No.49
July 20th 2021

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security **PUBLIC/UN-SPONSORED**

ENEA Buys AdaptiveMobile Security

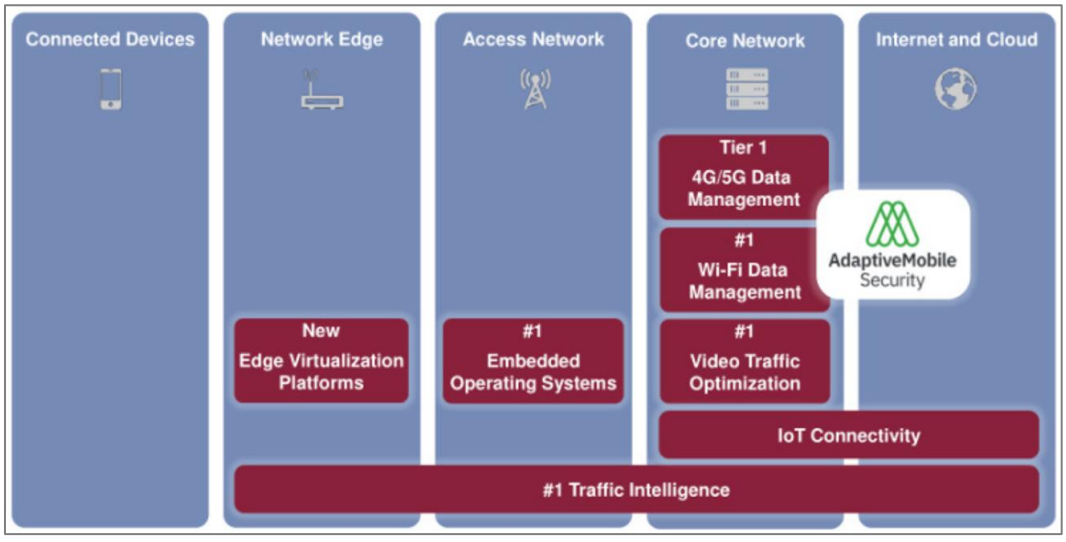
- ENEA looks like a good parent for AdaptiveMobile Security. AdaptiveMobile looks like a good fit for ENEA. Both vendors' customers should welcome this acquisition.
- The portfolios are complementary. Combining ENEA's DPI and data management strengths and AdaptiveMobile's control plane security drives a broader portfolio and faster innovation in 5G network security, including potentially in GTP Firewalls.
- Medium sized players like ENEA must be able to succeed through M&A to assure telcos the sustainable supply chain diversity that they need – and that government regulators require of them – in 5G core software.

Ever looked at a merger or acquisition of tech companies and wondered 'what on earth is that all about?" This isn't one of those.

On Thursday July 15th, ENEA announced the acquisition of AdaptiveMobile Security, the Dublin-based mobile network security specialist focused on signaling and messaging security. ENEA presented AdaptiveMobile to investors as having 135 employees and 80 mobile operator customers protecting more than 2 billion subscribers worldwide. AdaptiveMobile recorded net sales of €15.5 million in 2020, more than half of which came from recurring revenue. Its' annual sales are expected to grow by 10% in 2021 to reach €17.0 million. The acquisition was done at an enterprise value of €45.0 million.

Ever looked at a merger or acquisition of tech companies and wondered 'what on earth is that all about?" This isn't one of those. These two look like a good fit. ENEA's core branding - as a provider of "Innovative software for telecoms and cyber security" could easily be AdaptiveMobile's. ENEA reported revenues of SEK 915 million (€89 million) in 2020. Approaching three quarters of its revenues come from its Network Solutions business, which has been built up via previous acquisitions such as Openwave Mobility,

Complementary Portfolios That Target Telco Networking and Security Needs



Source: ENEA

(NFV platforms), Qosmos (Deep Packet Inspection engines), and Aptilo (policy and access controls for IoT and Wi-Fi). A substantial share of ENEA's Network Solutions business already drives a number of aspects of telecom network security.

As an example, in May this year, ENEA announced its participation in a multi-vendor, deployment of a 5G Stand Alone (5G SA) network with Telenor. This deployment supports network slicing on a 5G core. ENEA supplied a number of cloud native, 3GPP-specified 5G core network functions including its Unified Data Manager (UDM), User Data Repository (UDR) and Authentication Server Function (AUSF). One lead customer in the deployment, the Norwegian Armed Forces, has been leveraging the 3GPP-specified Subscription Concealed Identifier (SUCI) embedded in ENEA's UDM in its network slice.

This Acquisition Speaks to Two Critical Telco Requirements

This acquisition speaks directly to two critical requirements that telcos have, neither of which are new but they have nevertheless been given a lot of new impetus by the way the global telecom market has changed over the last two or three years.

A potentially significant opportunity for innovation lies in AdaptiveMobile leveraging ENEA's leadership in DPI for end-to-end threat monitoring, detection and mitigation across the mobile core.

- **Simplifying Increasingly Complex Security Requirements.** Cyber threats pose a substantially bigger challenge than they did. As security requirements become increasingly complex, many well-resourced telcos will continue selecting best of breed network security solutions from multiple vendors and integrating them themselves. Many others, however, will prefer to draw on rich, comprehensive, network security portfolios served up by a single vendor of the kind ENEA is building.
- **5G Core Supply Chain Diversity and Resilience**. A lot of western governments have prohibited their telcos from using Huawei for 5G on national security grounds. This leaves those telcos uncomfortably dependent on Ericsson and Nokia (and maybe Samsung) as primary end to end 5G system suppliers. It's therefore imperative for innovation and price competition in the telecom software market that independent suppliers of 5G core network functions should succeed. That, in turn, requires that medium sized players like ENEA grow through M&A. Hence it requires that smaller players like AdaptiveMobile can get access to the investment capital, account access, and economies of scale in R&D and SG&A that acquisition by a bigger player like ENEA offers.

ENEA's a Good Partner for AdaptiveMobile – and its' Customers

Sitting as it does in the core of the mobile network, AdaptiveMobile sees a lot of malicious traffic from bad actors, including nation states, from all over the world. This week's release of the first findings from the 'Pegasus Project', detailing widespread and continuing abuse of NSO Group's mobile phone hacking spyware, is only the most recent example of that type of threat, albeit a very high profile one. This gives AdaptiveMobile a highly sensitive, highly trusted, role in the mobile network.

On that front, customers should welcome ENEA as its new owner. AdaptiveMobile's management could have been tempted by an offer from private equity or from a vendor based in a country that might have made some customers and government regulators uncomfortable. Headquartered in Sweden, ENEA is highly unlikely to spark customer objections the way other buyers might have.

In terms of direct synergies, ENEA points to how the network signaling protected by AdaptiveMobile connects with ENEA's UDM portfolio. But that's pretty low hanging fruit. A potentially significant opportunity for innovation lies in AdaptiveMobile leveraging ENEA's leadership in DPI for end-to-end threat monitoring, detection and mitigation across the mobile core. ENEA's Qosmos ixEngine is an advanced DPI based classification engine that recognizes over 3,500 protocols. With its' approach to 'First Packet Processing', ENEA is targeting a number of networking and security use cases including SD-WAN and Secure Access Services Edge (SASE).

ENEA's DPI has strong potential to provide visibility into GTP-U traffic on the user-facing side of the 4G and 5G mobile core, something which AdaptiveMobile lacks as of today. This option could potentially take AdaptiveMobile into contesting the GTP Firewall space against the likes of A10 Networks, Palo Alto Networks, Juniper Networks, and Fortinet, albeit with potential to differentiate with control plane security.

Differentiation in 5G security is going to come from security monitoring and policy enforcement beyond what is currently specified by 3GPP. Threat intelligence-driven correlation between what AdaptiveMobile sees from GTP-U inspection across 4G and 5G with what it can already see from inspecting GTP-C on the telco network side in 4G and HTTP/2 in 5G is an obvious direction for AdaptiveMobile's roadmap to take. ■

More Information

- ENEA Q2 2021 Webcast with CEO, Jan Haglund, announcing the acquisition of AdaptiveMobile Security.
- HardenStance White Paper: "Supply Chain Security for Telecom Operators"
- HardenStance White Paper: "Learnings from Real World Telco Security Incidents"

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a leader in custom cyber security research and leading publisher of cyber security reports. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The Cyber Threat Alliance, The GSM Association, OASIS, ETSI and TM Forum.

HardenStance Disclaimer