



Confidence in a connected world.

# Symantec Endpoint Protection 11

- Symantec революционизировала рынок антивирусов своим новым решением для защиты конечных точек сети, минимизируя ваши усилия по управлению и уменьшая расходы, связанные с защитой ноутбуков, настольных ПК и серверов
- Благодаря объединению ключевых технологий в едином агенте и на единой консоли управления вы получаете возможность защитить свое предприятие от завтрашних угроз при вчерашнем уровне расходов

## SEP 11.0

### Антивирус и

### антишпионское ПО

- Обнаруживает, блокирует и удаляет
  - Вирусы
  - Шпионское ПО
  - Руткиты
  - Другие угрозы

### Антивирус и антишпионское

ПО



Symantec Endpoint  
Protection Manager

### Защита от сетевых угроз

### Защита от сетевых угроз

- Обнаруживает и блокирует внешние угрозы
- Фильтрует входящий и исходящий трафик
- Правила, зависящие от местонахождения

### Превентивная защита от угроз

- Защита от нераспознаваемых угроз
- Блокирование доступа к устройствам на базе правил

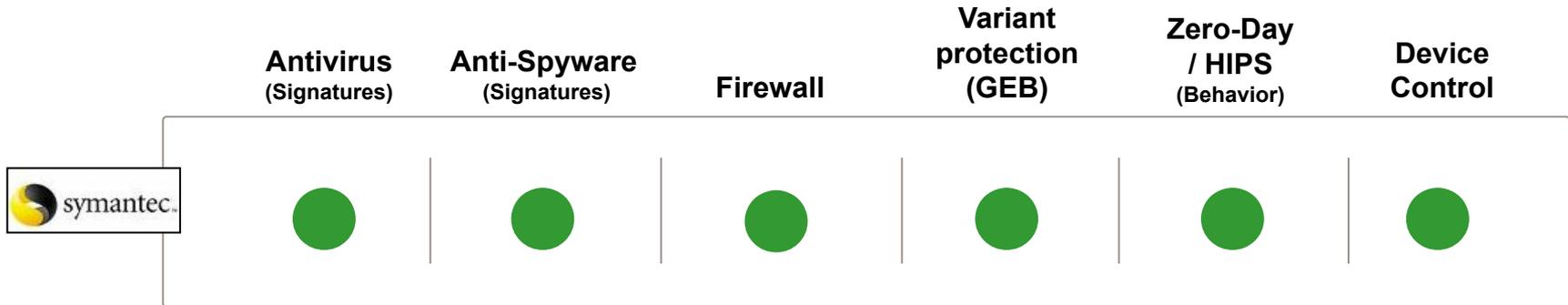
### Превентивная защита от угроз

### Управление доступом к сети

### Управление доступом к сети

- Гарантирует соблюдение правил в конечных точках сети
- Блокирует доступ к неавторизованным беспроводным узлам
- Предотвращает вторжение со стороны удаленных работников

## SNAC 11.0



- Решение, позволяющее бороться как с текущими проблемами, так и с еще неизвестными проблемами (Zero-day protection)
- Комплексное решение, вне зависимости от размера предприятия
- Возможность борьбы с инсайдерами (Device control)
- Централизованное управление и интеграция всех компонентов системы

# Новый пользовательский интерфейс клиента



## Пользовательский интерфейс клиента

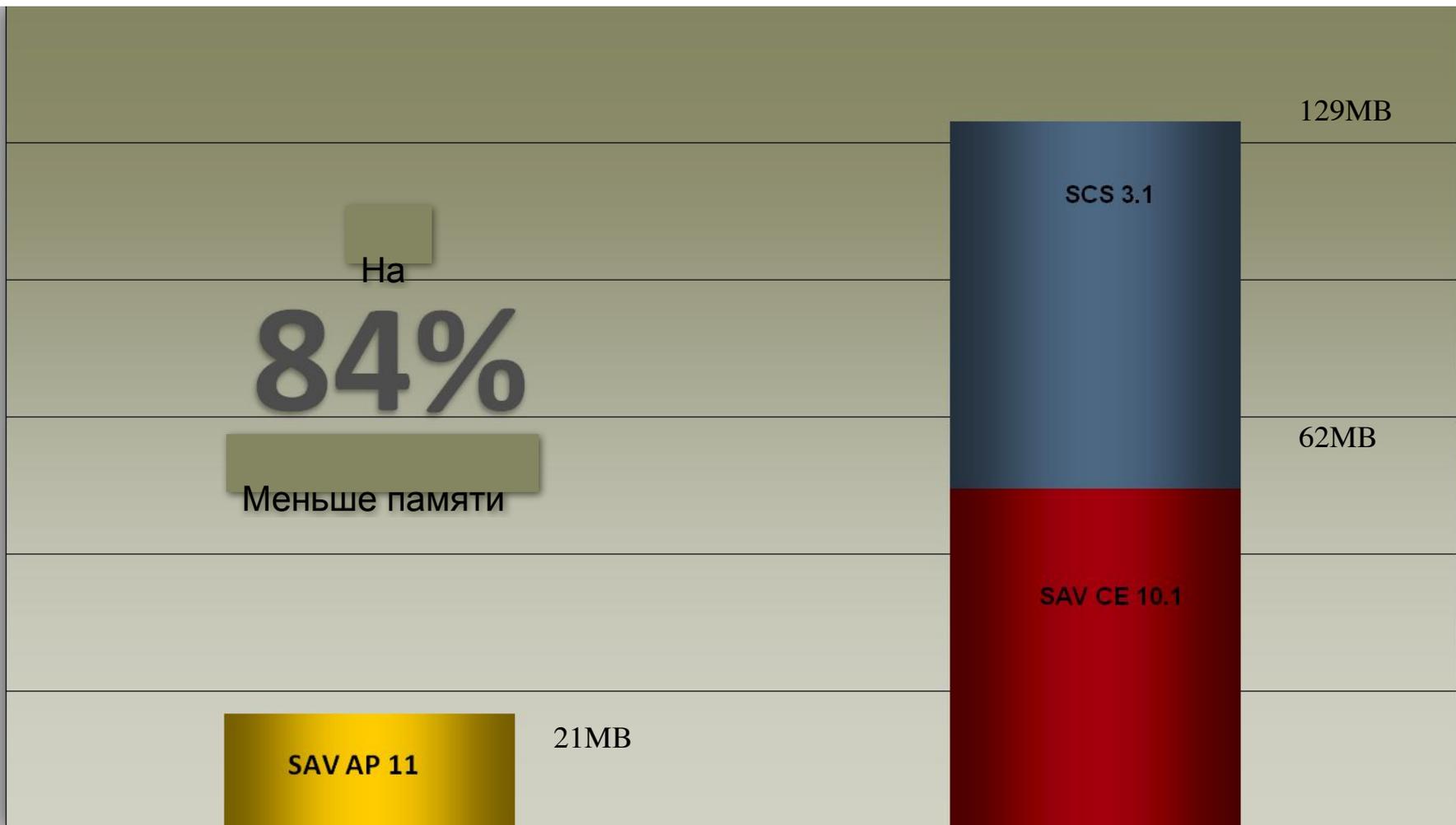
- Интерфейс клиента сосредоточен на удобстве конечных пользователей
- Позволяет быстро находить и просматривать параметры настройки

The screenshot displays the Symantec AntiVirus application window. The title bar reads "Symantec AntiVirus". In the top right corner, there is a "Help & Support" button. The main content area is titled "Status" and features a large green banner with a checkmark icon and the text "Your computer is protected." Below this, the "Protection Technologies" section lists installed features:

Technology	Status	Options
<b>AntiVirus and AntiSpyware Protection</b> Protects against viruses, trojan horses, and spyware Definitions: <b>January 31, 2007 r25</b>	On	Options
<b>Network Threat Protection</b> Protects against network threats Definitions: <b>January 31, 2007 r25</b>	On	Options
<b>Proactive Threat Protection</b> Provides zero-day protection against unknown threats SKAS version: <b>November 15, 2006 r1</b>	On	Options

At the bottom of the window, there is a "Connected to Enforcer" status with a checkmark icon and an "Options" link. The Symantec logo is visible in the bottom left corner.

# Клиент расходует меньше памяти





Вирус



Шпионское ПО



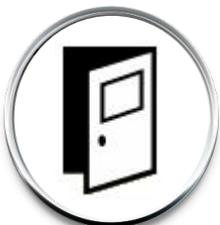
Червь



Вредоносное ПО

## Основные функции антивирусного и антишпионского ПО

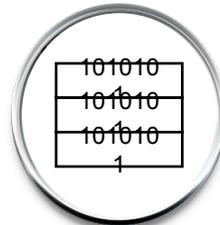
- Лучшая в своем классе защита от вредоносного ПО
  - Улучшенная система обнаружения и блокирования в режиме реального времени
  - Автоматическое удаление
- Улучшенная защита от шпионского ПО
- Новые средства защиты от руткитов
- Повышенная производительность
  - Улучшенная защита с меньшим влиянием на систему
- Новый пользовательский интерфейс клиента



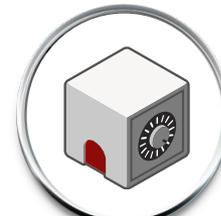
**Потайной  
ход**



**Комбинирован-  
ные угрозы**



**Переполнение  
буфера**



**Известные  
эксплойты**

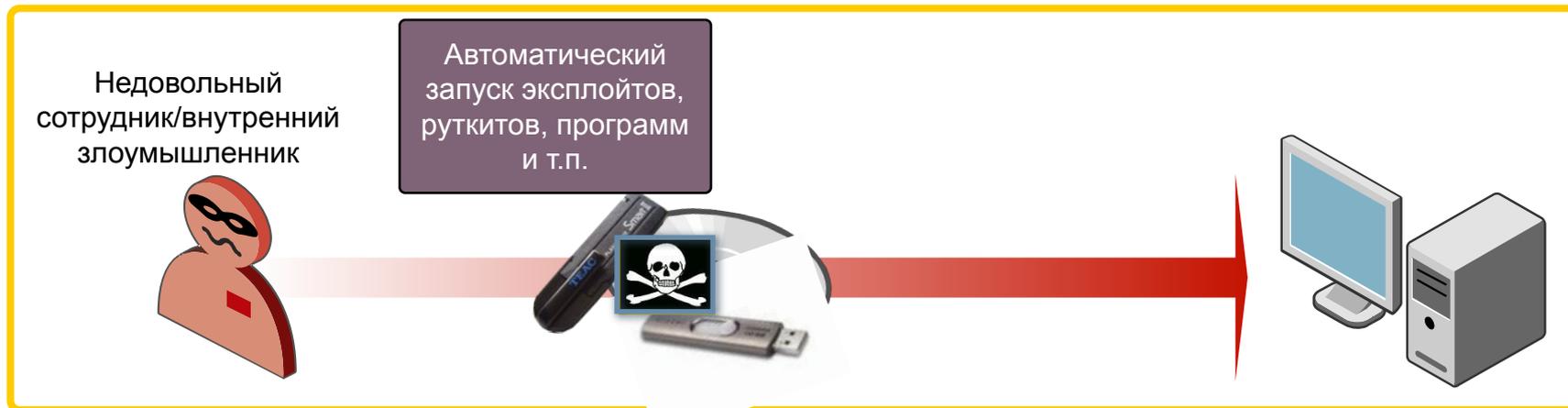
## Основные средства защиты от сетевых угроз

- Лучший в своем классе механизм межсетевого экрана на базе правил
  - Специальные правила для адаптера
  - Исследование зашифрованного и открытого сетевого трафика
- Механизм IPS
  - Блокирование классов эксплойтов (Generic Exploit Blocking - GEB)
  - Система предотвращения вторжений (IPS) на базе пакетов и на базе потока
  - Специальные сигнатуры IPS, использующие Snort™
- Учитывает местонахождение



## Основные функции превентивной защиты от угроз

- Защита от угроз на основе поведения
  - Полная интеграция Security Confidence Online
  - Обнаружение и блокирование вредоносного ПО без использования сигнатур
  - Защита от нераспознаваемых атак
- Управление устройствами
  - Блокирование периферийных устройств
  - Блокирование чтения, записи и исполнения
- Функции блокирования системы и защиты ОС защищают локальную файловую систему и приложения



## Функции защиты устройств

- Блокирует устройства по типам (Windows Class ID)
- Блокирует чтение/запись/исполнение со сменных носителей

## Порты блокирования устройств

Поддерживает все обычные порты

- USB
- ИК
- Bluetooth
- Последовательный
- Параллельный
- Firewire
- SCSI
- PCMCIA



**Некондиционные  
конечные точки**



**Удаленные  
работники**



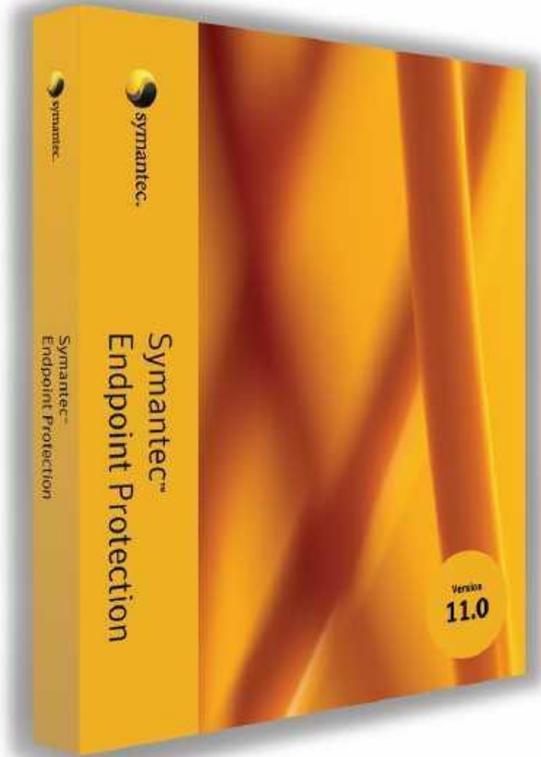
**Неавторизованные  
конечные точки**



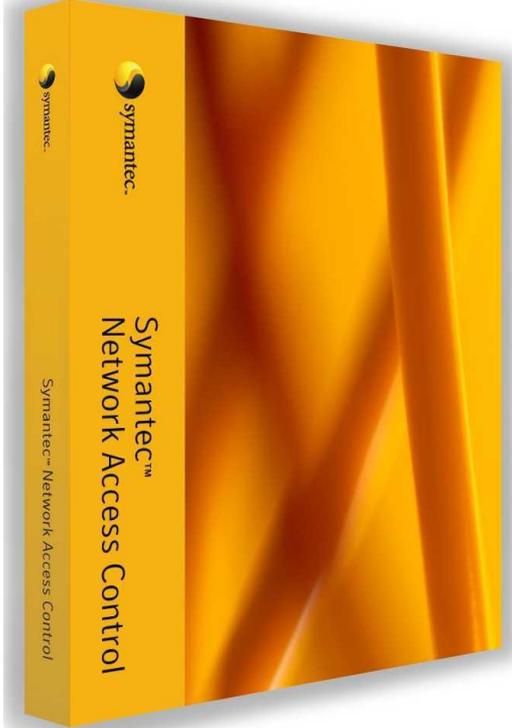
**Беспроводные  
сети**

## 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 ОС и сервисных пакетов
- Лучшие в своем классе средства проверки конфигурации
- Наиболее полный спектр подходов NAC



**Symantec Endpoint Protection 11.0**



**Symantec Network Access Control 11.0**