

Challenges

The essential foundation for delivering information technology as a service (ITaaS) is a common pool of shared resources (compute, network, and storage) that can be dynamically applied to applications as needed. However, a shared common infrastructure introduces new problems since formerly separate applications and business processes now use the same hardware, and managing them and keeping them secure, private, and confidential becomes increasingly difficult.

Secure Multi-Tenancy Architecture

Secure Multi-Tenancy (SMT) architecture is a blueprint for a dynamic multi-tenant data center environment from Cisco, NetApp, and VMware for enterprises and service providers. It expedites the building of shared ITaaS offerings, reducing costs and increasing IT agility, while providing flexibility, efficiency, and security needed in a dynamic shared infrastructure. With additional features such as industry security audits, certified Microsoft workloads (Microsoft Exchange, SQL, and SharePoint), on-demand workload mobility, a simplified management framework with third-party APIs, and advanced security capabilities, enterprises and service providers can pool virtual data center resources (compute, network, and storage), reduce the number of silos, and securely create ITaaS offerings.

Business Benefits of Deploying SMT Architecture

- **Business agility:** Virtualization at all levels—computing, unified fabric, and storage
- **Data center efficiency:** 50 percent savings in operating expenses (OpEx) and capital expenditures (CapEx) through unified fabric, consolidation of assets, and reduced power and cooling
- **Security, isolation, and control:** End-to-end application and data security—from the virtual machine to the fabric to storage
- **Ease of operational management:** Complementary architectures that deliver efficiency with simplicity and tight integration with the virtual machine level
- **Cohesive delivery and support:** Shared partner network and support alliances to help ensure successful implementation and reduce risk

SMT Architecture Markets

SMT architecture will benefit enterprises and service providers that need to create a shared pool of resources for end-to-end secure isolation of application and data from one group to another group: for example, health-care, government, defense, university, service provider, and telco markets and large enterprises with multiple business units.

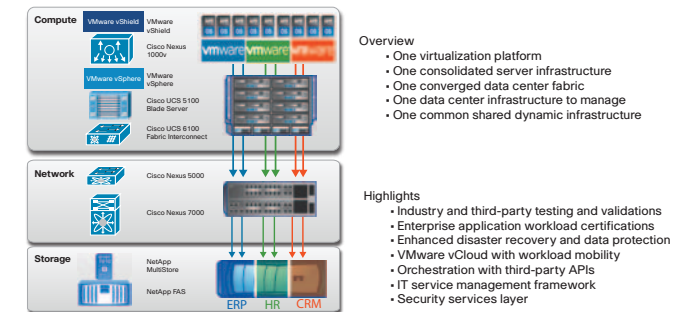
SMT Architecture Enhancements

The enhanced SMT architecture (Figure 1) includes Cisco®, NetApp, and VMware products with the following additions:

- **Industry and third-party testing and industry validations:** These independent reports validate the security of the overall SMT architecture. They include Payment Card Industry Data Security Standard (PCI-DSS) self-assessment and third-party security audit of architecture (ICSA).
- **Enterprise application workload certifications:** These certifications demonstrate the performance of each isolated application workload in a shared environment. These workloads include Microsoft Exchange, SQL, and SharePoint and Virtual Desktop Infrastructure.
- **Enhanced disaster recovery and data protection:** Improved disaster recovery and data protection plans are applied to application workloads running in a secure, shared environment.
- **Support for VMware vCloud:** This solution provides self-service provisioning for development and test environments. With SMT, organizations can build a foundation that fully supports the VMware vCloud environment.
- **Orchestration and IT service management framework:** This framework facilitates third-party service management of the SMT architecture, using storage, compute, and network APIs, allowing enterprises to create a single-pane view for end-to-end management.
- **Application services:** The availability, visibility, and security capabilities of the SMT architecture are enhanced through the use of virtual services such as VMware vShield, Cisco Nexus® 1000V Network

Analysis Module (NAM) Virtual Service Blades, Cisco Application Control Engine (ACE), Cisco Intrusion Prevention System (IPS), and Cisco firewall technologies. These together create a flexible and feature-rich environment that addresses tenant specific requirements.

Figure 1 Enhanced Secure Multi-Tenancy Architecture



Cisco, NetApp, and VMware: Building a Virtualized Dynamic Data Center

A virtualized dynamic data center represents one of the most effective foundations for secure cloud computing and the realization of ITaaS. Together, Cisco, NetApp, and VMware provide the primary solution components for this foundation.

Deploy and Operate with Confidence

Cisco, NetApp, and VMware solutions have been jointly tested and proven so you can deploy them quickly with confidence. Our SMT solution, for example, is a Cisco Validated Design. The entire solution has been lab tested and qualified to enable rapid deployment and optimal capabilities and is fully backed by cooperative support from Cisco, NetApp, and VMware.

For More Information

Visit <http://www.imaginevirtuallyanything.com>.