HPE Reference Configuration for vArmour Distributed Security System on HPE Hyper Converged 380
Contents

Executive summary.............................................................................................................. 3
Solution overview............................................................................................................. 3
  Key technologies............................................................................................................. 4
Solution diagrams.......................................................................................................... 6
  Reference Configuration: small deployment................................................................. 6
  Reference Configuration: medium deployment............................................................. 7
  Reference Configuration: large deployment................................................................. 8
Design considerations and solution components............................................................. 9
Summary......................................................................................................................... 13
Resources and additional links....................................................................................... 14
**Executive summary**

IT departments everywhere are under constant pressure to increase situational awareness and maintain regulatory compliance while being faced with a proliferation of connected devices and applications in the data center. Traditional security solutions were not designed for easy visibility into the devices transacting in the infrastructure and the context of those transactions in the consolidated virtualized data center and multi-cloud environments.

Policy controls remain rigid, complex, and slow to change, forcing organizations to find new ways to segment and protect their most critical assets in the face of these potentially vulnerable attack surfaces. Traditional network segmentation was based on hardware-bound zones of firewalls or VLANs. Modeled after traditional perimeter controls, these segmentation technologies create static non-elastic silos with no automation even though the data centers they are protecting have become dynamic, fast, and simple to operate.

Hewlett Packard Enterprise and vArmour (vA) have partnered to introduce an industry-leading secure data center solution leveraging an HPE platform and the vArmour Distributed Security System (DSS). The joint solution provides automated segmentation, network, user, and application (Layer 2 to Layer 7) level visibility, coupled with fine-grained policy enforcement for all workloads running on Hewlett Packard Enterprise platforms.

In addition to the security advantages, this solution offers measurable CapEx and OpEx savings compared to the deployment and ongoing maintenance of traditional firewall solutions, which offer limited value in highly virtualized hyperconverged cloud environments.

**Target audience:** This document is a Reference Configuration written for Solution Architects, Cloud Infrastructure Designers, and others wishing to learn more about this solution from vArmour and Hewlett Packard Enterprise.

**Document purpose:** This document describes the basic principles of vArmour on VMware® ESXi installed on an HPE Hyper Converged 380. The document establishes the physical and logical network topologies required to interoperate vArmour, ESXi, and the HPE Hyper Converged 380. Furthermore, the document delivers a series of Reference Configurations for small, medium and large clusters. And lastly, the document describes operational dependencies and automation between the HPE Hyper Converged 380 User Interface, VMware vCenter and vArmour Director. This Reference Configuration describes solution testing performed in September 2016

**Solution overview**

When moving to cloud, the traditional notion of a network zone evolves. First, siloed infrastructure is fundamentally at odds with consolidation. Consolidation is about shared resources and the concept of shared resources is fundamental for a cloud scenario. Second, the traditional network design for a DMZ, or a specialized segment, envisioned a static environment where a perimeter control or a network control was implemented. These are fine in traditional physical 3-tier architectures but not in the cloud model. The very nature of cloud workloads is that they are virtual and dynamic, and give operators the ability to spread workloads across the infrastructure. Older paradigms, like placing workloads and hard coding networking to each workload, are not options, as doing so will break the network connectivity anytime there is a workload mobility event such as VMware vSphere vMotion. Even when anticipating these changes, it is extremely challenging to manage change both for the network and security level in that network.

To solve the problem, the first step is to address it by understanding it. There is no point to consolidation or building your own private cloud unless you build security into your design.

When designing appropriate controls for your cloud, vArmour and Hewlett Packard Enterprise address four design philosophies:

1. **Independent controls** – Operators want a set of controls that are independent of the workload and the underlying network. These controls deliver the broadest range of flexibility while preserving an independent perspective on traffic, from which to administer policy.

2. **API driven** – Controls must be extensible with the ability to be instantiated from multiple orchestration systems. This allows the controls to be extended or augmented with current cloud technologies so that controls can be composed as part of the workflow just like any other element of the design.

3. **Scalability** – The ability to scale to address the largest of environments is a fundamental requirement. Performance considerations for 100,000 workloads, 1,000s of nodes and many gigabits of throughput (10Gb+) are essential.

4. **Actionable** – Controls need to deliver a range of capabilities to identify traffic based upon user, network and application, and then deliver capabilities to permit, deny, quarantine and divert traffic.
Key technologies
The key technologies that comprise this Reference Configuration include the HPE Hyper Converged 380 (with VMware vSphere 6.0 pre-installed) and vArmour DSS 3.0.

HPE Hyper Converged 380 system

For customers who are looking for a configurable, scalable, agile and highly-available hyperconverged virtualization system, the HPE Hyper Converged 380 delivers a simple solution stack with extended flexibility and manageability. It builds on the powerful, industry-standard HPE ProLiant DL380 Gen9 server platform and is combined with VMware vSphere. Using the HPE OneView User Experience to add full lifecycle management, hardware provisioning and updates in a single pane of glass provides a unified, global experience. The HPE Hyper Converged 380 delivers a turn-key virtualization solution for medium-sized businesses, enterprises, and IaaS providers.

Designed from the ground up for the software-defined data center, the HPE Hyper Converged 380 enables a standardized approach to virtual server deployment, available in three workload configurations: General Virtualization, CloudSystem, and a Virtual Desktop Infrastructure (VDI). VDI is offered as a Reference Architecture. Unlike many hyperconverged systems, the HPE Hyper Converged 380 can be customized at the time of order and will be ready for virtualized workloads in a few simple clicks.

The HPE Hyper Converged 380 Management User Interface (UI) is designed to allow deployment and management of virtual machines (VMs). The HPE Management UI also features detailed graphical resource monitoring, alert reporting, and task status and history.

The HPE Hyper Converged 380 includes the Hyper Converged 380 Management User Interface (UI) offering the following features:

- **Virtual machines.** Using the HPE Hyper Converged 380 Management UI you can create VMs in just a few clicks. In addition to creating VMs, you can manage VM resource templates, VM images, and Open Virtualization Archive templates for quick deployment of VMs.

- **VM management.** The HPE Hyper Converged 380 Management UI allows you to easily manage VMs. Available functions include accessing the VM console, editing VMs, assigning users, taking VM snapshots, powering on/off, and restarting.

- **VM monitoring.** The HPE Hyper Converged 380 Management UI allows you to monitor HPE Hyper Converged 380 system resources and individual VMs. System monitoring functions include system alerts, system resources, and individual VM CPU, memory, and storage usage.

- **Solution lifecycle management.** The HPE Hyper Converged 380 Management UI provides solution lifecycle management by simplifying the upgrade process. The HPE Hyper Converged 380 Management UI and node Service Pack for ProLiant (SPP) updates are combined into one update file.

- **Advanced analytics with HPE Cloud Optimizer.** When connected, Cloud Optimizer provides additional functionality to detect and troubleshoot performance issues, optimize capacity, and predict future capacity requirements.

Details for HPE Hyper Converged 380
- Built on the industry-standard HPE ProLiant DL380 Gen9 server platform
- HPE OneView User Experience integrates virtual machine management and vending, live automated server firmware updates, and operations analytics
- Compact form factor – A 2-node hyperconverged computing system in a 4U form-factor with single 2U-node expansions and up to 16 total HPE Hyper Converged 380 nodes in a single cluster
Flexible pre-integrated use case choice points:

- HPE Hyper Converged 380 General Virtualization for development environments, Web/App servers and lightweight applications
- HPE Hyper Converged 380 with HPE CloudSystem
- HPE Hyper Converged 380 Virtual Desktop Infrastructure Persistent/non-persistent and graphics enabled

Configurable:

- Processor – Choice of Intel® Xeon® E5 processors
- Memory – 128GB to 1536GB
- Storage – 3.4TB to 40.2TB usable
- Graphics – Selection by workload
- Network – 10Gb, 1Gb
- Power – Redundancy
- Virtualization Software and Licensing

Software:

- VMware vSphere
- HPE CloudSystem 9
- HPE OneView User Experience

Easy to install, use and upgrade:

- Pre-integrated virtualization platform powered with VMware vSphere 6
- Data services from HPE StoreVirtual
- HPE OneView User Experience for full lifecycle management and monitoring
- VMware vCenter for day-to-day management

Hardware Availability features:

- Cluster expansion without downtime
- Hot-pluggable HDD and SSD (SSD in Hybrid Storage configurations only)
- Redundant power supplies
- Integrated storage controller with battery-backed cache
- HPE Integrated Lights-Out (iLO) 4 Remote Management

Services:

- HPE Insight Remote Support delivers 24x7 secure remote support
- Product is customer-installable and partner-serviceable
- 3-year HPE Hyper Converged 380 solution support included for best support experience

vArmour Distributed Security System

The vArmour DSS solution addresses data center and cloud security challenges by delivering the industry's first distributed security system that provides Layer 7 application-aware visibility and micro-segmentation capabilities, coupled with security analytics, and integrated deception functionality.

The vArmour DSS solution is built and delivered entirely in software to provide a true software-defined security model. vArmour DSS is architected to scale security across multi-clouds with deep insight and control of individual workloads. With its patented application-aware micro-segmentation capabilities, vArmour DSS moves security controls that were traditionally at the perimeter down next to each asset,
wrapping fine-grained protection around every workload, regardless of where it resides. As workloads move or migrate across the data center, vArmour’s security policy moves with the workloads, ensuring consistent application policy controls.

vArmour DSS is designed as a multi-tier network fabric with one common control and data plane. vArmour DSS leverages this network-centric approach to provide consistent segmentation, policy enforcement, and application visibility between all workloads. There are no modifications required to your existing network topology or data path for vArmour to operate.

Workload-level visibility and control of inbound, outbound, and lateral traffic patterns from vArmour DSS helps organizations detect and prevent application misuse, policy violations, and advanced persistent threats across complex multi-cloud environments from a single system. Furthermore, the workload visibility solves the primary use case that confronts customers moving to cloud: how to secure dynamic virtual assets that share the same infrastructure.

Whether you are regulated by PCI (Payment Card Industry), HIPAA, an IT Governance program, or a third party, a private cloud strategy offers a compelling approach to improve speed of business while reducing costs via consolidation. However, consolidation can be a challenge for regulatory compliance needs unless assets are logically separated. vArmour DSS with HPE Hyper Converged 380 delivers this use case enabling assets of different sensitivities (PCI and non-PCI) to share the same underlying infrastructure (hypervisor, network, storage, compute) without additional hardware or changes to the network. The combined solution provides capabilities to pool resources and assets while vArmour isolates assets in the cloud or virtual estate with Layer 7 application visibility and control throughout the system.

Solution diagrams

Reference Configuration: small deployment

The small-deployment configuration consists of four HPE Hyper Converged 380 nodes and the vArmour DSS secure data center solution, as shown in figure 2.

Figure 2. Four HPE Hyper Converged 380 nodes and the vArmour DSS secure data center solution
There are four main components to the vArmour DSS solution (see figure 2 above):

- **vArmour Directors**: The vArmour directors provide a highly available management and control plane for the DSS architecture. The directors are responsible for the overall “fabric” health of the system, as well as being the centralized security policy point. The directors also provide the API interface for the entire DSS fabric, which allows for programmatic and automated security operations.

- **Enforcement Point Interceptors – (EPI)**: The vArmour EPIs perform all of the Layer 2 to Layer 7 network, user, and application level visibility, inspection, and enforcement functionality. In addition, the EPIs provide session state information to the upstream Enforcement Point layer to support workload movement and recovery operations. There is no “punting” of network traffic to other vArmour entities, and as such, the EPI provides an extremely scalable security policy enforcement point.

- **Enforcement Points – (EP)**: The vArmour EPs are responsible to provide session backup and recovery to the EPI layer, as well as provide security policy relay functionality from the directors to the EPIs. The EPs are stateless in nature, but provide session state tracking required for the EPI layer during workload movement or migration.

- **vArmour Analytics Platform**: The vArmour Analytics Platform, also referred to as vAAP, is the aggregation point for all of the Layer 2 to Layer 7 security information that is seen or enforced by the EPI layer. It provides streamlined reporting mechanisms and security analytics based on the log information it receives.

The vArmour fabric is designed as a distributed software architecture built for enterprise scalability. A single instance of the vArmour fabric supports the following vArmour components:

- 32 EPIs per EP
- 16 EPs per vArmour Director

**Reference Configuration: medium deployment**
The medium-deployment configuration consists of eight HPE Hyper Converged 380 hosts and the vArmour DSS secure data center solution, as shown in figure 3.

![Figure 3. Eight HPE Hyper Converged 380 nodes and the vArmour DSS secure data center solution](image-url)
In figure 3 above, the hyperconverged infrastructure increased to eight HPE Hyper Converged 380 platforms. As the compute platform is deployed, a vArmour EPi is added to each host to segment and protect the new workloads. The process can be automated and simply occur as part of the compute workflow.

**Reference Configuration: large deployment**

The large-deployment configuration consists of sixteen (and more) HPE Hyper Converged 380 hosts and the vArmour DSS secure data center solution, as shown in figure 4.

In figure 4 above, the hyperconverged infrastructure is increased again, resulting in sixteen HPE Hyper Converged 380 platforms. As the amount of compute increases, it becomes even more important for vArmour to support the scale out and automation of security services for the data center workloads. Because the vArmour DSS is a scalable software platform the additional rollout and automation is easily accomplished as the data center requirements increase.
Design considerations and solution components

After the initial deployment of the HPE Hyper Converged 380 infrastructure, the baseline setup for the VMware virtual network needs to occur. Once the VMware virtual network is configured, the vArmour components can be installed and an administrator can almost immediately begin gaining visibility into workload traffic flows. This helps the administrator to discover flows of critical assets and other workloads in order to create protection policies and provide segmentation via vArmour DSS. Figure 5 depicts an overview of deploying the solution.

Figure 5. Deployment overview of HPE Hyper Converged 380 and vArmour DSS secure data center solution

Figure 6 below shows the VMware vSwitch view in vCenter after installing the HPE Hyper Converged 380 platforms and prior to any rollout of the vArmour components.

Figure 6. HPE Hyper Converged 380 deployment (pre-vArmour installation) – vSwitch view
The initial vArmour installation leverages the vArmour installer package and allows the administrator to connect directly to vCenter. To deploy the vArmour solution, follow these steps to reproduce a solution similar to figure 7 below:

1. Log into vCenter to start the vArmour installer.
2. Select the hypervisors to protect with vArmour DSS.
4. Review and deploy the vArmour DSS solution.

![Figure 7. HPE Hyper Converged 380 deployment (post-vArmour installation) – VM view](image-url)
After the vArmour DSS solution is deployed, there are several new vArmour virtual machines created. These provide visibility and enforcement for the customer workloads, in this case the “Test” and “Test1” virtual machines in figure 8 below. Two vArmour Director VMs have been deployed to provide a highly available and redundant control and management plane for the vArmour DSS Fabric. Two vArmour Enforcement Points (EPs) have also been deployed to provide a mechanism for recovery of session states for any VM workload migration activities. A vArmour EPi is deployed on each ESXi hypervisor that provides all Layer 2 to Layer 7 traffic visibility, inspection, and enforcement functionality.

Figure 8. HPE Hyper Converged 380 deployment (post-vArmour installation) – vSwitch view
After the vArmour DSS components are deployed, the vArmour EPI entity is configured to connect into the existing vSwitch (either vSphere Standard Switch (vSS) or vSphere Distributed Switch (vDS)), as a Trunked / Promiscuous port, to enable it to listen and report on all VM workload application communications. This network connectivity is shown in Figure 9 below.

**HPE Hyper Converged 380 and vArmour 3.0 - Networking Overview - vA Tap Mode (2nd vSS with two additional 10 GbE NICs)**

![Diagram showing network connectivity with vSphere Standard Switch](image)

Figure 9. Single node / hypervisor network connectivity (with vSphere Standard Switch)

This non-disruptive transparent network insertion model allows the vArmour DSS solution to profile and build out a respective security policy based on historical application and network traffic. The vArmour DSS solution can transition from Visibility (TAP) mode to Enforcement (INLINE) mode in a completely automated fashion, with a high degree of success, since the enforced security policy will be constructed from real application traffic flows.

The vArmour DSS solution is tightly integrated with vCenter and vSphere, and will also insert Distributed Resource Scheduler (DRS) rules to ensure the following:

- Directors run on separate ESXi hosts (Anti-Affinity)
- EPs run on separate ESXi hosts (Anti-Affinity)
- EPIs are bound to a specific ESXi host (Affinity)
After the installation, vArmour DSS is successfully monitoring all application and network traffic between workloads. This visibility mode can be seen in the vArmour Director as TAP mode as displayed in Figure 10.

Figure 10. vArmour Director TAP mode

TAP mode provides the baseline for the next step which is workload application-based micro-segmentation and policy enforcement. This is an automated process and can be completed in three easy steps:

1. Select the network segments where you wish to enable micro-segmentation.
2. Select the hypervisor where you wish to enable micro-segmentation.

Summary

Data center technologies have advanced to provide better resource utilization, application availability, and automation. As the data center transformation has occurred, many of the security technologies to protect these critical data center assets have not advanced to match the core data center fabric capabilities. Many of today's data center security offerings are simply a rebooted instance of current perimeter-based systems. These are not able to match the dynamic capabilities, and in many cases force rigidity and manual engagement back into the process.

Hewlett Packard Enterprise and vArmour have partnered to bring to market an industry-leading secure data center solution. By leveraging the HPE Hyper Converged 380 with vArmour DSS, the solution provides application-based segmentation, network, user, and application (Layer 2-Layer 7) level visibility, and fine-grained policy enforcement for all workloads running on the HPE Hyper Converged 380 systems.

vArmour’s Distributed Security System has been purpose-built for today’s data center architectures. vArmour is built on a distributed software architecture creating a security fabric that provides scalability, elasticity, and automation for private and public cloud environments. The robust API provides an extensible way to add new offerings and integration with data center platforms.

The joint solution provides a scalable, automated, and secure solution for the hyperconverged infrastructure.
Resources and additional links

HPE Hyper Converged systems, hpe.com/info/hyperconverged
HPE Solutions, hpe.com/solutions
HPE Reference Architectures, hpe.com/info/ra
vArmour Distributed Security System Solutions, varmour.com/solutions
vArmour Distributed Security System Resources, varmour.com/resources

To help us improve our documents, please provide feedback at hpe.com/contact/feedback.