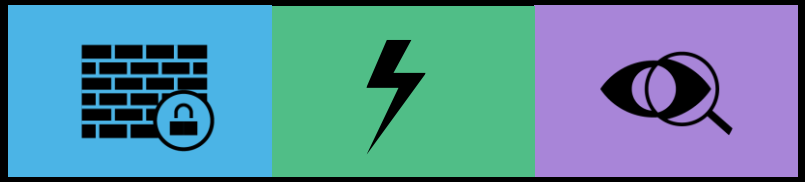
Det finns inte fler produkter att köpa – för att uppnå “cyber resiliance”

Johan Ström
Solution architect

Current state

- Market-leading solutions
- Cyber SOC
- CSIRT
- Public breach information

There are three important principles in this ideology:



1	2	3
Apply the concept of least privilege.	Assume that breach is inevitable or has likely already occurred.	Every transaction must be authenticated and authorized.

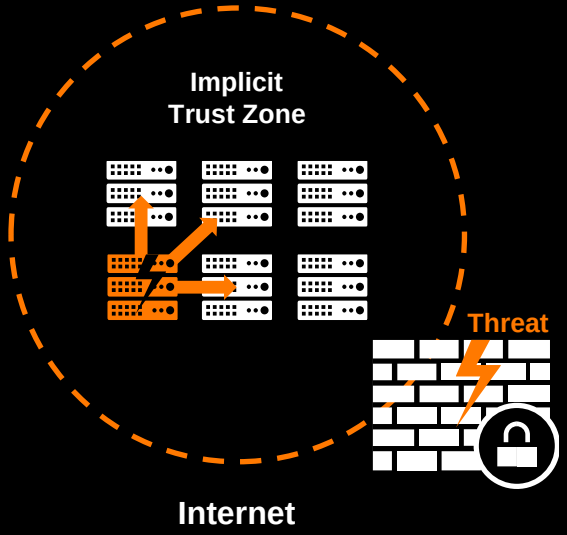
What is Zero Trust?

Zero Trust is a design ideology that state threats can be anywhere
- All networks are considered equal
There are no internal or external

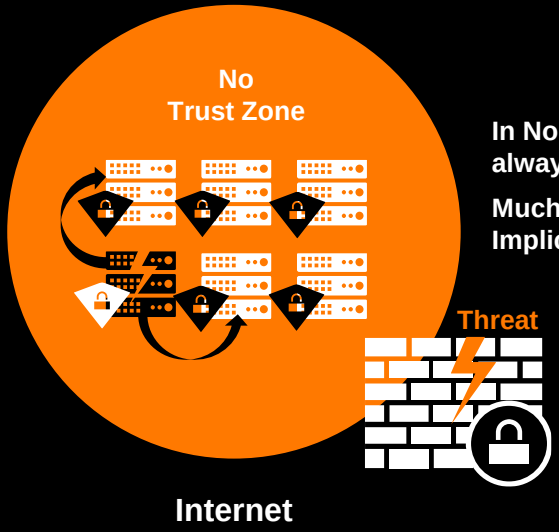
Overall goal of implementing Zero Trust:
Limit the blast radius of an attack to protect business continuity and limit the cost of it.

Zero Trust

Traditional Single Perimeter Defense



Zero Trust Defense Focuses on Resourec Protection



In No trust Zone, never trust, always verify first!

Much smaller Implicit Trust Zone

Why Zero Trust?

Secure your digital transformation

Drastically reduce attack surface

- Still to easy to be breached and work unnoticed
- Cyber Security Insurances are not the future
- Hard to find Cyber Security resources

Increase Cyber resilience - NIST

- The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

Compliance

- By 2025, 60% of organizations will use cybersecurity risk as the primary determinant in conducting third-party transactions and business relationships. (Gartner)

Top 8 Cybersecurity predictions for 2022-23

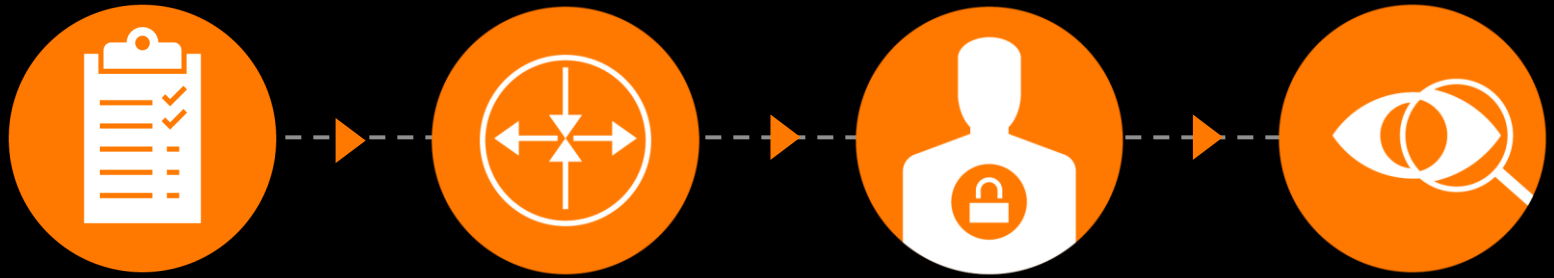
60% of organizations will embrace Zero Trust as a starting point for security by 2025. More than half will fail to realize the benefits

The term **zero trust** is now prevalent in security vendor marketing and in security guidance from governments. As a mindset — replacing implicit trust with identity- and context-based risk appropriate trust — it is extremely powerful.

However, as zero trust is both a security principle and an organizational vision, it requires a **cultural shift and clear communication that ties it to business outcomes to achieve the benefits**.

https://www.gartner.com/en/newsroom/press-releases/2022-06-21-gartner-unveils-the-top-eight-cybersecurity-predictio

Zero Trust
Design principles



Outcomes
By focusing on business, outcomes security can be seen as an enabler

Inside to out
Understand what you need to protect. Design outward from there.

Access
How and what should have access.

Inspect and log
Log and inspect all Traffic up to layer 7

5 steps to implementing Zero Trust

1

Define the protect surface.

2

Map the transaction flows.

3

Build Zero Trust architecture.

4

Create Zero Trust policy.

5

Monitor and maintain the network.

1 Define the protect surface.

Single DAAS element – Critical to your business
You will have many protect surfaces
A protect surface is much smaler compared to your attack surface

- Smaler focus
- Well defined and documented

DAAS:
Data – Sensitive data (Toxic)
Assets – Scada, Point of sales terminals, medical equipment, IoT
Applications – off the shelf or custom software
Services – DNS, DHCP, Active Directory

2 Map the transaction flows.

To properly design a network. It’s critical to understand how systems should work and how various **DAAS components** interact with other resources.

The way traffic moves across the network, specific to the data in the protect surface, determines how it **should be protected.**

3 Build a Zero Trust architecture

With your protect surface defined and flows mapped, you can then begin to build your Zero Trust architecture.

- IdP
- Networksegmention
- Microsegmentation
- VPN / Security Service Edge
- Conditional Access
- Privileged Access management

4 Create Zero Trust Policy

Context based policy to determine who or what can access to your protect surface

Who should be accessing a resource?
What application (DAAS)
When is the asserted identity trying to access the resource?
Where is the packet destination?
Why is this packet trying to access this resource
How is the asserted identity of a packet accessing the protect surface

5 Monitor and maintain the network.

Monitor and maintain the environment:

Inspect and log all traffic

The telemetry provided by this process will not just help prevent data breaches and other significant cybersecurity events but will provide valuable security improvement insights.

5 steps to implementing Zero Trust

1

Define the protect surface.

2

Map the transaction flows.

3

Build Zero Trust architecture.

4

Create Zero Trust policy.

5

Monitor and maintain the network.

How can Orange Cyberdefense help?