MPLS+SDN+NFVWORLD
→PARIS2017

SHIELD

SECURING AGAINST INTRUDERS AND OTHER THREATS
THROUGH A NFV-ENABLED ENVIRONMENT
[H2020 - Grant Agreement No. 700199]

https://www.shield-h2020.eu/

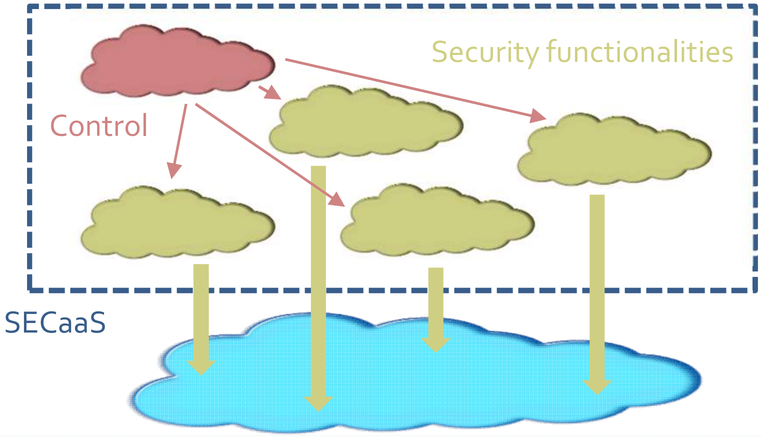
Security Enhancements

By means of NFV and Cognitive Security

Managed Security Services (MSS) and NFV

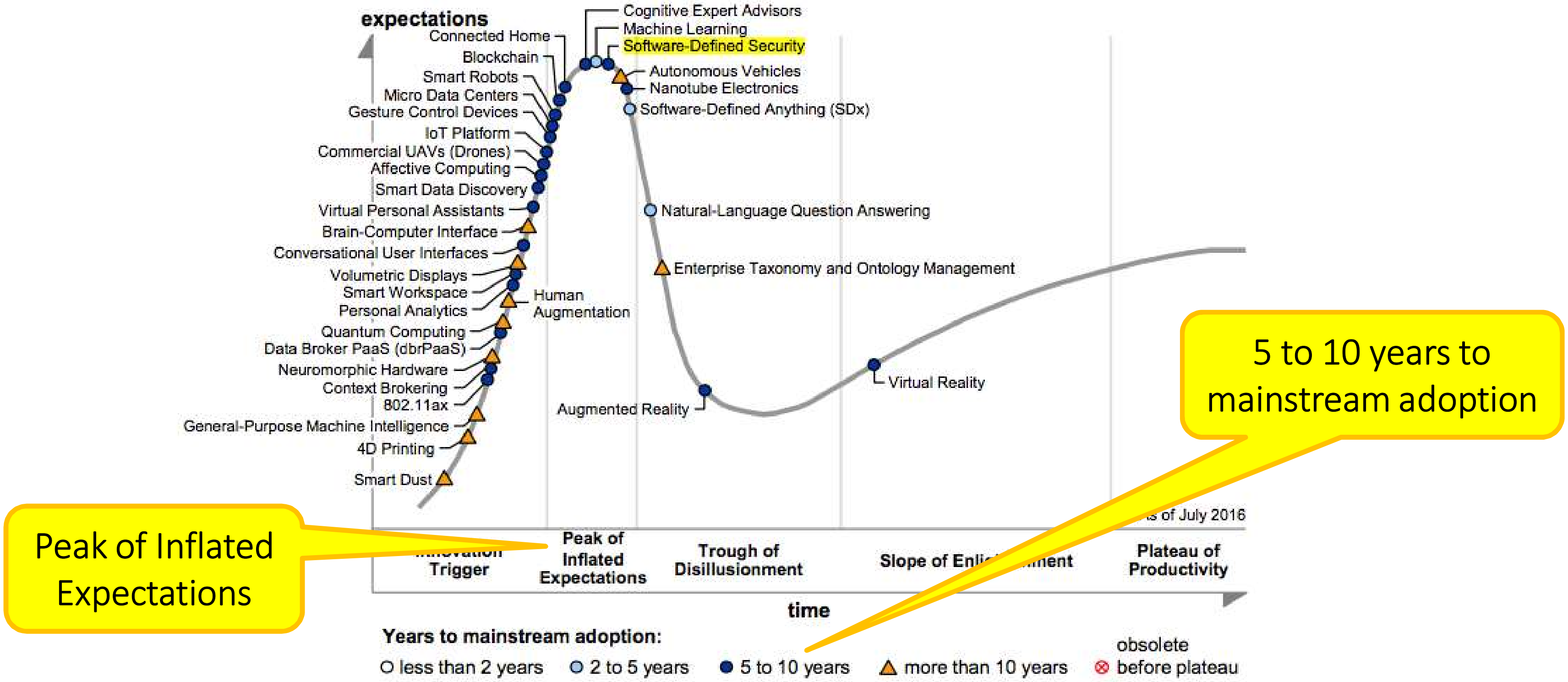
- NFV becomes a key enabler for security services
  - Security VNFs are emerging (new or legacy appliances)
  - New security services are demanded

- Next Steps: create dynamic security policies abstracted from the underlying hardware or location
  - Multiples names for this concept
    - Security as a Service (SECaaS)
    - Software-Defined Security (SDSec)



Is the technology mature?

Gartner Inc.'s Hype Cycle for Emerging Technologies, 2016



Peak of Inflated Expectations

5 to 10 years to mainstream adoption

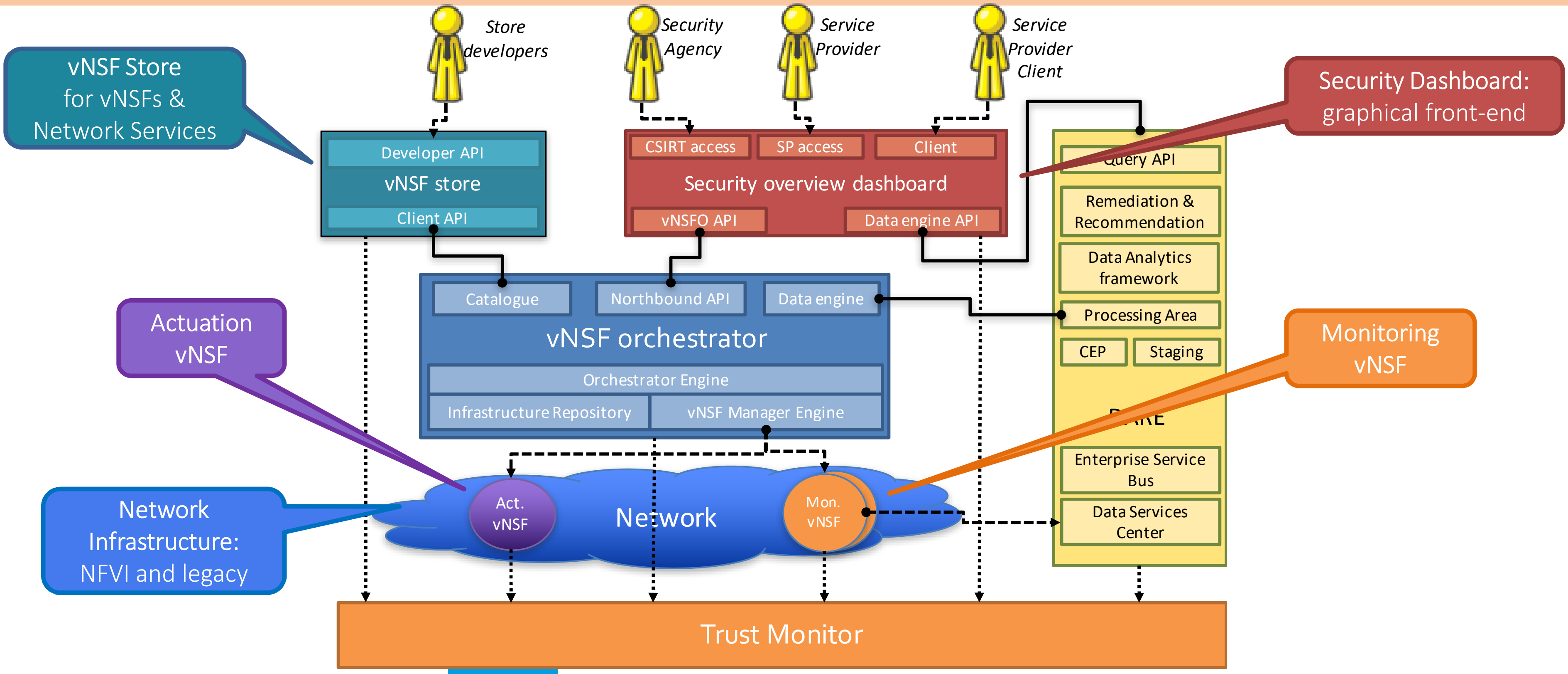
Challenges for NFV-based security services

- DevOps applied to security
  - Agile onboard, instantiation and scale
  - Quick integration of new security capabilities (a.k.a. third-party VNFs)
- Visibility and control on virtualized and dynamic environments
  - Attestation and validation of topologies (SDN) and applications (NFV)
  - Dashboards and metrics
- Cognitive knowledge applied to security
  - Network-based Big Data (i.e. traffic flows, application logs, etc.)
  - Machine Learning algorithms

Proposed solution: *SHIELD*

- New telco-oriented Cybersecurity Framework
  - EU H2020 program from Sept-2016 to Feb-2019
- Security as a Service based on NFV+SDN architecture
  - ETSI MANO reference model
- Includes Big Data engine and Machine Learning capabilities
  - Real-time incident detection and mitigation
- Support virtualized security appliances as VNFs
  - Virtualized Network Security Functions or vNSF
- Trustworthiness
  - Pervasive Trust Computing in NFVI , VNFs (VM and Containers) and SDN

SHIELD High Level Architecture



Store developers

Security Agency

Service Provider

Service Provider Client

vNSF Store for vNSFs & Network Services

Developer API

vNSF store

Client API

CSIRT access

SP access

Client

Security overview dashboard

vNSFO API

Data engine API

Security Dashboard: graphical front-end

Query API

Remediation & Recommendation

Data Analytics framework

Processing Area

CEP

Staging

DARE

Enterprise Service Bus

Data Services Center

Catalogue

Northbound API

Data engine

vNSF orchestrator

Orchestrator Engine

Infrastructure Repository

vNSF Manager Engine

Actuation vNSF

Monitoring vNSF

Network Infrastructure: NFVI and legacy

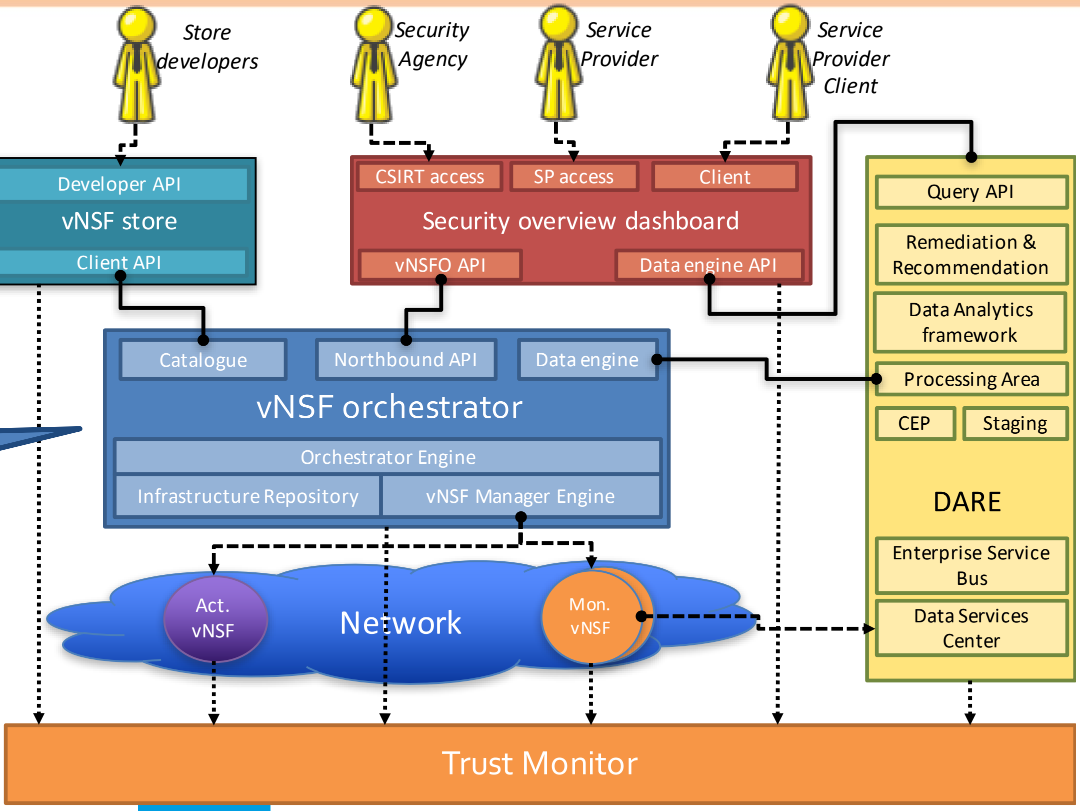
Act. vNSF

Network

Mon. vNSF

Trust Monitor

SHIELD High Level Architecture



vNSF orchestrator managing vNSF lifecycle

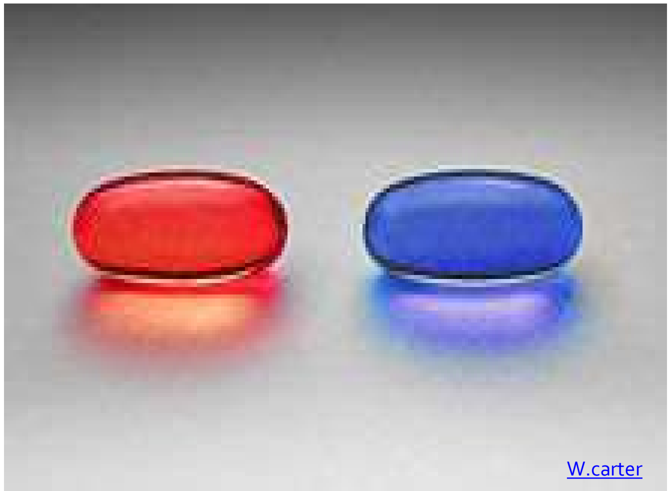
Trust Monitor attesting infrastructure & services, validating their integrity

Data Analitics & Remediation Engine real-time analysis, incident detection and mitigation

Where is cognitive security?

- Machine Learning algorithms applied to network traffic
  - DARE is the module in charge of applying Machine Learning techniques

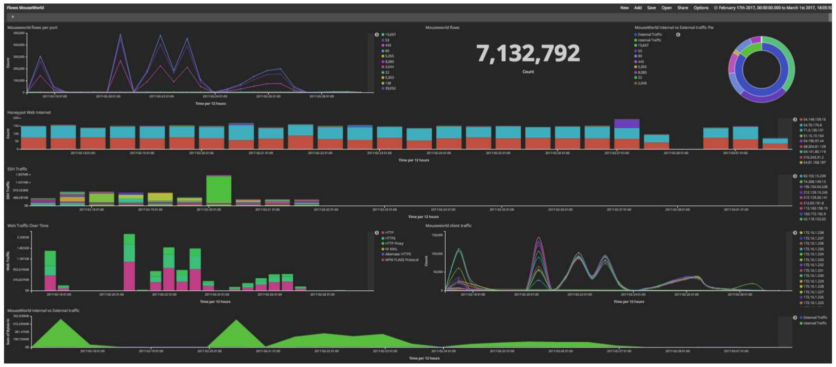
- How can we train algorithms?
  - Real traffic
    - High volume and performance required
    - Privacy concerns arise
    - Best in final stages of testing and validating
  - Synthetic traffic
    - Controlled environment
    - Tagged traffic for supervised training
    - Volume and type of traffic based on needs
    - Best in initial stages to test different algorithms

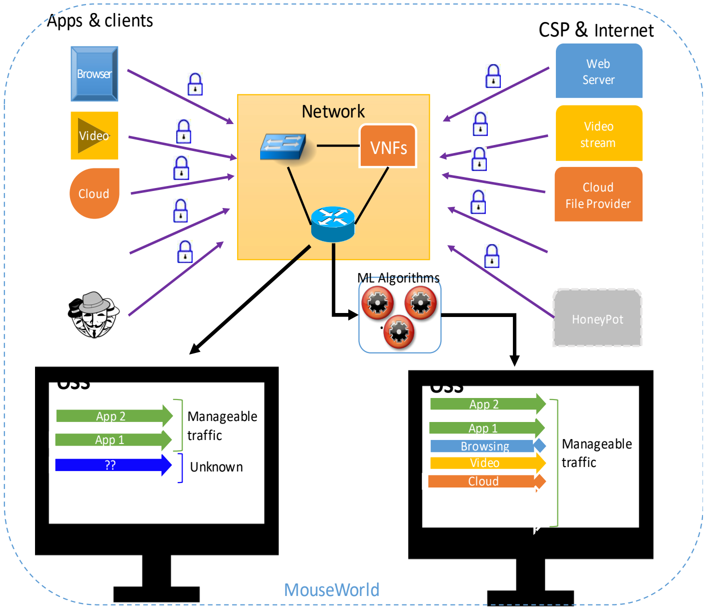


W.carter

Telefonica's Mouseworld

- Synthetic traffic laboratory
  - An environment that allows to apply Machine Learning (ML) concepts in a controlled way
  - Using configurable mixes of synthetic and real traffic
  - Including mechanisms like honeynets and adapted malware
- Initially conceived as part of the CogNet[1] project


Flows MouseWorld
New Add Save Open Share Options
February 17th 2017, 00:00:00.000 to March 1st 2017, 18:05:5
Mouseworld flows per port
Time per 12 hours
Mouseworld flows
7,132,792
Count
MouseWorld Internal vs External traffic Pie
External Traffic
Internal Traffic
Honeypot Web Internet
SSH Traffic
Web Traffic Over Time
HTTP
HTTPS
HTTP Proxy
NI MAIL
Alternate HTTPS
MPM FLAGS Protocol
Mouseworld client traffic
MouseWorld Internal vs External traffic



[1] http://www.cognet.5g-ppp.eu/

Thank you !!

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 700199.
This text reflects only the author's view and the Commission is not responsible for any use that may be made of the information it contains.