Hewlett Packard
Enterprise

SDN / NFV panel @ SBRC

Sébastien Tandel
sta@hpe.com
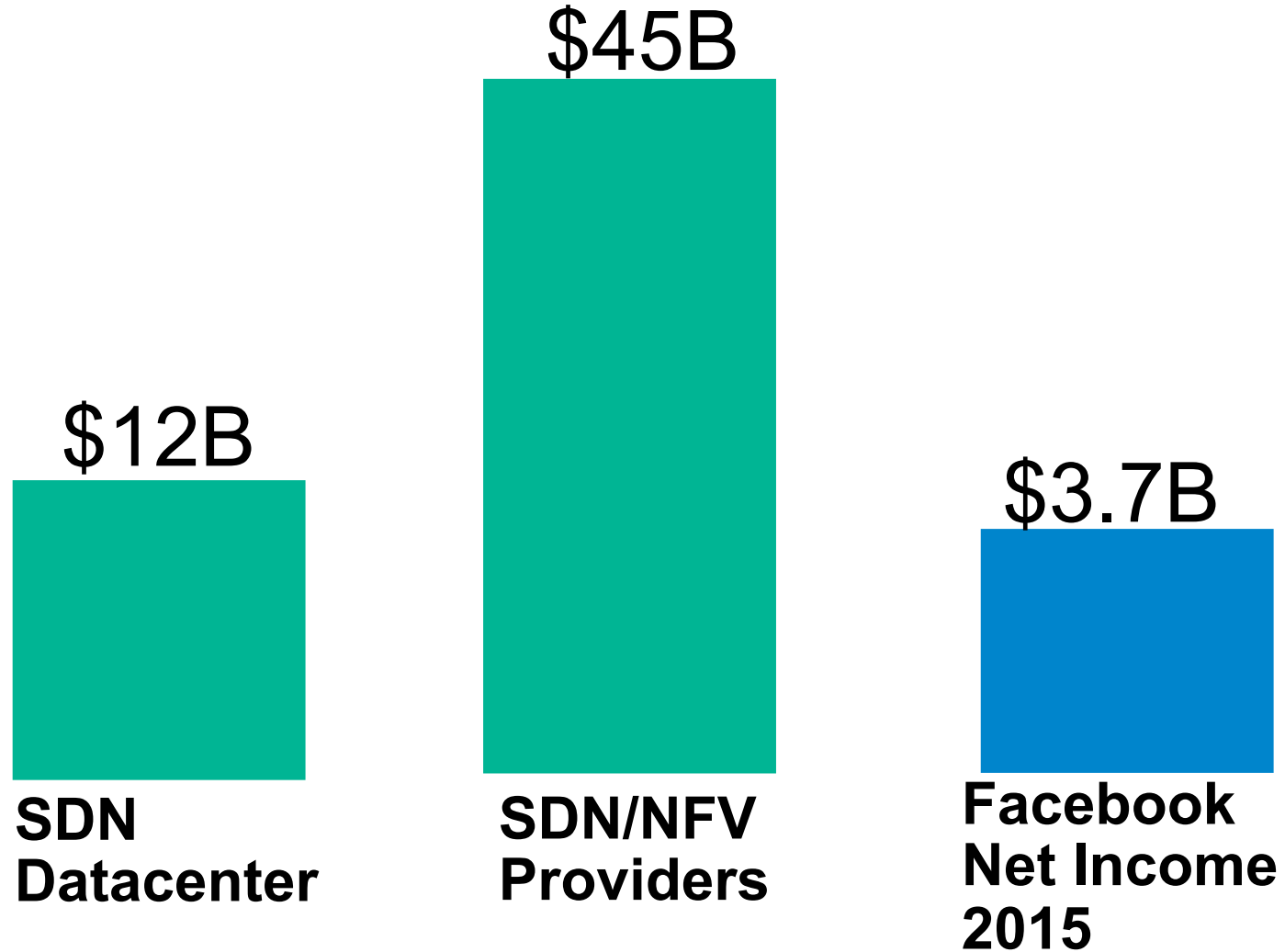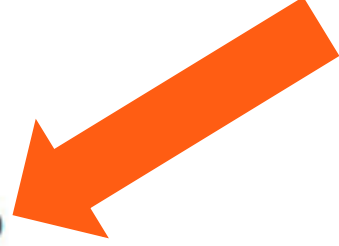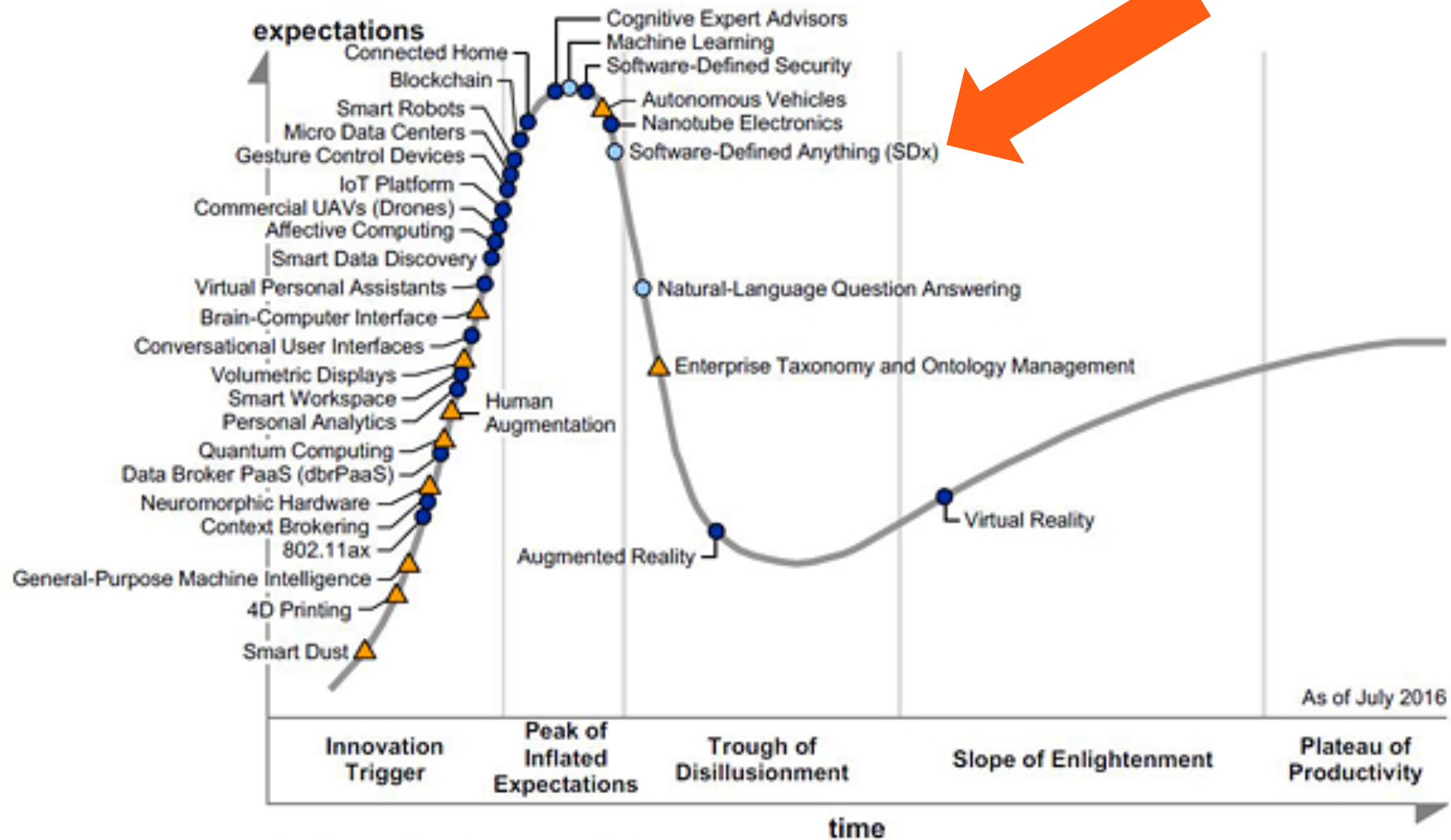slideshare.net/standel

May 2017

Sébastien Tandel

– Working within HPE Aruba CTO as a Principal Architect
- Technologist with sound business knowledge
- Software engineer with sound knowledge of hardware
- Product focused with sound experience in all innovation waves (research & advanced development)

– Lead me to drive many programs from Software-Defined Infrastructure & Intelligent Edge to Security Analytics

– Contributions in several aspects of SDN / NFV since 2010
- First Software-Defined Lync demo @ ONS'13
- First Software-Defined Security demo (IPS coupled to security analytics) @ ONS'14
- First HW accelerated SFC (MAC Chaining) including legacy physical SFCs demo @ Sigcomm'16
- Distributed Software-Defined Load Balancer, IoT Universal Profiler (identification & anomaly behavior detection)

views and opinions expressed are my own and does not necessarily reflect views or opinions of my employer

Hewlett Packard
Enterprise

SDN & NFV Markets by 2020

$12B — SDN Datacenter
$45B — SDN/NFV Providers
$3.7B — Facebook Net Income 2015

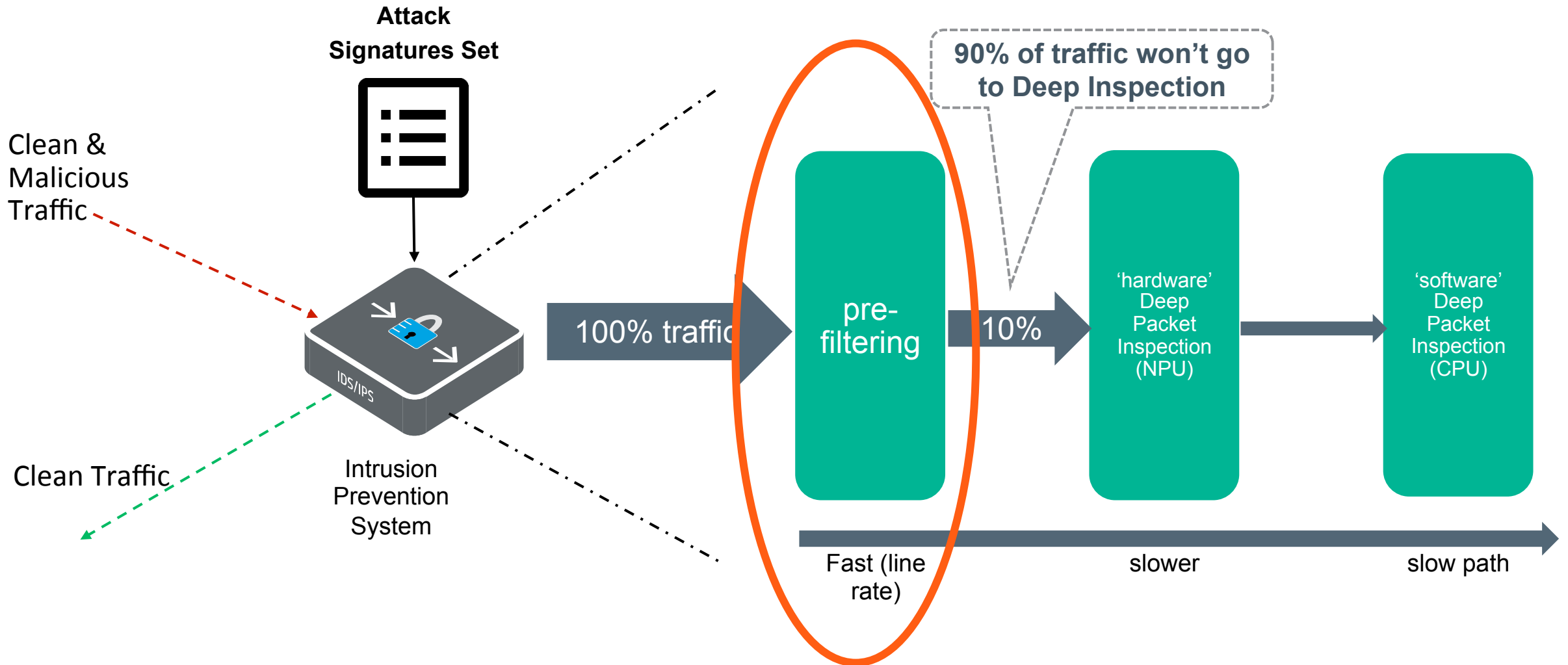Hewlett Packard Enterprise

Gartner Hype Cycle => Customer Focused and Realist !

Research … Where should I go?

I'll tell a story about security although you can apply it as model to other use cases

Hewlett Packard
Enterprise

Physical IPS appliance : 10,000 feet hardware architecture

Attack Signatures Set

Clean & Malicious Traffic

Clean Traffic

IDS/IPS

Intrusion Prevention System

100% traffic

pre-filtering

90% of traffic won't go to Deep Inspection

10%

'hardware' Deep Packet Inspection (NPU)

'software' Deep Packet Inspection (CPU)

Fast (line rate)

slower

slow path

a story of decomposition : pre-filtering as micro-VNF

Distribute pre-filtering function over all infrastructure

Switch
Performing Pre-Filtering

IPS only processes ~10% traffic (suspicious traffic)

20 Gb/s

~2 Gb/s

Less than 2 Gb/s

Clients

IPS

Regular traffic directly forwarded to destination 90% traffic

Clean ~18 Gb/s

Destination
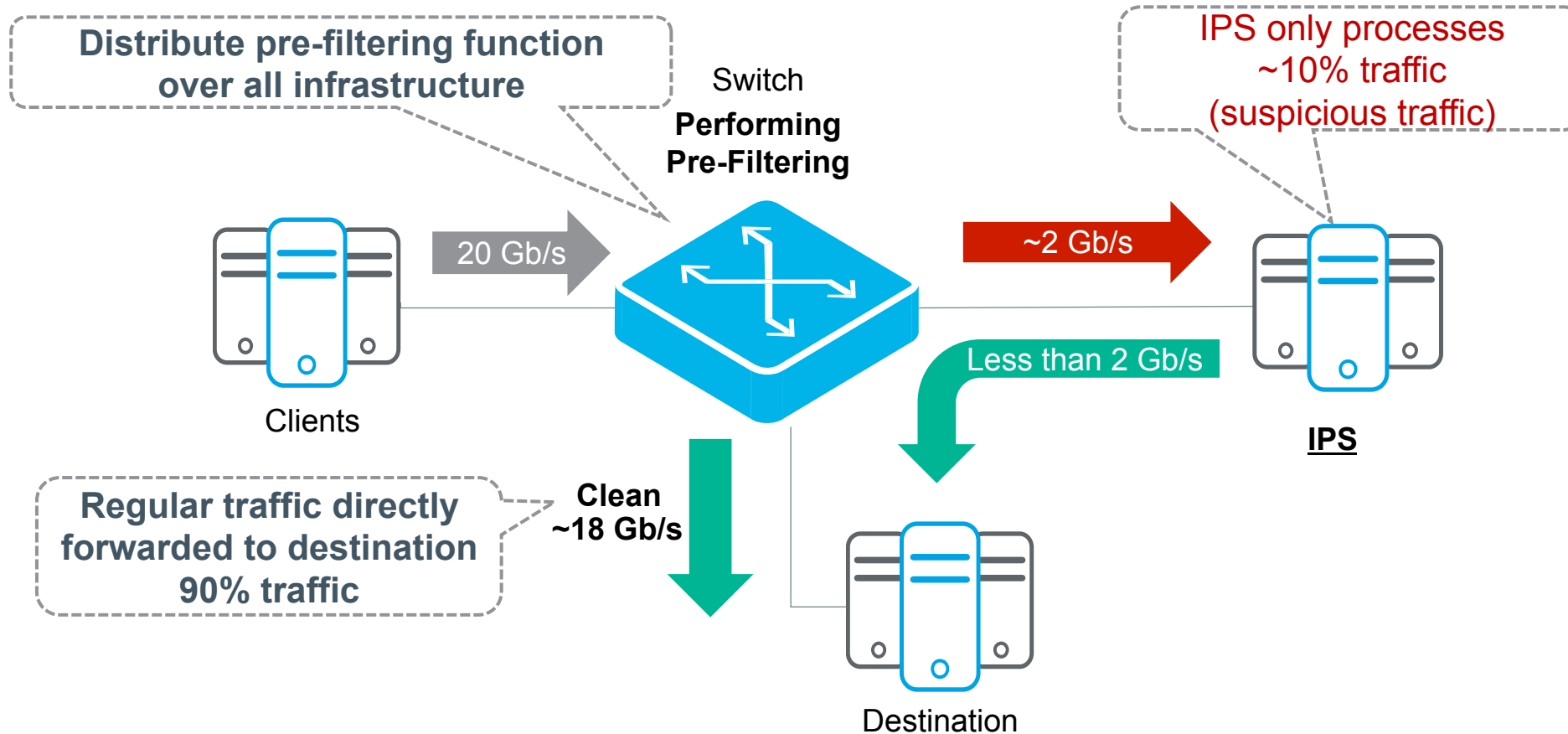
µVNF changes cost/performance

IPS	Max Inspection throughput (Gb/s)	Listing price (US$)	US$ per Gb/s of inspection
TPT S7500	20	500000	25000
Snort (4 proc)	2	10000	5000
pre-filtering µVNF + Snort	20	10000	500

✓ State-of-the-art Product Performance

✓ 50x cheaper than TippingPoint

Hewlett Packard
Enterprise

1. Research in physical µVNF

usual suspects: compression, encryption
➢ **take away : many other opportunities**

Software-Defined Security: IPSaaS model
Creating a Security Control plane

IPSaaS app on
SDN Controller

Attack
Signatures Set

Dynamic setup of
traffic redirection to IPS

SFC

Switch
with pre-filtering

Switch
with pre-filtering

IPS

Device 1

Device 2
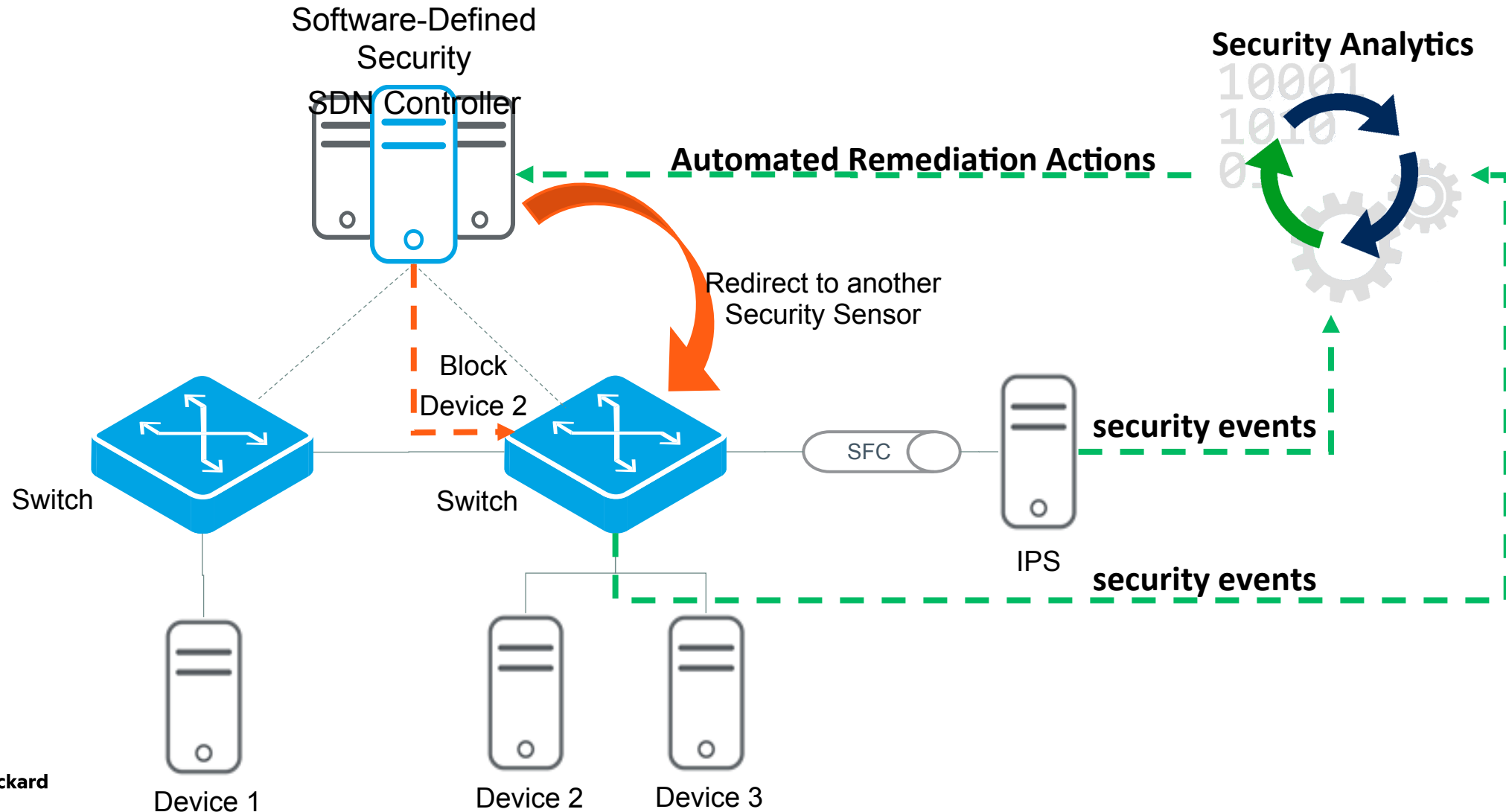
Device 3

Hewlett Packard
Enterprise
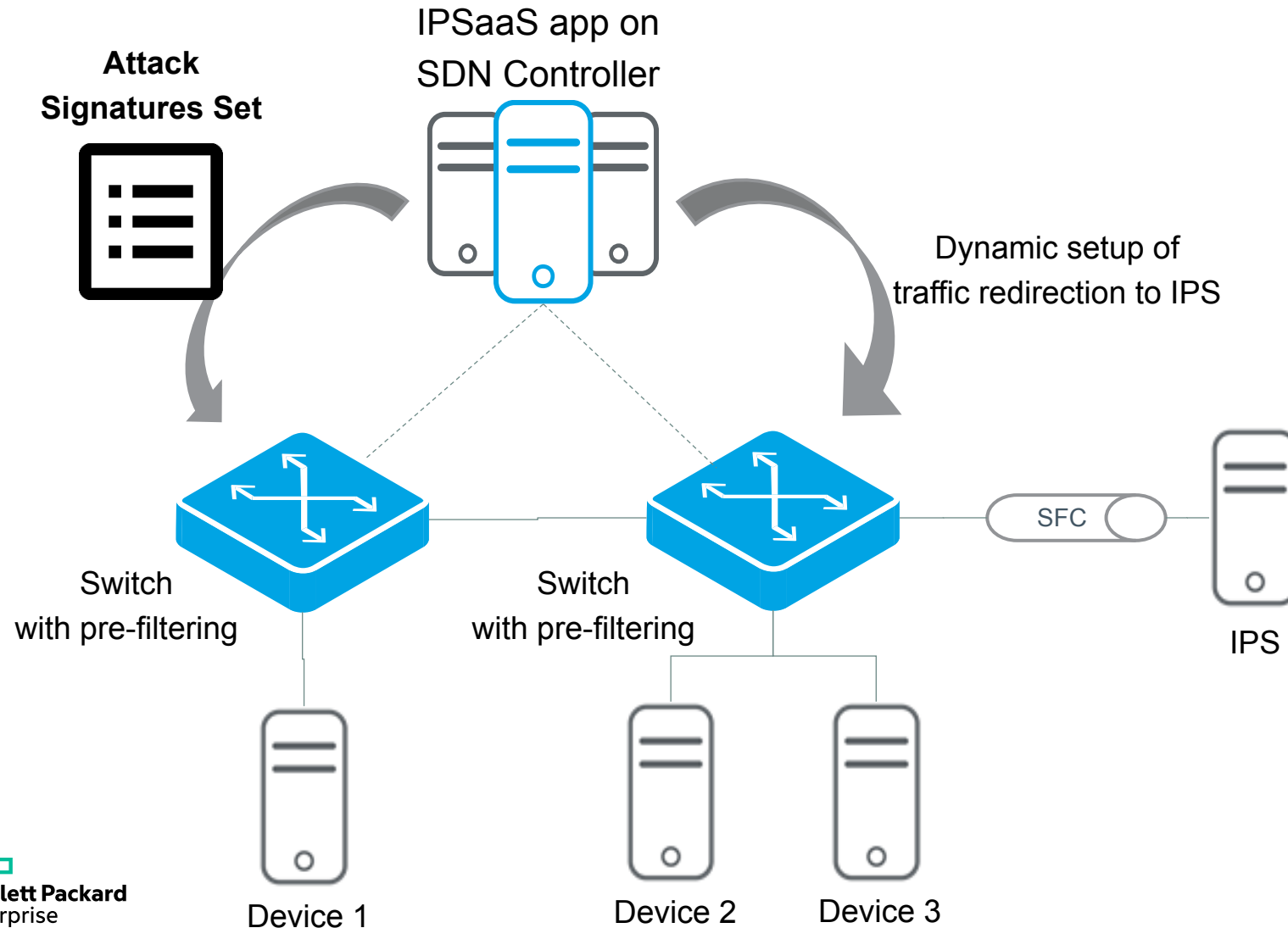
2. Software-Defined Security

**Opportunity for high-level security policies
BTW, Service Function Chain still challenge**

Software-Defined Security: Closing the loop
Making Sense of Security Events & Automate Remediation Actions

Software-Defined
Security
SDN Controller

Security Analytics

10001
1010
01

Automated Remediation Actions

Redirect to another
Security Sensor

Block
Device 2

Switch

Switch

SFC

IPS

security events

security events

Device 1

Device 2   Device 3

3. Big Data applied to Security

Big Data:
possible to analyze all packets ?
Where in the stack: Cloud, Edge?
Security Analytics:
how to make sense?

Summary

1. High Impact: Holistic Approach to Solve **Customer Headaches**

2. 3 research aspects for the next 2-5 years:
   – Physical μVNF ; Software-Defined Security ; Big Data applied to Security
   – It's a model working for other use cases

3. From idea to market? An top-down approach
   ➢ Cloud-first (SaaS) for fast TTM
      ➢ Edge Computing model
         ➢ μVNF for better scale and cost performance
   – Open APIs to avoid vendor lock-in & fragmentation

Hewlett Packard
Enterprise

14

Thank You

sta@hpe.com
www.slideshare.net/standel

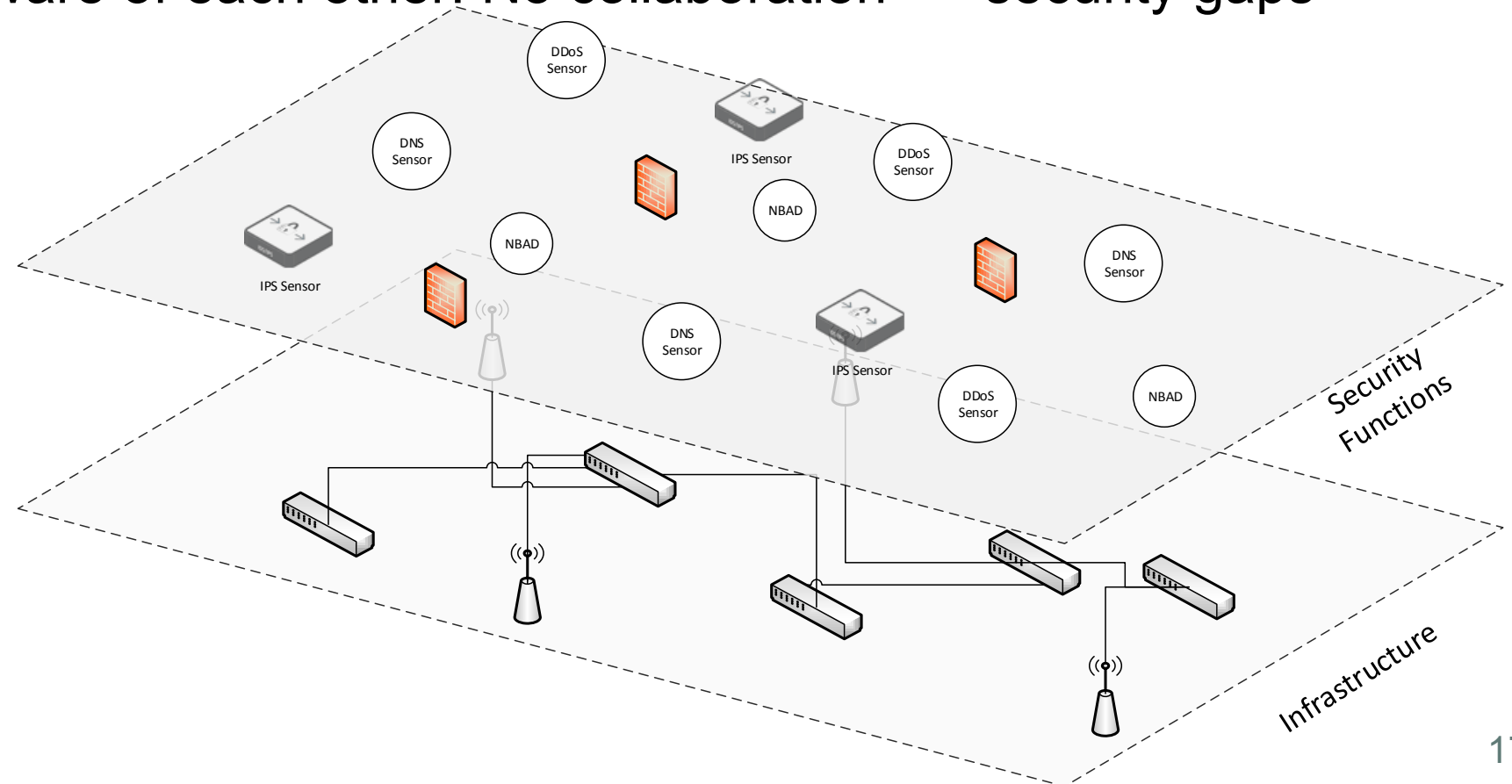**Hewlett Packard**
Enterprise

Backup

Hewlett Packard
Enterprise

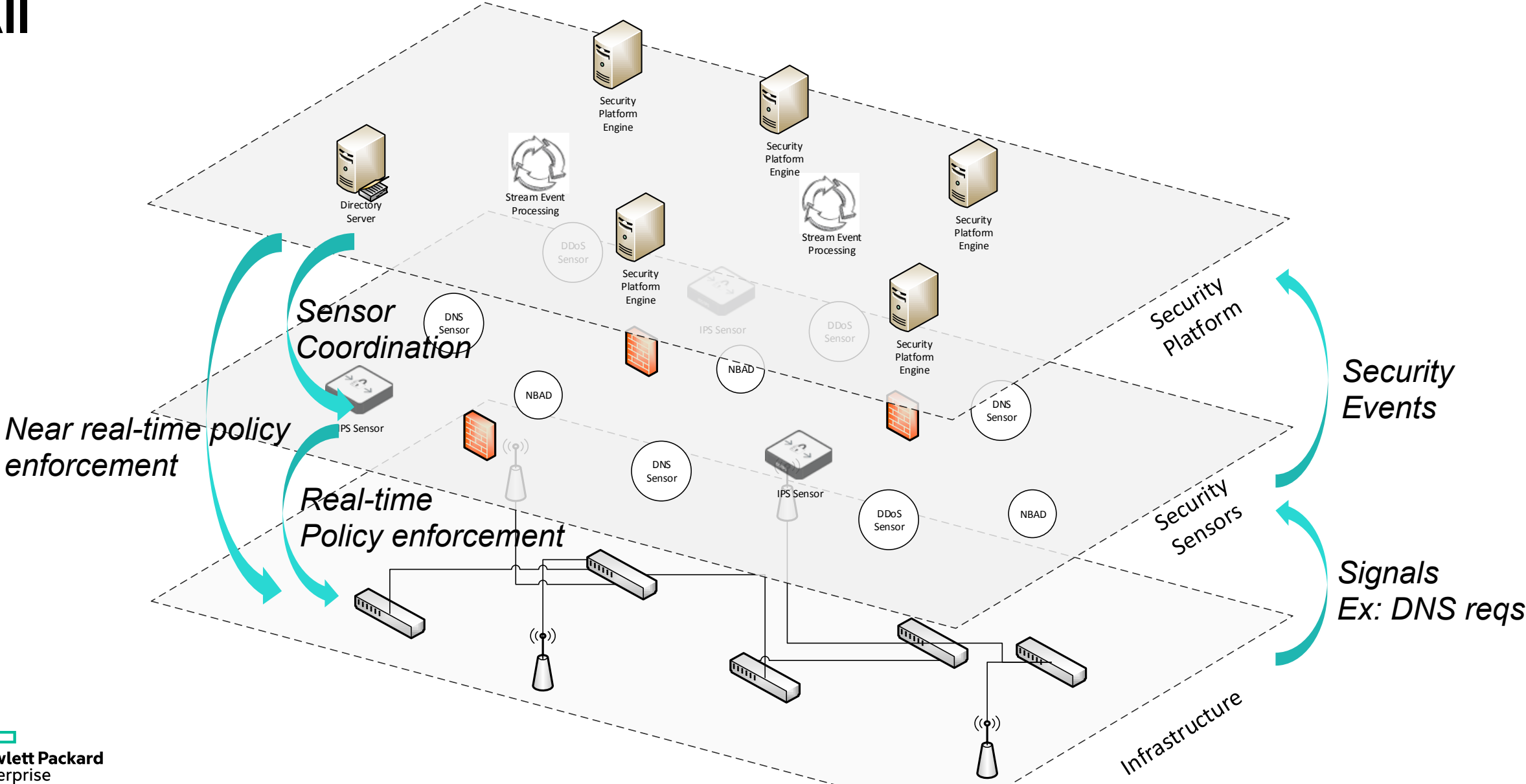# Current Infrastructure Security Architecture

Security boxes at fixed place, manually connected
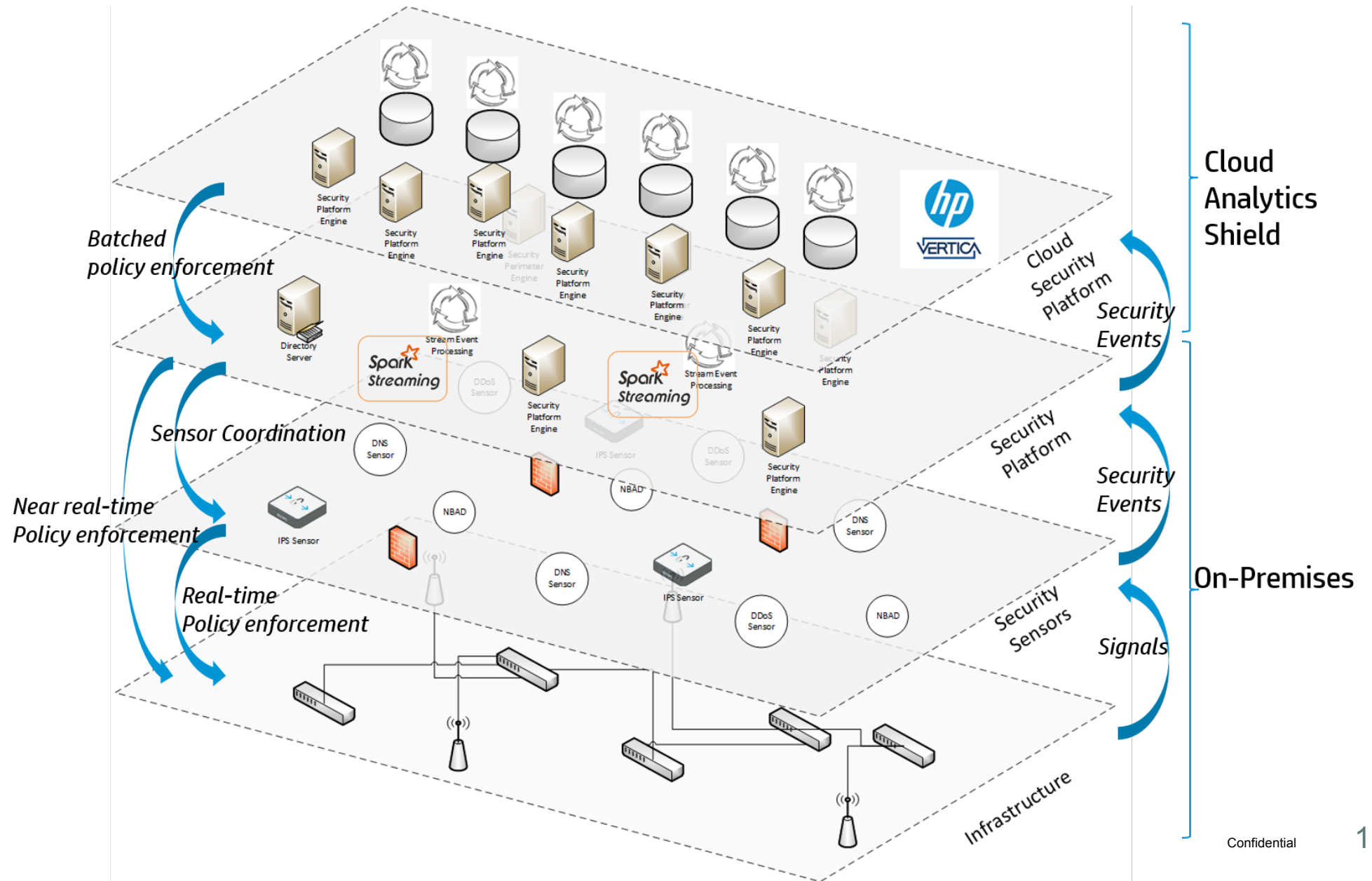
Edge / East-West weakly protected => BYOD, IoT

Security boxes unaware of each other: No collaboration => security gaps

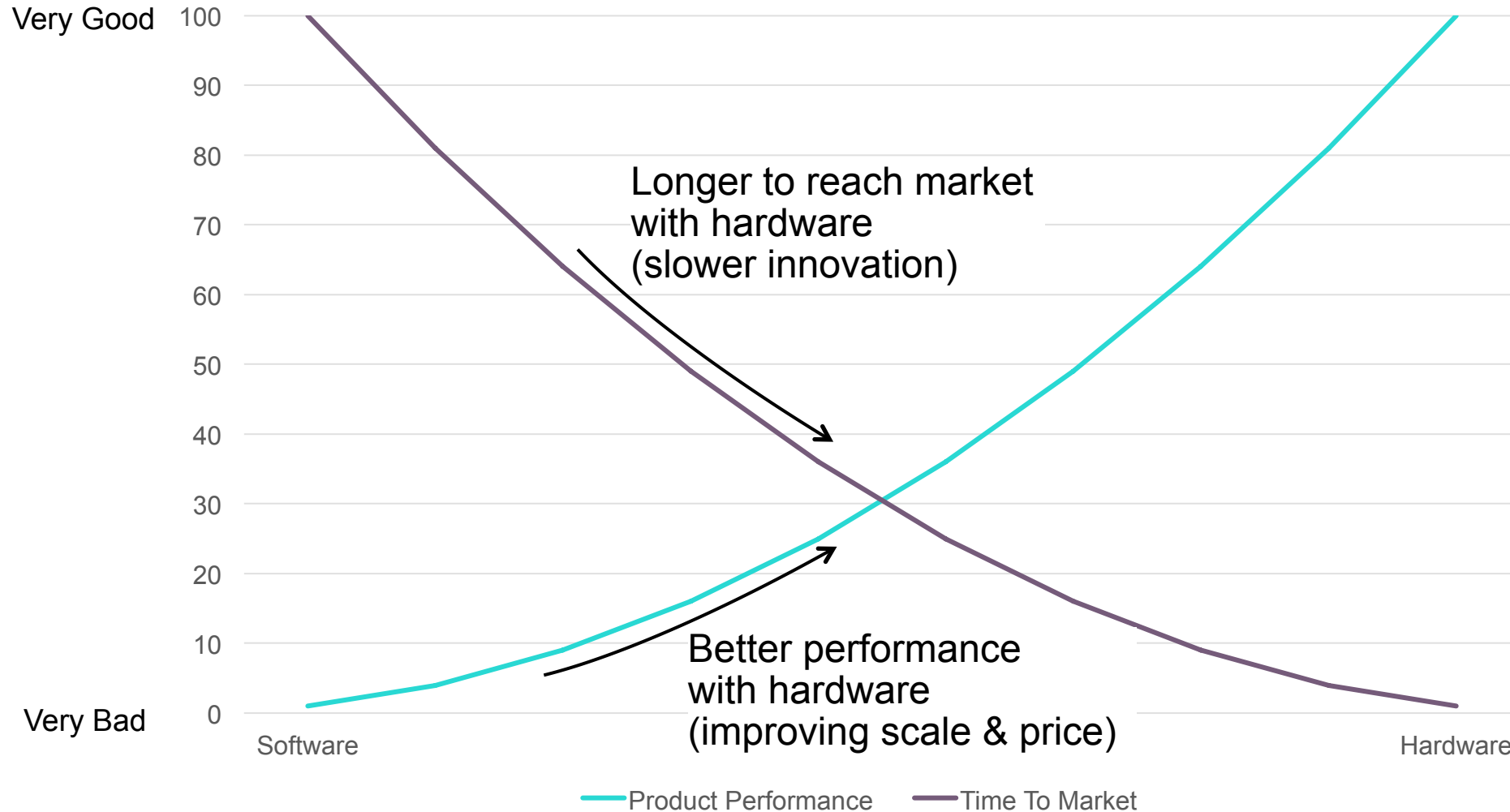# Software-Defined Security: a Security Control Plane to Rule them All

Software-Defined Security & Intelligent Edge

Key Take Aways

Product: Performance x Time-To-Market

Longer to reach market with hardware (slower innovation)

Better performance with hardware (improving scale & price)

Product Performance — Time To Market

Key Take Aways

Product: Performance x Time-To-Market

software is excellent starting point to test the market

How do you evolve?
What may remain software?
Open interfaces?

Product Performance   Time To Market

Software   Hardware

Very Good   100 90 80 70 60 50 40 30 20 10 0   Very Bad

Hewlett Packard
Enterprise

21