No.15
13th November 2018

HardenStance Briefing

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

Palo Alto Networks joins NGMN Alliance

Sponsored by Palo Alto Networks

- Palo Alto Networks is joining the NGMN Alliance as a Contributor to its work in driving the long-term architectural direction of mobile networks.
- It's good that Palo Alto Networks is joining. Other security vendors targeting the telecom operator market should consider joining the NGMN Alliance too.

It's good to see a leading network security solutions vendor like Palo Alto Networks joining the Next Generation Mobile Network (NGMN) Alliance as announced in the company's blog last Friday.

NGMN's members comprise C-Level – and only C-Level – representatives from most of the world's largest mobile operators. Think of a big-name operator and they're almost certainly a member. NGMN isn't as big – its power and influence isn't quite as far-reaching – as 3GPP, the global mobile standards body, or the GSM Association (GSMA). Nevertheless, it still plays a critical role in the mobile communications ecosystem.

NGMN focuses its attention on the ten-year planning horizon. Through its role as a Market Representation Partner (MRP) to 3GPP, NGMN provides direction around key architectural and operational requirements for mobile network evolution, including network security requirements.

NGMN plays a critical role in the mobile communications ecosystem.

For 5G, NGMN's 5G Security Group, previously led by Editors from Orange and Vodafone and now by Telecom Italia, has already published four reports with recommendations. The first three were on improving the access network; security threats arising with network slicing; and a third on mobile edge computing, low latency and consistent user experience. The latest, published in September, is on "Security Aspects of Network Capabilities Exposure in 5G."

NGMN has already made its mark on mobile network security by pulling together security expertise from within its operator members and a few Contributor networking vendors that happen to have a security division. But prior to Palo Alto Networks joining, the number of NGMN Contributors from among pure-play security companies numbered – wait for it – just one (Gemalto). So now there are twice as many pure-play security Contributors but is that enough?

Mobile networks are among the top targets of nation-state attackers

Operators have always been driven both by governments and their own commercial best interests to operationalize their networks and business processes to high standards of security and privacy. But the bar is being raised substantially now. 5G will be the first 'G' to launch in the era of intense - and intensifying - cyber-security threats. Critical infrastructure like mobile networks are among the top targets of nation state attackers.

Governments are driving new data protection like GDPR. Enterprise customers are having to navigate the same landscape of rising business risk arising from cyber threats. They don't just want technology partners that don't pose a risk to them. They want technology partners that can actively enhance their security posture.

Consider the challenge of augmenting the mobile network security architecture so that operators are equipped to defend against all the attacks that will be unleashed on them

in the years ahead – but without materially compromising on the richness, flexibility and ease of use of the new 5G growth engine that everyone wants. That's a big ask.

Some of the critical capabilities that pure-play security companies can bring to NGMN as Contributors include intimacy with the following:

- the long-term roadmaps for different security technologies and their potential as they are augmented with analytics, artificial intelligence and blockchain;
- the direction of travel in enterprise security as well as cloud and multi-cloud security. Through this, security specialists can bring NGMN insights into the way that enterprise, cloud and multi-cloud security will intersect with 5G;
- the performance and efficacy of security software in telecom networks as new releases evolve though different environments from virtual machines to containers, serverless computing and future variants.

Deutsche Telekom wants to be the largest provider of cyber security services in Europe within five years.

It's not as if being a Contributor to NGMN is just about contributing, either. There's plenty that a security vendor can take out too. For security vendors targeting the telecom operator vertical, there's the low-hanging fruit of early visibility into the security products that operators will need to protect their own network infrastructure.

More than that, many leading telecom operators are intent on growing their share of the enterprise security services market. Deutsche Telekom wants to become the largest provider of cyber security services in Europe within five years. AT&T recently acquired AlienVault as part of a long-term strategy to grow share. Having signaled its intent in this space with the acquisition of Trustwave in 2015, Singtel is rolling out enterprise security services across affiliates in Asia Pacific and further afield.

Greater software programmability and distribution of network functions to the edge are assured as mobile networks evolve to 5G. Operators are uniquely placed to exploit this in pursuit of growing enterprise security revenues. This is because it will create potential for greater meshing of enterprise and telecom networks than we have seen before – hence greater meshing of the operator's security functions with those of its enterprise customers.

I welcome the decision of Palo Alto Networks to join the NGMN Alliance. It should serve as a win-win. It would be good to see some other security companies join too. ■

- Contact HardenStance's Principal Analyst**:** patrick.donegan@hardenstance.com

- Register here for **free email notifications** whenever new IT and telecom security content is made available by HardenStance.
- **www.hardenstance.com**

HardenStance Ltd Disclaimer of Warranty and Liability

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, noninfringement, merchantability or fitness for a particular purpose of any material covered by this report.

HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd's negligence or by contingencies beyond HardenStance Ltd's control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same. The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.