



Централизованное управление безопасностью мобильных клиентов

Алексей Лукацкий

Security Business Development Manager

Содержание

- **Какие бывают мобильные устройства?**
- **Зачем они используются?**
- **Какие угрозы они с собой несут?**
- **Специализированные средства защиты**
- **Как управлять прямо сегодня?**
- **Как управлять завтра?**
- **Пожелание**

Что, где, зачем?



Начнем с фактов

- **26 июля 2004 года в Министерстве Энергетики США были запрещены все работы на компьютерах до тех пор пока не будет обеспечен необходимый уровень безопасности для всех мобильных и переносных устройств**



Какие бывают мобильные устройства?

- **Лэптопы**
- **Карманные компьютеры (КПК, PDA)**
- **Смартфоны и коммуникаторы**
- **Мобильные телефоны**

Зачем нужны мобильные устройства?

- Это удобно
- Это престижно
- Это модно
- Это выгодно

- Запретить их невозможно, как и остановить развитие информационных технологий



Угрозы и их отражение



3 угрозы

- **Утечка информации через мобильное устройство**
 - «Вынос» информации на мобильном устройстве
 - Кража мобильного устройства
- **Проникновение в корпоративную сеть через мобильное устройство В ОБХОД средств защиты**
 - Периметровые средства защиты практически бессильны
- **Несоответствие требованиям**
 - Законодательство, политика безопасности

Вспомним о комплексной безопасности

- **Безопасность информационной системы равна безопасности самого слабого звена**
- **Мы **должны** защищать мобильные устройства для обеспечения комплексной безопасности**
И защиты себя от возможных преследований (уголовных, административных и т.п.)

Централизованное управление



Централизованное управление



Основная проблема

- **Низкая квалификация владельцев**
- **Масштабность**
- **Распределенность**
- **Отсутствие постоянной связи**
- **Отсутствие постоянных адресов**

- **Пример Cisco Systems**
 - Десятки тысяч лэптопов**
 - Десятки тысяч смартфонов**

Игроки рынка



Игроки рынка мобильной безопасности

- **Pointsec Mobile Technologies**
- **Information Security Corporation**
- **Credant Technologies**
- **Ensure Technologies**
- **ArticSoft**
- **Mobile Armor**
- **Asynchrony**
- **Bluefire Security System...**

Пример: Altiris



Изучите «размер бедствия»

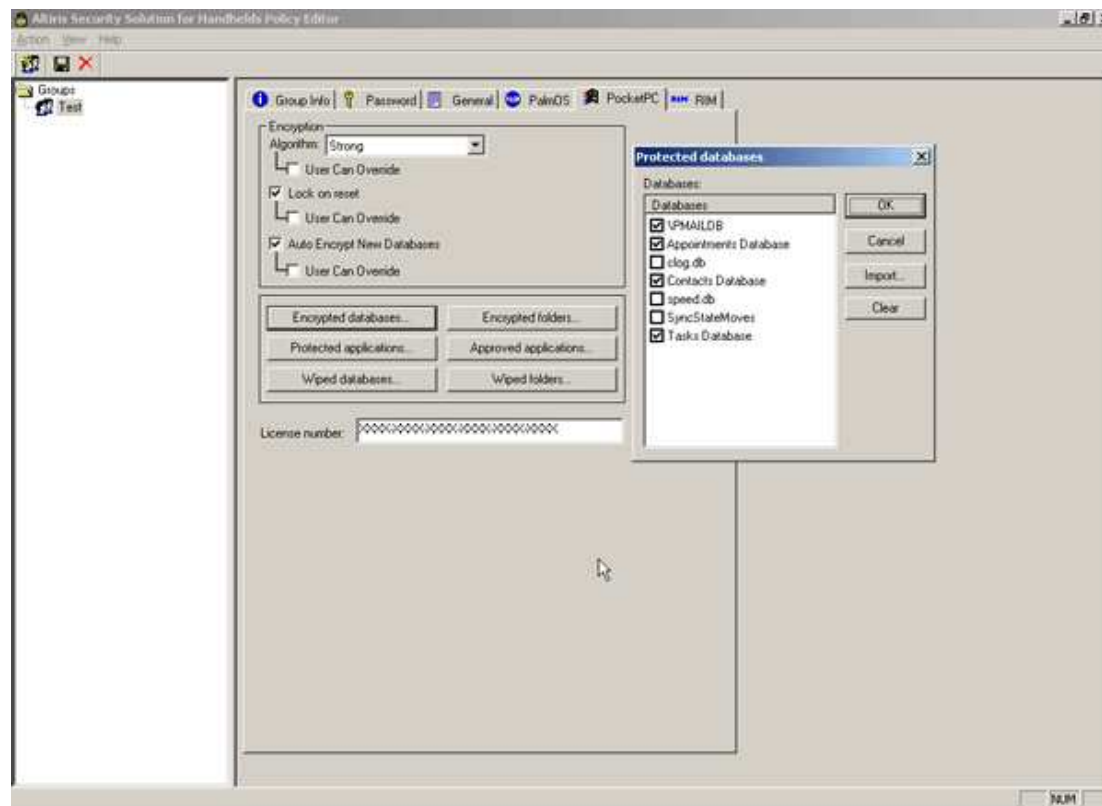
- Необходимо знать все, что творится на «несерьезных компьютерах»

The screenshot displays the Altiris Console web interface in Microsoft Internet Explorer. The browser address bar shows <http://localhost/Altiris/NS/Console.aspx>. The interface includes a navigation menu with tabs for Getting Started, Tasks, Resources, Reports, Configuration, Shortcuts, and Incidents. The 'Reports' tab is active, and the 'Count of Products' report is displayed. The report table has three columns: # Machines, Manufacturer, and Product Name. The data shows 37 rows of product information, including items from manufacturers like Altiris, AvantGo, Inc., DELL, Dell Computer Corporation, Microsoft, and Microsoft Corporation.

# Machines	Manufacturer	Product Name
4	Altiris	ResetPrompt Application
4	Altiris, Inc.	Altiris Pocket PC Agent
4	AvantGo, Inc.	AvantGo Connect
4	DELL	DELL NavButton
4	Dell Computer Corporation	Data Backup
4	Dell Computer Corporation	Home
4	Dell Computer Corporation	info
4	Dell Computer Corporation	Switcher Bar
4	Microsoft	VoiceCl Module
4	Microsoft	Windows CE
4	Microsoft Corporation	.NET Compact Framework
4	Microsoft Corporation	FAKEIME
4	Microsoft Corporation	InkWriter
4	Microsoft Corporation	mfcce300
4	Microsoft Corporation	Microsoft (r) JScript
4	Microsoft Corporation	Microsoft (R) Visual C++
4	Microsoft Corporation	Microsoft ADOCE Control
4	Microsoft Corporation	Microsoft Latin Character Recognizer
4	Microsoft Corporation	Microsoft Pocket Office
4	Microsoft Corporation	Microsoft Transcriber
4	Microsoft Corporation	Microsoft® DAS Client Components
4	Microsoft Corporation	Microsoft® Reader
4	Microsoft Corporation	olece300

Централизованное управление

- **Централизованно управляйте всеми настройками безопасности на портативных устройствах**



Неутешительный прогноз

- **До 2007 года компании не будут иметь единого решения по защите персональных информационных пространств**

Источник: “Mobile Security Exposures, Trends and Remedies”, Gartner

Что можно сделать уже сейчас?



Как должно быть?

- Разрешать подключение к сети **только аутентифицированным пользователям и устройствам** по защищенному каналу
- 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

Мобильная «песочница»

Перед установлением соединения выполняется проверка:

- Местонахождение – управляемый/неуправляемый компьютер?
- Установленное ПО: AV, МСЭ, malware?

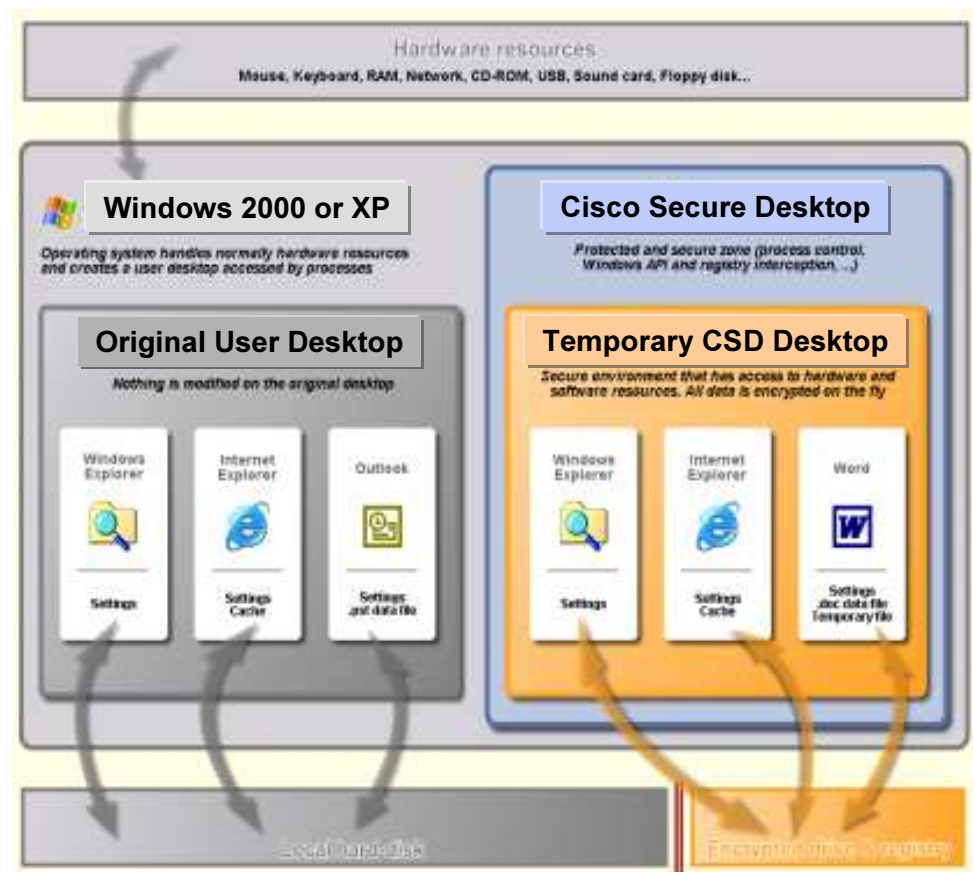
Максимальная защита сессии:

- Выделенный сегмент защищает данные на компьютере
- Обнаружение Malware с помощью Microsoft free anti-spyware software

Удаление данных после завершения соединения:

- Защищенный сегмент очищается
- Cache, history и cookie удаляются
- Скачанные файлы удаляются
- Пароли удаляются

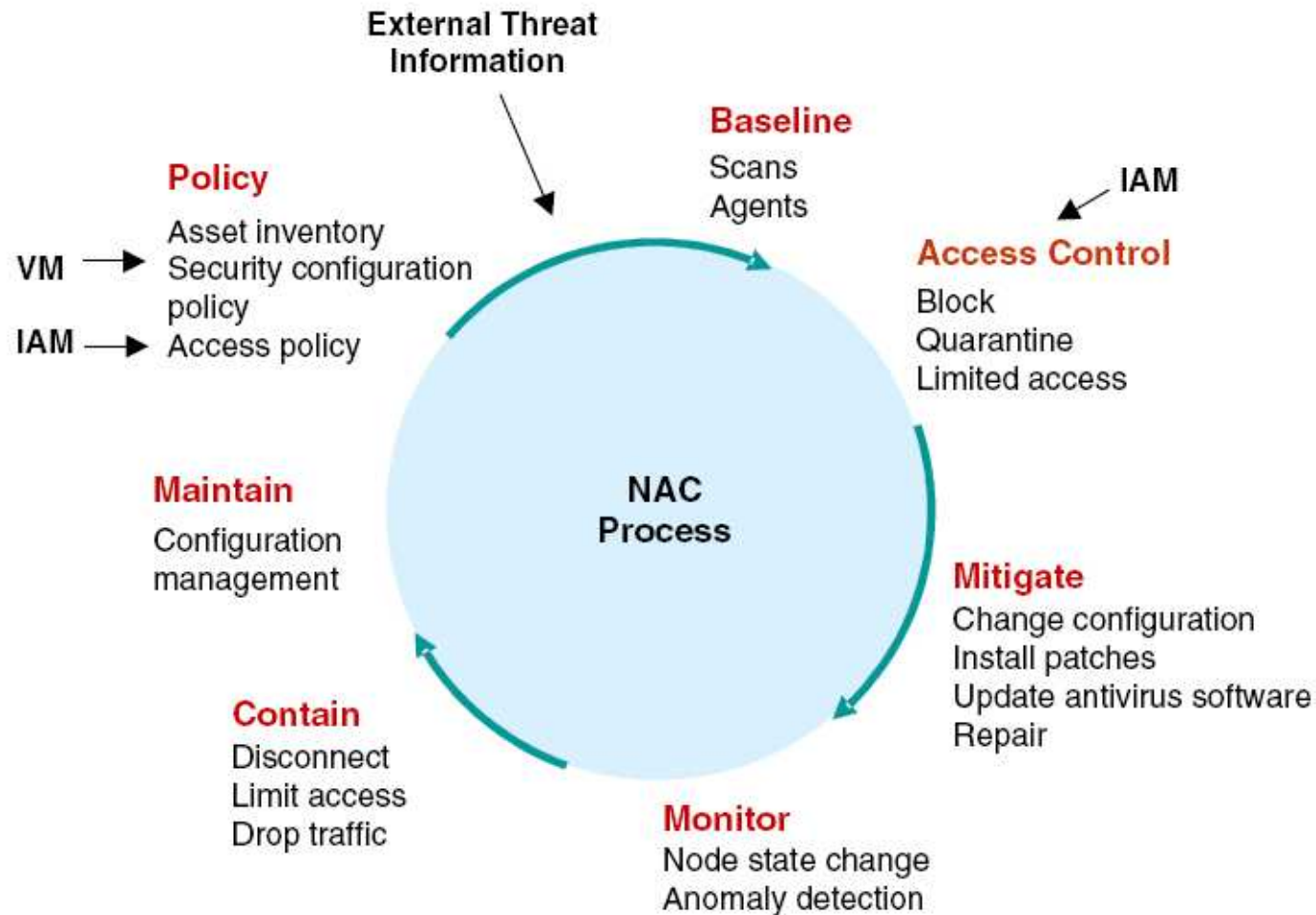
Работает с гостевыми правами
Не требует полномочий администратора



Локализируйте источник угрозы и проверьте соответствие политике

- Для локализации угрозы используйте технологию Network Access Control (NAC), которая позволяет **не пускать** в сеть (извне и изнутри) устройства, несоответствующие политике безопасности или зараженные вредоносной программой

Элементы NAC



IAM = identity and access management
VM = vulnerability management

Source: Gartner Research (December 2004)

Что можно сделать в будущем?



Наследование и распределение политик

“Создали один раз – внедрили много раз”

Что это такое?

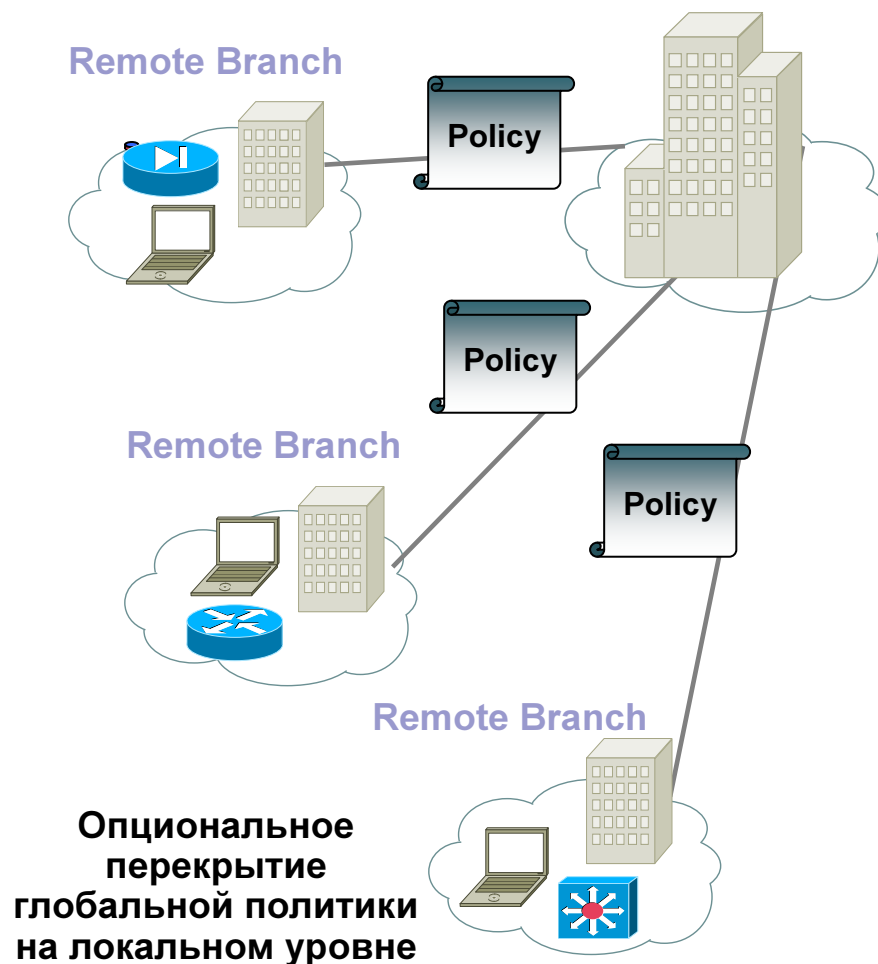
- Нарушение связи между устройством и политикой

Пример:

- Общие политики для групп устройств:
 - МСЭ в филиале
 - Site-to-site VPN
 - Управление устройством
- Обязательные политики:
 - Запрет IM и P2P
 - Разрешить SSH, SSL

Преимущества:

- Снижение сложности управления
- Не требует много ресурсов



Масштабируемое распределение

Что это такое?

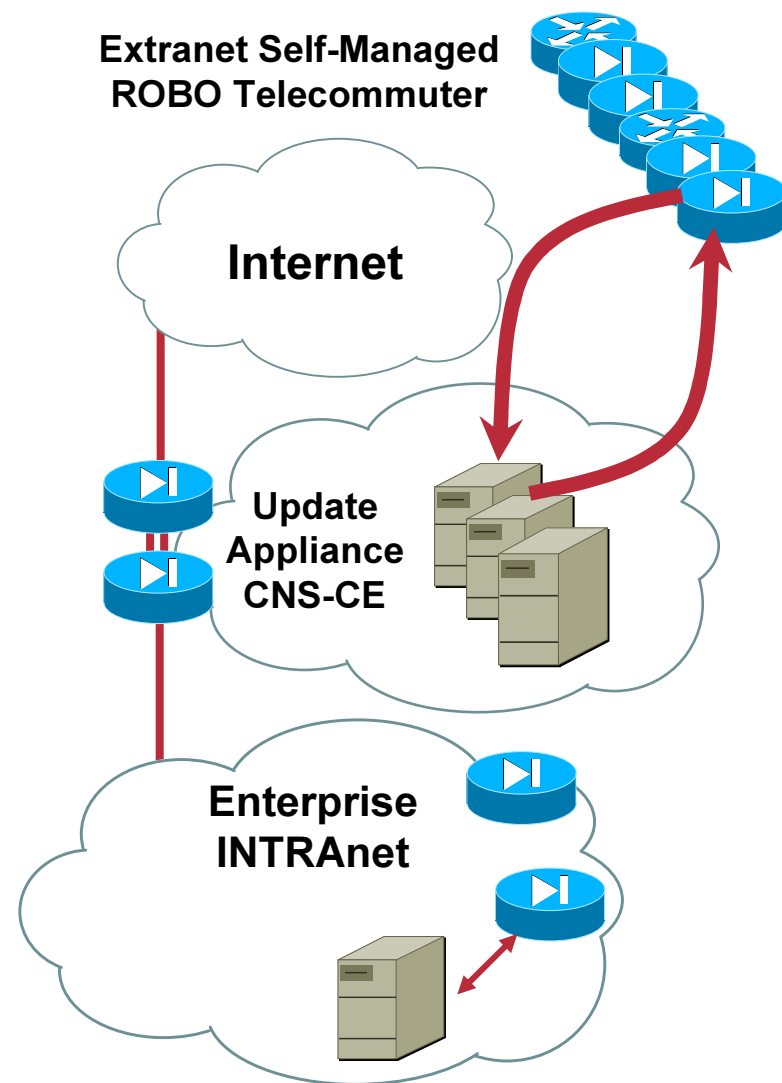
- Метод простого распределения политик и ПО на тысячи устройств

Пример

- Обновление большого числа удаленных МСЭ с динамической адресацией, нерегулярными линками или адресами за NAT
- Обновление конфигурации и ПО
- Обновление устройства, когда оно активно
- Масштабирование через Web-технологии

Преимущества

- Минимальные человеческие и временные затраты на построение защищенной сети



Документооборот

“Хочу контролировать и поставить свою подпись”

Что это такое?

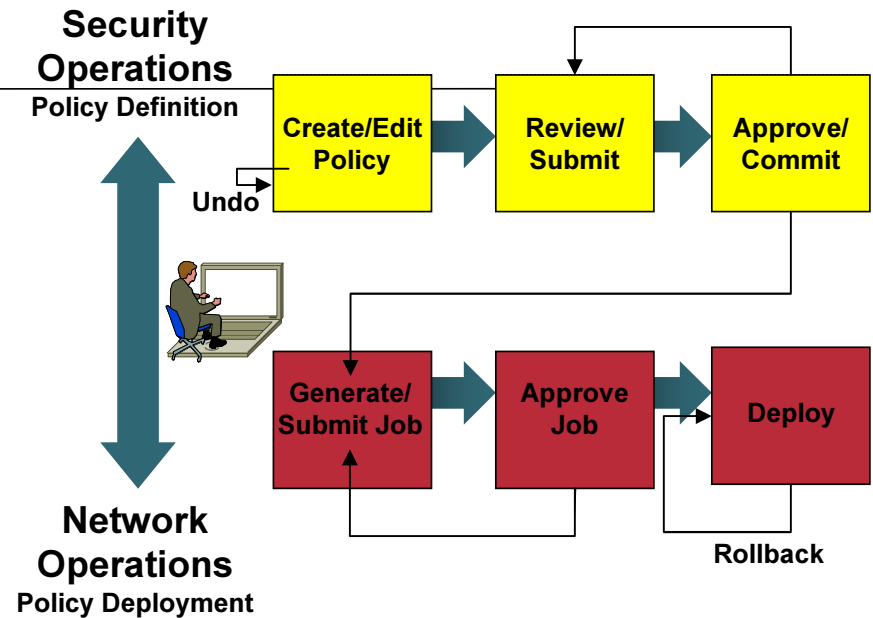
- Структурированный процесс контроля и утверждения изменений политики

Пример

- Кто создает политику?
- Кто утверждает политику?
- Кто применяет политику и когда?

Преимущества

- Эффективное взаимодействие NetOps и SecOps



MCЭ, VPN и IPS

Пожелание



90% будущих проблем

- **К 2006 году 90% мобильных устройств корпоративных пользователей не будут иметь сколь-нибудь серьезных средств защиты, способных противостоять среднеквалифицированному злоумышленнику**

Источник: “Magic Quadrant for Mobile Data Protection”, Gartner

**Давайте стремиться попасть
в оставшиеся 10%!**



Вопросы





**Дополнительные вопросы можно задать
по электронной почте
security-request@cisco.com**

CISCO SYSTEMS

