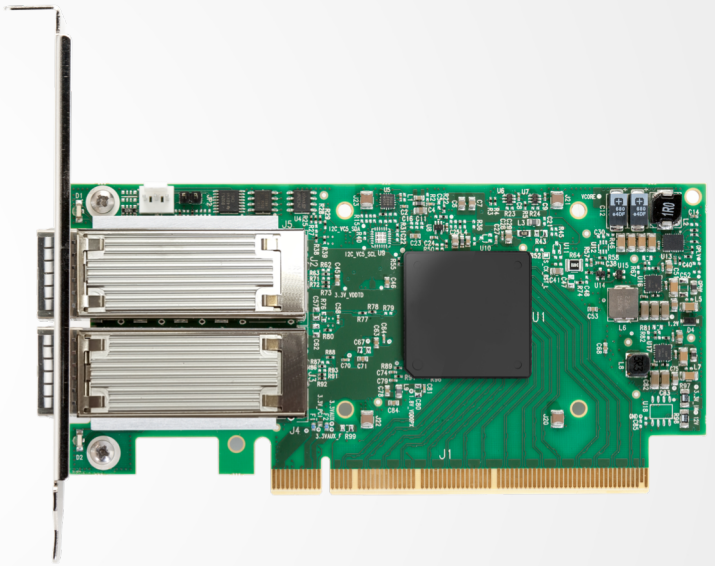
Creating an Isolated Data Center Security Policy Model Using SmartNICs



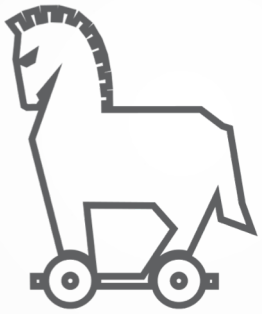
Ofir Arkin, VP Security

HITB Amsterdam 2018

Inherent Data Center Security Issues

A Broken Perimeter Centric Security Model

Lack of Visibility and Control



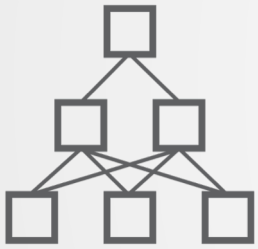
Attack Sophistication

Complexity of Networking and Software

Geopolitical

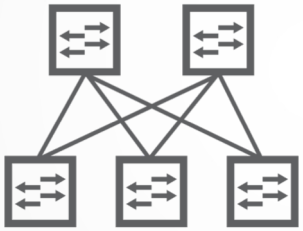
Modern Data Center Architecture

Delivering Networking Capabilities in a Scalable, More Agile and Cost Effective Manner



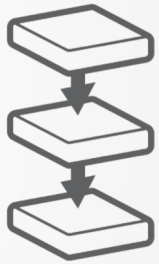
Modern Application Architecture

Massive Growth in East-West Network Traffic



Leaf-Spine Network Architecture

Network and Server Virtualization



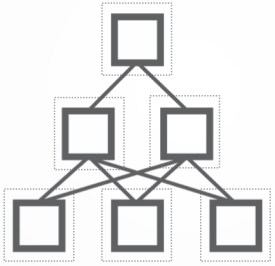
Software Defined Networking (SDN)

More Data to Process at Higher Speeds

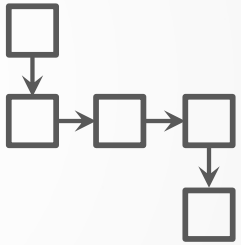
Changes to the Data Center Networking Environment are Forcing Security to Re-Invent Itself

Adaptive, Automated Security at the Edge of the Network

Granular Visibility and Control per Workload



Security Controls are Built Around Applications

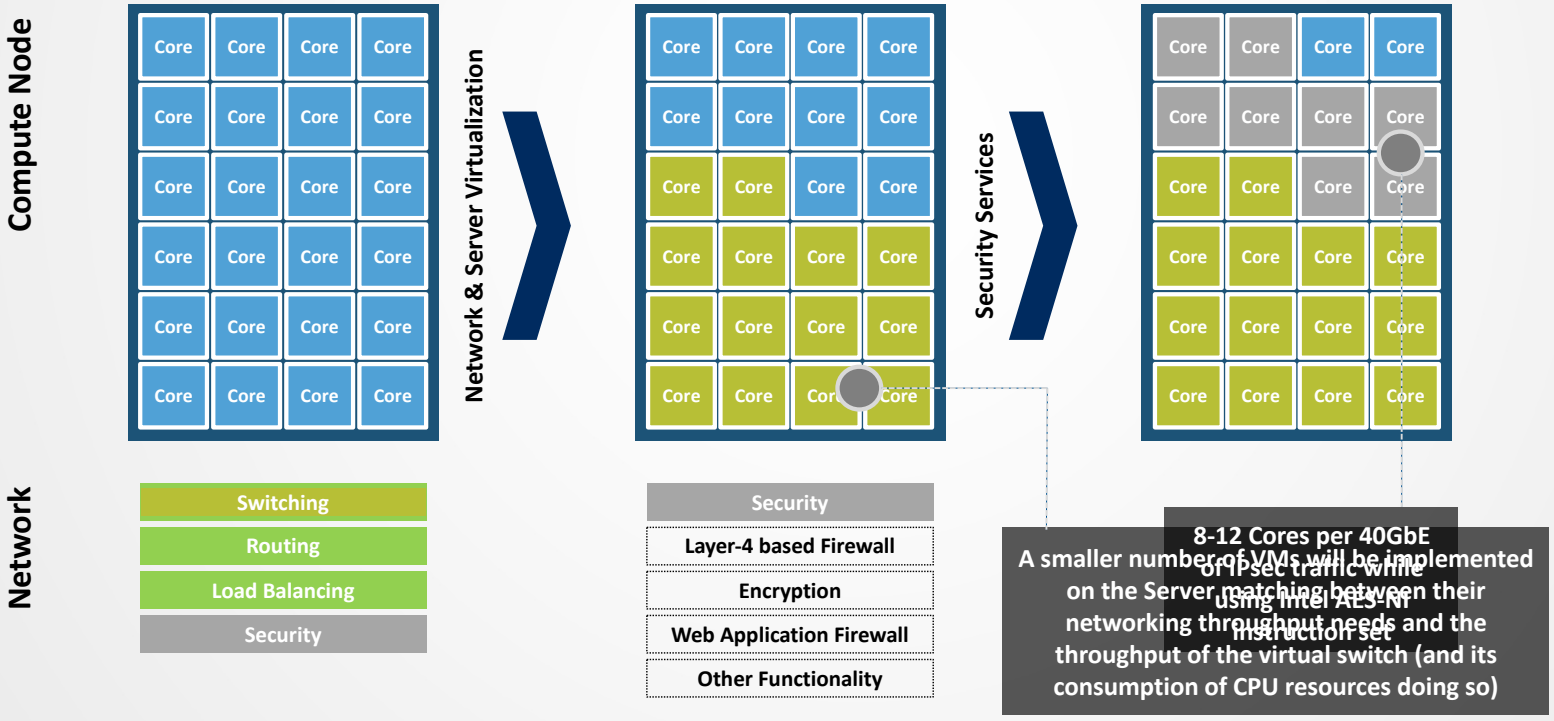


Automatic Provisioning and Orchestration of Security Controls

Massively Scales Utilizing a Host-based SDN Model

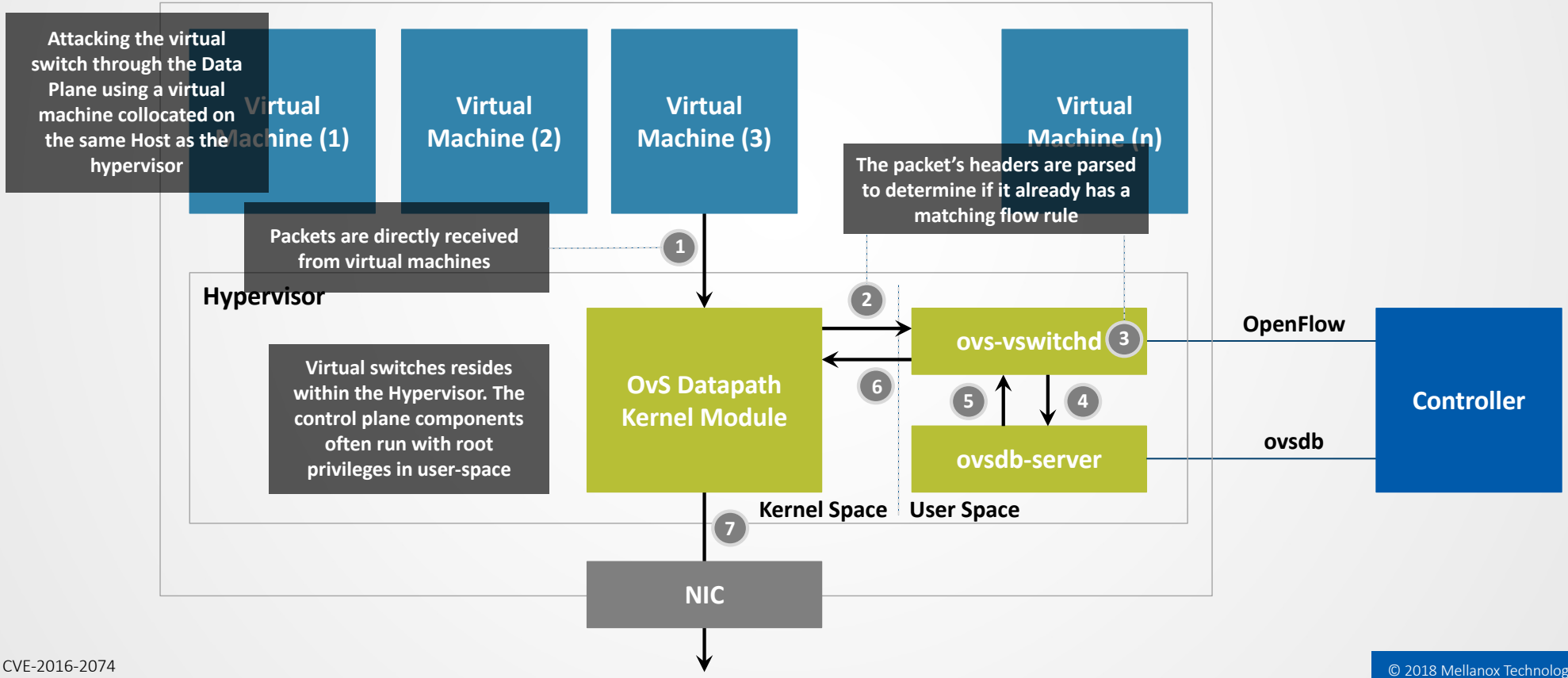
The Server CPU Bottle Neck

Software Efficiency is Significantly Reduced as Infrastructure Functionality is Implemented at the Host and More Data is to be Processed at Higher Speeds



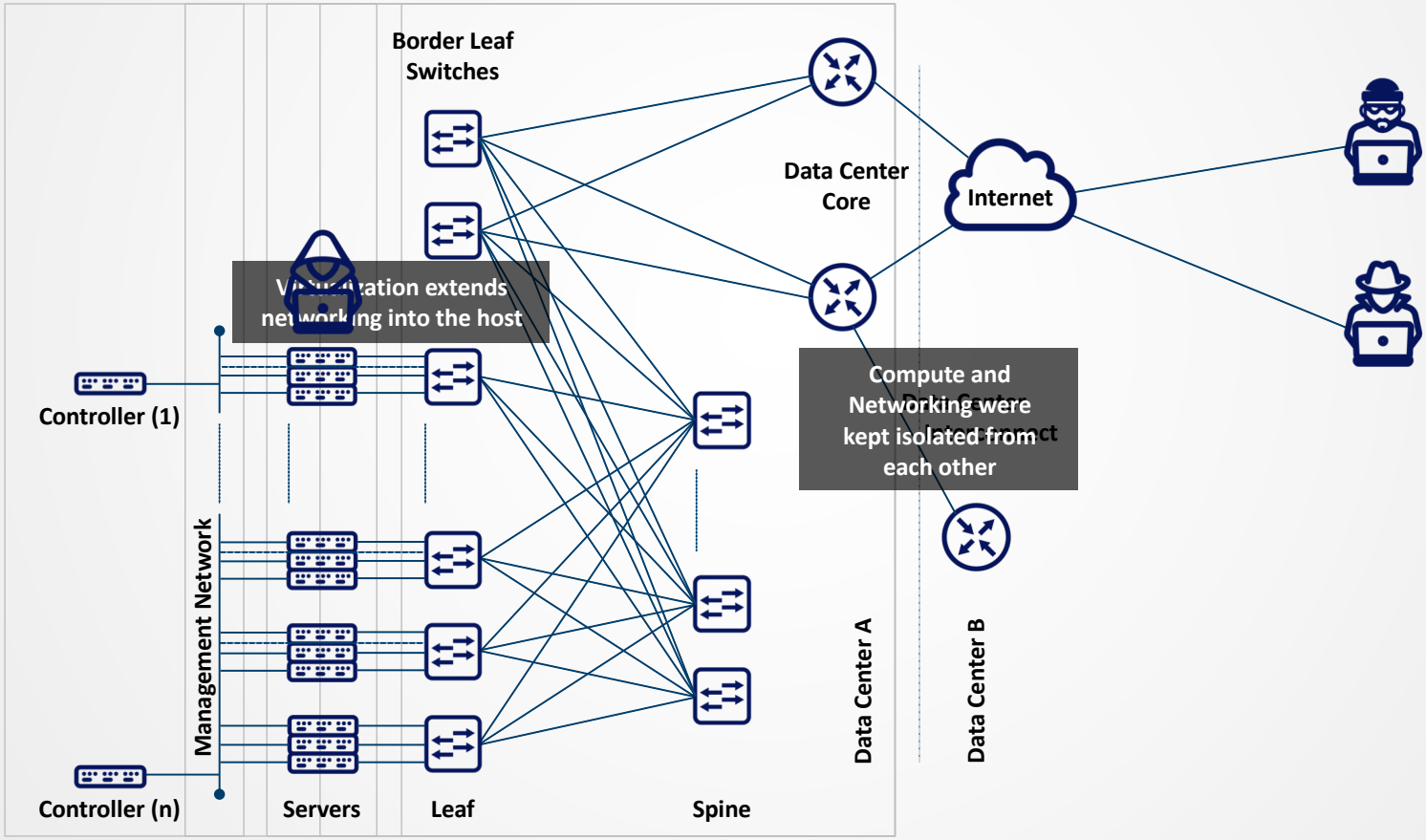
Complexity Expands the Attack Surface

Infrastructure Functionality and User Apps Are Commingled on Shared Infra.

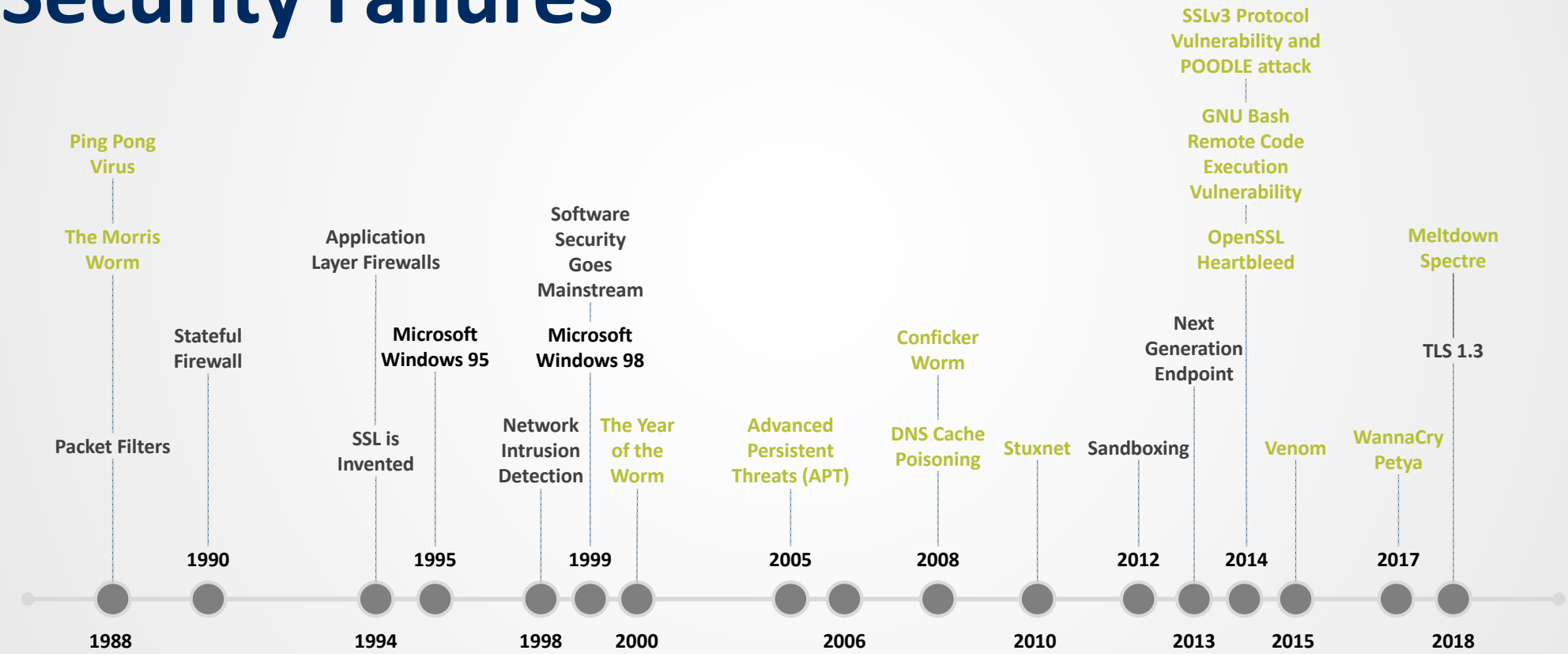


* CVE-2016-2074

Different Trust Domains Are Bridged



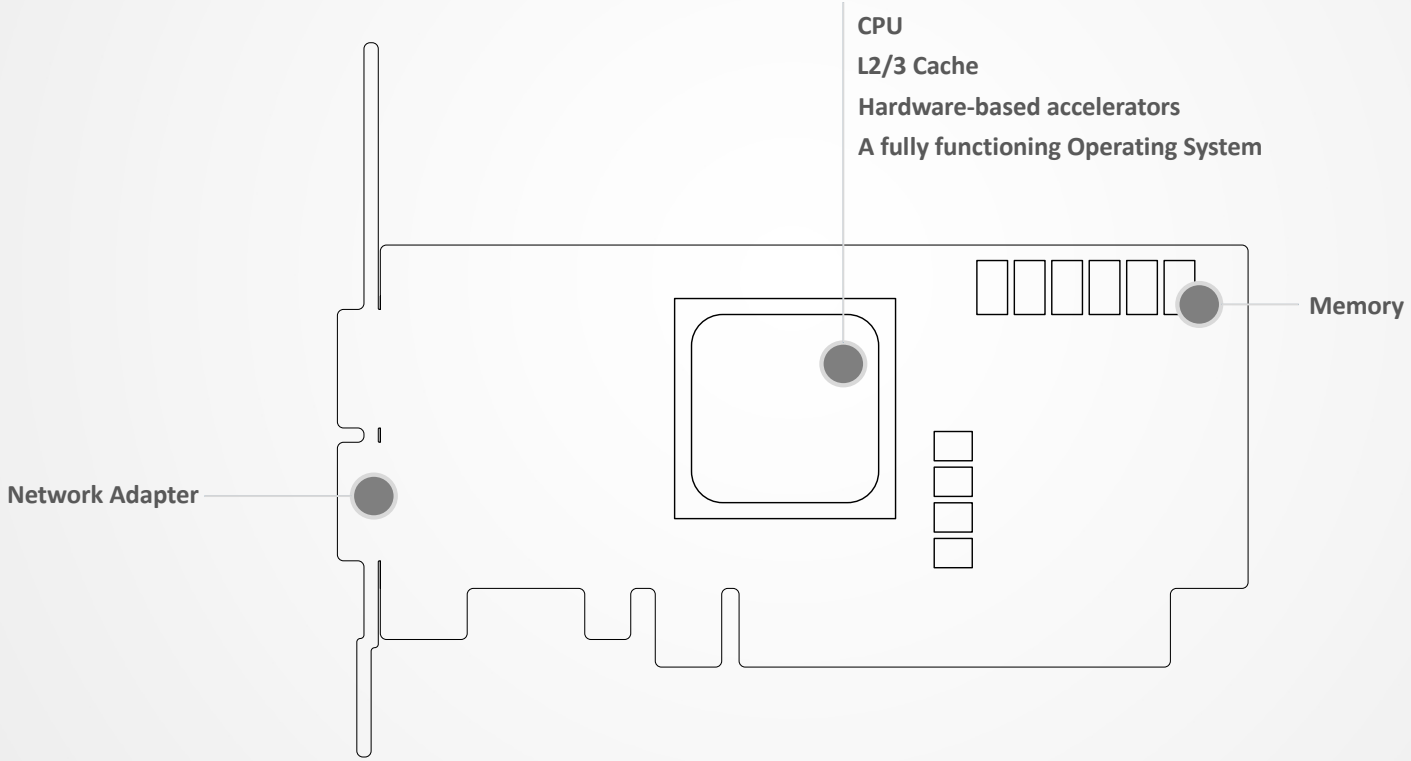
30 Years of Host-based Security Failures



WHAT HAPPENS TO HOST-BASED SECURITY, THEN, AS SOFTWARE SECURITY CONTROLS ARE PLACES IN THE SAME TRUST DOMAIN AS A POTENTIAL ATTACKER?

A SmartNIC is a Computer

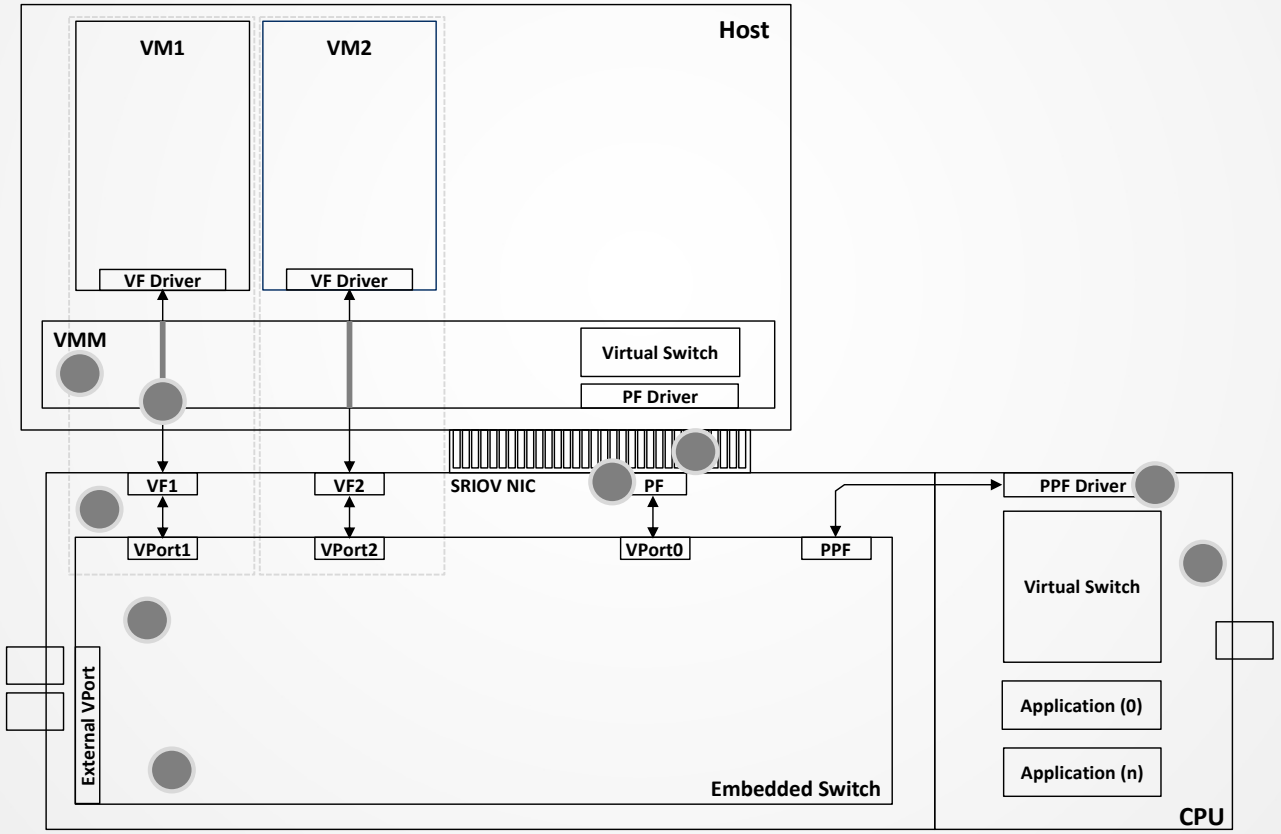
With Strict Power Consumption Restrictions



Function Isolation

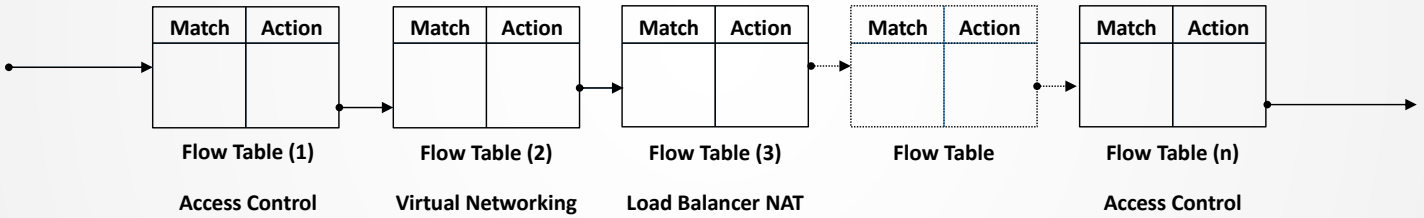
- Infrastructure functions (networking, storage, and security) **are fully implemented in**, **and offloaded by**, the smart network adapter in a manner that does not allow the host to interfere with their operation
- **Functionality runs (more) secure as it is isolated from the host**
- A successful attack against the host, or one of the workloads using it, **does not warrant the ability to alter the policies applied to infrastructure functions** as those are enforced by the smart network adapter

Creating an Isolated Trust Domain



Flow Tables

A Programmable Logic Used to Determine the Path Packets are to Take Based on Their Classification and the Policy Enforced

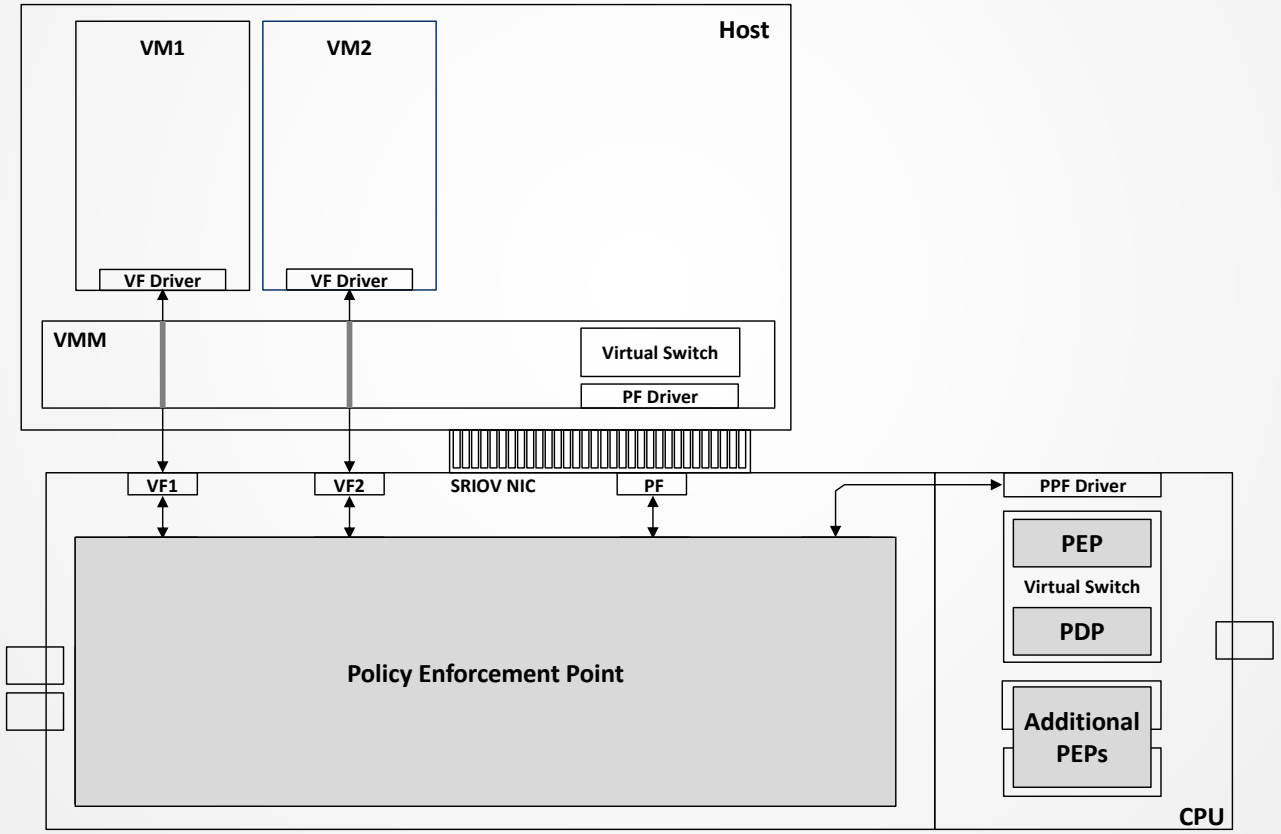


Match: VLAN ID, VXLAN VNI, GRE Key, SMAC/DMAC, SIP/DIP, Source Port/Destination Port, TCP Flags, Session, etc.

Actions: Allow, Deny, Route, Pop/Push, NAT, Modify, Encrypt/Decrypt, etc.

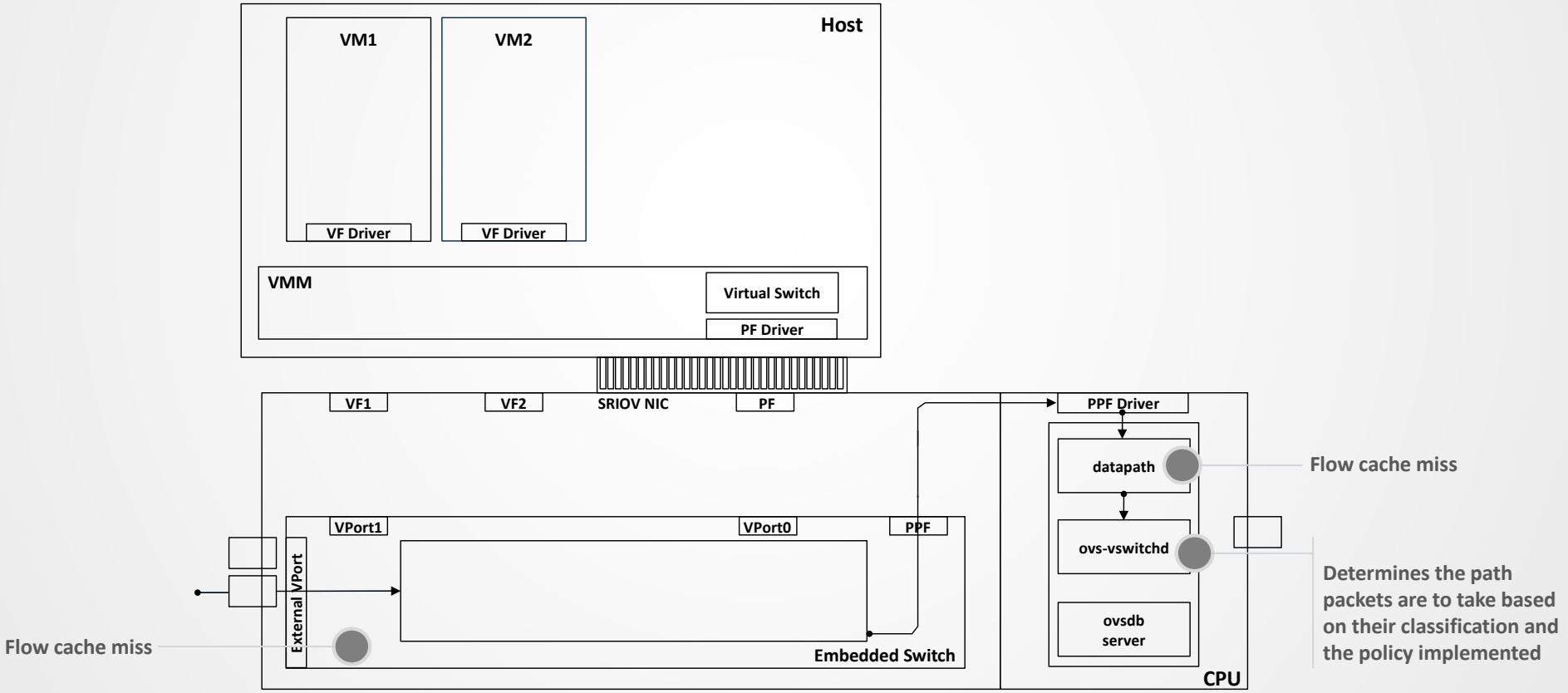
Controlling the Flow of Data

A Programmable Platform with a Dynamic Data Path



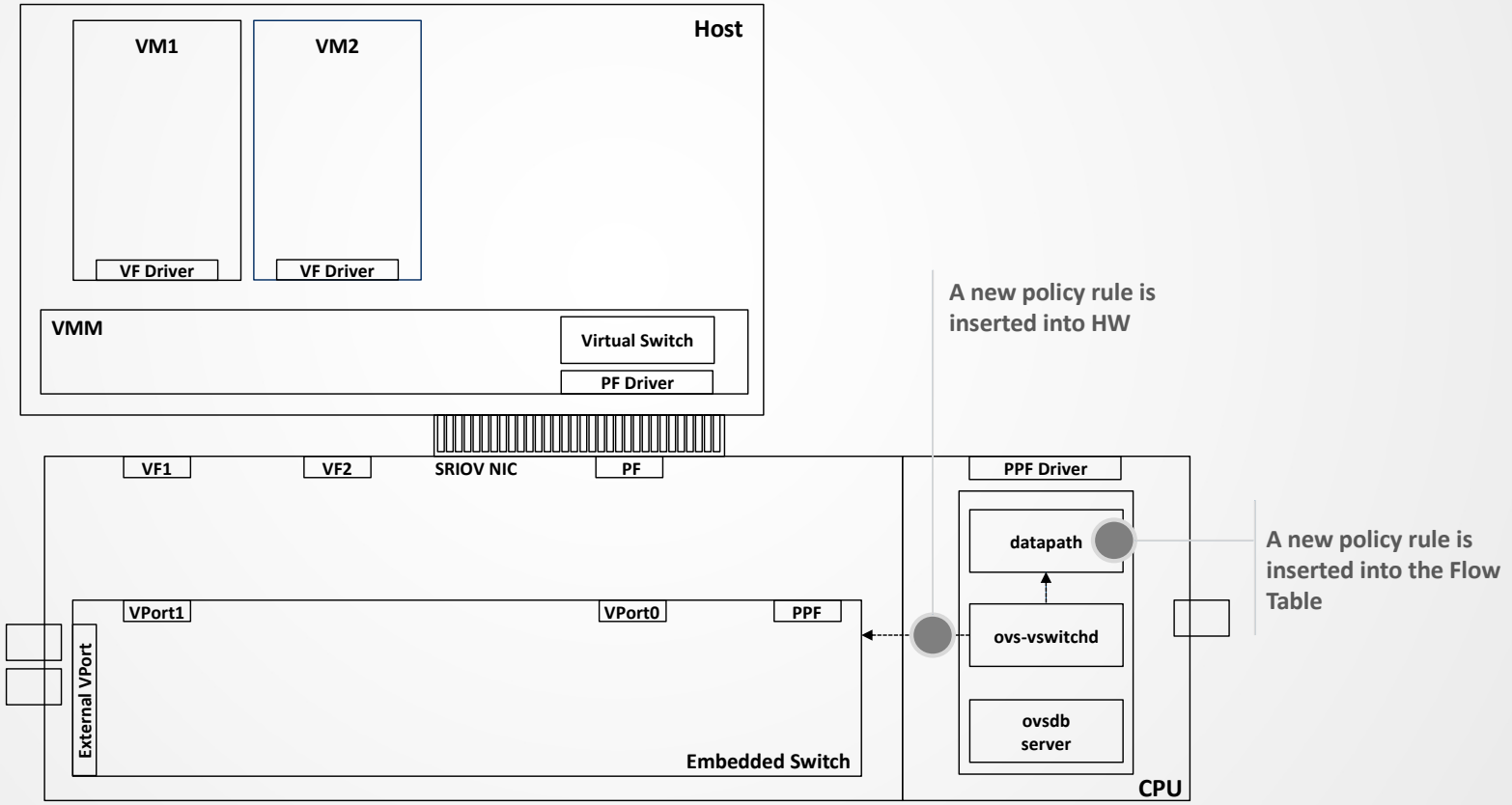
Applying Policy Per-Session

Control & Visibility Per Workload



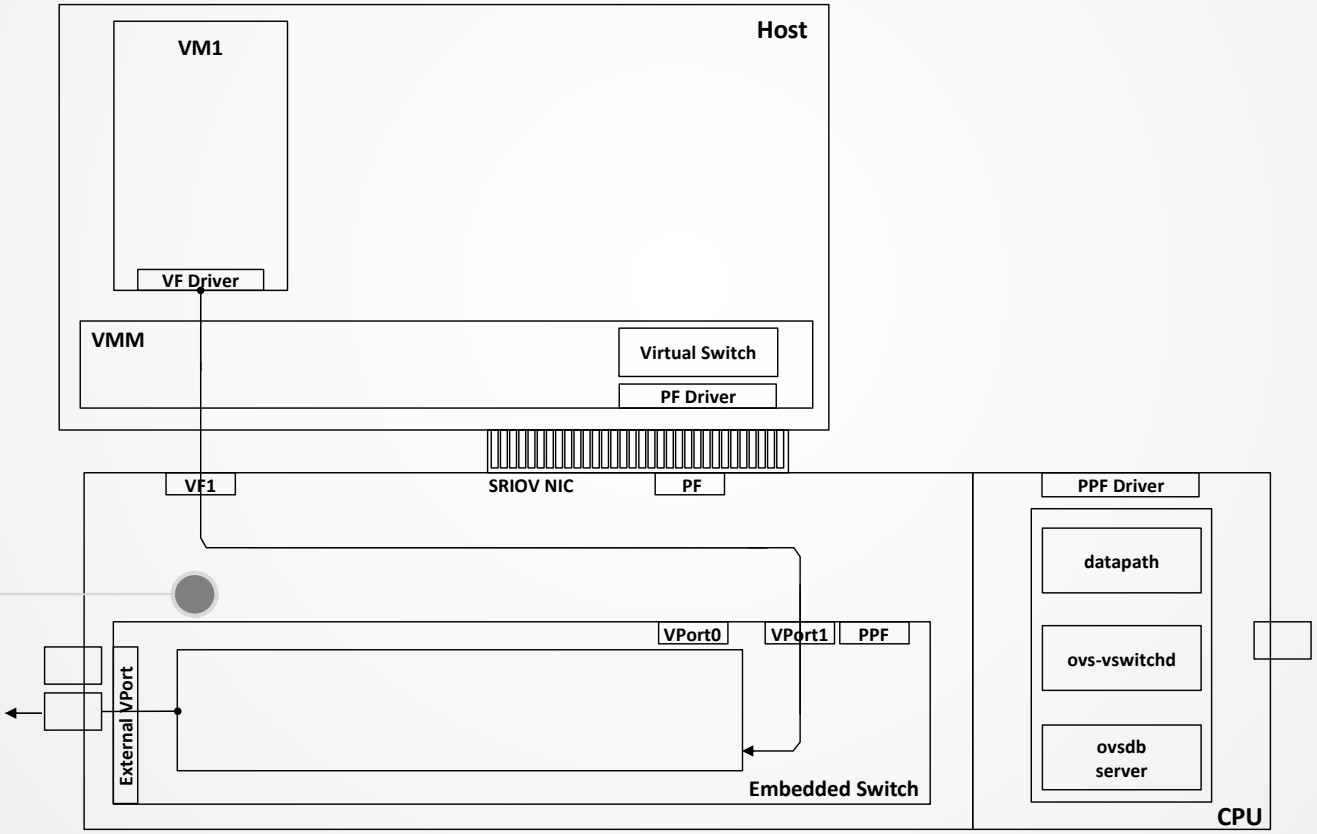
Hybrid Policy Enforcement

Applying a Session-based Policy



Hybrid Policy Enforcement

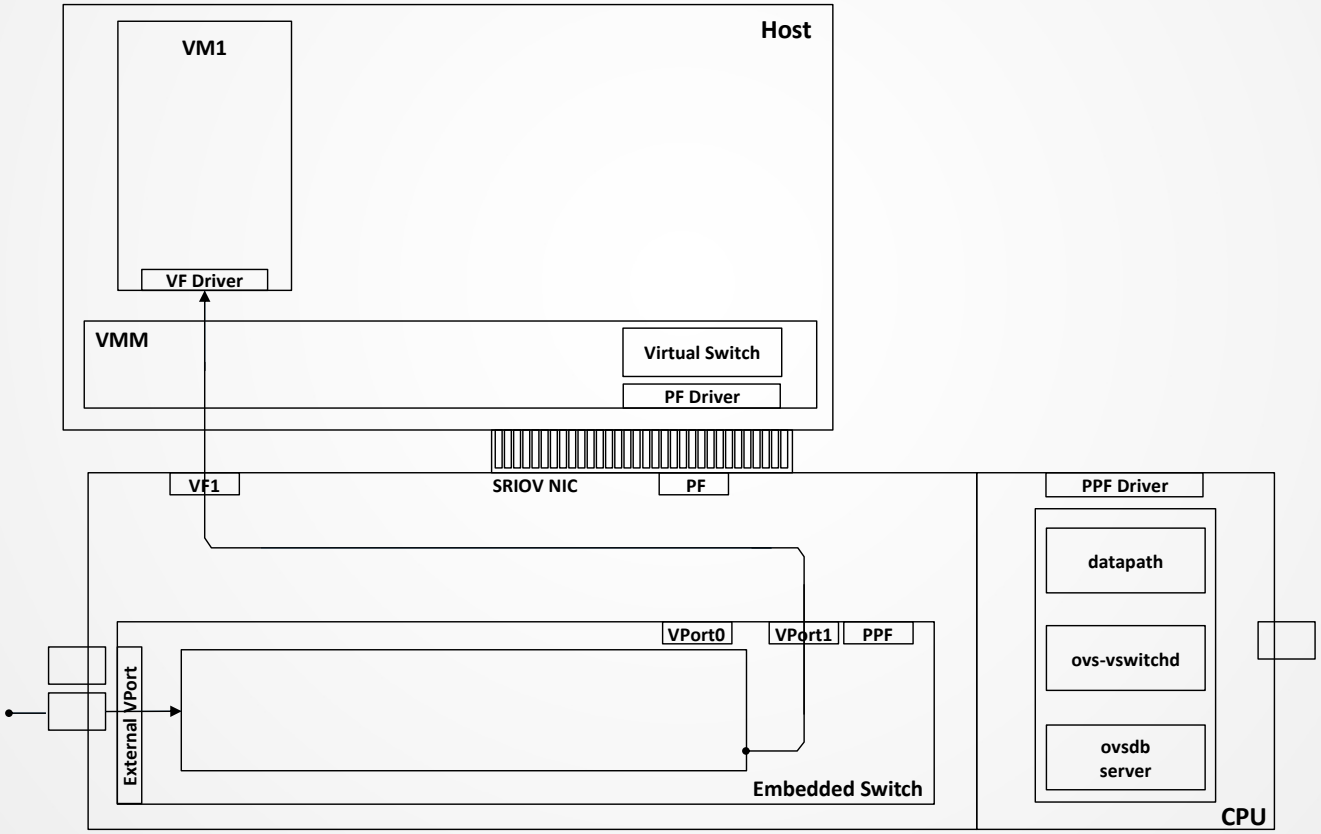
Policy Enforcement Moved to the Fast Path



Enforcement decisions are now made by the silicon (NIC) without additional software intervention

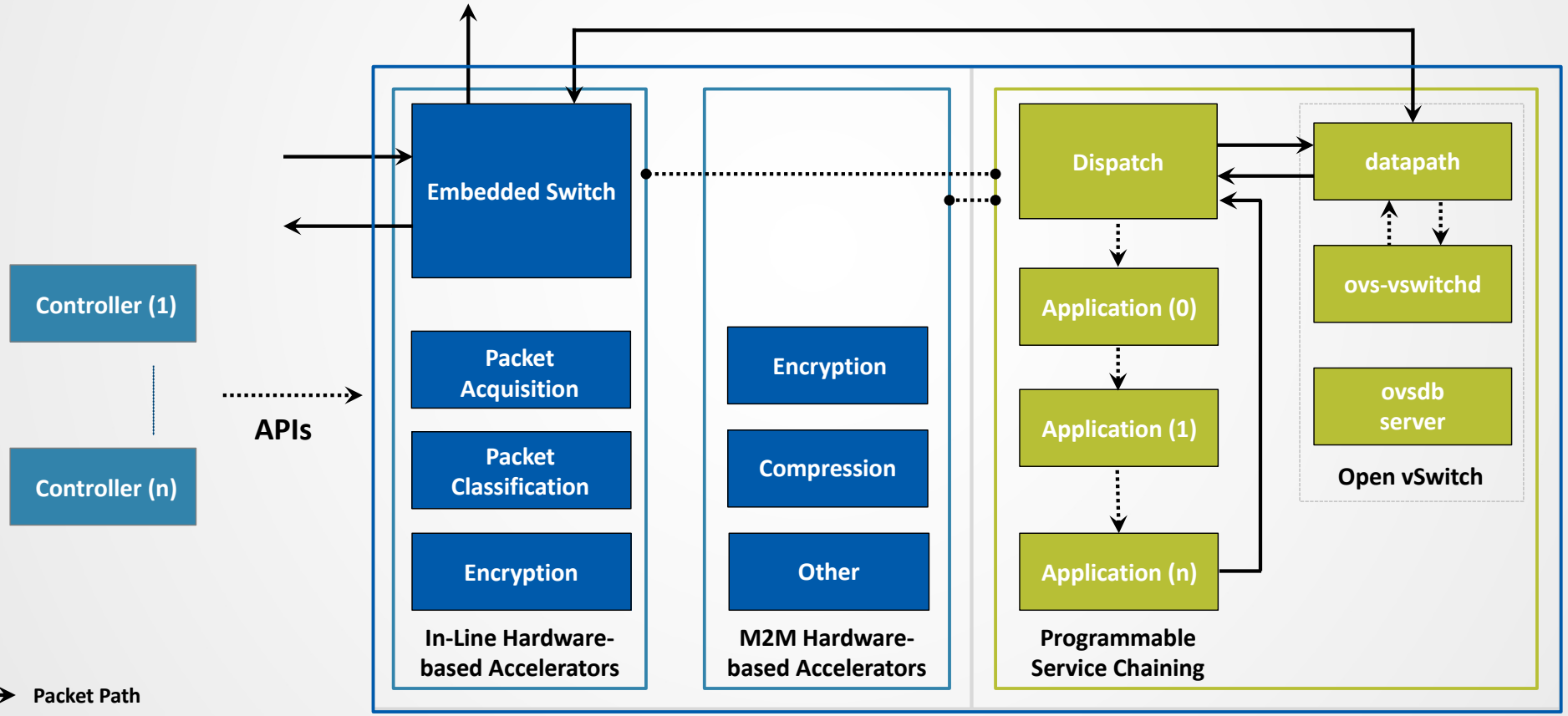
Hybrid Policy Enforcement

Policy Enforcement Using the Fast Path



A Programmable Platform

A Dynamic Data Path Configured By Policy



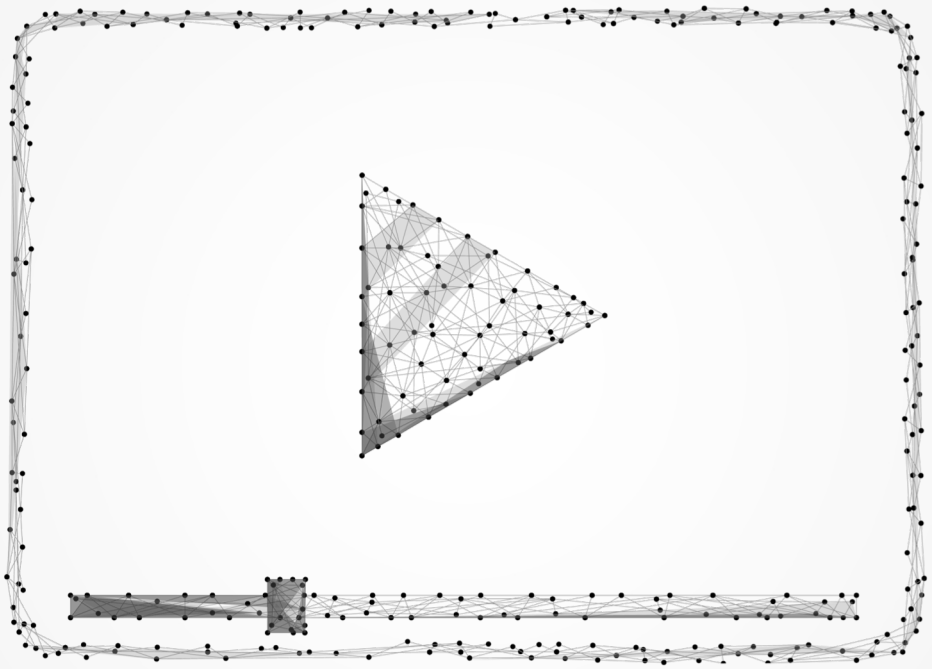
Sample Applications

Granular Visibility and Control per Workload

Micro Segmentation

Protection of Data-in-Motion and Data-at-Rest

Workload Behavior Monitoring



Thank You