



Symantec Network Access Control 11.0.4

Контроль доступа в корпоративную сеть

18 марта 2009

Головенко Олег

Новая концепция безопасности

SECURITY 1.0

Ограничение систем
Ограждение от плохого
Защита только инфраструктуры
Решения фиксированные
Изолированные решения

SECURITY 2.0



Баланс риска и возможностей



Только хорошее внутри



Защита информации и операций



Принятие решения
на основании репутации



Стандартизированные и
автоматизированные процессы



Symantec Network Access Control



- Проверка на соответствие политикам для конечных устройств
 - ✓ Антивирус установлен и обновлен?
 - ✓ Межсетевой экран установлен и запущен?
 - ✓ Требуемые патчи и SP установлены?
 - ✓ Требуемая конфигурация?
- Исправление несоответствий
- Контроль гостевого доступа

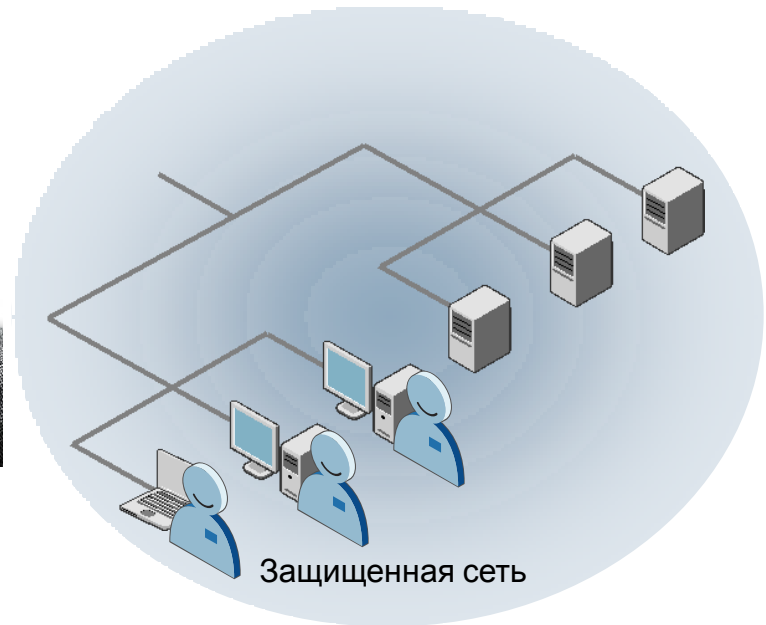
Network Access Control помогает предотвратить распространение вредоносного кода в сети

Авторизация не только пользователей, но и конечных точек сети (Symantec NAC)

- Управление доступом к сети = создание замкнутой системы с контролем за тем, с чем может работать
- Гарантия того, что прежде чем компьютер получит доступ к сети, на нем будут установлены все необходимые патчи, настроены конфигурации и системы защиты
- Автоматическое приведение конечных точек в соответствие с правилами безопасности
 - Гарантирует соблюдение правил до предоставления доступа



Антивирус установлен и обновлен?	✓
Межсетевой экран установлен и включен?	✓
Необходимые патчи и сервисные пакеты?	✓
Требуемая конфигурация?	✓



Управление доступом к сети – дополнение к SEP или самостоятельный продукт



Некондиционные
конечные точки



Удаленные
работники



Неавторизованные
конечные точки



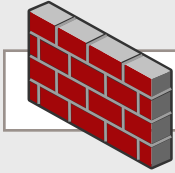
Беспроводные
сети

Основные функции управления доступом к сети

- NAC-ready endpoint protection
- Оценка и восстановление соответствия конечных точек сети
- Проверка наличия заданных антивируса, антишпионского ПО и межсетевого экрана
- Не зависит от поставщика — можно использовать AV, AS или PFW от других поставщиков
- Проверка наличия заданных операционных систем и пакетов обновлений
- Лучшие в своем классе средства проверки конфигурации
- Наиболее полный спектр подходов NAC

3. Enforcers

Host-based



Symantec Self-Enforcement

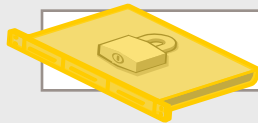
Хорошо

Network-based
(необязательно)

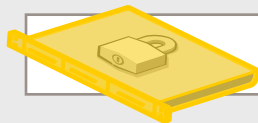


Symantec Gateway Enforcer

Еще
лучше



Symantec DHCP Enforcer

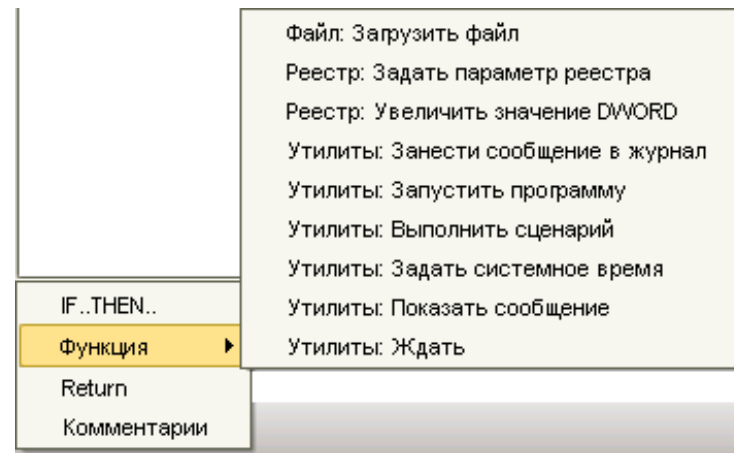


Symantec LAN Enforcer-802.1X

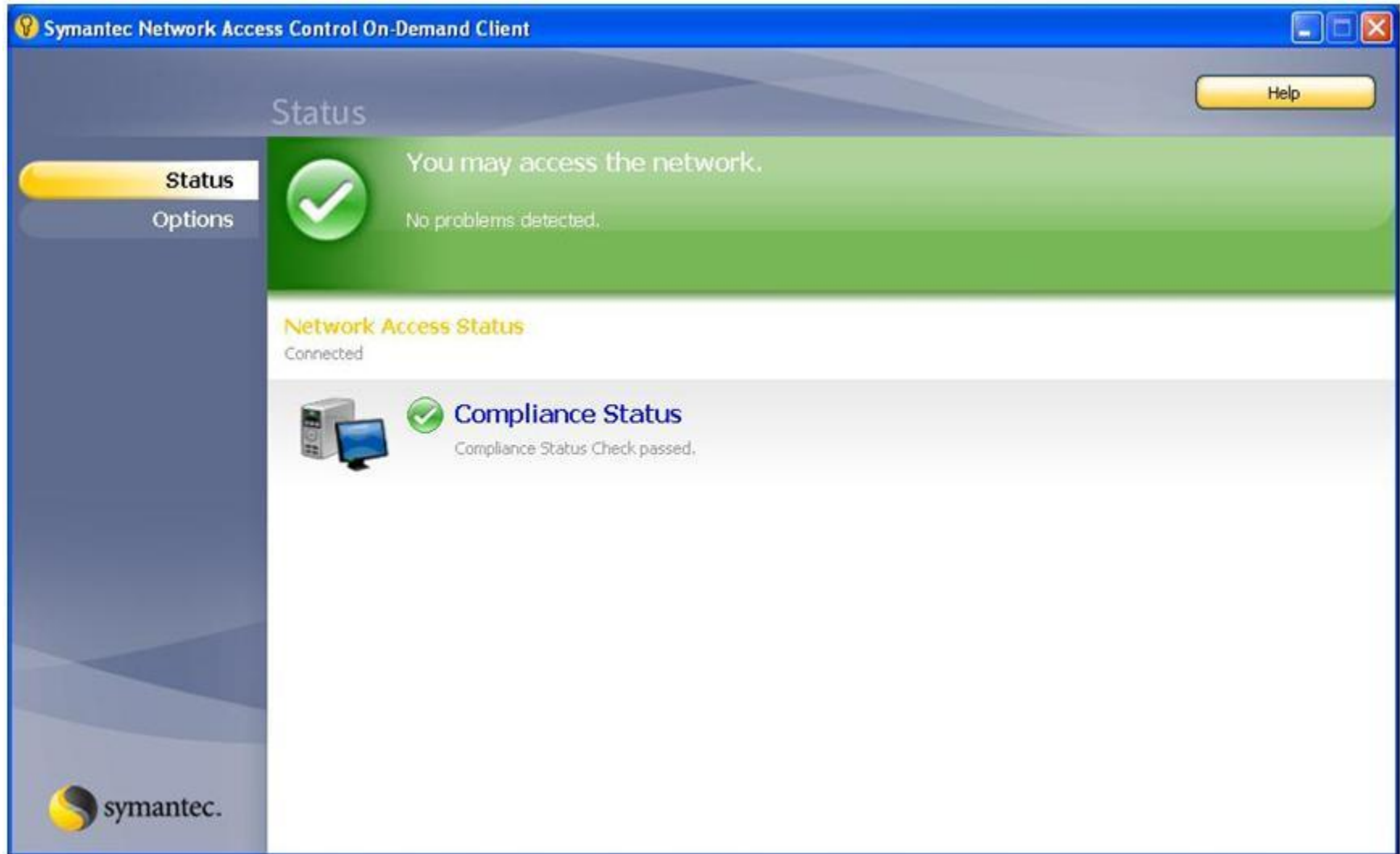
Отлично

Особенности SNAC

- Независим от вендора
- Self-Enforcement
- Комплексный подход
- Гостевой доступ
- Автоматическое исправление



Интерфейс SNAC On-Demand Клиент: проверка пройдена



Гостевой доступ через веб-интерфейс

User Login Page - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites

Address <http://10.127.34.67/webroot/verify.htm> Go

Symantec™ Network Access Control

Welcome

Network Access

You are attempting to access a protected network.

To access this network you are required to download the latest version of the Symantec Network Access Control Agent which will check your machine for security compliance before you are allowed to connect.

Please login to download.

Login

Password

Done Internet

Сообщение
можно задать

Проверка
данных через
RADIUS (LAN
enforcer), AD или
LDAP

Поддержка платформы Symantec Endpoint Protection

Операционные системы	32-бит	64-бит
Клиент SEP		
Windows Vista	X	X
Windows 2003 (включая SBS)	X	X
Windows XP	X	X
Windows 2000 (SP3 и старше)	X	
Windows 2008 (включая SBS)	X	X
MacOS	X	
Linux	X	X
Сервер управления SEPM		
Windows 2003/2008 (включая SBS)	X	X
Windows XP Pro	X	
Windows 2000 (SP3 и старше)	X	



Спасибо

Oleg_Golovenko@Symantec.com