Imagine Virtually Anything™

Solution Brief

# NetApp, Cisco, and VMware Deliver End-to-End Secure Multi-Tenancy

## KEY FEATURES

**Three industry leaders, one architecture**
An architecture to support secure isolation and security for multi-tenant environments

**NetApp MultiStore**
Storage security and isolation for data and applications

**NetApp Data Motion**
Always-on data mobility

**Cisco Unified Computing System**
Integrated network, compute, and storage access

**Cisco Nexus Series Switches**
Data center–class switches that provide end-to-end, role-based fabric security with TrustSec

**Cisco SAFE**
Security reference architecture for building highly secure and reliable networks

**VMware vSphere**
A secure cloud operating environment

**VMware vShield Zones**
Secure, isolate, and segment virtual machines and vApps

## THE CHALLENGE

Today's IT infrastructure too often suffers from siloed server and storage resources—leading to low utilization, gross inefficiency, and an inability to respond quickly and flexibly to changing business needs.

The arrival of cloud computing—and the adoption of cloud infrastructure to deliver IT as a service in data centers of all types—promises to overcome these limitations and reduce future IT spending by as much as 47%.

However, lack of confidence that data and applications will be securely isolated has been a major impediment to adoption of cloud-based services:

- Large enterprises need to isolate HR records, finance, customer credit card details, and so on.
- Organizations must make sure of the separation of business unit applications and data.
- Outsourced development requires separate areas for each development activity.
- Healthcare organizations must make sure of patient record confidentiality.
- Universities need to partition examinations, enrollment details, and commercial research.
- Telcos and service providers must separate billing, CRM, payment systems, reseller portals, and application hosting environments.
- Financial organizations need to isolate client details and partition trading, wholesale, and retail banking.
- Governments must partition records for taxation, welfare, healthcare, education, defense, and so on.

How can you be certain that applications, data, and customers are securely isolated as you migrate critical applications to an infrastructure in which servers, networks, and storage are all shared resources?

## THE SOLUTION

**A secure, virtualized dynamic data center**
NetApp, Cisco, and VMware have partnered to create a unique service-oriented infrastructure (SOI) that includes all server, storage, and networking hardware and software to facilitate sharing, reuse, and dynamic resource allocation. Our SOI minimizes the risk of making the transition to a cloud infrastructure while delivering the advanced capabilities you need to succeed.

"T-Systems' Dynamic Services deliver secure and reliable cloud services to our customers. With NetApp systems, NetApp MultiStore, Cisco Nexus products, and VMware, our data centers are able to provide shared yet secure clouds of server, network, and storage resources."

**Klaus Rubik**
Head of Engineering and Systems Management, T-Systems

Key features include an efficient, always-on infrastructure with elastic scalability; integrated data protection; advanced automation; and the ability to transparently migrate both applications and data across the infrastructure. We have brought together years of combined experience to create a multi-tenant SOI in which separate applications or customers can share the same server, storage, and networking infrastructure with complete isolation so sensitive information is never compromised.

The individual technologies are—by themselves—the best the industry has to offer. Together, these technologies offer unique synergies that greatly simplify the deployment and management of IT infrastructure and applications with:

- Unmatched end-to-end security and isolation in virtualized environments
- Simplified, unified architecture
- Lower cost
- Greater business agility
- Less risk

## THREE INDUSTRY LEADERS, ONE SECURE ARCHITECTURE

The traditional approach to guaranteeing application isolation requires dedicated, isolated hardware. A cloud infrastructure demands strict isolation between different clients, business units, departments, security zones, and layers in three-tiered Web architectures—as well as the ability to separate production operations from QA, development, and so on. Secure multi-tenancy enables you to partition a shared infrastructure in whatever way makes sense for your business. Data and data access are securely isolated, and workload performance is maintained.

To create our SOI, NetApp, Cisco, and VMware took a holistic approach that allows data storage, network fabric, and virtual servers to be efficiently shared. In a multi-tenant environment, virtual machines (VMs) or groups of VMs are securely isolated from other VMs or groups of VMs using VMware® vShield Zones technology. Once securely isolated, VMs are connected to storage systems through a network that is segmented and secured using the Cisco® Nexus family of products. The storage vFiler™ units to which they connect are also securely isolated from other vFiler units using NetApp® MultiStore™ technology, which results in an end-to-end, secure isolated storage system.

As industry leaders in their respective fields, each partner contributes proven technology to make sure of end-to-end security. With our SOI, we have combined technologies that provide layers of isolation—in many cases proven through years of use—into a single architecture with secure isolation of digital assets and resources in flight and at rest.

Close collaboration and careful integration eliminate the complexity of traditional IT infrastructure in favor of standardized components and consistent management practices that lower acquisition and operating costs, reduce staff skill set requirements, shorten provisioning times, and increase resource utilization, all while providing greater security.

## NETAPP: SECURE CLOUD STORAGE

The typical approach to storage forces you to buy different storage systems to accommodate different needs. With the NetApp Unified Storage Architecture, all storage requirements are met by a single storage solution, so you apply the same hardware, software, people, and processes to meet all your storage needs and achieve a level of efficiency that simply is not possible with other vendors' solutions. Innovative software helps you meet specific objectives for automation, data protection, and security.

**Secure storage multi-tenancy**
NetApp pioneered the idea of secure storage multi-tenancy over seven years ago with the introduction of NetApp MultiStore technology, providing a level of security and isolation for virtualized storage comparable to physically isolated storage arrays. Over 20,000 MultiStore licenses have been sold.

MultiStore lets you create multiple, completely isolated logical partitions on a single cost-effective Ethernet-based storage system, so you can share storage without compromising privacy. The results are secure, shared cloud storage and increased storage utilization. Individual storage containers can be migrated independently and transparently between storage systems.

NetApp Data Motion is a perfect complement to VMware VMotion™ and VMware Storage VMotion. With NetApp Data Motion you can migrate entire VMware datastores between storage systems to balance load, expand storage capacity, or refresh technology without disruption.

## CISCO: SECURE, UNIFIED COMPUTING

Today, IT organizations assemble their data center environments from individual components. Their administrators spend significant amounts of time manually accomplishing basic integration tasks rather than focusing on more strategic, proactive initiatives.

Cisco's Unified Computing architecture is a next-generation data center platform that unites compute, network, storage access, and virtualization in a cohesive system designed to reduce total cost of ownership and increase business agility. The Cisco Unified Computing System® seamlessly integrates with Cisco's Nexus Series of data center–class switches.

**Cisco unified fabric**
A typical data center environment supports three or four parallel networks: one for data, one for storage, one for management network, and possibly one for server clustering. This increases management complexity and imposes significant costs for interfaces, cabling, rack space, upstream switches, power, and cooling.

Unified fabric consolidates these different types of traffic onto a single, general-purpose, high-performance, highly available 10-Gigabit Ethernet network that greatly simplifies network infrastructure and reduces costs. To do all this, a unified fabric must be intelligent enough to identify different types of traffic and handle them appropriately. Cisco's unified fabric delivers a higher level of performance while guaranteeing the isolation and security of both user and data traffic.

**Cisco Nexus 1000V virtual switches**
Cisco Nexus 1000V Series Switches are an intelligent software switch implementation for VMware vSphere™ environments. Operating inside the VMware ESX hypervisor, the Cisco Nexus 1000V Series supports Cisco VN-Link server virtualization technology for policy-based virtual machine connectivity and mobile VM security and network policy.

**Cisco Nexus 2000, 5000, and 7000 Series data center switches**
The innovative architecture of the Cisco Nexus Series Switches simplifies data center transformation with a standards-based, high-performance, unified Gigabit Ethernet and 10-Gigabit Ethernet fabric that connects servers, storage, and users, greatly simplifying network management while delivering advanced capabilities with end-to-end security for all network traffic. Cisco TrustSec provides role-based security for all network traffic. TrustSec makes your network fabric role aware through secure access control, a converged policy framework, and pervasive integrity and confidentiality.

**Cisco SAFE**
Cisco SAFE consists of design blueprints based on Cisco Validated Designs and proven security best practices that provide the design guidelines for building secure and

vmware
- vSphere
- vShield Zones
- vCenter

CISCO
- Cisco SAFE
- Nexus 1000V
- Nexus 2000/5000/7000
- UCS
- 10GbE

NetApp
- MultiStore
- NetApp Data Motion
- 10GbE NFS/iSCSI/FC

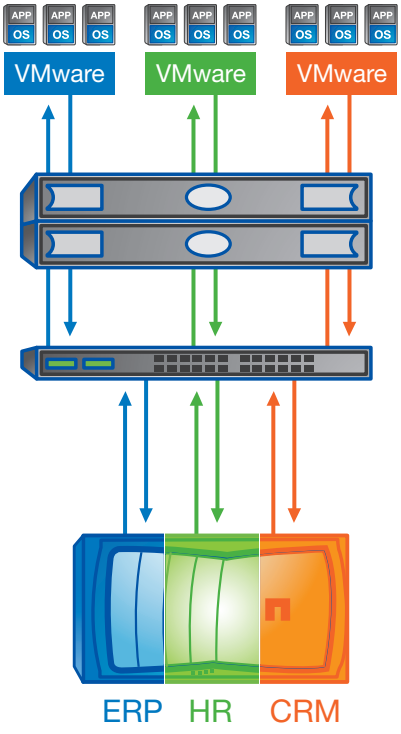


Figure 1) Design elements of the secure multi-tenant infrastructure.

reliable network infrastructures. Multiple layers of security controls are implemented throughout the network under a common strategy and administration. Cisco SAFE uses the Cisco Security Control Framework, a common framework that drives the selection of products and capabilities that maximize visibility and control, the two most fundamental aspects driving security. This framework facilitates the integration of Cisco's rich portfolio of security services designed to support the entire solution lifecycle.

## VMWARE: SECURE VIRTUALIZATION

Server virtualization is integral to the development of a cloud computing infrastructure. VMware continues to lead the way with value-added capabilities that foster new ways of doing business.

**VMware vSphere**
Bring the power of cloud computing to your IT infrastructure with VMware vSphere, the next evolutionary step in IT computing and the most trusted virtualization platform available. Built on a proven virtualization platform, vSphere provides a foundation for both internal and external clouds, using federation and standards to bridge cloud infrastructures and create a secure private cloud.

**VMware vNetwork Distributed Switch**
The VMware vNetwork Distributed Switch maintains the network runtime state for VMs as they move across multiple hosts, enabling inline monitoring and centralized firewall services. It provides a framework for monitoring and maintaining the security of virtual machines as they move from physical server to physical server and enables the use of third-party virtual switches such as the Cisco Nexus 1000V to extend familiar physical network features and controls to virtual networks.

**VMware vShield Zones**
VMware vShield Zones is a centrally managed, stateful distributed virtual firewall bundled with vSphere that takes advantage of ESX host proximity and virtual network visibility to create security zones. VMware vShield Zones integrates with VMware vCenter™ and leverages virtual inventory information such as vNICs, portgoups, clusters, and zones to simplify firewall rule management and trust zone provisioning.

## PROVEN PARTNERSHIPS

This SOI is not the result of new or untested relationships. NetApp, Cisco, and VMware have worked closely with each other for years, forging proven relationships that result in superior technology and the ability to provide coordinated support without needless finger pointing.

To facilitate delivery of the service-oriented infrastructure, we have qualified a team of system integrators to help you directly assess your needs and plan and implement all elements of the infrastructure, custom-tailored for your business. Depending on your preferences, you can make a complete transformation or evolve your existing infrastructure step by step.

## GETTING STARTED

To learn more about our secure multi-tenancy solution, read the Secure Cloud Architecture Overview or contact your local NetApp, Cisco, or VMware representative.

For more information visit
www.imaginevirtuallyanything.com.