



РЕШЕНИЕ LANDESK TRUSTED ACCESS

Алексей Лукацкий

Security Business Development Manager

Содержание

- **Общая проблема ИТ и ИБ**
- **Технология контроля сетевого доступа**
- **LANDesk Trusted Access**
- **Cisco Network Admission Control (NAC)**
- **Альянс Cisco, LANDesk и Microsoft в области безопасности**
- **Альянс Cisco, LANDesk и Intel в области безопасности**

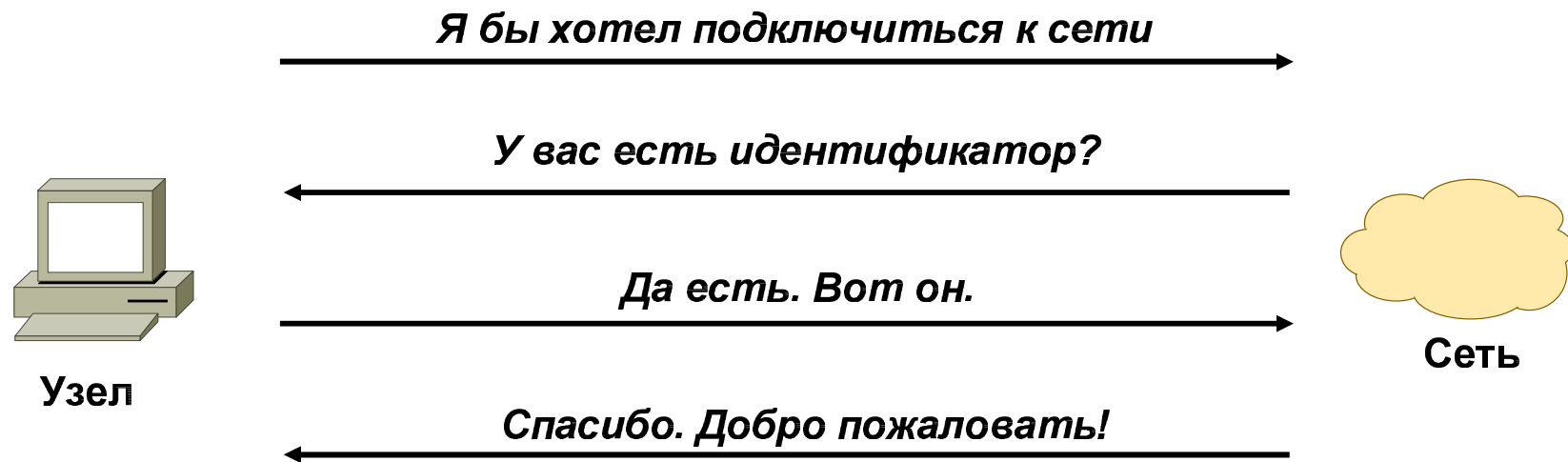
ОБЩАЯ ПРОБЛЕМА ИТ И ИБ



Проблема управления узлами

- **Сложность внедрения и контроля политик на тысячах узлов**
- **Несоответствие узлов требованиям политики ИТ и ИБ**
 - Собственные узлы и узлы внешних организаций**
- **Результат:**
 - Эпидемии вредоносных программ**
 - Несанкционированный доступ**
 - Отсутствие патчей и обновлений**
 - Отсутствие необходимого ПО**

Типовая модель подключения к ресурсу



- **Что осталось «за кадром»?**

Наличие определенных приложений и их статус

Наличие патчей и обновлений

Актуальность антивирусной базы данных

Настройки подсистемы защиты

Как расширить типовую модель?

- Проверять «здоровье» и статус узлов, подключаемых извне
- Быть уверенным в защищенности внутренних узлов сети
- Проверять «здоровье» и соответствие политике узлы удаленных офисов, подключаемых через VPN
- Проверять «здоровье» компьютеров посетителей
- Проверять «здоровье» и соответствие политике домашние компьютеры сотрудников

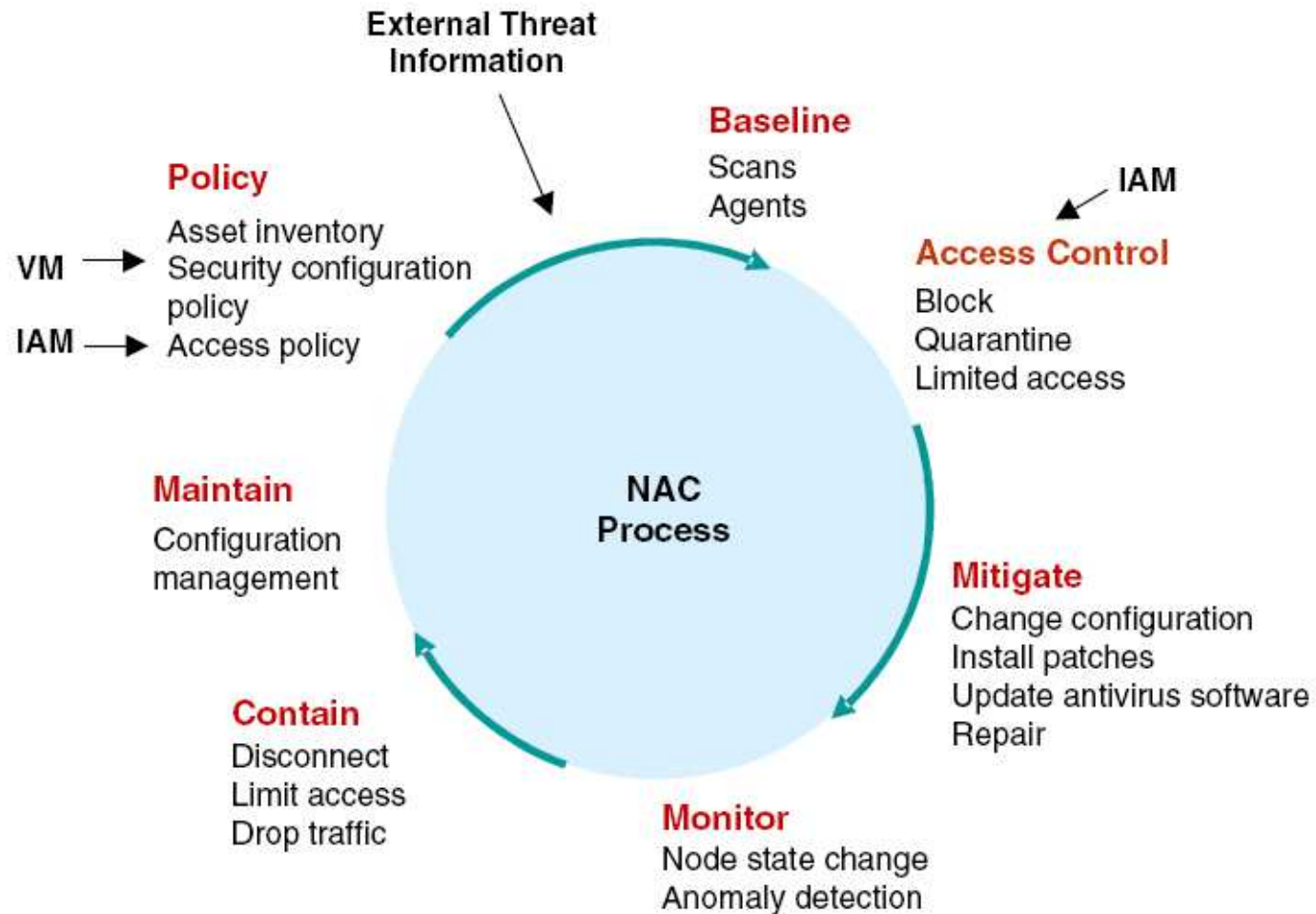
Что значит несоответствие политике?

- **Отсутствуют необходимые патчи и обновления**
- **Настройки подсистемы безопасности ОС или приложений не соответствуют требованиям**
Например, длина пароля меньше 8 символов
- **Нет антивируса, VPN-клиента или другой системы защита**
- **Система защиты установлена, но не запущена**
- **Антивирусная база не актуальна**

NETWORK ACCESS CONTROL



Network Access Control



IAM = identity and access management
VM = vulnerability management

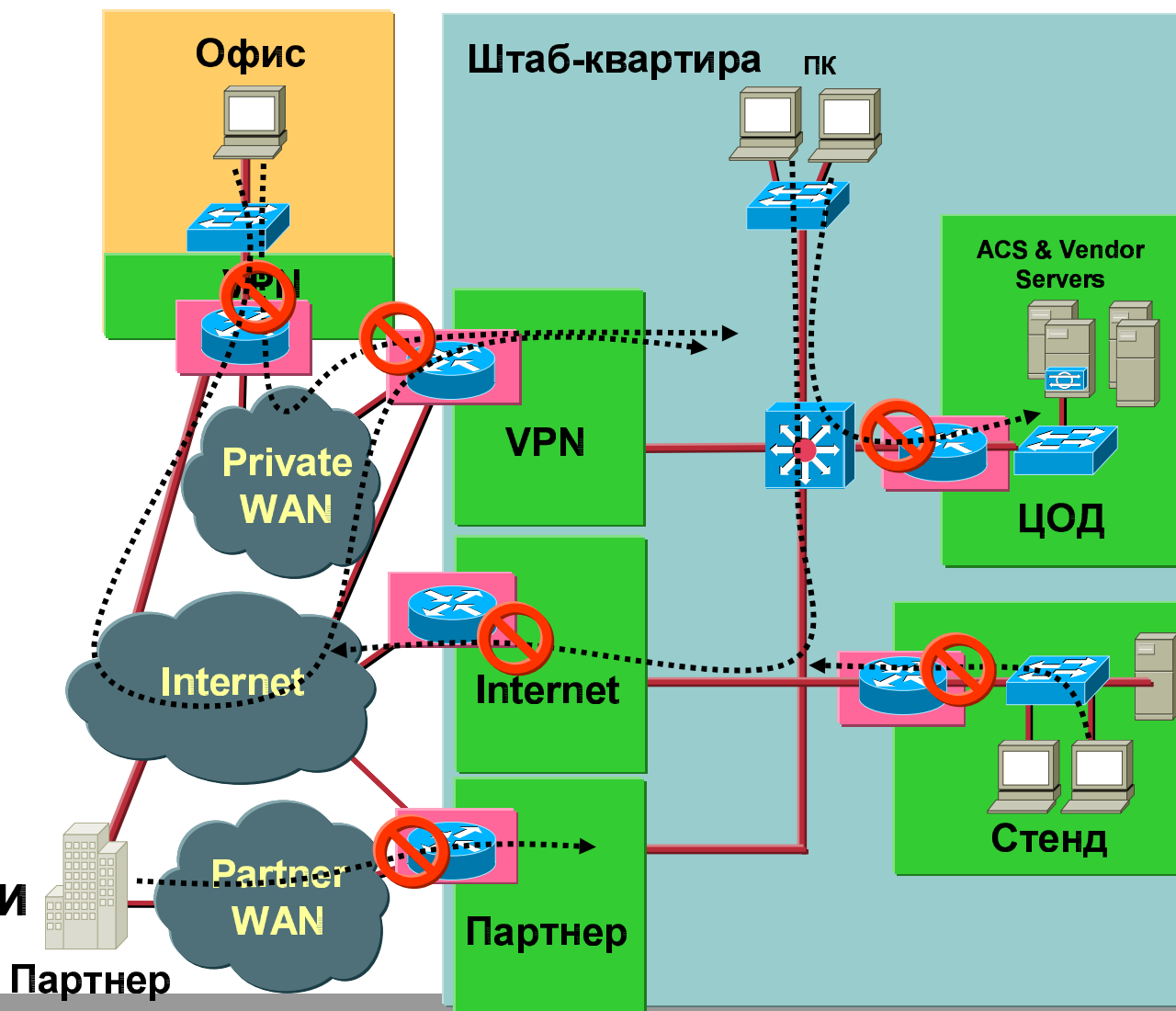
Source: Gartner Research (December 2004)

Как должно быть?

- Разрешать подключение к сети **только аутентифицированным пользователям и устройствам**
- Разрешить администраторам устанавливать **политику безопасности**
- **Проверять конфигурацию устройств** на соответствие политике безопасности до получения доступа к запрошенным ресурсам
- **Обнаружение несоответствующих политике узлов**
- **Карантин** для несоответствующих узлов
- **«Лечение»** несоответствующих устройств

Сценарии внедрения

- Удаленные офисы
- Партнеры (экстранет)
- Интернет
- Стенд
- Центр обработки данных
- Мобильные пользователи



LANDESK TRUSTED ACCESS



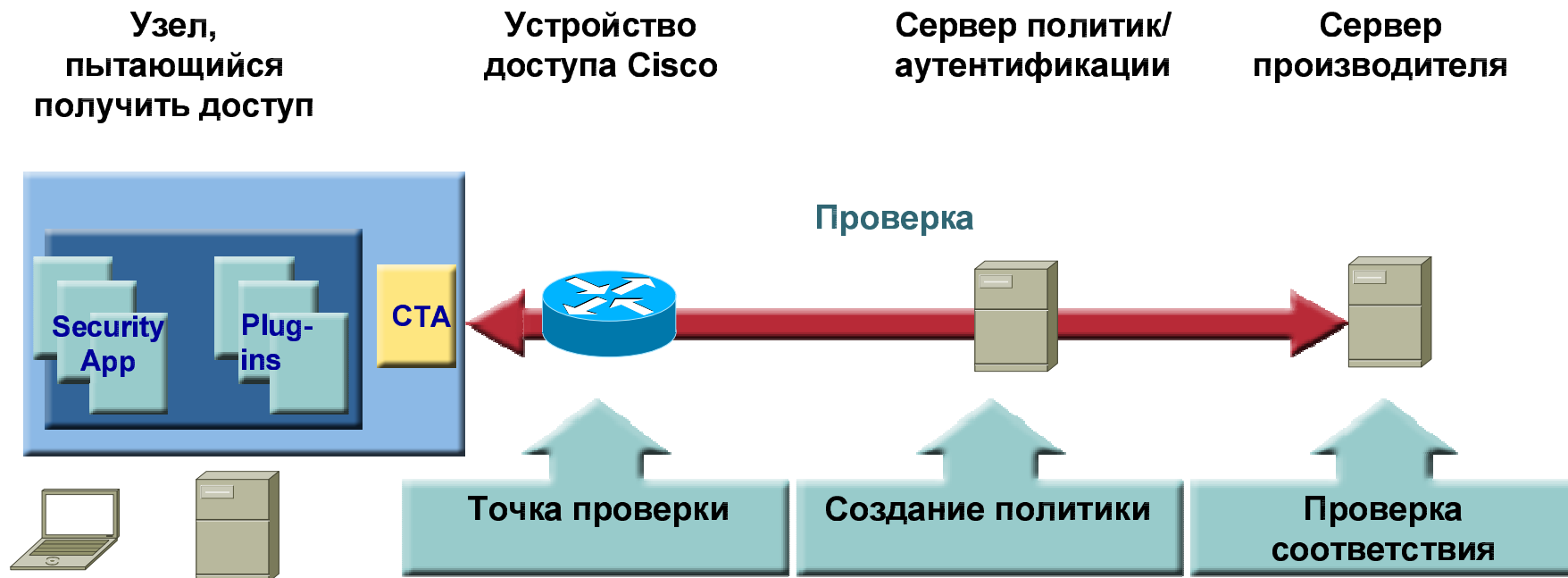
LANDesk Trusted Access

- **Cisco Network Admission Control (NAC)**
- **LANDesk DHCP Server**

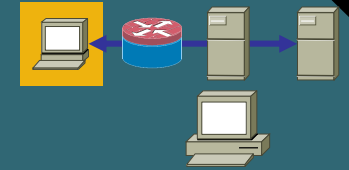
CISCO NETWORK ADMISSION CONTROL (NAC)



Cisco Network Admission Control (NAC)



- **Базируется на политике соответствия конечного узла требования корпоративной безопасности**
- **Пользователя обязывают выполнять требования политики безопасности**



Cisco Trust Agent (CTA)

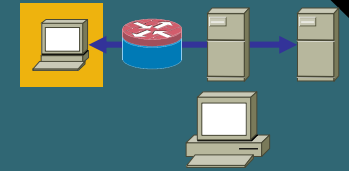
- **Собирает информацию о состоянии средств защиты, таких как антивирусы, CSA, обновления ОС, и связывается с сетевыми устройствами**
- **Данный агент уже встроен в решения Intel, LANDesk, Cisco Security Agent и др.**
- **Взаимодействие происходит по защищенному каналу**
- **Может быть бесплатно загружен с сайта Cisco**



LANDesk Security Suite

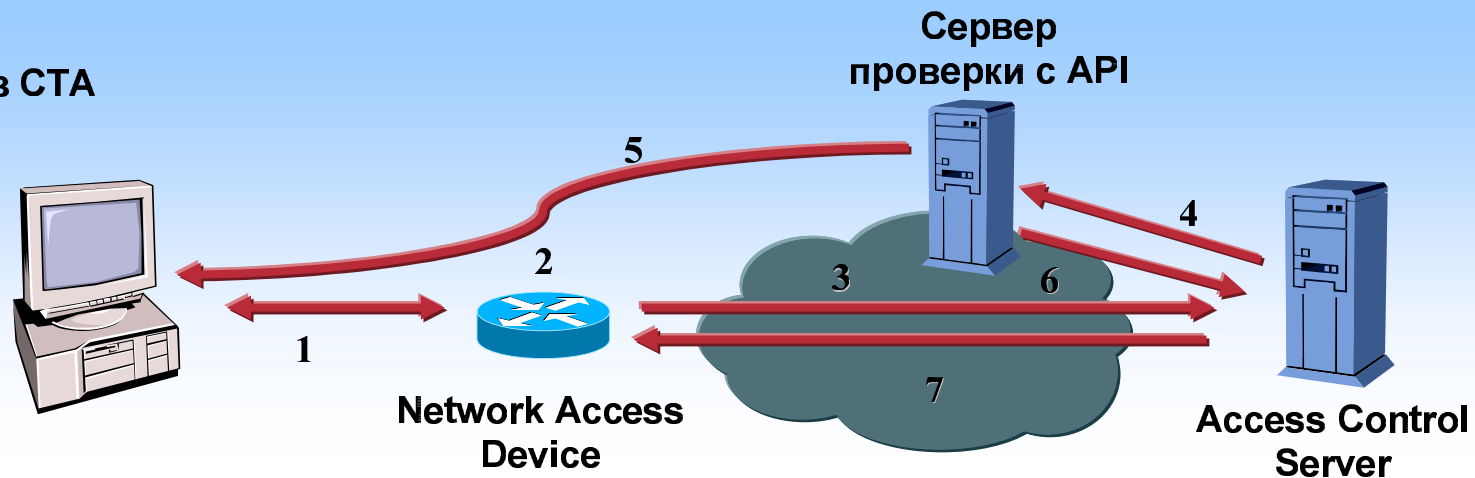
- Обнаружение узлов несоответствующих политике безопасности
- Изоляция несоответствующих узлов
- Удаление вредоносного ПО
- Установка обновлений
- При полной поддержке Cisco NAC





Что если на узле нет СТА?

Узел без СТА

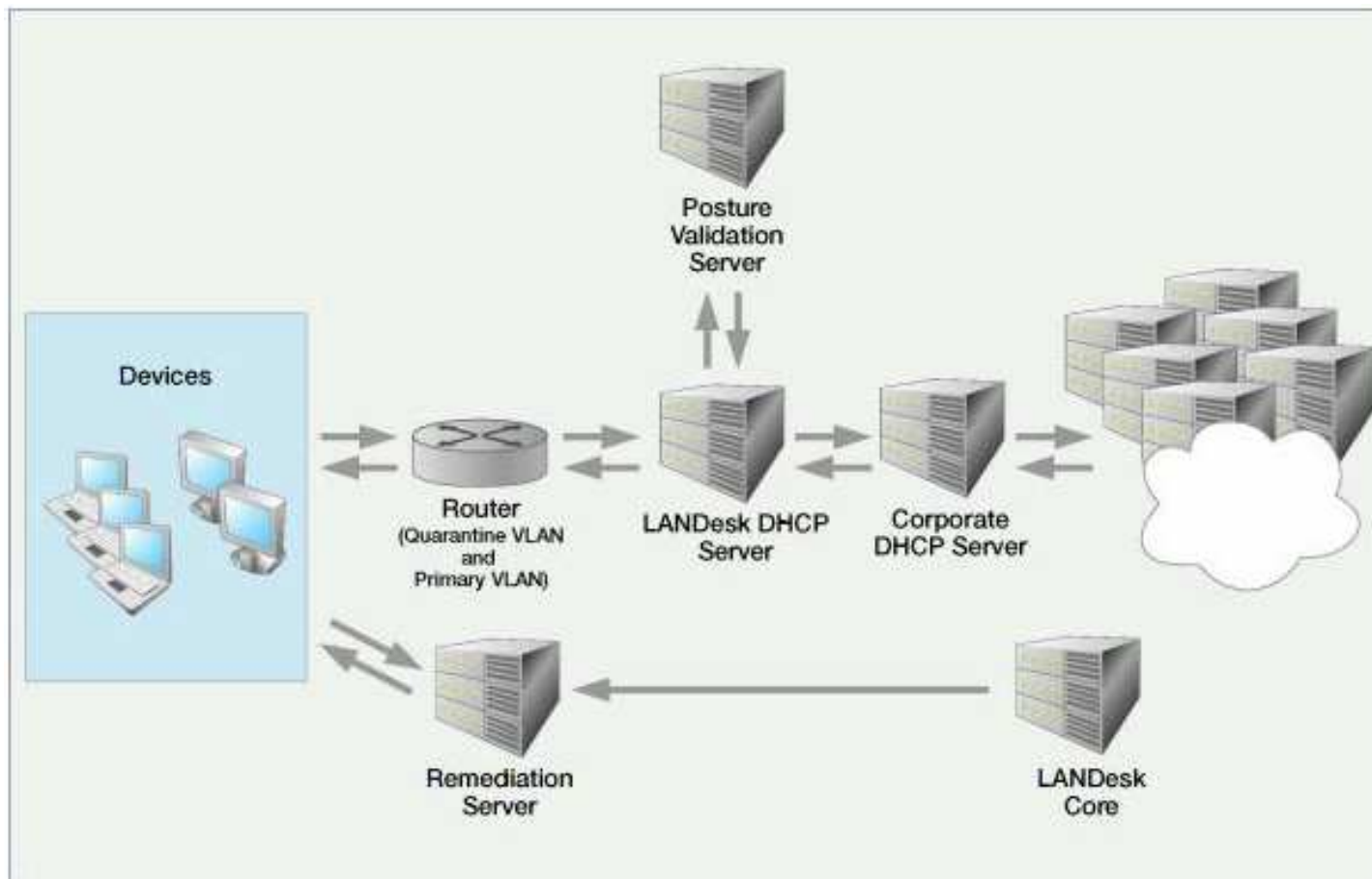


- **Список исключений на базе IP или MAC-адресов**
- **Список исключений на базе ACS Network Access Restrictions (NAR)**
- **Загрузка на узел СТА (при помощи Java, ActiveX и т.п.)**
- **Проверка с помощью сканера безопасности**

NETWORK ACCESS CONTROL OF LANDESK И MICROSOFT



LANDesk DHCP Server



LANDesk Trusted Access: за и против

Cisco NAC

За

Сильная защита

Поддержка *nix

Не требует больших затрат

Интеграция с NAP

Против

Ориентация на одного производителя

LANDesk DHCP

За

DHCP-фильтрация

Не зависит от сетевого вендора

Против

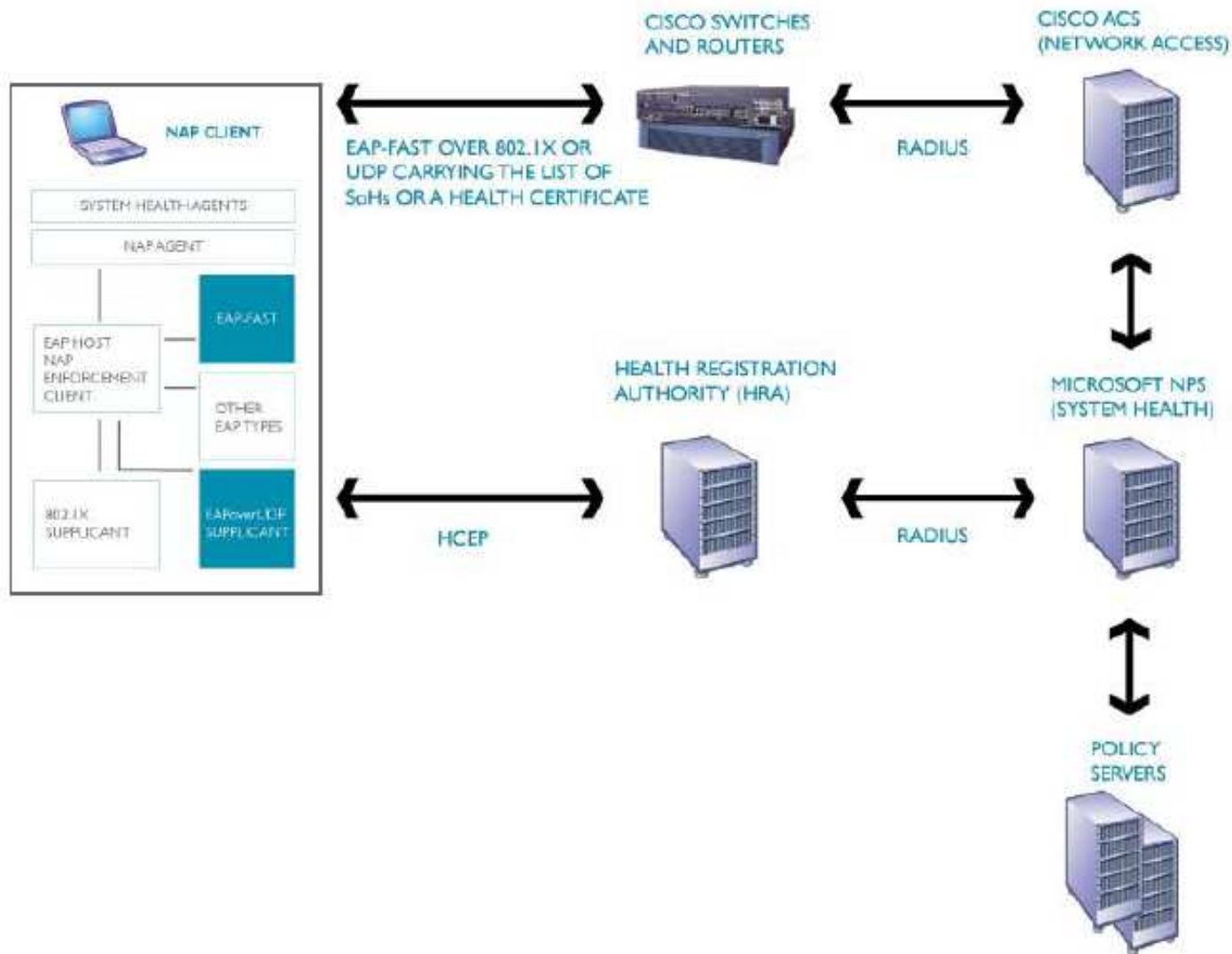
Менее защищено

Только Windows

Точка отказа

Требуется изменение топологии

Microsoft Network Access Protection (NAP)



АЛЪЯНС С INTEL И LANDESK



В преддверие альянса Cisco и Intel

**РАСШИРЕННЫЕ
СЕРВИСЫ**

Trusted Boot

**ДОВЕРИЕ
В СЕТИ**

NAC Framework

Cisco Trust Agent

Cisco Clean Access

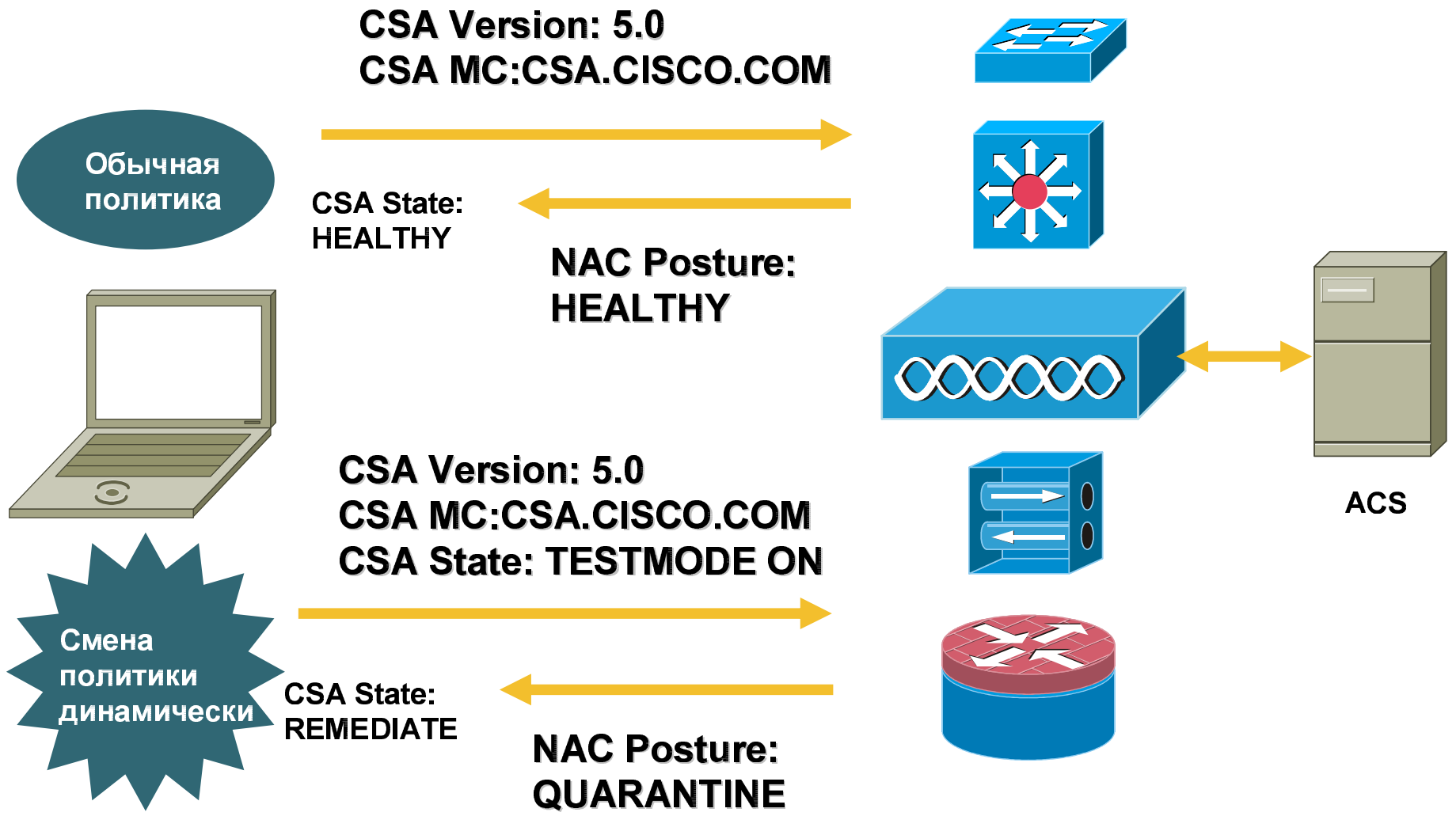
**ЗАЩИТА
ПК/СЕРВЕРОВ**

Cisco Security Agent

Cisco Security Agent

- **Предотвращение атак**
- **Персональный МСЭ**
- **Защита от вредоносного кода**
- **Контроль USB, CD, дисководов, PCMCIA**
- **Контроль Интернет-пейджеров (ICQ и т.п.)**
- **Защита от перехватчиков**
- **Контроль доступа к системному реестру и файлам**
- **Замкнутая программная среда**
- **Анализ журналов регистрации и т.д.**

Взаимодействие CSA и NAC



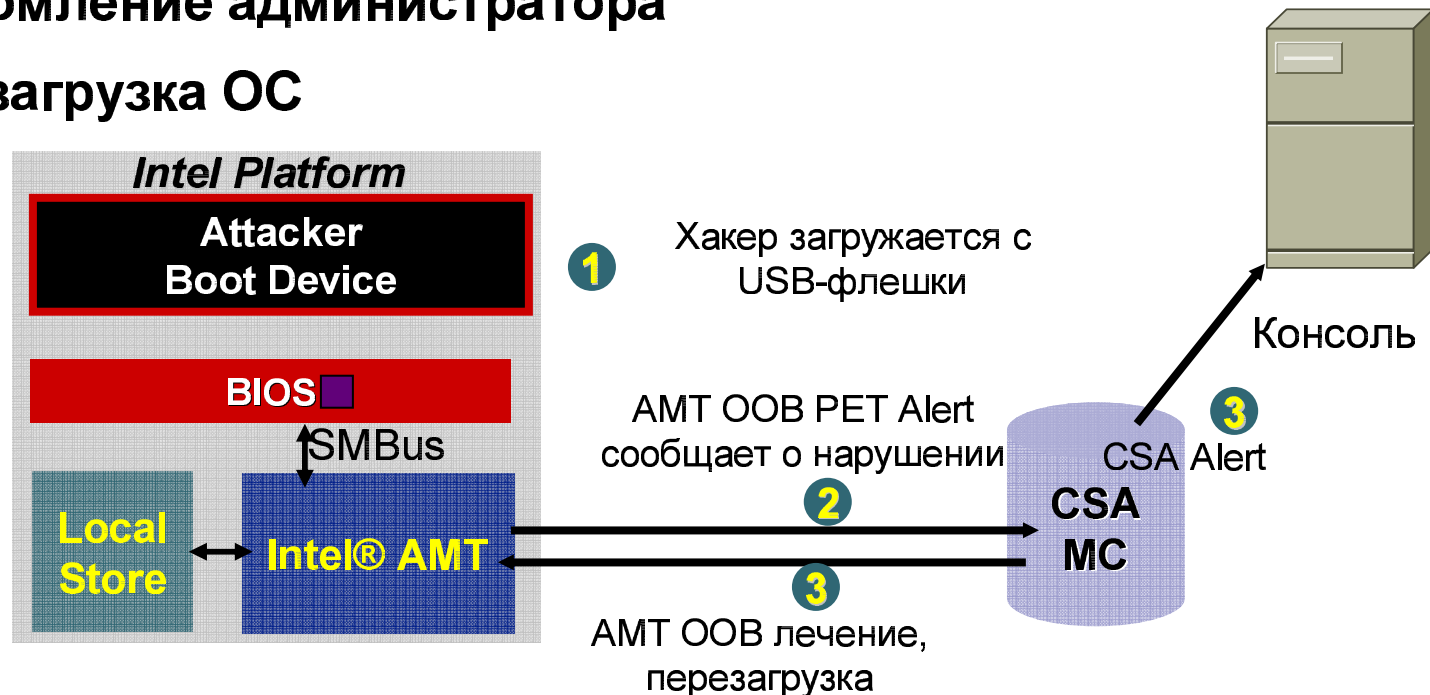
«Старая», но актуальная атака

- **Загрузка с альтернативного носителя или раздела**
 - Обход всех средств защиты
 - Установка троянцев или доступ к информации
- **Отсутствие методов централизованного или локального обнаружения этой атаки**



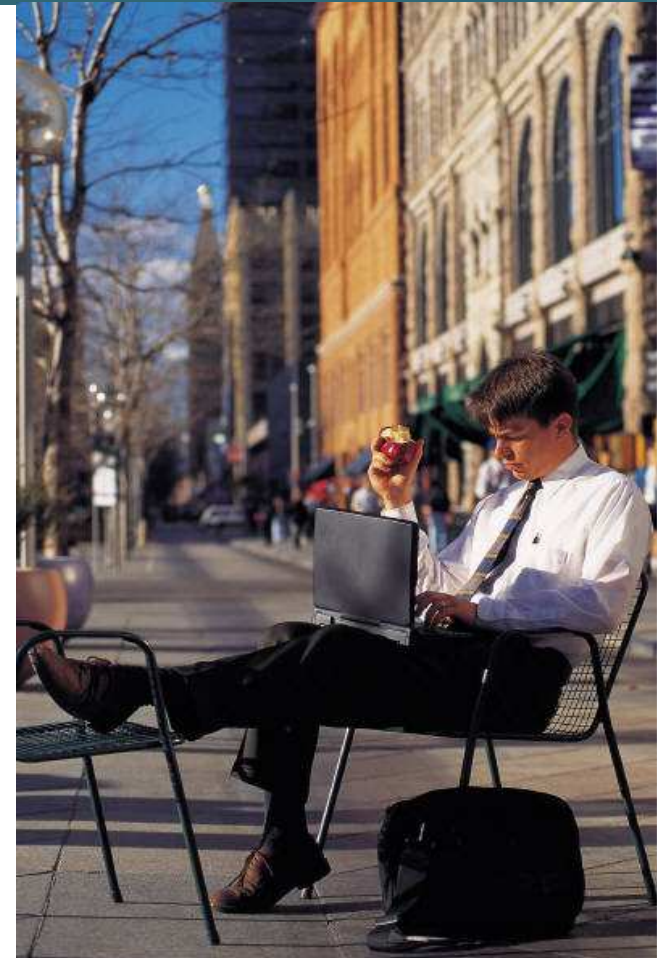
CSA Trusted Boot и Intel AMT

- Обнаружение загрузки с альтернативных носителей или разделов
- Независимость от ОС
- Уведомление администратора
- Перезагрузка ОС



Что контролирует Intel AMT?

- **Загрузка с неосновного раздела НЖМД (HDD)**
- **Загрузка с альтернативных носителей**
 - CD-ROM**
 - USB**
 - дискеты**
- **Загрузка из сети**
 - IDE-R**
 - PXE**



ЧТО ЭТО В ИТОГЕ ДАЕТ?



Преимущества NAC для владельца

NAC минимизирует простои в результате эпидемий вирусов и червей, обеспечивает сетевую целостность и доступность, управляет сетевым доступом и следит за внедрением политики доступа

- **Обеспечение соответствия всех узлов политике безопасности**
- **Снижение ИТ-затрат на предотвращение внешних и внутренних угроз**
- **Предотвращение заражения узлов от инцифированных сетей; снижение времени простоя от эпидемий**
- **Рост продуктивности и производительности**
- **Защита от уголовного преследования**



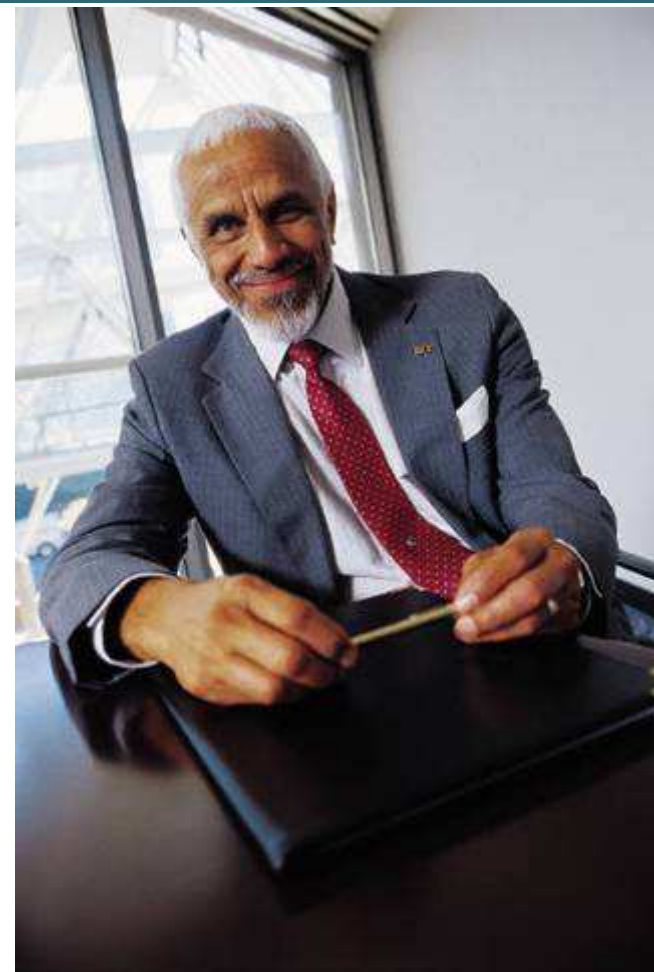
Защита инвестиций

- **НАС защищает инвестиции, потому что:**

На узлы, получающие доступ, уже установлен специальный программный агент

Этот агент входит в состав многих антивирусов, систем персональной защиты и т.п.

Поддержка НАС уже встроена в сетевое оборудование или операционные системы



Преимущества NAC для пользователя

- Не надо беспокоиться о защите своего компьютера
- Не надо думать, где раздобыть патчи и другие заплатки
- Не надо думать о лицензионном ПО
- Не надо думать об обновлении своего антивируса (если он есть)
- Можно переложить всю ответственность на чужие плечи
- Защита от уголовного преследования (ст.273 УК РФ)



NAS – ключевое отличие

- **Идеальное решение для инфраструктуры**

Заказчики могут применить NAS в уже построенной сети

Для ряда реализаций не требуется изменения топологии

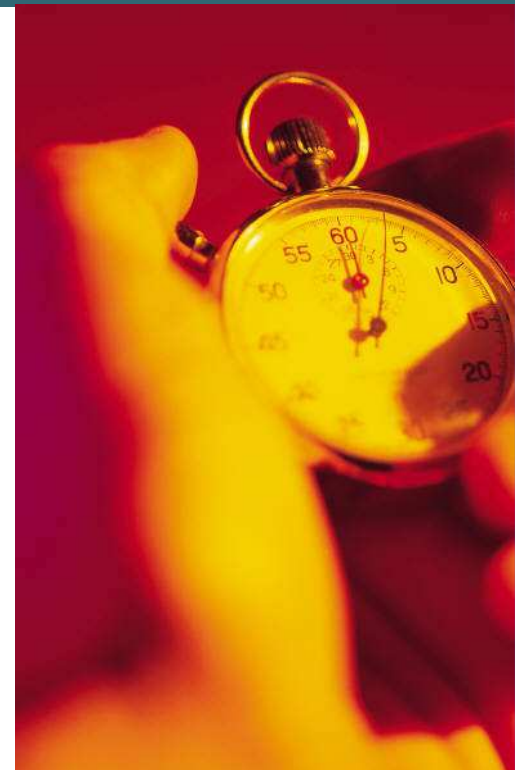
Зачастую требуется только обновление ПО

- **100%-я проверка узла и устройства**

- **Индустриальная инициатива**

Поддержка 65+ вендоров

Новый API позволяет подключиться к NAS всем производителям средств защиты



ВОПРОСЫ





**Получить эту презентацию, а также задать
дополнительные вопросы Вы можете по
электронной почте
security-request@cisco.com
или по телефону: (495) 961-1410**

CISCO SYSTEMS

