McAfee ePO Deep Command

Управление средствами защиты за пределами операционной системы позволяет снизить расходы на эксплуатацию

Сотрудникам вашей службы поддержки больше не придется так часто выезжать к клиентам и отвечать на звонки в службу поддержки в случае возникновения аварийных ситуаций, вирусных эпидемий или потери паролей шифрования. У администраторов наконец появилась возможность осуществлять развертывание, управление и обновление средств защиты на выключенных, деактивированных или зашифрованных конечных точках. Программное обеспечение McAfee® ePO™ Deep Command[1] использует технологию Intel® vPro™ Active Management Technology (AMT) для автоматизированного управления конечными точками за пределами операционной системы, что позволяет снизить эксплуатационные расходы, повысить уровень безопасности и нормативно-правового соответствия и сократить время на дистанционное устранение проблем ПК и устройств с фиксированными функциями.

Ключевые преимущества

- **Быстрое обнаружение компьютеров с поддержкой технологии Intel AMT и ее развертывание.** Быстрая идентификация ПК, оборудованных Intel vPro, с последующим включением Intel AMT для быстрой активации.
- **Безопасное разблокирование.** McAfee ePO Deep Command, используемый в сочетании с комплектами McAfee Complete Data Protection, дает возможность безопасно разблокировывать предзагрузочные среды зашифрованных конечных точек и получать к ним доступ.
- **Сокращение времени восстановления систем.** Управление удаленным восстановлением любого ПК или конечной точки в любой точке мира с помощью доступа на аппаратном уровне.

Администраторы, управляющие средствами защиты, находятся под постоянным давлением из-за роста издержек, увеличения числа угроз, а также повышения уровня требований со стороны своих компаний. Каждый вызов специалиста для решения проблем, вызванных вредоносными программами или другими угрозами, может стоить компании до 250 долларов. Кроме того, специалист из службы поддержки просто физически не в состоянии добраться до каждого пользователя. Удаленные офисы, сотрудники, работающие дома, вынуждены звонить в службу поддержки и посылать свои устройства в пункт технического обслуживания службами экспресс-доставки. Такие пользователи очень заняты, часто игнорируют возникающие у них проблемы и работают на уязвимых системах, не отвечающих нормативно-правовым требованиям, до тех пор, пока не произойдет крупная авария, не отключится система или не нарушится работа в результате действия вредоносных программ.

Всё это происходит на фоне постоянно растущих угроз безопасности для конечных точек! Тем временем киберпреступники быстро осваивают новые уязвимости и используют бот-сети и веб-сайты для распространения программ-невидимок и вредоносных программ «нулевого дня». Некоторые вредоносные программы уже в состоянии деактивировать защитные меры, принимаемые на уровне операционной системы, позволяя злоумышленникам привести компьютер и устройства с фиксированными функциями в полную негодность.

intel Security

Ключевые преимущества (продолжение)

- **Повышение производительности работы пользователей.** Выполнение ресурсоемких задач в нерабочее время сохраняет производительность пользователей.
- **Снижение затрат на ИТ.** Возможность избежать частых вызовов специалистов и продолжительных звонков в службу поддержки.
- **Снижение энергопотребления конечных точек.** Реализация программы экономии электроэнергии с сохранением доступа к системам для выполнения задач обеспечения безопасности и установки исправлений.

Еще больше усложняет ситуацию тот факт, что под давлением требований экономии электроэнергии руководители отделов ИТ рассматривают бездействующие настольные компьютеры в качестве потенциального фактора энергосбережения. Им хотелось бы отключить неиспользуемые системы от питания, но для этого им нужен надежный способ управления безопасностью и нормативно-правовым соответствием выключенных систем, а также механизм запуска необходимых процессов (поиск уязвимостей, установка обновлений или исправлений) в такое время, когда это менее всего мешает пользователям.

Как обнаруживать и активировать платформы с Intel vPro

Приложение McAfee ePO Deep Command позволяет в полном объеме использовать преимущества технологии Intel vPro, предлагающей такие функции, как Intel AMT Alarm Clock («Будильник»), удаленное включение систем, поддержку KVM-коммутаторов (для подключения клавиатуры, монитора и мыши), а также перенаправление IDE. С помощью модуля McAfee ePO Deep Command Discovery and Reporting вы сможете обнаружить в своем окружении ПК и конечные точки, оснащенные технологией Intel vPro AMT, и на основе подробных отчетов точно определить, на каких ПК и конечных точках можно провести развертывание агента McAfee ePO Deep Command. Кроме того, использование McAfee ePO Deep Command оптимизирует процедуру подготовки Intel AMT, упрощая процесс активации этой технологии. Установив программное обеспечение McAfee ePO Deep Command на компьютерах и конечных точках с поддержкой технологии AMT, вы сразу можете начать удаленно управлять ими на аппаратном уровне за пределами операционной системы.

Средства удаленного управления приходят на помощь

Теперь администраторы систем безопасности могут обмениваться информацией с конечными точками и управлять ими на аппаратном уровне, даже если системы выключены, деактивированы или зашифрованы. Подключение к оборудованию дает администраторам возможность удаленно управлять системами, добиваясь применения политик защиты и нормативно-правового соответствия, а также снижения эксплуатационных издержек. Помимо обеспечения более высокого уровня защиты средства удаленного управления позволяют реализовывать программы управления энергопотреблением с целью экономии электроэнергии без снижения доступности конечных точек. Благодаря использованию технологии Intel vPro AMT платформа McAfee ePO Deep Command сможет получать доступ к конечным точкам без участия операционной системы. Возможность доступа к системам на аппаратном уровне позволяет администраторам включать системы, выполнять задачи обеспечения безопасности и затем возвращать конечные точки в прежний режим энергопотребления. Платформа McAfee ePO Deep Command может даже инициировать безопасную загрузку системы на удаленных точках, на которых установлено программное обеспечение McAfee Complete Data Protection для шифрования конечных точек. При этом, для удаленного выполнения задач не нужно вводить учетные данные пользователя, обычно требующиеся для аутентификации. Все эти операции осуществляются путем автоматического включения компьютера либо с помощью функции Alarm Clock («Будильник»), либо путем включения компьютера по требованию.

Осуществляя обмен информацией с конечными точками на уровне, находящемся за пределами операционной системы, McAfee ePO Deep Command позволяет конфигурировать и обновлять трудноуправляемые конечные точки из центрального пункта, используя хорошо известную вам платформу управления — McAfee ePO.

Требования к системе

- McAfee ePO 4.6 (модуль Discovery and Reporting), McAfee ePO 4.6 (McAfee ePO Deep Command); McAfee ePO 5.0 и выше
- McAfee Agent 4.5 или выше
- McAfee Drive Encryption 7.0 и выше (для удаленного управления средствами шифрования)
- Поддерживаемые операционные системы: Microsoft Windows XP, Windows Vista, Windows 7, Windows 8, Windows Server 2003, Windows Embedded XP, Windows Embedded 7
- Поддерживает Intel vPro AMT версий 2.2 и выше
- Intel Setup and Configuration Software (SCS) 8.2 и выше

Пробуждение компьютера и принятие мер безопасности

У администраторов появится возможность в нерабочие часы, не отвлекая пользователей, выполнять текущее обслуживание систем и другие задачи, требующие больших затрат времени. Функция AMT Alarm Clock («Будильник») дает администраторам систем безопасности возможность включать и пробуждать конечные точки для выполнения следующих задач безопасности:

- обновление средств защиты и конфигураций (включая DAT-файлы);
- выполнение проверок по требованию;
- установка дополнительных защитных продуктов;
- формирование отчетов о событиях;
- установка пакетов исправлений для приложений и операционной системы.

Удаленное восстановление отключенных конечных точек

При возникновении таких проблем, как отключение операционной системы или отказ жесткого диска, на помощь администраторам и конечным пользователям приходят интегрированные средства управления, которые активируются с помощью решения McAfee ePO Deep Command. Независимо от того, где установлены соответствующие ПК/конечные точки — локально или удаленно, администратор может подключаться к выключенным ПК/конечным точкам и KVM-коммутаторам через AMT и проводить, например, удаленную загрузку ПК с другого ISO-образа, находящегося в сети. В большинстве случаев конечная точка не обязательно должна иметь кабельное подключение к сети. McAfee ePO Deep Command может управлять конечными точками с поддержкой защищенных подключений по Wi-Fi.

Функция Intel AMT Fast Call for Help («Быстрый вызов помощи») предоставляет пользователям простой способ связи с администраторами по программному обеспечению McAfee ePO для получения помощи. Администратор по программному обеспечению McAfee ePO может быстро выполнить следующие действия:

- настроить конечную точку на запуск с образа, находящегося в другой точке сети;
- полностью управлять локальным KVM-коммутатором;
- восстанавливать пользовательские пароли шифрования;
- провести чистку и восстановление зараженных, отключенных и помещенных в карантин систем без физического доступа к ним.

Защита, которая всегда опережает угрозы

Благодаря этому многофункциональному средству управления отделы информационной безопасности получили новые способы упреждающей защиты конечных точек от постоянно возникающих угроз. Появилась возможность обновлять системы еще до того, как они столкнутся с потенциальной угрозой, и удаленно активировать меры противодействия, обеспечивающие сохранность данных и предотвращающие падение производительности пользователей.

Рис. 1. McAfee ePO Deep Command может обнаруживать системы с vPro и проводить развертывание программного обеспечения для активации Intel AMT.

Снижение энергопотребления конечных точек

Благодаря возможности пробуждать компьютеры, обновлять политики, а затем безопасно возвращать конечные точки в исходный режим питания McAfee ePO Deep Command позволяет вашей компании без малейшего риска реализовывать отраслевые программы и меры, направленные на энергосбережение, не опасаясь снизить уровень своей безопасности. Свяжитесь с компанией McAfee, чтобы получить подробную информации о возможностях экономии электроэнергии.

Масштабируемость и отчетность корпоративного класса

McAfee ePO Deep Command расширяет функциональность платформы ePolicy Orchestrator® (McAfee ePO™), зарекомендовавшей себя как надежное средство управления, масштабируемое до сотен тысяч конечных точек. Платформа McAfee ePO, предназначенная для поддержки распределенных архитектур и отделов по управлению средствами защиты, позволяет централизованно управлять политиками безопасности и средствами отчетности в масштабах всей инфраструктуры защитных продуктов McAfee, используемых в вашей организации. Теперь же с ее помощью вы можете расширить сферу действия политик безопасности и нормативных-правовых требований, распространив ее за пределы операционной системы. Увеличив объем информации, отображаемой на панелях мониторинга и в отчетах McAfee ePO, вы получаете более полное представление о степени нормативно-правового соответствия каждой конечной точки и об общем уровне безопасности своей организации. Наличие сопоставленных данных облегчает проведение аудиторских проверок.

Для получения дополнительной информации посетите веб-страницу **www.mcafee.com/ru/products/epo-deep-command.aspx**.

Программное обеспечение McAfee ePO Deep Command можно приобрести либо в виде отдельного продукта, либо в составе комплектов McAfee Complete Data Protection. Для получения более подробных сведений посетите наш сайт **www.mcafee.com/ru/products/data-protection/index.aspx**.

Рис. 2. McAfee ePO Deep Command дает службе поддержки возможность выполнять некоторые задачи либо локально, либо удаленно.

McAfee. Part of Intel Security.
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
БЦ «Башни на набережной»,
Башня «А», 15 этаж
Телефон: +7 (495) 653-85-13
www.intelsecurity.com

1. Программное обеспечение McAfee ePO Deep Command можно приобрести либо в виде отдельного продукта, либо в составе комплектов McAfee Complete Data Protection. За дополнительной информацией обращайтесь по адресу **www.mcafee.com/ru/products/data-protection/index.aspx**.