

ETSI SECURITY WEEK - SETTING THE SCENE FOR NFV CHALLENGES

Michael Lazar – DataArt

Michael.Lazar@dataart.com

THE NETWORK FUNCTION VIRTUALIZATION (NFV) "PROMISE"



Service Providers want to make their networks agile and efficient to meet the challenges of exponential bandwidth demands and be able to create revenue streams with innovative services and new business models.

Network Function Virtualization (NFV) and Software Defined Networking (SDN) has emerged as the paradigm that has the potential to transform these the industry by delivering cloud style agility and innovation and enhancing economic viability.

By 2020 SNS Research estimates that SDN and NFV can enable service providers (both wireline and wireless) to save up to \$32 Billion in annual CapEx investments

ACG Research estimates that NFV will reduce capital expenditure by 68% and reduce operating expenditure by 67%

NFV Security – No one said this will be easy



VIRTUALIZATION AND SECURITY

DATAART

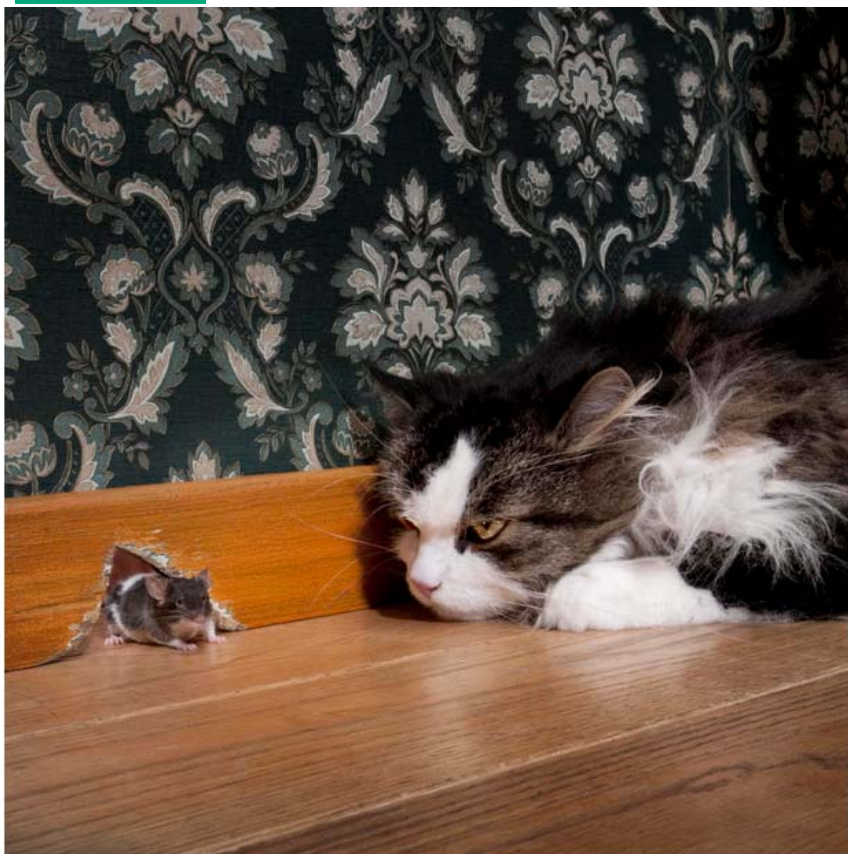
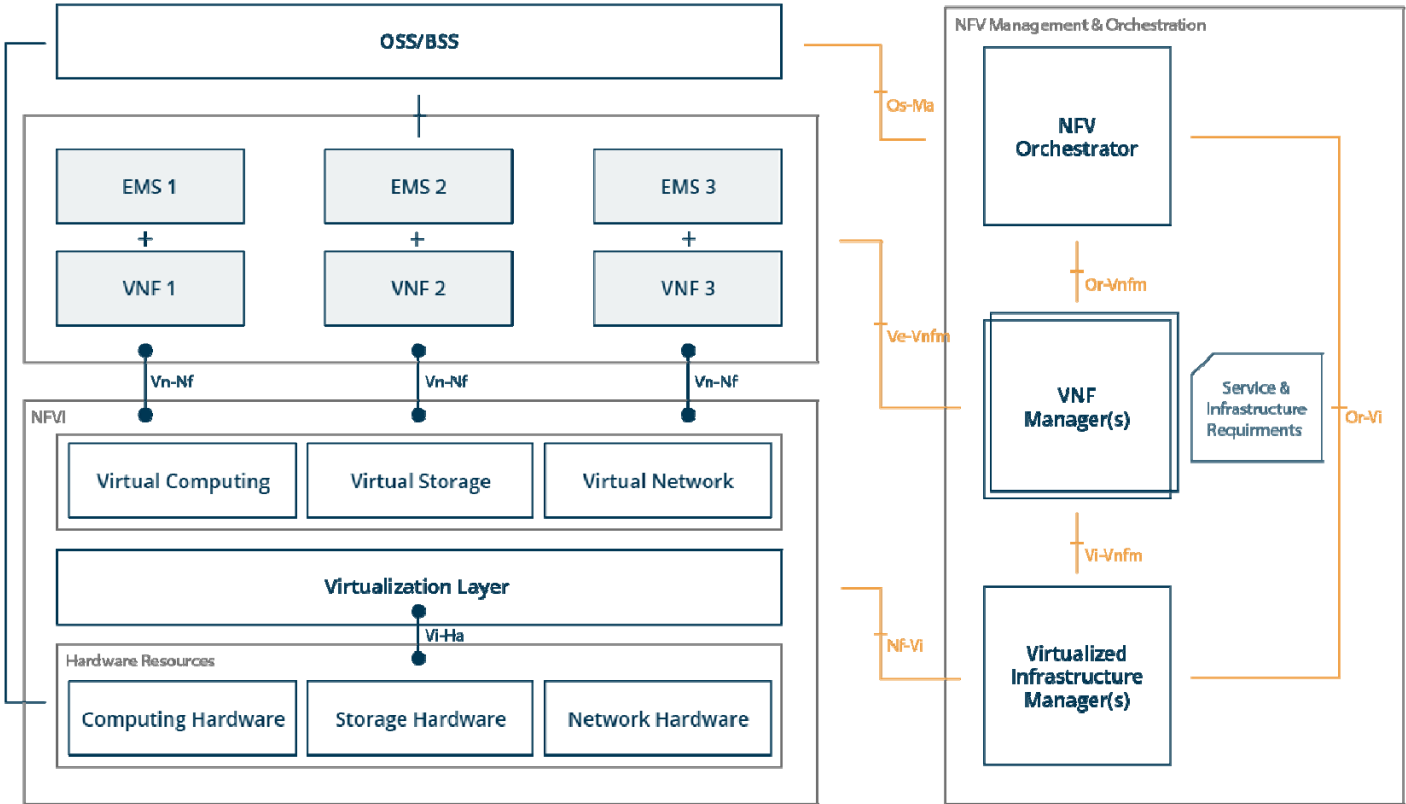


Image - Eric Isselée

- Security is and always will be a cat-and-mouse game
- Tradeoffs between performance and security may need to be made but the impact should be understood
- Low level security provides a foundation to build on
- Some remediation techniques can add significant management burdens
- Virtualization brings unique security issues that may not be apparent until everything is put together (fully functional system)
- **SECURITY IS EQUAL PARTS PROCESS, PEOPLE AND TECHNOLOGY –**
Technology alone is never the answer

ETSI NFV REFERENCE ARCHITECTURE



● — ● Execution Reference Points + Other Reference Points + Main NFV Reference Points

ETSI Security Week NFV

- **Session 1: NFV Security Challenges: Today and Future**
- **Session 2: NFV Security Monitoring and Management**
- **Session 3: Building on the Roots of Trust**
- **Session 4: Panel Discussions – Industry Perspective on NFV**
- **Wrap up and concluding remarks**