Heavy Reading White Paper

The Antifragile Telco: Assuring the Virtualized Network

James Crawshaw – Senior Analyst, Heavy Reading

BY

ABHISHEK GUPTA

FRIDAY GROUP MEETING

APRIL 13, 2018

UCDAVIS

Antifragility

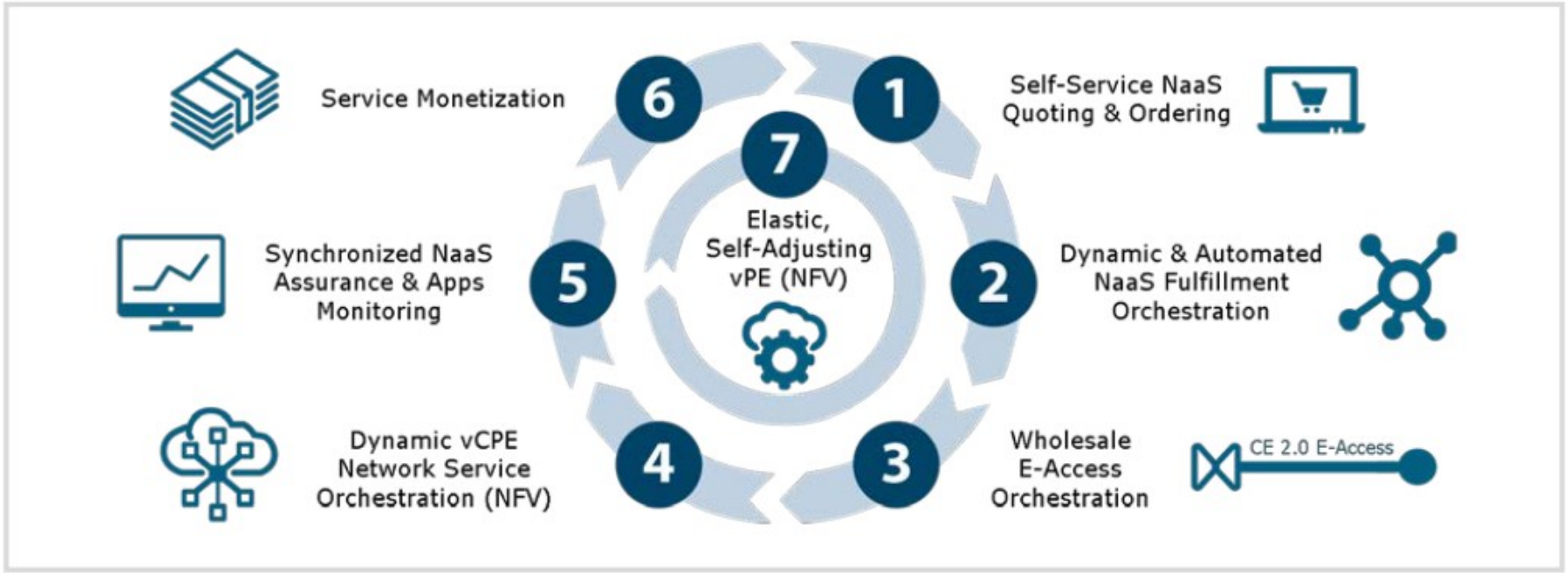
- Distinct from robustness and resiliency
- Robustness: resist failure
- Resiliency: recovery from failure
- Antifragile: benefit from stressors, faults and attacks, by becoming more robust and resilient

Antifragility in ICT

- Five design principles: modularity, weak links, redundancy, diversity and fail fast
- Can anti-fragile telecom systems be built using cloud-computing technologies?
- Deliberately introducing local failures to quickly detect vulnerabilities is one way.
  - Important to monitor since all failures cannot be simulated. So, a monitoring infrastructure is required

Antifragile Service: Zero-Touch NaaS over an Elastic Network

Figure 1: Zero-Touch NaaS Over an Elastic Network



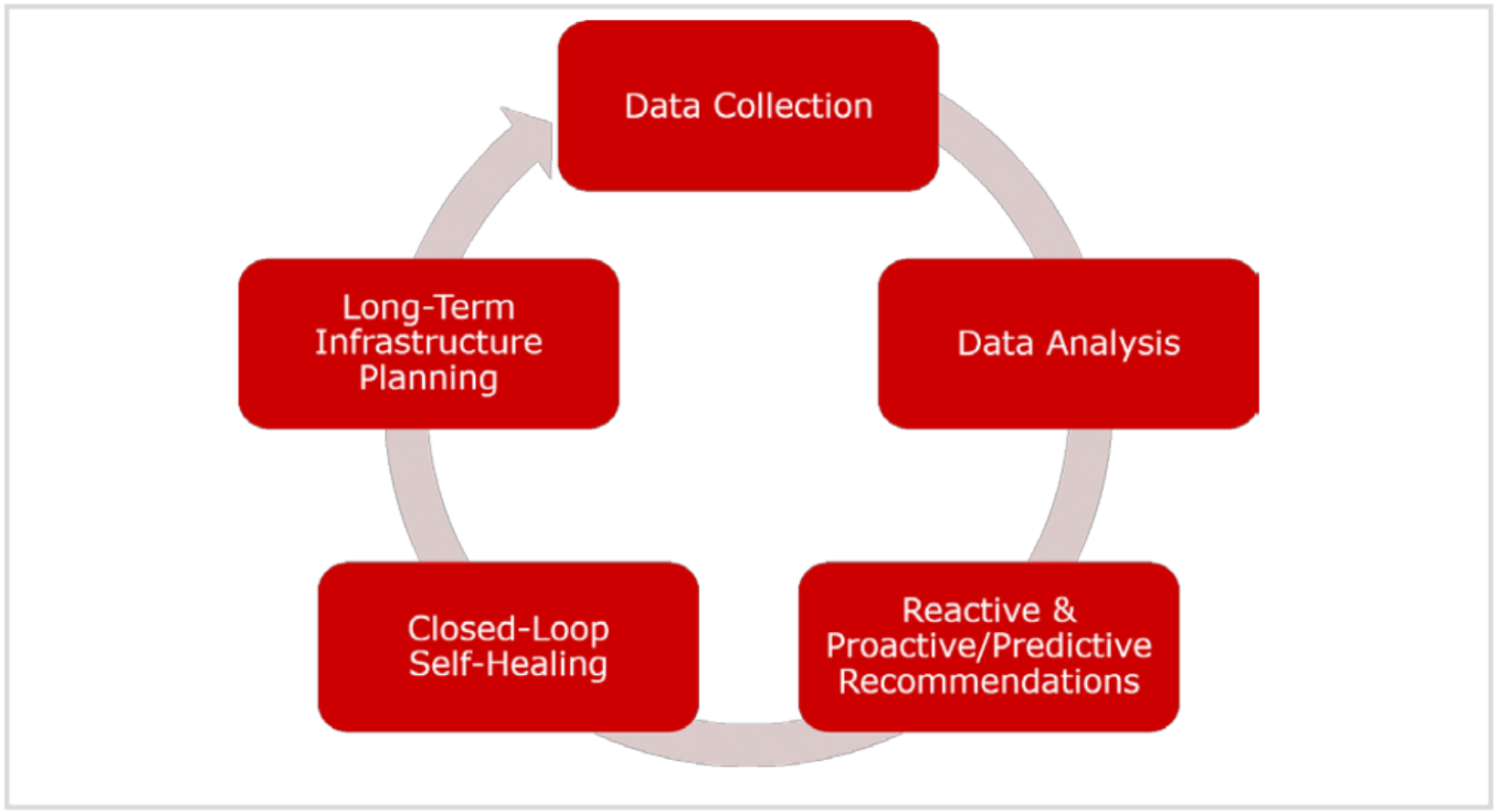
Source: InfoVista

- Above applies for 5G mobile networks since elastic transport network with network slice and SLA support will be required.
- Monitoring is key: a smart network must learn from these failures to reduce the probability of their recurrence.

UC DAVIS
UNIVERSITY OF CALIFORNIA

Service Assurance – Key to Network Performance

Figure 2: Service Assurance Cycle for the Antifragile Network



Source: Heavy Reading

Service Assurance Challenges of NFV

- SLAs that elastic network will fulfill.
- Operating environment is highly dynamic because of customer requirements.
- Problems in physical layer can be propagated up to virtualized layer. Fault isolation becomes difficult.
- Increased automation requires reliable monitoring systems.
- Current assurance systems: alarm-based and reactive. Deployed in vendor-specific silos. Lot of integration work.

Rules-Based Alarm, Passive and Active Probes

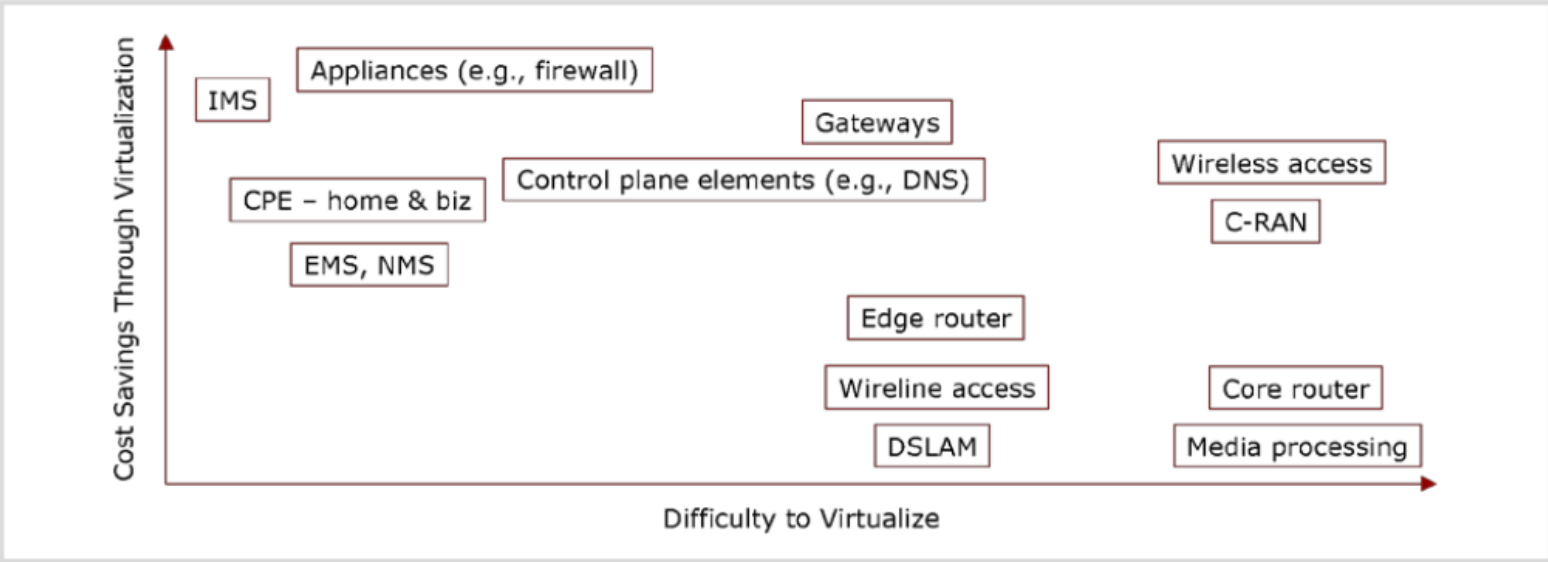
- Hardware issue can raise alarm at software layer. So, 2 sets of alarms are triggered.
- Additional intelligence for dynamically tracing interactions between different layers.
- This is facilitate correlation between faults with impacts on VNF performance.
- These correlations need to be change from static to dynamic owing to the dynamic nature of NFV.
- Further, service assurance platforms will need to support APIs.

Continued….

- NFV introduces new sources of data for service assurance like NFVI, VNFs and management layers (VIM, NFVO, etc).
- The probes also need to be virtualized.
- Passive virtual probes on VNF interface:
  - Detailed VNF transaction records (flow, session and transaction records).
  - Control-plane message stream.
  - User-plane stream.
- For gray failures, active probes are required:
  - Generate synthetic traffic to measure performance metrics for SLA (latency, availability, completion rate, defect rate, QoS, etc.).

Hybrid Networks Will Persist Indefinitely

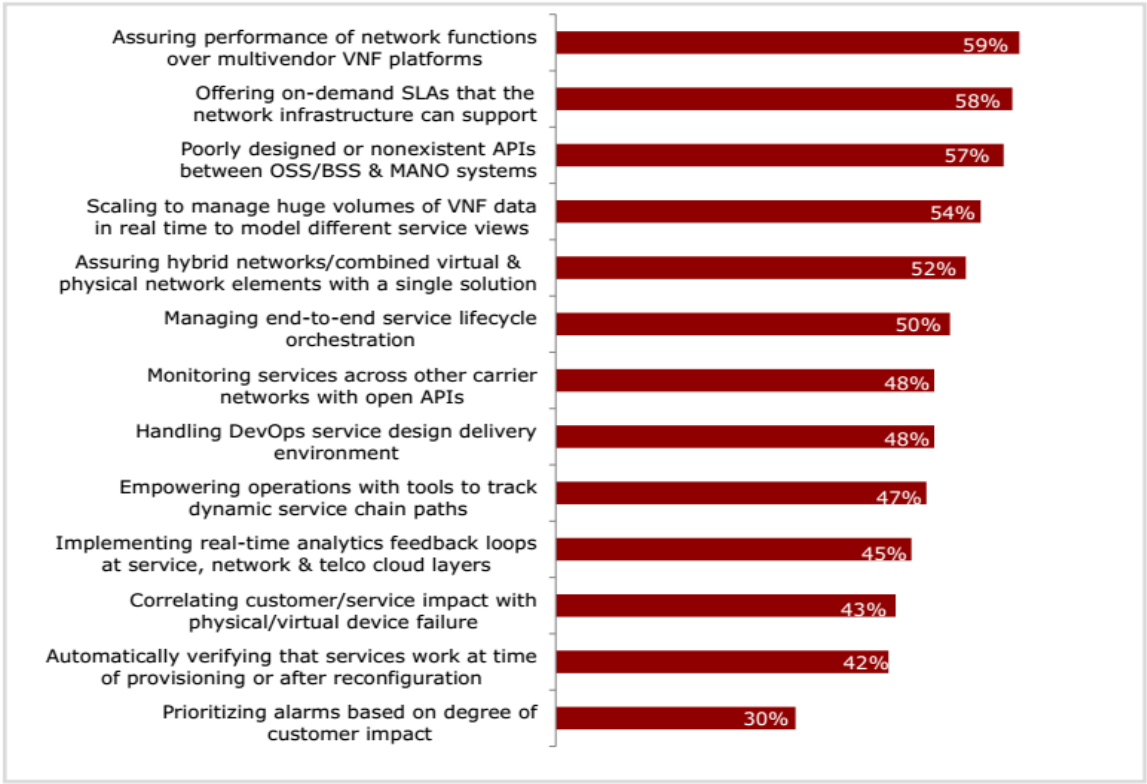
Figure 3: Cost-Difficulty Trade Off for NFV



Source: Heavy Reading graphic, adapted from Medamana & Siracusa, "Building the Network of the Future," Chapter 3 – Network Functions Virtualization

Key Challenges for NFV Assurance - Survey

Figure 4: Service Assurance Challenges of NFV

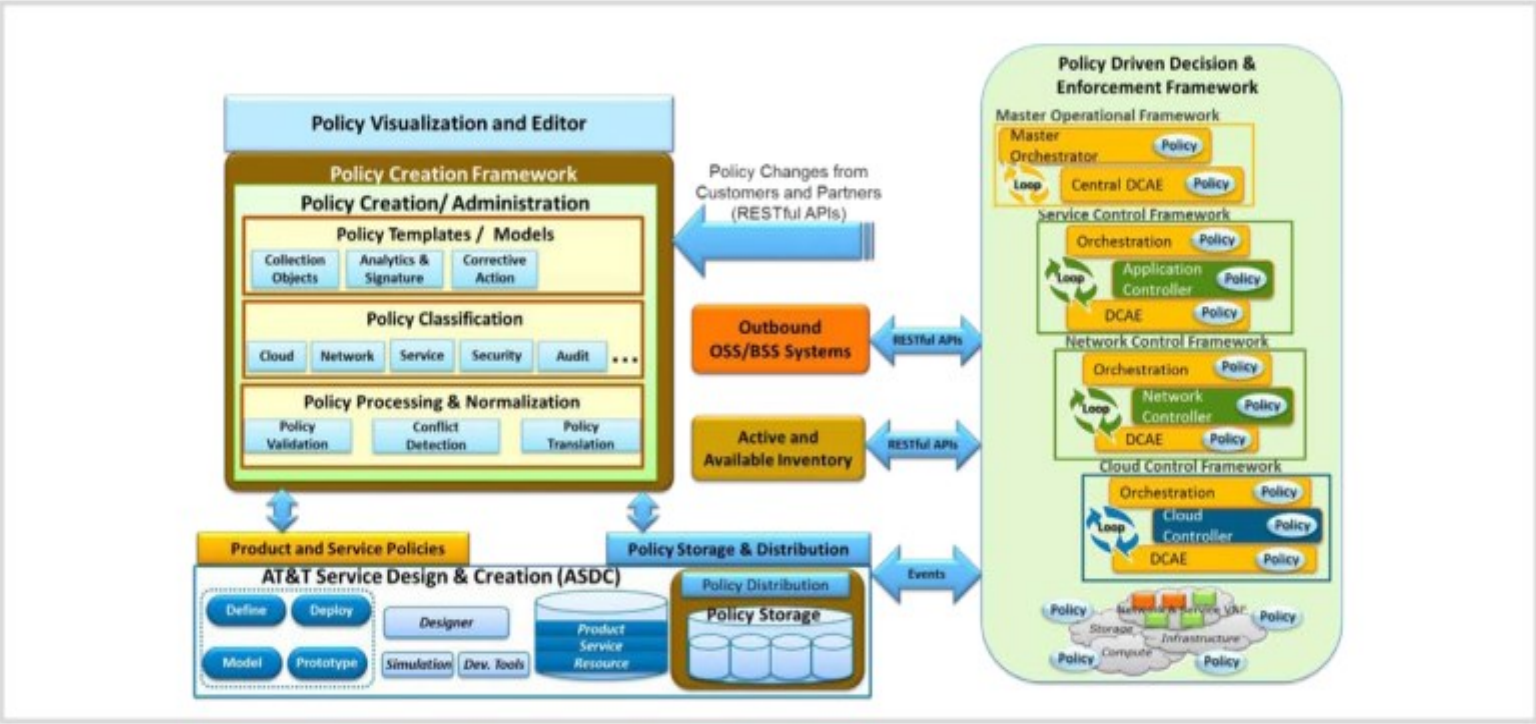


Source: Heavy Reading survey, September 2017; n=102. Measure is sum of responses indicating a service assurance function was a massive or significant challenge, as opposed to moderate, minor or no challenge.

UCDAVIS
UNIVERSITY OF CALIFORNIA

Service Assurance – Delivery Targets

Figure 5: Domain 2.0 Policy Platform Architecture

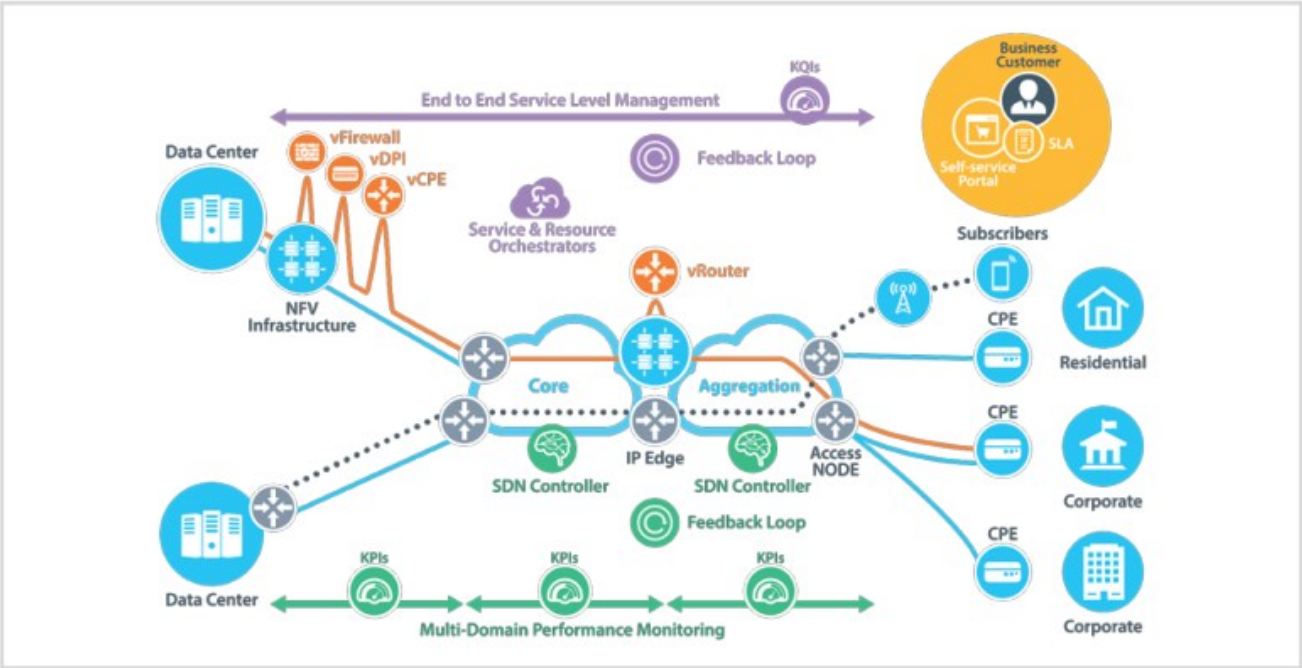


Source: AT&T

Continued…

- Programmable configurations to enable greater automation.
- Open and published API for interoperation.
- Service assurance system should be common across network.

Figure 7: End-to-End Service Level Management



Source: InfoVista