Microsoft Zero Trust Security

Context

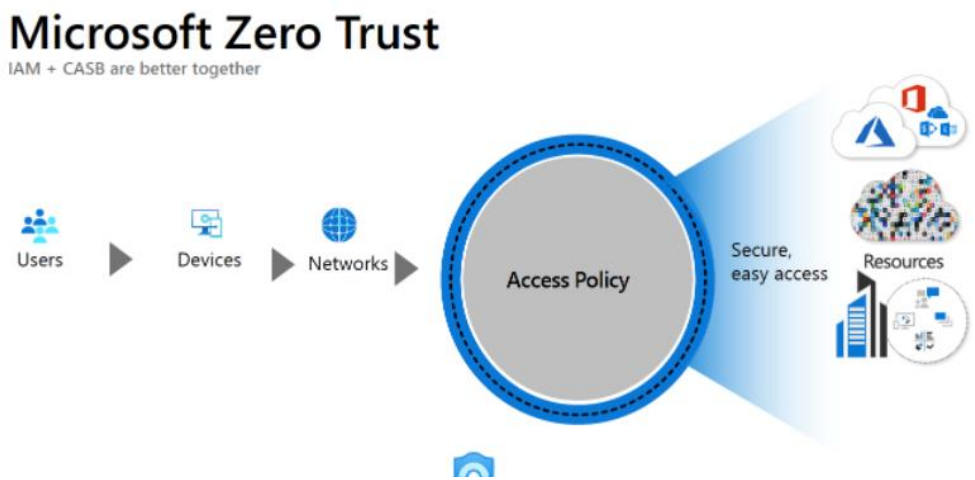
The increased use of the cloud, the growth of teleworking and the use of personal devices to access corporate information are reducing the control that enterprises have over their sensible data. At the same time, the level of threat is increasing.

In this context, traditional information security measures, such as firewalls, tenants or VPNs, are facing limitations.

The Zero Trust model overcomes these security problems by changing the concept of perimeter.

Zero Trust is primarily an architectural concept that improves the security of access to resources and services rather than a technology.

NRB can assist you to define and identify areas of efforts to move towards a Zero Trust architecture based on Microsoft solutions.



Microsoft Zero Trust Security – High Level Assessment and Recommendations

WORKSHOP Content

- Microsoft ZeroTrust Models and Concepts
- Azure AD Identity Governance
- Privileged Identity Management
- Microsoft MFA Authentication, Zero Password
- Microsoft Conditional Access
- Microsoft Access Control Overview
- Defender for Cloud Apps (CASB)
- EndPoint Review

WORKSHOP Objectives

- Improve you Security considering a Zero Trust strategy
- Define a first High-level Security Roadmap in line with your objectives

WORKSHOP Deliverables (5 days)

- Microsoft Zero Trust Introduction
- Understanding of your expectations and specificities
- Risk Mitigation
- Security Approach Roadmap high level Report
- Report and budget Presentation

Cost

- 5.000€

Please contact us to align on the scope and get an individual proposal from us