IFIP/IEEE INTERNATIONAL SYMPOSIUM ON INTEGRATED NETWORK MANAGEMENT

IM™2015 OTTAWA, CANADA • MAY 11-15 2015

Nakina Systems

Security Challenges in the eye of the Hurricane: Navigating the perfect networking storm of Virtualization, Mobility and the Internet of Things

Chris Ullock
Product Line Management

May 15, 2015

Abstract

- The business challenges faced by communication service providers are well known. Specifically, revenues remain threatened by increasing competition from more agile competitors. As a result, service providers are turning to new technologies, such as Network Function Virtualization (NFV), to enable both new service innovations and to reduce costs. In order to realize the full commercial benefits, identifying and overcoming some of the practical and critical operational considerations will be required. Security is one of the most critical considerations, which must not be an afterthought. Identity Access Management strategies must accommodate a variety of network equipment, multiple generations of technologies and scale to support hundreds of thousands of equipment types, including virtual infrastructure, virtual network functions, servers and systems.

Agenda

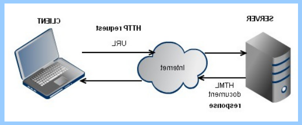
- Part 1 – Why Virtualization now
- Part 2 – Industry and Security trends
- Part 3 – Security challenges of Virtualization

Greatly Simplified Schematic of Compute and Network Evolution

COMPUTE

Special purpose

Mainframe



Client Server / Web

Virtual

Telegraph

Telephone

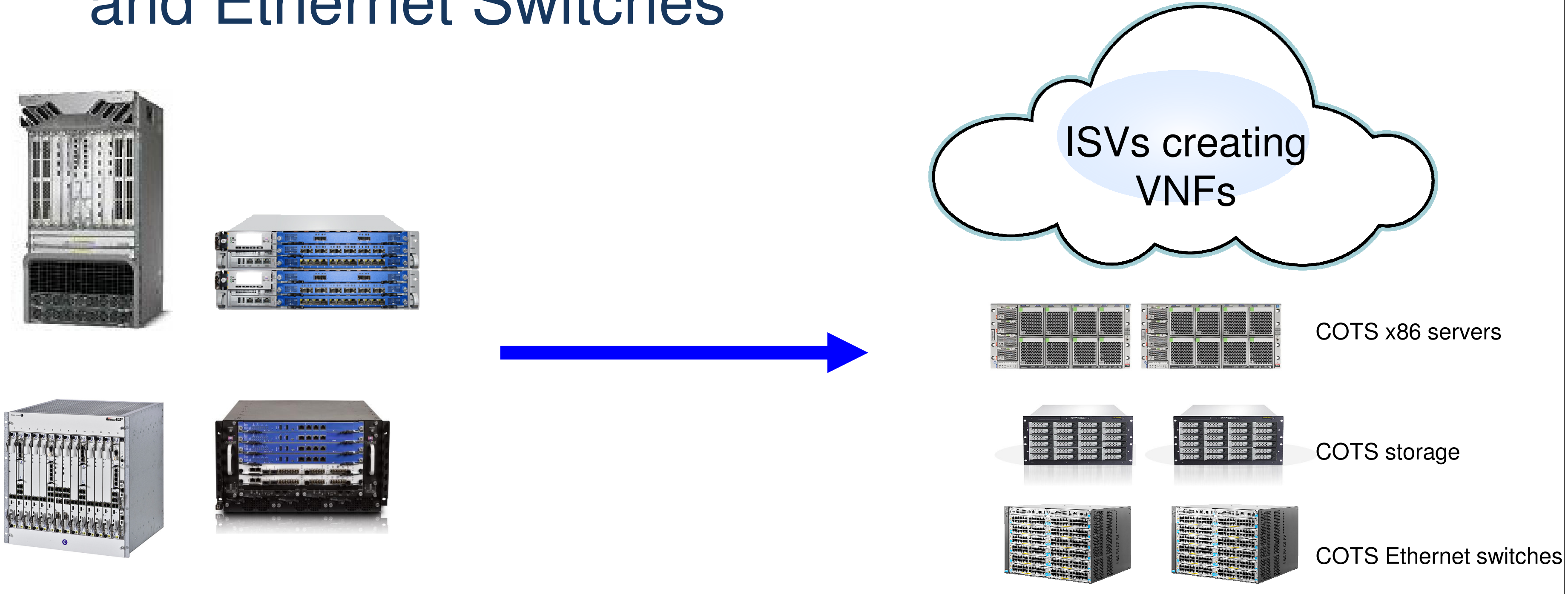
Data on Big Iron

Virtual

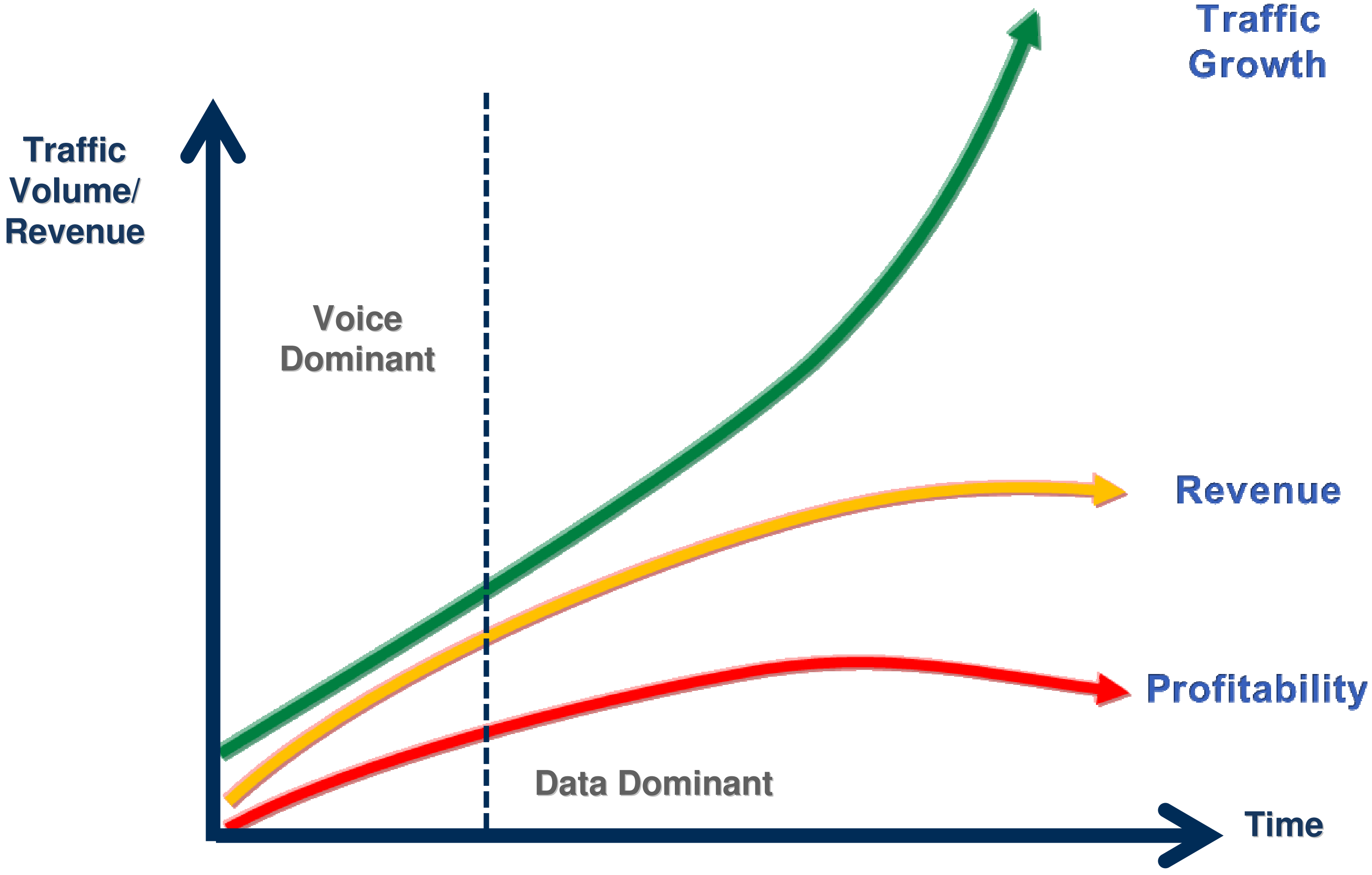
NETWORK

What is Network Functions Virtualization?

- Moving from the appliance based networking model of today and virtualizing the network to run on standard low cost COTS servers, storage and Ethernet Switches



Why Virtualization Now?
1. Service Provider Dystopia

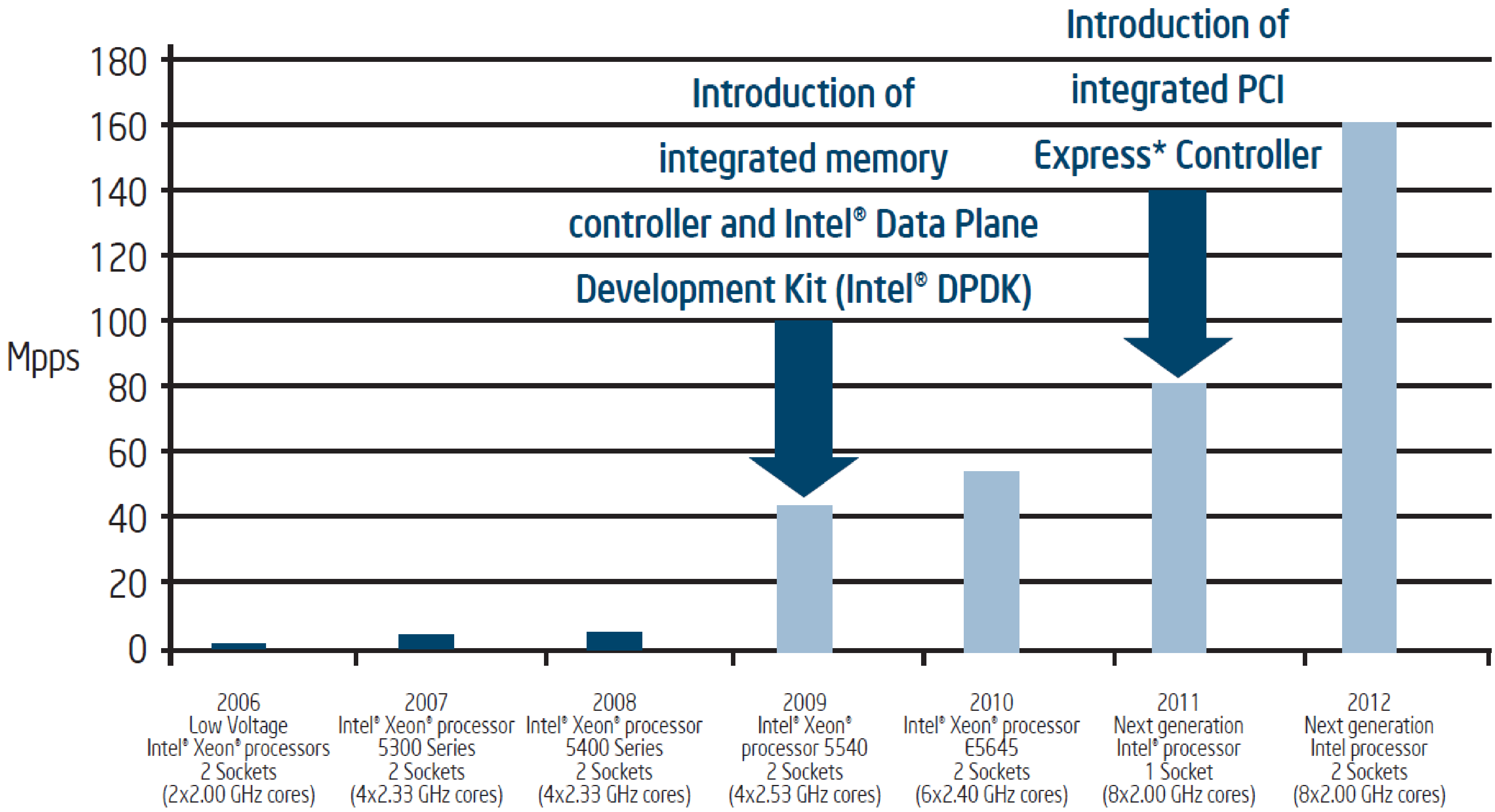


Bandwidth explosion + flat or declining revenue = Need for Transformation

Why Virtualization Now?
2. “Silicon and Software” Advancements

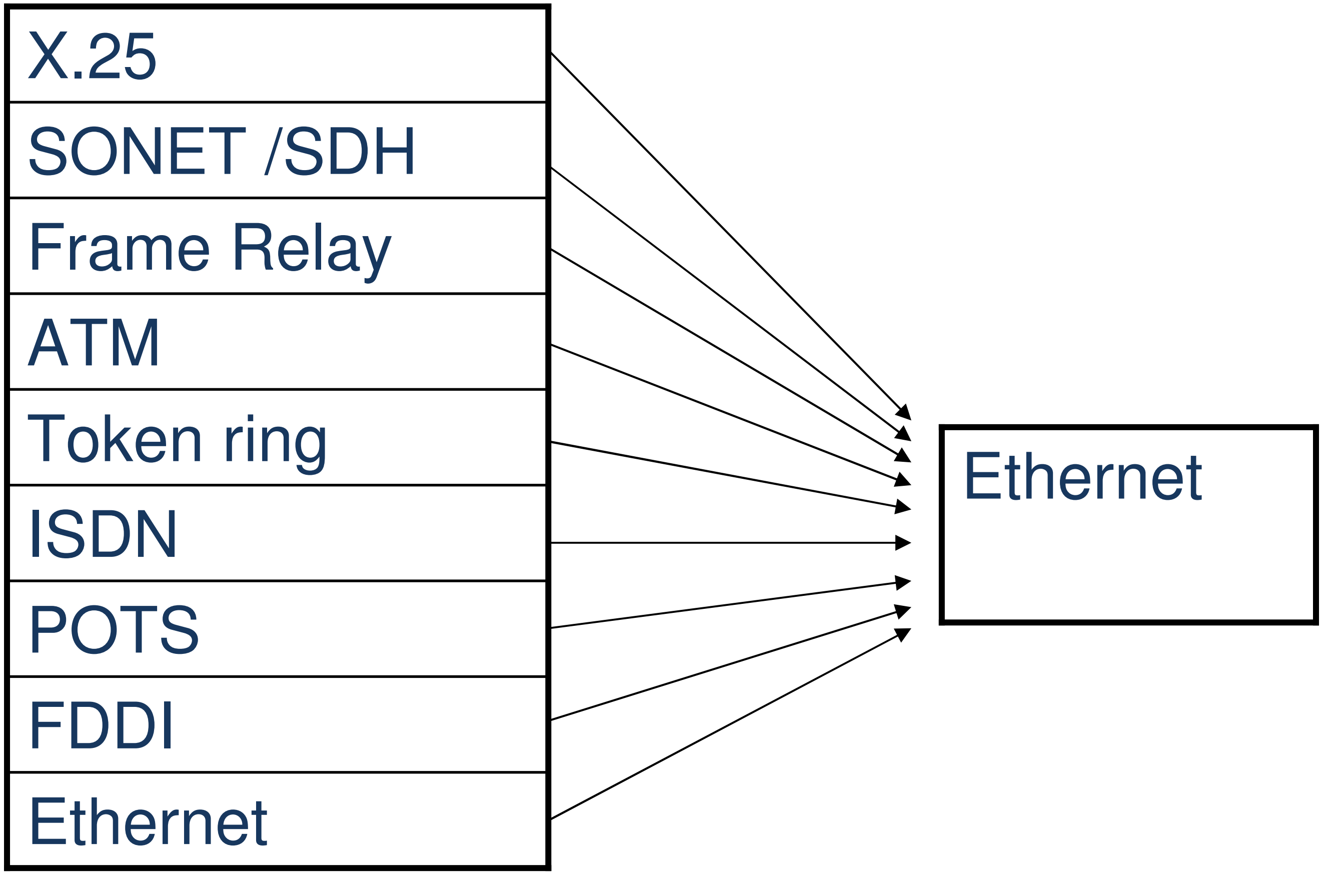
Nakina Systems

Source: Intel



IPv4 Layer 3 Forwarding Performance for Various Generations of Intel Architecture Processor-based Platforms

Why virtualization now?
3. IP/Ethernet Everywhere



Why Virtualization Now?
3. Data Centre Example

Nakina Systems

Operational Efficiency

1 : 20,000 servers
Each admin can managed ~20K servers

CSP: <1 : 100
Significant operations cost across all parts of the network

Service Deployment Time

Every 11 seconds
Up to 30K servers simultaneously

CSP: Months
Long service introduction times, limited automation

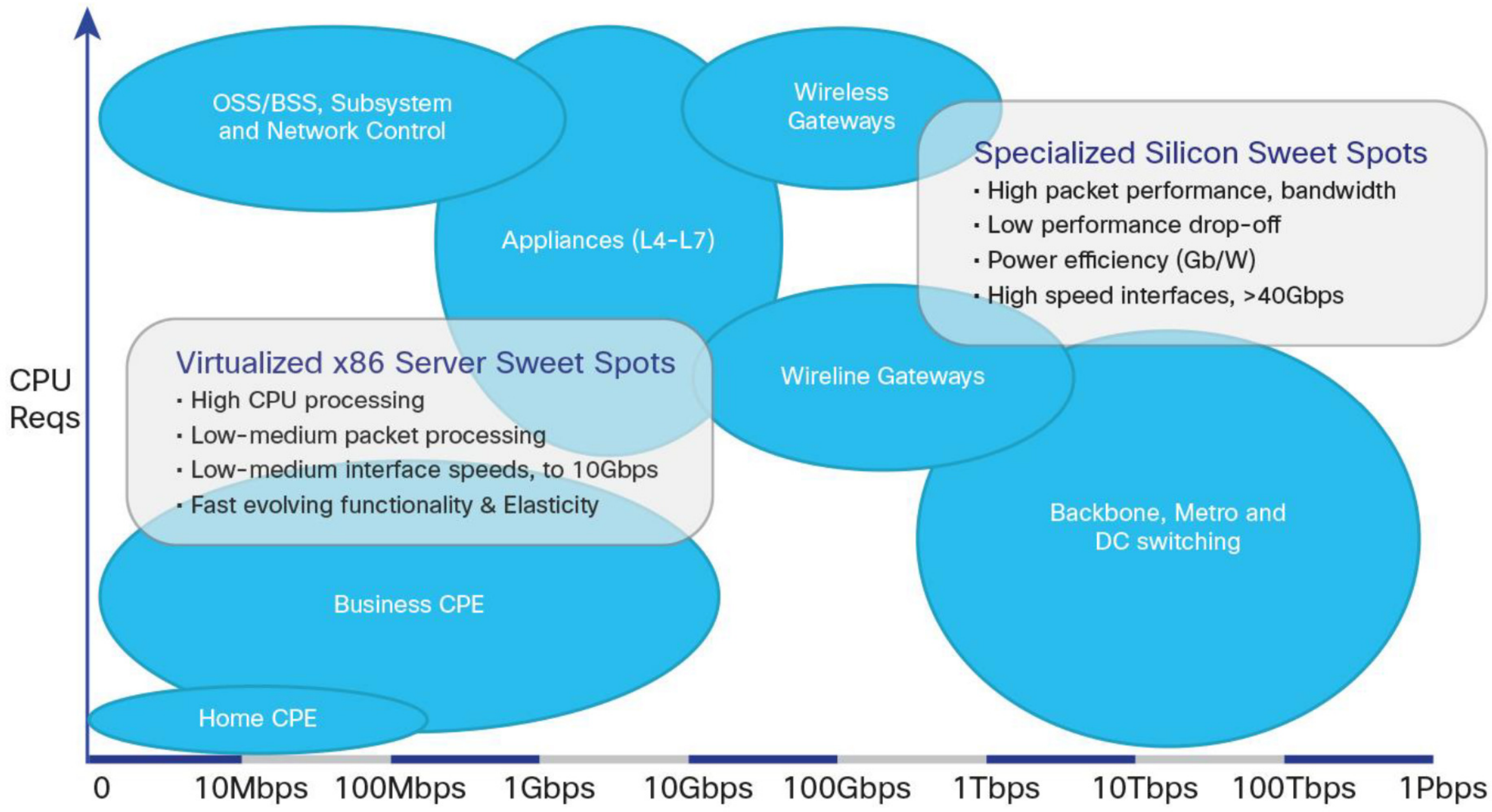
Operational Complexity

10s of Configs

CSP: 1000s of Configurations
Thousands of configurations, SKUs, and service options to manage

CSP Dilemma: High Opex, Low Utilization, High Complexity, Slow Time to Market for New Services

Where to deploy NFV



Specialized Silicon Sweet Spots

- High packet performance, bandwidth
- Low performance drop-off
- Power efficiency (Gb/W)
- High speed interfaces, >40Gbps

Virtualized x86 Server Sweet Spots

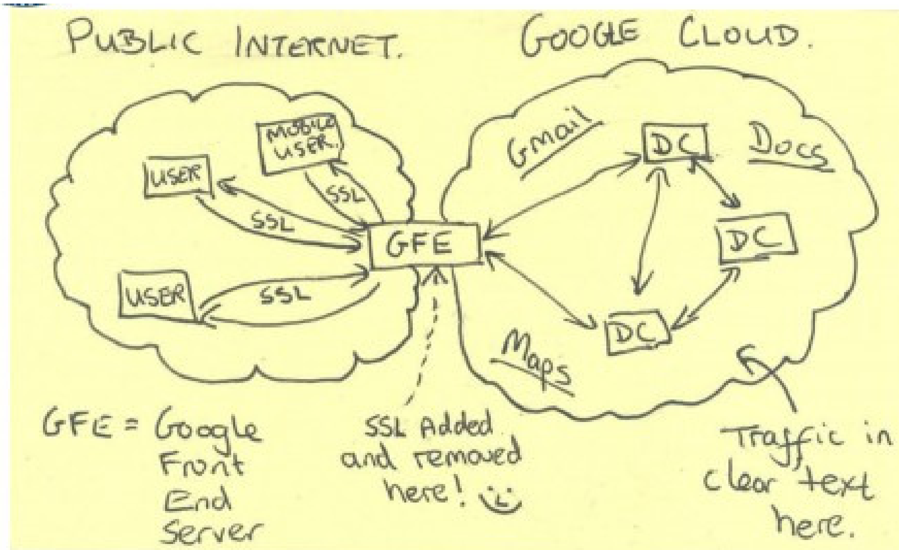
- High CPU processing
- Low-medium packet processing
- Low-medium interface speeds, to 10Gbps
- Fast evolving functionality & Elasticity

Source: Cisco

Industry and Security Trends

1. Fate of the Perimeter model of security
2. Rise of the Machines
3. SSO and Access Management
4. Math and big Data

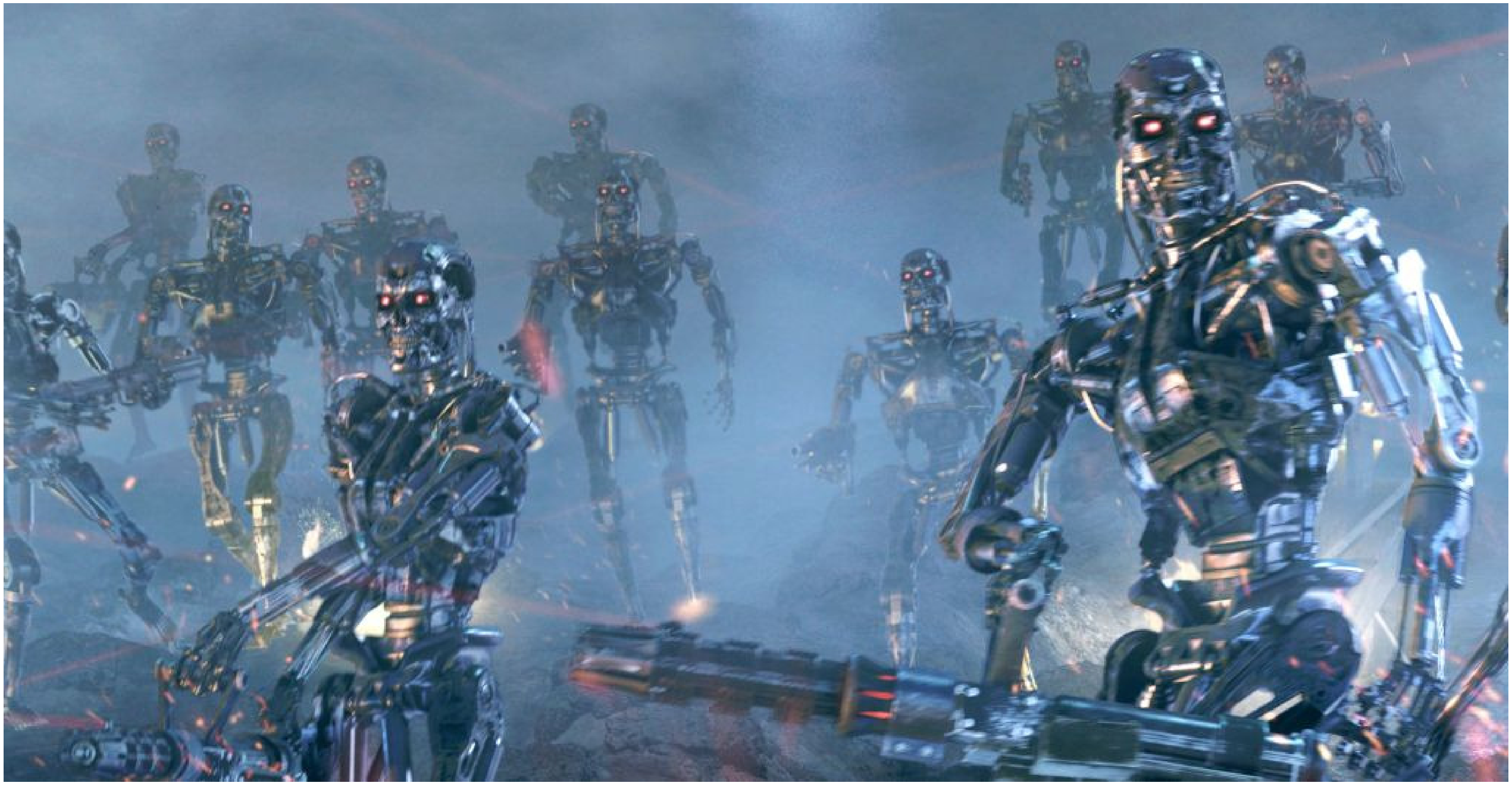
1. Fate of the Perimeter Security Model


PUBLIC INTERNET.
GOOGLE CLOUD.
MOBILE USER.
USER
SSL
SSL
GFE
USER
SSL
Gmail
DC
Docs
DC
DC
Maps
GFE = Google Front End Server
SSL Added and removed here! ☺
Traffic in clear text here.

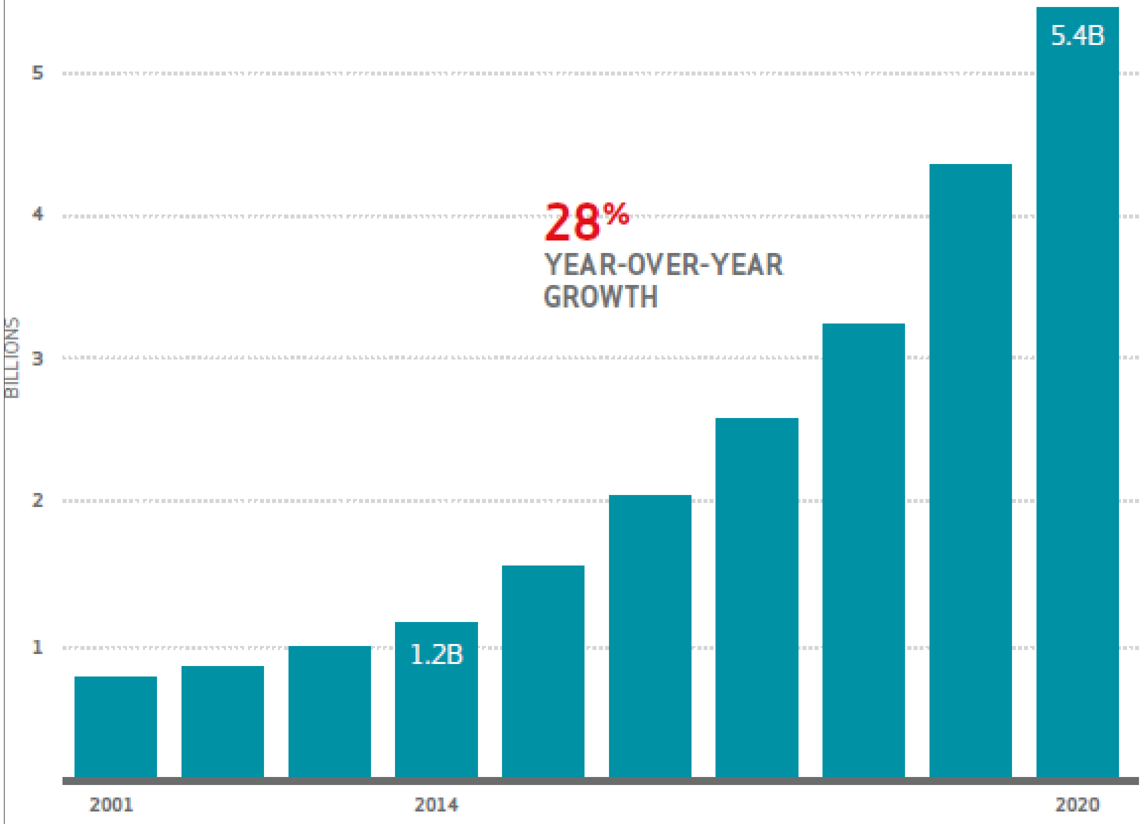
Lessons from the history of Warfare: The story of the Castle

- Zero trust model needed
- AT&T Astra’s “rings around things”

2. Rise of the Machines



Growth in connected things



Source: Verizon 2015 Data Breach Investigations Report (DBIR)

O~~$~~S

3. Data breaches and insider threat - > SSO and Access Management

Nakina Systems

SONY

TARGET

THE HOME DEPOT

belgacom

2011

2014

Sony playstation hack - $170 million

Bitcoin hack - $460 million

Linked in - $6 million user records stolen

Target hack

- $150 million by target
- $200 million from banks

Belgacom GCHQ - $15 million +

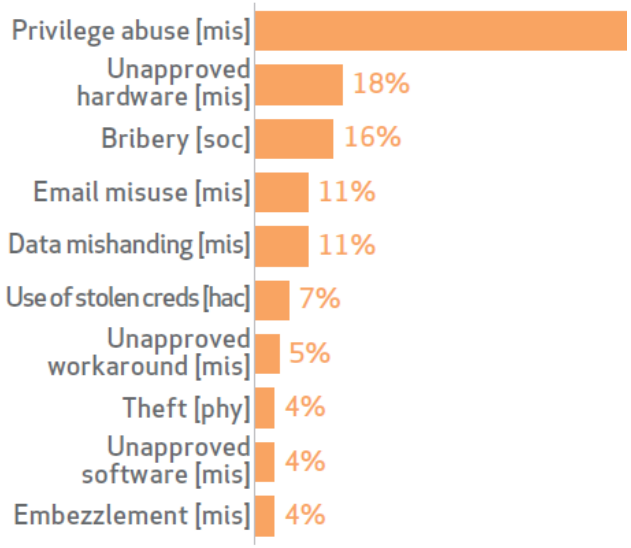
Sony hack - $15 million +

Home Depot hack - $60 million

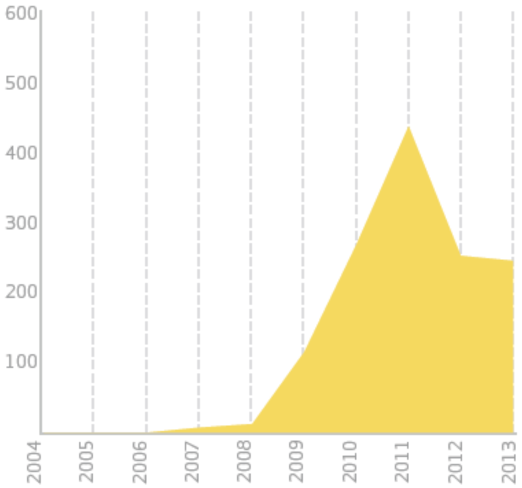
Ebay – 145 million user records stolen

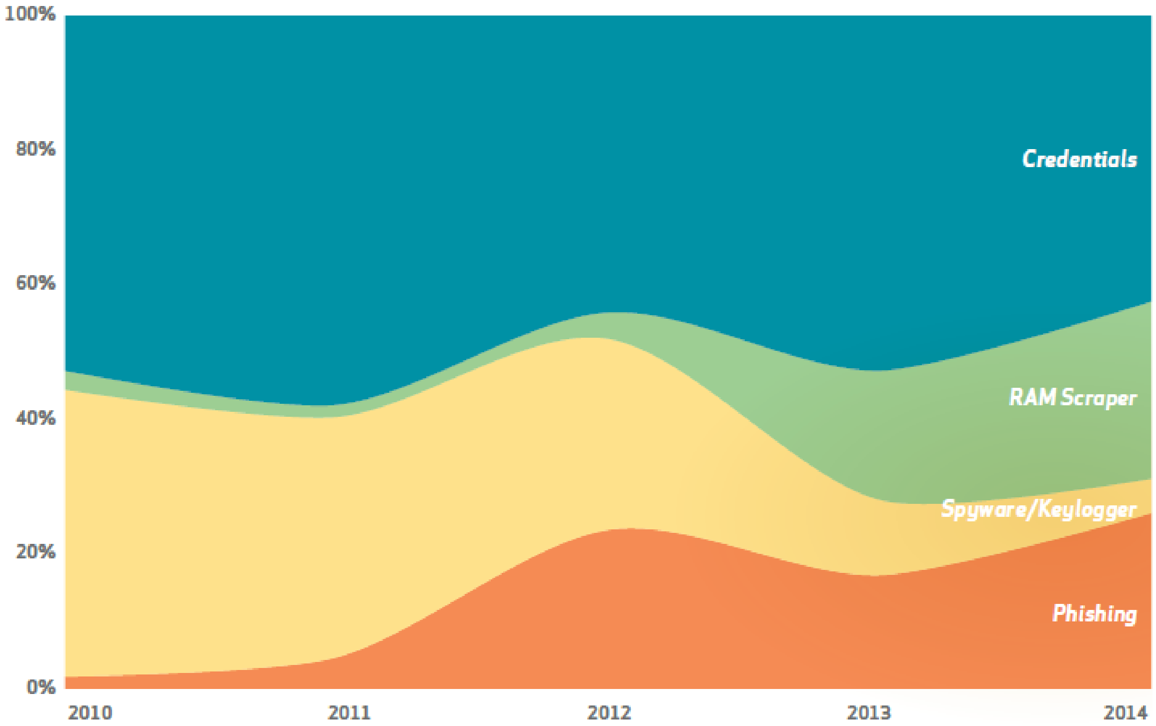
Verizon Data Breach Investigations Report

Top 10 threat action varieties within Insider Misuse (



Credentials

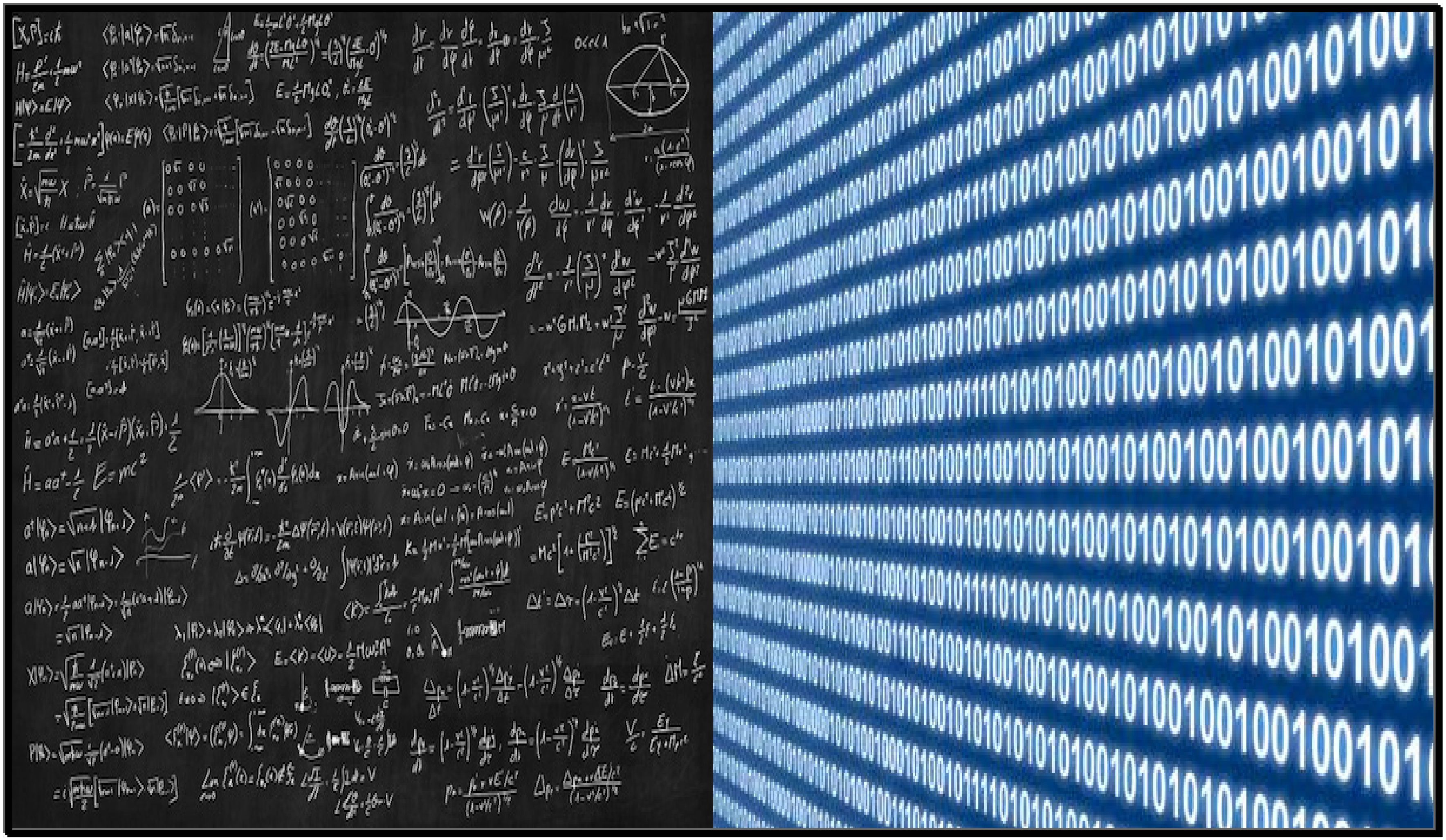




5. SSO & Access Management

- Drivers
  - Regulation (e.g. PCI DSS, Indian DoT)
  - Vendor Access
  - Legacy devices
  - Insider threat
  - PAM (Privileged Access Management)
  - Audits and Analytics
- How does it work?
  - Separating user credentials and network credentials
  - Proxy between users and network
  - Capture sessions in CLI and Video logs
  - Credential and password management/rotation

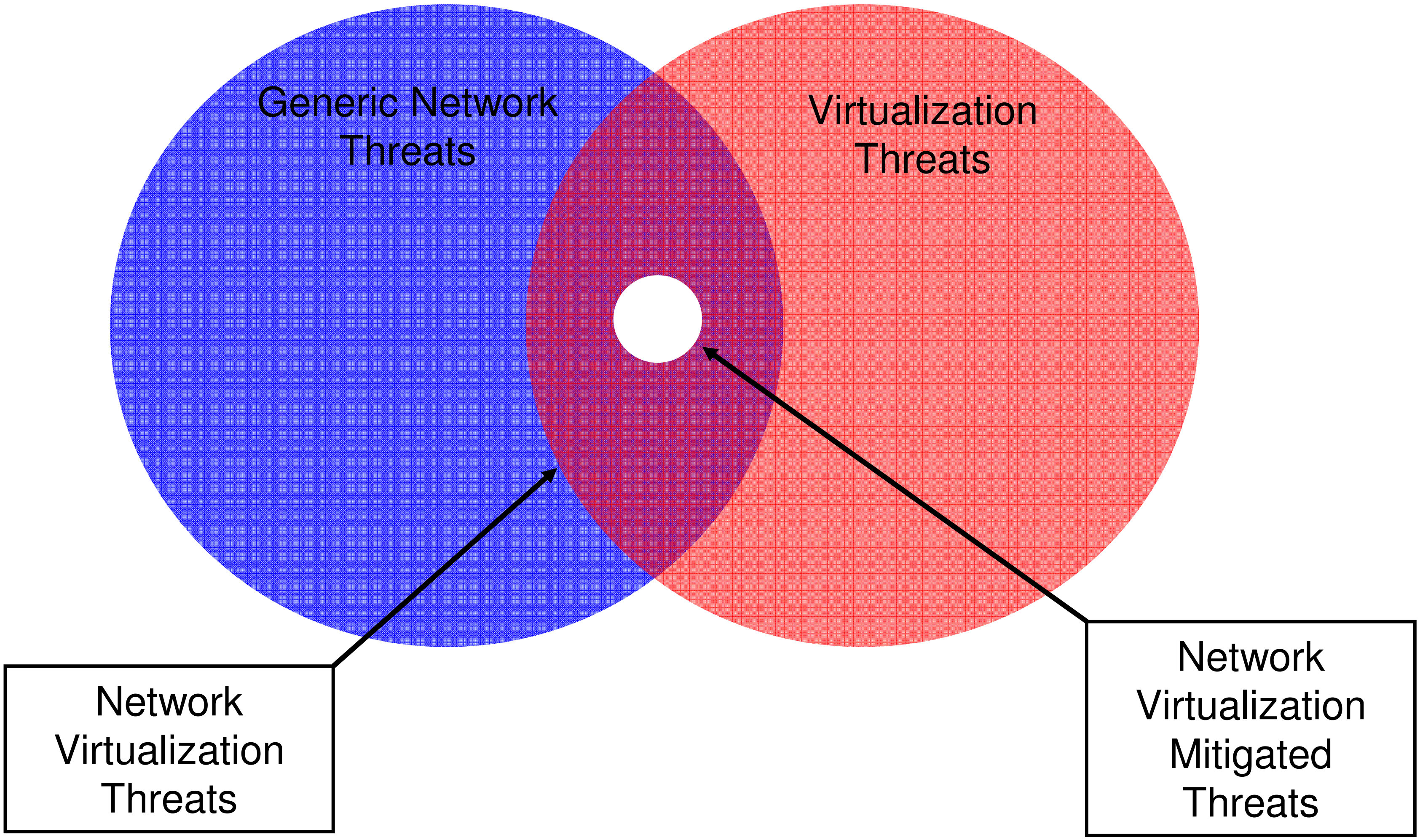
4. Math and big Data



Bringing big data to security

- Some random companies
  - Cylance – Anti-virus
  - Interset – threat detection with behavioral analytics
  - Bitsight – company Security rating indexes
  - ThreatConnect – threat intelligence
- Identity and Access Management Example
  - Profile of a typical telecommunications service provider
    - 100,000s of network elements
    - 1,000s of users
    - 100,000,000 CLI sessions captured annually → 50 TB data
    - 10,000,000 video log hours captured annually → 800 TB data
    - Approx 1 PB data year
  - Session analytics
    - Detecting anomalous behavior
      - Multiple factors
    - Overlaying session behavior with network change

Network Virtualization Threat Diagram


Generic Network Threats
Virtualization Threats
Network Virtualization Threats
Network Virtualization Mitigated Threats

Security Pitfalls with Network Virtualization

- Additional software attack surfaces
- Immature software
- Resource sharing & Multi-tenant
- Industry regulation

Securing NFV: Many Layers and Dimensions to Consider

Nakina Systems

Virtual Network Functions require secure access.

VNFs could belong to different end customers, users.

Unique policies and access management needs.

Virtual Network Infrastructure supports all services: maintaining integrity is vital.

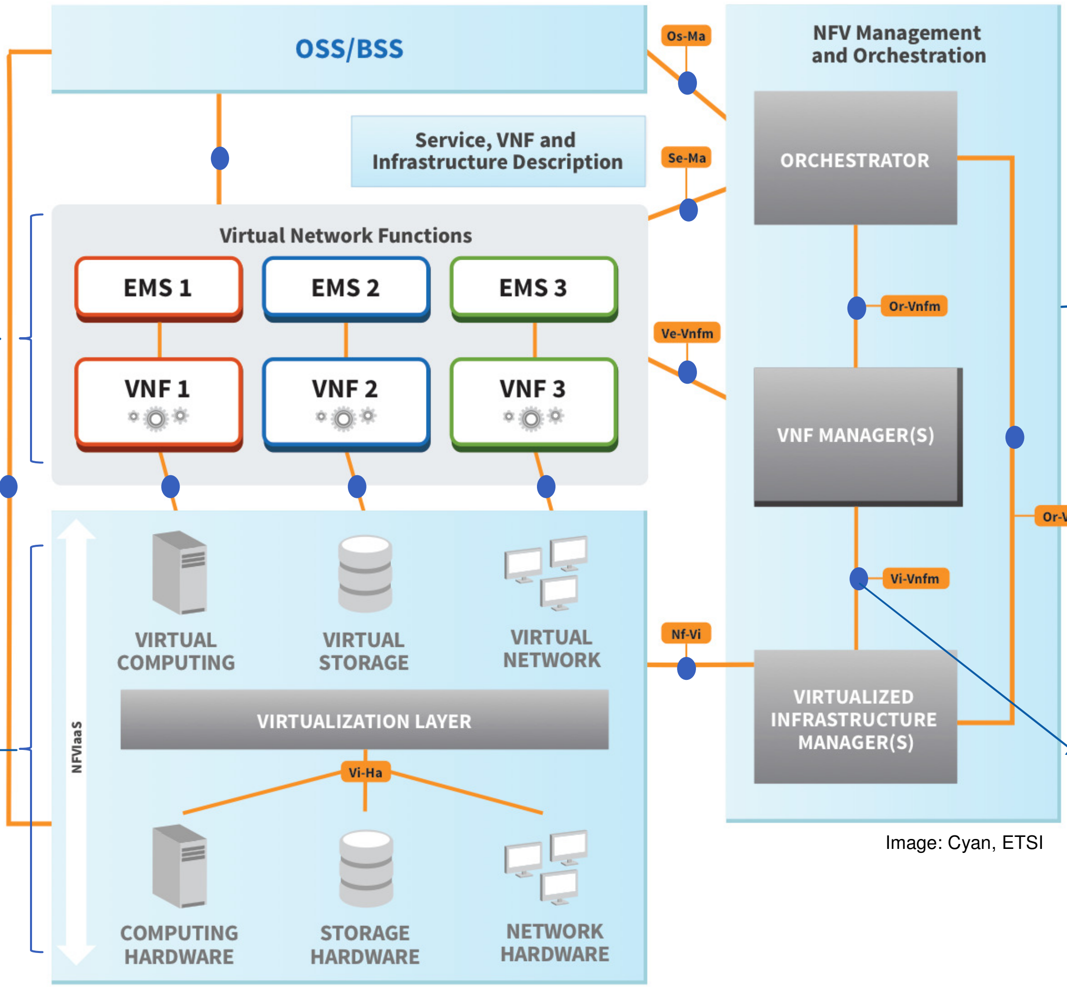


Image: Cyan, ETSI

Multiple Management and Orchestration sub-domains.

Multiple orchestrators and VNF Managers possible.

Which systems can communicate to physical and virtual resources? To each other?

Multiple management interfaces to secure.

Interplay, policies, etc.

Pitfalls continued….

- The promise
  - “A single, common server architecture can be used to build in the redundancy and availability organizations require within their data center environment. No longer do organizations need to purchase and maintain expensive equipment to keep as spares; in the event of a failure, the shared virtualized infrastructure can simply move workloads to ensure ongoing capacity and performance.” SDX Central

- The dangers
  - New attack surfaces
    - Hypervisor compared to “big iron”
  - Inexpensive commodity hardware
    - Can be acquired by anyone, anywhere at low cost
  - Handful vendors
    - Processors, network cards, etc.
  - Magnification of vulnerability
    - Compromise of hypervisor → compromise multiple VNFs
    - Single vulnerability → compromise different types of VNFs
    - Heartbleed, shellshock as hint of what’s to come?

Mitigating the pitfalls - Part 1

- Redefining the Perimeter
  - “rings around things”
- On-demand policy change
  - Firewall rule
- Security Zones
  - VNF placement
- Traffic Isolation
  - e.g. management VLANs
- Encrypt Everything
- Centralized control
  - Visibility into patch

Mitigating the pitfalls – Part 2

- Software Integrity Protection
  - Software signing
  - Secure boot
  - runtime
- Access & Credential management
  - SSO and centralized control of credentials
  - Log machine-to-machine session traffic
- Analytics & Alarming
  - Critical for finding needle in the haystack
  - Real-time counter measures
  - Closed loop
- Protect MANO infrastructure
  - Secure APIs
- Multi-tenant capable security infrastructure
  - Instance based security model

Open debates – example of Hypervisor Introspection versus VM based security

- Hypervisor Introspection
  - Allow hypervisor visibility into hosted VMs (easier to detect root kits)
  - Shared security at hypervisor level
  - Infected VM/VNF cannot hide from hypervisor, but if hypervisor is compromised…
  - More attack surface in the hypervisor
- VM based security
  - Each individual VM and VNF is responsible for its own security
  - Higher resource consumption
- Factors
  - Different business models, tenant-landlord relationships

Cautionary note

Walk before we run

So we avoid this

Nakina
Systems