Security in a Virtualized Network Environment

EXECUTIVE SUMMARY

Over the last year or so, security of networks of all kinds has risen up the news agenda as evidence of major information and communications technology (ICT) systems being compromised or data stolen come to light. Scarcely a week goes by without another story. And if security has become one of the major real-world tech storylines, then virtualization has matched it for newsworthiness inside the telecom industry.

So it is not surprising that many inside telecom are asking: "What is the impact on security of virtualizing network functions and the infrastructure on which applications run and from where services are delivered? Will virtualization help or hinder efforts to be secure? Will security have to be completely rethought, or do the same principles apply in a virtualized world as in the physical?"

As network operators forge ahead with efforts to virtualize and distribute their network functions, as well as build new sets of services from resources within their data centers and from elsewhere, they are discovering that these processes potentially open up their networks to new types of security risk. At the same time, operators can see the opportunities they have to help their business customers with security: It's a pressing concern for businesses of all sizes – and something that many do not have the skills or resources to keep on top of for themselves.

Network, application and data security is under the spotlight as never before. And the open nature of "the cloud" means that it's not possible to simply build higher walls and dig deeper moats round network infrastructure. Much of the old thinking needs to be jettisoned. It will be a wise operator that calls in advice from those that have done the deepest thinking and that can demonstrate the most credible vision. The stakes are very high.

Security in a Virtualized Network Environment considers how virtualization changes the state of security in telecom, both from the perspective of carriers’ own network security and the opportunities that arise to deliver managed security services to business customers. It digs into the challenges of securing virtualized and hybrid network environments, as well as the approaches, solutions and products that are being suggested and deployed. It reviews the supply-side landscape for relevant products and profiles 14 leading suppliers, ranging from large network equipment providers to smaller specialists.

VIEW TABLE OF CONTENTS

The report delivers a timely and important competitive analysis in this rapidly growing market, including these 14 leading suppliers.
There is a very broad range of solutions to these challenges proposed by vendors, which generally fall into one or more of the domains shown in the following excerpt. The space is complex and no hierarchy is assumed – virtualization tends to collapse and blur layered models. Some vendors position their solutions within more defined layers, which can be seen in figures later in the report.

**Excerpt: Where Security Can be Addressed as Services & Network Functions Virtualize**

![Diagram of security domains](source: Heavy Reading)

**Security in a Virtualized Network Environment** is published in PDF format.