HYTRUST
Cloud Under Control

Решение HyTrust для защиты виртуальной инфраструктуры

Гольдштейн Андрей, менеджер по развитию бизнеса продуктов ИБ
agold@netwell.ru, +7 (967) 285-85-68

HyTrust, Inc

Mission: Mitigate the concentration of risk and potential for catastrophic failure that virtualization and cloud infrastructure introduces, enabling organizations to securely virtualize all workloads and move faster to the cloud.

Strategic Partners:

Investors:

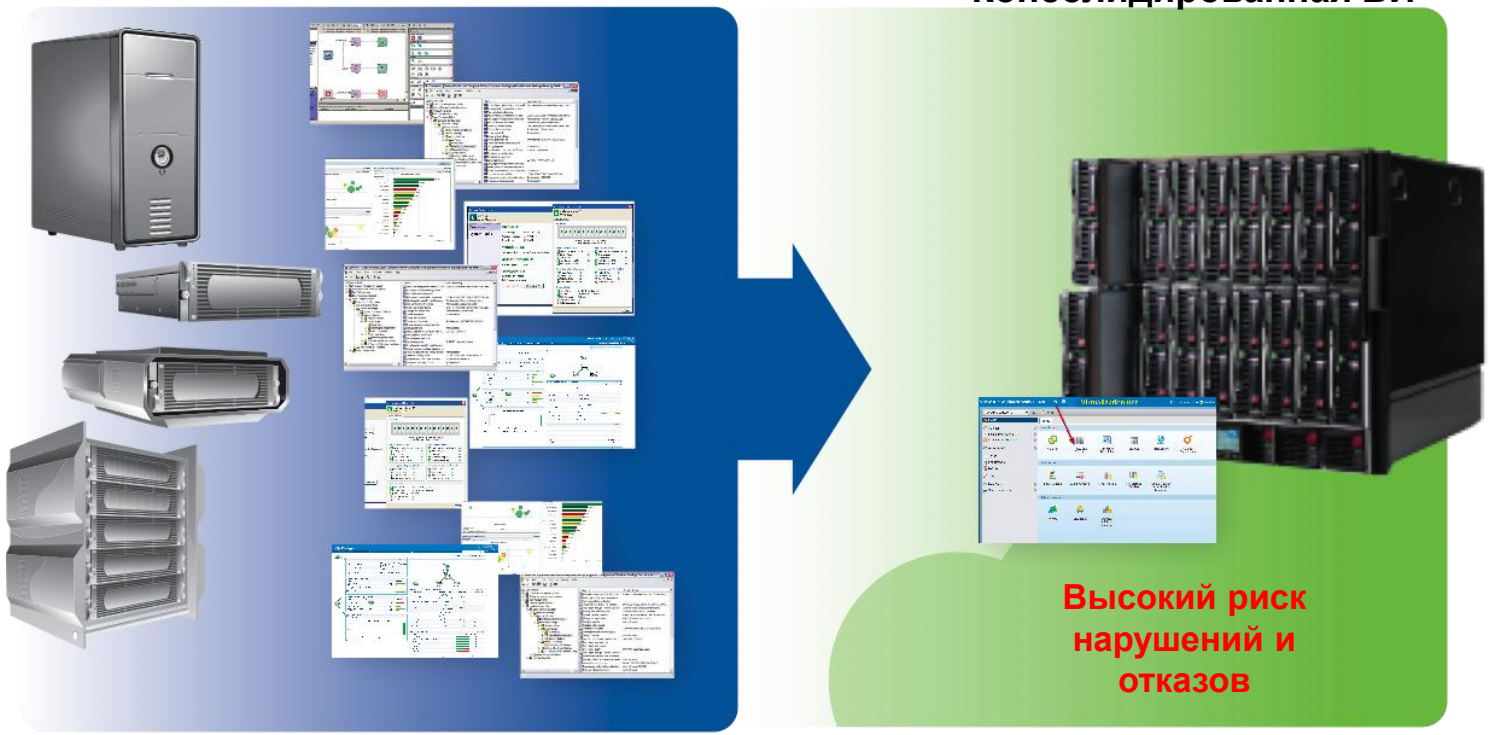
Strong IP Protection: Five foundational patents granted covering access control, hardening and logging for cloud infrastructure, automated tagging, policy enforcement based on tags, key management, and VM encryption.

Representative Customers:

С бОльшими возможностями приходит бОльшая ответственность…

Традиционные ЦОД

Частное облако
Консолидированная ВИ



10,000 серверов, 1,000 свичей & рутеров
Управляется из различных мест
различными людьми

Вся инфраструктура (более 10,000+
компонентов) в 1 системе, управляется
неконтролируемым администратором с
высокими привилегиями

Лучшие практики от экспертов

- “**Ограничить и защитить административный доступ** в виртуализированной инфраструктуре”
- “**Защитить каждый интерфейс управления**”
- “**Мониторить и анализировать логи** на всех уровнях виртуальной инфраструктуры”[1]

NIST National Institute of Standards and Technology U.S. Department of Commerce

- “**Уменьшить уровень привилегий и разделить обязанности**”
- **“Критичным моментом должно стать логирование всей активности отдельным решением**”
- “**Требование многофакторной аутентификации** для всех административных функций”[2]

PCI Security Standards Council

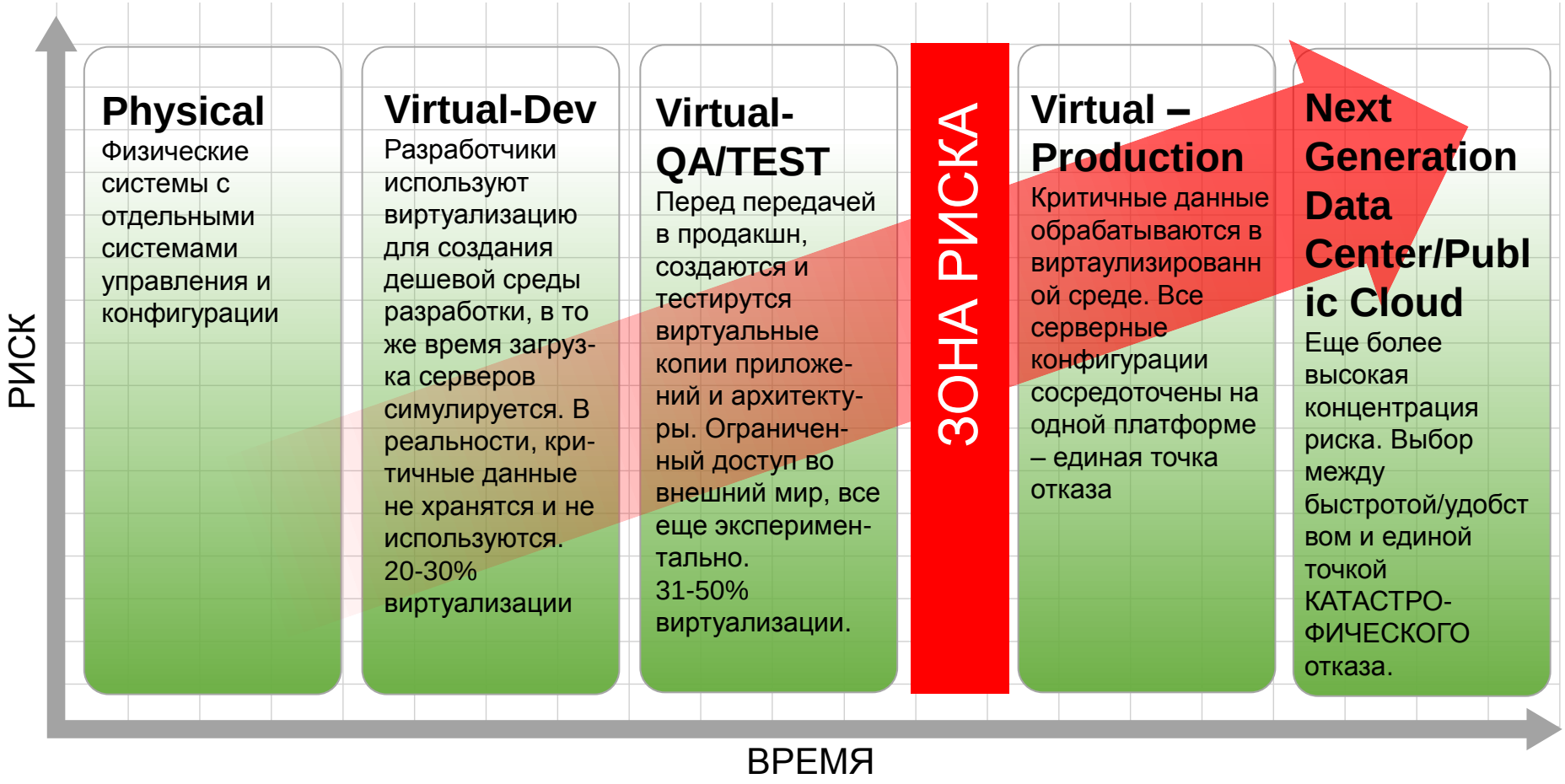
- “**Административный доступ к гипервизору должен жестко контролироваться**”[3]

Gartner

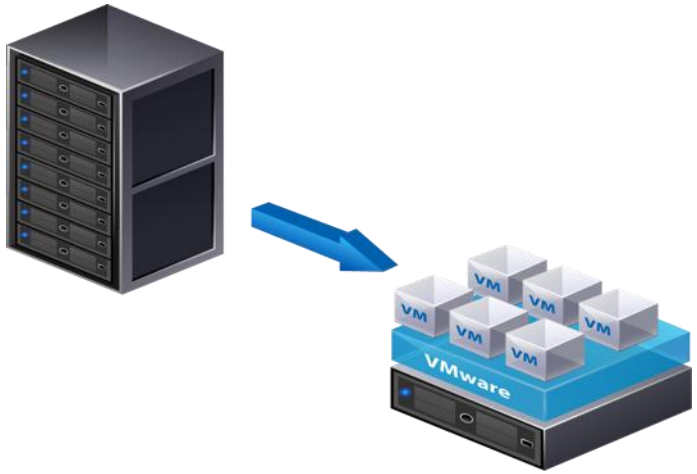
[1] NIST SP 800-125: Guide to Security for Full Virtualization Technologies
[2] PCI-DSS 2.0 Information Supplement – Virtualization Security
[3] Neil MacDonald, vice president and Gartner fellow

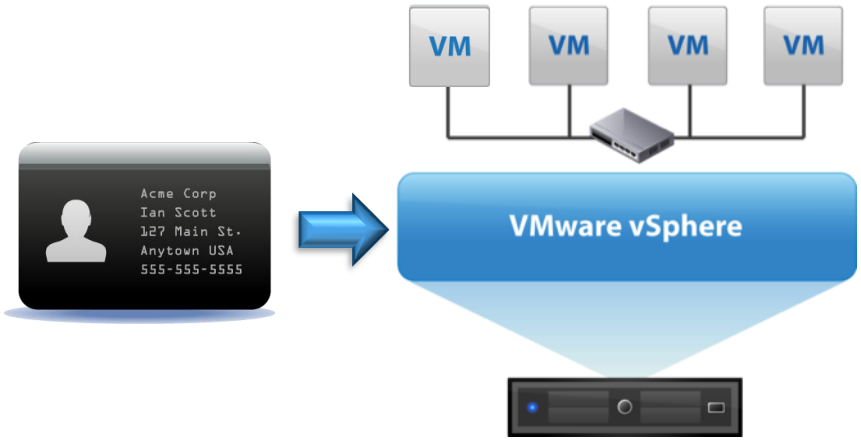
Виртуализация и сосредоточение риска

Только соответствующий контроль может помочь компаниями избежать «зоны риска»



Риски при работе с VMware





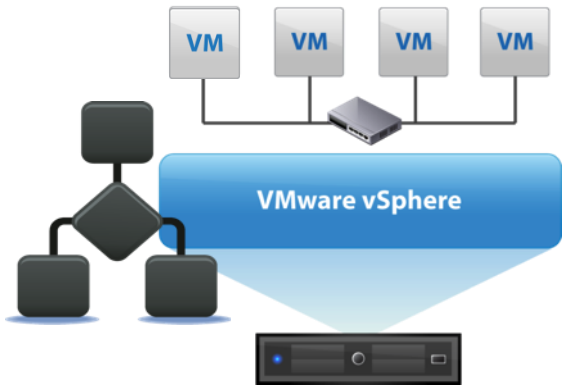
Поддержка целостности среды

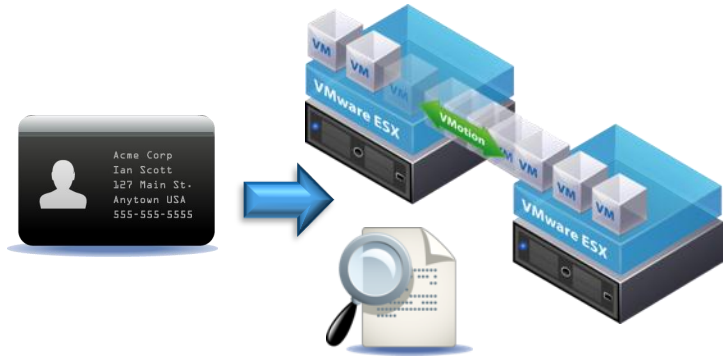
- ↓ Новый тип среды
- ↓ Любая компрометация на этом уровне может поставить под угрозу всю инфраструктуру
- ↓ Последствия атак серьезнее в следствии консолидации ресурсов
- ↓ Сложность проверки целостности среды

Контроль привилегированного доступа

- ↓ Прямой доступ (root, ssh) обходит аутентификацию в vCenter
- ↓ Учетная запись root зачастую используется сразу несколькими сотрудниками
- ↓ Нет поддержки многофакторной аутентификации

Риски при работе с VMware





Применение политик

- ↓ Нет контроля прямых команд к хосту
- ↓ Отсутствие гранулированных настроек политик
- ↓ Остутствие технологии маркирования объектов
- ↓ Отсутствие возможности подтверждения доступа «по запросу»

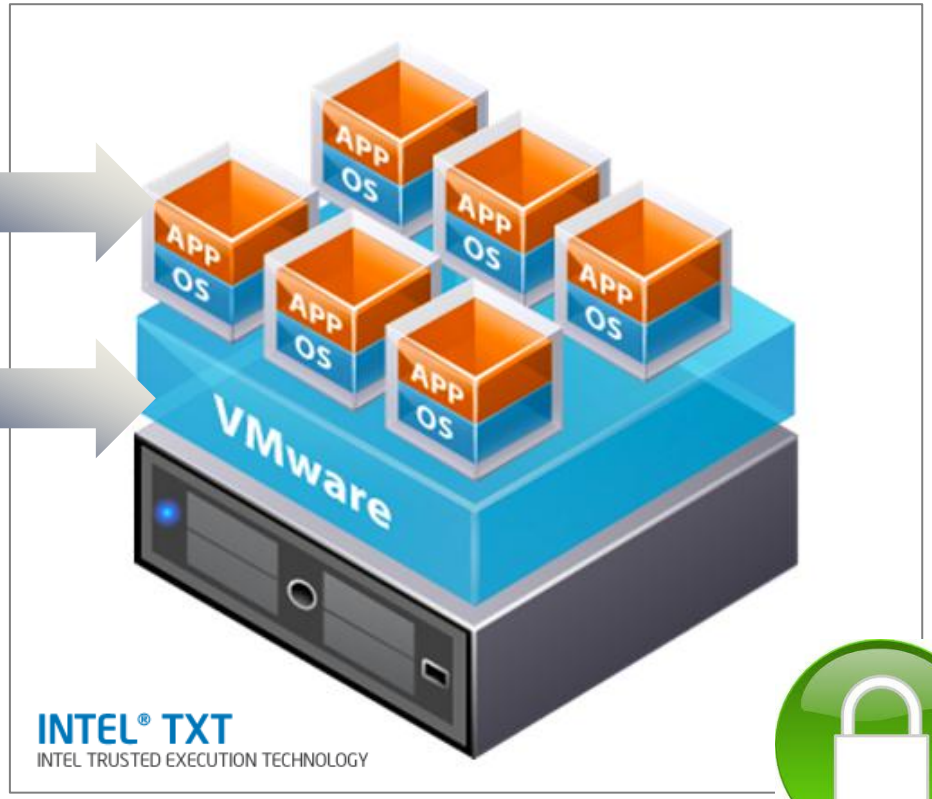
Ограниченная видимость и аудит

- ↓ Штатное логгирование vCenter не фиксирует все предпринятые изменения, IP-адреса
- ↓ Остутствие детализации по параметрам хоста
- ↓ Без централизованной системы анализ, корреляция и хранение логов затруднительны

Комплексный подход к виртуализации дата-центров

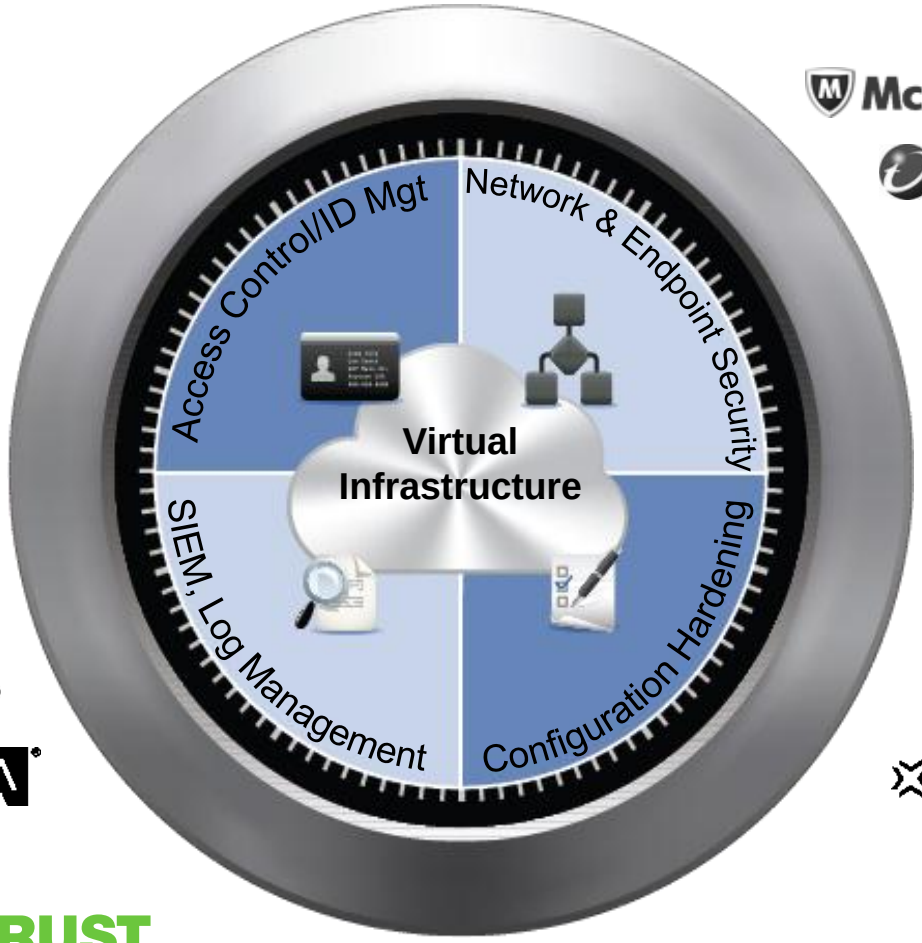
Защита сети и конечных станций от VMware, McAfee, и других

HyTrust® Appliance защищает саму виртуальную инфраструктуру (hypervisor, network, storage, TXT)



При защите виртуальных инфраструктур требуется комплексный подход, от классической защиты до специализированных средств контроля среды виртуализации

Ключевые аспекты защиты ВИ – “The 4 Must Haves”



HYTRUST Cloud Under Control

McAfee

catbird

TREND MICRO

paloalto NETWORKS

JUNIPER

Symantec

vmware

CISCO

McAfee

Labs

splunk>

ArcSight

RSA

HYTRUST Cloud Under Control

vmware

reflex

HYTRUST Cloud Under Control

HyTrust: Защита ЦОД нового поколения

Защита гипервизора и ВИ:

Рациональный подход к безопасности

- Ролевая и объектная модель мониторинга, оповещение на основе контекстного анализа
- Ролевая и объектная модель доступа, в том числе привилегированного
- Детальный лог аудита
- Поддержка усиленной многофакторной аутентификации
- Проверка целостности платформы

Благодаря мониторингу в режиме реального времени, логированию и контролю облачной инфраструктуры HyTrust, вы можете получить огромные преимущества от консолидации при этом оставаясь защищенным от рисков визуализации.

Преимущества HyTrust: Безопасный переход к виртуализации

Для бизнеса …

- *Безопасная* виртуализация всех ресурсов с защитой от неприемлемых рисков
- Быстрая готовность к переходу к виртуальной инфраструктуре

Для управления рисками …

- Визуализация и контроль в режиме реального времени
- Защита от плохих актеров в разделении обязанностей и доступом с низшими привилегиями
- Жесткая изоляция любой нагрузки в мультиарендном облаке
- Быстрое детектирование злонамеренного использования привилегированных учетных записей
- Защита администратора от компрометации
- Выполнение требований аудиторов

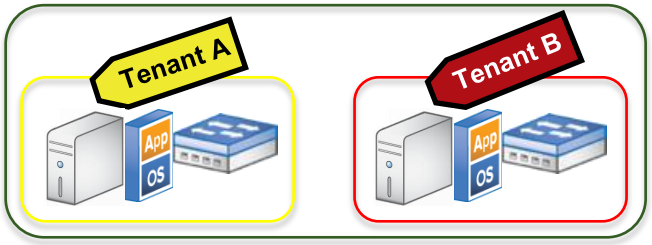
4 Ways HyTrust CloudControl Secures Management Plane

1. Strong Authentication

3. Audit-Quality Logging

Date	Priority	User	Operation	Resource Name	Resource Type	Status
11/12/2013 10:45:53 AM	INFO	ken	ReconfigVM_Task	client.demo.hytrust.com	VM	PERMIT
11/12/2013 9:44:44 AM	INFO	ken	ReconfigVM_Task	HighCloud VMV	VM	PERMIT
11/05/2013 9:16:50 AM	WARN	ken	ReconfigVM_Task	Accounts Payable	VM	DENY

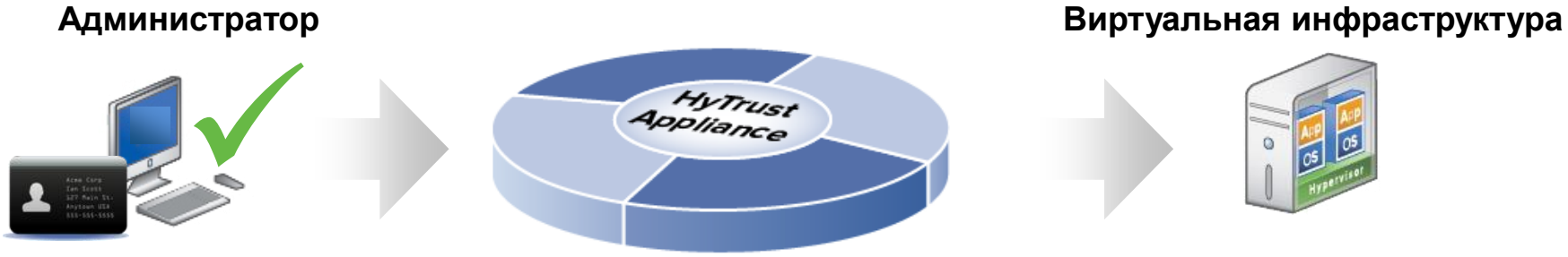
2. RBAC, Smart-tagging, Secondary Approval



4. Infrastructure Hardening with Root Password Vaulting

Description	Date/Time	Result
Verify Image Profile and VIB Acceptance Levels	11/12/2013 3:16:03 PM	Passed
Ensure that vpxuser password meets length policy	11/12/2013 3:16:05 PM	Passed
Ensure that vpxuser auto-password change meets policy.	11/12/2013 3:16:07 PM	Passed
Set a timeout for the ESXi Shell to automatically disabled idle sessions after a predetermined period	11/12/2013 3:16:10 PM	Passed
Disable DCUI to prevent local administrative control.	11/12/2013 3:16:10 PM	Passed
Disable SSH	11/12/2013 3:16:10 PM	Passed
Disable ESXi Shell unless needed for diagnostics or troubleshooting.	11/12/2013 3:16:10 PM	Passed
Limit sharing of console connections. Expected value is either 1 or 2	11/12/2013 3:16:10 PM	Warning
disable VM-to-VM communication through VMCI.	11/12/2013 3:16:10 PM	Warning
Do not send host information to guests	11/12/2013 3:16:10 PM	Warning

Проверка личности и аутентификация: Централизованная система для всего привилегированного доступа



- Последовательная, централизованная аутентификация
- Поддержка всех методов и протоколов (vSphere Client, web client, SSH, etc.)
- 2x факторная аутентификация (RSA SecurID, CA ArcotID, Smart Card), интеграция с Active Directory для использования существующей инфраструктуры
- Root passwords “vaulted”, гранулированный временный доступ к хостам, исключение практики использования одной учетной записи разными пользователями

“With HyTrust Appliance in place, Denver Museum of Natural Science has been able to limit access to virtual infrastructure at an extremely granular level, determining what systems can be accessed by whom.”

Ограничение и контроль доступа:
Детальный контроль над пользователями и объектами ВИ

- “Метки” для объектов (хосты, виртуальные машины, свичи) для классификации
- Использование метаданных инфраструктуры и партнеров HyTrust для расширения политик доступа
- Применение политик доступа в информационной инфраструктуре для соответствия политиками компании в области безопасности и соответствии требованиям регуляторов
- Требования второго подтверждения для отдельных операций, для предотвращения дорогостоящих ошибок

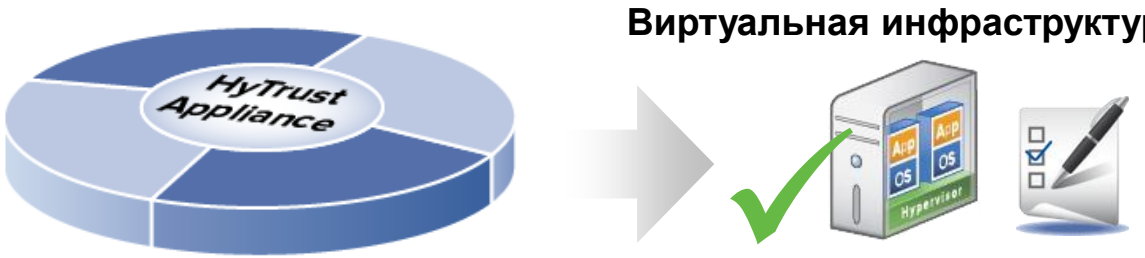
“As CEO, what I find exciting about HyTrust is that it enables companies like ours to have the best of both worlds: improved margins from cutting-edge virtualization alongside secure customer information, satisfied auditors, and happy board members,” said Mike Heinstein, CEO of Art.com.

Мониторинг активности:
Полная запись всего административного доступа

- Гранулированный, по пользователям, читабельный журнал всей активности виртуальной инфраструктуры (включая доступ root)
- Обеспечение мониторинга, оповещения, поиска неисправностей, процесса разбора инцидентов и т.д..
- Экспорт в Syslog и rSyslog (SIEM и т.д.)
- Глубокая корреляция и интеграция с решениями CA ELM, RSA enVision и Splunk

Council of Europe Development Bank tried using VMware's logging capabilities but needed a better way to consolidate the information. "Getting at those logs was nontrivial so we ended up using HyTrust to provide a central log of all activity."

Проверка целостности ВИ



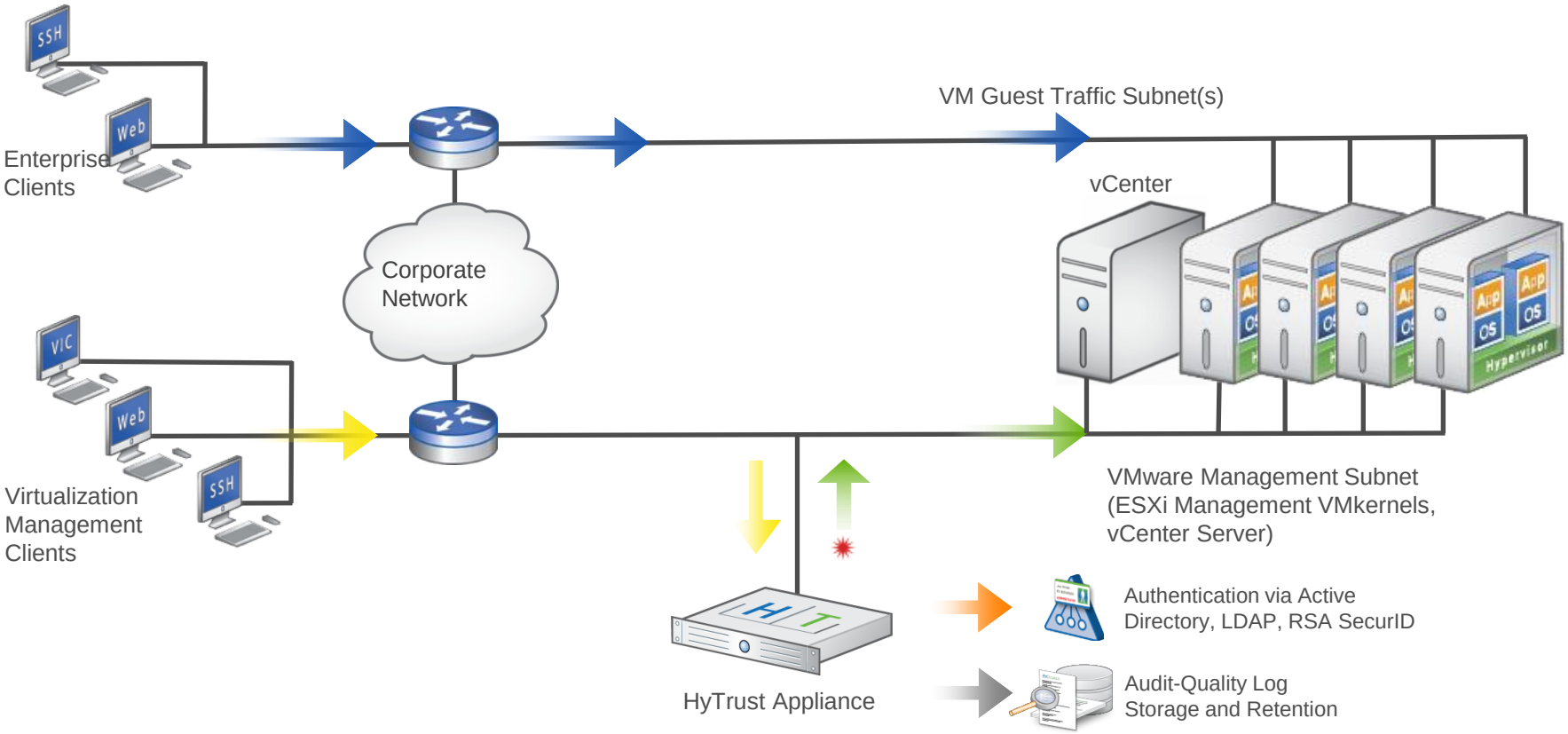
- Сбор текущего состояния виртуальной инфраструктуры
- Анализ целостности гипервизора за счет предустановленных темплейтов, таких как PCI-DSS, VMware Best Practices, и C.I.S.
- Возможность решения проблем с конфигурациями без перевода гипервизора в режим отладки
- Контроль доверенной загрузки оборудования за счет технологии Intel TXT

“This solution is ideal for managing access to our records and other critical data.”
- Gurusimran Khalsa, Systems Group Supervisor, State of New Mexico

Ключевые преимущества для заказчиков

- Получение полной видимости и контроля над ВИ
  - Логическая сегментация обеспечивает мультиарендность; Критичные сервисы могут функционировать в той же инфраструктуре
  - Разделение задач в облачной инфраструктуре
  - Журналирование и аудит
- Соответствие требованиям регуляторов
  - Контроль и журналирование для виртуализации критичных процессов
  - Снижение затрат на аудит соответствия требованиям регуляторов
- Повышение эффективности ИТ среды
  - Эффективное управление виртуальной инфраструктурой за счет автоматизации процессов и процедур

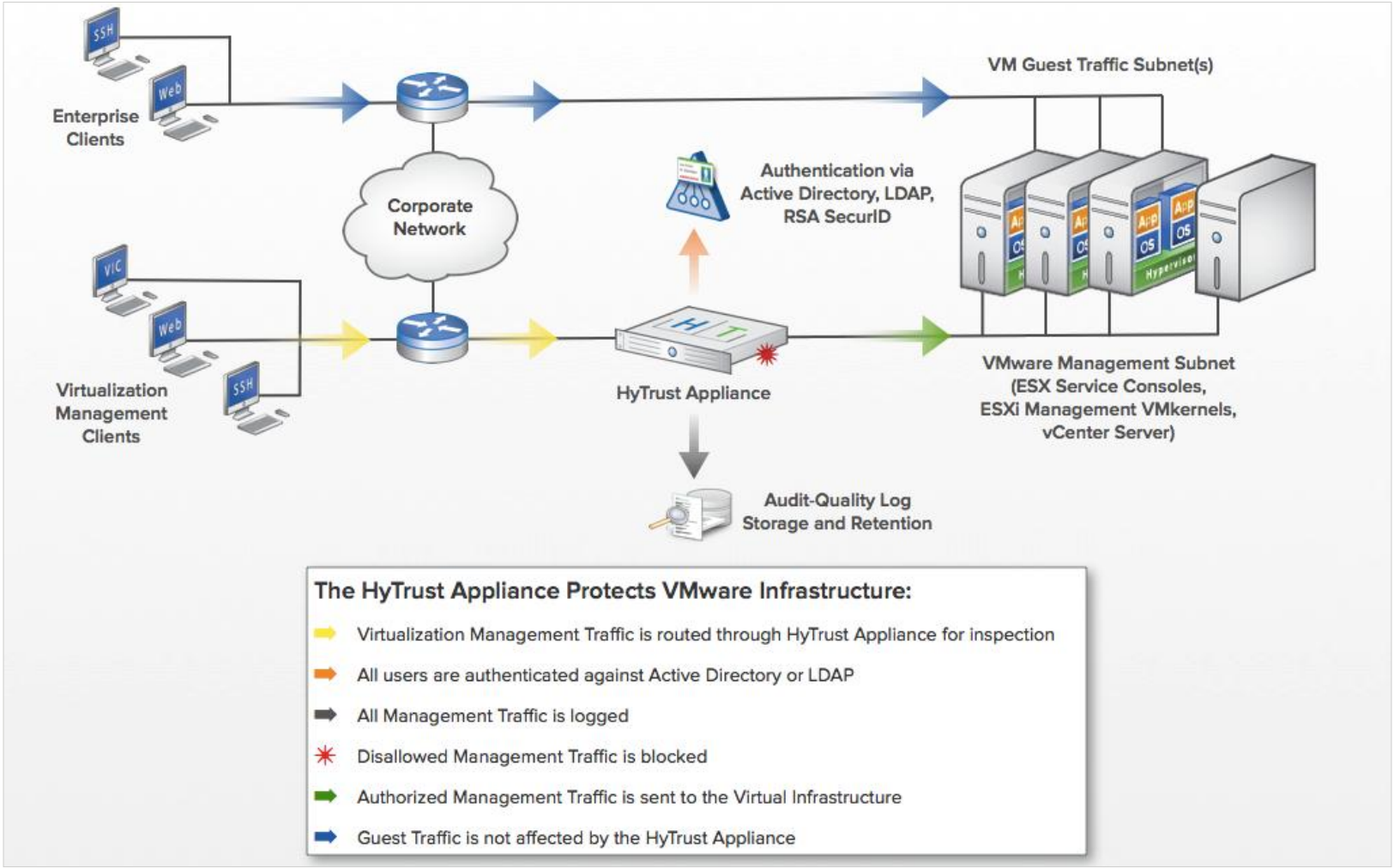
Внедрение системы HyTrust в режиме перенаправления трафика



The HyTrust Appliance Protects VMware Infrastructure:

- Virtualization Management Traffic is connected to Published IP and routed through HyTrust Appliance for inspection
- All users are authenticated against Active Directory
- All Management Traffic is logged
- Disallowed Management Traffic is blocked
- Authorized Management Traffic is sent to the Virtual Infrastructure
- Guest Traffic is not affected by the HyTrust Appliance

Внедрение системы HyTrust «в разрыв»



HYTRUST
Cloud Under Control

Вопросы?