



Osvaldo Aldao

ENEA

Portfolio Overview & Strategic Focus

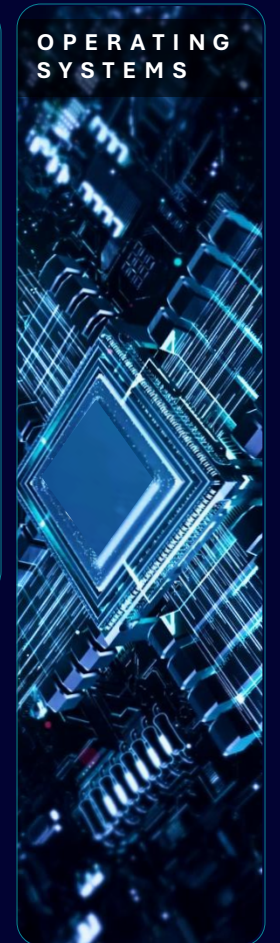
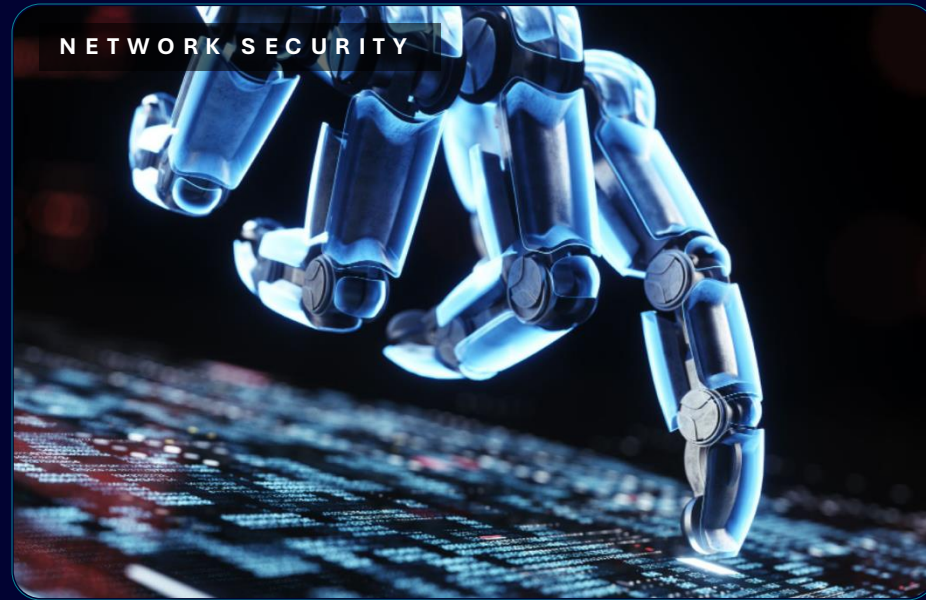
ENEA CAPITAL MARKETS DAY

OSVALDO ALDAO, CTO

The Markets We Serve



Enea Portfolio



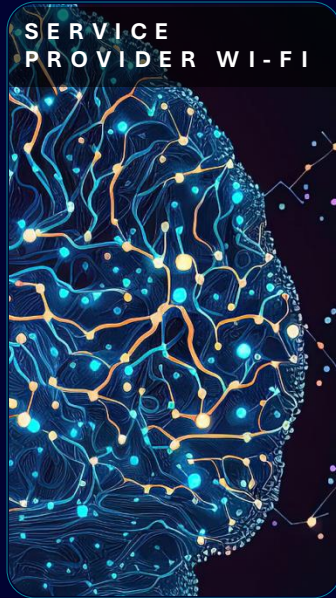
Enea Portfolio & Markets We Serve



Enea Portfolio & Business Focus Areas



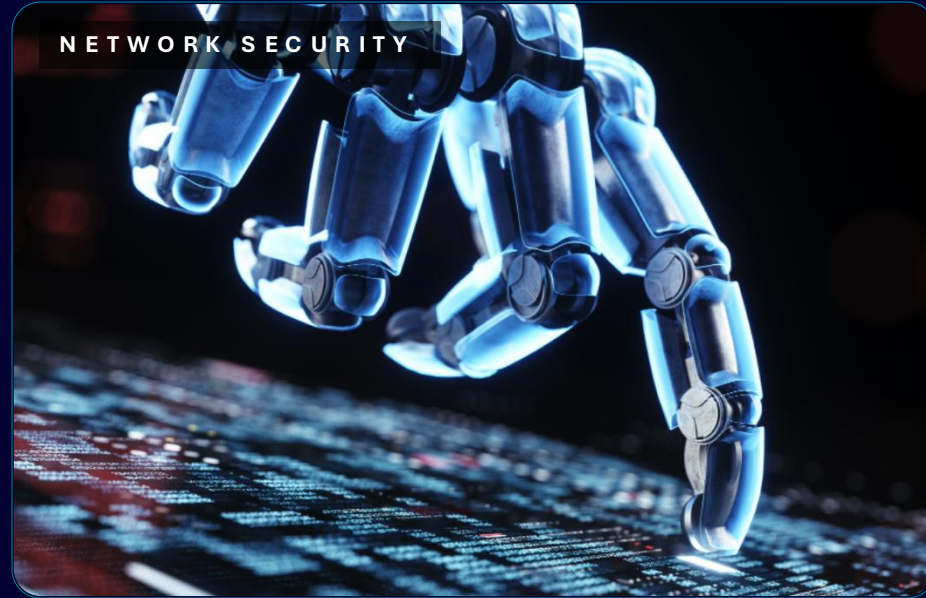
DATA MANAGEMENT APPLICATIONS



SERVICE PROVIDER WI-FI



NETWORK DATA LAYER



NETWORK SECURITY



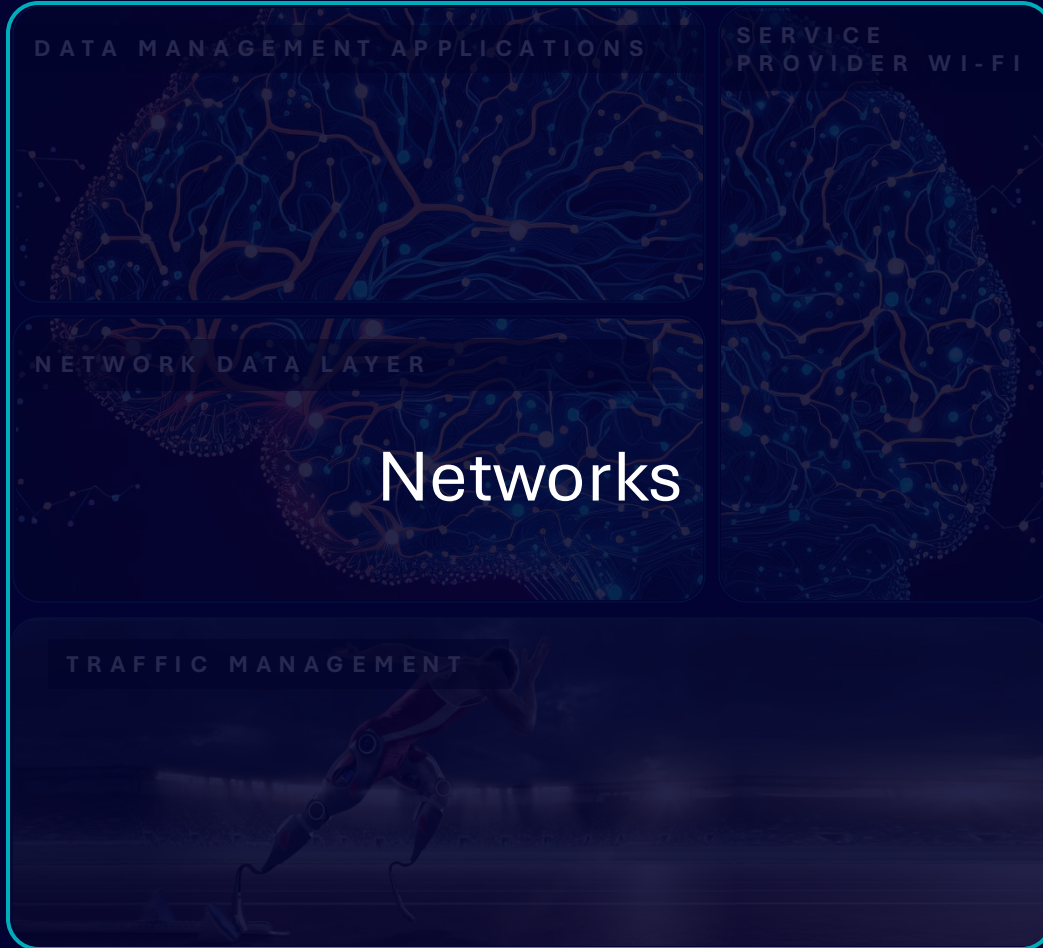
TRAFFIC MANAGEMENT



EMBEDDED SECURITY

No
Operating
Systems
Business

Business Focus Areas



DATA MANAGEMENT APPLICATIONS

SERVICE PROVIDER WI-FI

NETWORK DATA LAYER

Networks

TRAFFIC MANAGEMENT

The Networks focus area is represented by a dark blue background with a glowing network of orange and blue nodes and lines. The central text 'Networks' is in white. Surrounding text includes 'DATA MANAGEMENT APPLICATIONS' at the top left, 'SERVICE PROVIDER WI-FI' at the top right, 'NETWORK DATA LAYER' in the middle left, and 'TRAFFIC MANAGEMENT' at the bottom left. A stylized robot arm is visible in the bottom left corner.



NETWORK SECURITY

Security

EMBEDDED SECURITY

The Security focus area features a dark blue background with a glowing blue robot hand reaching down. The central text 'Security' is in white. Surrounding text includes 'NETWORK SECURITY' at the top left and 'EMBEDDED SECURITY' at the bottom left. A padlock icon is visible in the bottom left corner.

World Leader in Security for communications

GLOBAL MARKET PRESENCE

80+

Countries where Enea software is deployed

100+

Networks using our software

Tier #1

Three market segments:
Operators, CPaaS, Cybersecurity vendors

INSIGHTS AT SCALE

2.4 billion

mobile subscribers and devices protected worldwide

50 billion

events/day processing identifying threats & securing in real time

Intel

Global threat intelligence & AI/ML augmented protection

TRUSTED REFERENCE



World Class Security Portfolio

PEOPLE



- We protect **people's privacy**
- Prevent **location information** leakage
- Stop **scams messages** and **fake calls**

COMPANIES



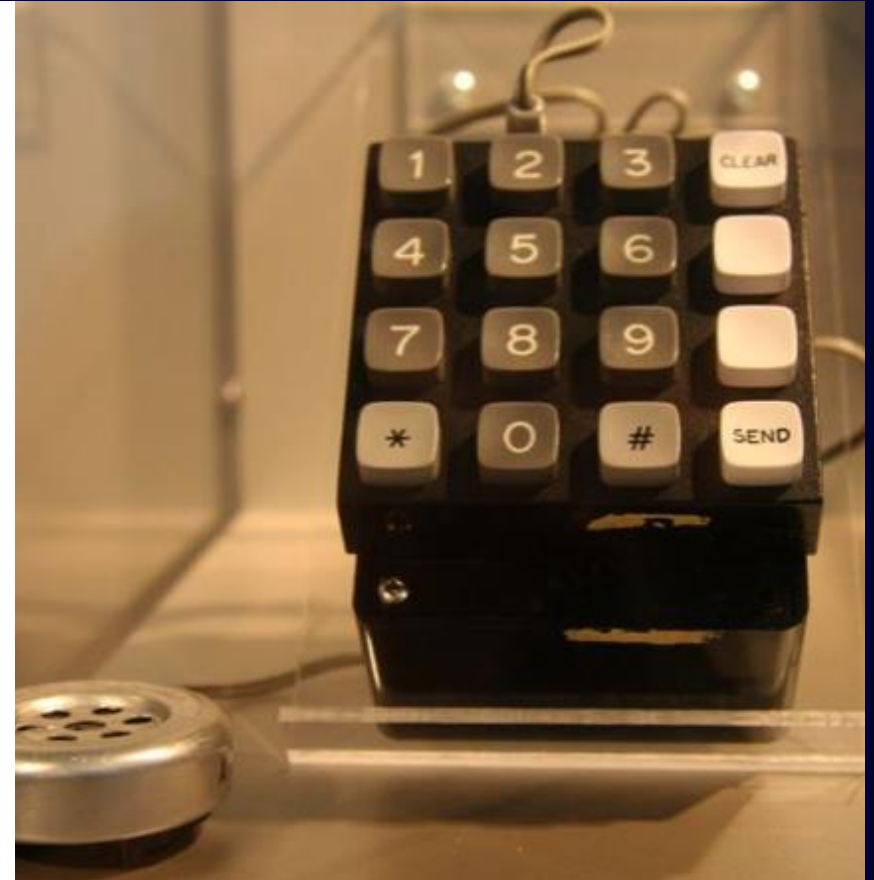
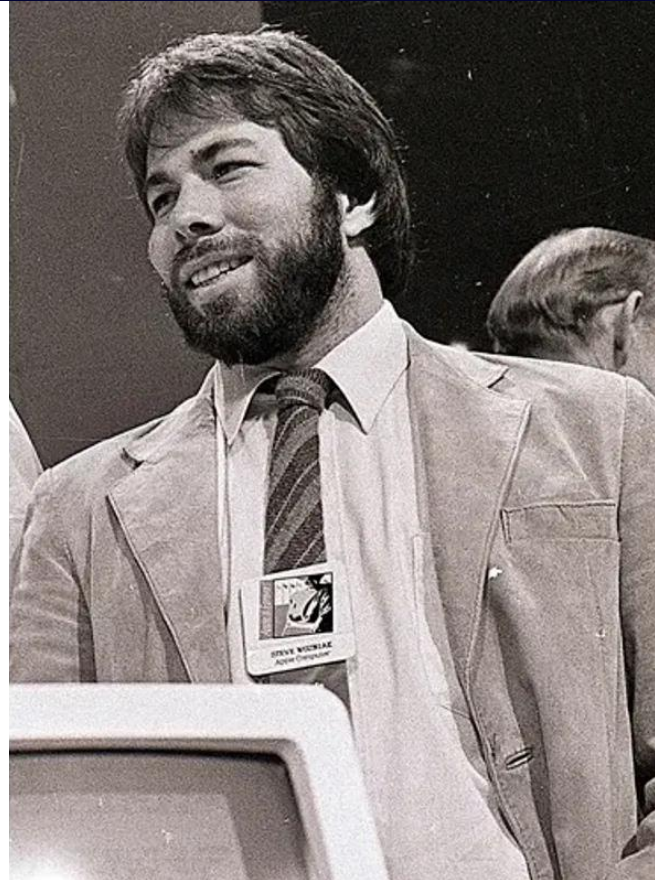
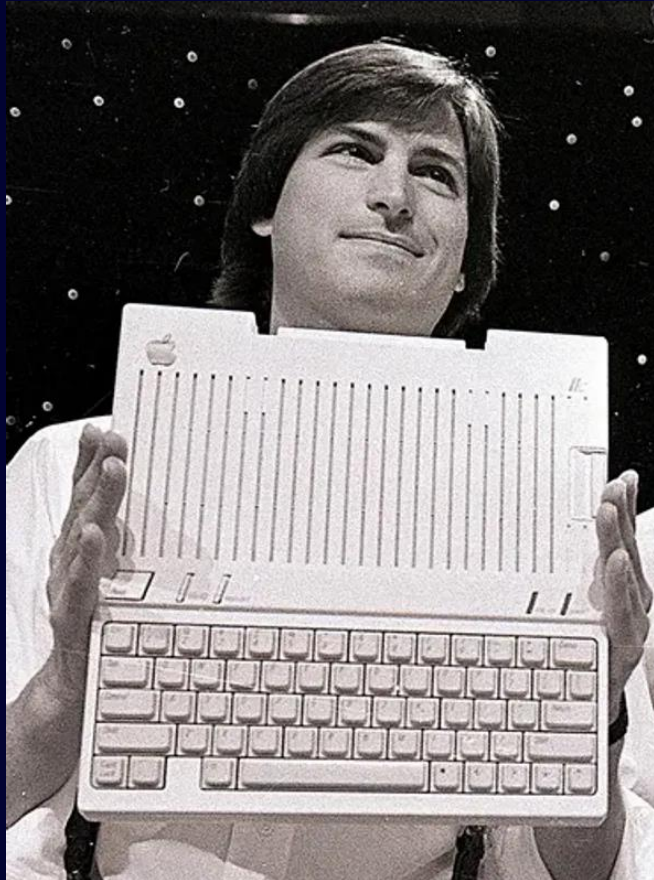
- We stop attacks by **foreign actors**
- **Defense** of national **communications**
- Protect the **networks** from operators

DATA



- Threat detection to **security vendors**
- Safeguard **critical assets** - Intrusion Protect
- **Secure & Encrypted** IoT communication

Wozniak and Jobs – 1972 – Blue box



From Inbound to Outbound Control



Inbound Control



Outbound Control




Security Flaws in Mobile Networks

“Surveillance companies can enter any phone number and track the device associated with it, wherever it is in the world...”

In contrast to spyware-based surveillance, these services do not interact with the target’s phone. Instead, they trick wireless carriers’ servers into revealing the information...

...hacking services exploit flaws in two technologies, known as Diameter and Signaling System 7 (SS7). These two technologies are used by wireless carriers around the world ”



February 29, 2024

Wyden Urges Biden Administration to Crack Down on Surveillance Companies and Shore up Security of Wireless Networks

“Surveillance companies and their authoritarian foreign government customers have exploited lax security in U.S. and foreign phone networks for at least a decade to track phones anywhere in the world,” Wyden said in his letter addressed to President Biden. “Authoritarian governments have abused these tools to track Americans in the United States and journalists and dissidents abroad, threatening U.S. national security, freedom of the press, and international human rights.”

Wyden detailed the vulnerability of wireless phone carriers: “These phone company hacking services exploit flaws in two obscure technologies, known as Diameter and Signaling System 7 (SS7). These two technologies are used by wireless carriers around the world to deliver text messages between phone companies, and for roaming by their customers traveling abroad. For the last decade, cybersecurity researchers and investigative journalists have highlighted how wireless carriers’ failure to secure their networks against rogue SS7 and Diameter requests for customer data has been exploited by authoritarian governments to conduct surveillance.”

Security Flaws in Mobile Networks

Medium Search Write Sign up Sign in

securityaffairs

EFF About Issues Our Work Take Action Tools Donate

**DEMONSTRATE HOW TO STEAL...
ING SS7 ISSUES**

**...S HACK WHATSAPP ACCOUNTS
S7 PROTOCOL**

May 10, 2016

**Why SS7 Attacks Are the
Security, Exploiting Glob**

You may or may not know that SS7 is the backbone of the telecommunication network. It is the function that lies a dan

**METRO BANK
DISCLOSED S
CUSTOMERS**

Pierluigi Paganini Feb

**EFF to FCC: SS7 is Vulnerable, and
Telecoms Must Acknowledge That**

BY COOPER QUINTIN AND BABETTE NGENE | JULY 15, 2024

**Cyber Official Speaks
Out, Reveals Mobile
Network Attacks in U.S.**

NEWS

JOSEPH COX · MAY 16, 2024 AT 9:01 AM

A CISA official breaks with the government narrative and tells the FCC that SS7 and similar networks and protocols have been used to track people in the U.S. in recent years.

It's unlikely you've heard of Signaling System 7 (SS7), but the world is connected to it, and if you have ever roamed near an [SMS message](#) overseas you have used it. SS7 is a set of protocols that cellular network operators use to exchange

**Metro Bank h
bank to discl
customers, b
isolated case.**

SS7

EN

ENEA

<Customer Case Telia>

ENEA CAPITAL MARKETS DAY

Market Outlook 2025

Market Drivers

1. Revenue assurance emerges as a focus area in Telco cybersecurity i.e. TM, FWs
2. Global regulation focus Voice Caller Line Identification Spoofing
3. Rich Communication Services (RCS) in messaging
4. Secure Access Service Edge drives DPI library capacity
5. Adoption of artificial intelligence in cybersecurity (Offensive & Defensive sides)

Market Development

• Mobile Packet Core	+2% Y/Y in 2025 ¹⁾
• Telecom Security	+8,4 % CAGR 2023-2028 ²⁾
• IT Security	+10,8% CAGR 2023-2028 ²⁾
• Secure Access Service Edge (SASE)	+13% CAGR 2023-2028 ³⁾
• Communication Providers (CPaaS)	+14% CAGR 2023-2028 ⁴⁾

¹⁾ Dell Oro, Q2 2024

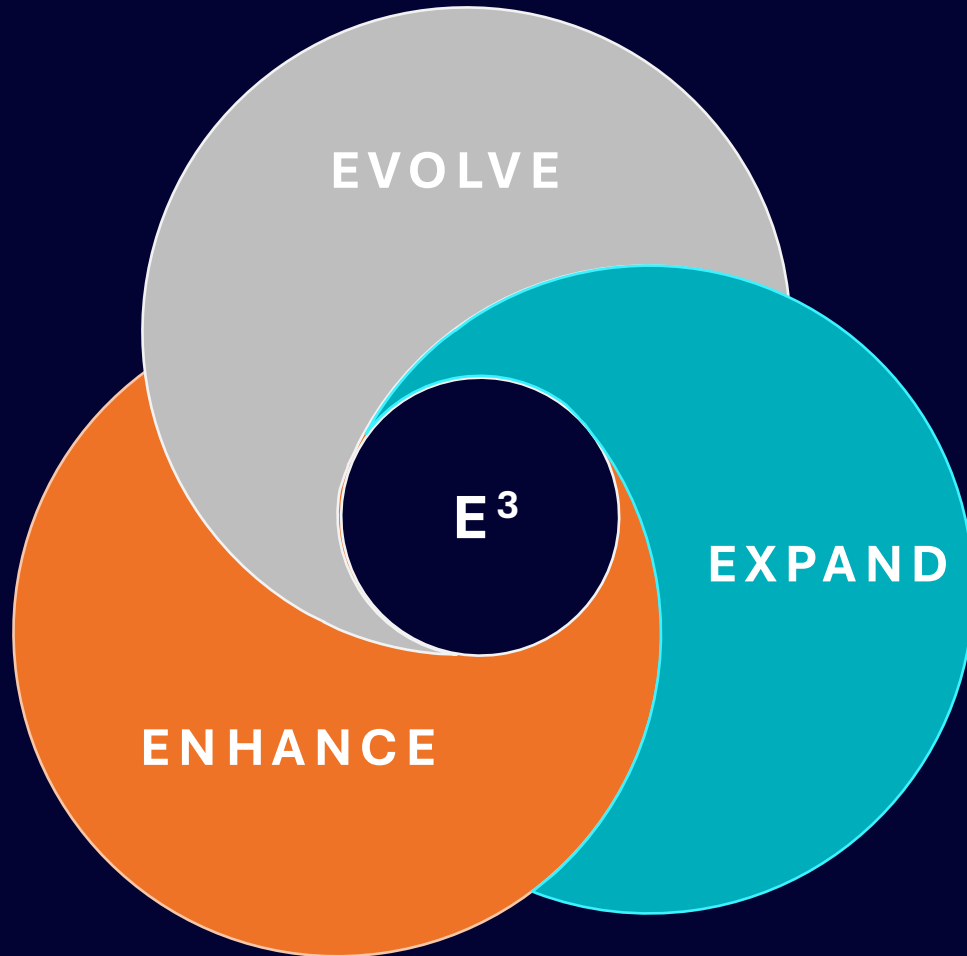
²⁾ GlobalData, July 2024 report

³⁾ Q2 2024 Dell' Oro, Mobile Core Network, excluding China

⁴⁾ Mobilesquared, CPaaS remains an under-utilised;

⁵⁾ Gartner, Top Trends in Cybersecurity, 2024

Growth Strategy & Choices



Evolve

- Zero Trust Signaling Protection
- Unified Telecom and IT threat detection systems
- AI-based classification the blinding encryption (TLS 1.3/ECH)

Expand

- Multichannel messaging AI-based messaging defense
- AI-based anomaly detection for Signaling threats hunting
- Cybersensor addressing the MSSP & “Non-Code” market

Enhance

- Voice Firewall CLI Spoofing, Wangiri, Robocalls
- Threat Detection with DPI visibility & metadata
- Qosmos Probe Cyberdefence and Governments

ENEAA

Don't be Surprised.
Be Ready.

www.enea.com