swisscom
Broadcast

Proof of Concept: Zero Trust

– Rapid Pilot (4 – 6 weeks)

Measurably higher security. Without a major IT project.

Do you want to reduce **IT security risks** caused by overly broad access, gain transparency, and pragmatically implement a Zero Trust architecture—without months-long transformation programs? With the Rapid Pilot, we implement a clearly defined Zero Trust use case in 4–6 weeks as a proof of concept—including measurement, reporting, and a basis for decision-making regarding the next steps.

You benefit from:

- Direct operationalization of Zero Trust by Switzerland's largest Cloudflare partner
- Use-case focus: fast results, low project risk, clear metrics—tailored to the Swiss market and regulations
- Cloudflare technology as the world's leading ZTNA platform

Why this Rapid Pilot?

Many organizations face the following IT security challenges:

- **Implicit trust after login**
  Traditional access methods such as VPN authenticate the user once and then grant broad network access—without continuous verification and without restriction to specific applications.

- **Third parties as an underestimated risk**
  External partners often receive more access than necessary—without device control, without granular restrictions, and with full potential for lateral movement within the network.

- **Lack of traceability**
  Granular logs, clear authentication policies, and device posture checks are missing—and with them, the foundation for robust audits.

Find out in 15 minutes if the Rapid Pilot does match with your business.

Your contact

Jean-Louis Fantino
Tel. +41 79 197 63 76
jean-louis.fantino@swisscom.com
www.swisscom.ch/zero-trust

swisscom Broadcast

Scope of Services

- PoC Scope: 1–2 applications, 1 user group (e.g., external partners or admins), 1 – 2 locations/regions
- Target scenario: clear definition of use case, risk assumptions, and success criteria
- Integration: Connection of relevant systems (e.g., identity/SSO, required access)
- Policy Design & Pilot Operation: controlled, traceable access policies
- Measurement & Reporting: KPI tracking, findings, basis for decision-making
- Decision Workshop: Evaluation of results and recommendations for Zero Trust rollout and next steps
- Policy Design & Pilot Operation: controlled, traceable access policies
- Measurement & Reporting: KPI tracking, findings, basis for decision-making
- Decision Workshop: Evaluation of results and recommendations for a company-wide Zero Trust roll-out and next steps

Excluded from the scope of services are an enterprise-wide Zero Trust rollout, app refactorings, a complete IAM overhaul, and large-scale network restructuring.

Process duration: 4–6 weeks

1. **Kickoff & Scope (Week 1)**
   Definition of scope, objectives, stakeholders, KPI benchmarks, and access
2. **Setup & Integration (Weeks 1–2)**
   Integrations, pilot group, technical foundations
3. **Policy Design & Operation (Weeks 2–4)**
   Policies, testing, controlled operation within the defined scope
4. **Validation & Decision (Weeks 4–6)**
   KPI measurement, reporting, next steps

Minimum requirements

To ensure the PoC yields results quickly, we need:

- Designated app owners and a defined pilot group, including a PoC SPOC
- Access to relevant systems (e.g., Identity/SSO) and necessary admin accounts

Weekly time commitments (rough estimates):
IT/IAM (4 hrs) | Network (4 hrs) | Security (8 hrs) | App Owner (4 hrs)

In collaboration with:

CLOUDFLARE