Risk Reduction with 5G

Ericsson Enterprise Wireless Solutions

Hosts: Peter Silva & Alex Ryan

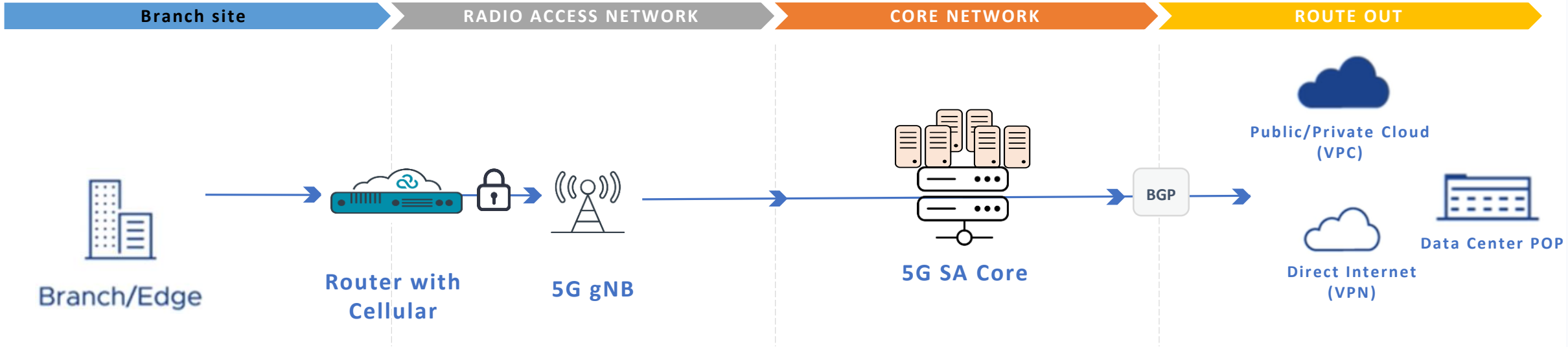
AGENDA

- WHY 5G: ENTERPRISE BRANCH TO IOT
- 5G NATIVE SECURITY AND ZERO TRUST ARCHITECTURE
- EXISTING SECURITY STACK INTEGRATION
- 5G ATTACKS IN 2023-2023 AND PREDICTIONS
- STINGRAY IN 5G IS A NO-GO

WHY USE 5G?

- HIGH BANDWIDTH, LOW LATENCY, SD-WAN
- FASTER PROVISIONING
- ESSENTIAL TO HIGHLY MOBILE AND IOT ENVIRONMENTS
- 5G NATIVE SECURITY
- HIGHLY SCALEABLE MANAGEMENT SOLUTIONS

5G Native Security



Data in transit

- MFA with standardized on Extensible Authentication Protocol (EAP)
- Zero Trust Microservice enabling them

SD-WAN

Router has multiple WAN connections Cellular, fiber, wire

Advanced integrity protection of the user plane

User plane traffic includes integrity checks (hashing) to mitigate man-in-the middle attacks

Improved core network agility and security

Network functions authenticated (OAuth2) and encrypted (TLS)

Network Slicing for traffic isolation

Expanded roaming security

User plane data is protected by GPRS Tunneling Protocol (GTP).

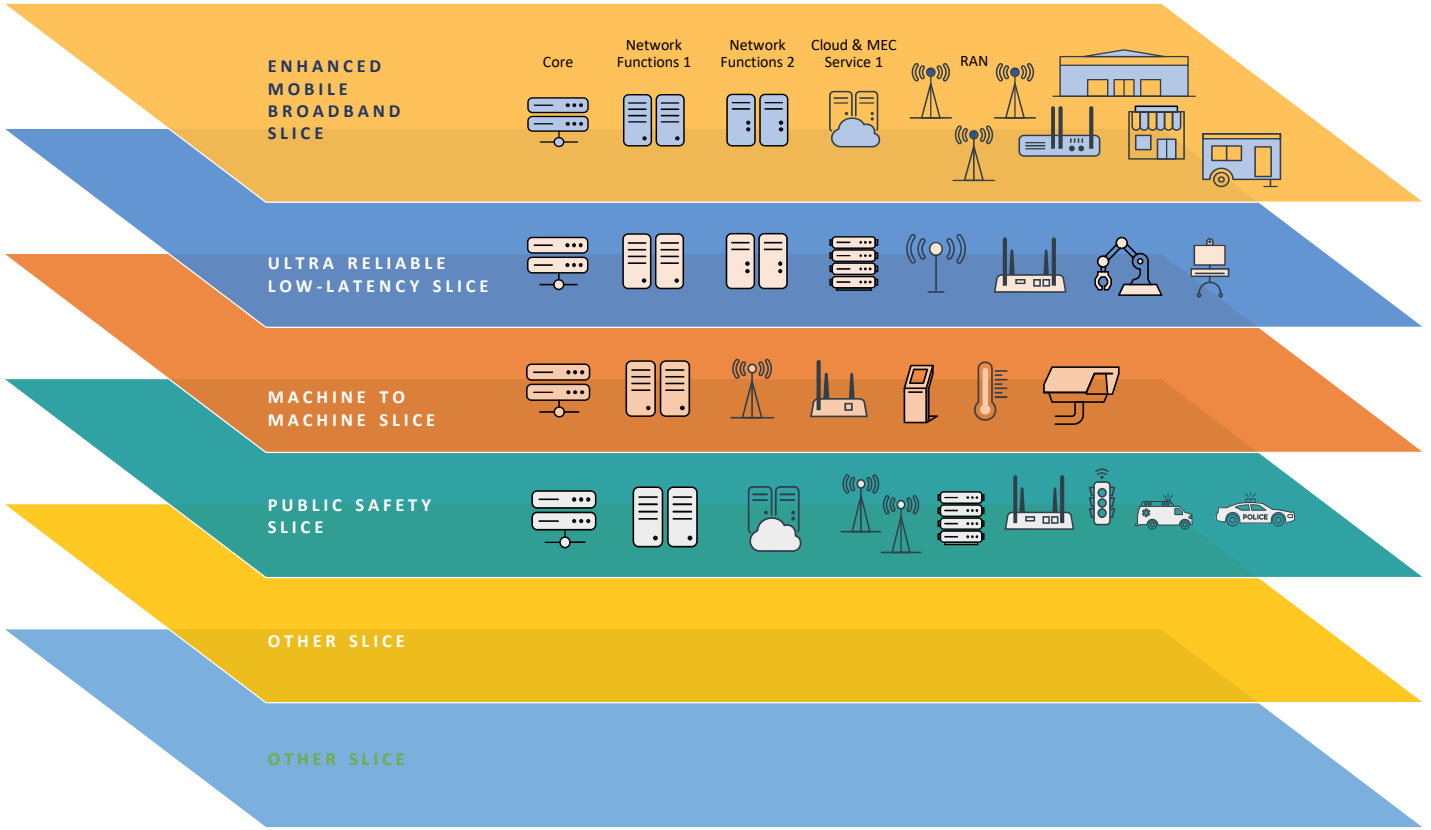
ATTACK SURFACE REDUCTION

Network Slice Selection Function (NSSF):
Network Slicing (VLAN-like)

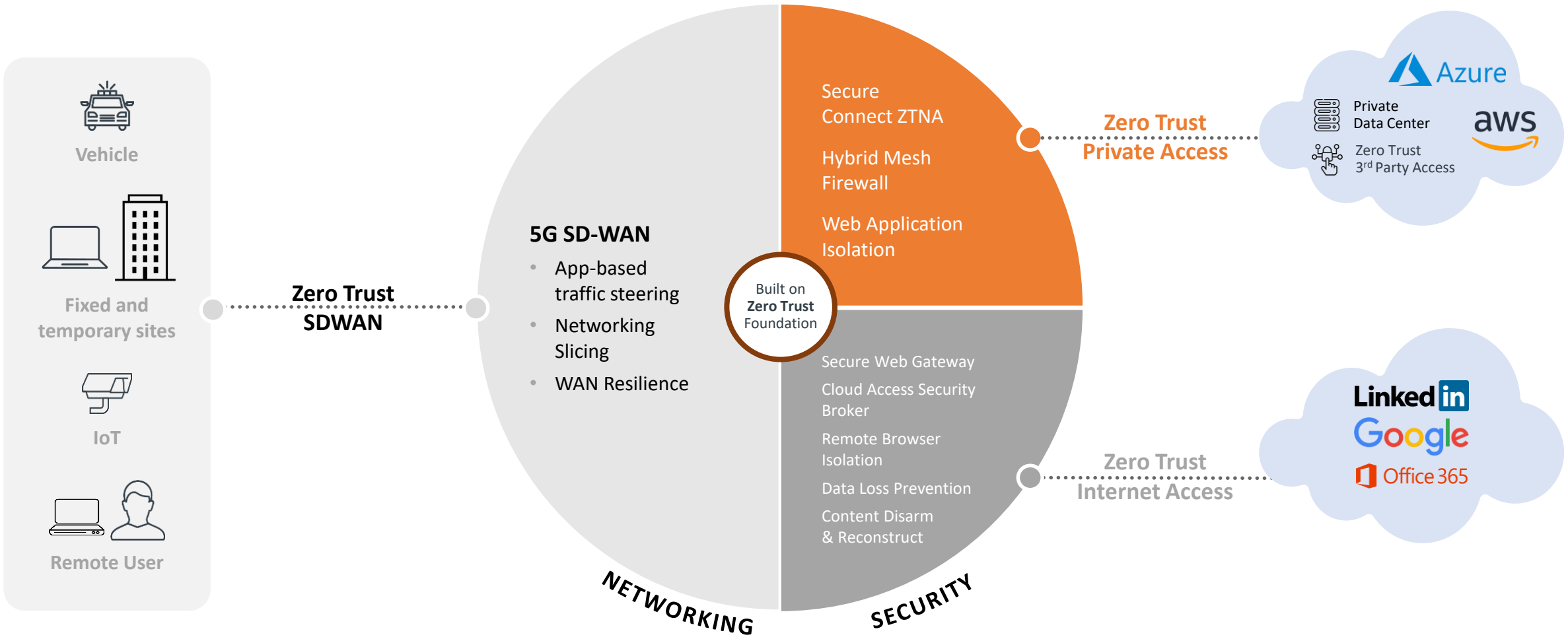
Access & Mobility Management Function (AMF):
EAP authentication

Capability Exposure Function (NEF):
API for cellular WAN device management at scale such as security policy and configurations by group.

5G SA NETWORK SLICING



NetCloud SASE Services



“Is 5G Secure?” FUD Removal Funnel

WHAT VERSION OF G?	4G, 5G Non-Standalone (NSA) 5G Standalone (SA)
WHERE IN THE DATA FLOW IS THE VULNERABILITY?	SIM swapping / SIM Card PIN and IMEI Lock Base station impersonation / VPN Integration technology / assess their controls
WHAT TECHNOLOGY HAS THE FLAW?	Identity provider issue / Federated ID backup API authentication / Assess use requirements
WHAT IS THE LIKELIHOOD? THREAT X IMPACT	Likelihood given your deployment and exposure Impact on your organization's security posture (i.e. accepted risk)
WHAT SECURITY CONTROLS MITIGATE THE RISK	Zero Trust Architecture MFA using authentication application Document residual risk

5G ATTACKS 2023-2024

AKA BYPASS	Downgrade attack, requires local presence Enforce protocols and security settings
BASEBAND HARDWARE VULNERABILITIES	Cellular antenna to transmit data, requires local presence Data encryption is complete before transit
RAN HARDWARE VULNERABILITIES	Requires local presence, 5G authentication controls Data encryption by IPsec/GRE tunnel
WHAT IS THE LIKELIHOOD? THREAT X IMPACT	Requires physical proximity and downgrade attack If data in transit is encrypted by IPSec/GRE, then the impact is a denial of service.
WHAT SECURITY CONTROLS MITIGATE THE RISK	Zero Trust Network Access with 5G slicing Use microtunnel IPSec/GRE encryption for data in transit

5G ATTACK PREDICTIONS: ECOSYSTEM

THIRD PARTY MANAGEMENT	At scale management platforms for IoT devices
API CONNECTIVITY TO 5G CORE	Stolen credentials, API key leakage, no key rotation
CELLULAR HARDWARE	Carrier hardware Cellular device hardware
BREAKING ENCRYPTION	Using advanced decryption technology such as quantum computing

GLOBAL LEADER IN SORTING MACHINES

Zero Trust Private Access

Challenges

- Provide sorting services for recycling companies, agriculture companies
- Hundreds of different customers globally
- Employees, contractors and subcontractors coming in remotely and on-premises and need access to OT system for remote monitoring/ maintenance

Solution

- NetCloud ZTNA

Results

- IdP integration to track subcontractor access; might only work for a couple of weeks
- Auditing capabilities down to the flow level to track who is trying to access what.

Stingray

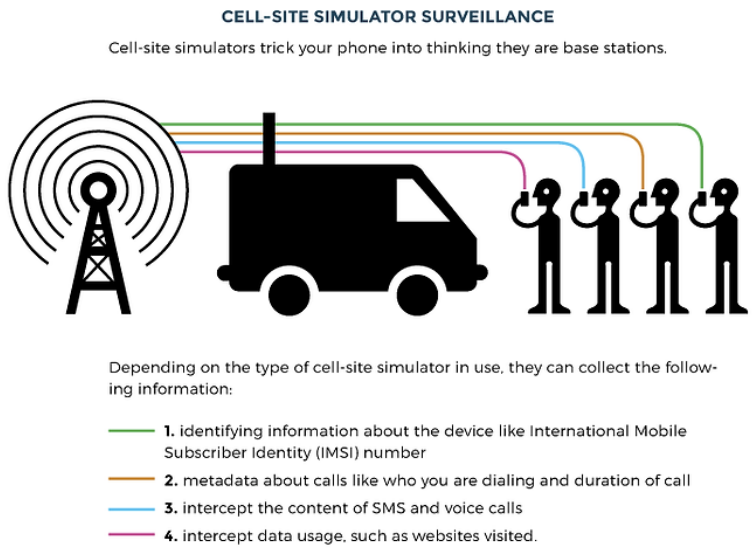


Image credit hackers-arise.com

- 5G ENCRYPTS IMSI, USES DYNAMIC SUCI
- 5G ENCRYPTION AES-ALGORITHMS
- 5G AUTHENTICATION KEY DURING ATTACHMENT
- DISALLOW DOWNGRADE TO 4G
  ENCRYPT DATA BEFORE SENDING

Resources

- ERICSSON ENTERPRISE WIRELESS THREAT INTELLIGENCE BLOG
- WWW.5GAMERICAS.ORG
- CISA.GOV/5G
- THREAT RESEARCH KEYWORDS
  - CELLULAR WIRELESS WAN
  - MOBILE SERVICE PROVIDER
  - TELECOMMUNICATIONS
  - 5G / STANDALONE
  - IOT CELLULAR WAN

Sources

- Cracking the 5G Fortress: Peering Into 5G's Vulnerability Abyss
- VPN & Private APN Replacement with Zero Trust Architecture - YouTube
- **“NUTHIN BUT A G THANG EVOLUTION OF CELLULAR NETWORKS”**
  TRACY MOSLEY, DEFCON 31

Thank you!