

The Eviden logo is rendered in a white, stylized, outlined font. The letters are blocky with a double-line effect, giving it a modern, digital appearance. The background of the slide features a large, abstract graphic of overlapping, concentric circles in various shades of teal and blue, creating a sense of depth and movement.

EVIDEN

5Guard

Securing 5G Networks from Edge to Cloud

Stay connected.
Stay protected.

19.09.2023

© Eviden SAS – For internal use

an atos business

EVIDEN



Vasco Gomes

Global CTO Cybersecurity Products
& Digital Security Offering
Technology Lead

Eviden

EVIDEN

Content overview

01

Unlocking 5G potential

02

5G security perspective

03

5Guard value proposition

04

Use Cases

05

Key benefits

EVIDEN

01. Unlocking 5G potential

5G market context

Overview

Brings added value

5G networks advantages

Faster speeds

Lower latency

Greater network capacity

Increased connectivity

Enhanced mobility

Improved reliability

Transforms businesses

Customer benefits

Improve operational efficiency

Increase productivity

Create new revenue streams

Deliver better use experiences

Demands increased protection

Security challenges

Larger attack surface

Virtualization and cloud technologies

Wide range of new use cases

More devices and data

Advanced persistent threats

More sophisticated attacks

A huge potential to unlock

A phenomenon that creates new value...

\$3.6 trillion

is the expected economic output enabled by 5G technology by 2035

...hindered by concerns about the security posture...

Only
9%

of security practitioners say they are highly confident their security posture is ready for 5G rollout

...due to an increased attack surface

32%

of operators point to an increased attack surface as a key challenge (IoT, cloud and data threats more specifically)

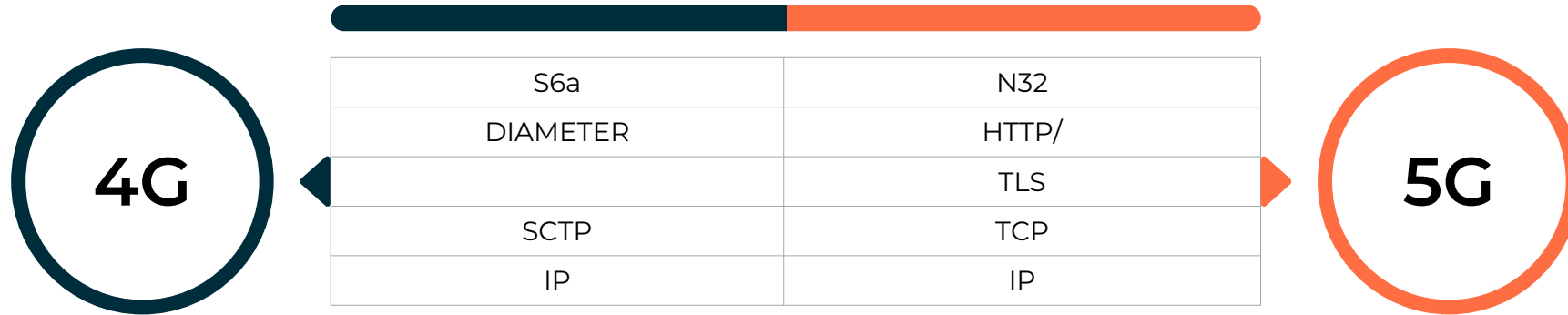
Source: WEF [The Impact of 5G](#), (2020); AT&T Cybersecurity Insights Report: [5G and the Journey to the Edge](#) (2021); Trend Micro and GSMA Intelligence (2021)

EVIDEN

02. 5G Security perspective

From 4G to 5G Networks

New IP Protocol stack



Historically, operator networks have mainly used proprietary protocols for network management



5G moves to an IP based protocol stack, allowing interoperability with a wider number of services and technologies



As these protocols are used in IT industry, their use could increase the impact of vulnerabilities within these protocols



Familiar set of tools and existing solutions for IT providers, making it easier to overall address the 5G network infrastructure

Source: [GSMA | Securing the 5G Era - Security](#)

5G security risks

The perfect environment for security incidents

Use of internet technologies

New-generation mobile networks require new signaling protocols in the network core, resulting in a wider range of threats already facing Internet systems

Compatibility with previous-generation networks

Taking care of security not only for 5G networks, but for the transition and interworking with previous-generation networks as well

Network slicing

Significant security implications due to the configuration of a larger number of slices with greater complexity and service requirements

SDN and NFV

Trying to reduce the number of monitoring points, blind spots may appear, making it impossible to detect malicious activity

Internet of Things

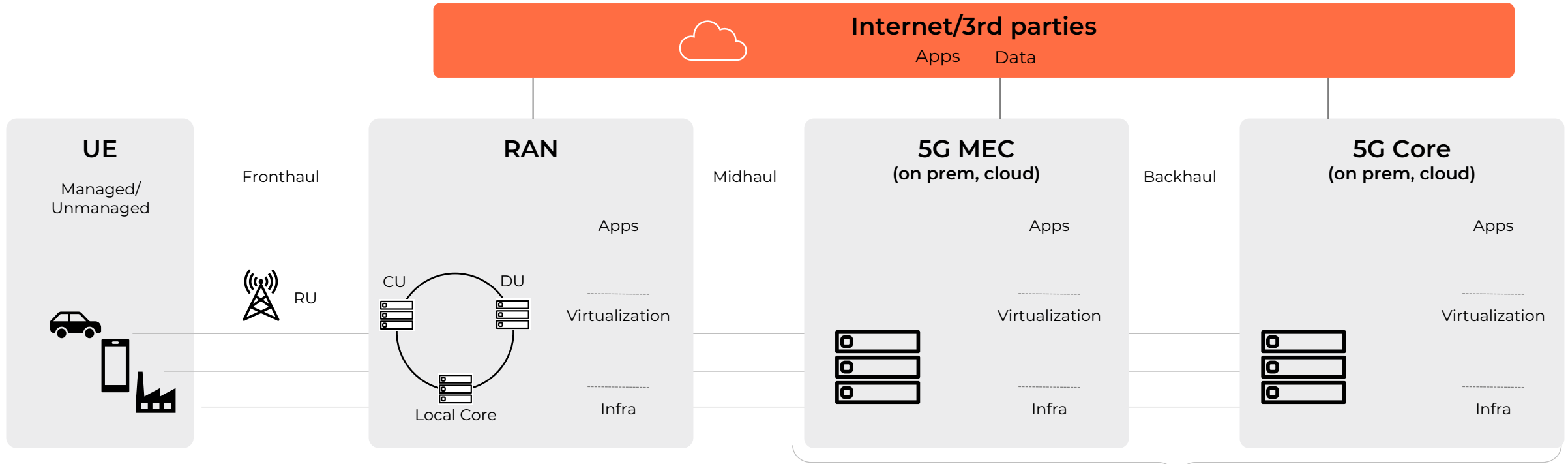
The existing threat model, developed for identification of suspicious activity in the context of a human subscriber, will not work for the IoT

Containerization

Networks elements are becoming more customizable and require the use of containers and virtual machines, that might contain specific vulnerabilities

5G attacks

5G has enhanced security, but vulnerabilities remain



- Malware
- Bots/DDOS
- Firmware hacks
- MitM attacks
- Tampering

- MitM attacks
- Jamming

- Rogue nodes
- FI manipulation
- Authentication issues
- Insecure X2/Xx/S1 interfaces

- DDOS attacks
- Insecure N6, Sx
- Control/User plane sniffing
- Side channel attacks
- MEC server vulnerabilities
- Apps vulnerabilities

Multi-Cloud

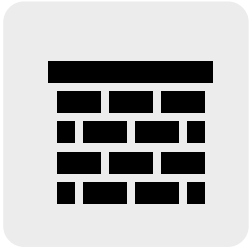
- Virtualization issues
- DDOS and DOS attacks
- Network Slicing issues
- API vulnerability
- Improper access control/identity

3GPP: Focus on security in 5G

3GPP standards provide a solid foundation for 5G security

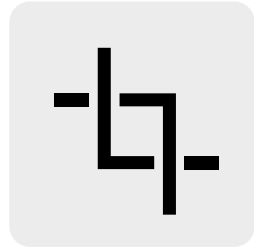
3GPP System Architecture Evolution (SAE) – Security Architecture

IPsec is the standard recommended by 3GPP for MNOs and MVNOs



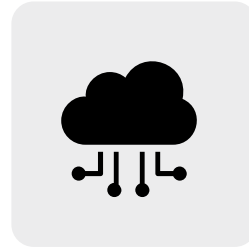
Security Gateway

- IPsec VPN aggregator
- FW demarcation point between Core and RAN
- Carries communication from RAN to Core for CP & UP
- Carries OAM traffic for RAN management
- N1, N3, F1-U, F1-C, E1



Interfaces Security

- IPsec should be used to protect E2 traffic and F1, E1, X2, Xn, NG
- TLS should be used to protect the traffic between the O-RAN system and other network elements
- SSH should be used in O1 interface



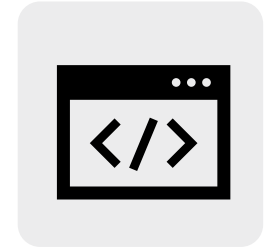
CGNAT

- Support for both IPv4 and IPv6 protocols
- Provide scalable and efficient address translation,
- Enable the mapping of multiple private IPv4 addresses to a single public IPv4 address



Roaming

- Signaling roaming security
- GTP-C should be used between the visited network and the home network for signaling messages
- GTP-U should be used for carrying user data traffic



API Security

- Protection for exposure functions
- SCEF (4G NB-IoT com)
- NEF (capability exposure)
- SEPP (5G Roaming)

3GPP standards: Why is it not enough?



What protection you can expect

Focus only on the data & interfaces of 3GPP network functions

5G Standalone (SA) brings:

- Integrity protected user traffic*
- Enhanced Subscriber Privacy
- Concealing the SUPI (IMSI)
- Protection of control data over the roaming interface
- DTLS for control plane
 - Mutual control signaling authentication*
 - Encrypted and integrity protected control signaling traffic*

*optional



What protection you won't find by default

How to optimally implement 3GPP reqs
Network-level security
Cloud/containers platform security
End-user protection

What is missing:

- The optimal implementation of 3GPP recommendations
- Network-level protection (segmentation, DDoS, lateral movements, ...)
- Interconnect to other networks (Roaming, RAN sharing, Internet)
- L7 end-user traffic protection (IPS, UTM, AV, ...)
- Cloud/K8s infrastructure security
- Image vulnerability protection
- Scoring of security configuration
- API Security for Telco Cloud

EVIDEN

03. 5Guard value proposition

Innovation ecosystems and partnerships for 5G



Why Fortinet?

Leader in Magic Quadrants for network firewalls and WAN edge infrastructure, enabling enterprise security to any edge at any scale

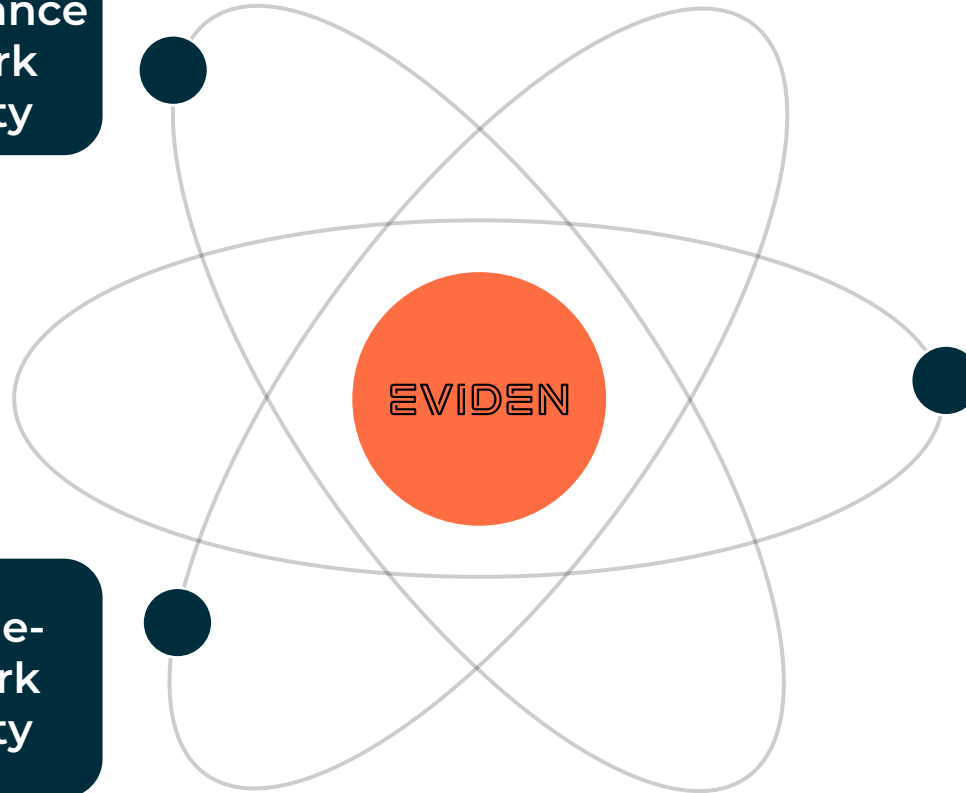
High-performance network security



Why Microsoft?

Built-in protection from the edge to the cloud and extensive investment in Azure to build a unique 5G network

5G Edge-Network security



Evidian

Best-of breed products

Lifelink

Trustway

Why our products?
Strengthen confidentiality and sovereignty with certified solutions and control over the roadmap

Alsaac

IDnomic

cryptovision



5G security portfolio overview

5Guard

Workloads, communications, monitoring

Identities, permissions, encryption

Network security

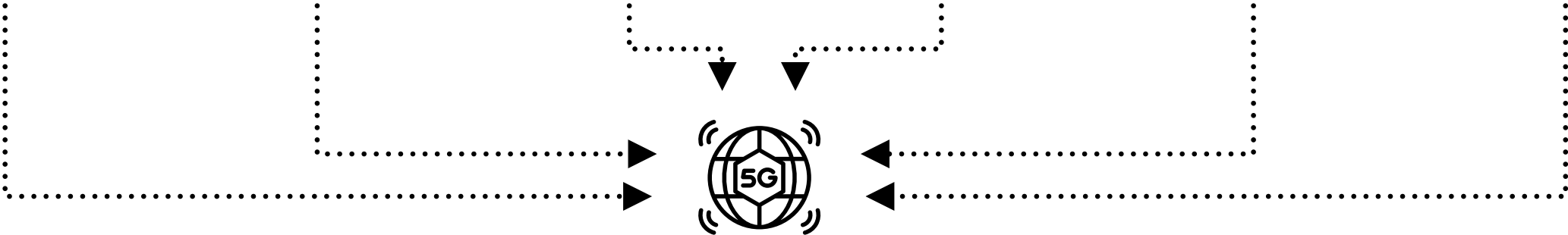
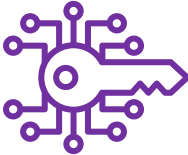
Cloud security

Detection and response

Identity and access control

PKI

Encryption



5Guard

5Guard Cybersecurity mesh

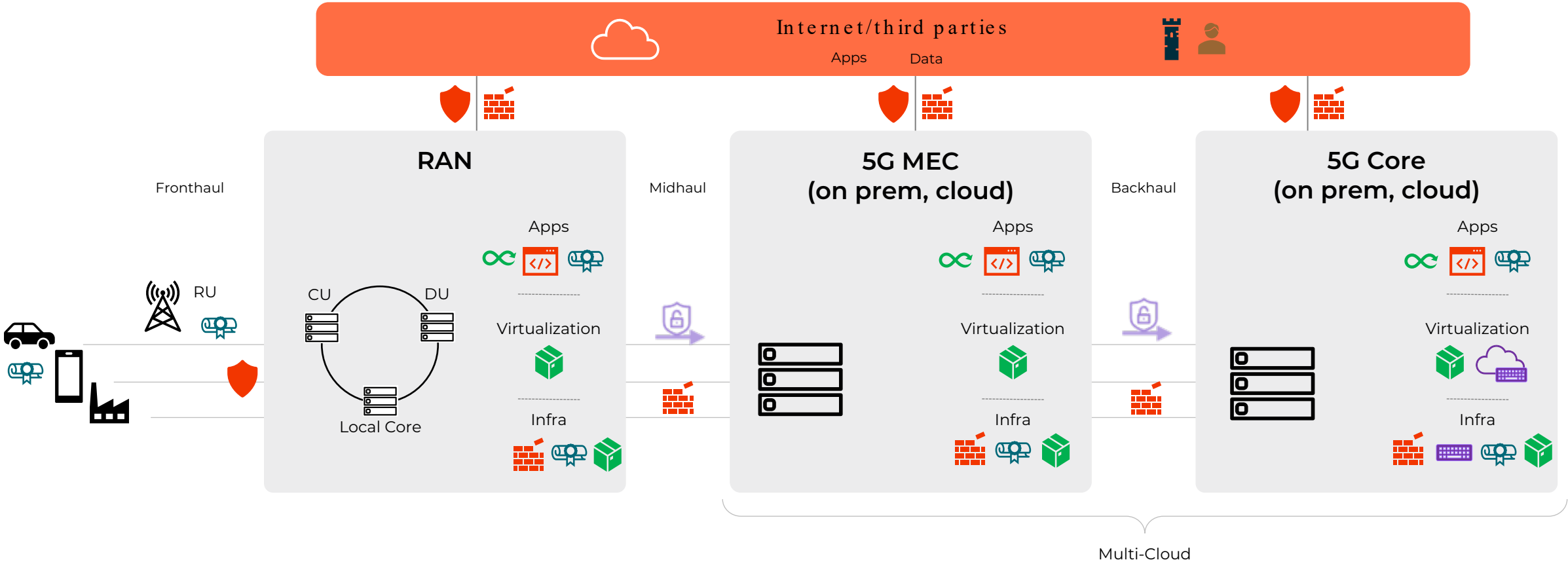
From device to multi-cloud, granular and industrialized security

EVIDEN
Services

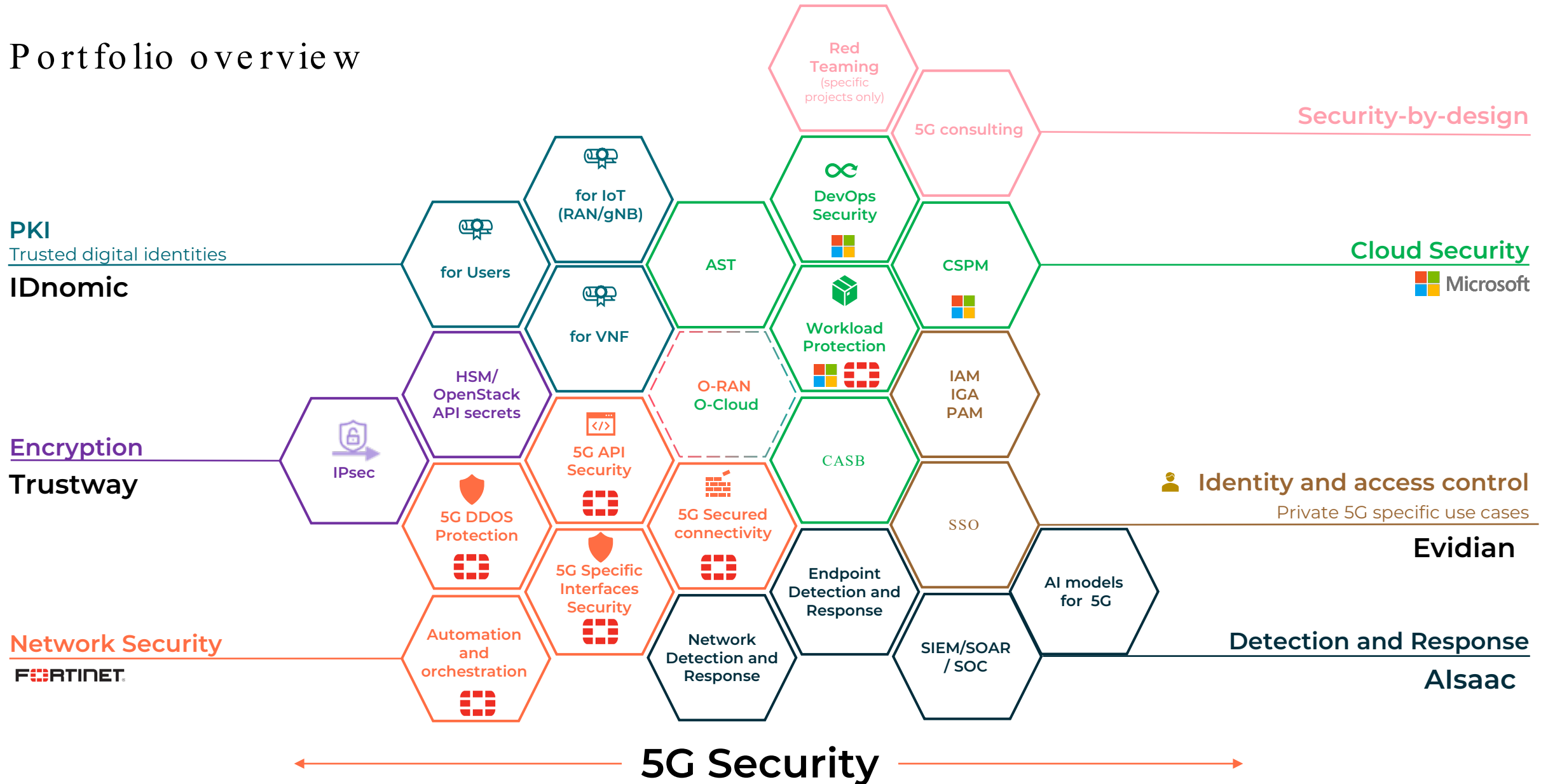
Cloud Security
Detection and Response
Network Security

EVIDEN
Products

Identity and access control
PKI
Encryption

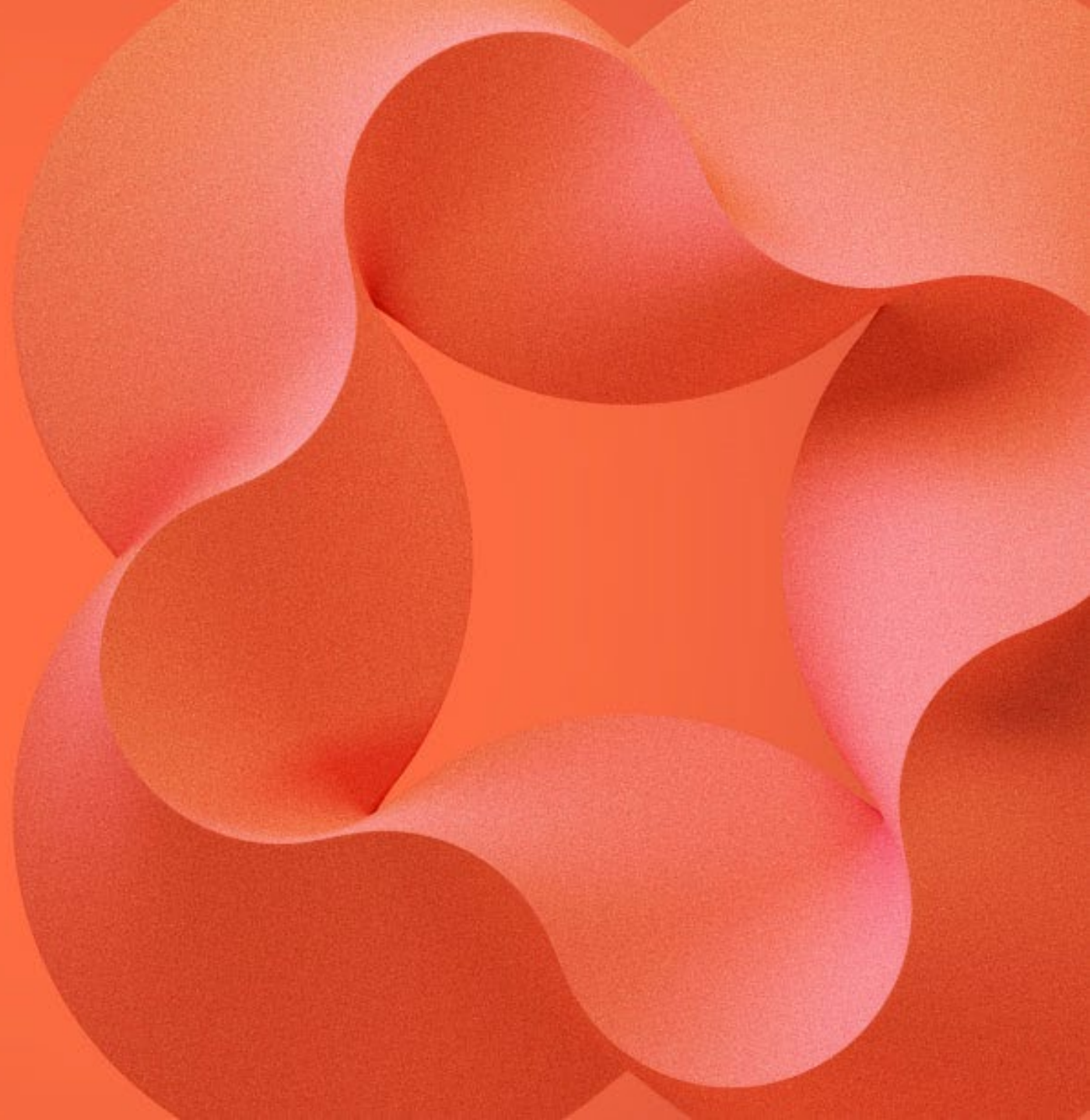


Portfolio overview



EVIDEN

04. Use cases



How we support 5G security

Overview

Ensure service availability and data integrity

RAN security infrastructure that provides a common set of tools

Protect the SBA functions from attacks

Protect against API exploits

Operator security for infrastructure and activities

Integrate strong security capabilities within the MEC ecosystem

Securing workloads in 5G environments

Help in detection of cybersecurity threats within and around containers

Securing OT/IOT environments

Protect industrial 5G against IoT attacks, signaling storms, and malfunctions











Improve security operations



Enable effective, efficient and automated security operations

5Guard use cases

How to...?

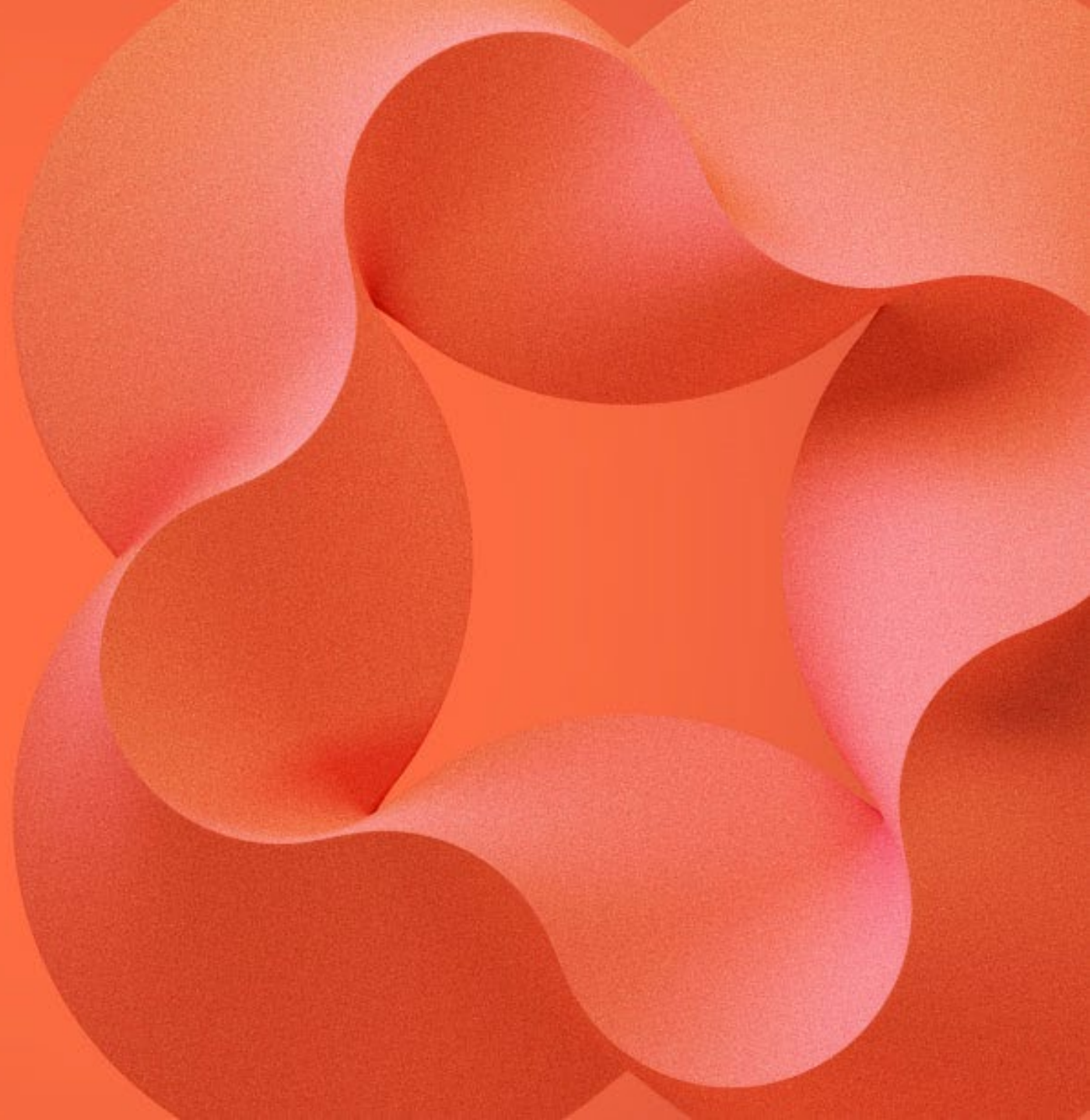
Dev-SecOps  Secure cloud containers |  Defend the application layer

	RAN	MEC	5G core
	Deploy secure IoT/telco networks	 Protect your MEC	 Secure mobile roaming
	Secure your RAN environment	 Protect the cloud environment supporting 5G \geq and manage the security posture	
		 Safeguard virtualized networks	
	Eliminate API exposure vulnerabilities \geq and deploy IAM strategies in 5G APIs		
	Secure data in transit and at rest		
	Protect Packet Data Network (PDN)		
	Secure workloads in 5G environments		

	Threat detection and response	Proactively defend against threats in the 5G network Leveraging security analytics		Bring Zero trust to your 5G environment	Automate configuration and deployment of security devices and Avoid privileges escalation in 5G
-------------------------------------------------------------------------------------	--------------------------------------	---------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------	------------------------------------------------	----------------------------------------------------------------------------------------------------

EVIDEN

05. Key benefits



Key benefits from 5Guard

Proactive defense in-depth

Identify vulnerabilities and threats across your 5G network infrastructure and remediate in almost real-time



Compliance and expertise

Leverage the experience of certified teams all along your 5G security strategy development and in accordance with your regulatory requirements



Efficiency boost

Reduce IT teams alert fatigue through the support of our global community of experts around orchestration and monitoring of your 5G network



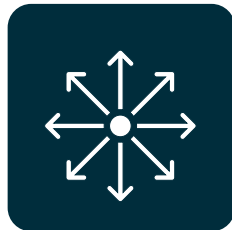
Network convergence

You connect and protect any edge at any scale with fully integrated networking capabilities, such as SD-Branch, SD-WAN & 5G



Ease of deployment

Reduce your time to deploy and configure security on your network with powerful managed security services



24/7 Threat Intelligence

Get enhanced analytics and threat hunting, with better investigations to support faster threat remediation with Eviden MDR



EVIDEN

Ranked #1 worldwide in managed security services by revenue in Gartner 2021 Market Share report

Over 6,500 security specialists

Worldwide network of 16 security operation centers (SOCs)

EVIDEN

Customers/partners interaction

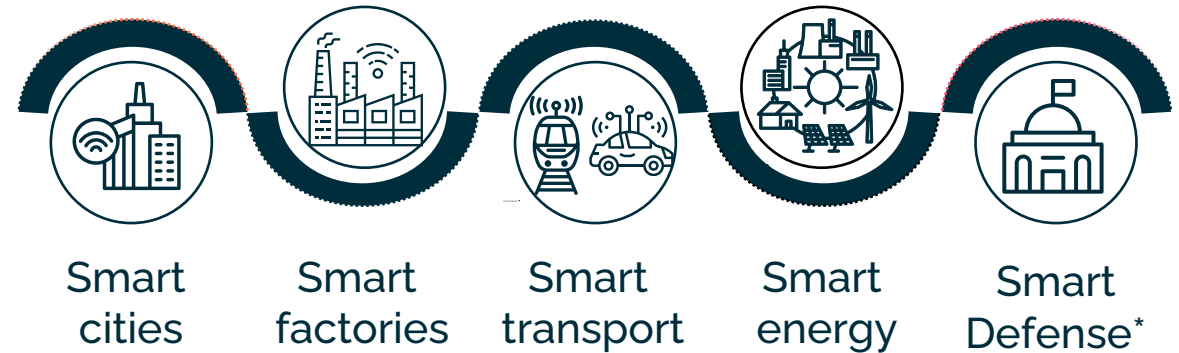
Who is interested?

Communications Service Providers (CSPs)



- **Tier 2/3 CSPs** are the main interested parties with many requests for security or technology products to extend or secure their portfolios.
- **Tier 1 CSP** are well equipped; but are interested by specific solutions or services blocks to complete their portfolio.

Industries & Public Sector



Industries operating in harsh environments, with critical systems.

- Energy & Utilities: Windfarms, Oil & Gas ...
- Transportation
- Manufacturing: Factories in specific areas

RFPs/large programs requiring system integration & security.

- Large systems (regional, national scale) refoundation / renewal
- Regulatory security constraints (critical systems / essential infrastructures)
- Sovereignty required (data – technology – operations)

A wide range of collaboration models

The way forward

As customers

Managed security services for the operator internal needs (IAM, Cloud, SOC, IoT and OT security...)

For joint offerings

Establish a common delivery and service level agreement (SLA), engage in joint go-to-market (GTM) efforts, and integrate our offerings to create an integrated solution

As resellers of Eviden offerings

Leverage Eviden broad ecosystem of products and services to generate business in original equipment manufacturer (OEM) mode

Driven by co-innovation

Integration of Eviden state-of-the-art products to the operator's solution and custom capabilities to create new products

Widely optimized collaboration models

As-a-service pricing model

Product line = on-premises or as-a-service
Save CAPEX
Avoid maintenance
Pay-as-you-use
Transparent KPI on as-a-service ROI vs. on-prem investments

Trustway

Key management as a service cheaper in average until **10 000** KEK(*)

Automation and AI-based

AI-based detection and remediation
Operational efficiency and cost-effectiveness

Alsaac

~ **70%** improvement in response time
~ **80%** improvement in mean time to detect

High ROI building blocks

Cost saving on help desk
Mutualization of identity and access management solutions

Evidian

~ **25%** savings on your help desk costs
Shared IAM solutions

Major International Telecom provider

Secure 4G and 5G networks

The challenge

- 4G and 5G antennae need to be secured by implementing PKI technology, i.e., deploying a digital identity for each equipment through specific protocols.
- This international Telecom provider project required set up of a security management center to generate and deliver security features for IoT services.
- Eviden has deployed in the past a PKI to secure the 4G network. The second step was now to secure the 5G Networks by 2023 and ensure compliance with 3GPP standards (TS 33.210, TS 33.310, TS 33.401)

The solution

A PKI for the management of credentials for 4G/5G networks :

- **Certificate Authority Module:** IDnomic ID CA is a trust entity that enables secure, centralized management of Certificate Authority lifecycles and the production of digital certificates.
- **CMPv2 Connector**, enabling enrollment of 4G/5G antennae in order to manage their digital identity lifecycle
- **Professional Services** to accompany deployment and integration of PKI at the customer

The impact

- Migration of the existing 4G solution « Meta PKI » to a 5G solution « IDnomic PKI » for CORE and RAN.
- High Level of support
- Federation of all PKI solutions into one single IDnomic PKI instance

Our security success stories

Unified security and trust from IT systems to networks

Enterprise security



Enabling Ooredoo's customers to benefits from new levels of managed security services, including web and email security, EDR, threat intelligence services and more [>>](#)



Accelerating Deutsch Telekom transformation by establishing a secure framework for migration applications on key AWS services, leveraging the expertise on containerization, IaC and CI/CD [>>](#)



Detecting and preventing system and application threats through Azure workloads protection for a network operator in the Netherlands



Enforcing security policy and access control for a Tier 1 Telecom operator in Germany with a E-SSO solution for 500.000+ accounts and 60,000+ users

Network security



Securing the communication of the Internet of Things within the LoRa network of Objenious with our Trustway HSM for IoT and Eviden IDnomic PKI [>>](#)



Providing a secure NFV foundation for a French Tier 1 operator leveraging a HSM and key management platform



Securing RAN (4G and 5G) for a Middle East tier 1 operator through a PKI solution to deliver and manage digital identities for their core network (gateways, 4G/5G antennas, 5K Enodes)



Protecting all inter-site communication for a high-tech industrial company with up to 300 IP encryptor appliances and assisting the customer with the integration

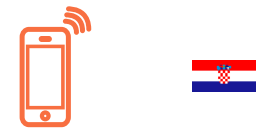
Critical communications



Supplying critical communications solutions for offshore wind farms [>>](#)



Full managed services provided for a European tier 1 telecom operator covering all telecom services needed to maintain the network (capacity planning, emergency recovery, patching, SLA and KPI management...)



Designing the overall architecture, simplifying and organizing communication and implemented agents and service logic for provisioning of this telecom operator

EVIDEN

Questions?



EVIDEN

Thank you!



Vasco GOMES

Cybersecurity Products CTO & Digital Security Offerings Technology Lead

Eviden Scientific Community member | Cybersecurity Distinguished Expert

M +33 633 867 565

vasco.gomes@eviden.com  

Confidential information owned by Eviden SAS, to be used by the recipient only.
This document, or any part of it, may not be reproduced, copied, circulated
and/or distributed nor quoted without prior written approval from Eviden SAS.

© Eviden SAS – For internal use

Follow Eviden:

eviden.com

