Zero trust architecture design principles

Eight principles to help you to implement your own zero trust network architecture in an enterprise environment.

Zero trust is an architectural approach where inherent trust in the network is removed, the network is assumed hostile and each request is verified based on an access policy. To learn more read our Introduction to Zero Trust.

What is this guidance for?

The principles within this guidance will help you design and review a zero trust architecture that meets your organisations individual requirements.

There are many vendors and open source offerings providing zero trust based services. These principles will help you select which combination of services can best support your journey to zero trust.

Who is this guidance for?

This guidance is aimed at those implementing a zero trust architecture in an enterprise environment - this includes public and private sectors.

If you're new to zero trust architecture, or this is the first time you are reading this guidance, read our Introduction to Zero Trust, which covers some key concepts and terminology.

For **board level readers** read the Introduction to Zero Trust and the overview of the principles on this page.

For **technical readers** and **cyber security professionals** all sections are relevant, but we encourage you to read the key concepts and terminology before you jump into reading the principles in detail.

Product vendors and open source projects can use this guidance to aid the development of zero trust architecture products and services.

Overview of the principles

Includes some context and an summary of the principle's objectives.

1. **Know your architecture, including users, devices, services and data**
   In order to get the benefits from zero trust, you need to know about each component of your architecture. This will allow you to identify where your key resources are, the main risks to your architecture and also avoid any late stage pitfalls integrating legacy services which do not support zero trust.

2. **Know your User, Service and Device identities**
   An identity can represent a user (a human), service (software process) or device. Each should be uniquely identifiable in a zero trust architecture. This is one of the most important factors in deciding whether someone or something should be given access to data or services.

3. **Assess your user behaviour, devices and services health**
   User behaviour, and service or device health, are important indicators when looking to establish confidence in the security of your systems, making them important signals for policy engines. Therefore, having the ability to measure user behaviour, device and service health is key in a zero trust architecture.

4. **Use policies to authorise requests**
   Each request for data or services should be authorised against a policy. The power of a zero trust architecture comes from the access policies you define. Policies can also help to facilitate risk managed sharing of data or services with guest users or partner organisations.

The policy engine is a key component of the zero trust architecture, it uses multiple signals and provides a flexible and secure access control mechanism that adapts to the resources being requested.

5 **Authenticate & Authorise everywhere**
Authentication and authorisation decisions should consider multiple signals, such as device location, device health, user identity and status to evaluate the risk associated with the access request. We do this as we assume the network is hostile and want to ensure all connections that access your data or services are authenticated and authorised.

6 **Focus your monitoring on users, devices and services**
In a zero trust architecture, it is highly likely that your monitoring strategy will change to focus on users, devices and services. Monitoring of these devices, services and users behaviours will help you establish their health. Monitoring should link back to the policies you have set to gain assurance in their configuration.

7 **Don't trust any network, including your own**
Don't trust any network between the device and the service it's accessing, including the local network. Communications over a network, to access data or services, should use a secure transport protocol to gain assurance that your traffic is protected in transit and less susceptible to threats.

A zero trust architecture changes the way traditional user protections such as malicious website filtering and phishing protection are implemented, these may need to provided by different solutions in your zero trust architecture.

8 **Choose services designed for zero trust**
Services may not support zero trust and thus may require additional resources to integrate and increase support overhead. In these scenarios it may be prudent to consider alternative products and services that have been designed with zero trust in mind.

Using products that utilise standards-based technologies allows for easier integration and interoperability between services and identity providers.

PUBLISHED

23 July 2021

REVIEWED

27 February 2023

VERSION

1.0

WRITTEN FOR

Large organisations

Public sector

Cyber security professionals