



End-to-End Visibility: State Government Virtualization's Secret Sauce

Renault Ross CISSP,MCSE,VCP5,CHSS

United States Security & Privacy Architect
Symantec Strategic SLED Programs

Agenda

1

Managing the Virtual Environment

2

Securing the Virtual Environment

3

Compliance & Event Monitoring

4

Automation with Virtual Environment

5

Virtual Desktop Initiative & Application Virtualization

6

Backup & Availability of Virtual Environments



Virtualization is a technology, not a strategy

Virtualization Strategy

- Vision and Mission

- Vision: *People should be able to work and play freely in a connected world*
- Mission: *We enable customers to have confidence in their connected experiences - infrastructure, information, and interactions*

- Virtualization 101

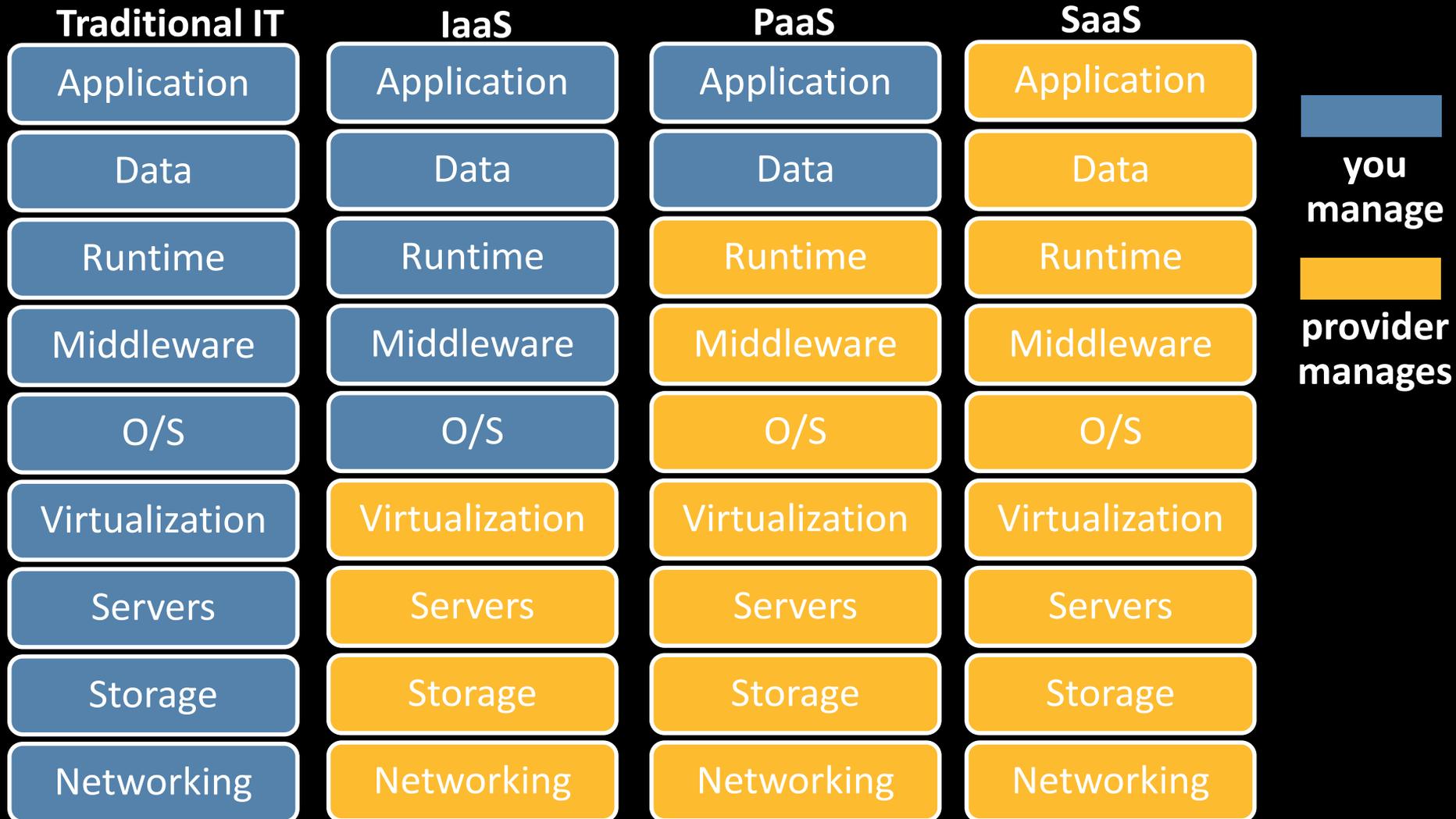
- Virtualization is the abstraction and simulation of resources

- Platform Virtualization/Virtual Machines (VMs) are software simulations of physical machines, an innovation that allows *more than one running OS per physical machine*

- How will virtualization change computing paradigms?

- What new opportunities emerge from that change?
- How must our existing approaches change?
- Will our existing markets and approaches be relevant or continue to exist?

Interfacing with the Cloud



Managing your Virtual Environments

Server Virtualization Requirements

Users need:

1. Full IT lifecycle management of VMs
2. One console for managing physical and virtual

Requires company-wide coordination. EPM is one of several players.

Simplify Virtualization Management

- Manage virtualized servers with the IT management tools I already know and the infrastructure I've got in place
- Common capabilities for Discovery, Inventory, Provisioning, Software and Patch Management, and Monitor for Physical and Virtual environments

Maximize Virtualization Benefits

- Manage virtualization layer from traditional IT Operations mgt tools
- Integrate with high-end virtualization management capabilities
- Transform traditional IT mgt tools to get full advantage of virtualization

Help Me Get To The Cloud

- Help Build Private Clouds – secure and manage VMware private clouds
- Connect to Public/Hosted Clouds – provide new on-premise to cloud solutions, deliver MSP friendly solutions
- Leverage Public Clouds – offer Risk and Compliance management for cloud

It all starts with a managed environment

“A Well managed virtual environment, is a more Secure Server”

- Inventory & Baseline solution will detect new VM's that have been created and baseline them.
- Once Detected vendor solutions can ensure that the VM has the appropriate configuration applied to it.
- Monitoring of the Virtual and Physical.
- Remote Diagnostics of VM's and the physical environment it resides on.

Systems Management Platform

Traditional Vendor Management Platform Components

Client Management

- Deployment & Migration
- Inventory & Application Metering
- Software Packaging & Delivery
 - **Software Virtualization**
- Remote Control & Diagnostics

Server Management

- System Provisioning
- Inventory & Baselining
- Hardware & System Monitoring
 - **Virtualization Management**
- Remote Diagnostics

Service & Asset Management

- Incident & Problem Management
 - Asset Management
 - License Compliance
 - CMDB

Add-On Solutions

Workflow Solution

Software Virtualization Pro

IT Analytics

Integration Components

AntiVirus

Backup

Data Loss

Management portal access

- Consolidated view of the virtualization infrastructure in the network
 - Display of Host-VM relationships with Host and VM views
 - 100% based on agent less communications

Host Server View

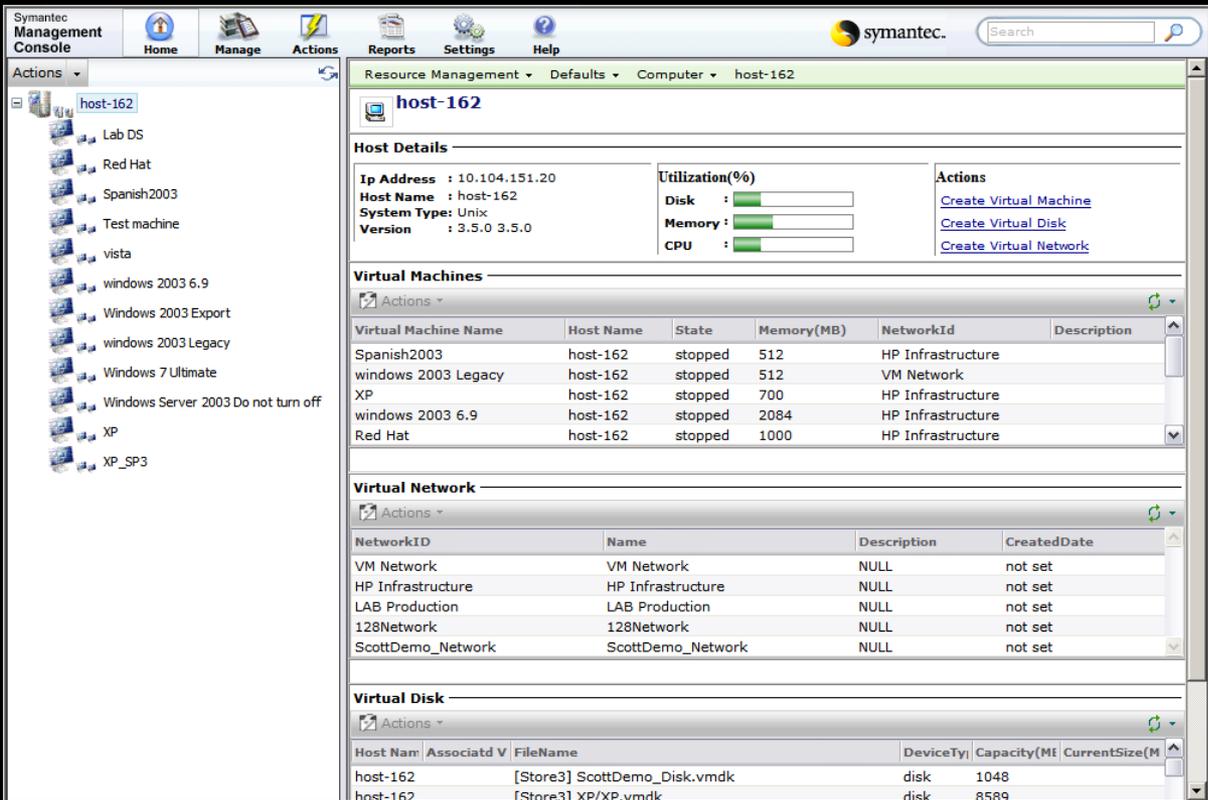
- Create VM, Disk, Network
- Get Host Inventory

Virtual Machine View

- VM Status Mgt
- Manage Snapshots

Create VM Wizard

VMM Tasks



Per Forrester

Virtualization management must be integrated. Virtualization issues are still lingering in the background of IT operations. This chapter must be closed quickly and integrated into current management tools as yet another layer of technology.

Securing the Virtual Environment

VMWare Environment

Challenges

- VMWare ESX Host is a RHEL kernel and increasingly subjected to vulnerabilities and attacks.
- A malware can potentially use the host as launching pad for attacks to the guest OS.



Industry capabilities that address

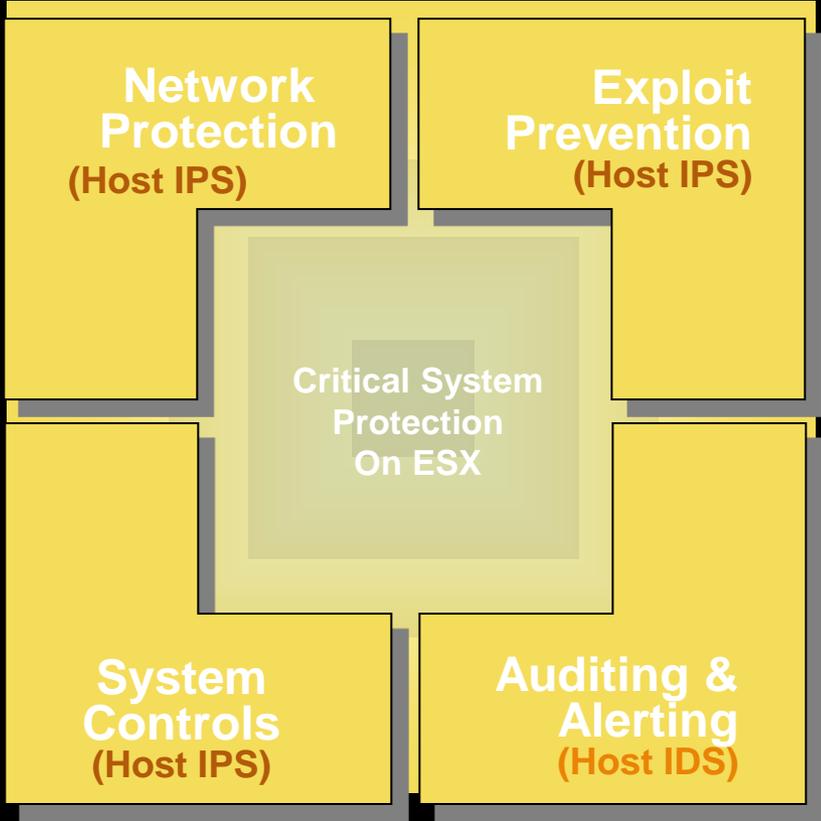
- Provides Host IDS to monitor user, system and resource activities and report on real-time intrusions
- Protects ESX host with its IPS policies to provide firewall protection, device control, configuration and system lock down, admin access control and file system protection
- Provides protection so you can comfortably put PCI Server in virtualization

Critical System Protection

“Hardens the guest OS”

- Close back doors (block ports)
- Limit network connectivity by application
- Restrict traffic flow inbound and outbound

- Lock down configuration & settings
 - Enforce security policy
 - De-escalate user privileges
- Prevent removable media use

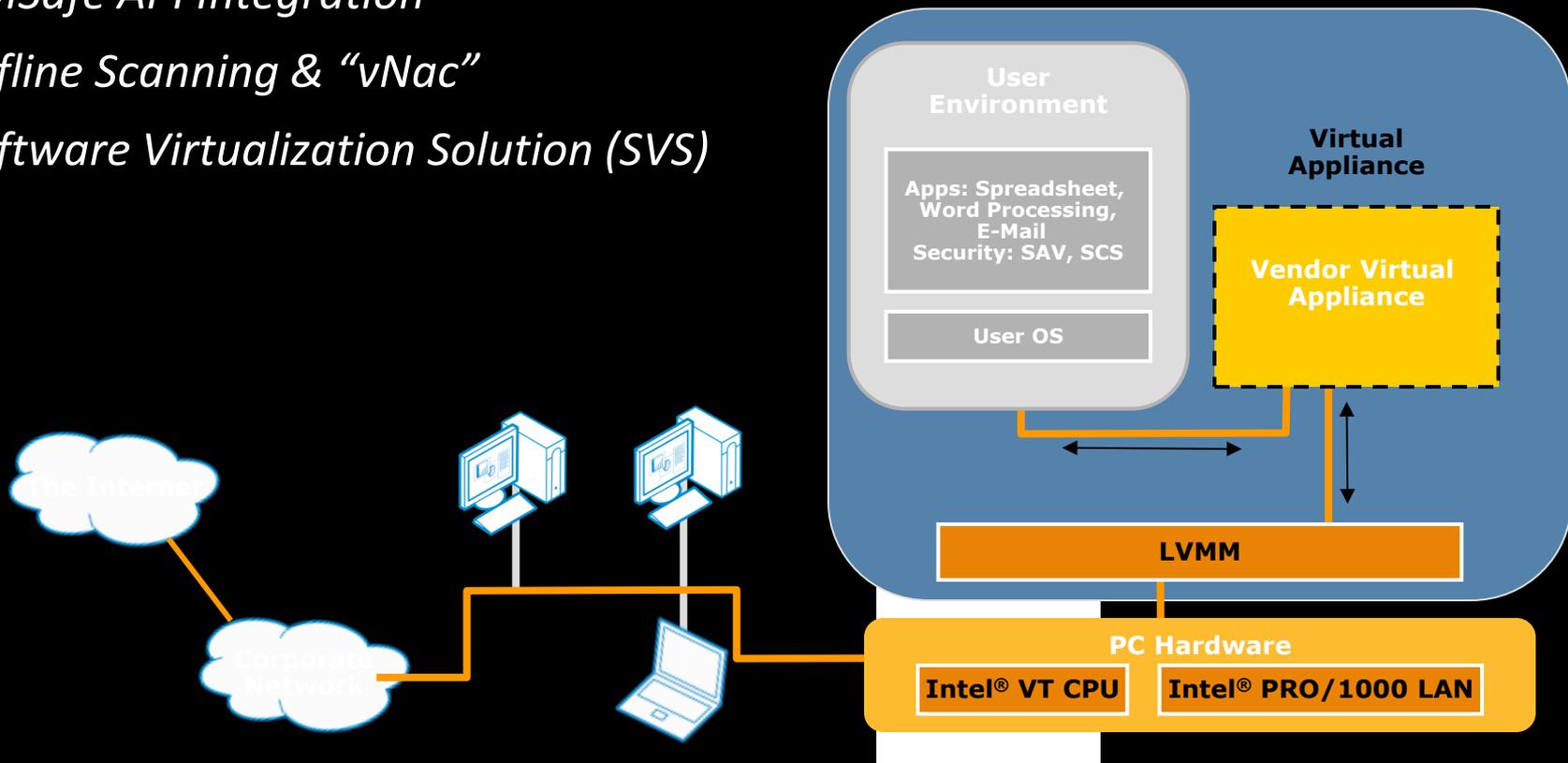


- Restrict apps & O/S behaviors
- Protect systems from buffer overflow
- Intrusion prevention for day-zero attacks
- Application control

- Monitor logs and security events
- Consolidate & forward logs for archives and reporting
- Smart event response for quick action

Malware Protection of guest

- *Virtual Security Solution (VSS)*
- *VMSafe API Integration*
- *Offline Scanning & “vNac”*
- *Software Virtualization Solution (SVS)*



Endpoint Protection Best Practices

- Randomized Scans to reduce concurrent requests for the same physical disks.
 - Definition Updates
 - Changes have been made in each MR since MR3 to improve disk I/O -
 - 81% reduction in reads
 - 37% reduction in writes
 - Use Randomization Feature
 - Scheduled Scans
 - Randomization and scan window
 - IDLE scan and Scan Less
- Randomized Definition updates to reduce memory utilization.
- Developing for later release, AV Whitelisting to reduce consumption on Host and Guest VM's.
- **Network Access Control**- Host Integrity Feature ensuring VM's are compliant and auto fix themselves or quarantine if they fail compliance.

Protect what's Important

Customer Information



Credit Card Info



Medical Records



SSNs and
Government IDs



Financials

Company Information



Intellectual Property



M&A and Strategy



Internal Auditing



Integrate At Both System And Management Levels



Integrate virtual
systems into
security programs



Integrate
virtualization
security data into
overall view of risk

Compliance of virtualized environment spans across

Configuration Hardening

Hypervisor settings

Server instance settings

Access Rights Management

Implement least privileged access

Prevent access escalation

Separation of Instances on a Shared Host

Threats jumping across instances

Compliance and legal issues as workloads move across zones

Limited Logging and Reporting

Logging for failed actions

Activity logging is not attributable

Rolls up to an Executive dashboard

Dashboards: Symantec Control Compliance Suite 11.0 - Windows Internet Explorer

http://mk-ccs-app/CCS_Web/DynamicDashboard/ViewDashboard.aspx?GUID=31e3430a-18d1-... Dashboards: Symantec Cont... x

Logged in as: [S. CCS Application Stack] | Home | Preferences | About | Help

Symantec Control Compliance Suite

Dashboards | Questionnaires | Policy | Risk Management | Downloads | Settings

Dashboards

Close

New Dashboard | New Panel | Edit | Copy | Delete | Import | Publish | Unpublish | Email Dashboard

VSM Assets and Assessments

Dashboards | Panels

All

Search Dashboard

Misc

- Compliance Administration - Assets
- Compliance Administration SCAP Benchmark Profile
- Compliance Administration - Standards
- Compliance Analysis - HIPAA Mandate
- Compliance Analysis - ISO Mandate
- Compliance Analysis - Mandates
- Compliance Analysis - NERC Mandate
- Compliance Analysis - PCI Mandate
- Compliance Analysis - Policies
- Compliance Analysis - SOX Mandate
- IT Operations
- VSM Assets and Assessments**

ESX Compliance Posture

ESX Host Name	RunWarn	RunPass
mk-83...@mk-10a-syma-nisa.com	4	6
mk-83...@mk-10a-syma-nisa.com	8	11
mk-83...@mk-10a-syma-nisa.com	8	11
mk-83...@mk-10a-syma-nisa.com	4	6
mk-83...@mk-10a-syma-nisa.com	7	3

VSM Pass and Fail Assessment Counts by Template

Template	RunWarn	RunPass
Template 1	10	1
Template 2	6	11

Count of Virtual Machi...

Category	Percentage
Category 1	16.67%
Category 2	25.00%
Category 3	16.67%
Category 4	16.67%

VSM Pass and Fail Assessment Counts by Test

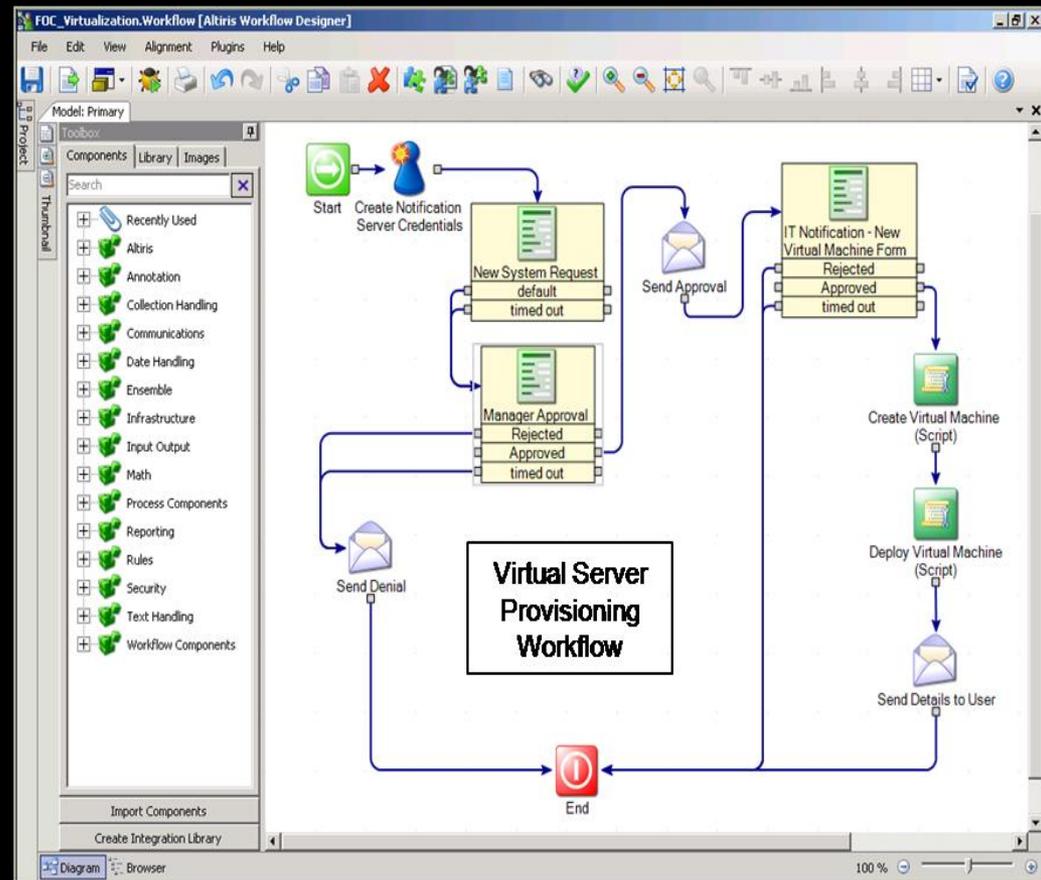
Test Description	RunWarn	RunPass
Snapshot all virtual machines	7	0
Set up log to a remote logging server	4	0
Prevent GuestOS processes from flooding ESXi host with informational messages.	4	0
Limit virtual machine log file size and number.	6	0
Ensure that the 'MAC Address Change', 'Forged Transmits', and 'Promiscuous Mode' p...	6	0
Ensure bidirectional CHAP authentication is enabled for iSCSI traffic. (Note: May take a...	6	0
Disable unnecessary or superfluous functions (hardware) inside virtual machines.	6	0
Disable copy and paste operations between GuestOS and Remote Console	6	0
Configure NTP time synchronization	4	0
Check trust status	5	0
Check root password vaulting	5	0
Check patch version	5	0
Check local accounts	5	0

Copyright © 2012 Symantec Corporation. All rights reserved. Symantec

Automation in Virtualization

Automating the Virtual processes

- Automate the Provisioning of VM's
- Decommission VM's via an Automated Process
- Leverage Workflow solutions to automate process kickoff from Security or non security events, IE System Lockdowns, Patching and more.



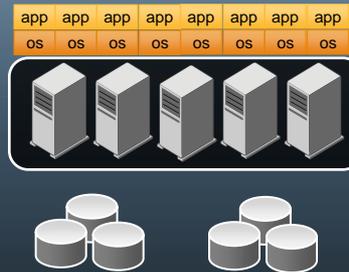
Workspace & Application Virtualization

Virtual Desktop Initiative and Application Virtualization

Givers User a portable Experience



Can Reduce Software cost



Can Improve App Management



How this aligns with industry capabilities



Virtual Distribution

Workspace Streaming

On-demand application delivery and license management system



Virtual Execution

Application Virtualization

Layering technology to contain applications and eliminate conflicts and OS degradation



Virtual Workspace

Thin Client Technology

Desktop connection broker with secure single sign-on and roaming desktop with location awareness



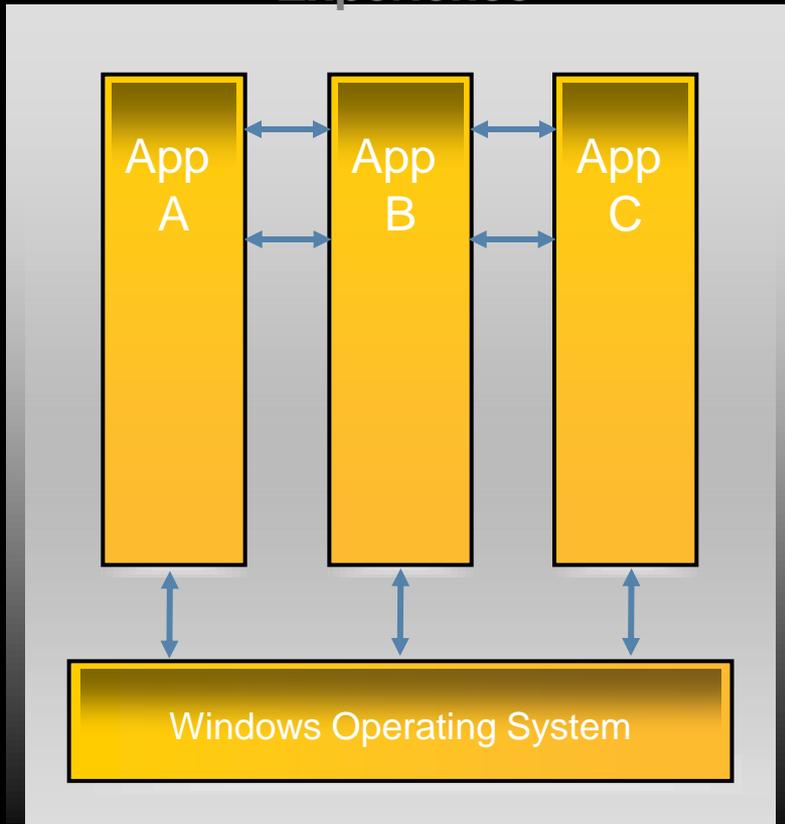
Virtual Profiles

User Profiles

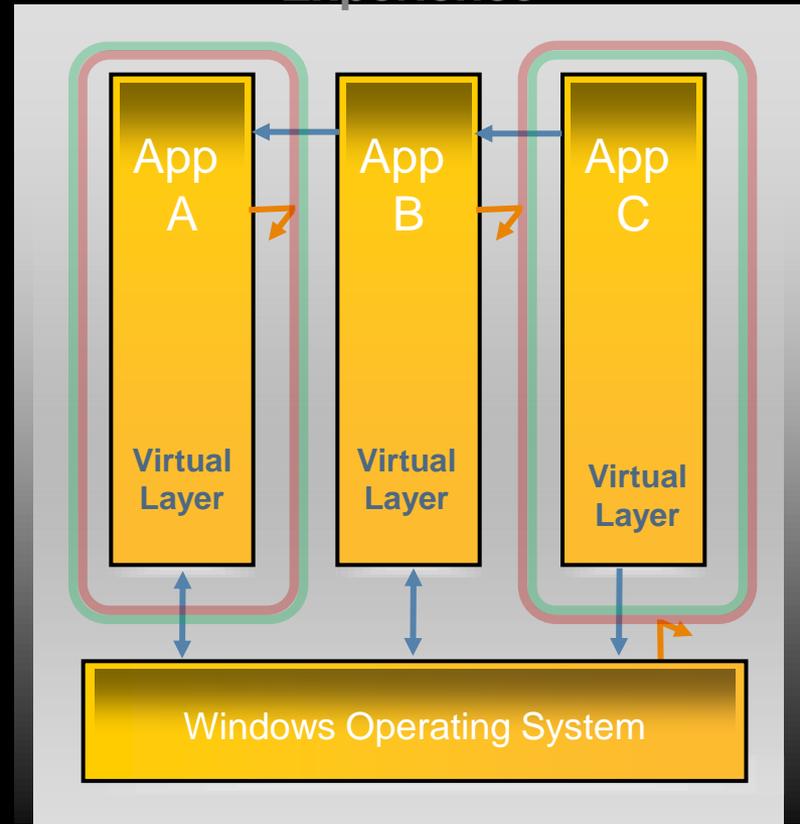
Personal workspace customization that follows the user across multiple devices

Virtual Applications

Traditional Apps Experience



Virtual Apps Experience



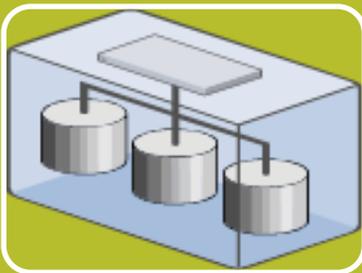
Backup & Availability of the Virtual Environment

Virtualization Poses Challenges for Backup & Recovery



Virtualization Slows Backup Processes

- Consumes server I/O & CPU
- Impact other applications
- Creates bandwidth problems



Virtualization Increases Storage Consumption

- Virtual machine “sprawl” requires backup & recovery
- Duplicate data stored across every virtual machine
- Disaster recovery = duplicate data (OS)



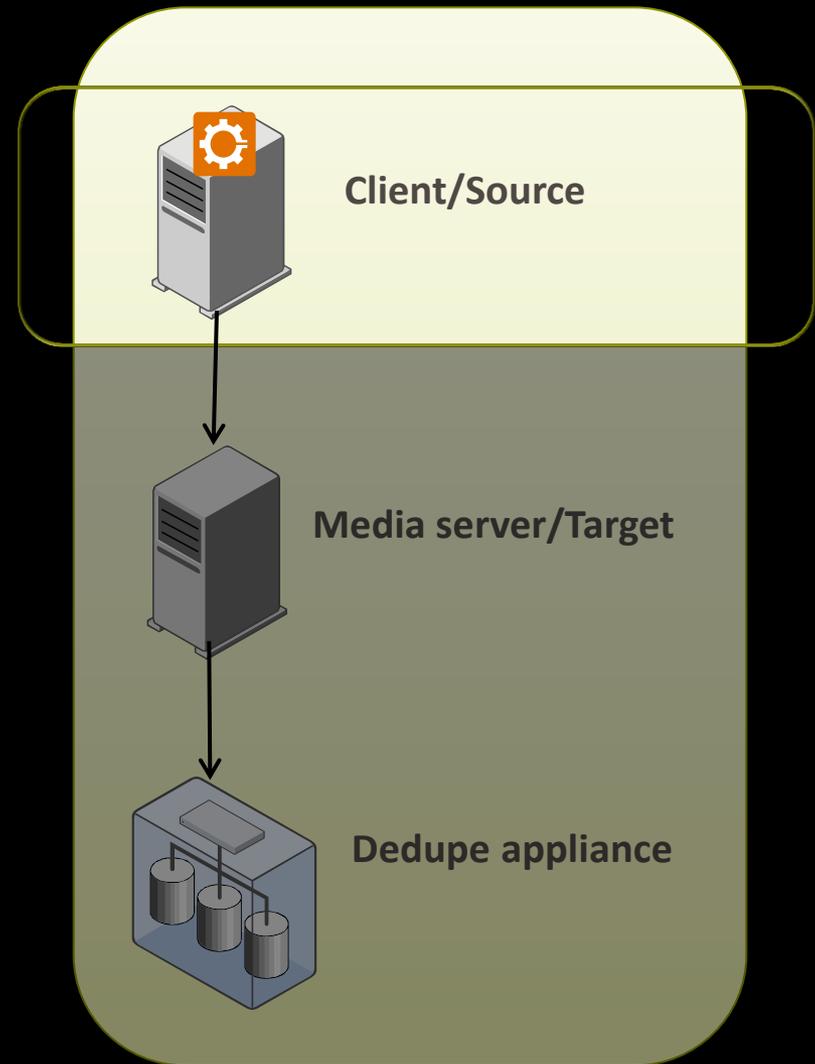
Virtualization Reduces Productivity of Backup Team

- Multiple tools for virtual and physical server recovery
- Finding individual files consumes time w/o a catalog
- Time to manage gap between protected machines and unprotected machines

Data Deduplication at the Source

- Data is deduplicated at the source/client **before** being sent across the network
- Benefits include:
 - Reduced WAN/LAN bandwidth impact
 - Reduced backend storage requirements
 - Transparent support for applications
- Ideal for:
 - Remote offices
 - Protecting virtual machines
 - File/folder & Database backups with low change rate

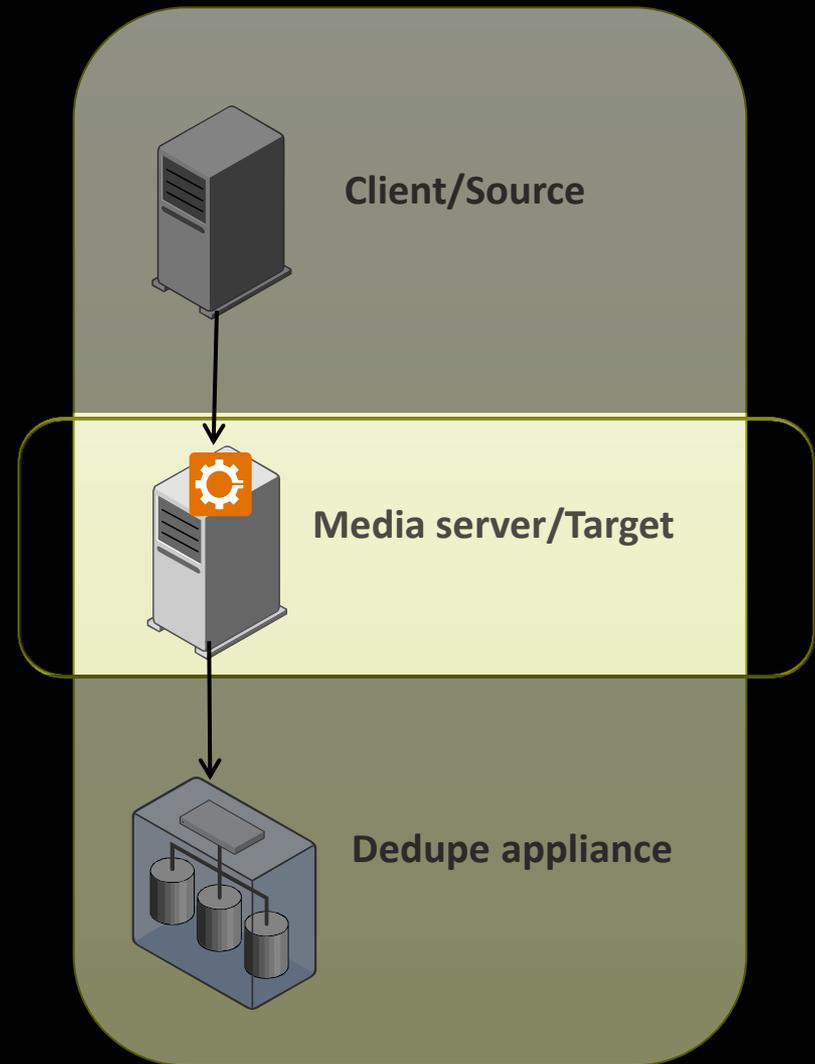
 = Deduplication engine



Server Deduplication

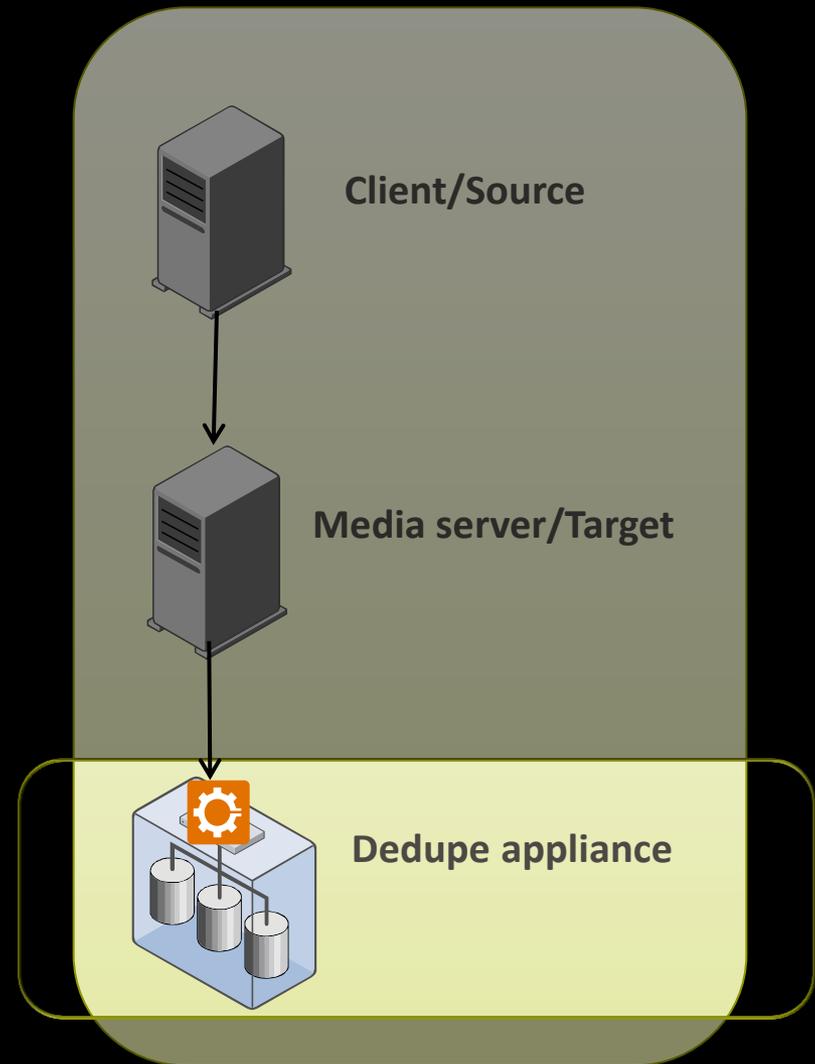
- Data is deduplicated **inline** at the media server **before** being stored on disk
- Benefits include:
 - No client impact
 - Leverage commodity hardware
 - Reduced backend storage requirements (1Gb/s vs. 10Gb/s)
 - Highly scalable
- Ideal for:
 - Data center environments

 = Deduplication engine

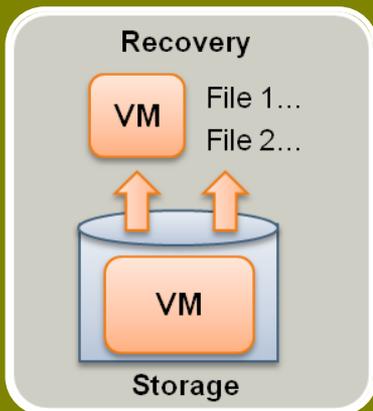


Deduplication Appliances

- Data is deduplicated at the appliance and centrally managed by NetBackup via OpenStorage API
- Benefits include:
 - Centralized policy management and replication control
 - Improved performance
- Wide range of supported appliances

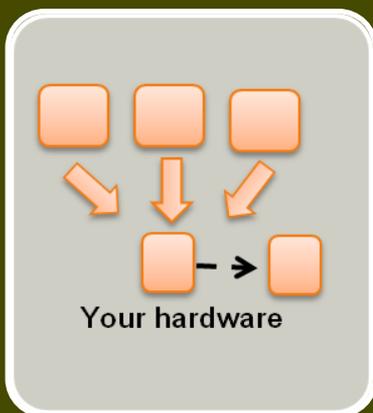


Reduce Storage



Gaining better insight of data

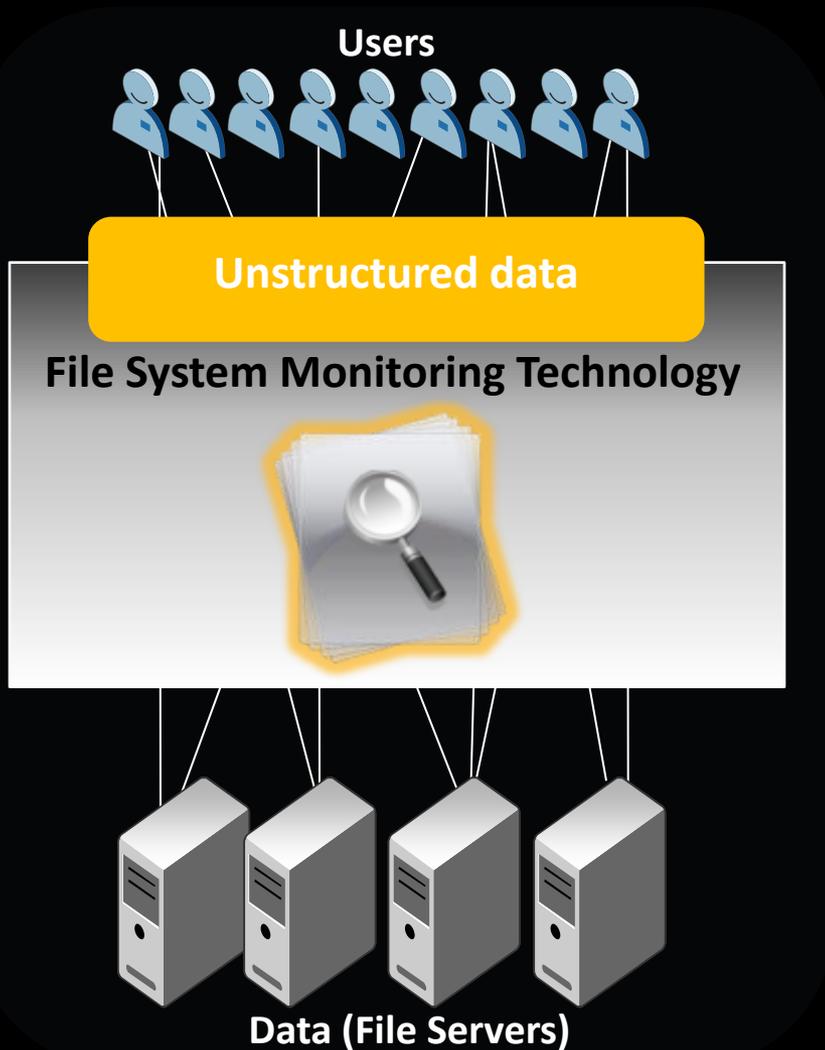
- Address unstructured data
- Effective consumptions/Chargeback
- Understand data utilization



Leverage Symantec Deduplication

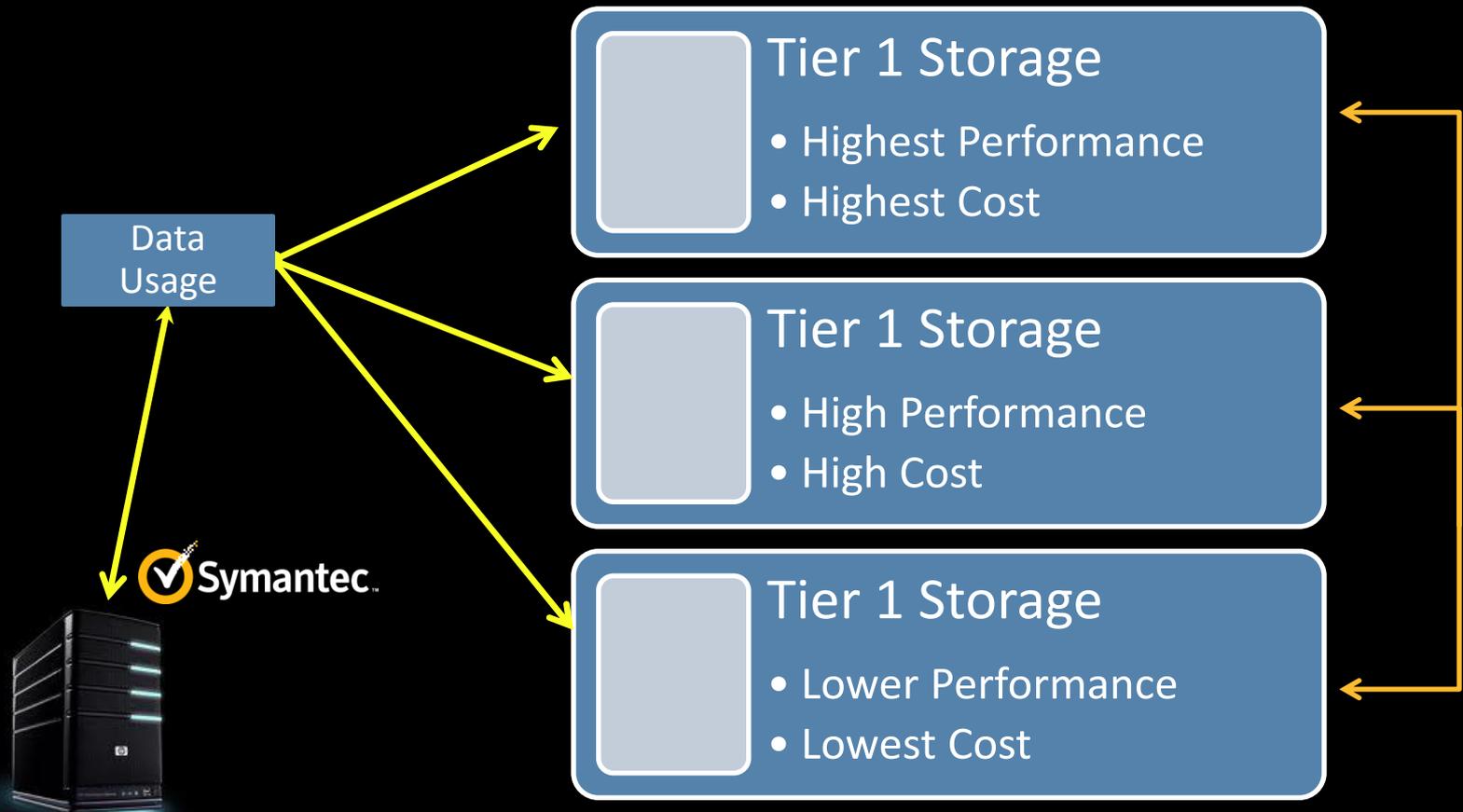
- 90% reduction in backup & DR storage
- You choose storage – we manage deduplication
- Source and/or target-based deduplication

Eliminate Unused Data



- Identify data *users*, not just data *owners*
- Identify inactive or orphaned data
- Understand storage consumption and trends
- Tie in to storage security

Use Tiered Storage Effectively



Automated real time data movement based on policy

Virtual Machine Backup Management

- **Centralize Administration**

- Automatic discovery of new VMs for VMware & Hyper-V
- Common policy management

- **Fast, Three Step Recovery**

- Centralized catalog – find the right file instantly
- Recover virtual to physical or to a new virtual

- **Monitor & Report on Exposure**

- Identify unprotected VMware or Hyper-V VMs
- Automatically generate daily reports
- Centralize reporting across different backup products / platforms (Backup Reporter)

Veritas NetBackup™ Operations Manager

Reporting > All Reports > Virtual Client Summary

Virtual Client Summary

Report Parameters

Context: /blitz2k (Change using the Context window)

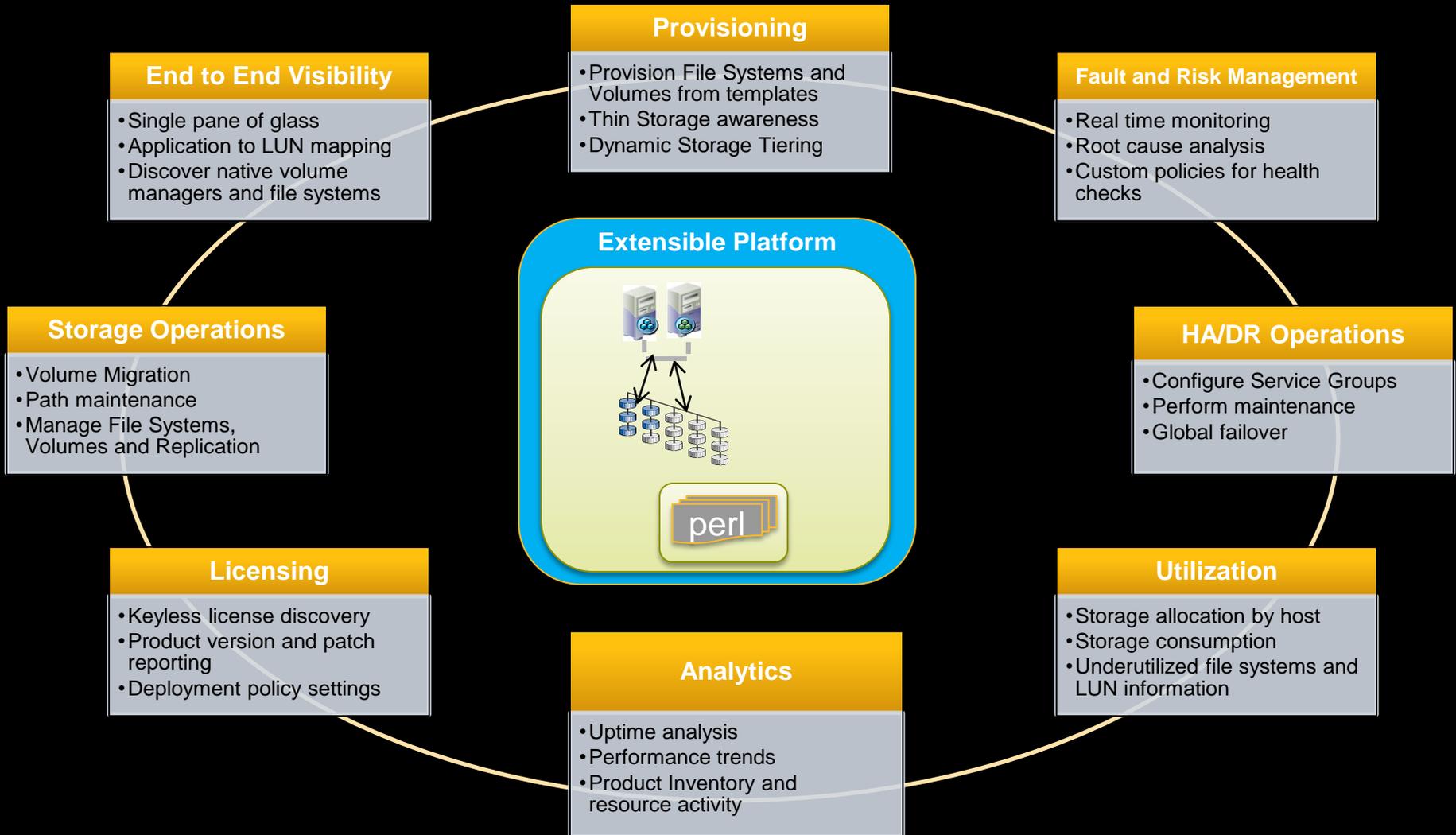
Report shows virtual machine details and shows if they are protected by NetBackup.

Virtual Server Name	Backup Proxy Name	Virtual Client Name	Uuid	IP Address	Type	Server Name	Exists in a policy	Last Backup Time
steep1e	orach	hava@steep1e	564d850-c6ee-7500-9559-11490448311	10.50.31.31	VMware		No	NA
steep1e	orach	hava@steep1e	564d1352-3b16-7255-bbab-743d411cb932	10.81.23.17	VMware		No	NA
steep1e	orach	192.168.1.27	5037a504-1421-6438-a673-43d6d698e05e	192.168.1.27	VMware		No	NA
steep1e	orach	192.168.1.27	503857e7-612d-53aa-c1ff-bdb6c459c763	192.168.1.27	VMware		No	NA
steep1e	orach	192.168.1.27	50397aed-1a2b-3e75-50e6-13267aee0da0	192.168.1.27	VMware		No	NA
steep1e	orach	192.168.1.27	564d3d03-ca02-0cfa-176e-d199a17d6ac3	192.168.1.27	VMware		No	NA
faq	orach	hava@faq	564de936-7ceb-5e9a-2211-b2ce296e4904	10.99.28.201	VMware		No	NA
faq	orach	hava@faq	564d4d85-d6c1-6983-c8e1-a52a83e5761a	10.99.28.201	VMware		No	NA
blitz2k	orach	hava@blitz2k	5037d161-135e-e58b-5ab3-c0e693cbe864	10.99.28.201	VMware	orach	Yes	Saturday, March 21, 2009 3:50:02 PM
blitz2k	orach	hava@blitz2k	564d488b-12e9-9d52-a0e6-398b72ee5e07	10.99.28.201	VMware	orach	Yes	Wednesday, April 29, 2009 1:32:07 AM
blitz2k	orach	hava@blitz2k	50398a55-610-b686-e755-0063983e1943	10.99.28.201	VMware	orach	Yes	Monday, April 20, 2009 10:59:40 PM
blitz2k	orach	hava@blitz2k	5037096e-8f02-0a2b-c0b3-b067277ade70	10.99.28.201	VMware	orach	Yes	Saturday, March 21, 2009 8:51:23 PM
blitz2k	orach	hava@blitz2k	501951c6-22ad-9baf-791a-f22be570390b	10.99.28.201	VMware	orach	Yes	Monday, April 20, 2009 3:15:53 AM
blitz2k	orach	hava@blitz2k	50388a1c-e10c-17bd-6804-be7472154119	10.99.28.201	VMware	orach	Yes	Wednesday, April 29, 2009 6:02:04 PM
hyperv	incredball	hava@hyperv	78a14e27-615d-48c1-9b04-04eD487f8159	10.99.28.201	Hyper-V	orach	Yes	Wednesday, April 22, 2009 6:52:22 PM
hyperv	incredball	hava@hyperv	213f3a98-9ae7-488f-afEE-7918AAE5FAE5	10.99.28.201	Hyper-V	orach	Yes	Monday, April 27, 2009 5:28:19 PM

Identify unprotected virtual machines (VMware & Hyper-V)

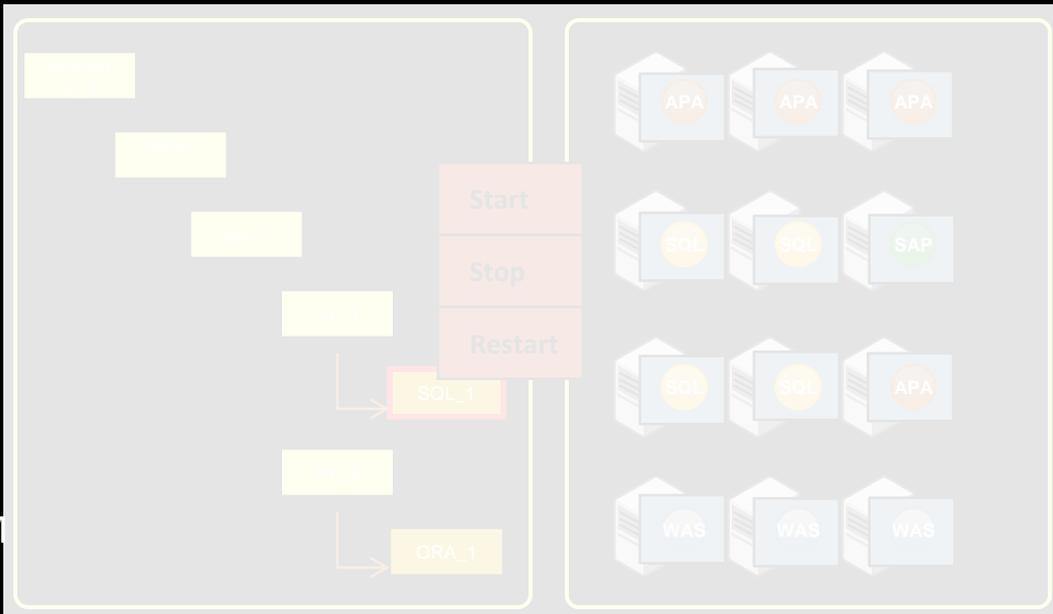
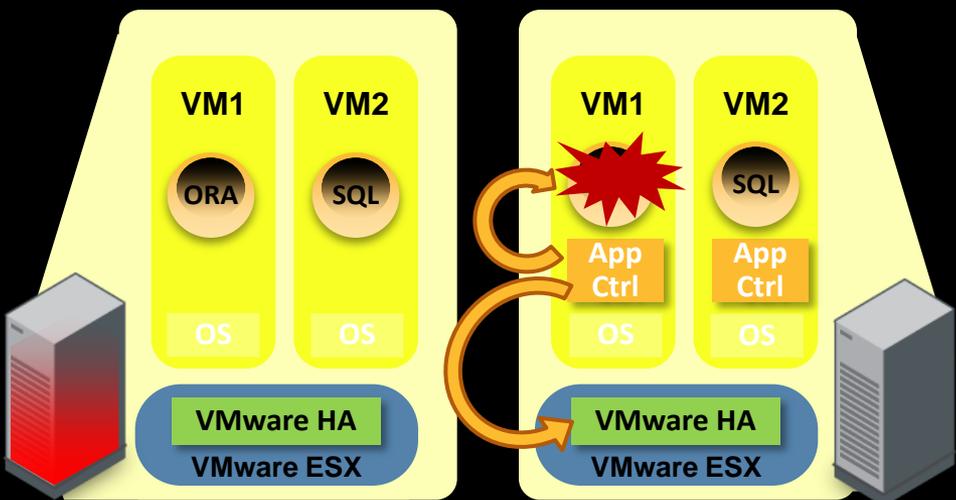
Storage Management and High Availability

Enterprise Operations Management Consoles



Leverage AppControl: Application-aware HA in VMware

- Integrated VMware-Symantec solution to improve app availability
- VMware HA + VCS for coordinated recovery of apps
 - Monitor apps, show health status, detect app failures
 - Restart apps. If needed, trigger VMware HA for VM restart
- vCenter + VCS plugin for visualization and control of apps
 - Visualize, Start, Stop apps in VMs
 - Customize app start/stop behavior
- Simple deployment
 - Push install to multiple VMs
 - Discover and auto-configure apps in VM



Automate High Availability and Disaster Recovery

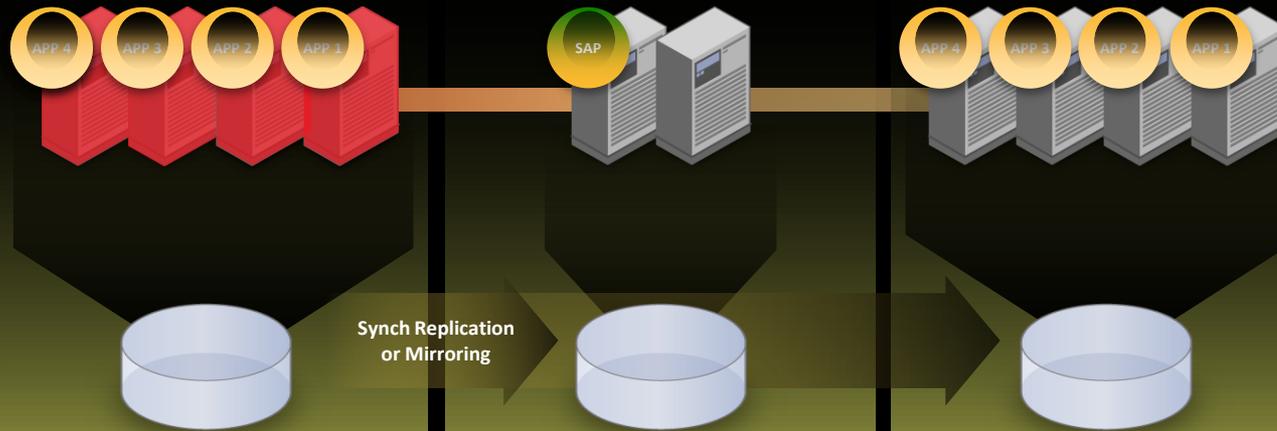
Symantec High Availability and Disaster Recovery

The Benefits

Local HA

Metropolitan HA (Stretch Cluster)

Wide-Area DR (Global Cluster)



- Recover faster
- Reduce reliance on personnel during an incident
- Reduce operator error
- Provide comprehensive data and application availability
- Simplify by using a single solution for:
 - Local HA
 - Campus/Metro DR
 - Global DR

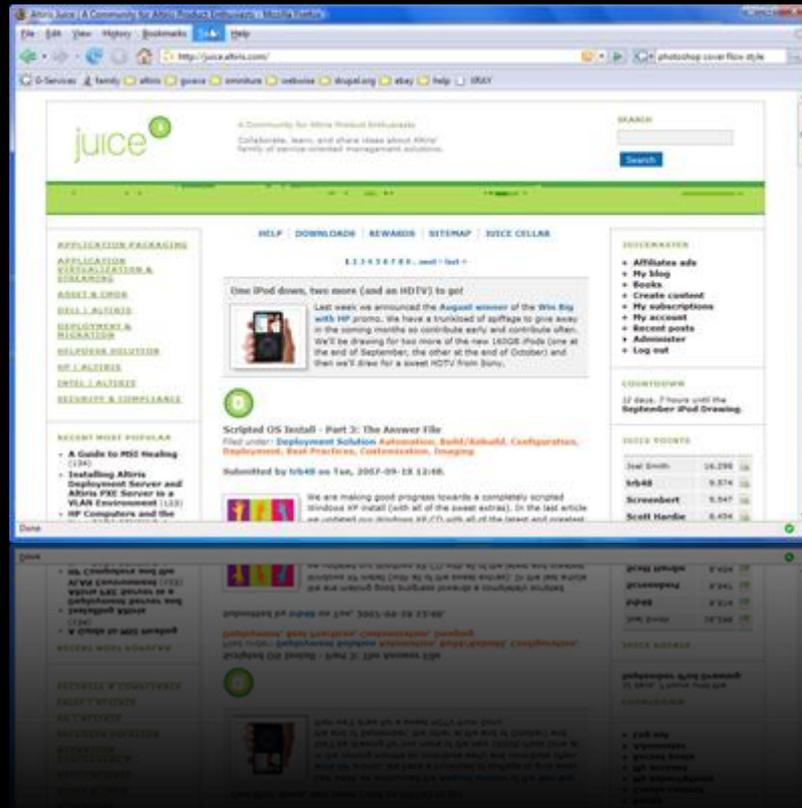


Summary

Summary End-to-End Visibility: State Government Virtualization's Secret Sauce

	Reduce Downtime	Manage Environment	Disaster Recovery	Optimize Storage	Data Protection
Systems Mtg. Strategy	✓	✓			✓
Security Strategy	✓				✓
Compliance Framework	✓	✓	✓	✓	✓
Automation Capabilities	✓	✓			
Data Protection Strategy	✓				✓
High Availability & Storage Mtg.	✓		✓	✓	

More information: Symantec Connect



- Breaking product news
 - In-depth articles
- Tips from the trenches
 - Tools and utilities
 - Training videos
 - Podcasts
 - RSS feeds
- Rewards program

www.symantec.com/community



Thank you!

Copyright © 2010 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.