Microsoft Forefront Client Security

Косинов Максим
Менеджер по продуктам
Центр Информационной Безопасности
SOFTLINE

Новый бренд Forefront = безопасность

Forefront Edge Security – Безопасность периметра сети

Internet Security & Acceleration Server 2006 (ISA)

Forefront Server Security – Защита Exchange, SharePoint, Office Communication Server

Forefront Server Security Management Console	Forefront Security for Exchange Server (2007)	Forefront Security for SharePoint (2007, 3.0)	Forefront Security for Office Communication Server

2008

Forefront Client Security – Защита рабочих станций и файловых серверов

Forefront Client Security + Forefront Client Security Management Console

Microsoft Forefront Client Security

Единая антивирусная защита для рабочих мест, ноутбуков и серверных операционных систем, легкая в управлении и контроле

Единая защита

- Одно решение для защиты от программ-шпионов и вирусов
- Построена на технологиях, используемых широко в мире
- Эффективный ответ на угрозы безопасности
- Дополняет другие продукты информационной безопасности Microsoft

Упрощённое администрирование

- Единая консоль для простоты управления ИБ
- Одна политика для управления агентами безопасности
- Простота установки агентов и обновлений безопасности
- Прозрачная интеграция с существующей инфраструктурой

Прозрачность и управляемость

- Единая информационная панель актуальной информации об угрозах и уязвимостях
- Детальные отчеты с возможностью анализа
- Информация о предупреждениях ИБ и результатах соответствия шаблонам безопасности

Сертификация Forefront Client Security

http://www.microsoft.com/forefront/clientsecurity/prodinfo/awards/default.mspx

Сертификация ICSA Labs

- После завершения тестирования в лаборатории ICSA Labs Anti-Virus Certification Testing Laboratory, сертификат для Microsoft Forefront Client Security на Windows Server 2003 был получен 27 Июля 2007

Награда Virus Bulletin 100%

- Microsoft Forefront Client Security получил награду VB100 для защиты Windows XP SP2 иWindows Vista x64 Business Edition

Сертификация West Coast Labs Checkmark

- Forefront Client Security получил сертификат West Coast Labs' Checkmark, выполнив все условия по защите от Вирусов, Нежелательного ПО и Троянов.

Finalists - 2008 Global Excellence in Anti-Malware Solution

- These prestigious global awards recognize security and IT vendors with advanced, ground-breaking products and solutions that are helping set the bar higher for others in all areas of technologies. Forefront Client Security was voted a finalist by more than 11,000 voters worldwide consisting of end-users, channel partners and readers of Info Security Products Guide. Winners will be announced in November.

Gartner – Endpoint Protection Platforms, 2007

http://mediaproducts.gartner.com/reprints/microsoft/vol8/article3and4/article3and4.html

Source: Gartner (December 2007)

Что входит в пакет FCS?

- Дистрибутив FCS-сервер включает:
  - MOM 2005 SP1
  - MOM 2005 Reporting SP1
  - Дополнения для MOM, необходимые FCS
  - SQL 2005 Enterprise Edition [опционально]
  - FCS консоль и модуль отчетов

- Дистрибутив FCS-клиент включает:
  - Агент FCS
  - Программу сканирования соответствия шаблонам безопасности (Security State Assessment)
  - Агент MOM 2005 SP1
  - FCSLocalPolicyTool.exe

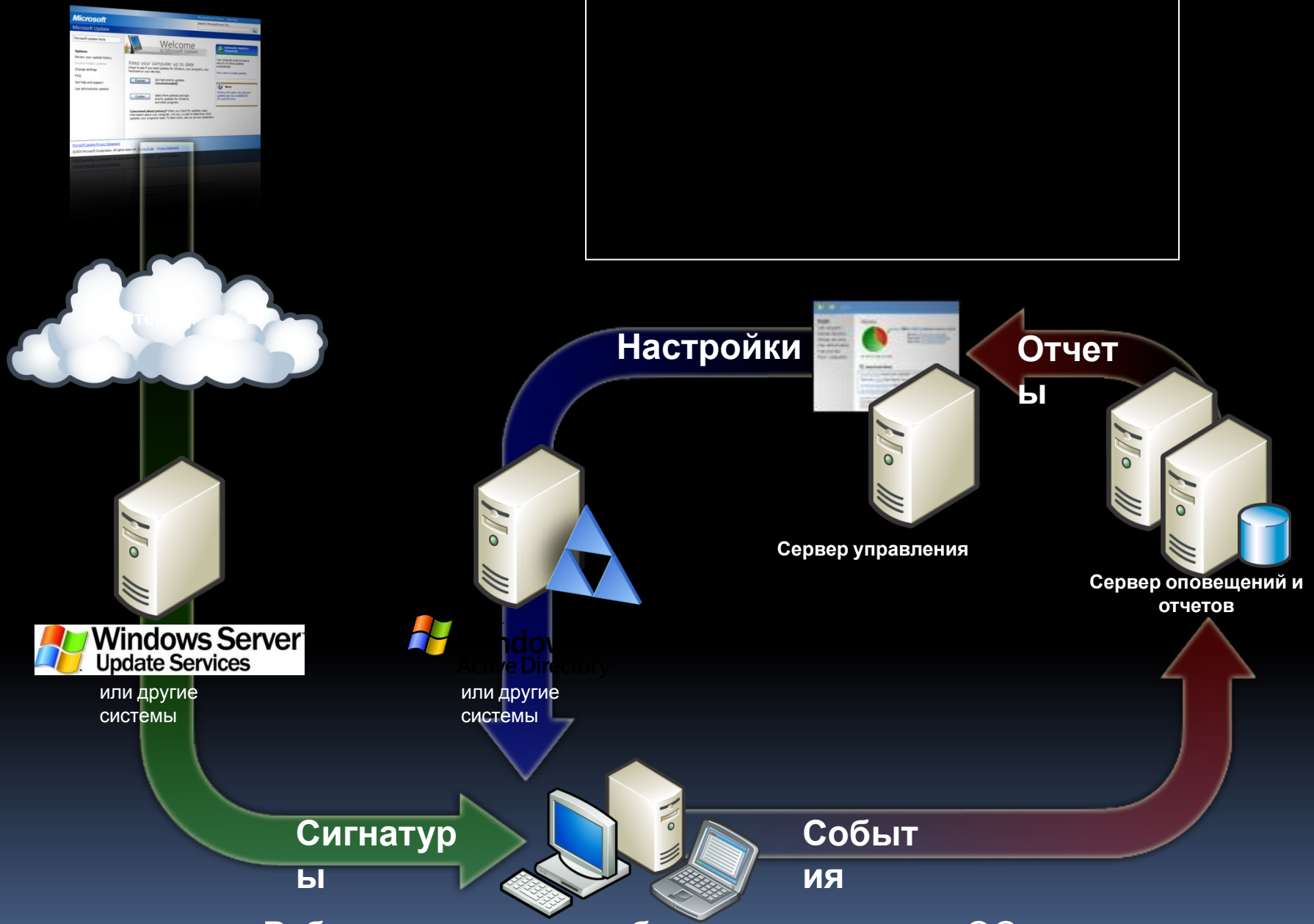
Поддерживаемые платформы

- Агент:
  - Windows 2000 SP4
  - Windows XP SP2, SP3
  - Windows Vista Business, Enterprise, Ultimate, Home, SP1
  - Windows Server 2003 SP1 & R2
  - Windows Server 2008 Standard, Enterprise
  - Поддержка x86 и x64
- FCS Сервер:
  - Windows Server 2003 SP1 & R2
  - SQL Server Standard or Enterprise
  - x86 only

Аппаратное обеспечение

- FCS Сервер:
  - Минимальное:
  - Процессор 1 GHZ
  - 1 GB RAM
  - 80 GB свободно на диске
  - DVD-ROM
- FCS Клиент
  - Минимальное:
  - Процессор 500 MHZ
  - 256 MB RAM
  - 350 MB свободно на диске

- Рекомендуемое:
- Процессор Dual 3.5 GHZ
- 3 GB RAM
- 250 GB свободно на диске
- DVD-ROM



Рабочие станции, ноутбуки или серверные ОС под управлением **Microsoft Forefront Client**

Варианты развертывания FCS

- 4 логических серверных роли:
  - Сервер управления (FCS console)
  - Сервер коллекций (MOM Ops + Operations DB)
  - Сервер отчетов (MOM Reporting + Reporting DB)
  - Сервер обновлений (WSUS)

- Варианты распределения ролей при масштабировании и использовании существующих серверов WSUS и SQL:
  - Один сервер – все в одном
  - Два сервера – Reporting DB + и все остальные роли
  - Сервер обновлений WSUS может быть вынесен на отдельный сервер
  - 4 сервера – каждая роль на отдельном сервере
    - Базы данных Operations и Reporting могут быть вынесены на отдельные серверы

Масштабируемость FCS

- FCS предназначен для использования на предприятиях среднего и крупного бизнеса
- Развертывание одного комплекта серверов FCS может обработать события от 10000 клиентов FCS
- Примеры внедрений:
  - Среднее предприятие (менее10 тысяч клиентов): один комплект FCS
  - Крупное предприятие (более 10 тысяч клиентов): несколько комплектов FCS
    - Каждый комплект обрабатывает события от 10 тысяч клиентов предприятия
    - Управление безопасностью в отдельных организационных единицах и/или доменах предприятия осуществляется локально на основании делегирования полномочий
    - В рамках программ пилотного внедрения (TAP/RDP) выполнены внедрения FCS на предприятиях с числом клиентов более 20 тысяч

Единая защита

Защита от широкого спектра угроз

- Один агент для защиты от вирусов и программ-шпионов
  - Общее ядро, используемое в таких продуктах как Windows Defender, OneCare, Forefront Server Security
- Защита на уровне ядра (Kernel mode) с помощью специального мини-фильтра, работающая в реальном времени
  - Основана на платформе Windows Filter Manager
  - Полный запрет на исполнение вредоносного кода – антивирус и анти-шпион
- Защита в пользовательском режиме работы (User mode), работающая в реальном времени
  - System Configuration, IE Add-ons & Configuration
  - Файлы, загружаемые IE и Office
  - Сервисы и драйвера
  - Исполнение и регистрация приложений
- Сканирование по расписанию и по запросу
  - Быстрое сканирование – процессы, находящиеся в памяти; целевые папки*, известные точки вхождения вредоносного кода в систему*
  - Полное сканирование – Быстрое сканирование + локальные диски

Единая защита

Защита от широкого спектра угроз

- Обновления сигнатур вредоносного кода и ядра агента
  - Один пакет обновлений для вирусов и программ-шпионов
  - Состоит из ядра (DLL файл), базы вредоностного кода и файла изменений, антивирусной базы и файла изменений
  - Динамическое обновление ядра без перезагрузки
  - Происходит ежемесячно или при появлении нового типа вредоносного кода
  - Загрузка только изменений обновлений
  - Публикуются на Microsoft Update 3-5 раз в день
  - Ежедневное обновление на Microsoft Update

Единая защита

Защита от широкого спектра угроз

- Поведением агента управляет ИТ администратор
  - Гибкие возможности настройки расписания сканирования (время и периодичность)
  - Частота обновления сигнатур, отказоустойчивость для мобильных пользователей
  - Исключения – расширения файлов, директории
  - Управление поведением при обнаружении сигнатуры
    - на основе кода
    - на основе категории кода
  - Управление интерфейсом пользователя
    - на основе политики – недоступны некоторые действия и настройки
    - полный запрет доступа к интерфейсу
  - Взаимодействие с сетью SpyNet
  - Совместимость с Windows Security Center и Vista NAP
    - Статус антивируса и анти-шпиона – включен/выключен и актуальность баз сигнатур.

Единая защита

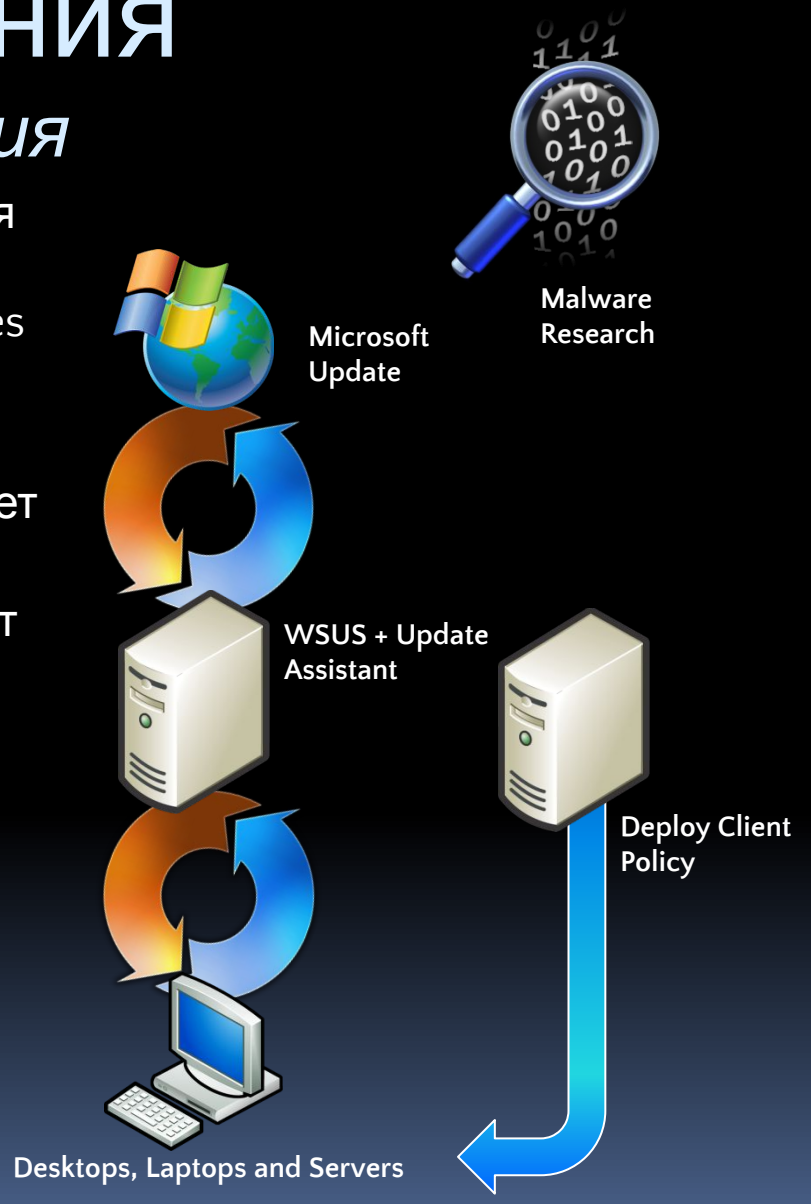
Защита от широкого спектра угроз

- Центр исследования вредоносного кода разрабатывает обновления баз данных сигнатур вредоносных программ для:
  - Forefront Client Security, Forefront Server Security, Windows Live OneCare, Windows Defender, Malicious Software Removal Tool (MSRT)
  - На данный момент под защитой этих продуктов находятся миллионы систем
- Команда исследователей использует различные источники для обнаружения угроз
  - Продукты: Windows Defender, OneCare, MSRT и т.п.
  - Другие источники: PSS, Hotmail, сканирование Интернет, сообщения клиентов
  - Партнерство с другими производителями программного обеспечения информационной безопасности
- Автоматизация при анализе: база данных вредоносного кода, автоматический учет сообщений, приоритет при выборе образцов для анализа
- Центр исследования и поддержки круглосуточно и ежедневно (24x7)
- Сертификация индустрии
  - West Coast Labs, ICSA Labs – в процессе

Простота управления

Возможности развертывания

- Дистрибутив клиента FCS оптимизирован для установки через веб-узел Microsoft Update (MU) и службу Windows Server Update Services (WSUS)
  - Пакет FCS публикуется на MU
  - WSUS синхронизируется с MU и загружает пакет клиента FCS
  - Администратор настраивает и применяет политику агента FCS
  - Клиент синхронизируется с WSUS – загружает, устанавливает агента и применяет политику
  - Отчет об установке на WSUS и FCS
- Можно использовать Microsoft SMS, командные файлы, групповые политики и любое ПО распространения приложений



Простота управления

Возможности развертывания

- Единая консоль для управления информационной безопасностью
- Одна политика управления настройками агента
  - Расписание сканирования
  - Включение/отключение защиты реального времени
  - Частота обновлений
  - Переопределение действий агента для программ-шпионов
  - Настройка сканирования соответствия шаблонам безопасности
  - Действия в случае неизвестного кода, классифицируемого как возможно вредоносный
  - Уровень оповещений
  - Настройки журналирования
  - Взаимодействие со SpyNet да/нет
  - Уровень блокировки интерфейса
- Варианты распространения профайла настроек агента:
  - Консоль Microsoft Forefront Client Security Console (использует AD/GP)
  - Файл политик ADM (использует AD/GP)
  - Экспорт в файл и распространение через существующее ПО

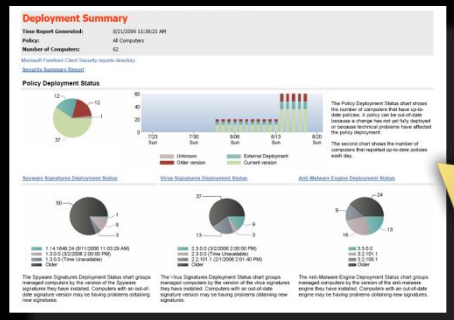
Простота управления

Настройка оповещений

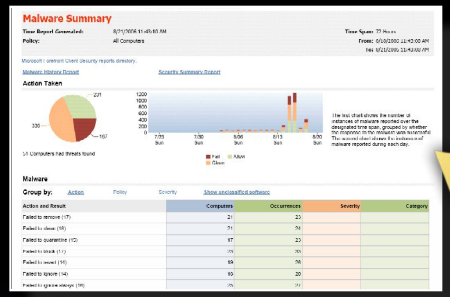
- Управление оповещениями через консоль оператора MOM 2005
- Дифференциация уровня оповещений (определяется политикой)
- Оповещения предупреждают администратора о:
  - Обнаруженном вредоносном коде
  - Коде, который не удалось удалить
  - Возможном начале вирусной атаки
  - Деактивации защиты
- Уровни настройки оповещений по типу и объему

Информативность & Контроль

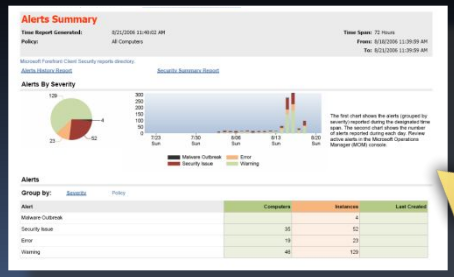
Сводные отчеты



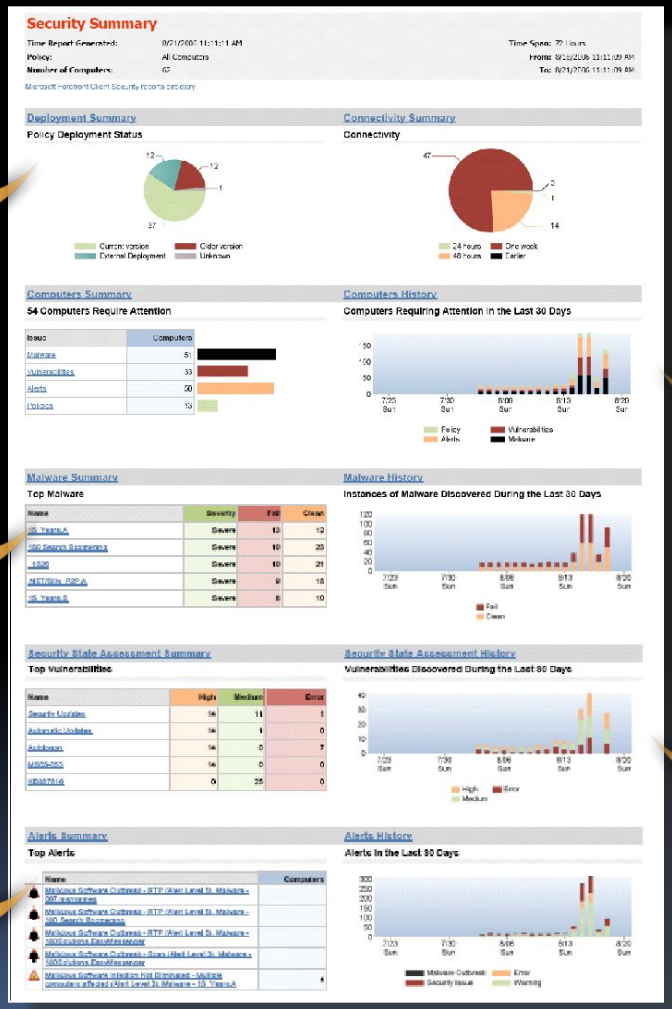
Deployment Summary

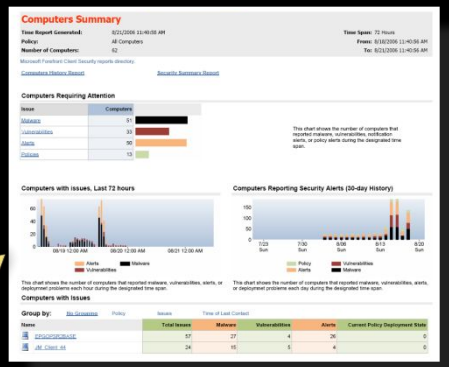


Malware Summary

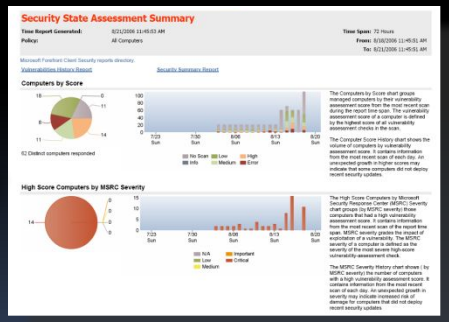


Alerts Summary





Computer Summary



Security State Assessment Summary

Информативность & Контроль

Сканирование соответствия шаблонам безопасности

SSA Host агент:

- Выполняет сканирование на основании шаблонов безопасности
- Сканирование выполняется на основании политики или по запросу

Проверяет

- Отсутствующие обновления безопасности, опубликованные на веб-узле Microsoft Update
- Сравнивает конфигурацию системы на соответствие шаблонам безопасности, основанным на рекомендациях по безопасности
  - Исследует данные реестра, файловую систему, WMI, метабазу IIS, SQL и т.д.
- Проверяет возможность обновления через Microsoft Update

Определяет "Оценку" и "Критичность" :

- Оценка – риск, связанный с обнаруженной проблемой безопасности
- Критичность – используется MSRC для обновлений безопасности

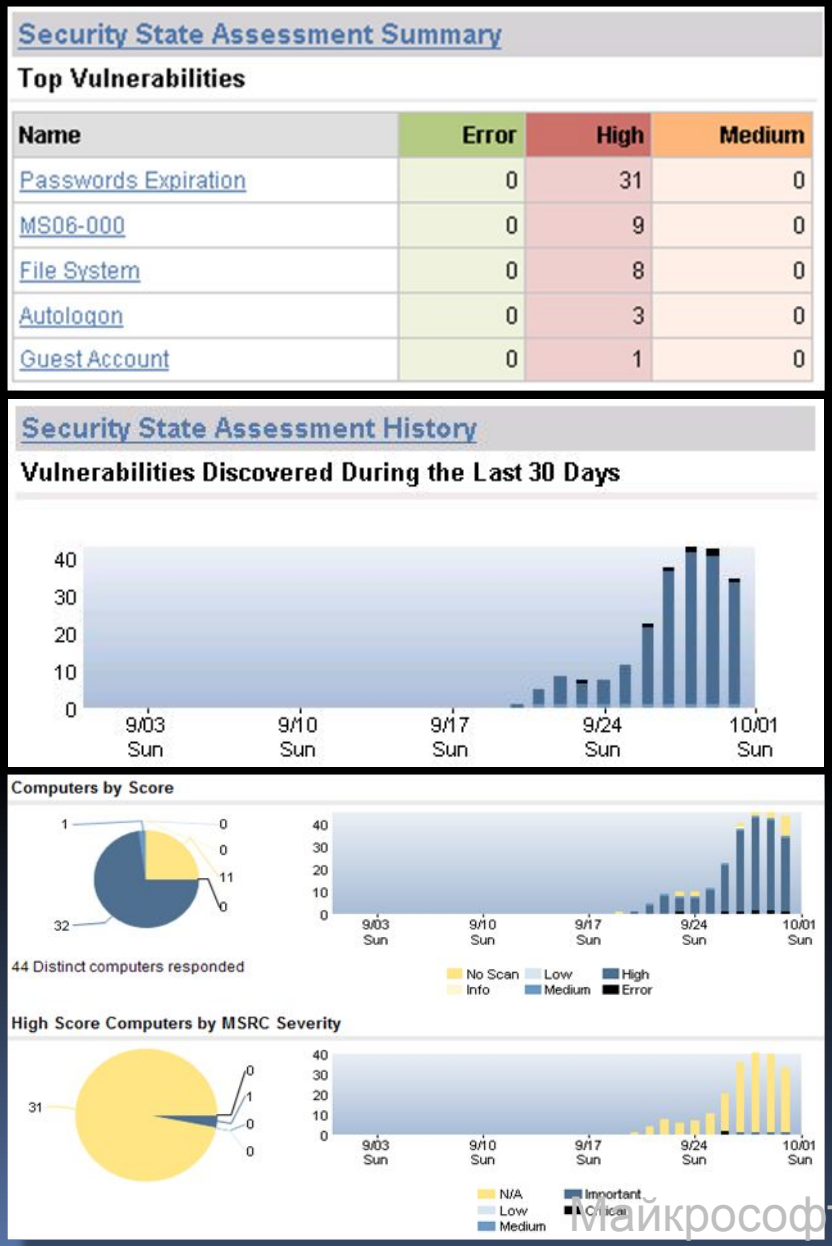
Отчеты позволяют провести детальный анализ каждой проблемы

Информативность & Контроль

“Соответствует ли моя инфраструктура рекомендациям по безопасности?”

“Как изменяется во времени уровень уязвимости системы?”

“Какая часть моей инфраструктуры наиболее уязвима?”



Security State Assessment Summary

Top Vulnerabilities

Name	Error	High	Medium
Passwords Expiration	0	31	0
MS06-000	0	9	0
File System	0	8	0
Autologon	0	3	0
Guest Account	0	1	0

Security State Assessment History

Vulnerabilities Discovered During the Last 30 Days

Computers by Score

44 Distinct computers responded

High Score Computers by MSRC Severity

Лицензирование

Ежегодные платежи по программам:

- Малый и средний бизнес – Open Value/ Open Value Subscription
- Крупные компании – Enterprise Agreement/ Enterprise Agreement Subscription

FCS лицензируется из расчёта количества польз./устройств = 16 USD (для Open Value)

+

FCSMC лицензируется из количества серверов управления = 3120 USD / 120 USD (для Open Value)

Case studies

Founded in 1986, Convergent Computing (CCO) is a Microsoft® Gold Certified Partner that helps customers better manage their IT networks. In early 2006, CCO wanted to replace its multiple security products because they had become difficult to manage. As a participant in Microsoft early adoption programs, CCO had heard about the upcoming Microsoft Forefront™ family of security software. The company knew that Forefront would integrate easily into its IT environment, which is based on the Microsoft server product portfolio. After testing beta versions of the software, CCO implemented a comprehensive security solution including Microsoft Forefront Client Security. CCO now benefits from an integrated IT environment that requires less time to manage and saves money.

Analog Devices makes more than 10,000 different integrated circuits that are used in electronic products. Security is critical to protecting its computing resources, including PCs, servers, and the network. Analog Devices had antivirus software to protect its PCs, but wanted to increase its level of protection and its ability to respond quickly to virus outbreaks. For that reason, Analog Devices deployed Microsoft® Forefront™ Client Security. The company has already benefited from faster identification and cleansing of viruses that could have affected its IT infrastructure. Forefront Client Security also provides easy-to-use administrative tools that help the company's IT department be more efficient in the deployment of antivirus and antispyware updates and policies. And it provides reporting functions that help IT staff clearly understand the state of the company's PC security.

Стоимость владения (TCO)

Стоимость внедрения Forefront Client Security = $16.50*

Эффект от внедрения (снижение кол-ва инцидентов)= $24*
Дополнительный эффект для IT администраторов = $7.50*
* - на одну рабочую станцию

Итог – реально эффективное решение

По данным исследования По данным исследования Value Prism Consulting

Дополнительная информация

- Microsoft:
  - http://www.microsoft.com/rus/forefront/clientsecurity/
  - Пробная версия на 120 дней!
  - Виртуальные лаборатории
  - Вебинары
- Softline:
  - Косинов Максим [Product-manager]
    Тел: +7 495 232 00 23 доб. 0390
    Моб: +7 903 220 05 69
    Email: maximKos@softline.ru

Спасибо за внимание!