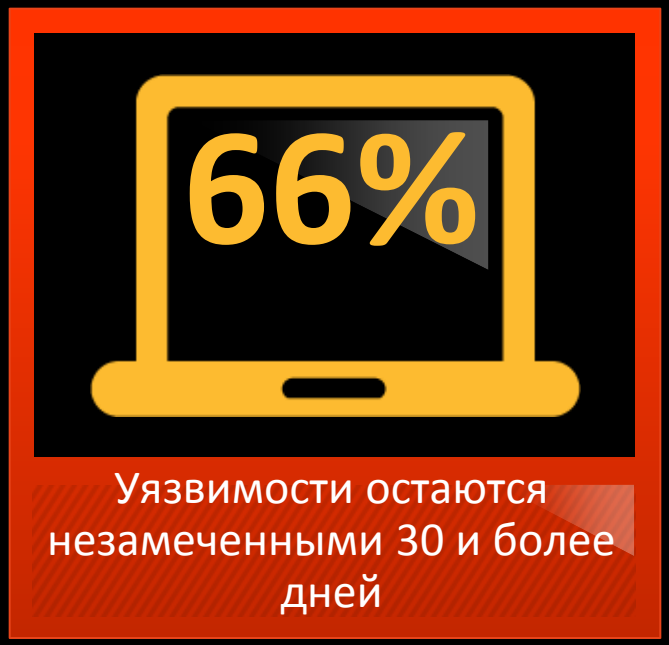
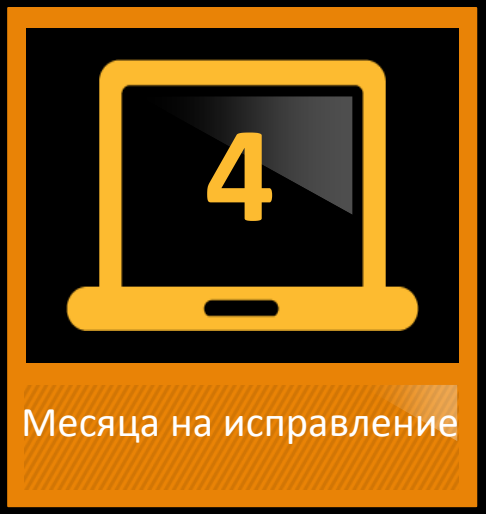
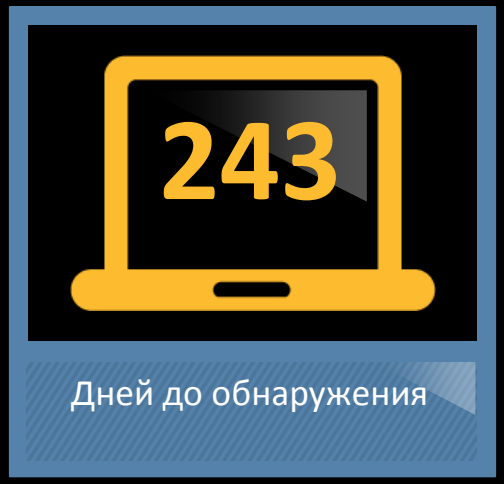
Защита от направленных атак

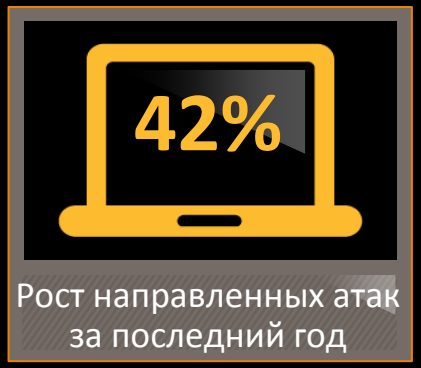
Олег Шабуров

Остановить направленные атаки крайне тяжело





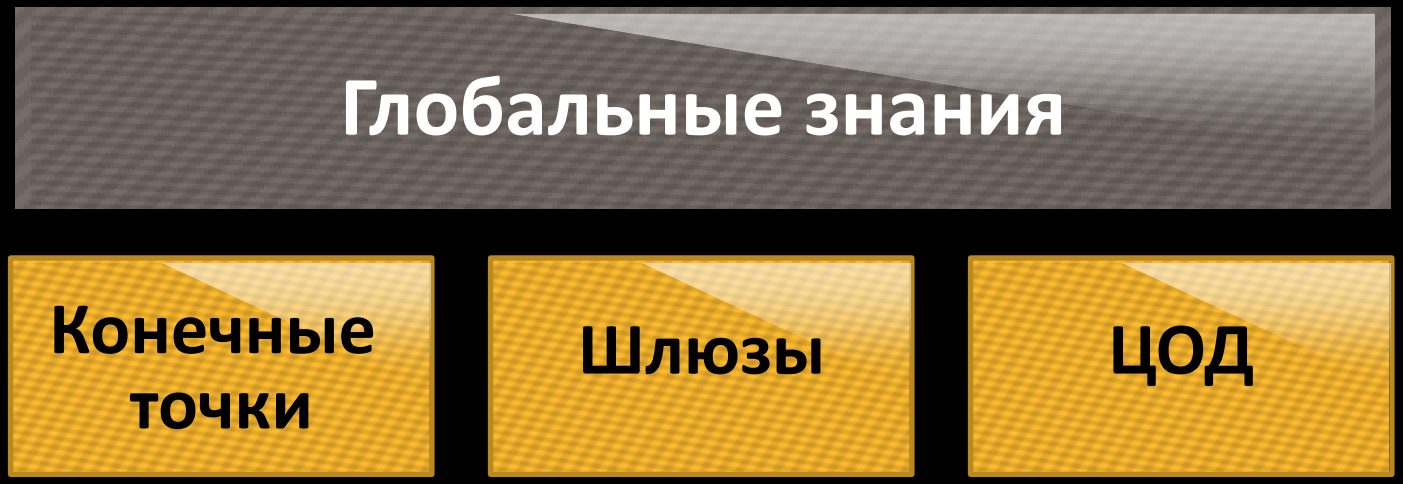




Касается не только больших компаний

- Самый большой рост в 2012 году среди компаний <250 сотрудников

Symantec останавливает направленные атаки уже сегодня



Информация о безопасности от Symantec

7 млрд

Классификаций файлов URL и IP

1 млрд+

Защищенных устройств

2.5 трлн

Записей событий телеметрии

550

Исследователей угроз ИБ

240 млн+

Пользователей и сенсоров

14

Центров мониторинга и реагирования

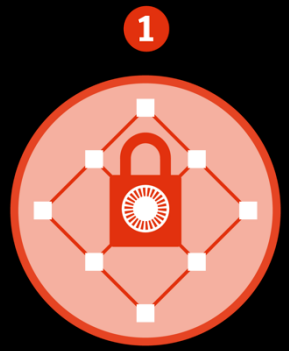
Глобальные знания

Конечные точки

Шлюзы

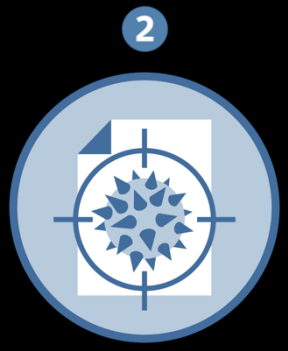
ЦОД

Проактивная защита на рабочих станциях:
Symantec Endpoint Protection



Intrusion Prevention

Защита на уровне сетевых подключений



Advanced Scanning

Файловые технологии детектирования

Insight Reputation

Репутационный анализ файлов

SONAR Behavior Blocking

Поведенческий анализ

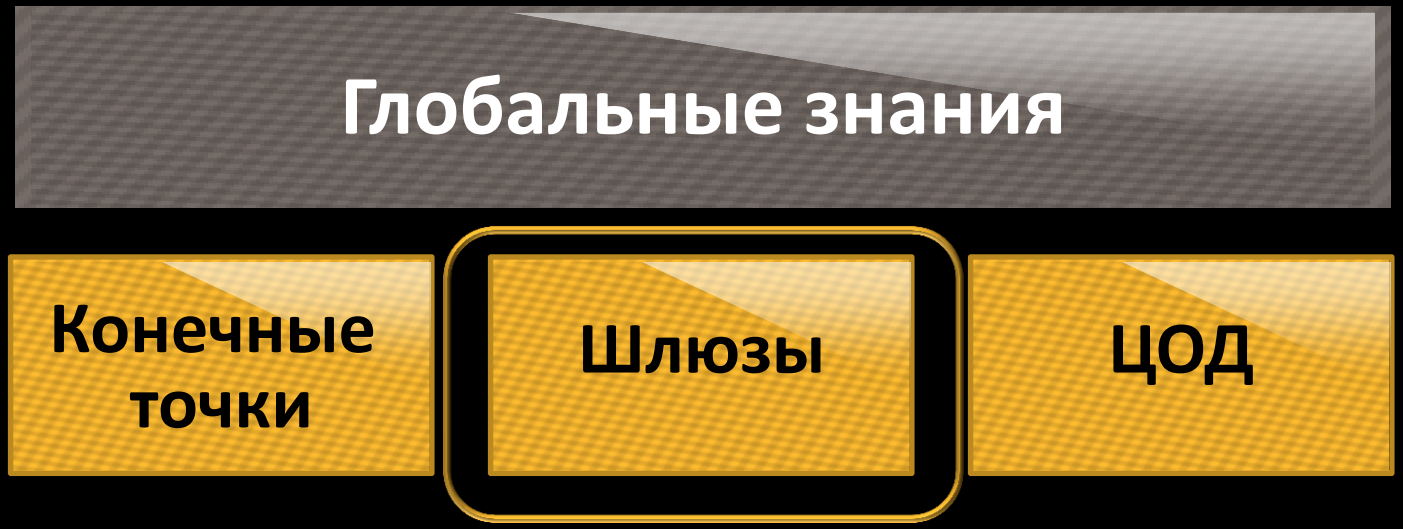
Symantec Maximum Repair

Устранение найденных проблем

Новое: сетевая защита для Mac

- Защита от опасных загрузок
- Защита от социального инжиниринга
- Детектирование событий на зараженных машинах
- Защита от атак через социальные медиа
- Защита от атак на незакрытые уязвимости

Остановить угрозу ДО момента, когда она повлияет на систему и данные


Глобальные знания
Конечные точки
Шлюзы
ЦОД

Проактивная защита шлюзов

Symantec Messaging Gateway

Symantec Email Security.cloud

Symantec Web Gateway

Тренды в направленных атаках (почта)

- Большинство направленных атак начинаются с отправки писем
- Использование атак нулевого дня во вложениях – популярный метод
- Пример: атака на RSA
- Обычные шлюзы безопасности это на заблокируют
- Еще пример: URL на вредоносные сайты и сокращенные URL

Новое на уровне шлюзов:
Технология Disarm в Symantec Messaging Gateway

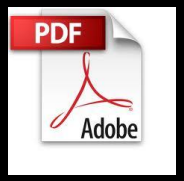
- Disarm удаляет весь активный контент, создавая чистую версию файла
- Чистая версия файла доставляется в режиме реального времени
- Пользователь **никогда не подвергается** атаке

Заблокировано

98%

0-Day эксплоитов в 2013

Работает с



Вложений

Технология, изобретенная Symantec

Шлюзы: проактивная защита
Email Security.cloud

Skeptic

Выявление аномалий

Поведение доставки, атрибуты сообщений, трюки соц.инженерии, методы вложений

Изменяющееся вредоносное ПО

Эвристика для определения вредоносного ПО

Следование по ссылкам

Обнаружение вредоносов в финальной точке

Направленные атаки, направленный фишинг, фишинг, спам

Технологии маскировки

Сокращенные URLs, задержки, несколько шагов по ссылкам, загрузка с нескольких сайтов

Шлюзы: проактивная защита
Web Gateway

- Использование анонимной телеметрии от тысяч машин для определения взаимосвязи файлов, машин и доменов
- Мониторинг практически всех исполняемых файлов в мире
  - Миллиарды известных файлов, миллионы новых каждую неделю
  - Использование времени жизни, распространённости, источника и других атрибутов для определения рейтинга репутации
- Аккуратное определение и блокирование редких угроз даже если они встречаются лишь у одного клиента Symantec

Плохая репутация
Файл **заблокирован**

Нет данных
Может быть заблокирован

Хорошая репутация
Файл **разрешен**

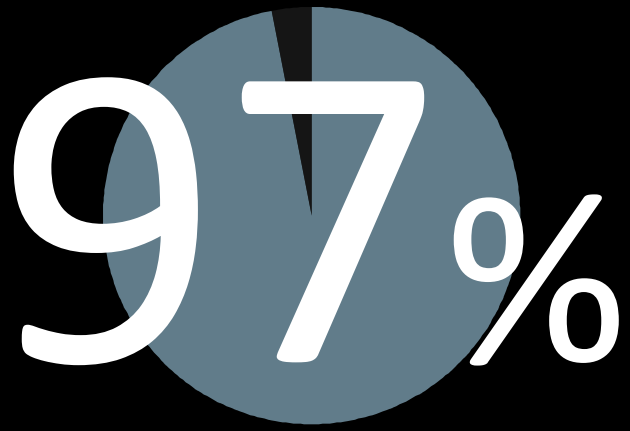
Глобальные знания

Конечные точки

Шлюзы

ЦОД

ЦОД: реальная цель

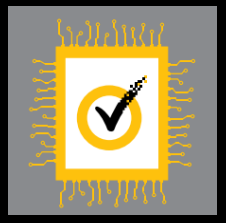


Данных украдено с серверов

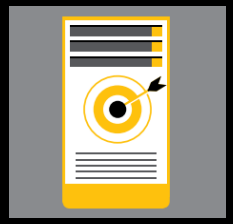
“ …. Рабочие станции и пользователи все чаше являются «точкой входа» в компанию, с которой злоумышленники начинают остальные стадии атак”

ЦОД: проактивная защита

Понижение привилегий с Symantec Critical System Protection



Усиление и защита инфраструктуры VMware



Защита контроллеров домена

Соответствие PCI

Остановка 0-day атак

Защита промышленных систем

Symantec останавливает направленные атаки

Глобальные знания

Конечные точки

Шлюзы

ЦОД

Сетевая защита для Mac

Disarm в почтовых шлюзах

Новое

Спасибо!