Zero Trust Journey

The increasing shift of assets and identities outside the corporate network requires stricter checks. Traditional security strategies, like the Trusted Network, are no longer sufficient to counter more advanced forms of attack.

Why do companies need Zero Trust?
Assets and identities are increasingly leaving the corporate network (BYOD, Homeoffice, Mobile & Cloud) and a growing number of internal and external users have access to corporate resources. Safeguarding their security requires directives, methods and applications for stringent, auditable user and authorisation checks. Advanced methods of attack enable identity theft, such as phishing and credential theft. Consequently, the security strategy provided by the "Trusted Network" is no longer sufficient to comprehensively protect the corporate network. Zero Trust offers a collection of policies and ideas to minimise uncertainty in enforcing reliably accurate access decisions with the least privileges per request in information systems and services. Its aim is to reduce costs caused by security incidents and prevent potential reputational damage. Our Security Consulting Team advises your company on the management and implementation of Zero Trust policies to comprehensively protect your infrastructure and business. Using our standardised procedures for introducing a Zero Trust architecture, we will guide you at your own pace to the required level of maturity.

How you benefit from a Zero Trust consultation

Creation of a roadmap and migration plan

Our experts draw up a roadmap and migration plan with strategic Zero Trust projects. ✓

Greater security – increased resilience

If Zero Trust policies are implemented consistently, attacks are averted, limited or detected earlier. ✓

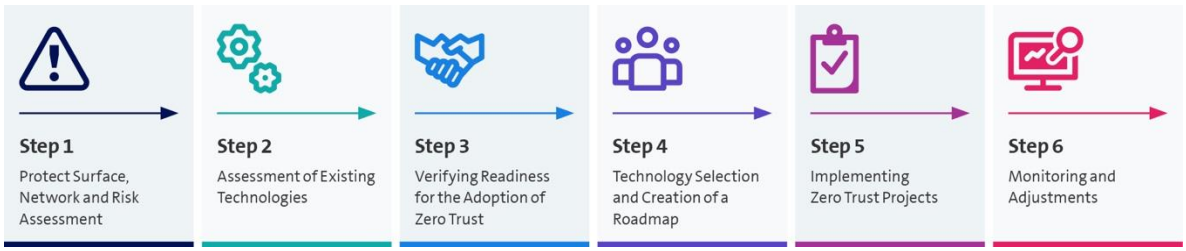
Awareness of compliance and regulatory requirements

Support in developing governance to manage Zero Trust projects. ✓

Maturity assessment

Determines your company's maturity level in terms of cultural and technology readiness. ✓

Consultation procedure for introducing a Zero Trust architecture



swisscom

Facts & Figures

Assessment & Workshops

- Customer workshops – determining the required maturity level
- Assessment of maturity and technology
  - Identifying the most important and valuable data, assets, apps and services
  - Identifying the most significant risks and the regulatory scope
  - Identifying identity and network solutions for end users and DC
- Roadmap with strategic Zero Trust projects
- Preparation of a roadmap with strategic Zero Trust projects
- Migration plan to the Zero Trust reference architecture

Awareness

- Cultural Awareness: Impact of Zero Trust on current corporate culture
  - Readiness to adopt a ZT security framework on the basis of critical resources, key risks, existing technologies and cultural factors
- Designing / implementing awareness campaigns for information security:
  - Performing security awareness training
  - Planning and implementing phishing campaigns

Project-based and organisational support

- Support in developing governance to manage Zero Trust projects and the entire Zero Trust adoption (Zero Trust Journey)
- Further developing the security organisation based on business requirements

You can find more information and the contact details of our experts at swisscom.ch/security-consulting

Swisscom (Schweiz) AG Enterprise Customers, Postfach,
CH-3050 Bern, Tel. 0800 800 900, www.swisscom.ch/enterprise