Zero Trust

Ensuring Business Continuity

Zero Trust models are increasingly coming to the fore to mitigate common cyber threats and help increase levels of assurance that systems and data are being accessed appropriately. Zero Trust approaches can be challenging to embed into existing solutions and can also bring complexity if not applied pragmatically and in line with the needs of the organisation.

Our team will work with you to identify the advantages of adopting Zero Trust approaches or whether alternative security patterns can offer you more appropriate protections. We will identify the readiness of the solutions in your environment to adopt Zero Trust access principles and identify approaches to implementing elements of a Zero Trust model in the most effective way for you.

Through the use of targeted automation we can help simplify response and management of the signals generated through your Zero Trust components to accelerate processing of access requests and management of risks arising from this approach.

Scenarios where Zero Trust might be right for you

- You have a complex and extensive supply chain with direct access from 3rd party managed (or unmanaged) devices to your data and / or services;
- Your business model relies on effective collaboration with 3rd parties on sensitive data where that data carries a high risk of harm if compromised;
- The nature of your business is dynamic (and potentially unpredictable) where notable shifts in behaviour and usage within your environment are highly likely to occur in a standard planning cycle (say, quarterly);
- The devices and services accessing your data are disproportionately outside of your own organisation or sphere of control;
- Preventing legitimate business usage (even if that is unexpected or irregular) is potentially more harmful than a breach or compromise.

If you can tick some or all of those boxes you should definitely consider Zero Trust. There's plenty more examples where it's a good fit.

So what should you do?

Ask these questions:

- How does this model support my business strategy? Can you show how it supports my organisational objectives?
- How much of my existing investment can work effectively in that model?
- Can you show how adopting this would allow our people to work effectively in an appropriately secure manner?

The 12 Dimensions of Zero Trust

A Zero Trust access model is typically going to consider all of the following dimensions:

- The User (Person)
- Identity
- Device
- Network / Connectivity
- Host
- Application
- Data
- Monitoring
- Session / State
- Location
- Time
- Policy

A Zero Trust solution may not consider all of these dimensions, but the policies and mechanisms surrounding it will typically be considering these. The exclusion of any dimension will typically reduce the effectiveness and granularity of control achievable but can also reduce the volume of datapoints being stored and processed and reduce the complexity of the implementation. All of these considerations should be balanced when deciding upon a solution.

We are a UK Sovereign, cyber security solutions company that designs, builds and supports end-users to use technology, securely. We are passionate about delivering the best possible front line experience and believe you should expect the same technology innovations in your work as you benefit from in your personal life. We deliver ecosystems accreditable to OFFICIAL-SENSITIVE to SECRET as part of our secure UK data sovereign private cloud, Platform FLEX.

Contact

+44 (0)2382 020300

www.nine23.co.uk

2 Venture Road, Chilworth,

Southampton, SO16 7NP