Банковские системы на стадии эксплуатации. Актуальные угрозы информационной безопасности и средства обеспечения защиты

Александр Суязов

Технический консультант

Виртуализированные сервисы

Невиртуализированные сервисы

Статичные сервисы (банкоматы, киоски и т.д.)
Наследуемые приложения

Виртуализированные сервисы

- Легкое создание новых/модификация имеющихся
- Практически любые ОС (от очень старых до самых новых)
- Высокая доступность
- Критично распределение ресурсов
- Только современное АО
- Только архитектура x86

- Безагентский/Файловый антивирус

Виртуализированные сервисы

- Защита средств виртуализации от атак
- Более жёсткий контроль администраторов виртуальной инфраструктуры
- Автоматизация базовой защиты виртуальных машин
- Защита сервисов на основе политик
- Снижение нагрузки на виртуальную инфраструктуру за счет отказа от клиентского антивируса

Невиртуализированные сервисы

- Тяжелые сервисы
- Редко меняются
- Сервисы, не поддерживающие виртуализацию
- Любое АО (от старого до ультрасовременного)
- Любые платформы (от x86 до RISC)
- Любые ОС
- Часто высокие требования к времени простоя

- От файлового антивируса до отсутствия средств защиты

Невиртуализированные сервисы

- Единая централизованно управляемая защита на уровне агента
- Жесткий контроль привилегий и взаимодействия процессов
- Работа для большом количестве ОС
- Управление через политики
- Мониторинг/защита

Статичные сервисы

- Не модифицируются в течении срока жизни/срока обслуживания
- Устаревшее ПО/ОС
- Устаревшее/слабое АО
- Слабые каналы связи

- Антивирус/белые списки

Статичные сервисы

- Создание неизменяемой среды при установке ПО
- Отказ от антивируса
- Минимальное влияние на производительность

Виртуализированные сервисы

Невиртуализированные сервисы

Статичные сервисы

Виртуализированные

Единое решение для защиты

Статичные сервисы

Symantec.

Виртуализированные сервисы

Невиртуализированные сервисы

Статичные сервисы

Data Center Security: Server 6.0

- Интеграция с платформой VMware NSX
  - Безагентская антивирусная защита
  - Репутационные технологии для снижения ложных срабатываний
  - Автоматическая масштабируемость при росте виртуальной инфраструктуры

Data Center Security: Server Advanced 6.0

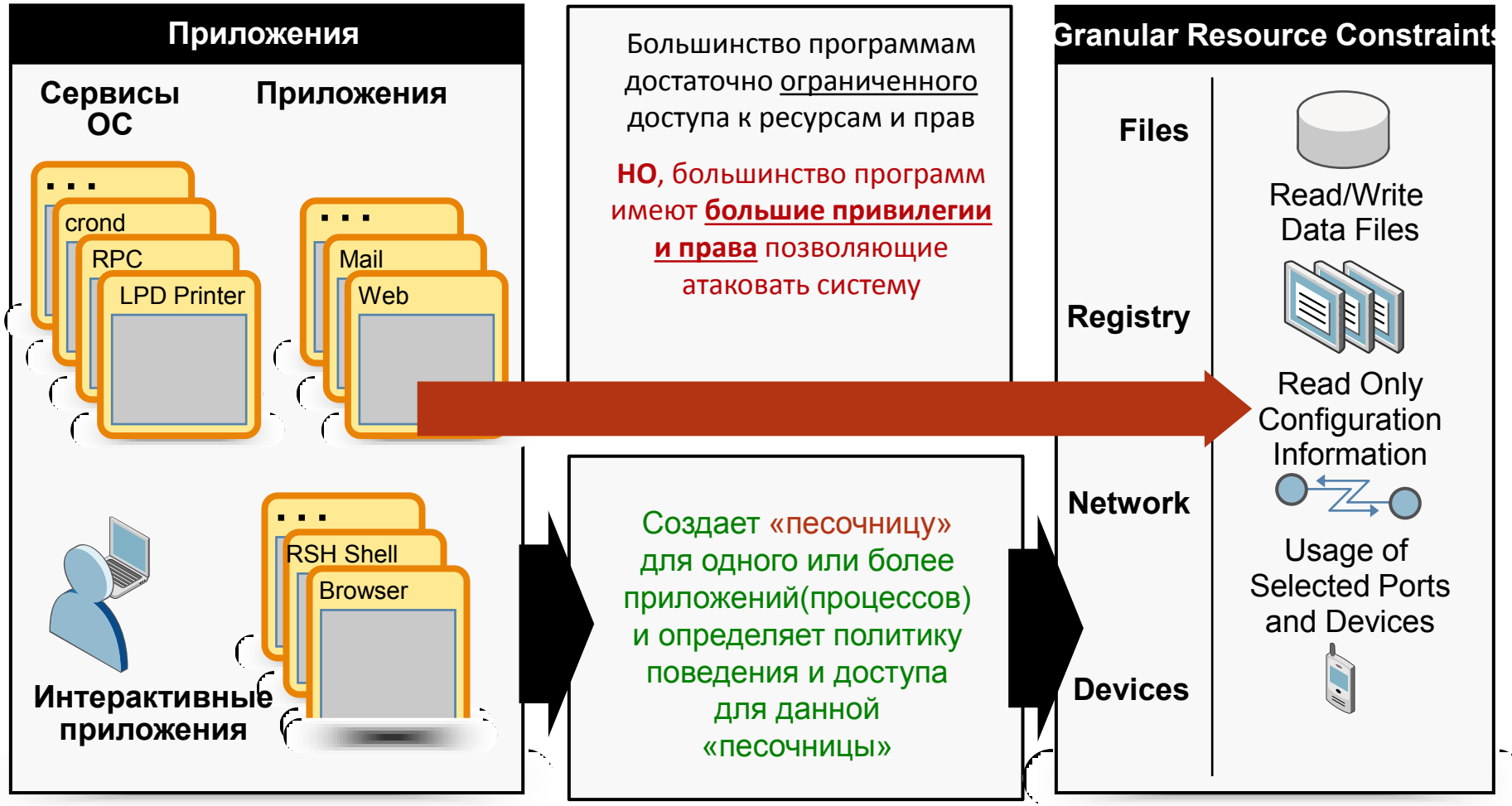
- Дополнительная защита к существующей в Data Center Security: Server
- Упрощенная защита серверов
  - Визард для построения политик защиты
    - Обнаружение приложений и встроенная репутация
    - Преднастроенные песочницы для общеизвестных сервисов: контроллеры доменов, базы данных, почтовые и веб-сервера

Data Center Security: Server Advanced

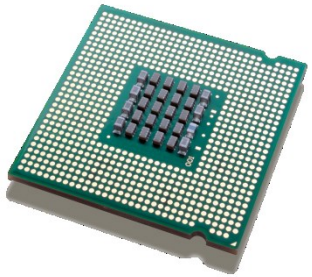
Поведенческий контроль	Контроль системы	Сетевая защита	Аудит Оповещения
Prevention			Detection
• Ограничение приложений и ОС на основе поведения • Защита от переполнения буфера • Белые списки • Защита от атак нулевого дня • Защита от эксплойтов	• Контроль файлов настроек • Применение политик безопасности • Понижение прав пользователей • Ограничение внешних носителей • Защита vSphere	• Ограничение доступа приложений в сеть • Ограничение исходящего и входящего трафика • Блокировка бэкдоров (блокировка портов)	• Мониторинг логов и событий безопасности • Объединение логов и передача для хранения и отчетности • Мониторинг целостности файлов в режиме реального времени • Настройка действий по событиям

Symantec.

Data Center Security использует «песочницы» для ужесточения настроек серверов



Использование ресурсов агентом Data Center Security



Потребление CPU: 1 – 6%

Потребление RAM: 20 – 40MB

Потребление HDD: 100MB

Symantec Server Protection
Un-compromised at Black Hat 2011 and 2012

Proven Security at "Capture The Flag" Challenges

- **Challenge:**
  - 'Flags hidden across un-patched Windows and Linux systems
  - Main flag protected with CSP and SEP out-of-the box prevention policy
  - 50+ skillful hackers/pen-testers from DoD, NSA, DISA, Anonymous, etc.

- **Attacks Techniques used:**
  - Backtrack 5 and custom tools used during penetration attempts
  - Zero day attack used and stopped on protected system
  - Recompiled version of Flamer stopped by CSP out of the box policy

- **Outcome:**
  - No one was able to capture the flag… now two years in a row…
  - Hackers said if they would have known that **Sandboxing** and **Whitelisting** was used, maybe not worth the time they put into it

Payment Card Industry (PCI)

- **Безопасность**
  - Protects PCI card data
  - Protects PCI servers from compromise (Req 5, 11)
  - Controls network access to PCI devices (Req 1)
  - Limit access to system components (Req 7)
- **Видимость**
  - Track and monitor user access (Req 10)
  - Use file integrity monitoring (Req 13)

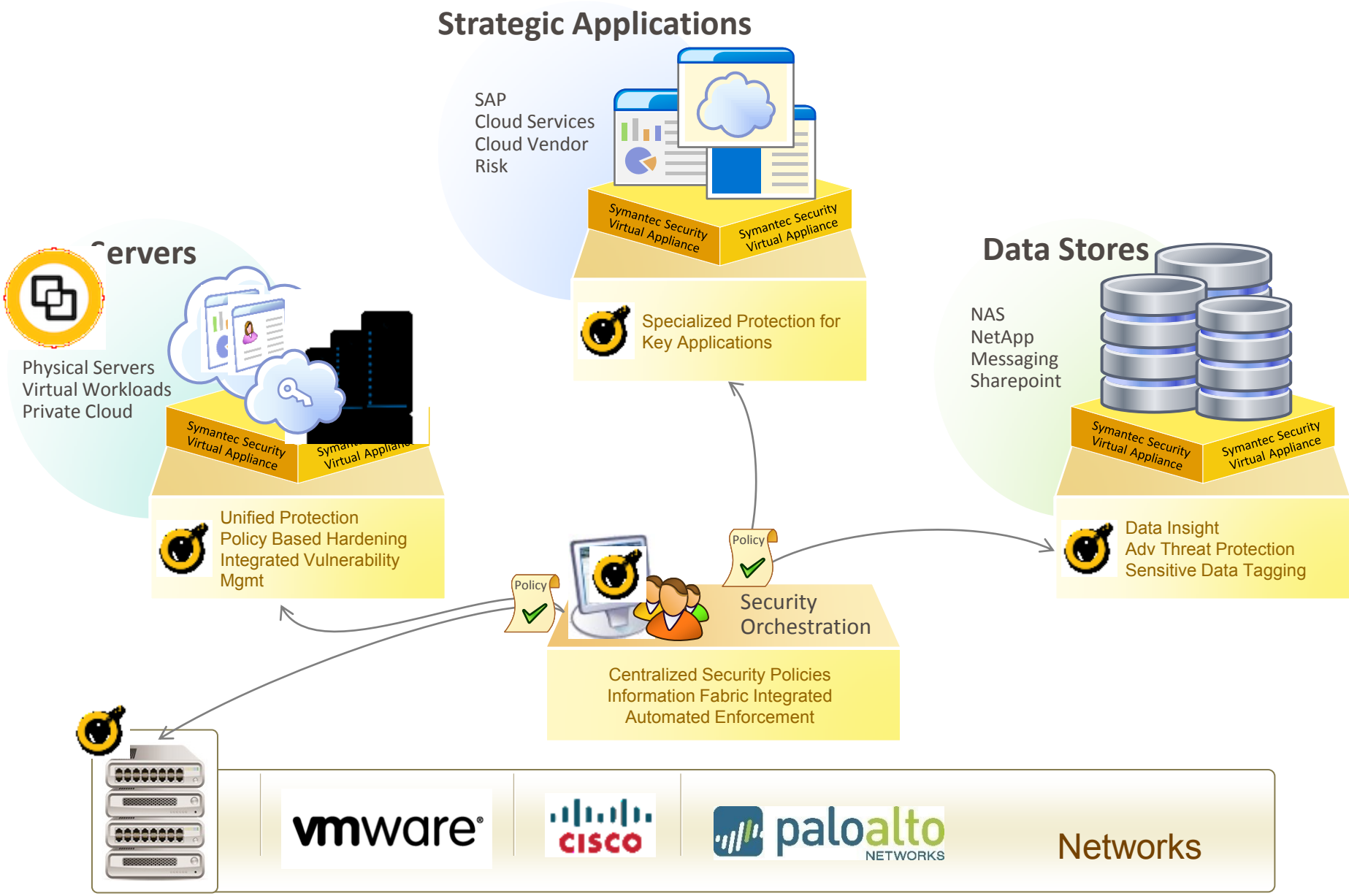
Виртуализированные сервисы

- Автоматизация базовой защиты виртуальных машин
- Защита сервисов на основе политик
- Снижение нагрузки на виртуальную инфраструктуру за счет отказа от клиентского антивируса

Как обеспечить безопасность виртуализации ?

SYMANTEC VIRTUALIZATION SECURITY MANAGER

- Строгая многофакторная аутентификация
- Детализированное журналирование
- Политики доступа
- Контроль конфигураций


Strategic Applications
SAP
Cloud Services
Cloud Vendor
Risk
Symantec Security Virtual Appliance
Symantec Security Virtual Appliance
Specialized Protection for Key Applications
ervers
Physical Servers
Virtual Workloads
Private Cloud
Symantec Security Virtual Appliance
Unified Protection
Policy Based Hardening
Integrated Vulnerability Mgmt
Data Stores
NAS
NetApp
Messaging
Sharepoint
Symantec Security Virtual Appliance
Symantec Security Virtual Appliance
Data Insight
Adv Threat Protection
Sensitive Data Tagging
Policy
Policy
Security Orchestration
Centralized Security Policies
Information Fabric Integrated
Automated Enforcement
vmware
cisco
paloalto NETWORKS
Networks

Спасибо!

alexander_suyazov@symantec.com

Тел: +7 (495) 6628300