RÉPUBLIQUE
FRANÇAISE
*Liberté
Égalité
Fraternité*

BACK TO BASICS
ZERO TRUST MODEL

The primary objective of the Zero Trust model is to reduce the implicit trust placed in a subject requesting access to the information system (IS).

Logical access control is therefore based on:

→ **a dynamic and regular assessment of the subject** requesting access to a resource;

→ **a dynamic and regular assessment of the subject's access context**, including the security status of the device used to access the information system;

→ **the criticality of the accessed resource**, in terms of availability, integrity, and confidentiality.

Zero Trust is not a new technology or an all-in-one commercial solution. It is a security model dedicated to better securing access to an entity's resources. It uses well-known **defense-in-depth principles**, including **systematic authentication, the principle of least privilege, and micro-segmentation.**

It should be adopted in a controlled and gradual manner, at the risk of weakening the IS and giving a false sense of security.

1/ A PROCESS OF TRANSFORMATION

→ **Integrate the Zero Trust model into a defense-in-depth and risk-based approach**. ZT should not be seen as an alternative to perimeter defense, but rather as a complementary strategy.

→ **Set a transformation roadmap by precisely defining the use cases for which the Zero Trust model meets a security objective:** who, in what contexts, for what resources?

→ **Define a logical access control policy in line with the security objectives set for each use case,** based exclusively on managed attributes - i.e. attributes that the entity is capable of keeping up to date and for which it knows the scope of coverage and quality level.

→ **Construct and maintain an up-to-date mapping of applications, data, users, equipment, and flows** between each of these components, in order to implement granular, dynamic, and regular access controls.

→ **Run security and functional tests of sufficient duration before going into production,** so as to ensure the reliability of logical access control decisions and the reporting of expected alerts.

→ **Pay particular attention to the centralisation of logical access control functions,** and consider the impact of the loss of these functions' availability and/or integrity on the IS.

2/ KEY TECHNICAL PRINCIPLES

→ **Deploy an authorisation control infrastructure based on the Attribute-Based Access Control (ABAC) model**, enabling the dynamic and continuous evaluation of access requests according to:

- subject attributes (e.g. function);
- resource attributes (e.g. level of confidentiality);
- environmental attributes linked to the context of the access request (e.g. level of compliance of the means of access used in relation to the entity's security policy, time, location, etc.).

→ **Deploy an identity and credentials management infrastructure for users, automatic processes, and devices.** The lifecycle of unique accounts and credentials must be controlled and progressively automated in order to facilitate their management.

→ **Deploy an asset and vulnerability management infrastructure for automatic processes and devices.** The process of identifying deviations from the security policy and ensuring compliance must be controlled and automated (e.g. management of security patches) where possible.

→ **Deploy a security monitoring infrastructure to collect and analyse security events for each user and device.** Controlled security monitoring, i.e. with a low rate of false positives and false negatives, is an essential prerequisite for any use in access decision.

→ **Use strong multi-factor authentication mechanisms for user access**. In the ZT model, a high level of trust in the user's identity is essential.

→ **Use hardened and controlled devices when accessing the entity's critical data.** Visibility into the security status of personal devices or the trustworthiness of the information returned by this type of device is insufficient.