



# Решения Symantec для защиты данных в виртуальных и облачных инфраструктурах

**Алексей Дудников**

Менеджер по развитию бизнеса ИБ

# Успешные модели использования облаков

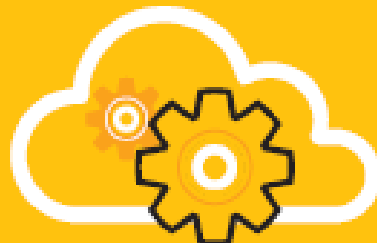
## Successful Cloud Adoption Models



**Consume  
Cloud Service**

**Transform Complexity  
to Simplicity**

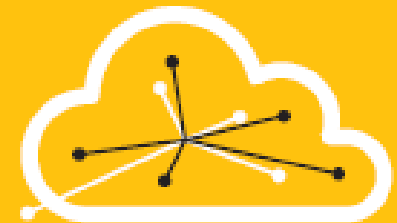
Companies consume products and solutions from the cloud



**Build  
Cloud Services**

**Deliver Highly Agile,  
Highly Reliable IT  
Services**

Solutions that enable the creation of secure and resilient public and private clouds



**Extend into  
Cloud Services**

**Establish Consistency  
Across Environments**

Solutions to enable customers to confidently leverage third-party cloud services

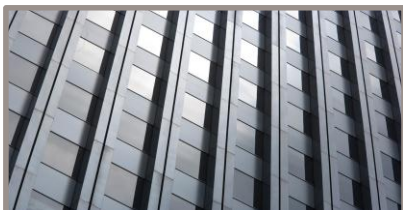
VALUE

DESCRIPTION

# Решения для построения облаков

- Вашей системе - ваши решения
- Безопасные и соответствующие виртуальной инфраструктуре
- Поддержка отказоустойчивости облаков
- Единая консоль для полноценного контроля

# Critical System Protection помогает решить ключевые задачи в виртуальной среде



## Reduce Cost

- Virtual Patching
- Single solution for HIPS/HIDS
- Single solution for vSphere 5.0 Protection



## Compliance

- Real-time File Integrity Monitoring
- Compensating HIDS/HIPS controls



## Breach Response

- Identify suspicious server activity
- Respond immediately with Targeted Prevention Policies (*New!*)



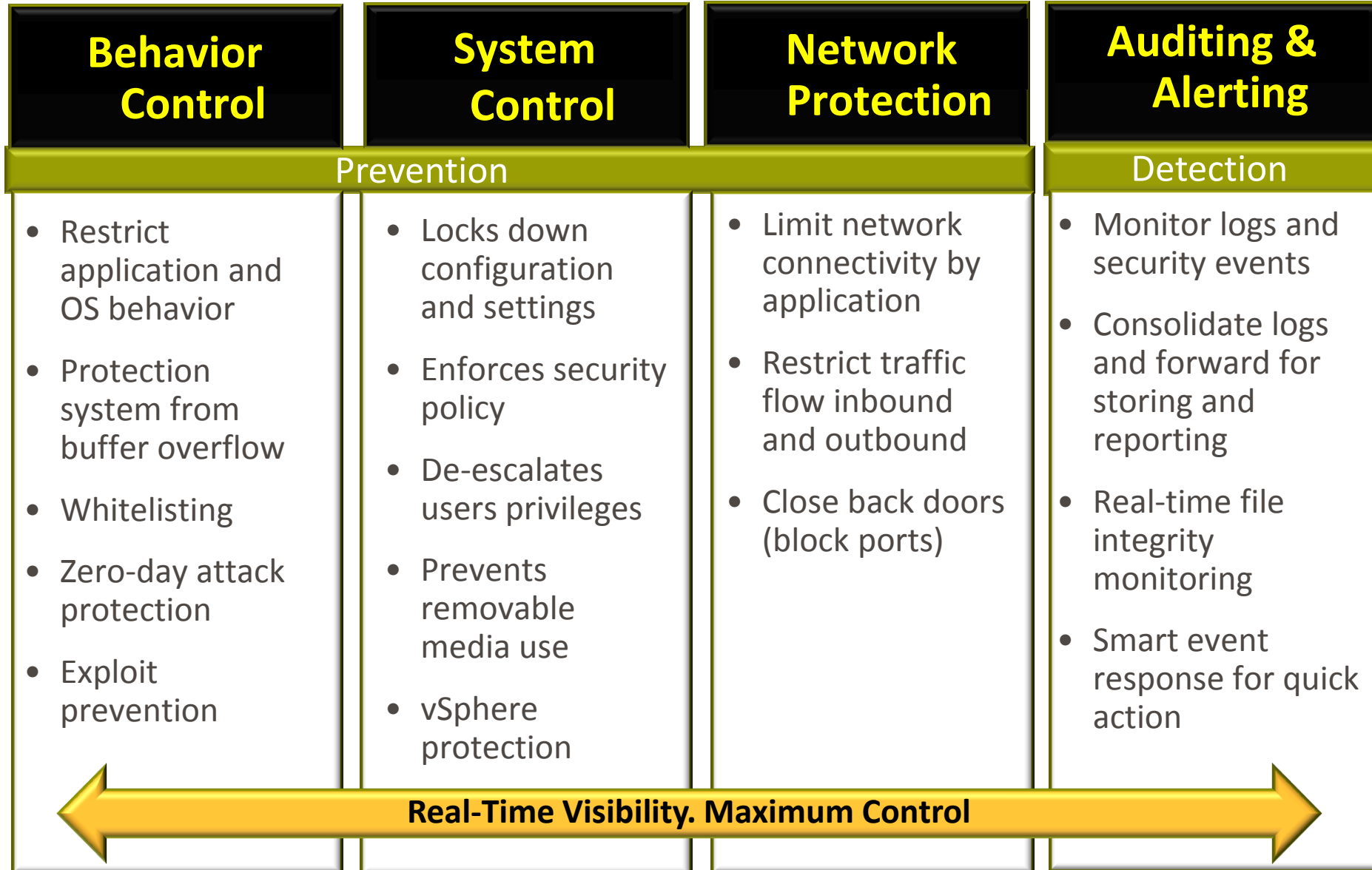
## Enhance Security Program

- Configuration monitoring
- Restrict administrative control
- Harden virtual fabric: guest, hypervisor, management server (*New!*)

# Critical System Protection Key Capabilities

<b>SINGLE SOLUTION</b>	<b>Monitoring (HIDS)</b>	<ul style="list-style-type: none"><li>• <i>Event Monitoring</i></li><li>• <i>File Integrity Monitoring</i></li><li>• <i>Intrusion Detection</i></li></ul>
	<b>Prevention (HIPS)</b>	<ul style="list-style-type: none"><li>• <i>Host Firewall</i></li><li>• <i>File and Configuration Lock Down</i></li><li>• <i>Admin Access Control</i></li><li>• <i>Malware and Exploit Prevention</i></li><li>• <i>Device Control</i></li><li>• <i>Application Control</i></li></ul>
	<b>Centralized Management</b>	<ul style="list-style-type: none"><li>• <i>Single Sign On and Central Mgmt</i></li><li>• <i>Out of Box Policy Templates</i></li><li>• <i>Multiple OS Support</i></li></ul>

# How does SCSP work?



# Behavior Control



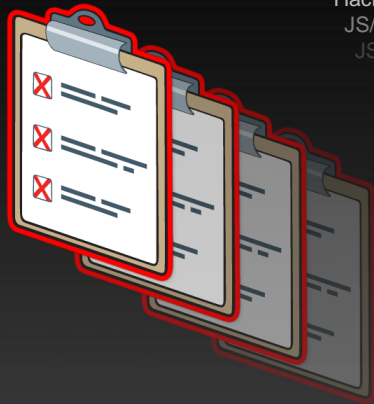
# Behavior blocking improves over traditional protection

Traditional approach:  
Blacklist Malware

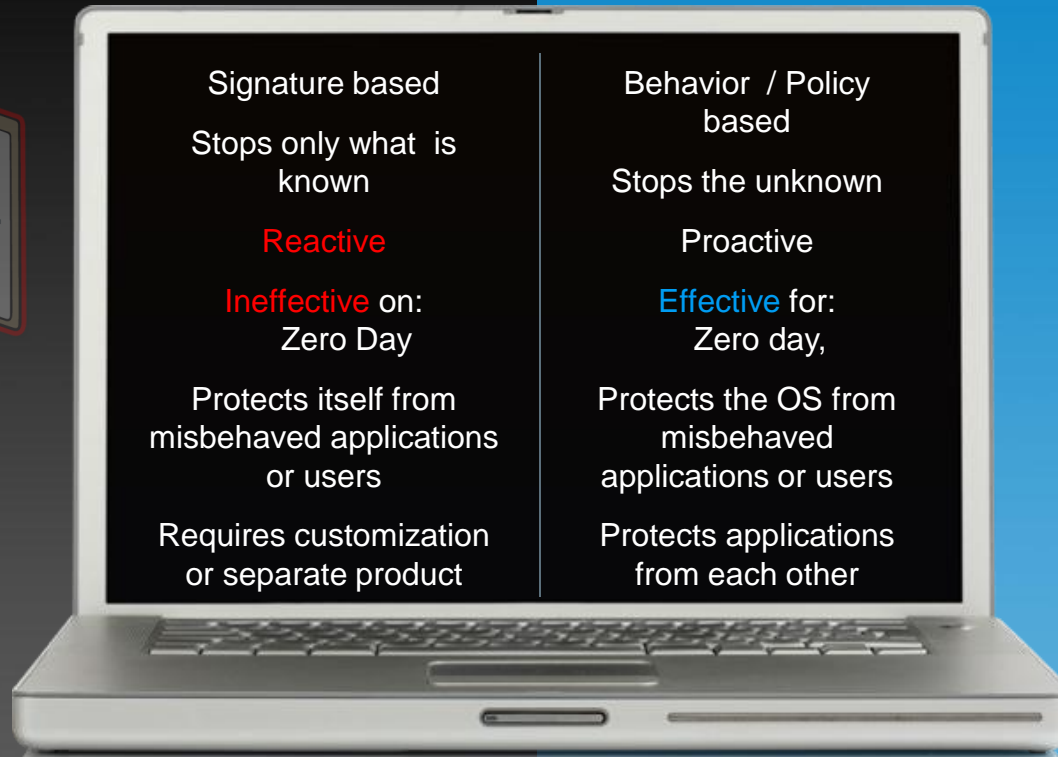
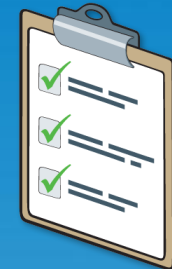
Behavior blocking:  
Sandboxing

Malware Signatures  
30 Million and growing @ xxx /  
Month

Loader.AMHZW \ Exploit\_Gen.HOW \  
Hacktool.KDY \ INF/AutoRun.HK \ JS/BornOrkut.A \  
JS/Exploit.GX \ JS/FakeCodec.B \ JS/Iframe.BZ \  
JS/Redirector.AH \ KillAV.MPK \ LNK/CplLnk.K

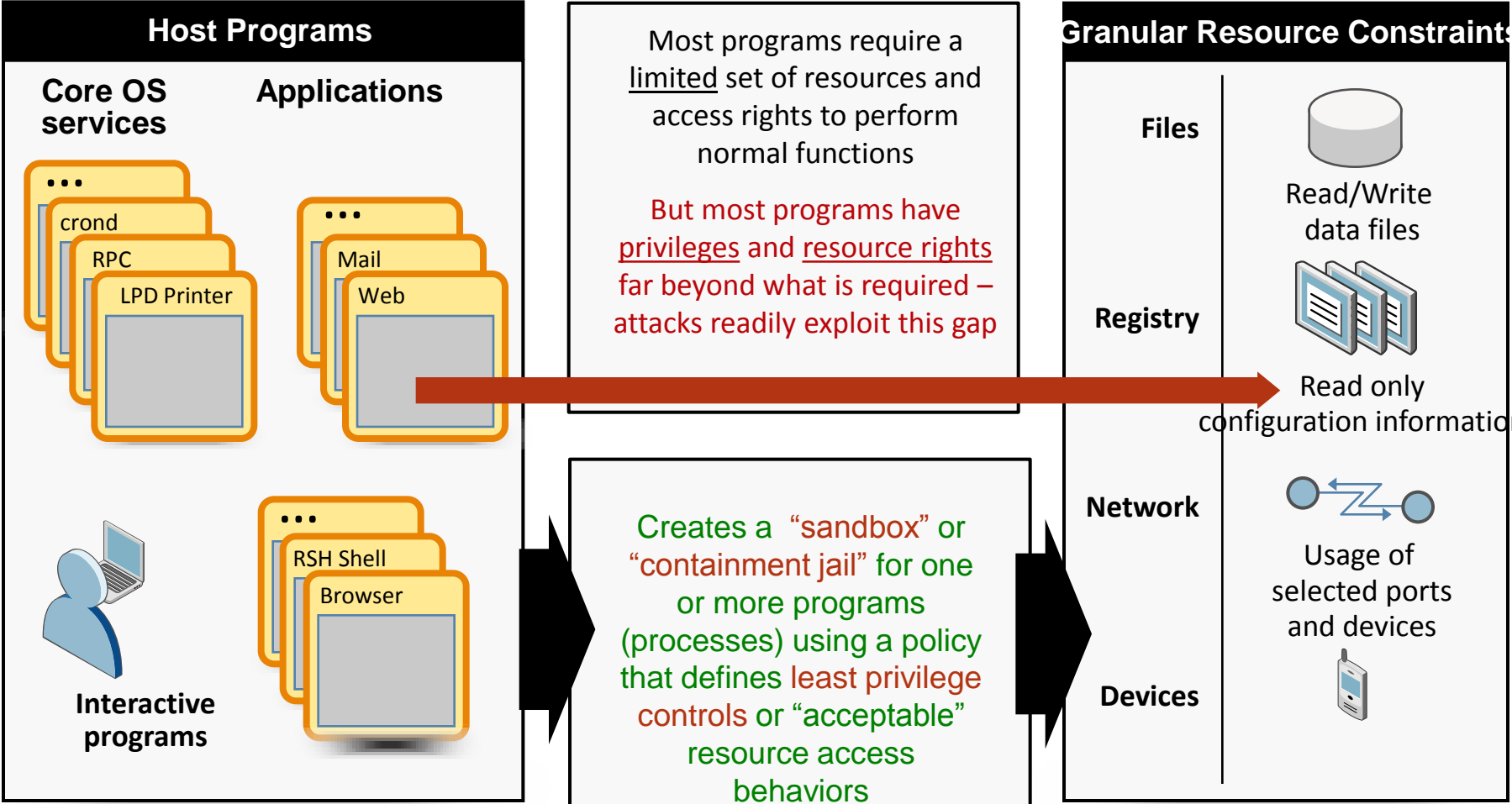


Application and OS Behavior  
Control  
As defined by prevention  
policy





# SCSP capabilities provide least privilege application control (sandboxing) to lockdown servers



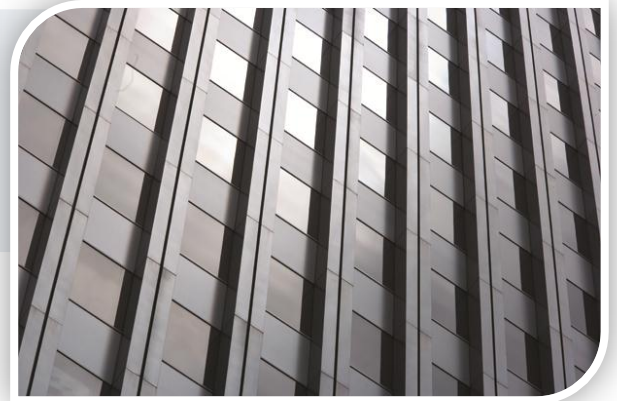
# Sandboxing is a highly effective on stopping zero-day attacks

Based on fundamental security principles and highly effective

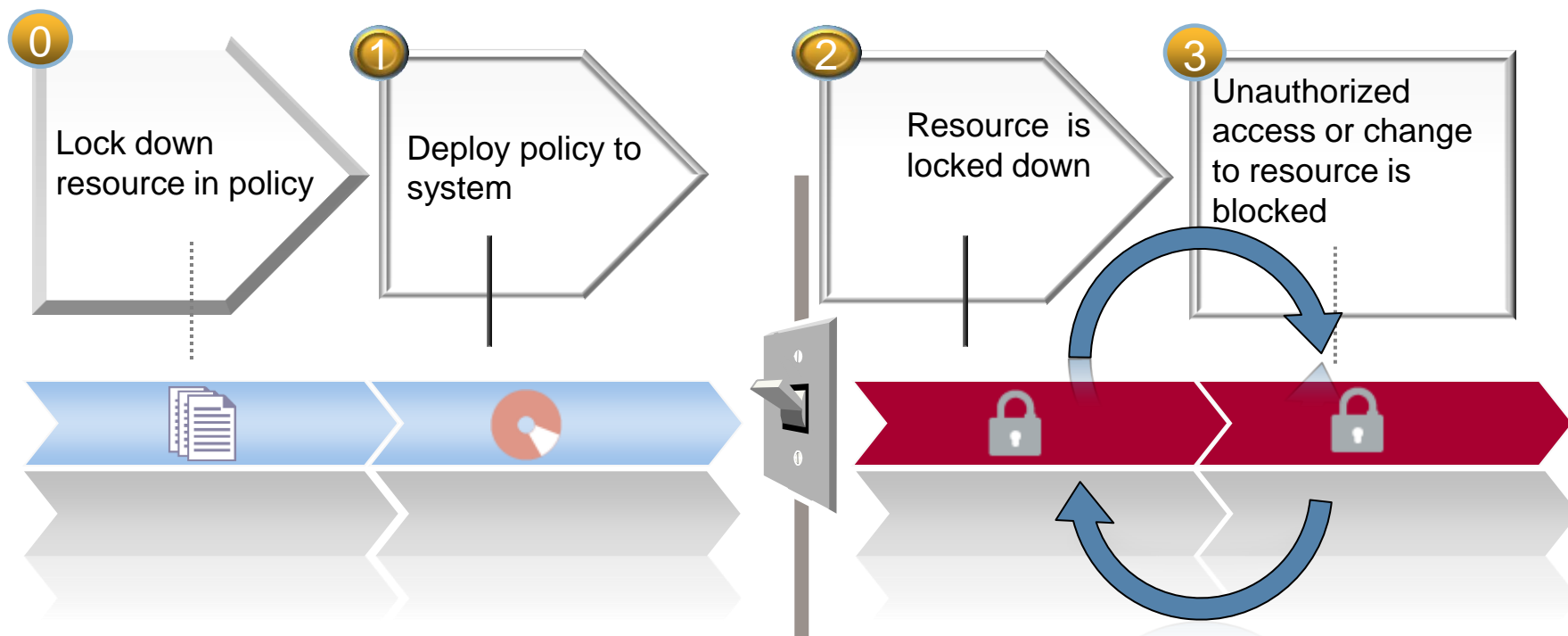
- Proactive protection against malware (known & unknown)
- The containment model limits the potential for exploitation
- Applicable to all environments and applications
- Effective against zero-day attacks
- Eliminates the need for patching applications
- Protects the OS from compromise



# System Controls



# System Control: How to protect system resources

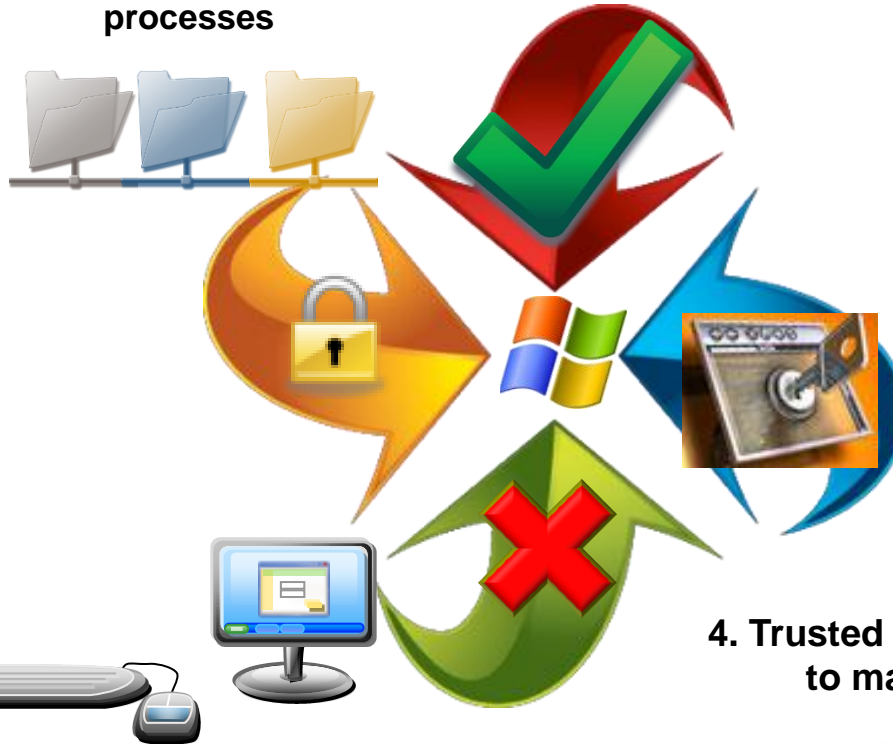


Resources can be a file, registry, device, and network connection

Policy controls what applications or users can access resources

# System Control: How to control privileged users access

1. CSP policies restrict access to critical resources by all users and processes



3. Policy can allow certain users or applications to make change



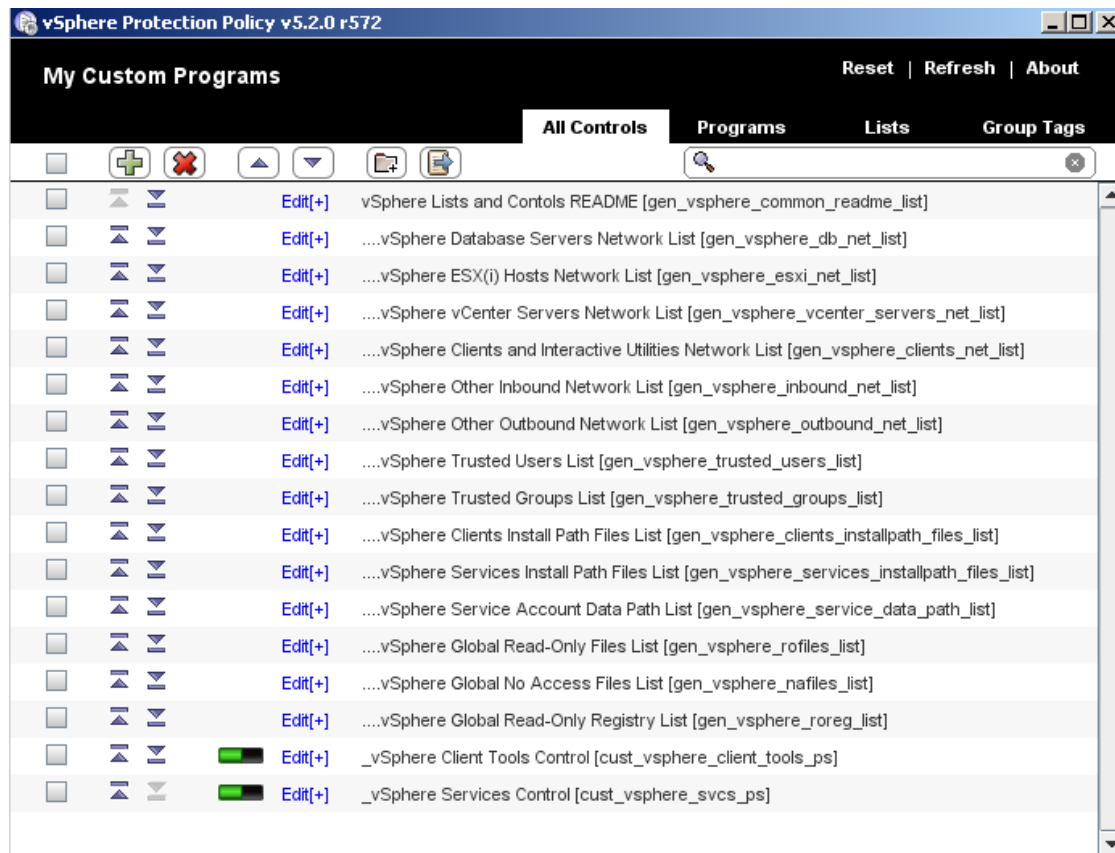
4. Trusted user or application allowed to make selective changes

2 Unauthorized access, regardless of privileges, is blocked

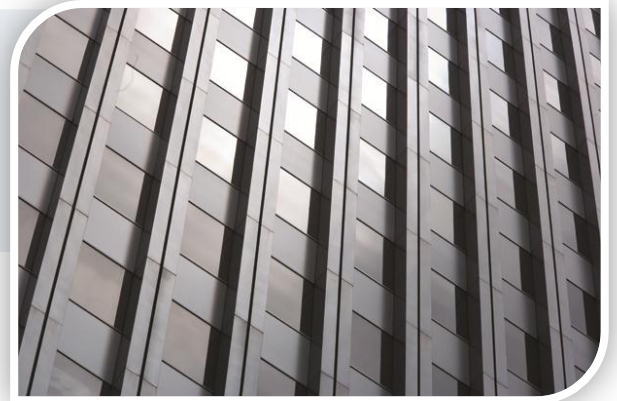
**ORACLE**<sup>®</sup>

# Use case: Hardens virtual environments

- VSC03 – Restrict access to SSL certificates
- VSH02 – Keep VMware center system properly patched
- VSC05 – Restrict network access to VMware vCenter server system
- VSH04 – Avoid user login to VMware vCenter server system
- VSC06 – Block access to ports not being used by VMware vCenter

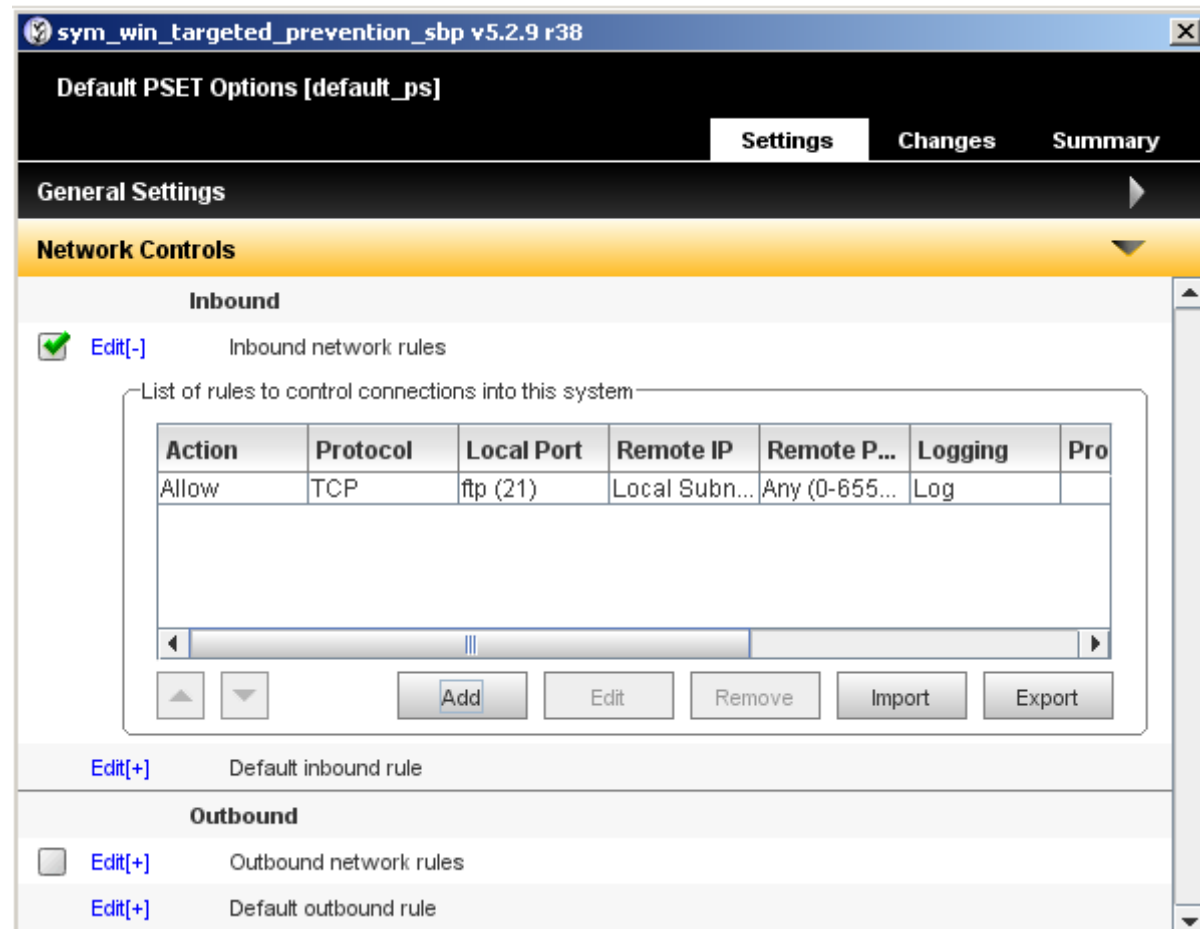


# Network Protection



# CSP provides network protection on critical servers

- Network access can be denied or allowed based on IP or port
- Access connections can be controlled based on application and user
- Less overhead than traditional deep packet inspection



The screenshot displays the Symantec CSP Network Controls interface. The window title is "sym\_win\_targeted\_prevention\_sbp v5.2.9 r38". The main heading is "Default PSET Options [default\_ps]". Below this, there are tabs for "Settings", "Changes", and "Summary". The "General Settings" section is visible, and the "Network Controls" section is expanded to show "Inbound" and "Outbound" network rules.

**Inbound**

Edit[-] Inbound network rules

List of rules to control connections into this system

Action	Protocol	Local Port	Remote IP	Remote P...	Logging	Pro
Allow	TCP	ftp (21)	Local Subn...	Any (0-655...	Log	

Buttons: Add, Edit, Remove, Import, Export

**Outbound**

Edit[+] Outbound network rules

Edit[+] Default outbound rule



# Detection: Auditing and Alerting



# CSP detection: Monitors for configuration changes

## Change Detection





- File and Registry Change Detection
- Security Configuration Changes
- Group Management Changes
- Active Directory Changes
- Shares Configuration Changes
- Domain Trust Changes
- User/Group Account Modification
- Fine Grained System Activity
- Malware/Spyware Detection
- USB Device Activity
- Monitors ESXi host configuration and VMX files

Master View - Event Details			
Agent Name	win2k3	Agent Version	5.2.9.312
Host Name	win2k3	OS Type	Windows
Host IP Address	127.0.0.1	OS Version	Server 2003 Service Pack 1
User Name	WIN2K3\admin	Agent Type	CSP Native Agent
Event			
Event Type	File Watch	Event Date	18-Jun-2012 13:22:13 PDT
Event Category	Real Time - Detection	Post Date	18-Jun-2012 13:22:15 PDT
Operation	Modified	Post Delay	00:00:02
Event Severity	Critical	Event Count	1
Event Priority	80	Event ID	619
Details			
Description	Watched File Modified (c:\certreq.txt)		
Policy Name	file monitoring		
Rule Name	filewatch		
Operation	Modified		
File Name	c:\certreq.txt		
Old Size	1236		
New Size	1243		
Old Modification Date	2012-06-14 16:47:41		
New Modification Date	2012-06-18 13:22:13		
Old Access Date	2012-06-18 13:21:17		
New Access Date	2012-06-18 13:22:13		
File Difference	22a22,1 > dsfds		

# Real-time change detection = Situational awareness

## PCI Section 11: File Integrity Monitoring Requirements (FIM)

- CSP offers continuous (real-time) File Integrity Monitoring (RTFIM)
- No scanning, no OS auditing required
- Captures server/file/user name, timestamp, change type, change content, program that made change
- Uses SH2 hashes

Features	Competitor FIM	CSP RTFIM
Real-time change detection and alerts		
Requires auditing enabled on Windows		

# CSP Detection: Monitors significant system security events

## System/Application Log Monitoring

- Logons/Logoffs Monitoring
  - Success, Failures, After Hours, Weekends, privileged user, Unusual access methods, password cracking attempts
- System/Services Monitoring
  - Service/daemon/driver failures, process tracking (privileged access, unusual usage)
- C2 Object Level Log Monitoring
- Web Log Monitoring
- Application Log Monitoring
  - Database logs
  - Application server logs (such as Esxi)
  - Security tool logs (such as AV)
  - Unix shell & sudo logs
  - vSphere logs

**Master View - Event Details**

Host Name	win2k3	OS Type	Windows
Host IP Address	127.0.0.1	OS Version	Server 2003 Service Pack 1
User Name	WIN2K3\admin	Agent Type	CSP Native Agent

**Event**

Event Type	NT Event Log	Event Date	18-Jun-2012 13:27:12 PDT
Event Category	Real Time - Detection	Post Date	18-Jun-2012 13:27:13 PDT
Event Log	Security	Post Delay	00:00:01
Event Severity	Warning	Event Count	1
Event Priority	59	Event ID	627

**Details**

Policy Name	Windows_Baseline_Detection
Rule Name	System_User_Configuration_Account_Disabled
Source	Security
Event Log	Security
Type	Success Audit
Event ID	629
Category	Account Management
Computer	WIN2K3
Description	User Account Disabled:
	Target Account Name: cgibbens
	Target Domain: WIN2K3
	Target Account ID: WIN2K3\cgibbens
	Caller User Name: admin
	Caller Domain: WIN2K3
	Caller Logon ID: (0x0,0x33681)



# Reduce Cost

## *Virtual Patching: Physical & Virtual Platform Support*

### VMware

ESX (3.5, 4.1) Guest  
ESX (3.5, 4.1) Hypervisor  
ESXi 5.0 Hypervisor  
vCenter 5.0 Management Server

### Windows

Windows 2008 R2 (Standard Edition and Enterprise Edition)  
Windows 2008 (Standard Edition and Enterprise Edition)  
Windows 2003 R2 (Standard Edition and Enterprise Edition)  
Windows 2003 (Standard Edition and Enterprise Edition)  
Windows XP Professional  
Windows XPe  
Windows 2000 (Advanced Server, Server and Professional)  
Windows NT4

### Supported Hypervisors <sup>(1)</sup>

Windows Server 2008 R2 Hyper-V  
Red Hat Enterprise Virtualization (RHEV)  
XenServer 6.0  
Oracle VM 3.0

### Community ENTerprise Operating System

CentOS 5

### SUSE Linux

SUSE Linux Enterprise Server 11  
SUSE Linux Enterprise Server 10  
SUSE Linux Enterprise Server 9  
SUSE Linux Enterprise Server 8

### AIX

AIX 7.1\*  
AIX 6.1  
AIX 5L 5.3 -- 64-bit kernel  
AIX 5L 5.3 -- 32-bit kernel  
AIX 5L 5.2  
AIX 5L 5.1

### Solaris

Solaris 10 -- No zones  
Solaris 10 -- Global Zone  
Solaris 10 -- Local Zones  
Solaris 9  
Solaris 8

### HP-UX

HP-UX 11i V3 (11.31) (64-bit)  
HP-UX 11i V2 (11.23) (64-bit)  
HP-UX 11i V1 (11.11) (64-bit)  
HP Tru64 5.1B-3

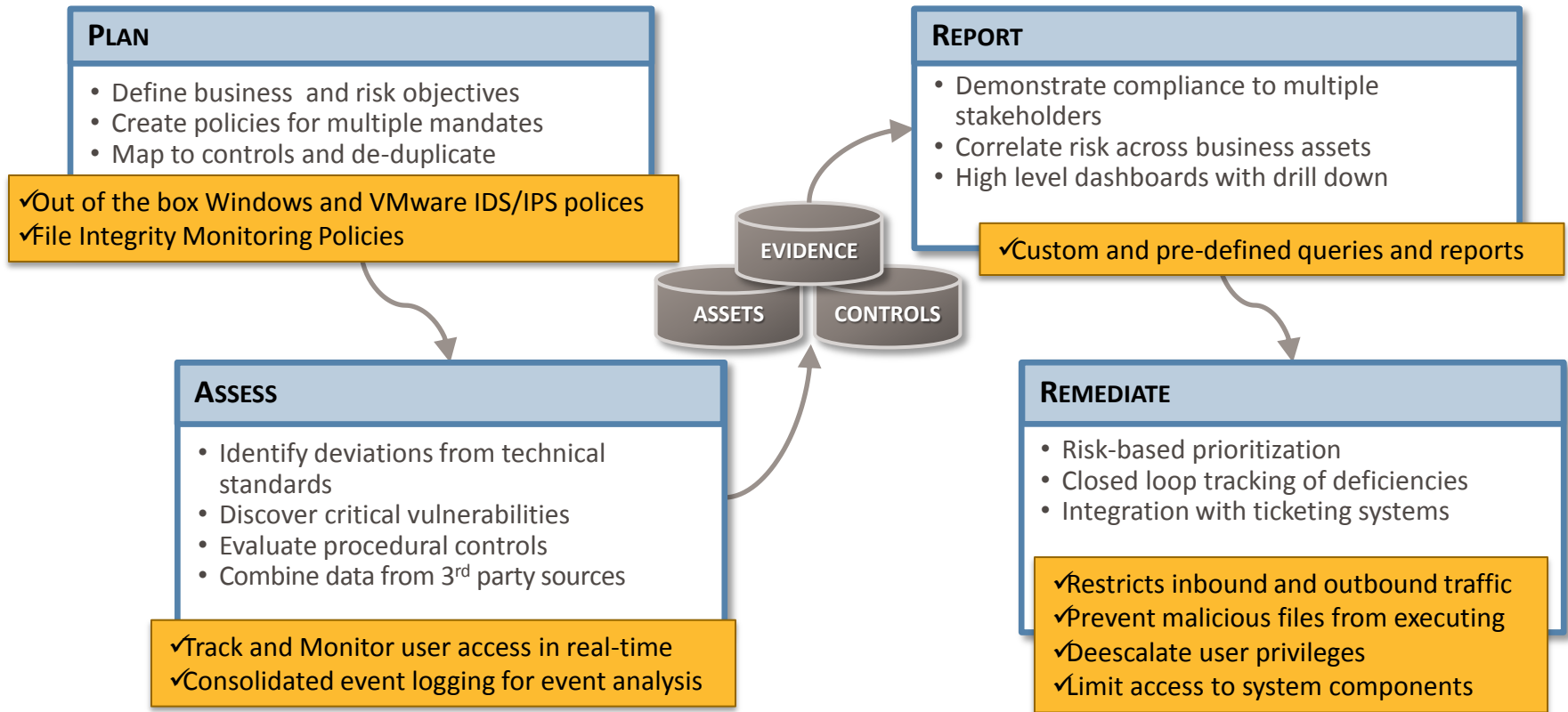
### Red Hat Linux

Red Hat Enterprise Linux 6  
Red Hat Enterprise Linux 5  
Red Hat Enterprise Linux 4  
Red Hat Enterprise Linux 3

(1): Guest Virtual machines with operating systems already supported by SCSP are also supported in these virtualized environments  
Source: Symantec Support Website (<http://www.symantec.com/business/support/index?page=landing&key=52463>)

# Demonstrate Compliance

## *Real-Time Visibility & HIDS/HIPS Compensating Controls*



**CRITICAL SYSTEM PROTECTION**

**CONTROL COMPLIANCE SUITE**

# Meets Primary Use Cases

## Compliance (PCI)

- Req 1.3.5: Restricts inbound and outbound traffic to PCI data environment
- Req 5: Malicious file execution
- Req 7.1: Limit access to system components
- Req 10: Track and Monitor user access
- Req 11.5: Use file integrity monitoring
- Req 11.4: Use intrusion detection and intrusion prevention systems

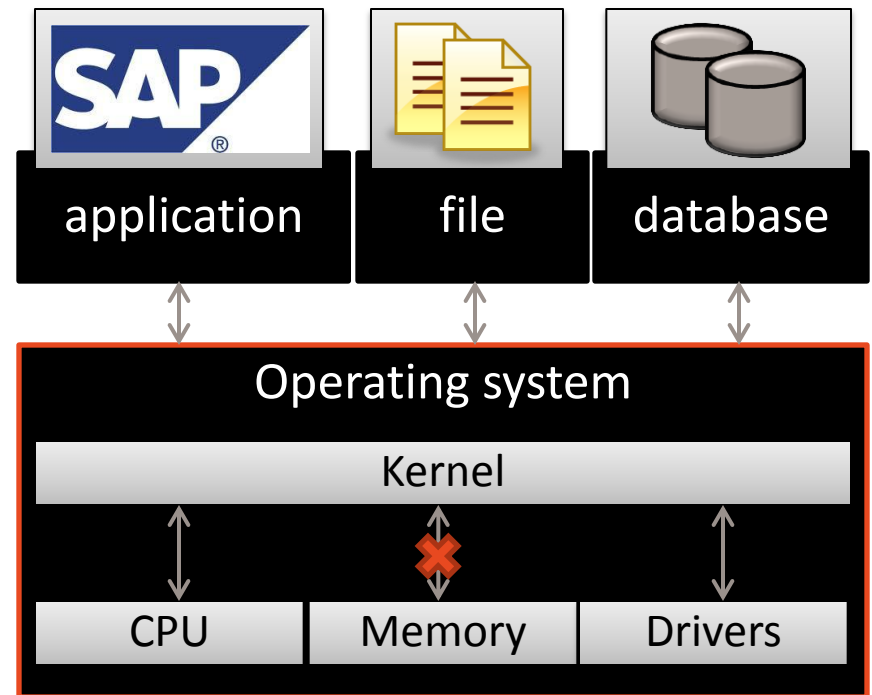
## Security

- Patch mitigation
- User access control
- Malware prevention
- System hardening
- Application control
- Configuration Monitoring

# Breach Response

## *Stop Attacks In Their Tracks With Targeted Prevention Policies*

- Attack Scenarios:
  - Restrict network access
  - Restrict access to specific files
  - Prevent further admin configuration changes
  - Block buffer overflows
- How it Works:
  - Begin with a blank policy
  - Select activities to block and/or OS resources that should not be accessed
- Easy way to harden servers without the fear of blocking a critical business process



Reduces Your Window of Exposure





# Control Compliance Suite

## Virtualization Security Manager



# Как защитить сервер



**Контроль доступа  
ОС и приложений**

**Контроль настроек и уязвимостей  
ОС и приложений**

**Физическая безопасность  
сервера**

*Армянский комсомол не ищет лёгких путей,  
а сначала создаёт трудности и только потом  
мужественно их преодолевает.  
(Советский анекдот)*

# Как защитить виртуальную инфраструктуру



Контроль доступа  
ОС и приложений

Контроль настроек и уязвимостей  
ОС и приложений

Контроль настроек и уязвимостей  
Гипервизора и ВМ

Контроль доступа  
к гипервизору и ВМ

Физическая безопасность  
сервера

# Как защитить виртуальную инфраструктуру

## Контроль доступа к гипервизору и VM

- **Один root** – управляет всем
- **Один гипервизор** – разные виртуальные машины
- **Одна настройка** – вся инфраструктура
- **Регистрация событий**

# Ролевая модель

Ролевая модель



VClient

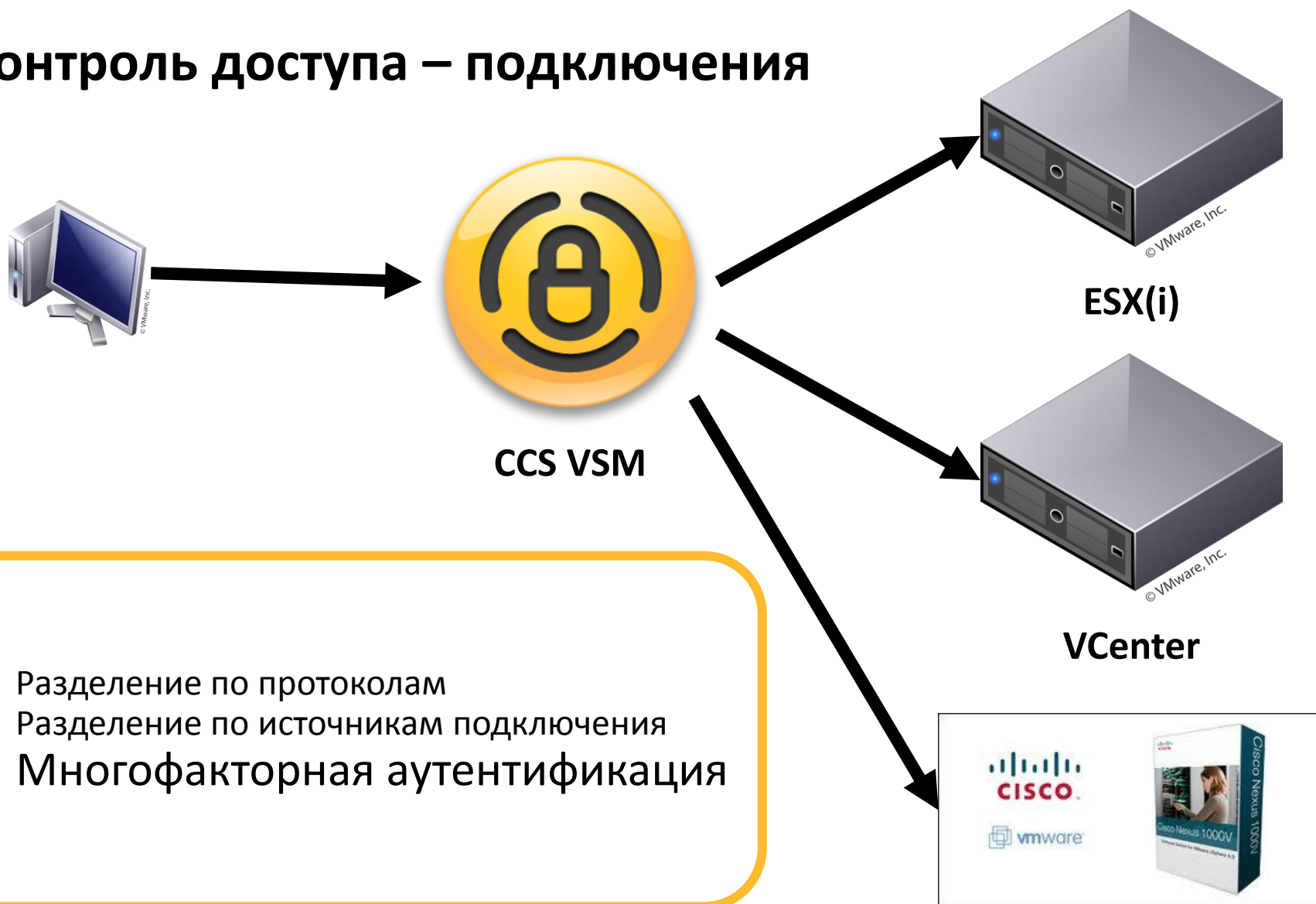


ESX(i)

# Ролевая модель



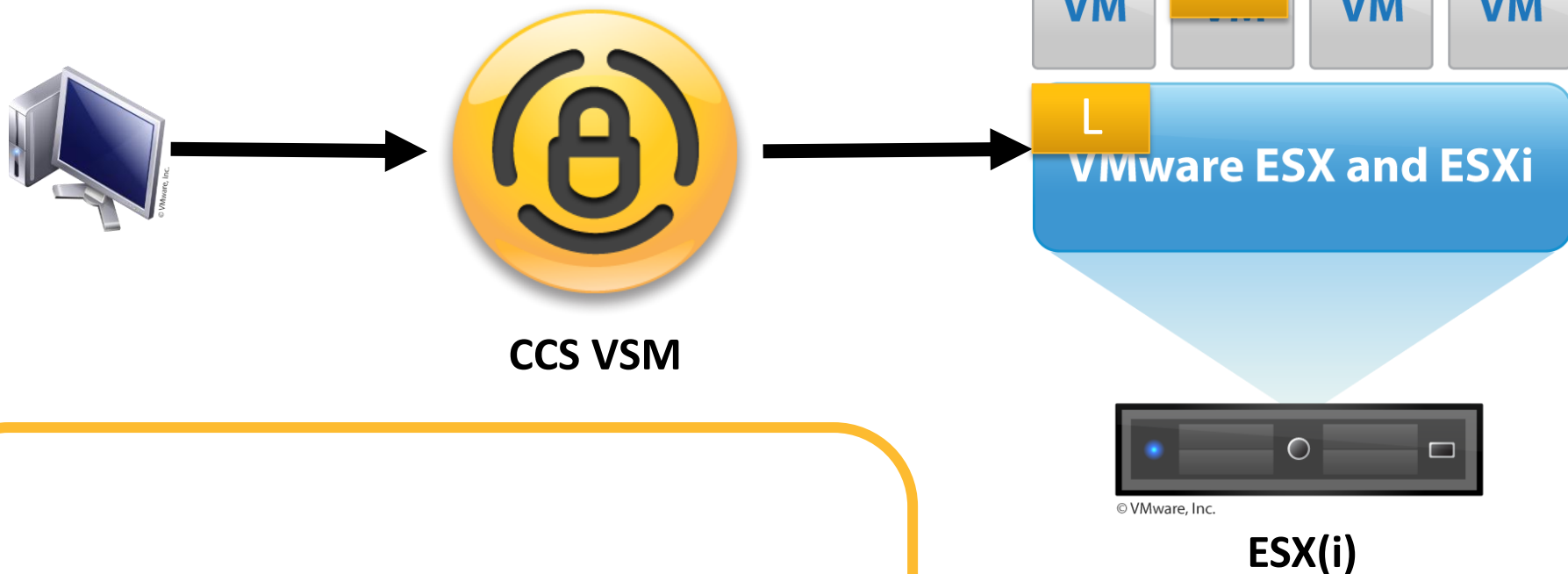
# Контроль доступа – подключения



- Разделение по протоколам
- Разделение по источникам подключения
- Многофакторная аутентификация

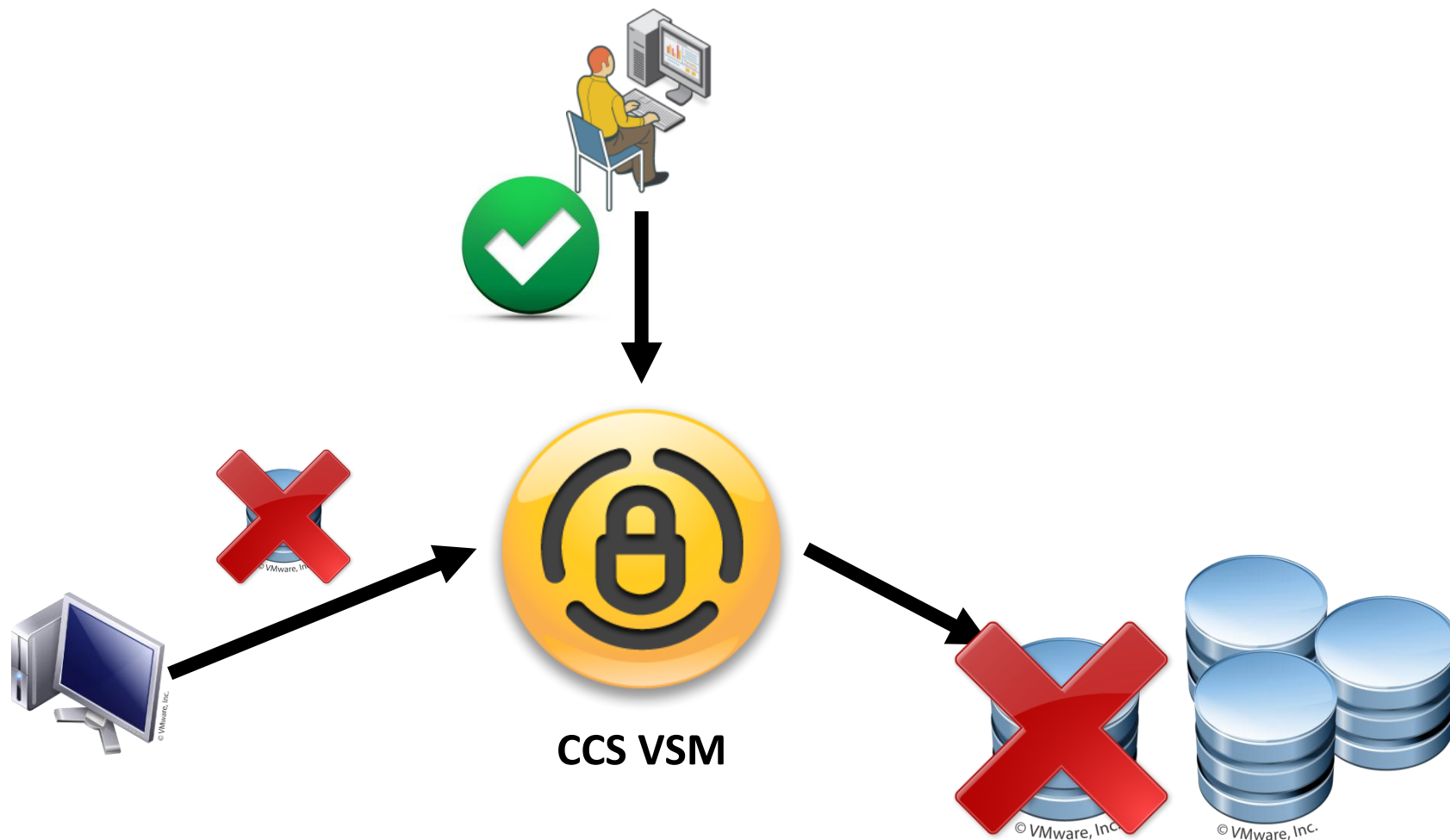


# Контроль доступа - метки



- Привязка VM к vSwitch
- Привязка VM к гипервизору
- Назначение прав для групп рабочих станций
- ...

# Подтверждение действий



# Подтверждение действий

**Secondary Approval**

Action  Approve  
 Deny

Request Time 10/03/2012 4:53:43 PM

Current Time 10/03/2012 4:59:18 PM

Requestor VIAdminUser

Resource Virtual Center: 192.168.1.48 > Datacenter: Symplified Virutual > VirtualMachine: DevRedHat


Operation Power Off VM

\*Start 10/3/12 4 : 59 PM

\*Duration (Hours) 2

\*Email

Comments



CCS VSM

# Скрытие root пароля

Замена root пароля на произвольный

Генерация временного пароля root по запросу

Замена пароля root на произвольный



VClient



CCS VSM



ESX(i)

# Регистрация действий

Log Viewer

Search:  Go ?

Fatal  Error  Warn  Info

Showing 1 to 20 of 574 Show: 20 50 100 200 All Pages: << < 1 2 3 4 5 6 7 8 9 10 >> >>

Date	Priority	User	Action	Message ID	Source	Destination	Message
06/29/2012 5:28:48 PM	INFO	SYSTEM	Add	ARC0027		10.216.133.3	ARC0027 SYSTEM performed operation: add template PcReportdbf8011f-d1e6-4f72-b010-1a1d7f61b8e5.
06/29/2012 5:19:45 PM	INFO	superadminuser	JobRunner	ARC0002		10.216.133.3	ARC0002 Job type ConfigType Service type SnmpService run on 10.216.133.3 using event type ProcessService.
06/29/2012 5:19:37 PM	WARN	superadminuser	JobRunner	ARC0033		10.216.133.3	ARC0033 Operation ProcessService of template ProcessService failed on host 10.216.133.3.
06/29/2012 5:19:37 PM	INFO	superadminuser	JobRunner	ARC0002		10.216.133.3	ARC0002 Job type ConfigType Service type SntpService run on 10.216.133.3 using event type ProcessService.
06/29/2012 5:19:32 PM	INFO	superadminuser	JobRunner	ARC0045		10.216.133.3	ARC0045 superadminuser performed operation SntpService on host 10.216.133.3
06/29/2012 5:19:32 PM	INFO	superadminuser	JobRunner	ARC0045		10.216.133.3	ARC0045 superadminuser performed operation SnmpService on host 10.216.133.3
06/29/2012 5:19:23 PM	WARN	superadminuser	JobRunner	ARC0033		10.216.133.3	ARC0033 Operation ProcessService of template ProcessService failed on host 10.216.133.3.
06/29/2012 5:19:23 PM	INFO	superadminuser	JobRunner	ARC0002		10.216.133.3	ARC0002 Job type ConfigType Service type SntpService run on 10.216.133.3 using event type ProcessService.
06/29/2012 5:19:18 PM	INFO	superadminuser	JobRunner	ARC0045		10.216.133.3	ARC0045 superadminuser performed operation SntpService on host 10.216.133.3
06/29/2012 5:13:23 PM	INFO	superadminuser	Create	GUI0033	10.216.58.44	10.216.133.3	GUI0033 superadminuser created the draft policy.
06/29/2012 5:12:49 PM	INFO	superadminuser	Deploy	GUI0017	10.216.58.44	10.216.133.3	GUI0017 superadminuser deployed the draft policy.
06/29/2012 5:12:05 PM	INFO	superadminuser	Update	GUI0019	10.216.58.44	10.216.133.3	GUI0019 superadminuser updated the draft policy.



VClient



CCS VSM



ESX(i) / VCenter

# Регистрация событий

https://192.168.1.37/?wicket:bookmarkablePage=Message+Detail:com.hytrust.gui.pages.search.LogMs - Windows Internet Ex...

**Date** 10/03/2012 3:52:17 PM

**Priority** INFO

**Message** VVM0010 Source: 192.168.1.50 Destination: 192.168.1.48 Operation: ReconfigVM\_Task User: SuperAdminUser, Parameters: operationID=E23BA7FD-0000009F; \_this=vm-25, attributes: xsi:type=ManagedObjectReference, type=VirtualMachine, serverGuid=7272CE56-0852-4680-A422-6C6F534932C3; changeVersion=2012-10-03T11:20:54.542385Z; operation=add; fileOperation=create; key=-100; diskMode=persistent; split=false; writeThrough=false; thinProvisioned=true; eagerlyScrub=false; startConnected=true; allowGuestControl=false; connected=true; controllerKey=1000; unitNumber=1; capacityInKB=1048576; .

Task Details

Name: **Reconfigure virtual machine** Target: [DevSystem](#) Initiated by: **Administrator**

Status: **Completed**

Related Events: [Hide](#)

- 10/3/2012 10:52:58 AM, Task: Reconfigure virtual machine
- 10/3/2012 10:53:01 AM, Reconfigured [DevSystem](#) on [192.168.1.85](#) in [Simplified Virtual](#)

# Logging

Log Data Provider	Data for Allowed Operation (example)	Data for Denied Operation (example)	Usability & Productivity
Virtualization Platform	User: root Time/date Target resource name, URL Operation executed	none	<ul style="list-style-type: none"> <li>• Separate log files for vCenter and each host server</li> <li>• Different log formats for vCenter vs. hosts</li> </ul>
CCS VSM	All above, plus: <ul style="list-style-type: none"> <li>• User ID</li> <li>• Source IP address</li> <li>• Resource reconfigured</li> <li>• Previous &amp; new resource state</li> <li>• Label (Production)</li> <li>• Required privileges</li> <li>• Evaluated rules/constraints</li> </ul>	<ul style="list-style-type: none"> <li>• User ID</li> <li>• Date/time</li> <li>• Source IP address</li> <li>• Operation requested</li> <li>• Operation denial</li> <li>• Target resource name, IP address, port, and protocol</li> <li>• Required privileges</li> <li>• Missing privileges</li> <li>• Evaluated rules/constraints</li> </ul>	<ul style="list-style-type: none"> <li>• Consolidated, centrally managed logs covering vCenter and all hosts</li> <li>• Single, uniform format for combined vCenter and host log data</li> <li>• Logs sent to central repository or SIEM via syslog</li> </ul>

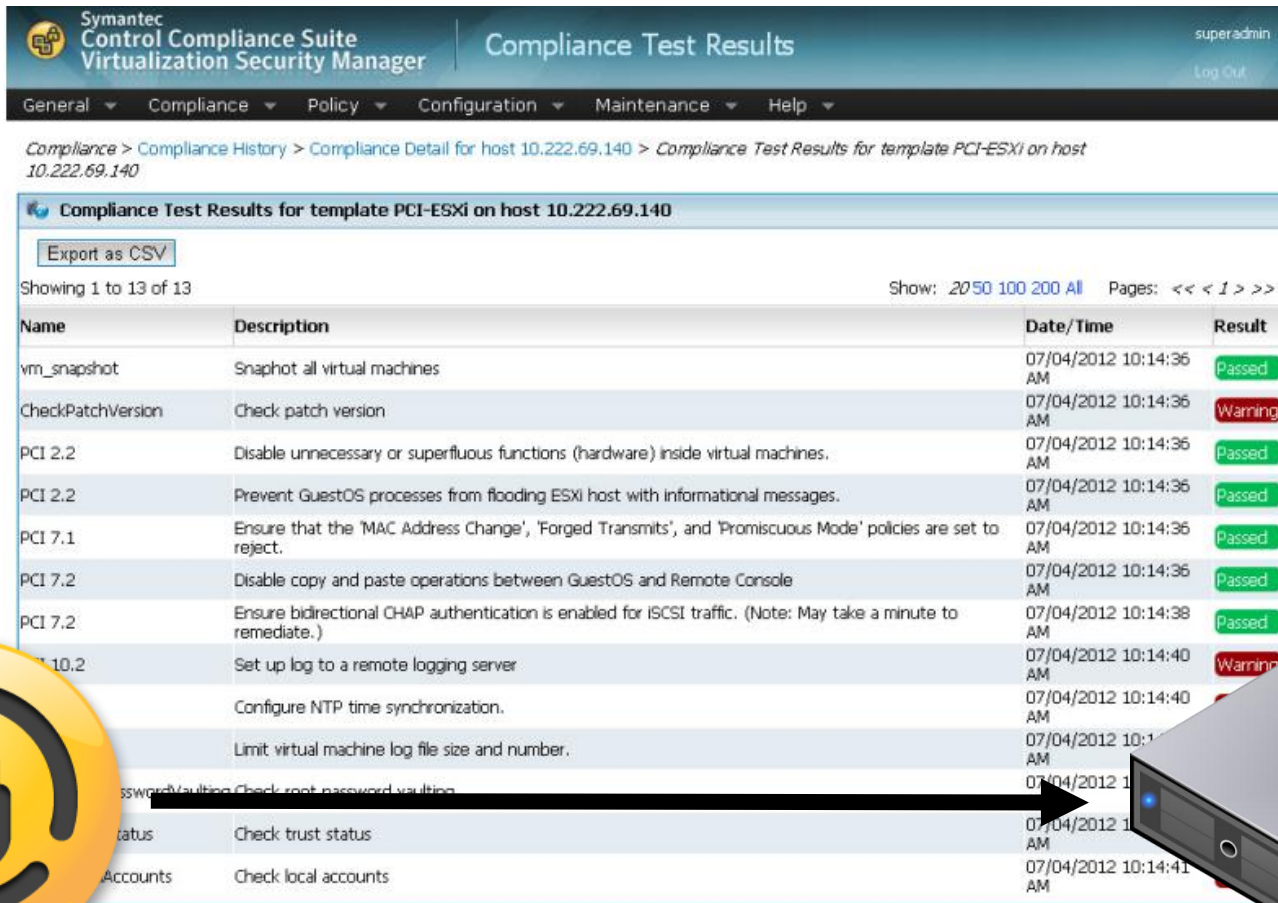
# Как защитить виртуальную инфраструктуру

## Контроль настроек и уязвимостей Гипервизора и ВМ

- **Ошибка настройки или уязвимость одного гипервизора** – риск для всей инфраструктуры



# Контроль соответствия



Symantec Control Compliance Suite Virtualization Security Manager Compliance Test Results

superadmin Log Out

General Compliance Policy Configuration Maintenance Help

Compliance > Compliance History > Compliance Detail for host 10.222.69.140 > Compliance Test Results for template PCI-ESXi on host 10.222.69.140

Compliance Test Results for template PCI-ESXi on host 10.222.69.140

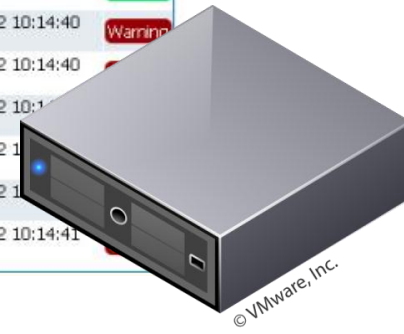
Export as CSV

Showing 1 to 13 of 13 Show: 20 50 100 200 All Pages: << < 1 > >>

Name	Description	Date/Time	Result
vm_snapshot	Snapshot all virtual machines	07/04/2012 10:14:36 AM	Passed
CheckPatchVersion	Check patch version	07/04/2012 10:14:36 AM	Warning
PCI 2.2	Disable unnecessary or superfluous functions (hardware) inside virtual machines.	07/04/2012 10:14:36 AM	Passed
PCI 2.2	Prevent GuestOS processes from flooding ESXi host with informational messages.	07/04/2012 10:14:36 AM	Passed
PCI 7.1	Ensure that the 'MAC Address Change', 'Forged Transmits', and 'Promiscuous Mode' policies are set to reject.	07/04/2012 10:14:36 AM	Passed
PCI 7.2	Disable copy and paste operations between GuestOS and Remote Console	07/04/2012 10:14:36 AM	Passed
PCI 7.2	Ensure bidirectional CHAP authentication is enabled for iSCSI traffic. (Note: May take a minute to remediate.)	07/04/2012 10:14:38 AM	Passed
10.2	Set up log to a remote logging server	07/04/2012 10:14:40 AM	Warning
	Configure NTP time synchronization.	07/04/2012 10:14:40 AM	
	Limit virtual machine log file size and number.	07/04/2012 10:14:40 AM	
passwordVaulting	Check root password vaulting	07/04/2012 10:14:40 AM	
status	Check trust status	07/04/2012 10:14:40 AM	
Accounts	Check local accounts	07/04/2012 10:14:41 AM	



CCS VSM




ESX(i)

# Контроль соответствия

**Summary Report**

PDF CSV

 PCI DSS Version 2 Summary Report

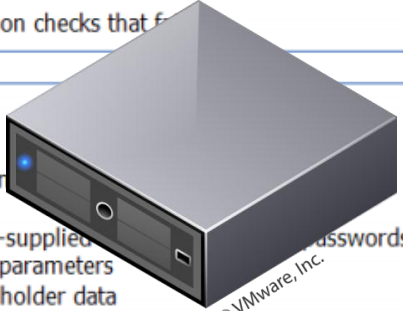

Report Generated: June 29, 2012 5:31:13 PM

Date Range: From: June 29, 2012 To: June 29, 2012  
Scope: Infrastructure Label: All VM Label: All  
Templates: ESX: PCI ESXi: PCI-ESXi

Overview

vSphere and Symantec VSM Operations	Authorized: null; Denied: null	Number of Authorized and Denied operations for vSphere and Symantec VSM
<a href="#">Number of Virtual Machines with Label</a>		Number of VMs with the selected label
Trend Micro Status (Overall)	Trend Micro is Disabled	Trend Micro Deep Security Server Configuration
<a href="#">Number of Resources with Label</a>		Number of vSphere resources with the selected label
<a href="#">Number of Hosts with Failed Configuration Checks</a>		Number of hosts with configuration checks that failed

Potential Violations (P)	Satisfied Controls (S)	Monitored Controls (M)
0	0	



Install and maintain cardholder data  
Do not use vendor-supplied passwords and other security parameters  
Protect stored cardholder data  
Develop and maintain secure systems and applications

CCS VSM

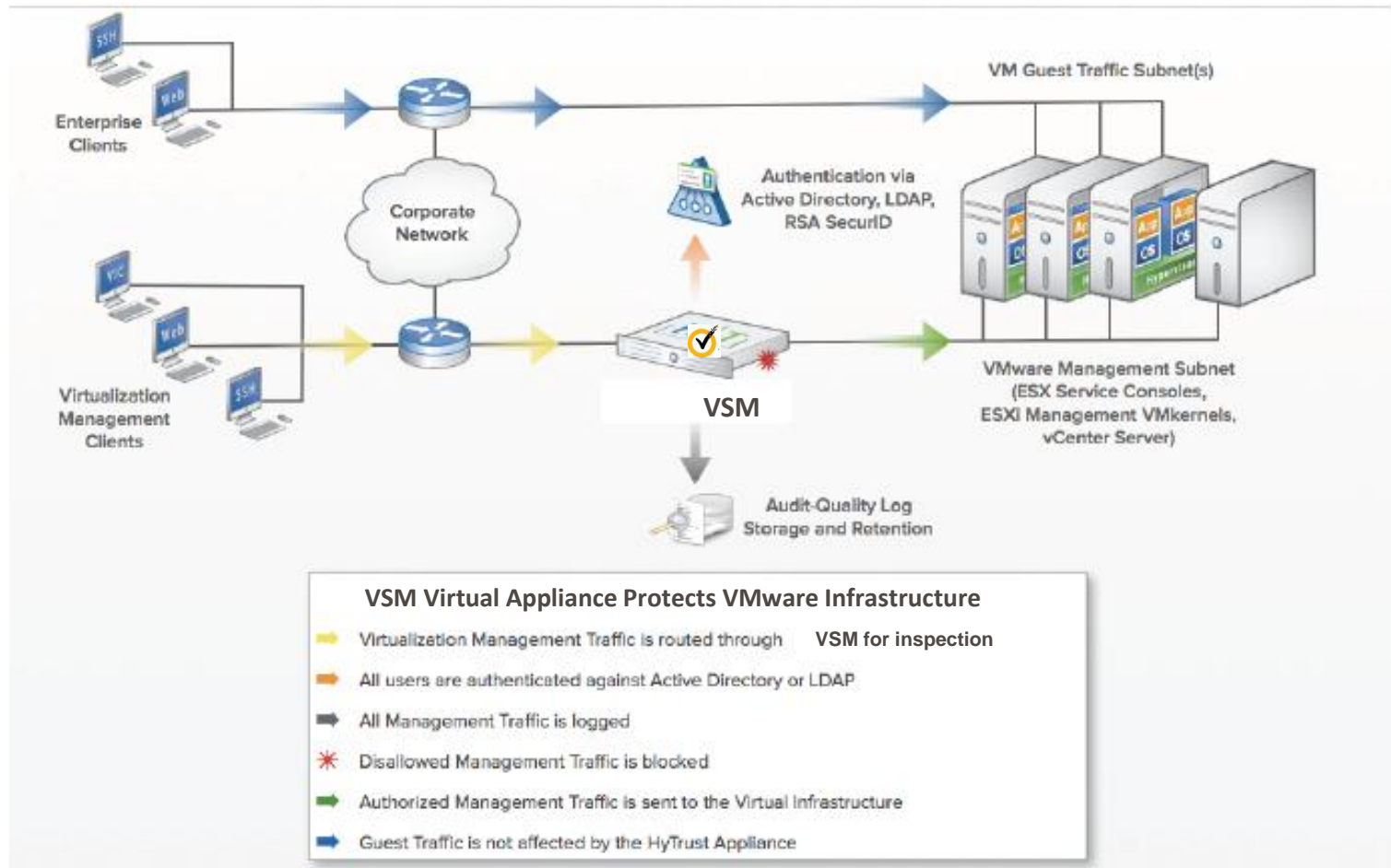
ESX(i)

## ESX & ESXi шаблоны оценки

- VMware Security Hardening Guide for ESX
- Center for Internet Security (CIS) Benchmark for ESX
- Payment Card Industry (PCI) DSS
- Sarbanes-Oxley (SOX)

# Архитектура





# Control Compliance Suite

**Policy Manager**

**Risk Manager**



**Standard Manager**

**Vulnerability  
Manager**

**Response  
Assessment Manager**

**Virtualization  
Security Manager**

# Critical Systems Protection + CCS VSM

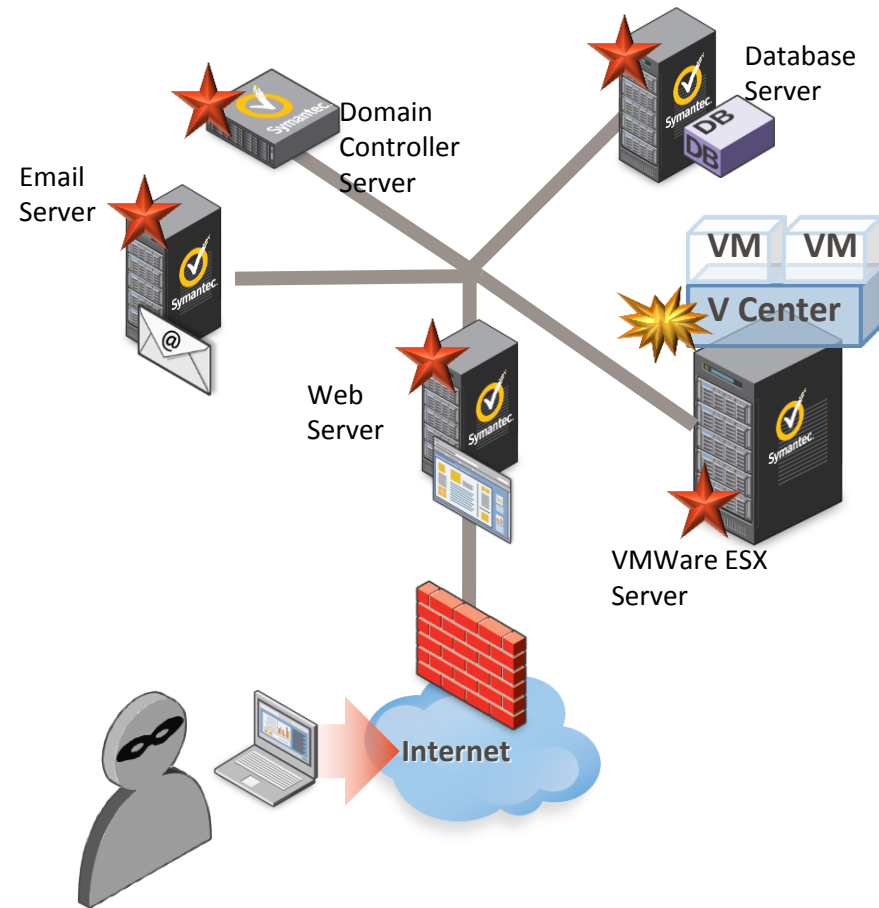
## CSP: Protect & Prevent

- Exploit prevention of both internal and external threats
- Targeted protection based on data and function
- Ensure availability of critical systems
- Configuration and access change monitoring

## CCS VSM: Comply & Report

- Regulatory and security guidelines
- Configuration assessment & reporting
- Logical separation to limit compliance scope
- Detailed activity reporting
- Single view of risk across physical & virtual assets
- Configuration assessment

# CSP + VSM = VM Exploit Prevention



- **Outside VCenter**

- ★ CSP monitors and prevents changes across the network infrastructure
- ★ CSP monitors and prevents access changes on ESX Server

- **Inside VCenter**

- ★ VSM monitors and prevents access changes
- ★ VSM monitors and controls VMotion functions



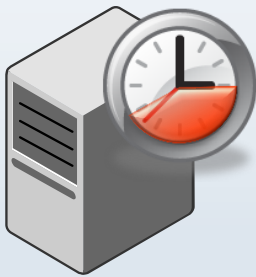


# Архивы, eDiscovery и все-все-все

# Symantec: «Резервная копия – для восстановления Архив – для расследования»

## Восстановление

- Восстановление систем после логического или физического сбоя
- Объекты – файл, БД, том, приложение
- Участники:
  - IT
  - Help desk



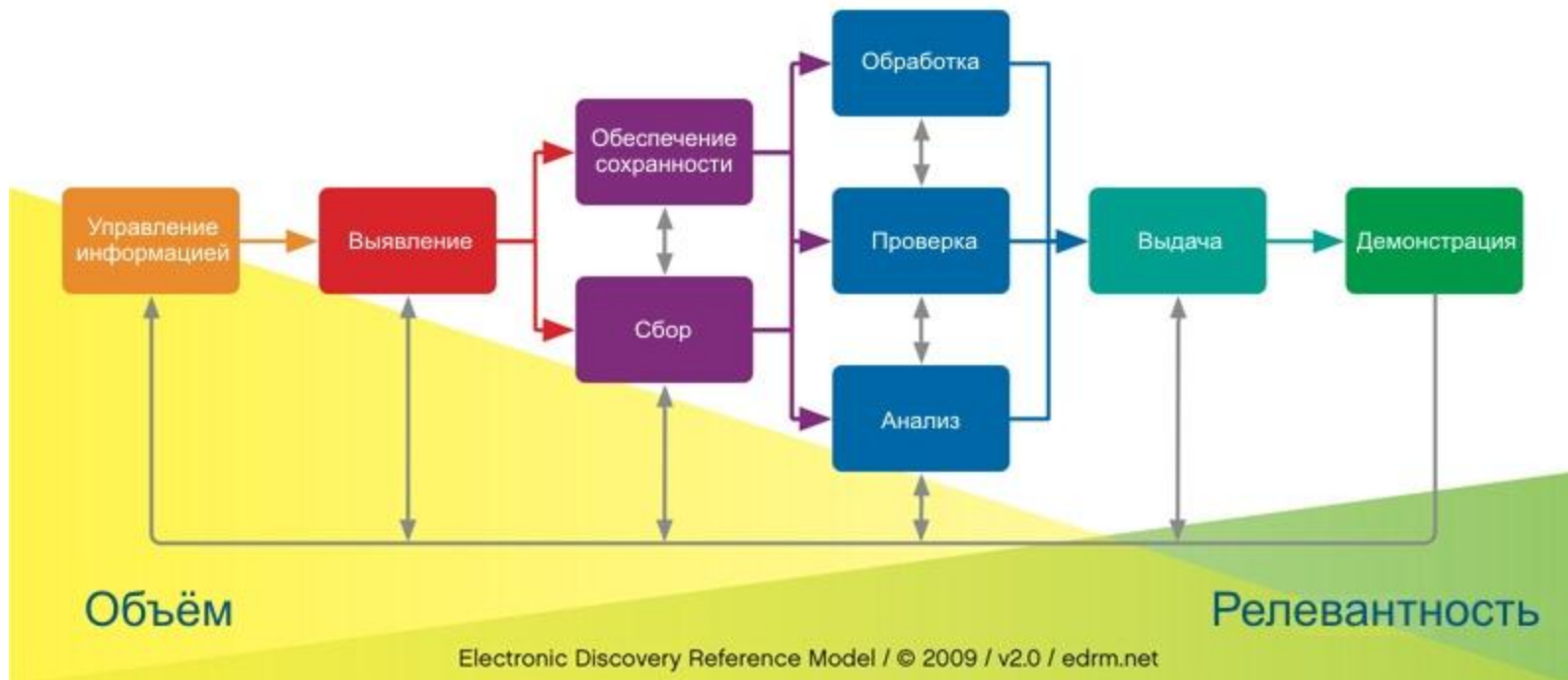
## Расследование

- Поиск по различным источникам – почта, файлы, портал SharePoint, мгновенные сообщения, социальные сети
- Судебные разбирательства, внутренние расследования, аудит
- Участники:
  - IT Security
  - Law
  - HR



# Electronic Discovery Reference Model

Базовая модель поиска, выемки и представления электронной информации (eDiscovery)



# Решения ключевых проблем управления данными



## Сохранение

ключевой  
информации



## Понимание

что и где хранится



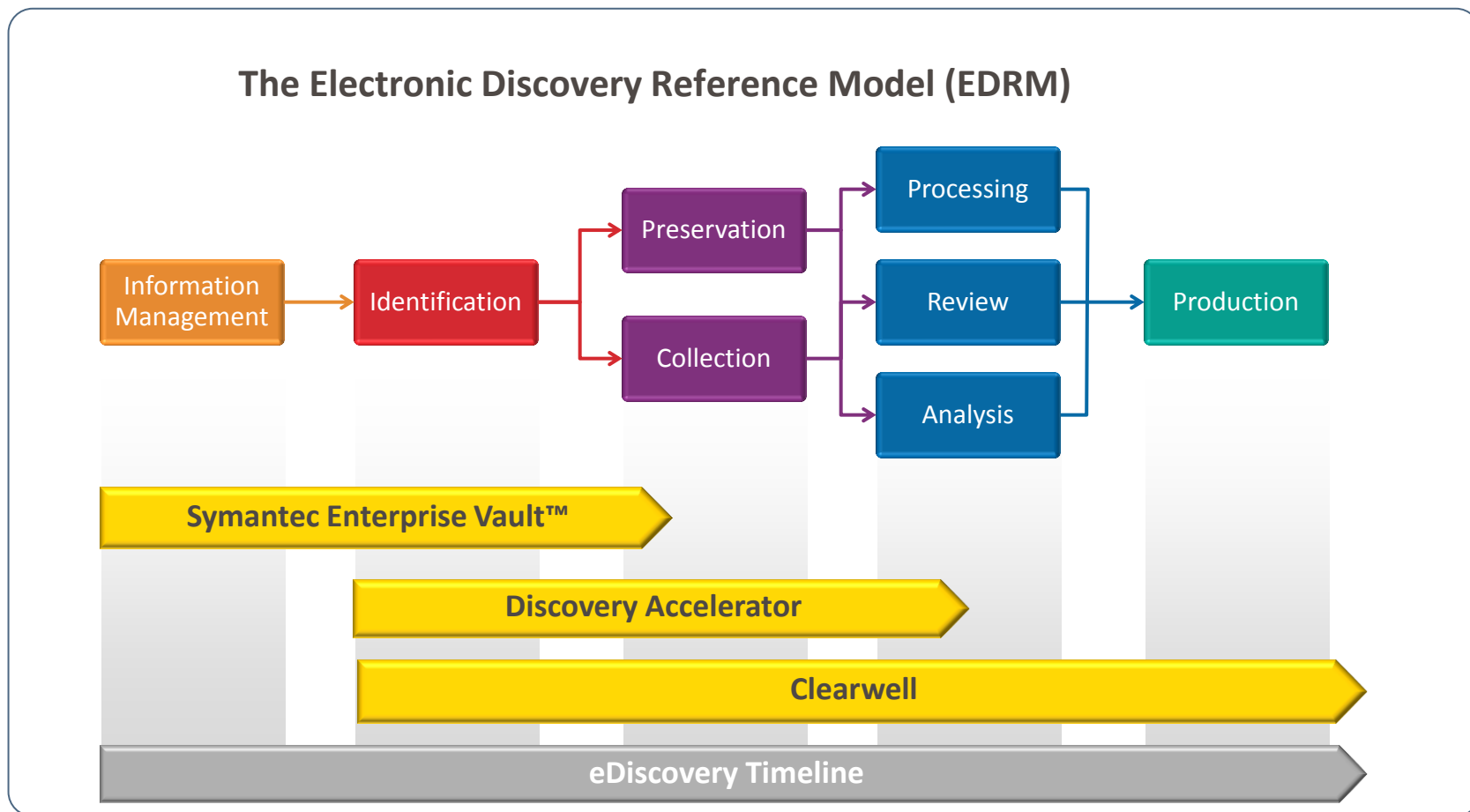
## Поиск

необходимого

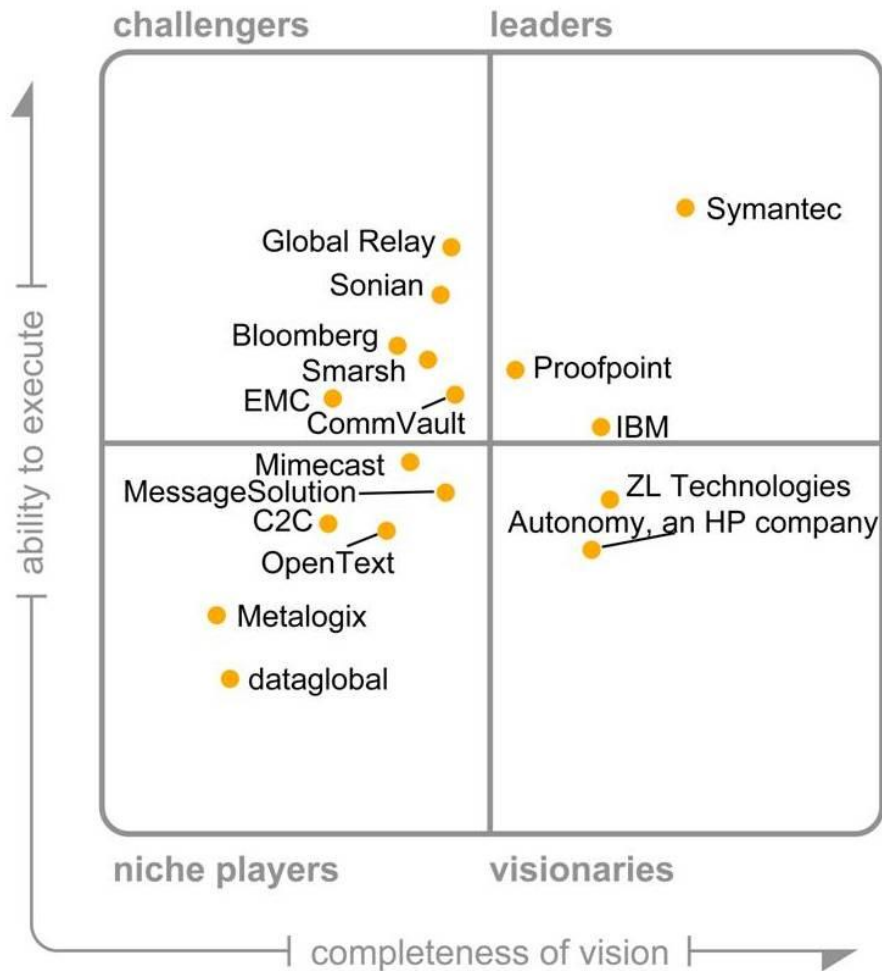
# Новый этап эволюции решений



# Решения Symantec относительно EDRM



# Symantec is Named a Leader in 2012 Gartner Magic Quadrant for Enterprise Information Archiving: Positioned Highest in Vision and Execution

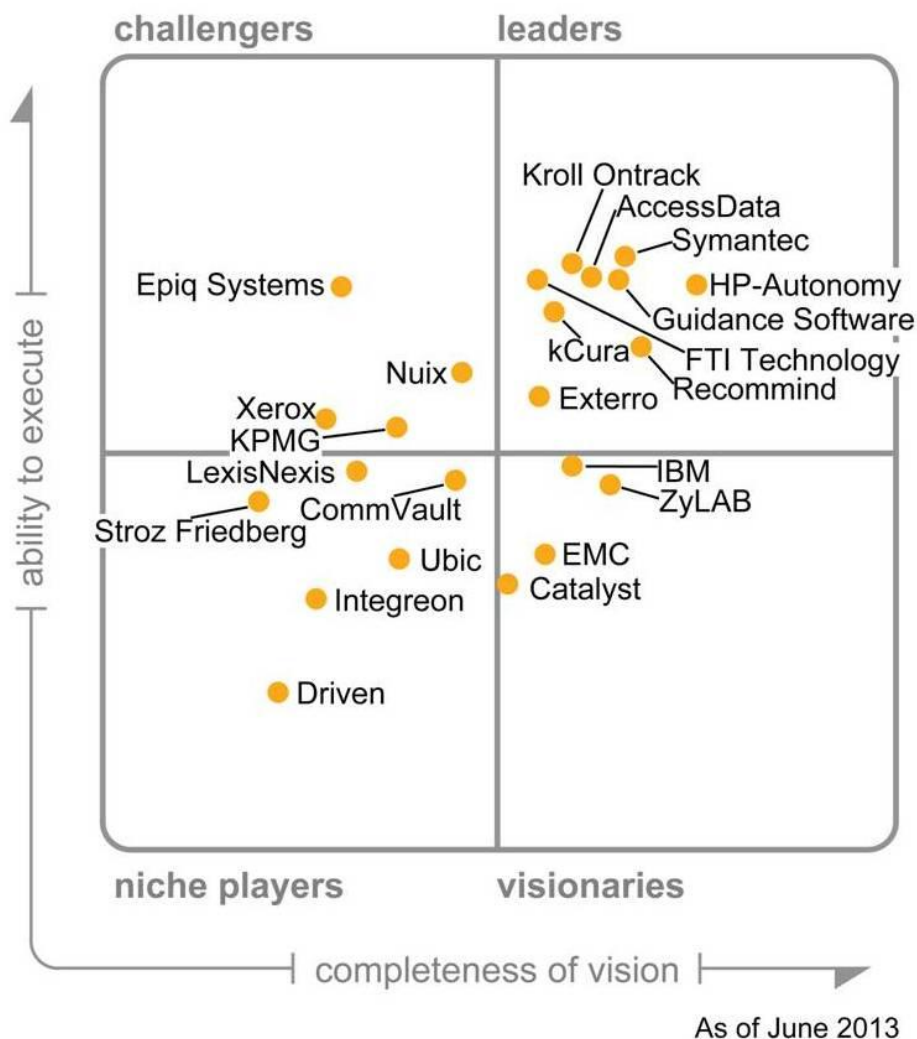


Source: Gartner, Inc., Magic Quadrant for Enterprise Information Archiving, Sheila Childs, Kenneth Chin, Debra Logan, Alan Dayley, December 13, 2012

This Magic Quadrant graphic was published by Gartner, Inc. as part of a larger research note and should be evaluated in the context of the entire report. The Gartner report is available upon request from Symantec. Gartner does not endorse any vendor, product or service depicted in our research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

As of December 2012

# Symantec is Named a Leader in 2013 Gartner Magic Quadrant for E-Discovery Software: Positioned Highest in Execution



Source: Gartner, Inc., Magic Quadrant for E-Discovery Software, Debra Logan, Alan Dayley, Sheila Childs, June 10, 2013

This Magic Quadrant graphic was published by Gartner, Inc. as part of a larger research note and should be evaluated in the context of the entire report. The Gartner report is available upon request from Symantec. Gartner does not endorse any vendor, product or service depicted in our research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose





# 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.