

HP TippingPoint Virtual Controller and Virtual Management Center

Solution brief

Is management of a virtualized environment a major concern? Does your business need a technology that helps you secure your virtual environments?

With the gaining popularity of virtualization in today's enterprise data centers, you need a virtual security solution that allows you to confidently adopt virtualization throughout your data center without compromising on your existing security postures.

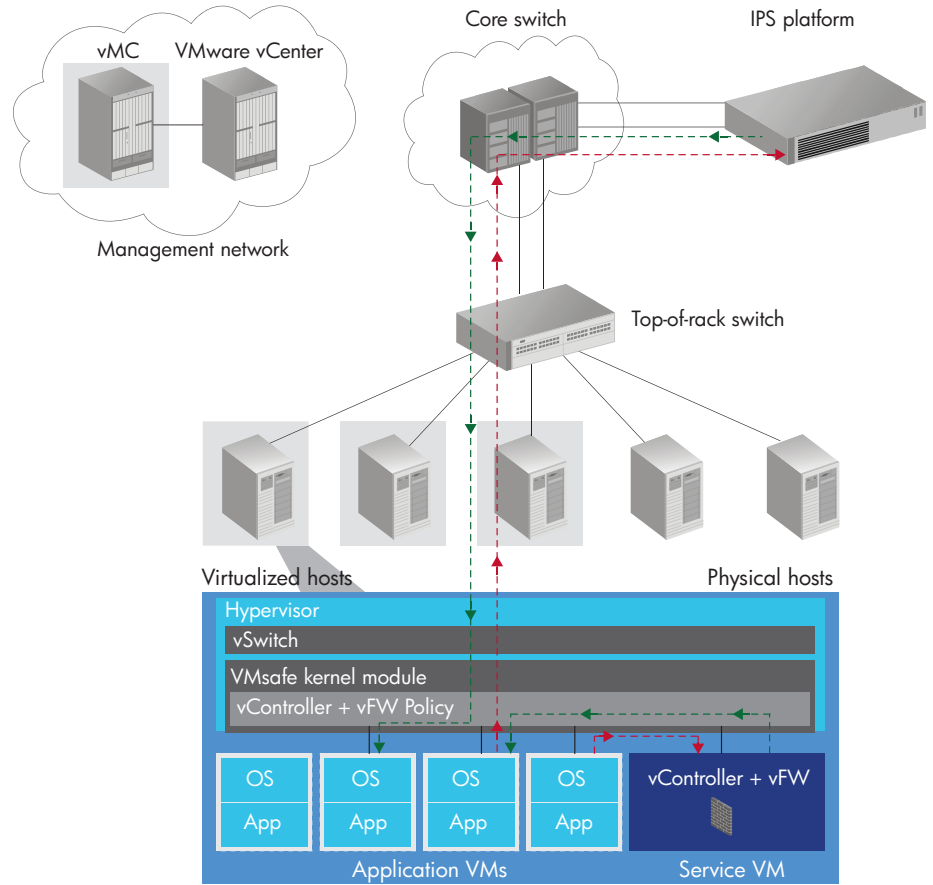
Data center segmentation

Consolidated data center security and management: The HP TippingPoint Secure Virtualization Framework is designed to provide IT personnel a single consolidated, yet flexible solution for extending the HP TippingPoint IPS Series with its excellent threat protection into the virtualized data center. The solution currently includes two components:

- Virtual Controller (vController)
- Virtual Management Center (vMC)—both the vMC server and client are included with vController

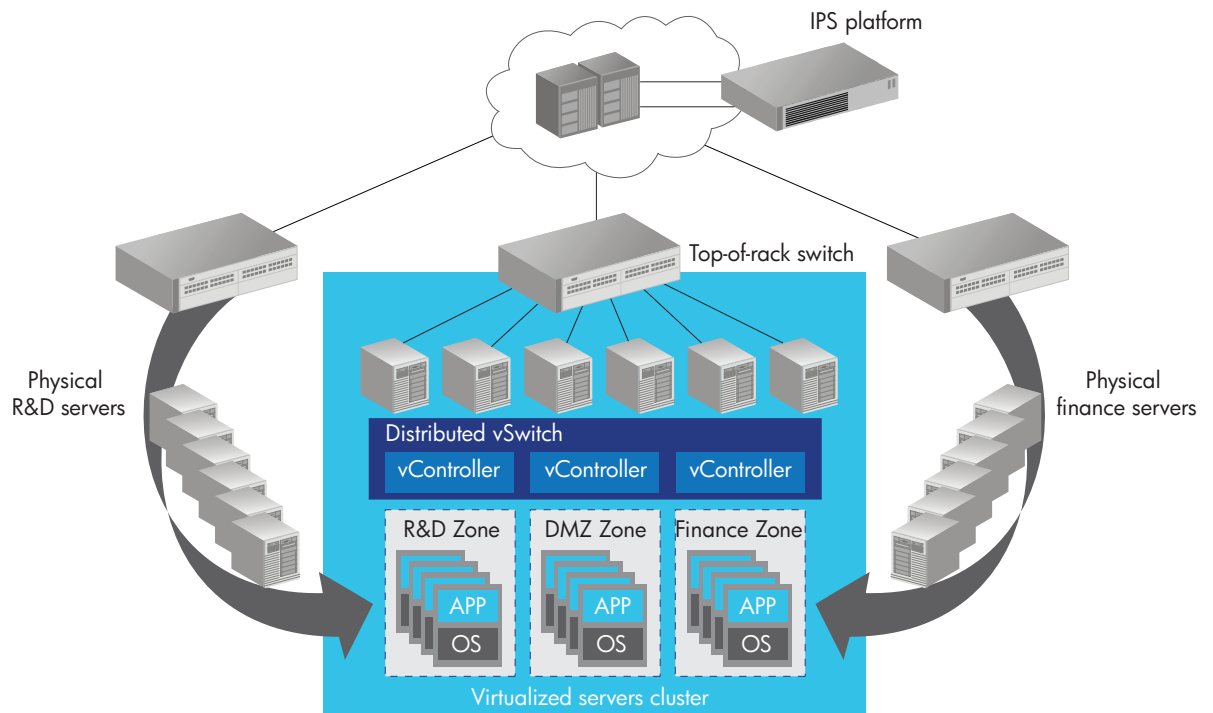


Figure 1: HP TippingPoint Secure Virtualization Framework



Purpose-built data center segmentation solution: The HP TippingPoint vController and vMC are purpose-built software solutions designed to enable the physical IPS platform to enforce full data center segmentation of trust zones for physical hosts, virtual machines (VMs), and even mobile VMs. The vController intercepts all packets within the hypervisor and based upon user-defined policies, tunnels packets to an HP N Series IPS for inspection.

Figure 2: Physical and virtualized data center segmentation with Secure Virtualization Framework



Extend IPS into the virtual data center:

The vController extends HP TippingPoint's industry-leading IPS and DV Labs security research capabilities into the virtual data center. The vController enables enterprises to apply IPS security policies to all traffic from physical hosts and virtual machines. This enables IT administrators to extend their existing security processes, methodologies, tools, and knowledge to secure their virtual infrastructure.

Leverage previous HP TippingPoint IPS platform investments:

With the vController solution, customers gain the peace of mind of continuing to use already-proven HP IPS technology. Further, the units that have been purchased for physical data center protection and segmentation can easily be utilized with the vController to also protect their virtual data center infrastructure. This makes virtual data center protection much simpler and cost-effective for IT administrators.

Protect the entire data center attack surface:

The vController as a component of the HP TippingPoint Secure Virtualization Framework can be used to protect the entire data center attack surface. This includes protection of or inspection of:

- Network infrastructure
- Host servers
- Virtualization tools including the hypervisor
- Operating systems
- Enterprise applications and Web applications
- Virtual desktop infrastructure (VDI)
- VM traffic, mobile VM traffic, and VM-to-VM traffic

Maintain security and separation of duties:

One of the difficulties imposed on IT by virtualization deployments is the inherent challenge in maintaining necessary separation of duties between networking, security, and other IT responsibilities. The HP TippingPoint vController security solution is completely managed by vMC, which is fully integrated with the HP TippingPoint Security Management System (SMS), making it easy to keep all security management functions contained and available only to IT security personnel and no one else.

Security enforcement

Proactive security policy enforcement: Automated policy enforcement across physical and virtual data center infrastructure virtually eliminates the need to respond to myriad alerts, or to clean up after cyber attacks have compromised network resources. IT security costs are reduced by eliminating ad hoc patching and alert response, while simultaneously increasing IT productivity and profitability through elimination of emergency patching and protection of critical applications.

Single set of security policies: Extending the HP TippingPoint IPS solution with vController into the virtual data center means IT security personnel can maintain and enforce security across the entire data center including physical hosts, VMs, and mobile VMs with a single set of security policies. The integration of SMS and vMC gives IT personnel a single console for data center security policy management.

Dynamic security policy enforcement: The vMC is used to automatically discover every VM in the data center and deploy vController on each virtualized physical host. This enables appropriate security policies to be dynamically applied and enforced by vController and the IPS platform for all deployed and discovered VMs.

Security policies follow VMs: Virtualization of data center infrastructure creates new challenges for security personnel due to the ease with which VMs can move from host to host and even data center to data center. However, the vController and vMC gives IT the tools to easily maintain visibility into the location and state of every VM so that the appropriate security policies are applied regardless of the VM state (on, off, or in motion).

Virtual patching: With the security expertise of HP TippingPoint DV Labs, filters are delivered which guard entire vulnerabilities, not just known exploits. These filters block the various exploits for a given software vulnerability, creating in essence a "virtual patch" for each vulnerability. This virtual patching capability is critical in today's virtualized data center to cover possible patch management issues created due to VM roll-backs and or server/VM shut-downs. The vController protects the data center infrastructure against these possible patch management issues.

Simple yet flexible policy creation

Create simple vController policies: The Virtual Management Center simplifies creation of vController policies. Within the vMC, IT personnel create simple routing policies based on defined services, trust zones, traffic direction, and associated action sets. These policies then get deployed to all vControllers on every virtualized physical host ensuring all VM traffic can be appropriately inspected on a physical or virtual IPS platform.

Easily create a list of services: The vMC makes it easy to create a list of services to be monitored within vController policies. Examples of services include DNS, DHCP, NFS, and HTTP. These services then become one of the key building blocks for vController policies.

Easily create a list of trust zones: The vMC makes it easy to create a list of data center trust zones for vController policies. These zones allow IT to keep

virtualized data center infrastructure segmented and/or isolated for security purposes. Trust zones will typically be groups of similar machines and VMs such as lines of business (e.g. HR, finance), or different physical data centers (e.g. Dallas DC, London DC), or even different VM administrators or IT departments. These trust zones then become one of the key building blocks for vController policies.

Create default VM policies: Virtualization makes the creation and replication of VM environments extremely easy. In fact, this is one of the key benefits of virtualization and the HP TippingPoint vController solution is designed to support this benefit by giving IT personnel the ability to create default vController policies. These policies are then applied to all newly created or untrusted VMs or zones so that security policies are applied to the entire data center as appropriate.

Cloned VMs inherit parent policies: The replication of VM environments can be extremely easy and for this reason the vController solution is designed such that all cloned VMs can automatically inherit the policies associated with the parent VM. Once again, the security policies are applied to the entire data center as appropriate.

VMware certified

VMware certified: Both the vController and vMC are certified by VMware facilitating proper interoperability and integration. Both products are certified on VMware vSphere 4 update 1 (ESX 4 and ESXi 4).

VMware vCenter integration: The HP TippingPoint vMC is integrated with VMware's vCenter management console for virtual data center discovery and visibility.

VMware hypervisor integration: The HP TippingPoint vController is integrated with the VMware hypervisor through the VMsafe API. VMsafe is an API developed by VMware that allows technology partners such as HP Networking to develop tightly integrated security functionality at the hypervisor level.

Easy deployment

Auto-discovery of VMs: Once installed, the vMC through integration with VMware's vCenter provides for auto-discovery of all VMs in the virtualized data

center making it easy for IT security personnel to contain the full scope of virtualization in the data center. This capability allows security personnel to maintain visibility and awareness of the virtualized data center environment, and to dynamically maintain enforcement of proper security policies for all VMs.

Auto-deployment of vController: The vMC makes it extremely easy for IT security personnel to automatically deploy vController to all virtualized hosts after VM discovery. It gives security teams confidence that the entire physical and virtual data center is protected with appropriate security levels and that all data center trust zones are appropriately segmented.

Visibility to control VM sprawl: The vMC gives IT security personnel complete visibility of the virtualized data center helping them control and secure the sprawl of VMs. Virtualization makes it easy to create, copy, and roll-back VMs creating an environment where VMs can propagate without proper oversight and security controls. The vMC/vController solution gives IT security personnel the tools to properly control and secure these heretofore uncontrolled environments.

PCI compliance

Meet current PCI-DSS requirements: The current version of the Payment Card Industry Data Security Standard (PCI-DSS) does not specifically outline requirements for virtualized infrastructure. However, the underlying security tenets in the existing PCI requirements still apply in a virtual environment. This is especially true where VMs containing cardholder data defined as a Cardholder Data Environment (CDE) resides on the same physical host as VMs containing other corporate applications/trust zones. The vController/IPS solution helps maintain the proper segmentation of the CDE in both physical and virtualized data center environments.

Prepare for future PCI-DSS virtualization requirements: The next version of PCI-DSS is likely to include requirements or at least security guidance for CDE in virtualized data centers. With the HP TippingPoint vController solution, an organization can get ahead of the PCI-DSS curve, accelerating and simplifying future PCI-DSS audits.



Get connected

www.hp.com/go/getconnected

Get the insider view on tech trends, alerts, and HP solutions for better business outcomes

