National Cyber Security Centre
a part of GCHQ

Zero Trust

2023-08-28

National Cyber Security Centre
a part of GCHQ

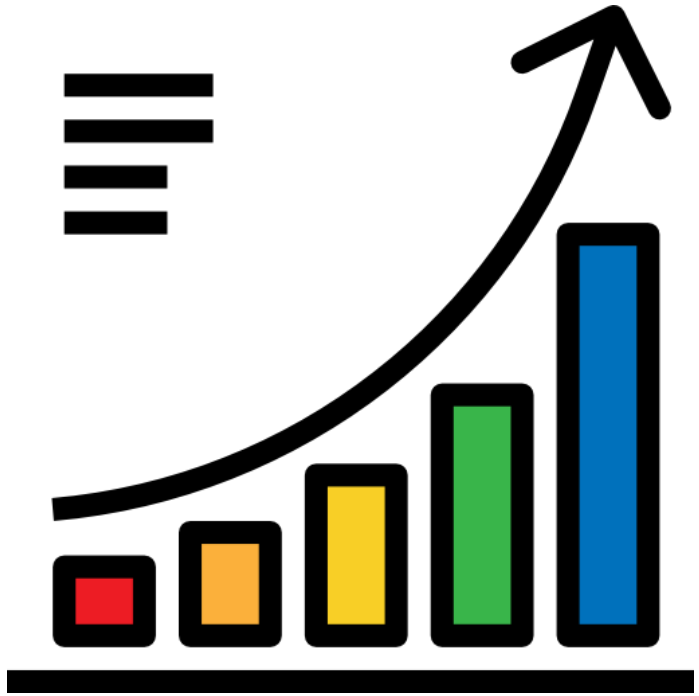
Benefits

Better visibility

Strong authentication and authorisation

Device health and attestation

Dynamic access decisions based on trust



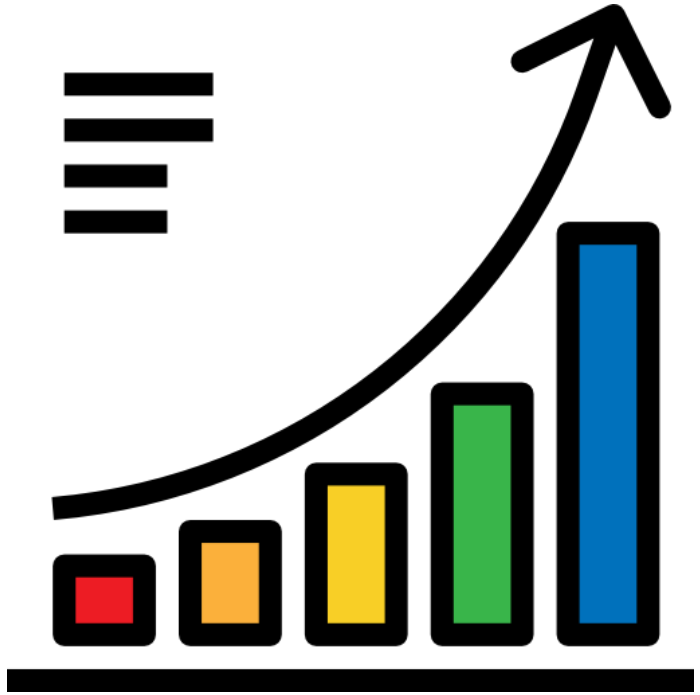
National Cyber Security Centre
a part of GCHQ

Benefits

Limit blast radius and lateral movement

Monitoring is required for zero trust to work, it's not an afterthought

Not just security benefits. Flexibility, scaling and useability can all be improved



zerotrust@ncsc.gov.uk

National Cyber Security Centre
a part of GCHQ

Our guidance to help enable implementation

Zero trust principles

Principles allow a more flexible approach to guidance

8 building blocks and considerations that the NCSC feel make up a Zero trust network

Migration blogs

Blogs on how to start your journey to zero trust and migrate to a system as described in the principles

zerotrust@ncsc.gov.uk

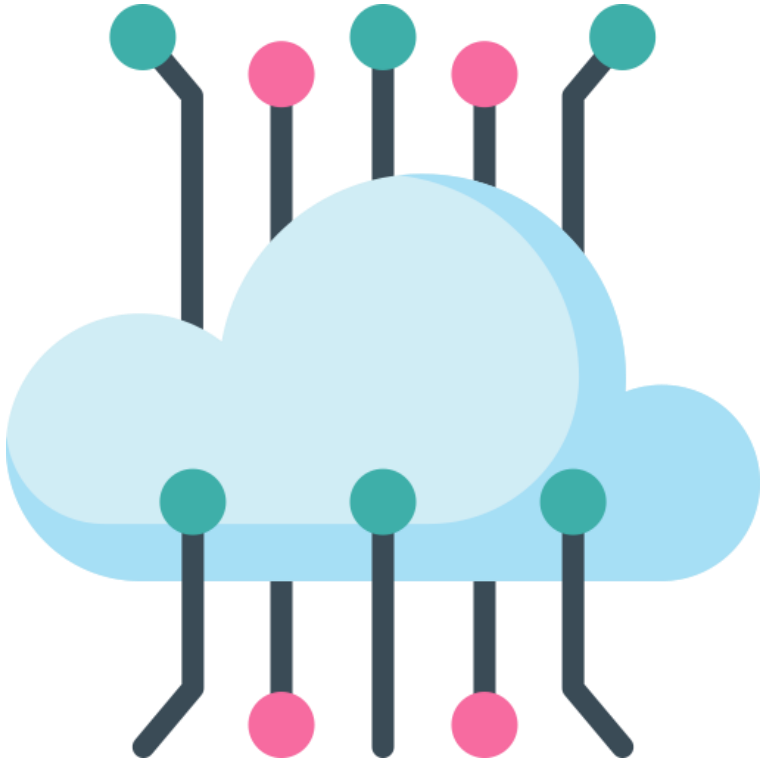
National Cyber Security Centre
a part of GCHQ

Zero trust and Supply Chain Security

Zero trust architecture in development and integration systems enhances their holistic security.

Using zero trust technologies in development environments and CI/CD pipelines, enhances the system integrity and provenance of software.

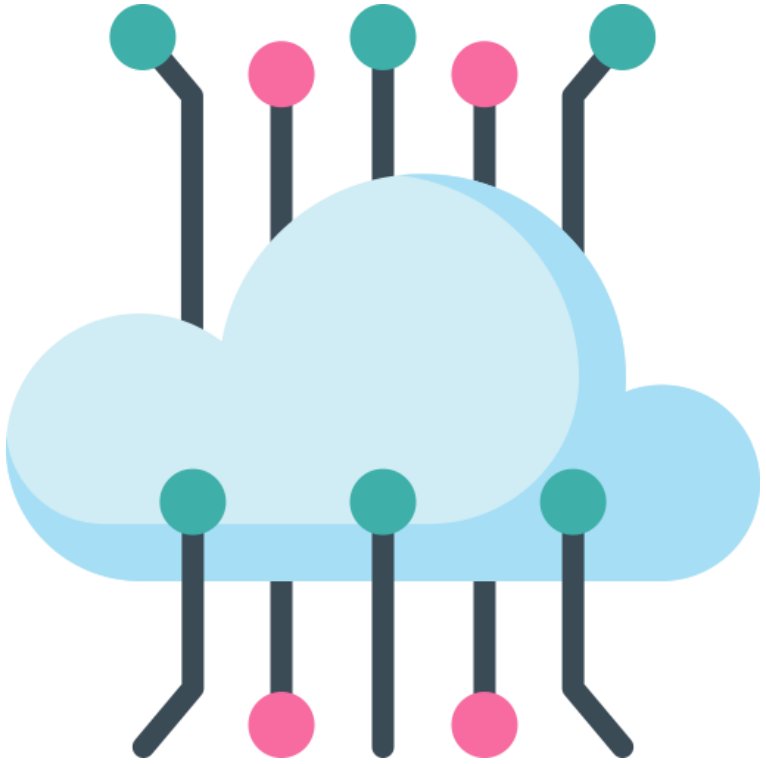
Can reduce likelihood of supply chain attack.



zerotrust@ncsc.gov.uk

National Cyber Security Centre
a part of GCHQ

Zero trust and Supply Chain Security



Zero trust architecture can reduce the impact of a supply chain incident.

Improved monitoring to identify malicious behaviour.

Micro-segmentation and protection of lateral movement can reduce the blast radius of a supply chain attack.

zerotrust@ncsc.gov.uk

National Cyber Security Centre
a part of GCHQ

Zero trust is not a product…

it’s a mindset.

National Cyber Security Centre
a part of GCHQ

Does zero trust address all of your threats?

Start with our first principal "Know your architecture"

- Users, devices, services, and data
- Knowing your assets, helps your migration plan

Are your systems ready?

- Can your application adapt to zero trust?
- Know what legacy systems can't use zero trust

zerotrust@ncsc.gov.uk

National Cyber Security Centre
a part of GCHQ

Does zero trust address all of your threats?

Threat modelling

- Understand your threats throughout design and migration
- This can also inform your policies

Test your solution

- Compare against your existing architecture
- Perform active testing / red team activities
- Phase the rollout of new architecture

zerotrust@ncsc.gov.uk

National Cyber Security Centre
a part of GCHQ

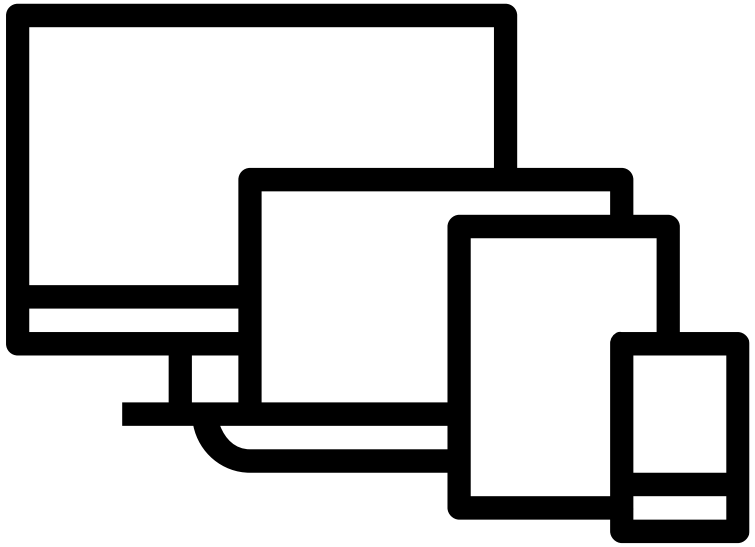
Example: Removing a VPN

A common theme we see is removing an always-on VPN too early

Benefits include better performance, scaling, remove single point of failure

However, the VPN is being removed before suitable controls are in place, putting systems at increased risk

For example, legacy protocols going over the internet or lack of controls to monitor network traffic and filter known malicious indicators of compromise.



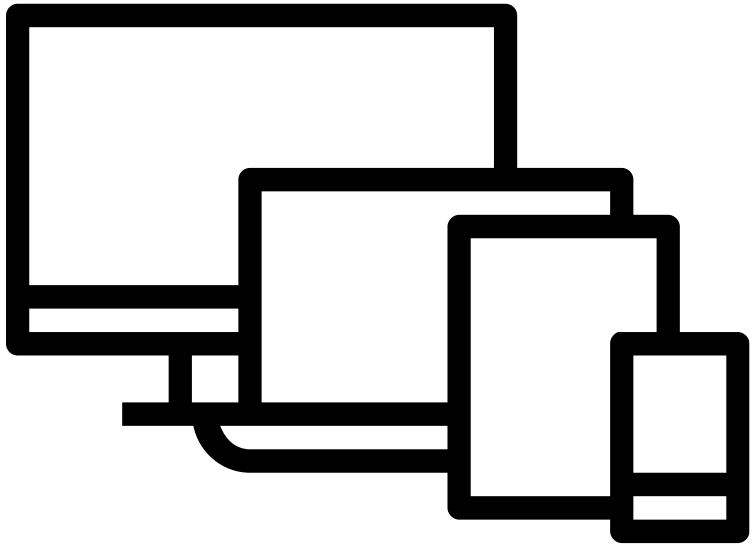
National Cyber Security Centre
a part of GCHQ

Example: Over-reliance on identity

Many architectures that claim to be zero trust only rely on authentication.

There are several recent examples of compromises due to poor authentication.

User authentication is only one of many signals that should be taken into consideration when making an access decision.



National Cyber Security Centre
a part of GCHQ

Any questions?

For Principles and Migration blogs visit;
https://www.ncsc.gov.uk/collection/zero-trust-architecture