



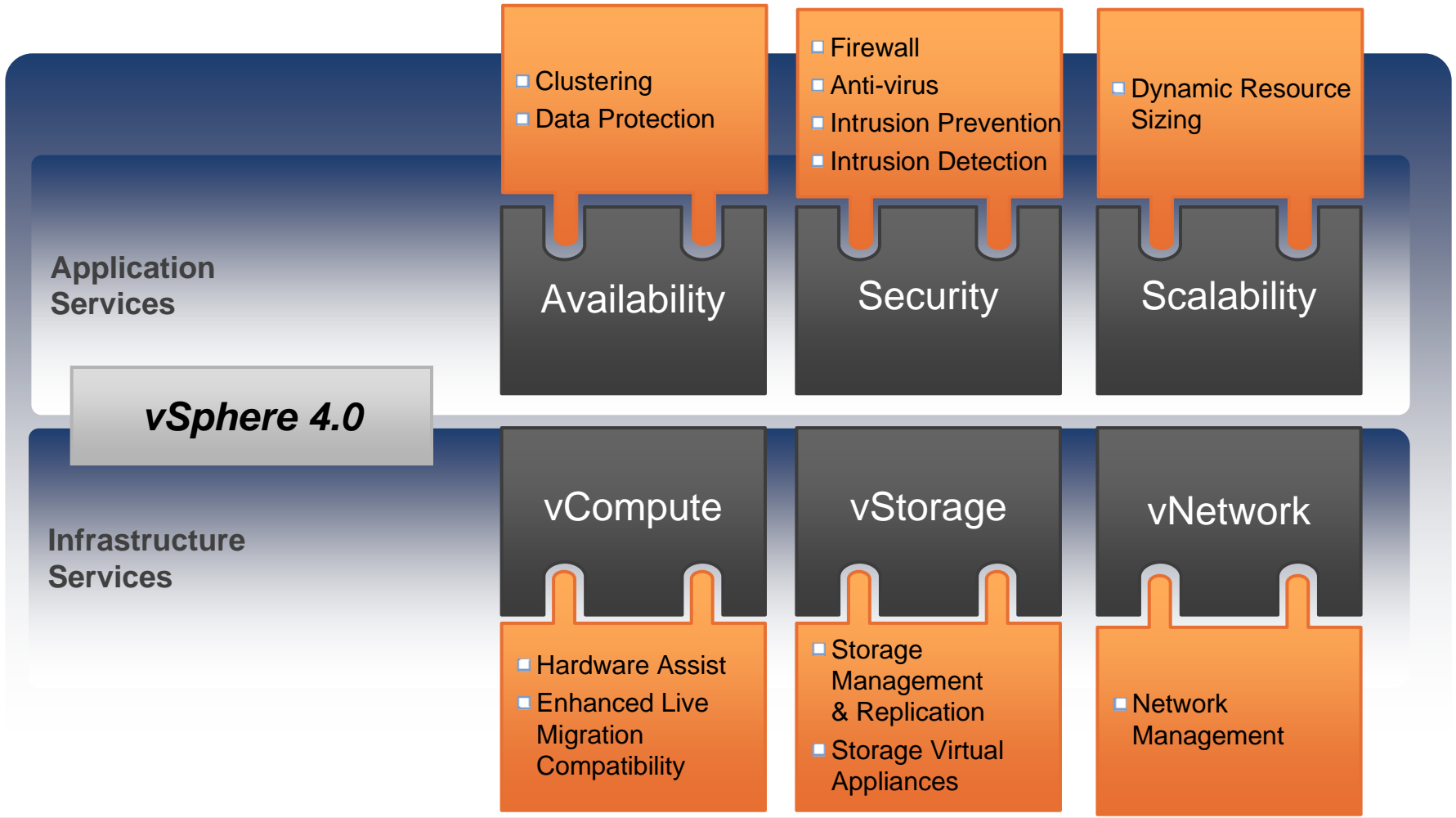
# VMware & Security: VMsafe

Bob van der Werf

Sr. Systems Engineer

VMware

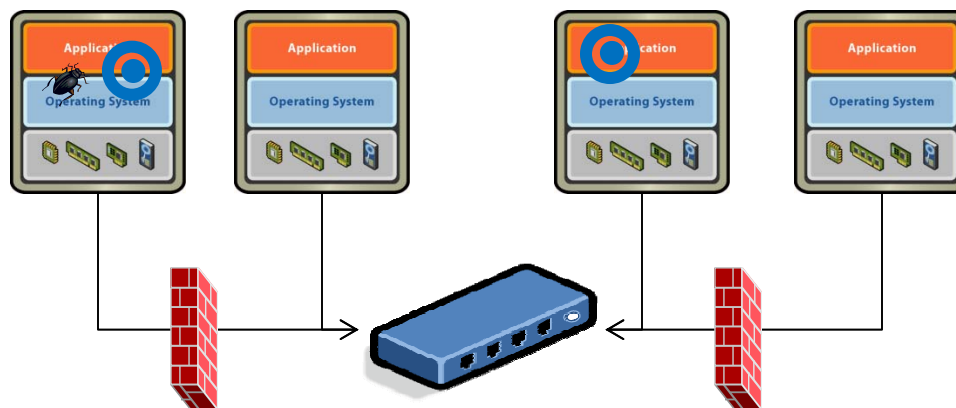
# VMware vSphere™ – Components



## Leveraging Virtualization To Solve Security Problems

### Security solutions are facing a growing problem

- Protection engines do not get complete visibility into the OS
- Protection engines are running in the same context as the malware they are protecting against
- Even those that are in a safe context, can't see other contexts (e.g. network protection has no host visibility).





# VMware VMsafe API's

# VMware VMsafe™

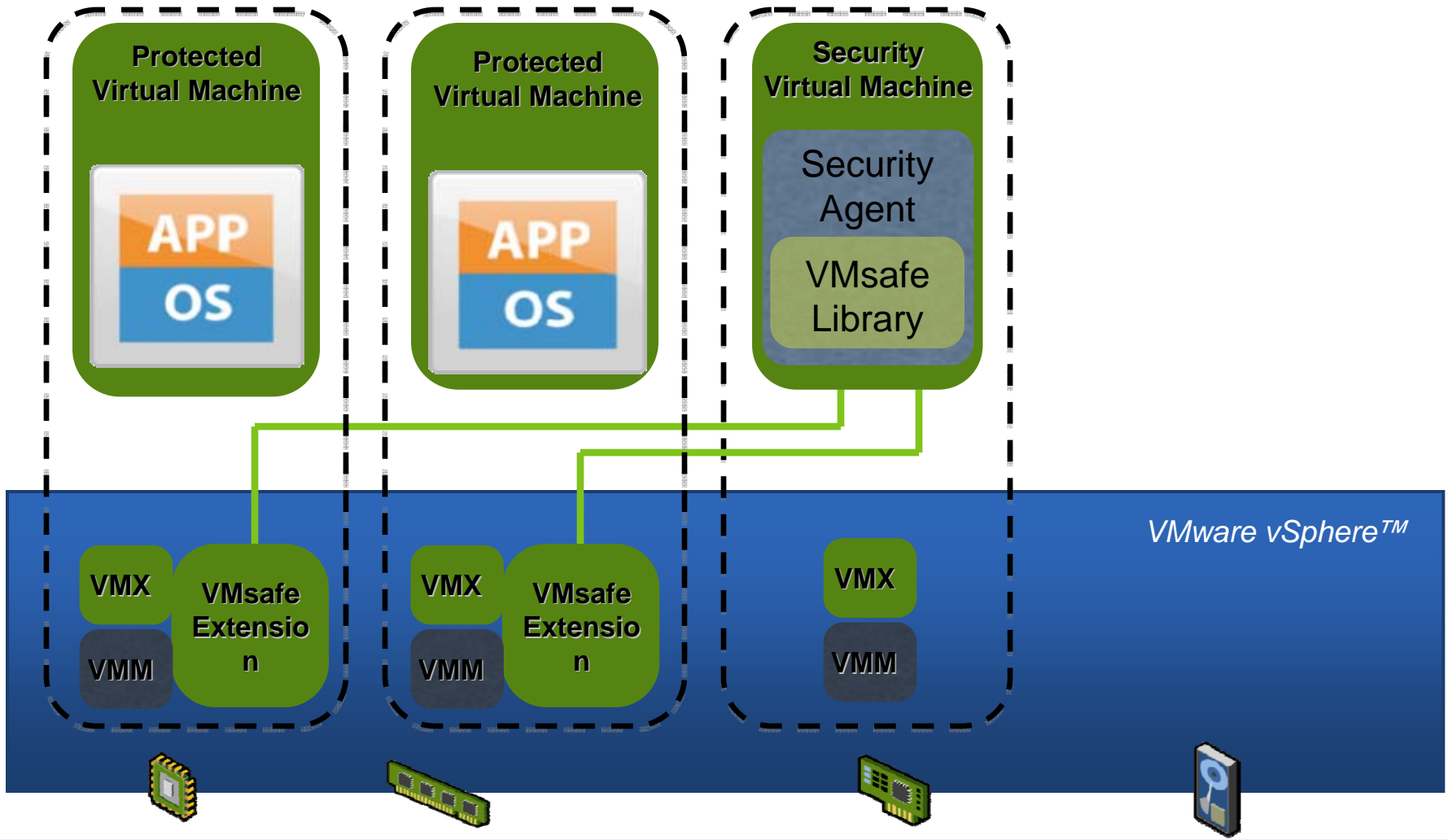
- > New approach to VM Security
  - Protect by inspection of virtual components (CPU, Memory, Network and Storage)
  - Functionality provided in Security Virtual Appliance
- > Complete integration with VMware vSphere, e.g.
  - Vmotion
  - Storage Vmotion
  - HA
- > Better Context
  - Isolated from the malware
  - In cooperation with the smaller, trustable codebase of the hypervisor



## VMsafe CPU/Memory API

- > Can inspect memory locations and CPU registers
- > Hypervisor Extension implemented as VMX/VMM modules
- > VMsafe API Library
  
- > Capabilities:
  - Detect current application state in the protected VMs CPU from general purpose register values
  
  - Sense system configuration state from the control registers on the protected VM

# VMsafe CPU/Memory Interface



# VMsafe CPU/Memory API Use Cases

## BIOS: Early Boot Security

- > Security Agents are up and running before the protected VM powers on

## System Integrity Protection

- > The Security Agent can monitor the protected VMs physical memory accesses

## Enforce Multiple Policies (verify-before-execute)

- > Defeats: Shellcode injection attack (overflow attack)
- > Defeats: Kernelcode injection attack (bypass driver-signing processes)

## Vmsafe Network Packet Inspection API

Provides distributed virtual filter (DVFilter) solutions to protect network packet streams

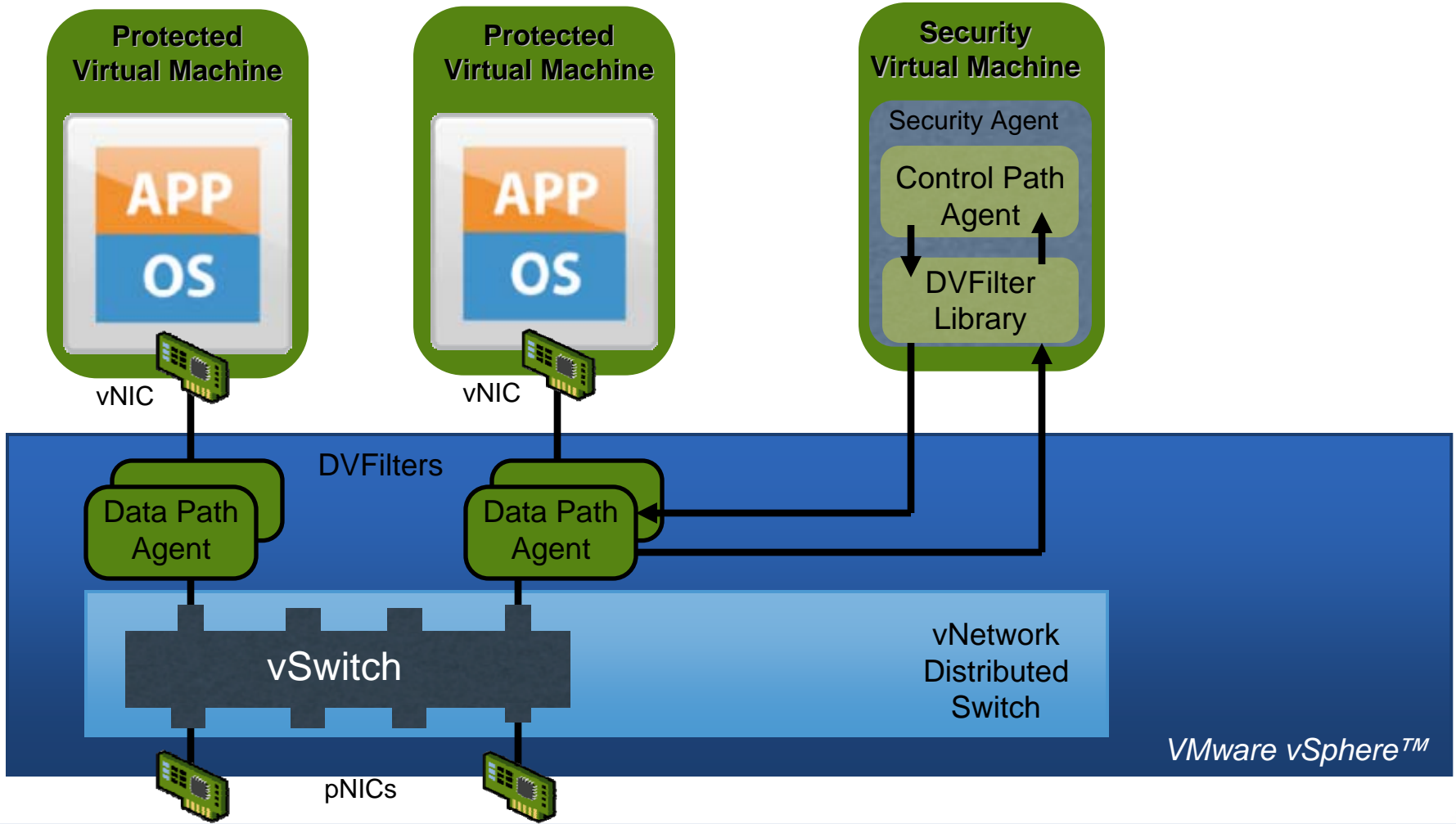
### **vNetwork Data Path Agent (Fast Agent)**

- > Installs as a kernel module and directly intercepts packets in the virtual network packet stream

### **vNetwork Control Path Agent (Slow Agent)**

- > Resides in a security virtual appliance and can be used for further thorough processing

# VMsafe Net Data/Control Path Agents



VMware vSphere™

## VMsafe Network Packet Inspection API Capabilities

- > Inspecting packets
- > Modifying packets
- > Passing a packet to the control path agent for further processing
- > Dropping packets from the packet stream
- > Injecting packets in the packet stream

## VMsafe Virtual Disk Development Kit

Provides interfaces that allow for applications with possibilities for direct manipulation of Virtual Machine Disk Format (VMDK) images

### **VDDK: Virtual Disk Development Kit**

- > Read/write data anywhere in a VMDK file
- > Create and manage redo logs (parent-child disk chaining)
- > Read and write disk metadata

## VMsafe Virtual Disk Development Kit: Use Cases

- > Read the VMDK image files offline, checking each sector for a virus signature
- > Perform a forensic analysis on the VMDK image files
- > Monitor compliance of configuration files on virtual disks
- > Scan for unauthorized content on virtual disks, such as credit card or social security numbers

# Current VMsafe Program Partnerships





# Thank You

Bob van der Werf

[Bvanderwerf@vmware.com](mailto:Bvanderwerf@vmware.com)

<http://www.vmware.com/go/security>

<http://www.vmware.com/go/compliance>