SRM: Стратегия надежного управления рисками McAfee

Сравнение данных Vulnerability Manager с измененными правилами безопасности предприятия для установки степени соответствия.

Защита данных

Network DLP Appliance

Поддержка классификации данных и поиска важных для предприятия сведений в корпоративных сетях, вследствие чего сокращается время проектирования дополнений DLP.

Доступно как: Network DLP Manager, Network DLP Monitor, Network DLP Prevent, Network DLP Discover

Host Data Loss Prevention

Защита конфиденциальных данных от несанкционированной передачи на конечных устройствах.

- **Реализация правил безопасности:** полный контроль доступа и отправки конфиденциальных данных по электронной почте, при помощи приложений P2P, IM, Skype HTTP, HTTPS, FTP, Wi-Fi, USB, CD, DVD, принтеров и мобильных запоминающих устройств.
- **Абсолютная защита файлов:** блокирование потерь данных даже при их изменении копировании, вводе, архивировании или кодировании.

В дополнение к размещенной на хосте защите доступно также устройство DLPAppliance для предотвращения потери данных (в частности в портативных компьютерах посетителей), серверов и устройств без агентов DLP.

Device Control

Управление использованием внешних носителей информации в сети.

- **Комплексное управление устройствами и данными:** регулирование способов копирования пользователями данных на USB-накопители, устройства iPod, записывающие CD и DVD, Bluetooth-и инфракрасные устройства.
- **Функции мониторинга и оповещения**

Encrypted USB

Защита мобильных запоминающих устройств.

- **Надежное запоминающее устройство USB-Flash:** защита мобильных дан ных с помощью установленного аппаратного кодирования AES-256.
- **Бездрайверная технология «Zero-Footprint»:** наибольшая универсальность без необходимости установки программного обеспечения или прав администратора.
- **Проверка подлинности при помощи двух факторов:** пароль и второй спо соб идентификации.

Endpoint Encryption

Защита данных во всех возможных местоположениях запоминающих устройств.

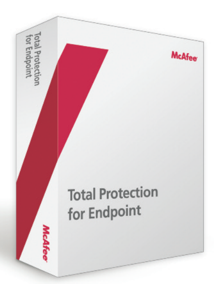
- **Кодирование на 360 градусов:** кодирование с надежной защитой данных на персональных компьютерах, в файлах и реестре,на мобильных устройствах, таких, как портативные компьютеры, виртуальные носители данных, а также носители изменяемых данных.
- **Мощный контроль доступа:** предотвращение несанкционированного доступа с помощью аутентификации перед загрузкой.

Total Protection for Data

Total Protection for Secure Business включая Email and Web Security Virtual Appliance-Software за исключением Endpoint Encryption for Devices

Безопасность системы

Total Protection for Endpoint



Защита от вирусов и шпионских программ, а также функции безопасной работы в Интернете для настольных компьютеров и серверов. Кроме того, такие защитные механизмы, как Host Intrusion Prevention, Desktop Firewall, а также защита сервера электронной почты от нежелательной почты и вирусов.
Улучшенная версия дополнительно содержит McAfee Network Access Control и McAfee Policy Auditor for Desktop для обеспечения отсутствия на конечных устройствах уязвимых местоположений, ошибок конфигурации, а также нарушения инструкций.

Total Protection Service

Встроенный сервис защиты настольных компьютеров, а также файловых серверов, от вирусов и шпионских программ McAfee.

Сетевой брандмауэр

Firewall Enterprise Appliance (Sidewinder)*

Контроль перемещения данных благодаря многофункциональному устройству Unified Threat Management (UTM).

- **Защита от угроз любого рода:** технология TrustedSource™ для упреждающего обнаружения рисков.
- **Фильтрация приложений:** защита веб-сайтов от посторонних скриптов, ввода команд SQL, поиска по директориям и т.д.
- **Защита от опасностей при помощи закодированных приложений:** Расшифровка и фильтрация перемещения закодированных данных с помощью SSH, SFTP, SCP и SSL/HTTPS.

*ранее Secure Firewall

UTM Firewall Appliance*

Надежные сетевые приложения для предприятий малого и среднего бизнеса.

- **Универсальность применения:** применение в качестве брандмауэра, шлюза VPN, безопаснось приложений UTM или полных надежных UTM сетевых приложений.

*ранее Secure SnapGear

Централизованное, полностью интегрированное управление и отчетность.

Предоставление Network Security Manager сведений об уязвимых местах с возможностью нейтрализации атак одного приоритета. Благодаря этому оператор может сконцентрироваться на существенных атаках.

Total Protection for Endpoint-Advanced McAfee NAC-Software

Централизованное, полностью интегрированное управление и отчетность.

Контроль уязвимых мест

Vulnerability Manager*

Идентификация и оценка риска уязвимых мест и недостатков защиты для установки приоритетов в устранении ошибок.

- **Соблюдение законодательных и корпоративных положений:** модели сертификации для SOX, FISMA, HIPAA, PCI и других законодательных положений, а также оценки реализации корпоративных нормативов.
- **Определение новых угроз и установление связи между ними:** при выявлении потенциального риска новых угроз с одновременным определением воздействия уяз вимых местоположений по отношению к ресурсам предприятия с помощью функции Threat Correlation.

*ранее McAfee Foundstone Enterprise

Импортирование уже существующих структур, инвентаризация и оценка данных, а также установленные защитные механизмы, которые объединяются при оценке обнаруженных уязвимых мест и таким образом повышают достигнутый уровень защиты.

Управление и отчетность

ePolicy Orchestrator®

Центральная консоль управления для оптимизации надежности ИТ и соблюдения нормативов.

- **Эффективные, распространяющиеся на продукцию возможности интеграции**
- **Унифицированное управление, а также отчетность и аудит**
- **Быстрая реакция на атаки вирусов и опасные ситуации**
- **Непревзойденная скорость обновления**
- **Консоль на основе сети с возможностью охвата в любом месте в любое время**
- **Открытая совместная организация: Інтеграция более 50 стратегических технологических партнерств в рамках McAfee Security Innovation Alliance (SIA) с целью защиты от угроз, минимизации рисков, а также обеспечения соблюдения нормативов.**

Интеграция в ePO обеспечивает легкость направления, централизованное управление и осуществление руководства на уровне всего предприятия.

Совместная работа Network Security Manager и ePolicy Orchestrator помогает при анализе атак (запрос имеющихся защитных механизмов, а также вирусов и событий Host-IPS).

Предотвращение вторжений в сеть

Network IPS*

Превентивная защита инфраструктуры сети и конечных устройств программ.

- **Защита предприятия в режиме реального времени:** перед современными и будущими угрозами, даже для неразработанных систем.
- **Панель мониторинга:** полный обзор угроз и системный обзор при помощи диспетчера оповещений в режиме реального времени и графические отчеты.
- **Защита сети следующего поколения:** также для имеющихся в распоряжении сетей 10 гигабит (единственное сертифицированное NSS Group решение IPS).*ранее McAfee IntruShield*

Контроль доступа в сеть

Network Access Control

Защита сети от несоответствующих правилам рабочих мест.

- **Определение нарушений правил:** распознавание управляемых и неуправляемых компьютеров, которые могут причинить вред сети.

Имеется также устройство NAC-Appliance, относящееся к Network Security Platform и подходящее, в частности, для проверок доступа на линию без дополнительной функциональности IPS.

Анализ поведения пользователя в сети*

Выделенные устройства NAC-Appliance, наблюдающие за всем доступом в сеть, а также за поведением пользователей, и приводящие его в соответствие с действующими правилами.

*ранее Securify

Total Protection for Compliance, включающее ePO Risk Advisor (ранее CARMA)

Передача данных инвентаризации и оценки с целью обеспечения централизованной базы данных и получения унифицированных, а также содержательных сообщений.

Vulnerability Manager передает информацию о слабых местах в Remediation Manager, с помощью которого они могут быть устранены.

Объединение с ePolicy Orchestrator предусматривает распределение диспетчеров Remediation Manager. Теперь отчет передается также по отдельной консоли.

Централизованное, полностью интегрированное управление и отчетность.

Модуль McAfee NAC для McAfee Network IPS поддерживает гостевой доступ при помощи согласования NAC и Network Intrusion Prevention

Анализ рисков и соответствия

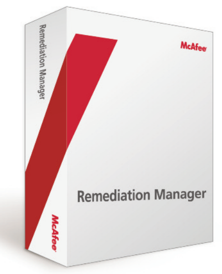
Risk & Compliance Manager

Автоматическая консолидация данных уязвимых мест, данных конфигурации и данных об угрозах для отчета о соответствии.

- **Отчеты о соответствии:** генерирование сводных и подробных анализов соответствия по всей ИТ-инфраструктуре.
- **Панель мониторинга для рисков безопасности:** в настраиваемом обзоре указываются консолидируемые уязвимые места и ошибки конфигурации.
- **Открытая архитектура:** интеграция в другие уязвимые места, управление пакетами исправлений, а также решения конфигурации через открытые API и SDK.

Управление пакетами исправлений

Remediation Manager



Реализация правил безопасности и устранение таких слабых мест, как пакеты исправлений, необеспеченные учетные записи пользователей, ненужные службы, ошибочные конфигурации и "черные входы".

Управление соответствием нормативам

Policy Auditor

Подтверждение соответствия при помощи правил безопасности.

- **Правила для всех устройств ИТ:** Policy-Templates для Sarbanes-Oxley, GBLA, HIPAA, NSA и SANS Top 20.
- **Панель мониторинга:** Первоначальное указание состояния соответствия, уязвимых мест и общего риска.

Безопасная работа в Интернете и с электронной почтой

Email & Web Security Appliance*

Защита от шпионских программ, вирусов и нежелательной почты, а также фильтрация содержимого для предотвращения угроз через Интернет и электронную почту.

- **Превентивная защита от вирусов и шпионских программ:** известные и неизвестные угрозы останавливаются непосредственно шлюзом (SMTP, Pop 3, HTTP, FTP, а также протоколы iCap).
- **Проверенная технология борьбы со спамом:** благодаря инновационным технологиям, таким как Domain-Name & IP-Reputation, фильтрация образов, анализ целостности, эвристическое узнавание, а также списки Blacklist и Whitelist.

*ранее McAfee Secure Internet Gateway

Content Security Blade Server

Обработка до 5 млн. сообщений в час при одновременной защите до 50 000 интернет-пользователей, включая фильтрацию URL и нежелательной почты, защиту от фишинга, а также поисковую машину с блокировщиком вредоносных программ.

Web Gateway Appliance*

Комплексное решение по защите для всех аспектов перемещения данных по сети Web 2.0.

- **Мощная фильтрация Web:** постороннее содержимое больше не попадает в сеть, вследствие чего сокращаются потери производительности, а также потребление полосы пропускания; предотвращается риск нарушения нормативов.
- **Упреждающая защита от вредоносных программ:** веб-страница и опознавание потенциальных угроз обеспечивают защиту от Malware , Spyware, атак Zero Day, скрытых угроз и целенаправленных атак.
- **Защита при перемещении закодированных данных:** исследование всего перемещения SSL приложениями, вследствие чего гарантируется надежность, целостность и защита данных транзакции SSL.

*ранее Webwasher

Email Gateway Appliance*

На рынке ключевых надежных приложений электронной почты предлагается полный ассортимент двунаправленных защитных технологий защиты входящих и исходящих электронных сообщений.

- **Соблюдение правил соответствия нормативам:** модуль кодирования сообщения предлагает подробное определение правил, вследствие чего могут приниматься LDAP или группы и нормативы Active Directory, а также определенные признаки сообщений.
- **Широкая защита от нежелательной почты:** контроль электронной почты с отклонением нежелательных сообще ний на основании репутации.
- **Фильтрация исходящего содержания:** автоматическое распознавание и защита конфиденциальных данных с помощью фильтрации, подгонки под образец, узнавания цифровых отпечатков, кластеризации, адаптивного узнавания слов и выражений.

*ранее IronMail

Передача сведений через Policy Auditor в Remediation Manager относительно обнаруженных уязвимых мест, ошибочной сервисной конфигурации и нарушений правил.

Total Protection for Endpoint-Advanced, включая Policy Auditor for Desktops

ООО «МакАфи РУС» \ Адрес: 123317, Россия, Москва \ Краснопресненская набережная, д.18 \ Блок «С», бизнес центр «Башни на набережной» \ 4-й этаж, офис 405 \ www.mcafee.com