Intro to Zero Trust

The need for cybersecurity evolution

Alana Scott Ericsson 2021-06-14

Agenda

- What is Zero Trust/Architecture?
- 5G Transformation
- Security Transformation
- Forces Driving ZTA
- 5G ZTA Ecosystem
- Key Takeaways

What is Zero Trust Architecture?

Zero Trust

A **concept** proposed in 2010 by John Kindervag of Forrester Research that eliminates trust in digital systems based on the principle that no network user, packet, interface, or device should be trusted.

Zero Trust Architecture

(ZTA) A cybersecurity **plan** that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies.

(NIST 800-207)

No one is blindly trusted & allowed to access company assets until they have been validated as legitimate & authorized

7 tenets of Zero Trust

All data sources and computing services are considered resources.

Access is provided based on a dynamic risk-based policy.

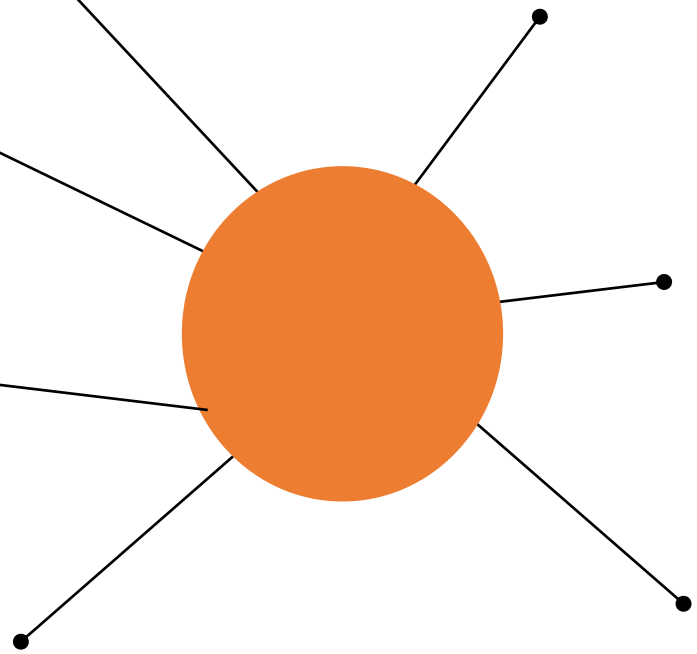
All communication is secured.

All devices should be in the most secure state possible. They should be monitored for this.

All access is provided ‘per-session’

Collect as much information about the network and infrastructure as possible.

Dynamic authentication and authorization is strictly enforced before granting access.



5G is transforming life and industry

Entertainment

Marketing

Healthcare

Military & Defense

AV Food Delivery

Service Industry

Manufacturing

Agriculture

Evolution of security approaches & architecture

Perimeter Security Model

- Operates on inherent trust
- Assumes that everything on the inside of a network is trustworthy
- Attackers able to move laterally once inside the perimeter

Zero Trust Security Model

- **Never makes assumptions about trustworthiness**
- **Operates under the assumption attackers are already inside the perimeter**
- **Prevents internal lateral movement by attackers**

The forces driving security evolution

Technology

Cloudification
Migration of network functions to the cloud creates new attack surfaces

Connectivity in everything
With 5G, the number of devices connected will expand, but so will the attack surface

Beyond the smartphone
Not all devices share the heritage of secure, hardware-based identities like SIM cards & hardware security modules

Artificial Intelligence
Machine learning for better detection of threats and breaches

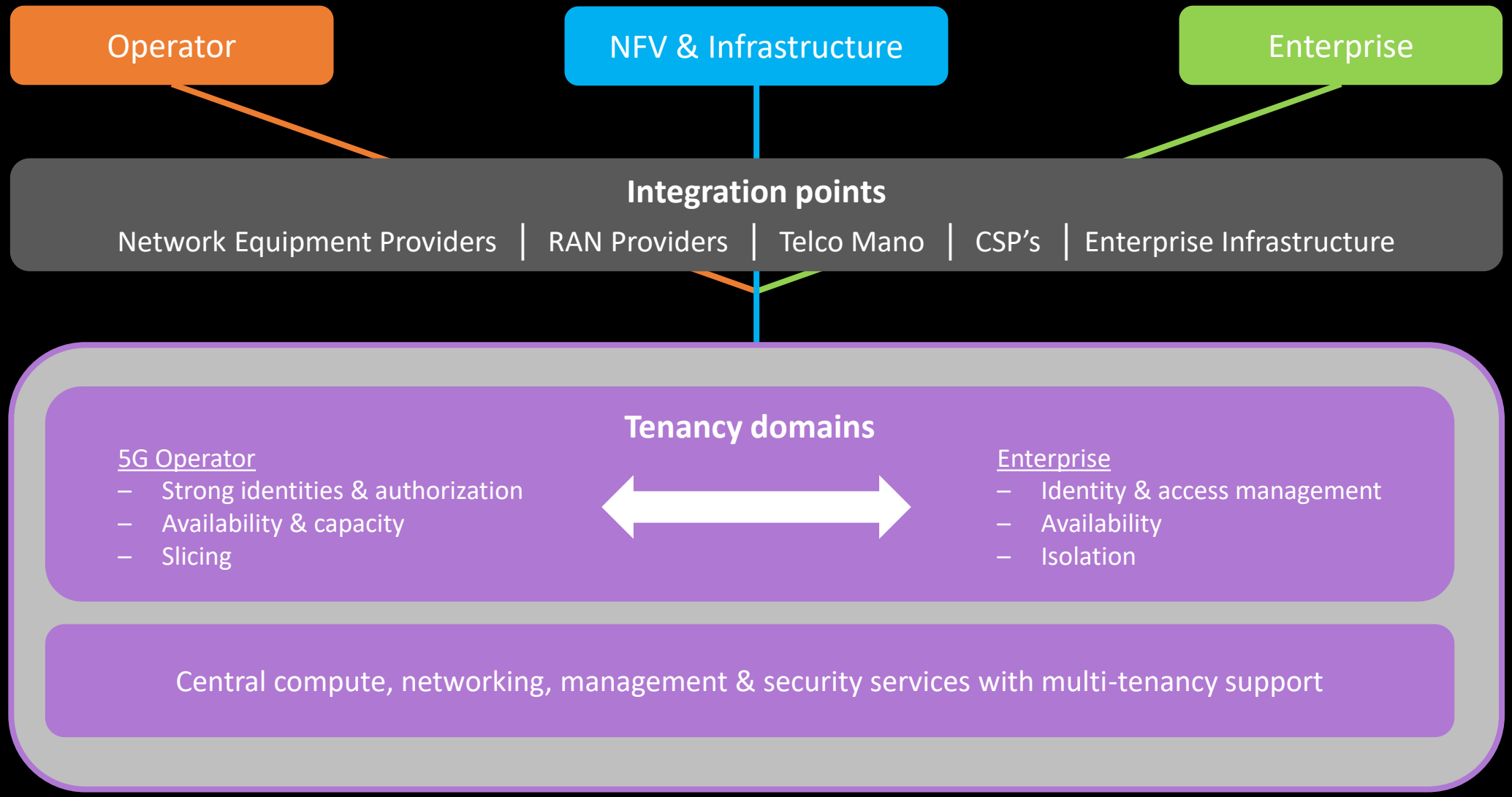
Society

High profile incidents
Colonial Pipeline, SolarWinds, Sony, etc.

Standards & Regulations
5G networks are considered national infrastructure that must be protected

Post pandemic society
Pre Covid only 30% of people WFH
Post Covid 70% of people WFH

5G ZTA ecosystem



Key insights for a successful ZTA