2020
NetSec-KR

5G 엣지 보안

- MEC 보안을 중심으로 -

출처:게티이미지뱅크, 무단 전재 및 재배포 금지

한국전자통신연구원 정보보호연구본부
박 종 근 (queue@etri.re.kr)

2020. 7. 16.

ETRI
한국전자통신연구원

출처:게티이미지뱅크, 무단 전재 및 재배포 금지

목 차
CONTENTS

5G+ 융합서비스 동향

5G는 산업구조 혁신을 통해 新 스마트 비즈니스 모델 및 산업 생태계를 창출하는 4차 산업혁명의 핵심 인프라

기술적 측면

유선 대비 인프라의 유연성, WiFi·LTE 대비 통신품질 및 전송지연 개선으로 융합서비스의 디지털혁신 추구 가능

경제·산업적 측면

5G 기반 디지털 융합산업의 글로벌 매출은 '26년경 1.3조 달러, 국내 경제 파급효과는 '30년경 47.7조원

사회·정책적 측면

「혁신성장을 위한 5G+ 전략」을 통해 국민 실생활과 밀접한 5대 핵심 융합서비스 선정 및 조기상용화 추진

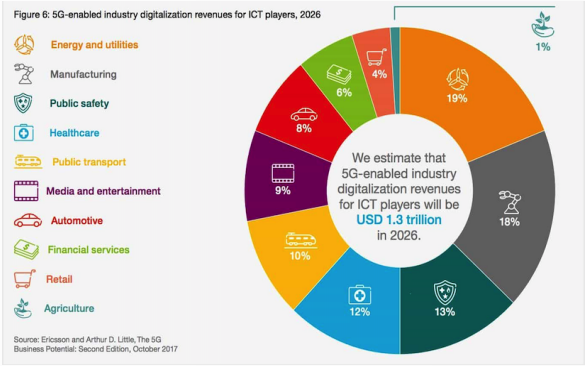
"5G B2B 新시장 창출"
(Private 5G Network 포함)

"5G 엣지에서의 안전한 이용환경 보장 필수"

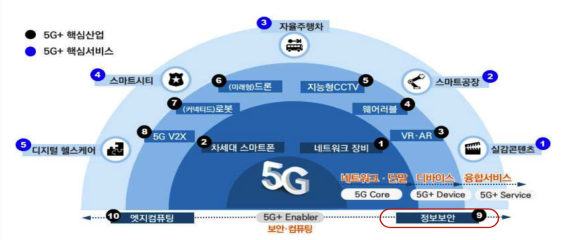
*참고: 관계부처합동, "5G 기반 스마트공장 고도화 전략(안)", 2019.10. / 한국무역보험공사, "5G 및 이동통신산업 동향 분석", 2018.11. / 관계부처합동, "혁신성장을 위한 5G+ 전략", 2019.04.08.

특성	유선 (TSN)	4G (LTE-A)	WiFi (802.11ax)	5G
이동성	X	O	O	O
전송지연	1ms	20~60ms	2~200ms	1ms
QoS 보장	O	O	X	O
최고전송속도	10 Gbps	1 Gbps	1.2 Gbps	20 Gbps
최대연결기기	-	100,000/km²	-	1,000,000/km²
에너지효율	-	1x	-	100x
설치·유지보수	복잡	단순	단순	단순

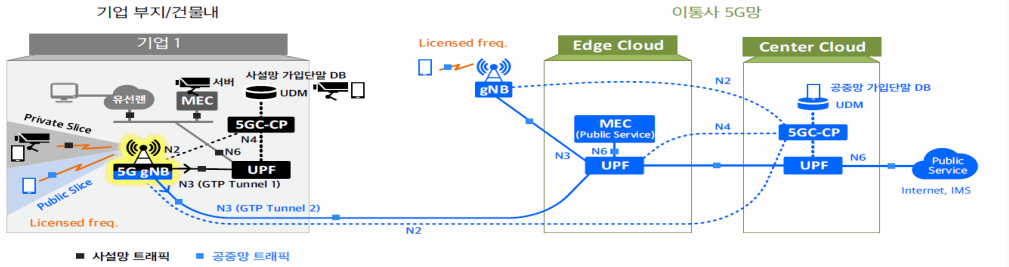
5G 기술의 특성 비교



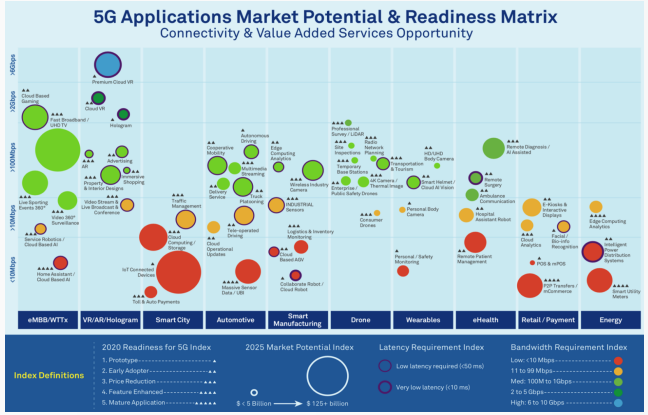
2026년 5G 기반 디지털 융합산업 글로벌 매출 전망 (에릭슨)



정부의 5G+ 전략상 5대 핵심서비스와 10대 핵심산업



Private 5G Network 서비스 구조 예시 (넷매니아즈)



5G 융합서비스 잠재시장 규모 및 준비도 (화웨이)

5G 보안 위협 동향

IMT-2020 비전 및 요구사항 충족을 위한 구조적 환경 및 서비스 특성 변화에 따른 새로운 잠재적 위협 존재

접속 환경 다변화
이동통신·WiFi 등 다양한 접속기술을 통해 수많은 다양한 종류의 센서·기기가 연결

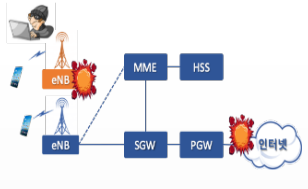
네트워크 소프트웨어화
SDN/NFV 기술을 통해 마치 프로그래밍하듯 네트워크 인프라와 서비스를 설계, 구축, 운용, 관리

분산 네트워크 구조화
네트워크 가상화와 MEC의 확산으로 SW 중심 네트워크 장비나 응용이 네트워크 전역 어디에든 설치, 운용

"공격접점 급증"
(Attack Surface)

"보안관제 및 대응 한계 직면"

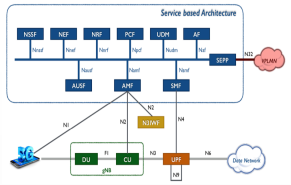
4G LTE 보안위협



3GPP 표준 기술 규격이 강화되었으나, 일부 위협은 여전히 5G에서도 유효함

- 무선재밍 공격
- 가입자 IMSI 탈취
- 허위기지국을 통한 중간자 공격
- 위치 추적
- 서비스 장애나 3G 강등
- 상호접속 프로토콜 (Diameter) 취약점 활용

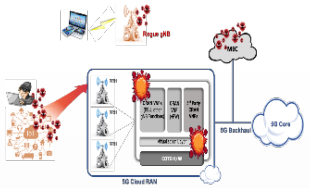
5G 코어망 보안위협



네트워크 가상화 및 서비스 기반 구조(SBA) 도입에 따른 새로운 위협 존재

- SDN/NFV 인프라 취약점 공격
- SBA 인터페이스 공격
- 5GC 제어 기능 이미지의 조작이나 감염
- 공유자원 고갈 위험
- 공개 소프트웨어 취약점 악용한 공격

5G 엣지 보안위협



초연결·초저지연 서비스 접속 및 MEC 도입에 따른 새로운 위협 존재

- 대규모 단말 동시 접속에 따른 서비스 거부 공격
- MEC 응용을 통한 악성코드 감염 또는 민감정보 유출
- 무선 및 공유자원 고갈
- 네트워크 슬라이싱 침해 공격

5G 단말 보안위협

다양한 종류의 대규모 센서·기기의 접속에 따라 단말 취약점 활용 가능

- 디바이스의 펌웨어나 SW의 악의적 변경
- 보안 기능이 탑재되지 않은 단말의 취약점 활용 공격

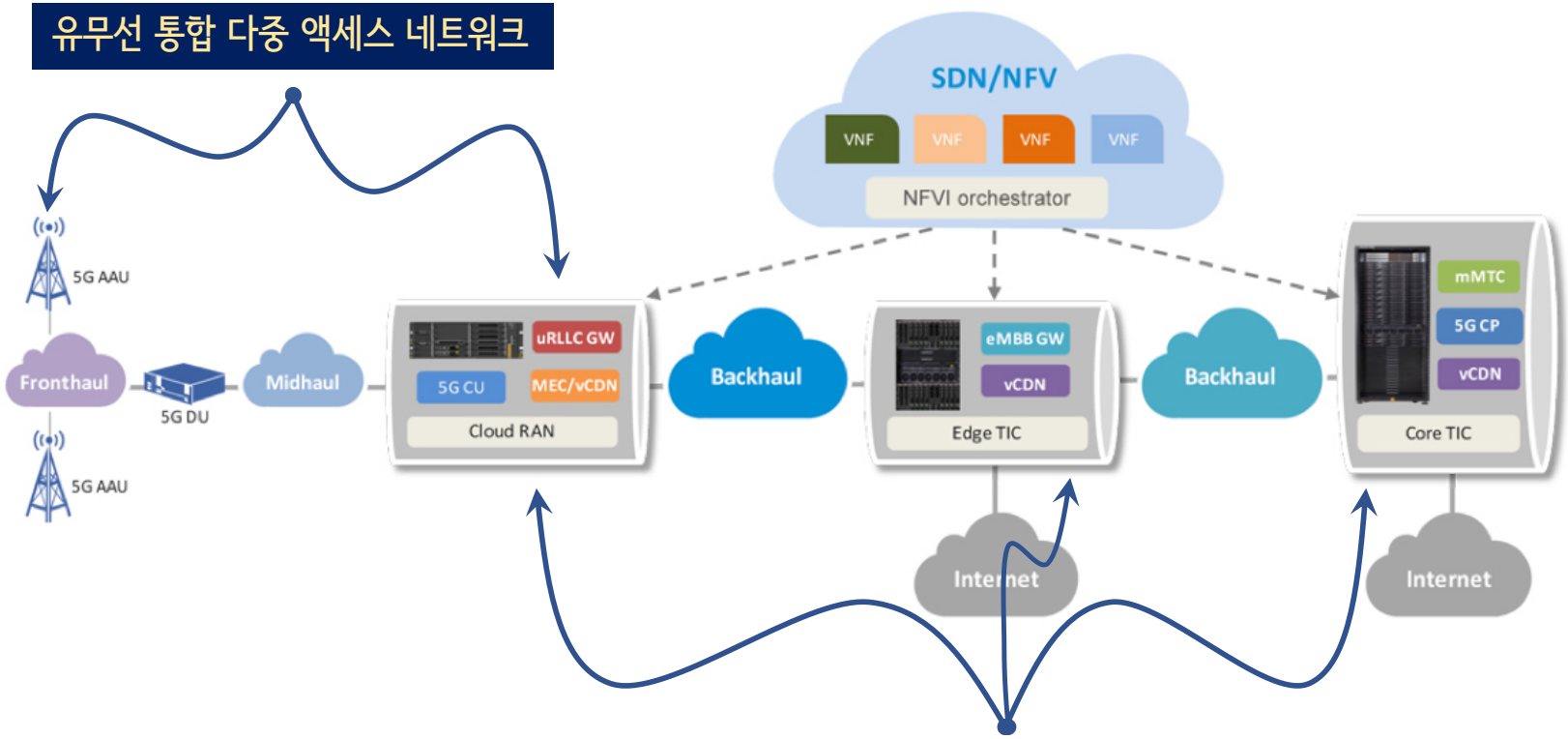
[NetSec-KR 2020] 5G 엣지 보안 기술

5G Challenges

수많은 다양한 종류의 센서·기기 연결

유무선 통합 다중 액세스 네트워크

본격적인 네트워크 인프라 가상화



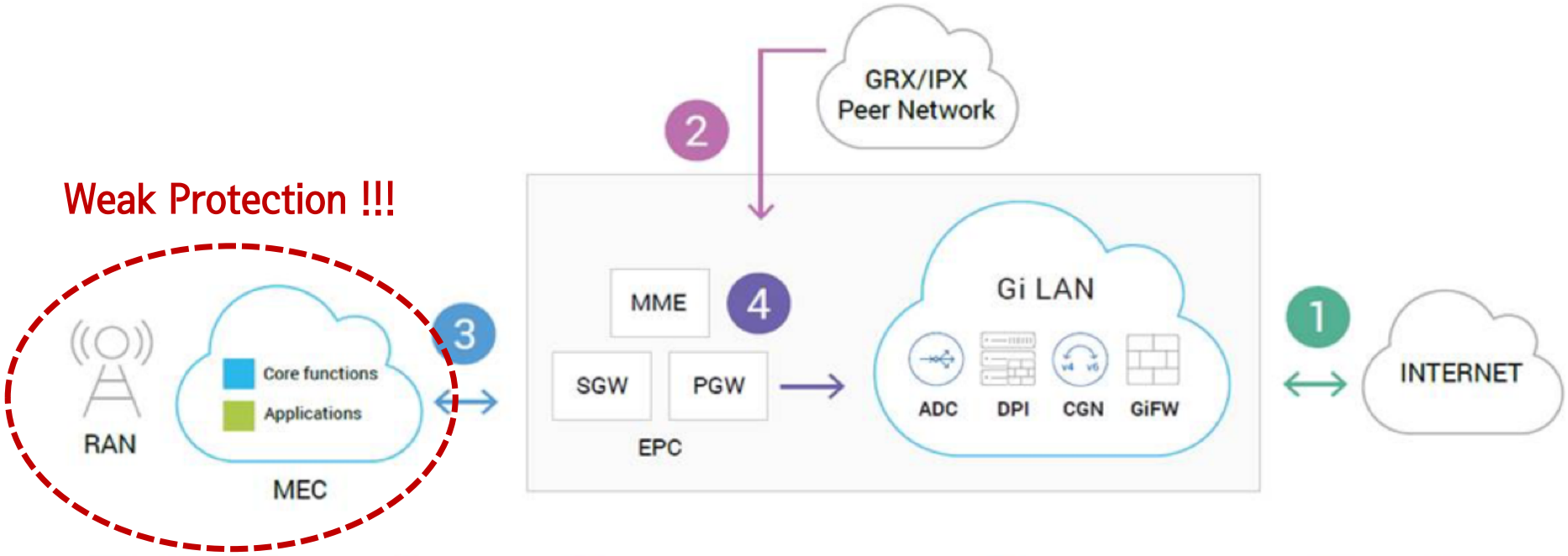
서로 다른 품질 특성을 갖는 다양한 서비스 융합

네트워크 코어 기능의 분산 배치

※ 그림출처: ZTE

5G 보안 이슈

코어망 경계 보안 중심의 보안 위협 대응 한계



1 Gi Firewall: Gi/SGi LAN Protection
Anti DDoS Protection

2 GTP/SCTP Firewall
- S8 Interface - GRX/IPX Protection
- S5 Interface - EPC Protection

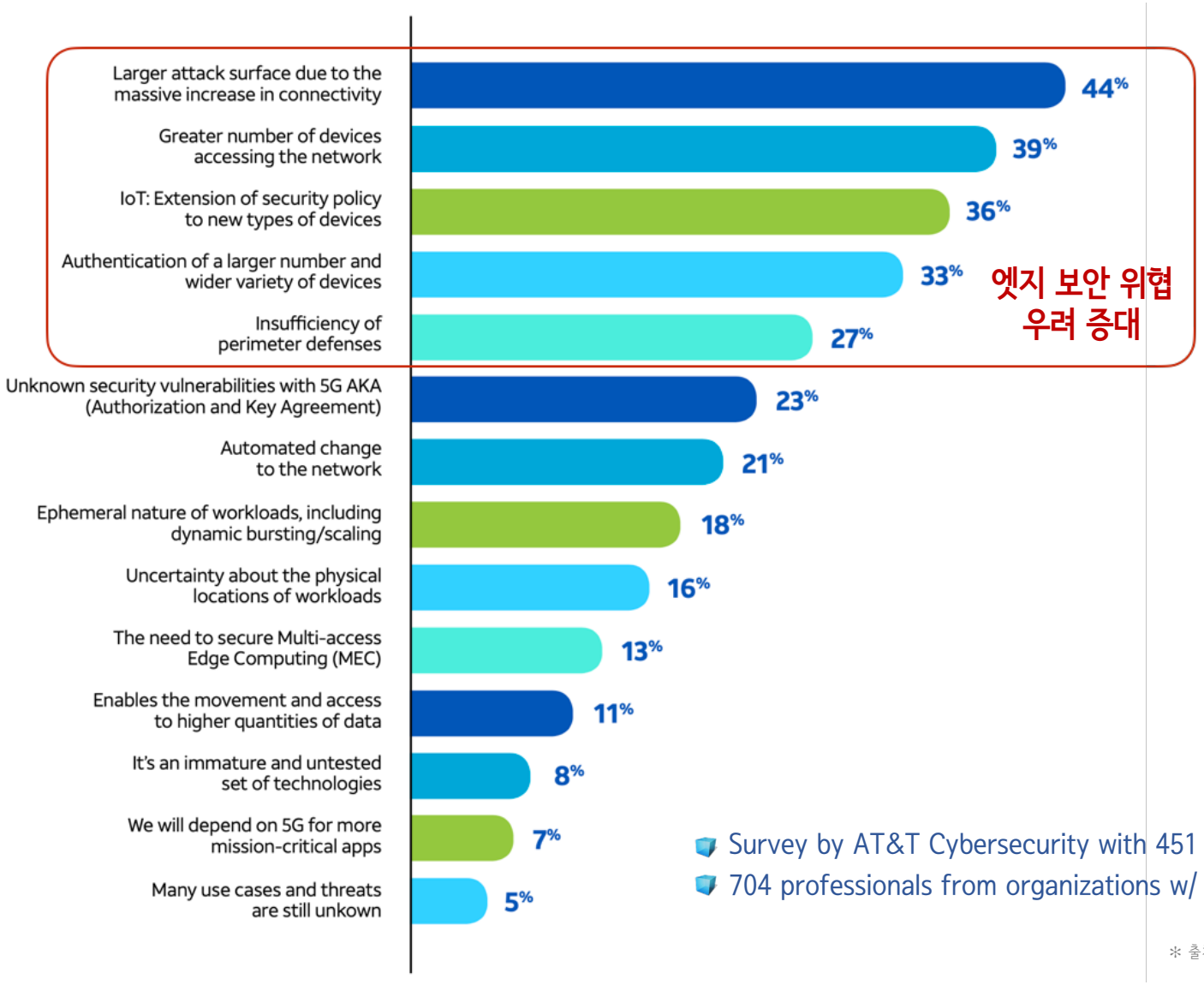
3 IPsec VPN for Mobile
Backhaul Protection

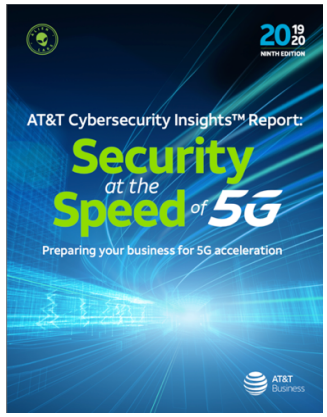
4 MME Protection

※ 그림출처: A10 Networks

5G 보안 이슈 - AT&T 5G Security Survey -

Top 3 5G Security Concerns



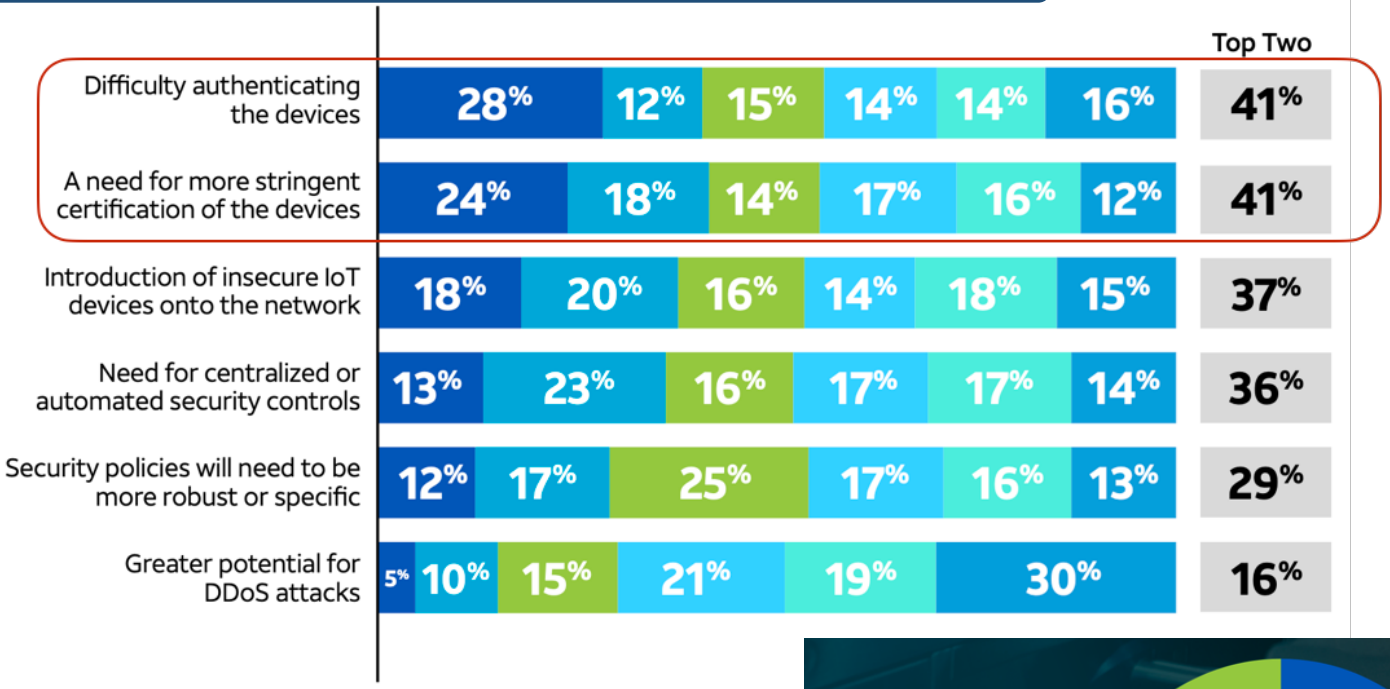


- Survey by AT&T Cybersecurity with 451 Research during '19.08.~'19.09
- 704 professionals from organizations w/ more than 500 employees

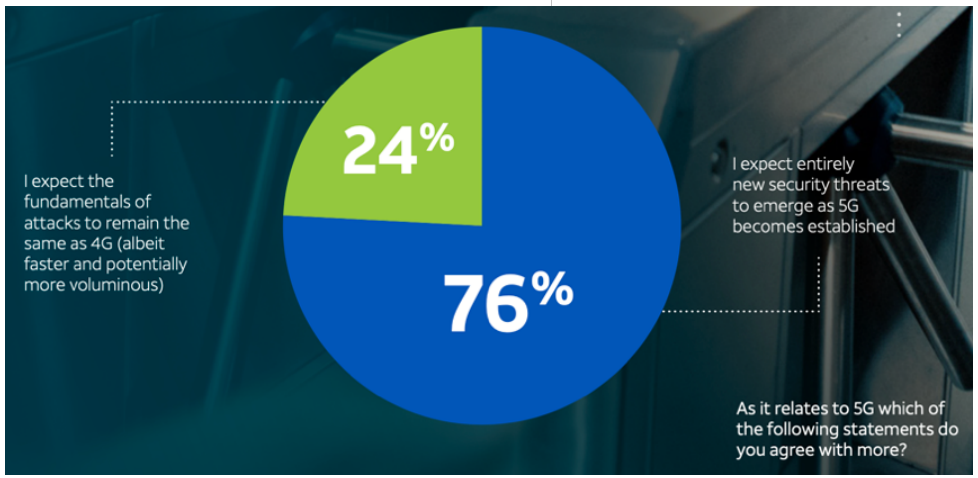
※ 출처: AT&T Cybersecurity Insights Report, 2019

5G 보안 이슈 - AT&T 5G Security Survey -

Most Important Challenges of New Devices under 5G



5G Security Perception



* 출처: AT&T Cybersecurity Insights Report, 2019

MEC 개념

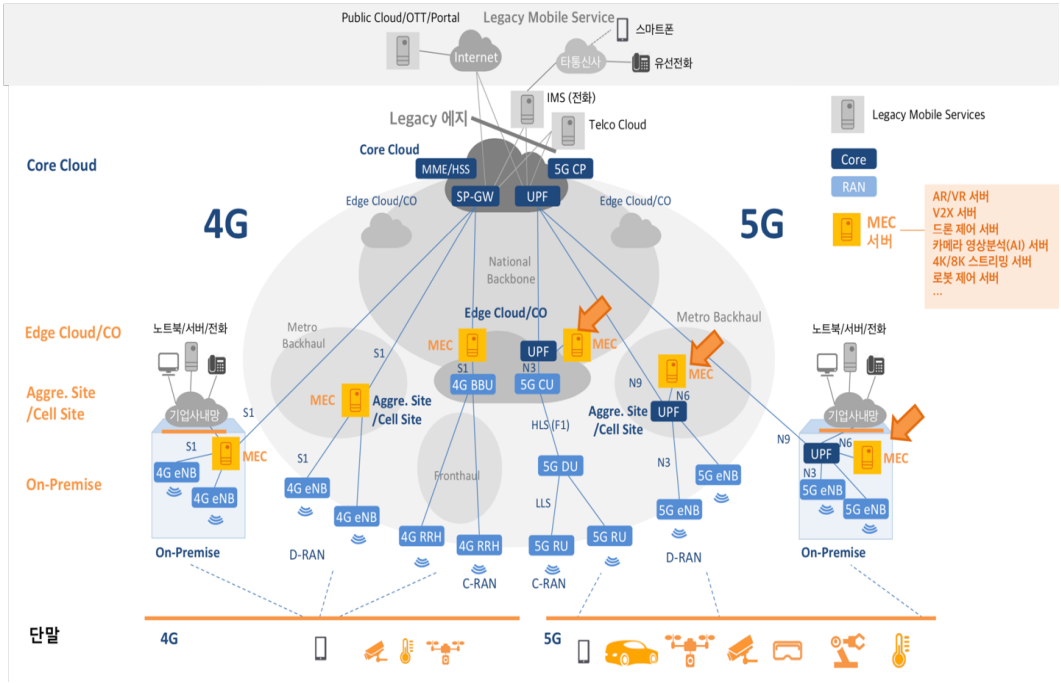
System which provides an IT service environment and cloud-computing capabilities at the edge of an access network which contains one or more type of access technology, and in close proximity to its uers [ETSI GS MEC 001, V2.1.1, 2019.01]

MEC 위치

- C-RAN (cell site)
- 지역/광역 국사
- 서비스 핫스팟
- 고객사내망 내부 등

MEC 특징

- 근접성 (Proximity)
  - 네트워크 지연시간 단축 및 백홀 대역폭 감소
- 위치기반 (Location Awareness)
  - 특정 지역 또는 기업별 맞춤형 특화 서비스 제공
- 고품질 서비스 (Quality of Experience)
  - RAN 상황정보를 활용한 전송 품질 조절 및 컨텐츠 캐싱 등 맞춤형 서비스 제공



※ 그림출처: 넷매니아즈

MEC 기술 이슈

이동성 (Mobility)

MEC 서비스 연속성 보장을 위해 사용자 이동시, MEC 응용의 이동성(migration)을 위한 핸드오버 처리 필요

자원제약 (Limited Resources)

중앙 클라우드 대비 상대적으로 제한된 자원의 효율적 관리가 요구됨

협업 (Collaboration)

사용자 핸드오버 및 응용 이동 등을 지원하기 위해 MEC 서버 간의 협업이 요구됨

정보보호 (Privacy and Security)

사용자 및 다양한 IoT 단말의 정보가 저장/처리됨에 따라 정보유출 및 사이버공격 대응 필요

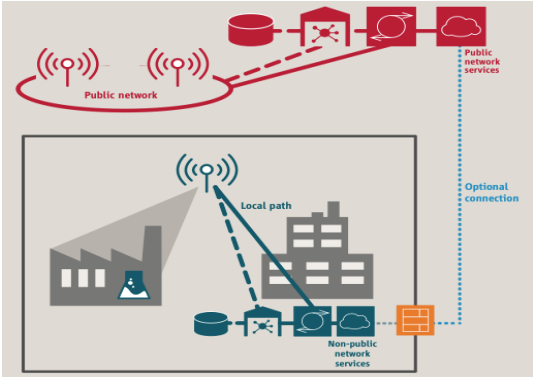
이식성 (Portability)

핸드오버 등으로 인해 MEC 응용이 서로 다른 MEC 서버에서도 실행될 수 있어야 함

5G Non-Public Networks (NPNs)

A NPN provides 5G network services to a clearly defined user organization or group of organizations. The organization deploys on its defined premises, such as a campus or a factory.

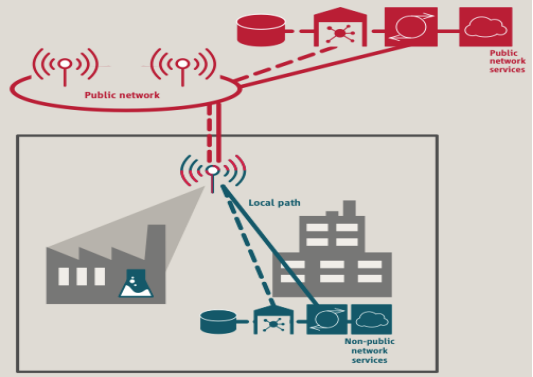
Standalone NPN



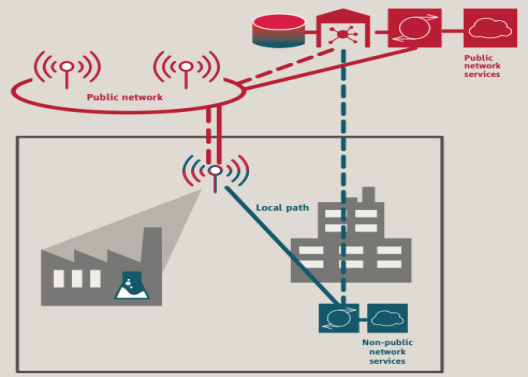
- 물리적 독립망 환경
- 높은 보안성
- 높은 CapEx / 낮은 OpEx
- 맞춤형 환경 용이
- 운용 전문성 요구

- 논리적 분리 환경
- 낮은 보안성
- 낮은 CapEx / 높은 OpEx

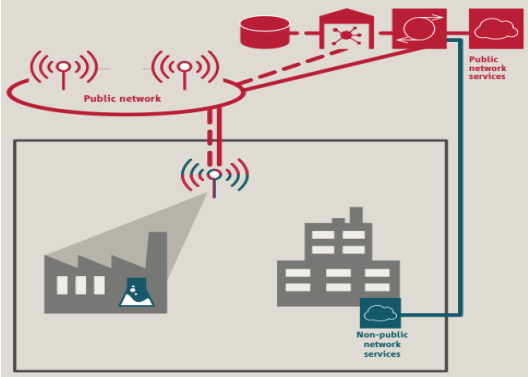
Public Network Integrated NPN



Shared RAN



Shared RAN & CP



NPN hosted by Public Network

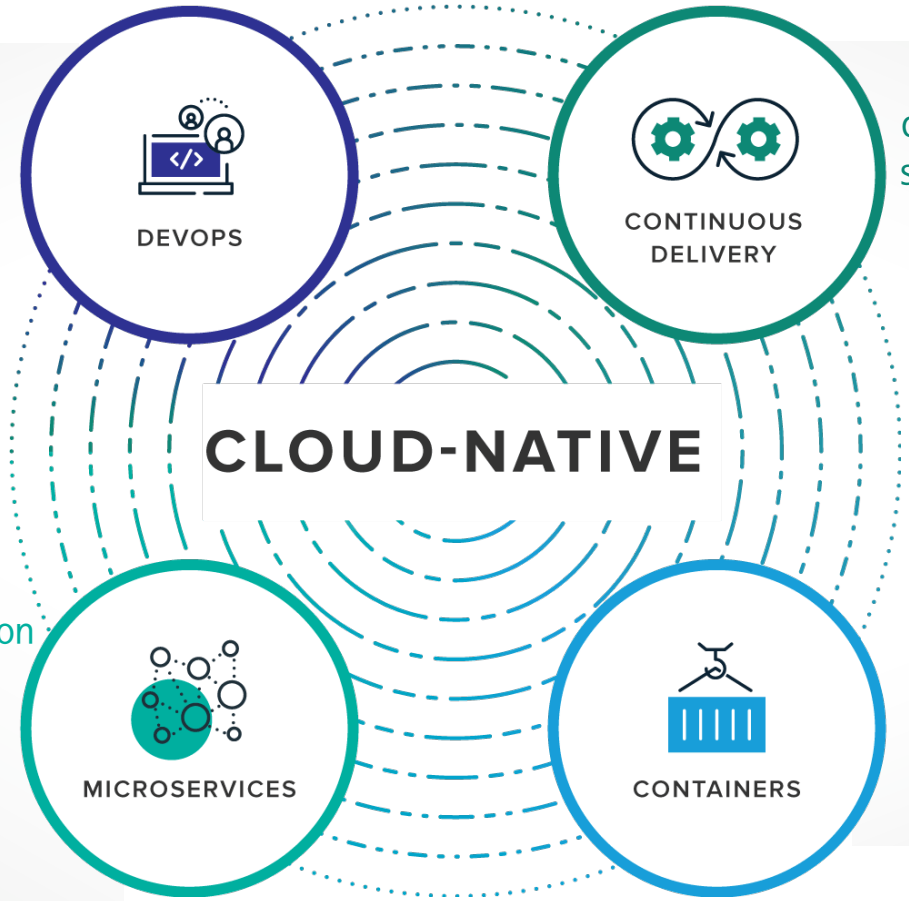
※ 출처: 5G-ACIA, "5G Non-Public Netowrks for Industrial Scenarios", 2019.7.

클라우드 네이티브

개념

- 유연성 · 확장성 · 가용성 등 클라우드 컴퓨팅 환경의 장점을 활용하기 위한 응용의 개발 및 운용 접근방법

The collaboration b/w Dev and Ops with the goal of constantly delivering high-quality SW that solves customer challenges



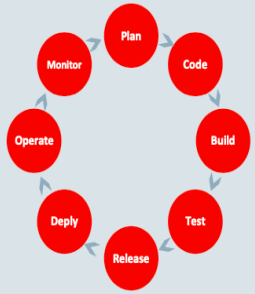
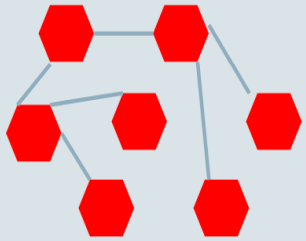
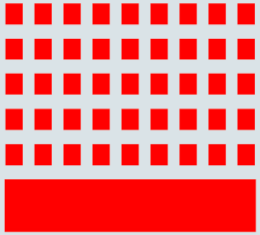
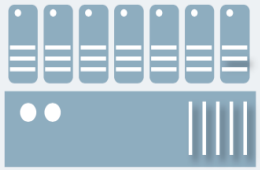
CD, enabled by Agile product development practices, is about shipping small batches of SW to production constantly, through automation

An architectural approach to developing an App as a collection of small services.
Each microservice can be deployed, upgrade, scaled, and restarted independent of other services in the App.

Containers using OS-level vritualization offer both efficiency and speed compared with standard VMs

*그림출처:https://tanzu.vmware.com/cloud-native

클라우드 네이티브 특징

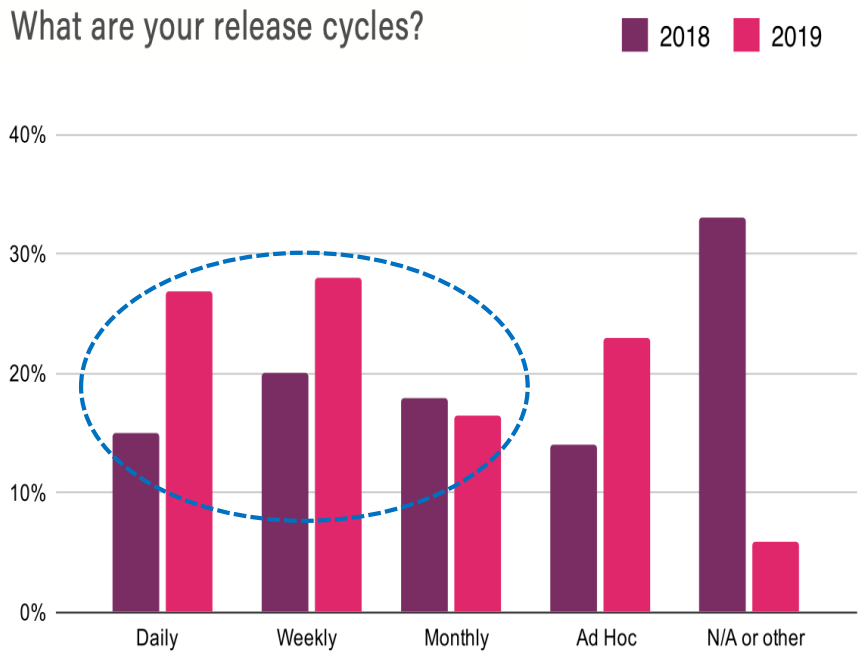
Development Process	Application Architecture	Deployment and Packaging	Application Infrastructure
DevOps 	Microservices 	Containers 	Cloud 
Agile 	N-Tier 	Virtual Servers 	Hosted 
Waterfall 	Monolithic 	Physical Server 	DataCenter 

*그림출처:Oracle

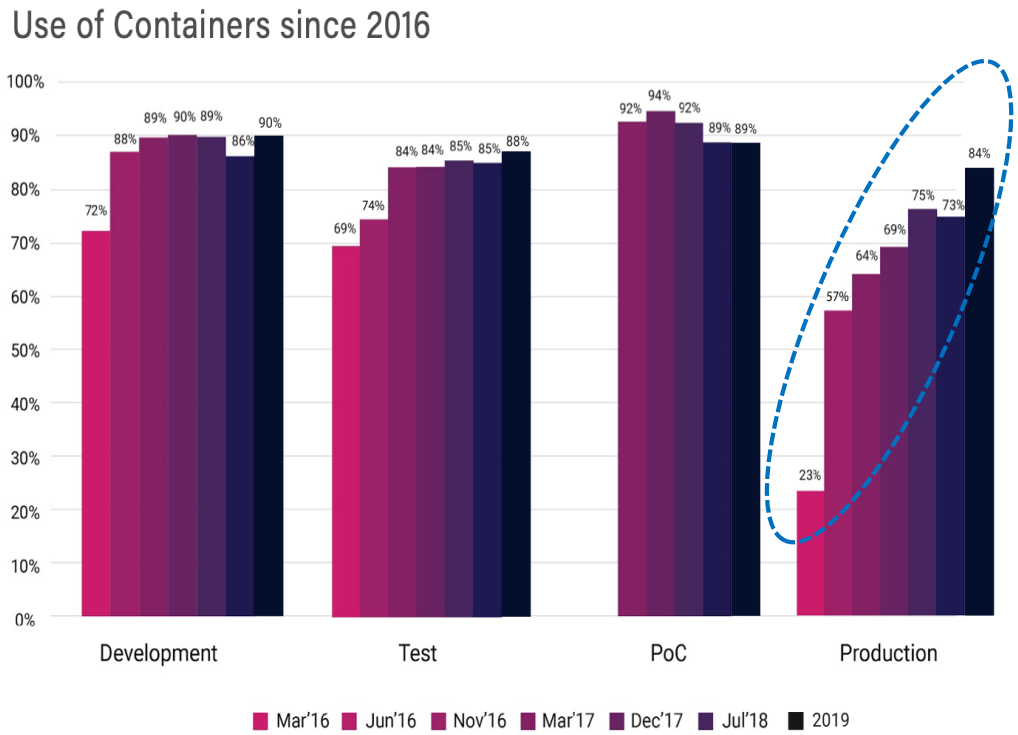
클라우드 네이티브 확산 - CNCF Survey -

주요 설문 결과

- 소프트웨어 배포 주기 가속화: 매일(15% ➤ 27%), 매주(20% ➤ 28%), 매월(18% ➤ 16%)
- 컨테이너 기반 응용 상용화 응답자 비중 증가 (23% ➤ 73% ➤ 84%)



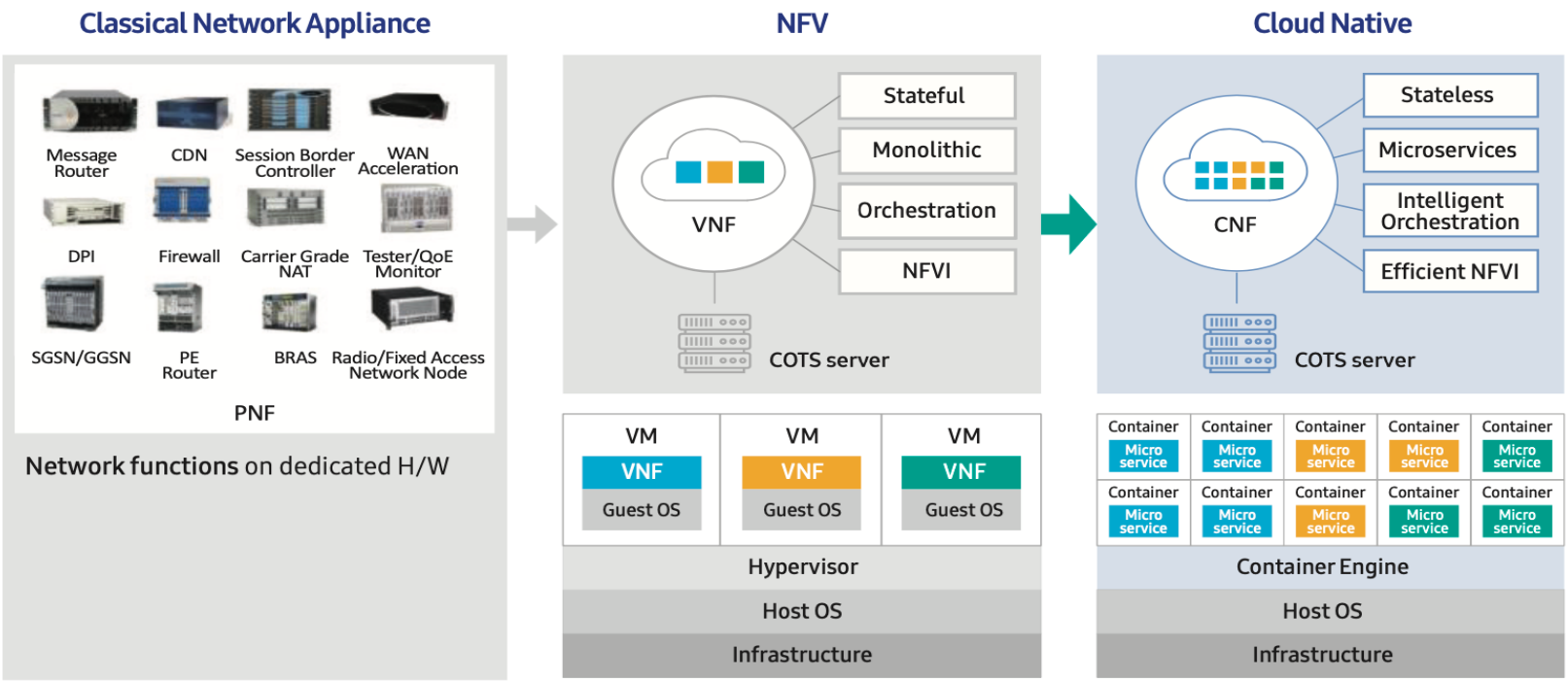
*Responses were multiple choice in 2019 vs. fill in the blank in 2018



Survey of CNCF's community during '19.09.~'19.10 with 1,337 responses

*출처:CNCF Survey 2019, https://www.cncf.io/wp-content/uploads/2020/03/CNCF_Survey_Report.pdf

클라우드 네이티브로의 진화

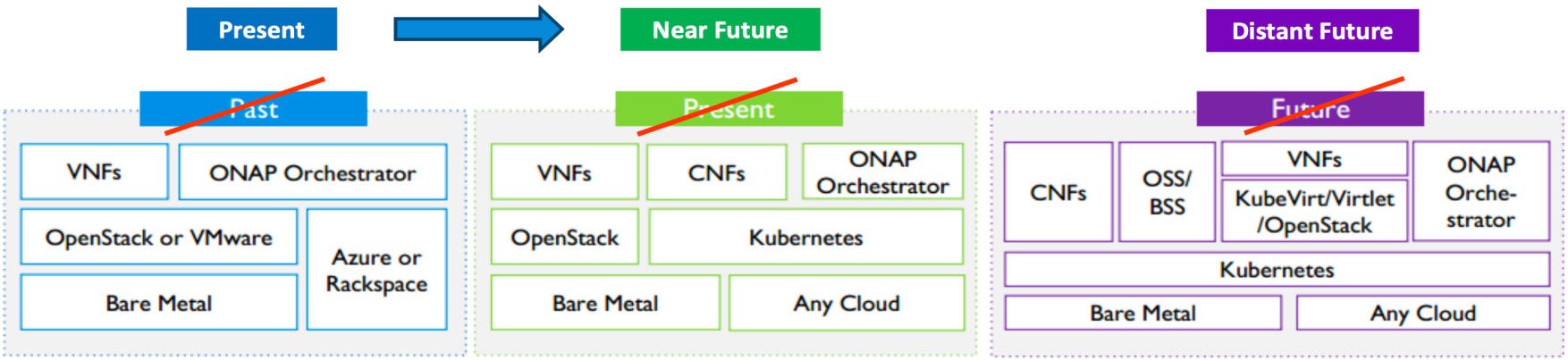


PNF: Physical Network Function

VNF: Virtualized Network Function
VM: Virtual Machine

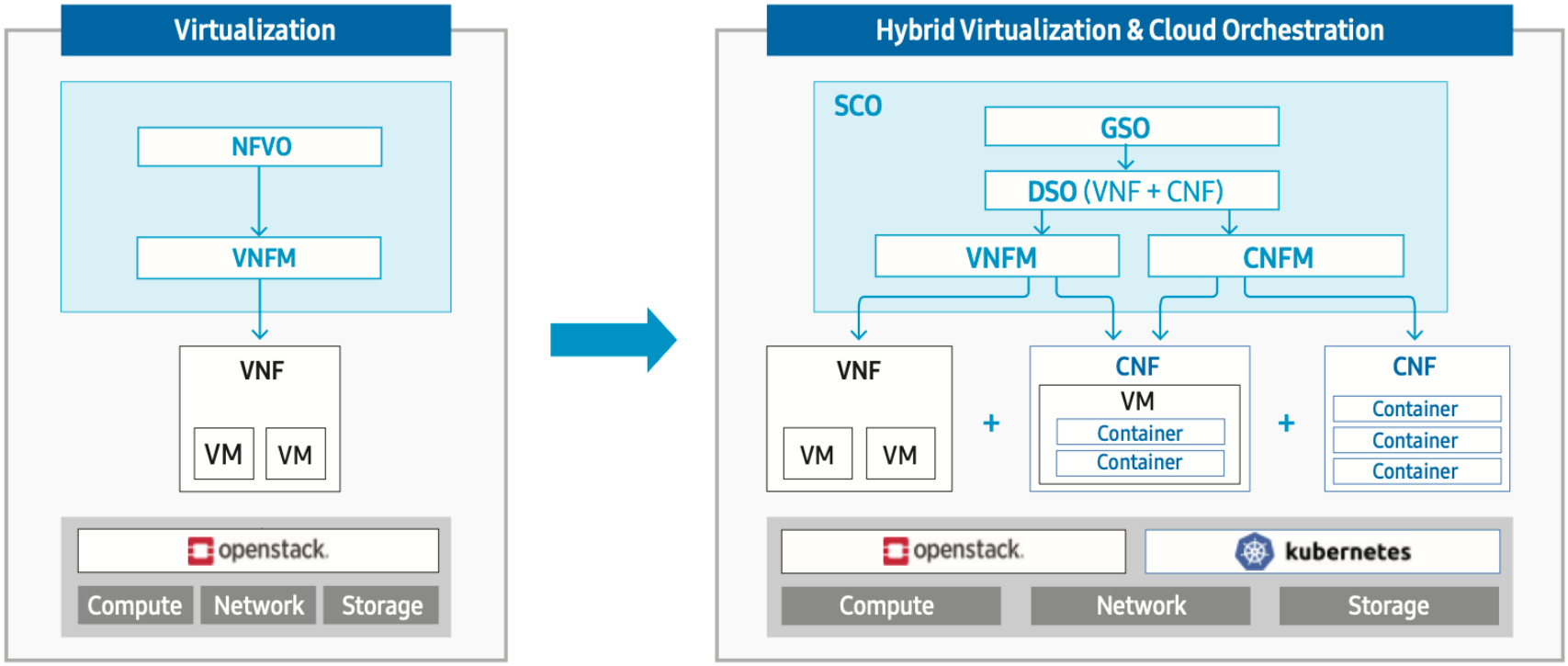
CNF: Cloud Native Network Function

※ 그림출처: 삼성전자



※출처: 박종한, "Cloud Native for Telco", Krnet 2020, 2020

삼성 클라우드 네이티브 5G 코어



CNF : Cloud native Network Function
CNFM : CNF Manager
DSO : Domain Service Orchestrator
GSO : Global Service Orchestrator

NFV : Network Function Virtualization
NFVM : NFV Manager
NFVO : NFV Orchestrator
VM : Virtual Machine

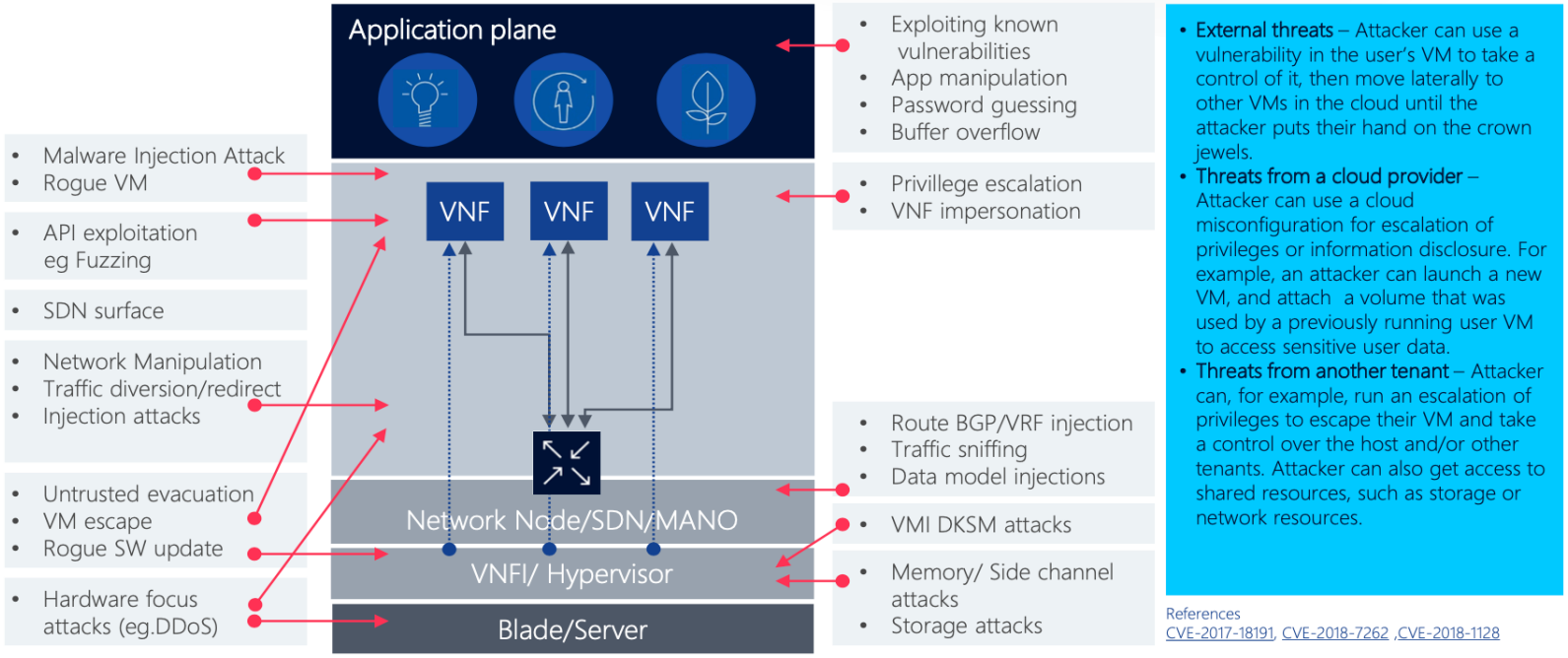
VNF : Virtualized Network Function
VNFM : VNF Manager
SCO : Samsung Cloud Orchestration

*그림출처: 삼성전자, "Cloud Native 5G Core", Vol.2, 2020

MEC 보안위협 및 대응

MEC 시스템 보안

- **(네트워크 기반 침해위협)** MEC 플랫폼 및 응용 서비스에 대한 대규모 단말 동시 접속 또는 서비스 장애(DDoS 등) 유발
  - 초저지연 서비스의 경계 보안을 위한 컨테이너 기반 경량·저지연 네트워크 보안 장비를 통한 침해위협 탐지 및 차단
- **(MEC 플랫폼 및 응용 보안위협)** 3rd party 응용 등의 악성코드 감염이나 조작으로 인한 서비스 장애 또는 민감정보 유출
  - 인가되지 않은 시스템 및 응용으로의 접근, 권한 조작, 변조 및 운용 제어 등에 대한 통제
  - 부채널 공격 등 실행중인 응용 간 데이터 유출 또는 자원 점유 경쟁으로 인한 자원 고갈 방지
  - 로밍 및 핸드오버 과정에서 이전 MEC에 캐싱된 사용자 및 서비스 정보의 유출 방지 등



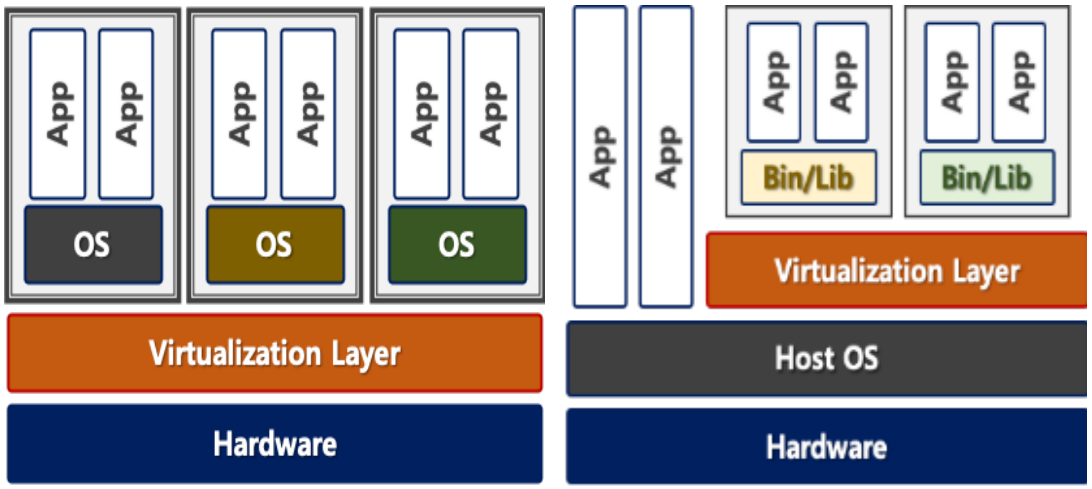
*그림출처: S. Bhattiprolu(NOKIA), "5G Trust model: Recommendations and best practices for CSPs", RSAC, 2020

MEC 보안위협 및 대응

클라우드 네이티브 보안

- (컨테이너 보안위협) 클라우드 네이티브 환경 지향에 따라 가상머신 대비 보안성이 취약한 컨테이너의 비중 증가 및 빈번하고 지속적인 업데이트에 따른 비정상 이미지 유입
  - 컨테이너 런타임 이상징후 탐지
  - 배포 대상 컨테이너 이미지의 무결성 검증 및 비인가 이미지 유포 차단
  - 컨테이너 이미지의 악성코드 내포 탐지
  - 컨테이너 이미지 및 컨테이너 API의 취약성 검증 등

시스템 가상화	구분	운영체제 가상화
독립적인 이종 다중 OS	운영체제	단일 OS 커널 공유
높음	격리	낮음
낮음	효율성	높음
제한적	확장성	무제한
완전히 격리된 독립 인스턴스	특징	빠른 빌드 & 경량 인스턴스



시스템 가상화 vs. 운영체제 가상화

과제 개요

과제명	5G+ 서비스 안정성 보장을 위한 엣지 시큐리티 기술 개발
과제목표	초고속·초저지연·초연결 5G+ 서비스의 안전한 이용환경 제공을 위하여 무선 액세스 및 엣지 네트워크의 보안 상황을 분석하여 위협을 탐지·대응할 수 있는 지능형 5G 엣지 시큐리티 기술 개발 및 실증서비스
총 수행기간	2020. 4. 1. ~ 2023. 12. 31. (총 45개월) (당해연도(1차년도): 2020. 4. 1. ~ 2020. 12. 31. (9개월))
주관기관	ETRI
참여기관 (가나다 順)	성균관대학교 SUNGKYUNKWAN UNIVERSITY, sga, SK telecom, SOMANSA, 숭실대학교 Soongsil University, sysmate, LG U+, WINS

과제 목표 및 연구 내용

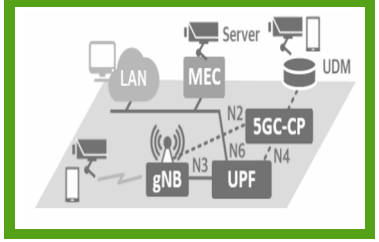
최종 목표

초고속·초저지연·초연결 5G+ 서비스의 안전한 이용환경 제공을 위하여
무선 액세스 및 엣지 네트워크의 보안 상황을 분석하여 위협을 탐지·대응할 수 있는
지능형 5G 엣지 시큐리티 기술 개발 및 실증서비스

연구내용 → 상세 기술

5G 엣지 네트워크 보안

- 5G RAN 비정상 데이터 분석
- 고성능 실시간 패킷 수집 및 위협 분석 플랫폼
- 사설 5G용 Secured MEC-DP 스위치
- 비정상(허위) 기지국 탐지
- 컨테이너 기반 cIPS群, cFW群, cDLP

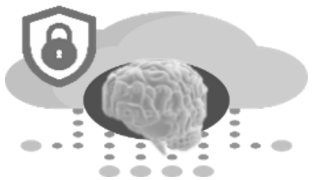


MEC 및 컨테이너 보안

- 가상화 플랫폼 보안위협 탐지 및 대응
- 컨테이너 런타임 이상징후 탐지
- 컨테이너 이미지 무결성 검증 및 권한 관리
- 3rd party MEC 응용 취약성 검증

지능형 보안 분석 및 관제

- 5G 엣지 보안 모니터링 및 관제
- 5G 엣지 네트워크 보안위협 분석 및 탐지
- 5G MEC 보안위협 분석 및 탐지
- 대용량 로그 수집/처리/인덱싱 기술
- STIX/TAXII 위협정보 공유 및 연동

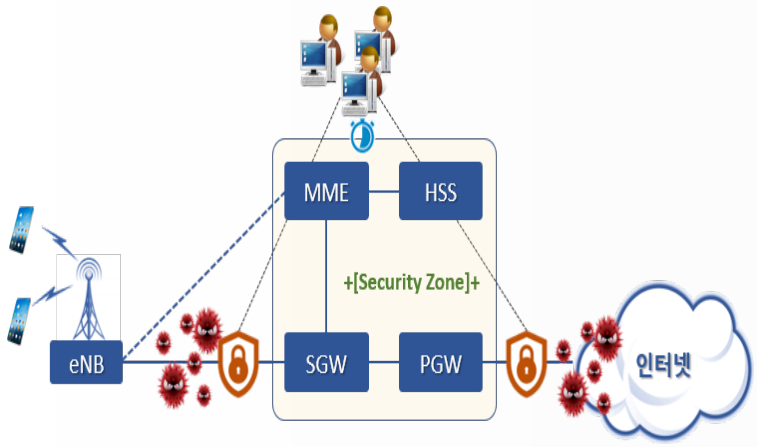


5G B2B 핵심서비스 실증

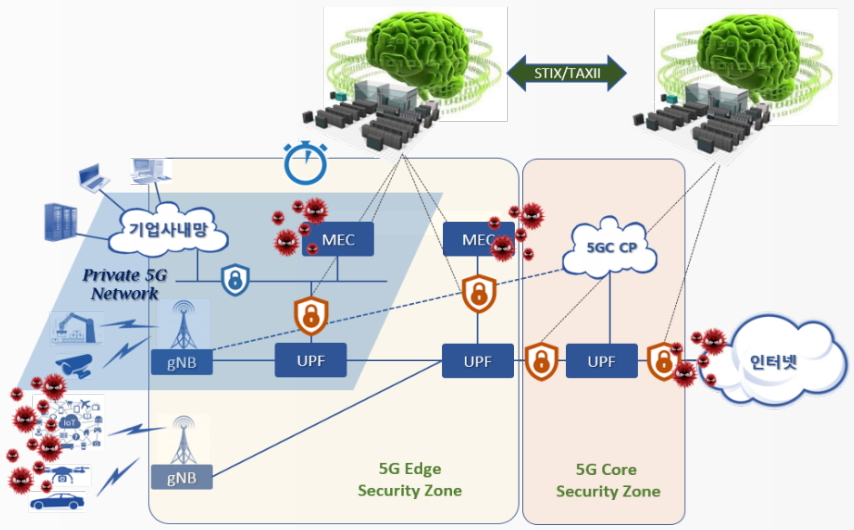
- 5G 스마트공장 보안모델 및 표준화
- 5G 스마트공장 보안 실증 테스트베드 참조모델
- 스마트공장 모델환경 보안 실증
- 5G 스마트공장 실증 테스트베드 구축
- 5G 스마트공장 보안 실증서비스

개발 기술의 특징

	기존 기술	5G 엣지 보안 기술
단말	스마트 단말 중심의 제한된 소규모 접속에 대한 위협 대응	다양한 종류의 센서·기기의 대규모 접속에 대한 위협 대응
서비스	광대역 인터넷 서비스에 국한된 보안 위협 대응	초연결·초저지연·초고속의 융합서비스 중심의 보안 위협 대응
서비스 제공방식	코어망을 경유한 인터넷으로부터의 서비스 위협 차단	코어망 경유없이 MEC를 통한 서비스 위협 차단
위협분석 및 관제	트래픽 정보 중심 위협 탐지 관제요원 중심의 수동 분석 및 대응	트래픽 및 행위 정보 중심 위협 탐지 인공지능 기반 자동 분석 및 대응



기존 코어망 경계 중심의 위협 대응



5G 엣지에서의 선제적 위협 대응

요약 및 정리

5G는 다양한 미래 ICT 융합서비스의 플랫폼으로서 **B2B 新시장** 창출 및 활성화 전망

IMT-2020 비전 및 요구사항에 따라 **5G 네트워크의 구조적 변화** 불가피

5G에서는 **공격 접점이 급증**하고, LTE 보안위협 뿐만 아니라 **새로운 잠재적 보안 위협** 존재

5G 전체 네트워크 보호를 위해 엣지에서의 보안 위협을 **엣지에서 대응 • 해결** 필요

5G 융합서비스의 안전한 이용 환경 보장을 위해 **지능화된 5G 엣지 보안 기술** 필요성 급증

감사합니다!

미래사회를 만들어가는 국가지능화 종합 연구기관
National AI Research Institute - Making a Better Tomorrow

ETRI
한국전자통신연구원