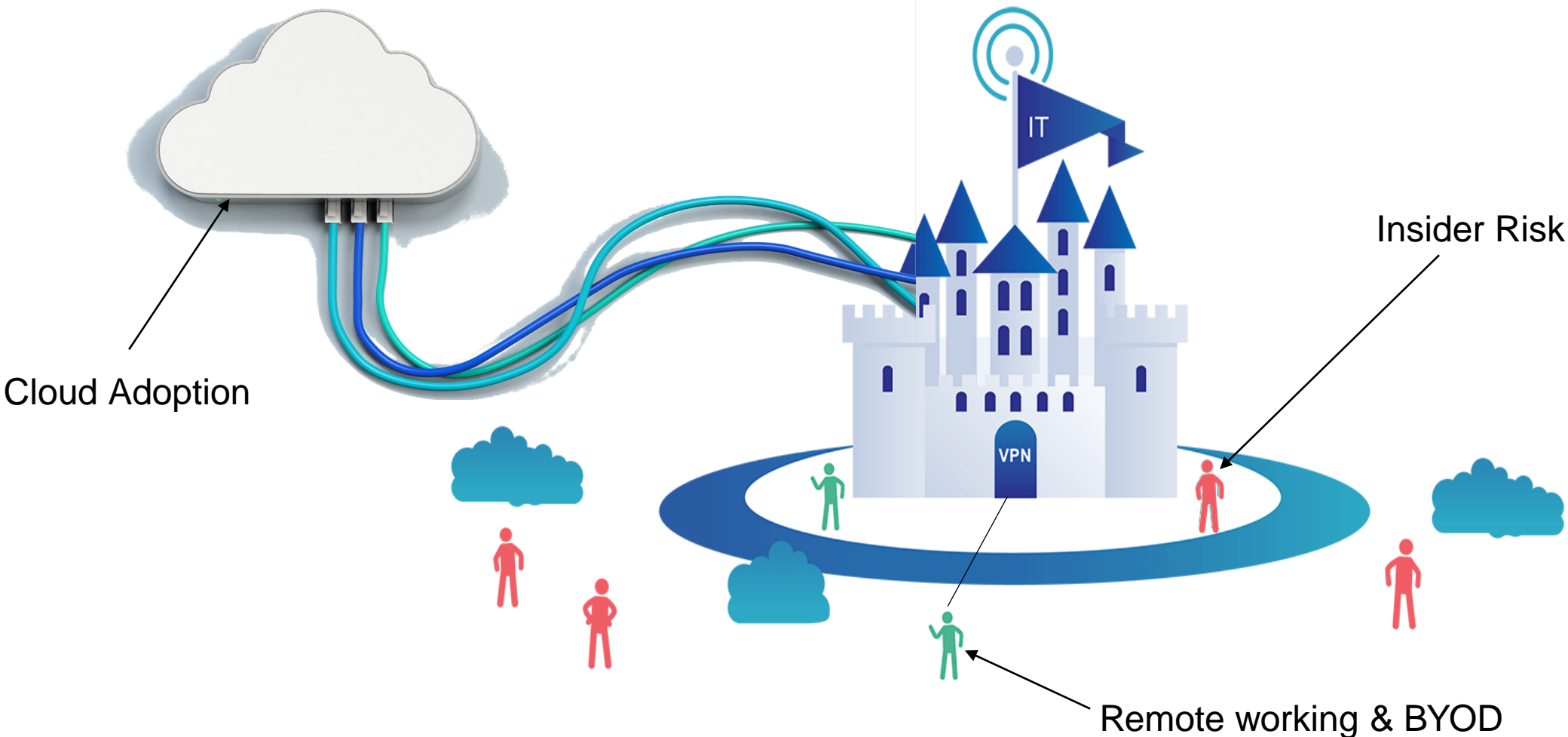
Intranet = Trusted

DMZ = boundary services



# Why move to Zero Trust?

So why move?



# BT's Zero Trust adoption approach



# Architectural Principles

The architecture of our estate is governed by the following high level principles:

## 1. **Compartmentalisation**

We compartmentalise our estate at multiple levels to limit connectivity and data exchange. Compartmentalisation is applied at multiple levels to ensure high level separation policies are enforced as well as low level separation appropriate to the individual applications. Compartmentalisation enables the impact of any exposure due to failure or compromise to be restricted.

## 2. **Defence in depth**

We use different enforcement mechanisms to apply levels of compartmentalisation to provide defence in depth. This ensures that any failure through compromise, misconfiguration or bug is restricted and constrained.

## 3. **Authentication**

We authenticate all user, device and application interactions and verify that those interactions are authorised and logged. We apply a policy of zero trust and base authentication on multiple factors. We do not allow connectivity based solely on IP address or originating security compartment.

We ensure connectivity is limited to the time period it is required and is reverified during its duration rather than enabled permanently.

## 4. **Protect data**

We do not trust our physical assets or security of their location to protect data. Where viable we encrypt connections to applications and data at rest. For network traffic we carry customer traffic without further encryption but do not persist it on our network devices.

## 5. **Compliance and Monitoring**

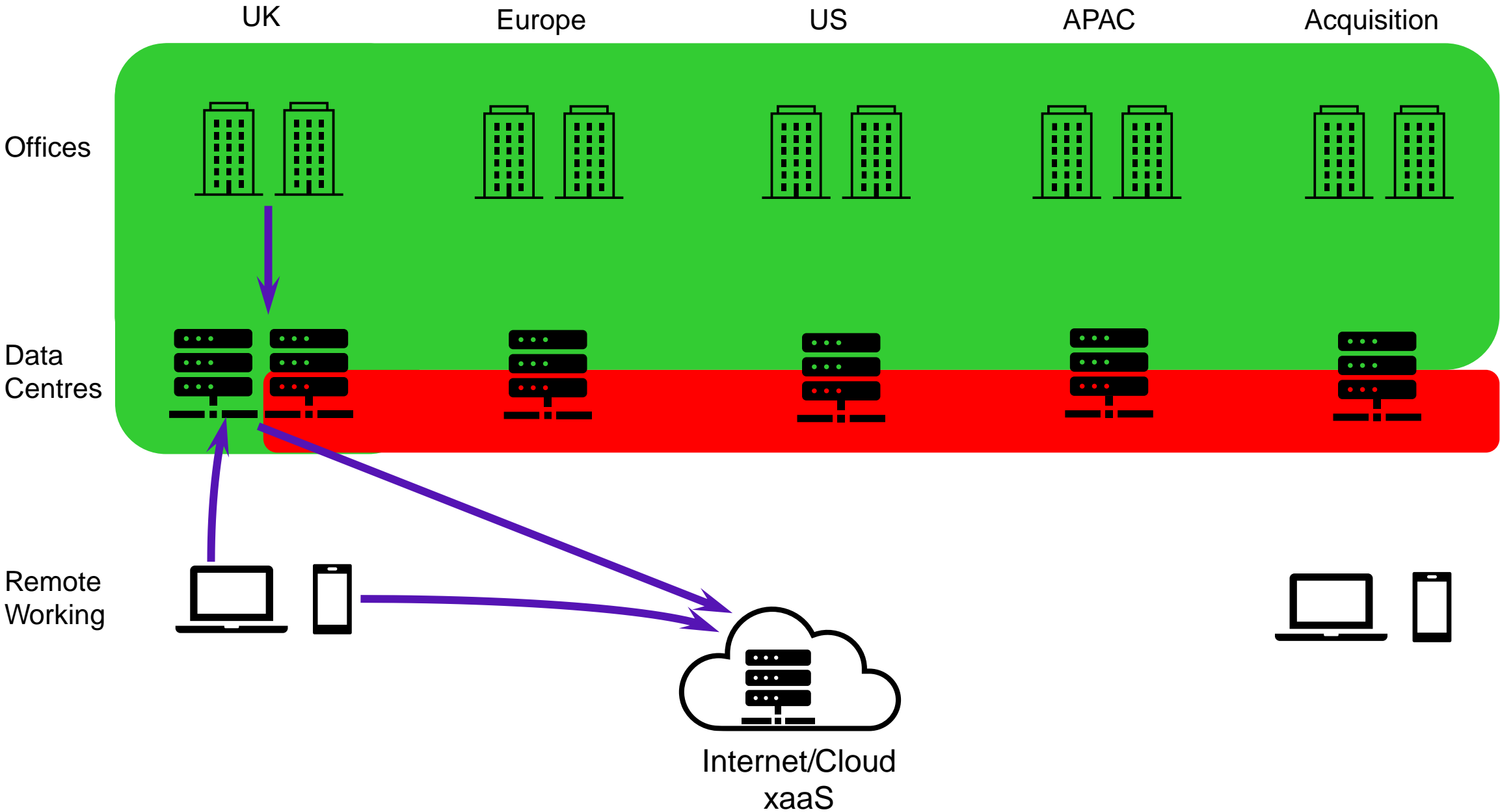
We apply multiple levels of monitoring across the estate to validate correct operation and detect anomalies and attacks. This is an integral part of our security practices and provides a compliance and enforcement mechanism to validate correct operation. We codify our policies and automate compliance verification against these to ensure continued compliance. Our monitoring tools enable us to detect anomalies and protect against DDOS and malware.

## 6. **Simplicity**

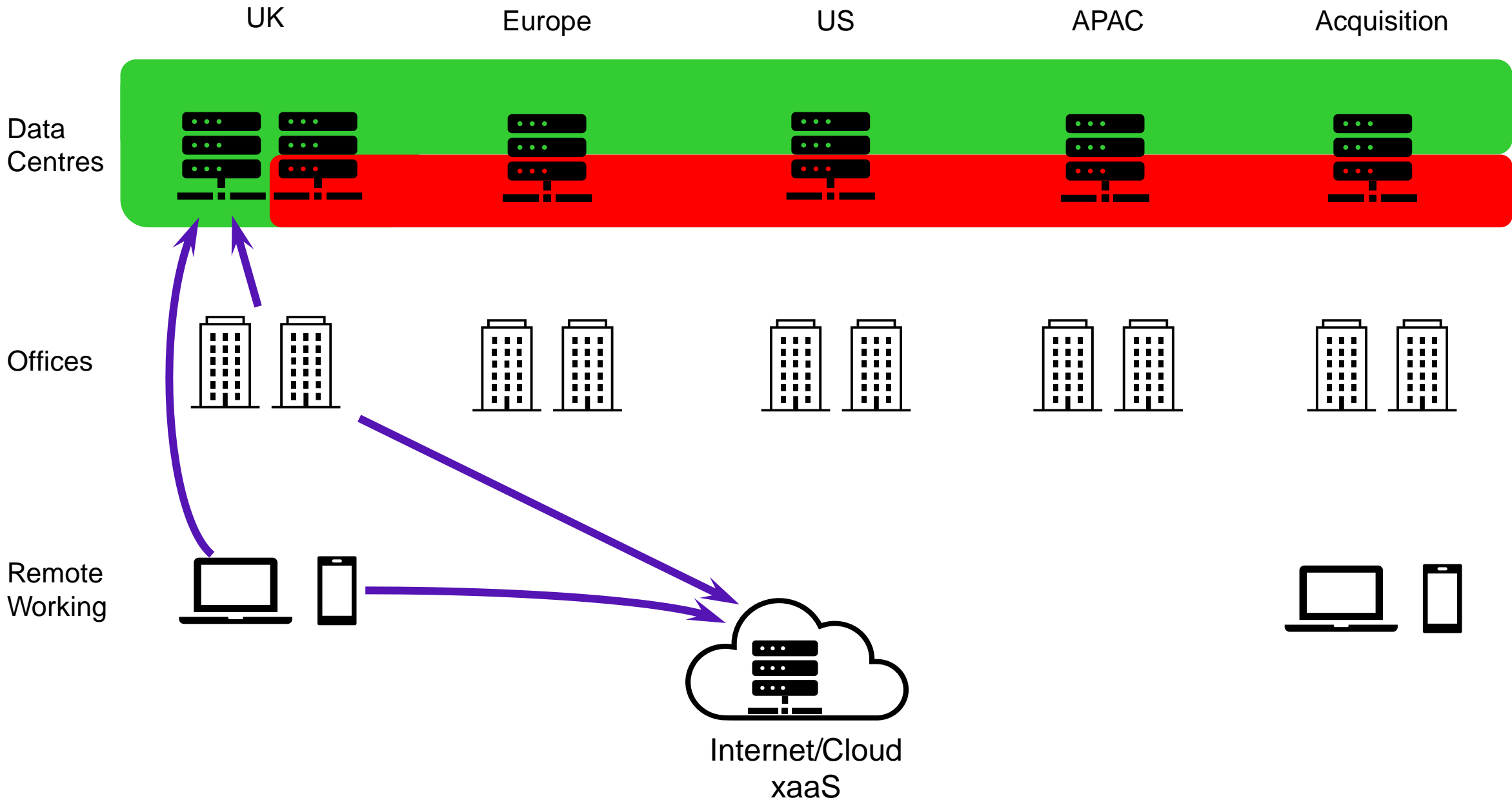
We ensure our security polices are simple to understand, easy to use and apply. This minimises chance of them being mis-implemented or ignored

We apply common technology solutions to minimise complexity but duplicate instances of technology across each compartment as required

# The start of BT's journey



# Reducing the scale of trust – our offices



# Zero trust Offices transformation

## BWP Sites

- Standard user experience
- One Network Design (including EE stores)
- User Type (Persona) Authentication

## Security by design

- Wi-Fi 1st strategy for Info Workers
- Wired capability for Contact Centres

## Traditional Sites

- >50 resources

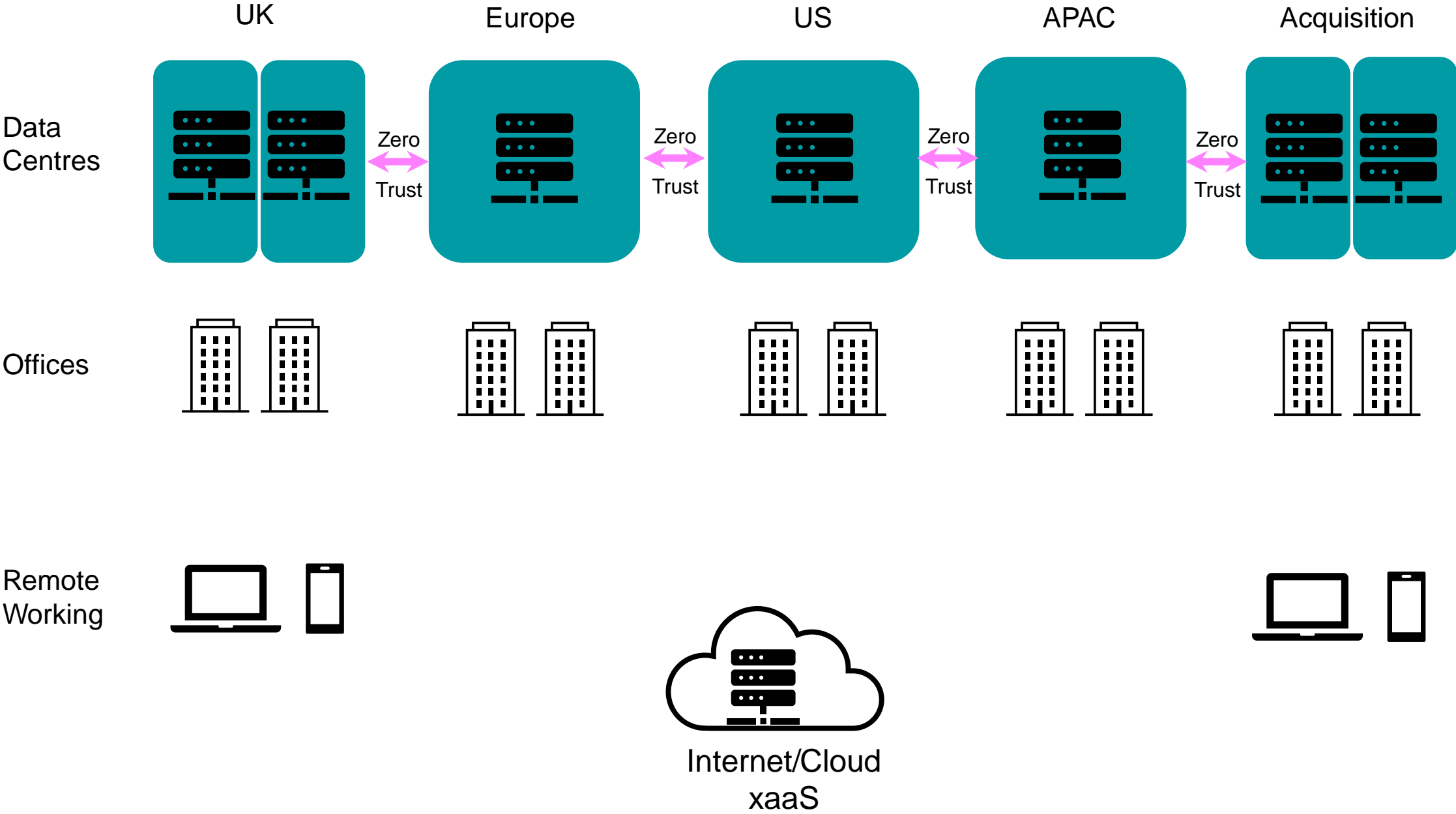
Same BWP Network Design

- <50 resources

Wi-Fi for Service Office

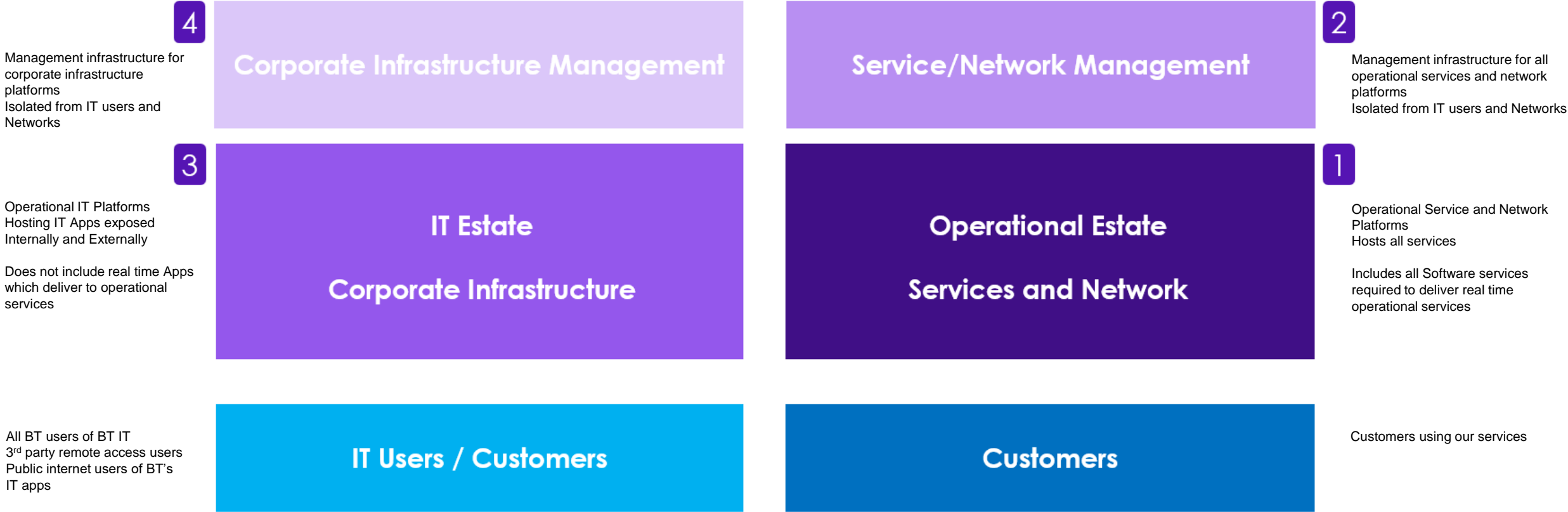
Environment

# Creating smaller trust islands



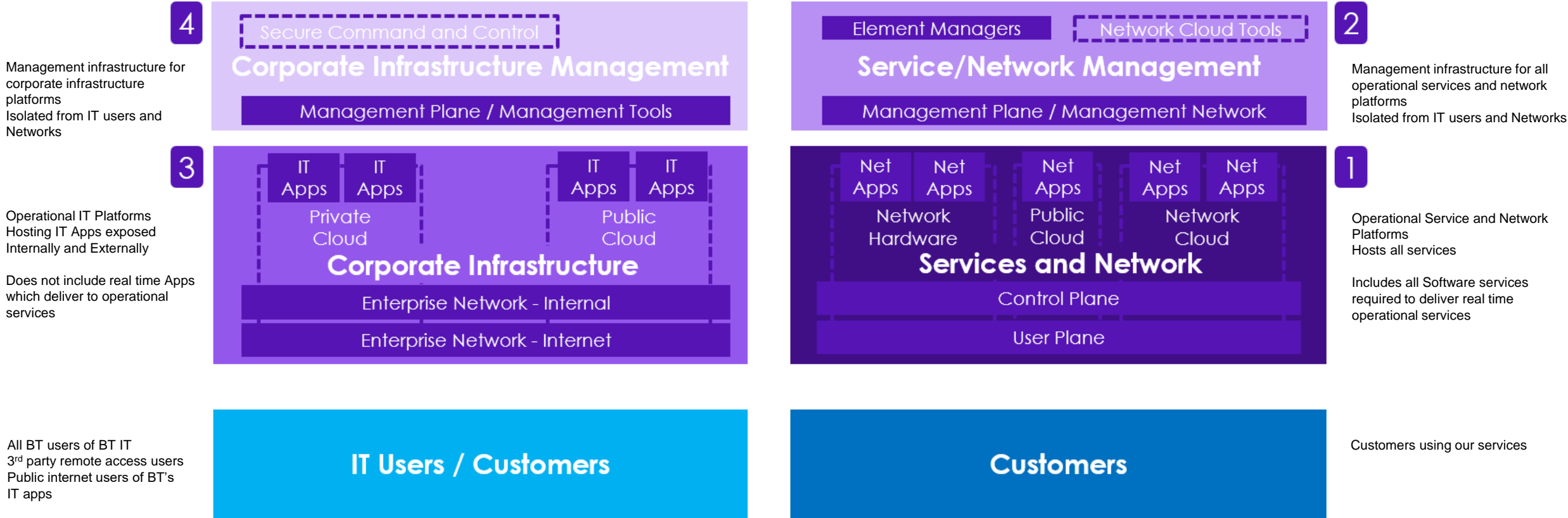
# Domains

We compartmentalise our infrastructure into 4 separate domains, supporting customers and users:

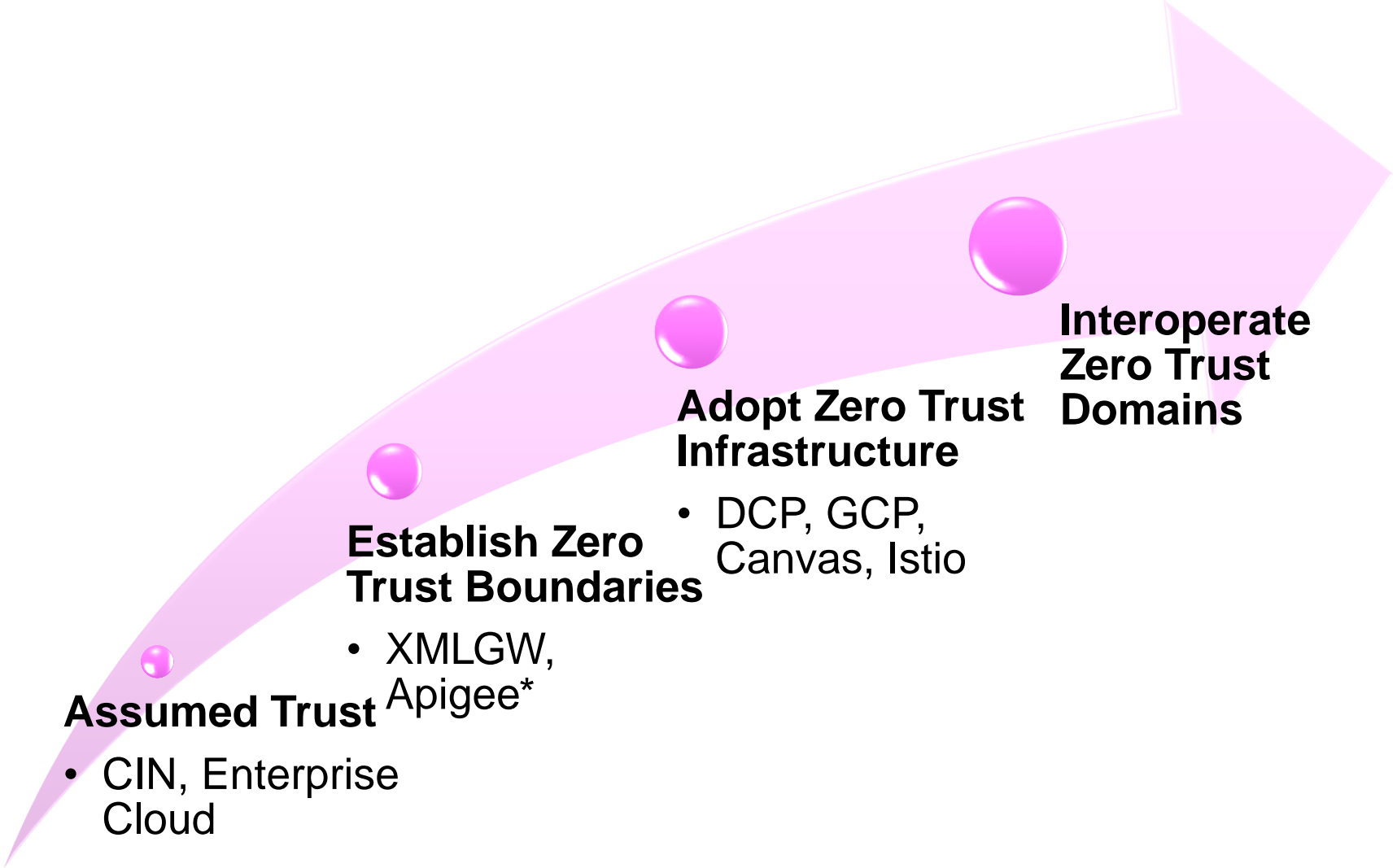


# Domains - Microsegmentation

Each infrastructure component falls within only one domain:

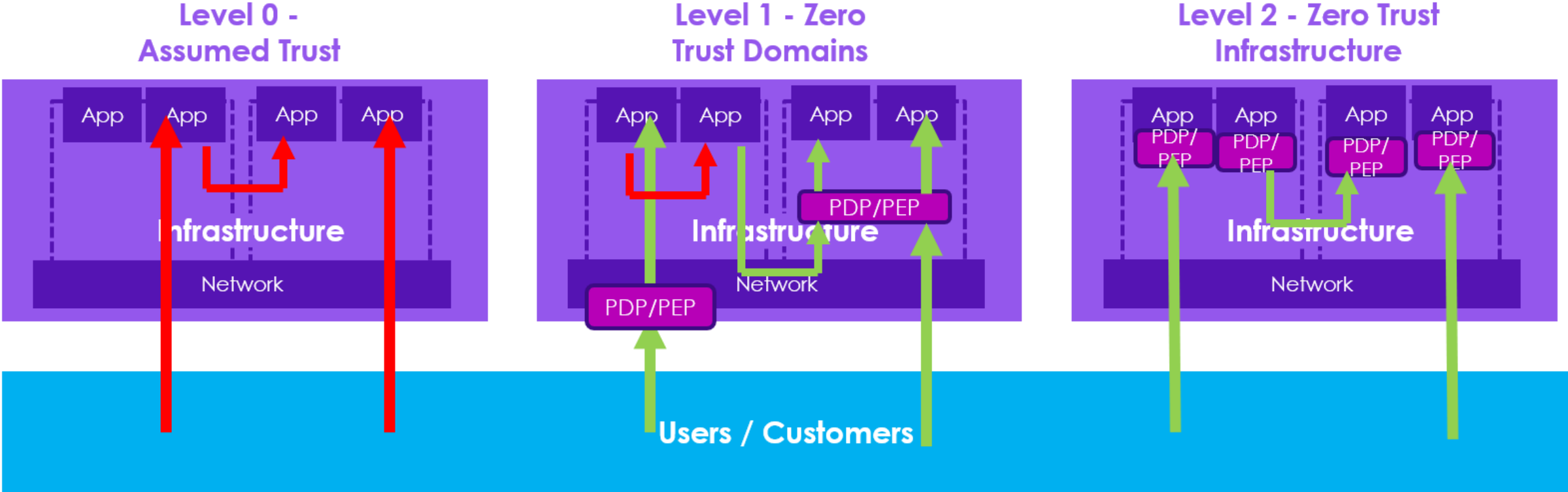


# Data Centre Zero Trust Maturity





# Maturity Examples



With the right tools in each for: Protecting data; Measuring compliance; Detecting and responding

# Benefits of Microsegmentation



**Reduce impact  
of an attack**




**Improve breach  
containment**



**Strengthen  
compliance**



# ZT Identity & Authentication Initiatives

- **Migration of legacy user authentication to Azure AD & Passwordless**
  - **Onboarding of Privilege accounts for critical apps to CyberArk**
  - **Security Service Edge (SSE) Adoption**
  - **Continuous Biometric Authentication (CBA)**
  - **Identity Transformation**
- 

# A Glimpse into the Future: How Zero Trust will Revolutionise Our Estate

ACCURATE INVENTORY  
OF INFRASTRUCTURE

IMPROVED  
MONITORING AND  
ALERTING

IMPROVED END-USER  
EXPERIENCE

STREAMLINED  
SECURITY POLICY  
CREATION

FLEXIBILITY WHEN  
MOVING APPS, DATA  
AND SERVICES

MINIMISATION OF  
LOST OR STOLEN DATA