Программное обеспечение IBM
Tivoli

Обеспечение безопасности и соответствия нормативным требованиям для распределенных конечных устройств

ПО IBM Tivoli Endpoint Manager, построенное на базе технологии BigFix, обеспечивает глобальный контроль и управляемость инфраструктуры

Ключевые моменты

- Решение проблем управления и соблюдения нормативных требований при повышении степени безопасности.
- Представление актуальных данных и средства контроля с помощью единой консоли управления.
- Автоматическая установка исправлений для разных операционных систем и приложений.
- Повышение скорости окупаемости распределенной ИТ-инфраструктуры.

Современные сложные среды объединяют множество различных серверов, настольных и переносных ПК, а также специализированное оборудование, такое как торговые терминалы, банкоматы и киоски самообслуживания. В качестве общего названия для всех этих устройств в рамках единой инфраструктуры принят термин «конечные точки». В условиях, когда количество конечных точек растет беспрецедентными темпами, традиционных схем защиты, таких как межсетевые экраны, уже недостаточно. Количество удаленно работающих сотрудников быстро увеличивается, как и парк мобильных устройств, и сегодня уже нельзя очертить четкий периметр корпоративной среды, который необходимо защищать. Периметром по необходимости должна быть сама конечная точка.

Конечные точки по своей природе являются чрезвычайно уязвимыми для атак. Это могут быть нарушения в работе систем, обусловленные действием вредоносных программ, похищение конфиденциальной информации посредством фишинга и дискредитация личных данных через социальные сети. Это также может выражаться в снижении продуктивности из-за рассылок спама, прерываний или нестабильной работы системы. Такие слабости могут представлять значительный риск, включая потерю управления над конечными точками и возможность утраты важных данных. Подобные угрозы в той или иной степени присущи для любой конечной точки в вашей организации.

Многих из названных проблем являются результатом того, что на конечных точках не установлены критически важные исправления либо имеются ошибки в конфигурировании, которые оставляют устройства открытыми для атак. К примеру, вирус Stuxnet использует для атаки хорошо известные слабости, связанные с использованием USB-накопителей, и функции автоматического воспроизведения Microsoft® Windows®. Это может быть исправлено за счет согласованной политики конфигурирования и обновления по всей организации.

Неприятности, связанные с проблемами безопасности, возникают не только из-за атак, но и из-за применяемых организацией способов защиты. Система защиты может оказаться сложной, дорогостоящей, отнимающей много времени у ИТ-персонала и требующей много затрат. После установки защиты многим организациям приходится следить за ее соответствием нормативным требованиям, за соблюдением внутренних политик, стандартов безопасности и законодательных норм. Помимо забот, связанных с изначальным соблюдением требований, следует также контролировать изменение этих предписаний в дальнейшем. После того как уровни соответствия достигнуты, организациям нужно обеспечить их постоянное соблюдение.

ПО IBM Tivoli® Endpoint Manager, построенное на базе технологии BigFix®, отвечает всем этим потребностям и может использоваться как небольшими, так и крупными организациями благодаря единой, легко развертываемой технологии. Оно обеспечивает контроль и управление в реальном времени для каждого устройства и позволяет решать задачи постоянного обеспечения безопасности и соблюдения нормативных требований.

Контроль и управление — основы безопасности

В организациях может насчитываться от сотен до нескольких сотен тысяч конечных устройств, которые должны быть хорошо защищены, чтобы эффективно справляться с рисками, минимизировать расходы и обеспечить соблюдение нормативных требований. Для решения задач управления при наличии такого масштабного и разнообразного набора технологий вы должны знать, сколько и каких устройств у вас имеется. Вам нужно проверять и обновлять программные исправления и политики безопасности для всех конечных точек, а также обеспечивать соблюдение внутренних политик ИТ-службы и соответствие внешним нормативным требованиям. И все это нужно делать достаточно быстро, чтобы постоянно поддерживать вашу систему безопасности на должном уровне.

Как добиться этого в большой и сложной среде, где угрозы исходят из нескольких направлений, а мишенью их зачастую становятся отдельные конечные точки? Как вам управлять тысячами разнообразных устройств, в том числе мобильных?

Решение состоит в том, чтобы развернуть единый, унифицированный инструмент, который не только позволяет устранить риски, возникающие при угрозах для безопасности, но и избавиться от излишних сложностей, сократить расходы и снять нагрузку с ИТ-персонала, обеспечив при этом соблюдение обязательных нормативных требований. Организациям нужен более простой, эффективный, масштабируемый инструмент с возможностями контроля и совершенствования, обеспечивающий непрерывную защиту в современных распределенных средах.

Идеальный инструмент для управления конечными точками предоставляет более интеллектуальные, быстродействующие и автоматизированные средства управления, которые используют возможности, имеющиеся в современном взаимосвязанном мире, и в то же время адаптированы к решению проблем, присущих конкретной среде. Имея такой инструмент, вы можете контролировать и защищать все физические и виртуальные конечные точки инфраструктуры, будь то настольные ПК, мобильные компьютеры с выходом в Интернет, серверы или специализированное оборудование, такое как торговые терминалы, банкоматы и киоски самообслуживания. Вы можете обеспечить безопасность вашей среды независимо от используемой операционной системы – Microsoft Windows, UNIX®, Linux® или Mac, в любом сочетании – с одной консоли, используя одну и ту же инфраструктуру управления.

ПО Tivoli Endpoint Manager обеспечивает быстрый результат

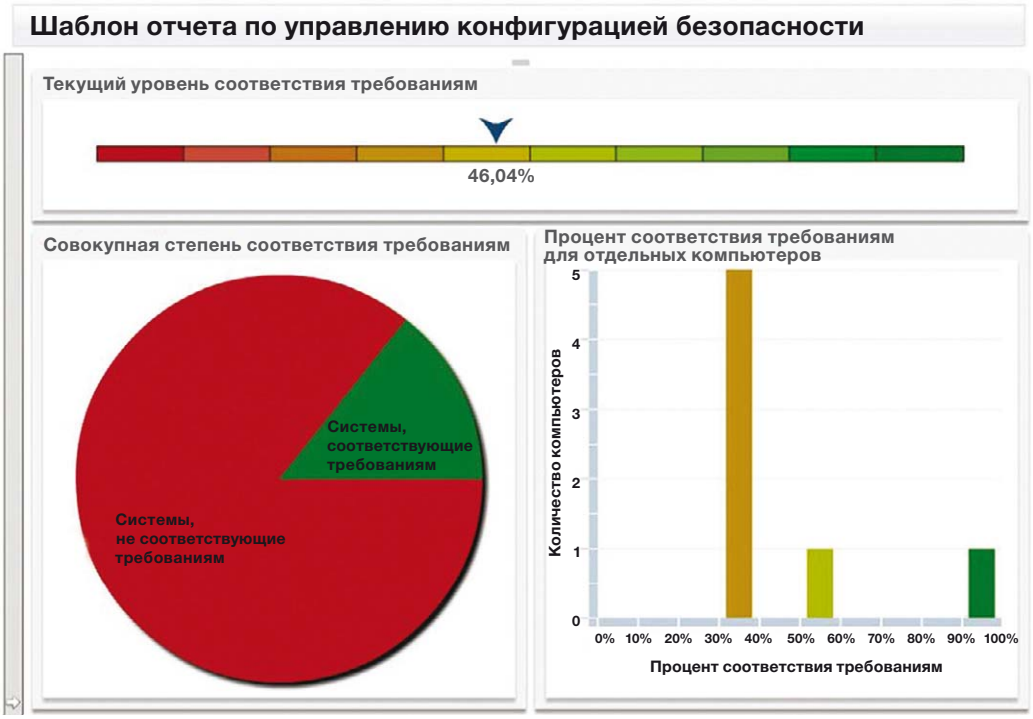
ПО Tivoli Endpoint Manager позволяет выполнить развертывание системы за несколько часов или за несколько дней, в зависимости от сложности вашей инфраструктуры, обеспечивая всеобъемлющую защиту в масштабе всей организации. Это унифицированное решение позволяет управлять сотнями тысяч конечных точек с одной консоли и с использованием одного управляющего сервера, а также быстро выявлять угрозы для безопасности и в реальном времени ликвидировать слабые места.

Решение способно выявлять конечные точки в сети, о существовании которых вы можете не знать, включая устройства, не принадлежащие к вашей сети, а также другое оборудование, которое в настоящий момент не охвачено системой управления. Быстро развертываемый

интеллектуальный агент в составе ПО Tivoli Endpoint Manager идентифицирует используемые на данный момент исправления и уровни конфигурирования, сравнивает их на соответствие принятым политикам. Затем он быстро и точно устанавливает обновления операционной системы и приложений вне зависимости от места размещения конечных точек, типа подключения или статуса, после чего непрерывно проверяет соблюдение действующих политик, даже если устройства не подключены к сети. Решение также способно быстро обнаруживать уязвимые места и устранять их, анализировать конечные точки на наличие известных слабостей с использованием заранее установленных политик и предпринимать действия по устранению слабых мест.

Уникальный интеллектуальный агент в составе ПО Tivoli Endpoint Manager постоянно корректирует политики обеспечения безопасности вне зависимости от состояния подключения конечной точки. В традиционных системах управления конечными точками используются агенты, которые полностью зависят от инструкций, получаемых от центрального сервера. Интеллектуальный агент, встроенный в решение IBM, в автономном режиме инициирует обновления и действия по конфигурированию. Таким образом, для конечного устройства предлагаются новейшие исправления и обеспечивается соответствие действующим политикам, передаваемым через сообщения IBM Fixlet®. Агенты загружают на устройство соответствующие исправления, конфигурацию или иной контент только по мере необходимости. При этом также непрерывно отслеживается соблюдение политики, а в случае выявления изменений на консоль управления посылаются сообщения об изменении статуса.

Агент Tivoli Endpoint Manager непрерывно отслеживает соответствие конечных точек нормативным требованиям, сообщает об их состоянии и обеспечивает контроль в реальном времени через единую, централизованную консоль. Благодаря использованию постоянно обновляемой базы данных политик, состоящей из тысяч сообщений IBM Fixlet, а также возможности для пользователей создавать собственные сообщения Fixlet управляющий сервер Tivoli Endpoint Manager всегда располагает актуальной информацией о конфигурации, статусе и соответствии требованиям для всех конечных устройств. Таким образом, можно легко сформировать необходимые отчеты в реальном времени.



Формирование отчетов в различных удобных для восприятия форматах через централизованную консоль обеспечивает контроль в реальном времени над конфигурацией и степенью соответствия нормативным требованиям.

Tivoli Endpoint Manager решает весь спектр задач, связанных с обеспечением безопасности

Tivoli Endpoint Manager предоставляет основные возможности для обеспечения безопасности, в том числе:

- **Поддержка стандартов безопасности.** Готовые оптимизированные методики, соответствующие нормам U.S. Federal Desktop Configuration Control (FDCC). Также поддерживается весь ряд стандартов Security Content Automation Protocol (SCAP) и Open Vulnerability and Assessment Language (OVAL), направленных на использование открытого и публично доступного контента. Решение поддерживает протокол Secure Content Automation Protocol (SCAP) и технические указания по обеспечению безопасности Security Technical Implementation Guides (STIG) Агентства по защите информационных систем Defense Information Systems Agency (DISA). Оно также способно получать предупреждения об уязвимых местах и рисках для безопасности, публикуемые институтом SANS, и предпринимать необходимые действия.
- **Управление программными исправлениями.** Всеобъемлющие возможности для установки исправлений на распределенные конечные точки применительно к любым операционным системам и приложениям. Сокращение затрат времени на установку исправлений и обновлений без ущерба для функционирования даже в условиях низкой пропускной способности сети, глобально распределенных сетей или в случаях, если устройства находятся за пределами межсетевого экрана организации.
- **Управление конфигурацией безопасности.** Предоставление значимой информации о работоспособности и безопасности конечных точек вне зависимости от их местоположения, операционной системы, установленных приложений или типа подключения.
- **Контроль и устранение слабых мест.** Анализ конечных точек на наличие уязвимостей, определенных в соответствии со стандартом безопасности, установленным OVAL, и формирование в реальном времени отчетов о несоответствии нормативным требованиям для устранения слабых мест по всем устройствам.
- **Диспетчер клиента для защиты конечных точек.** Единый центр управления антивирусными продуктами и межсетевыми экранами сторонних поставщиков, включая Computer Associates, McAfee, Symantec и Trend Micro, позволяющий организациям улучшить масштабируемость, повысить быстродействие и надежность решений защиты.
- **Автоматическое помещение в карантин внутри сети.** Автоматический анализ конечных точек на соответствие конфигураций обязательным требованиям. В случае обнаружения несоответствия решение может поместить устройство во внутрисетевой карантин до тех пор, пока соответствие нормам не будет обеспечено. Доступ к серверу Tivoli Endpoint Manager для выполнения задач управления сохраняется, но доступ ко всем другим активам блокируется.
- **Межсетевой экран.** Дает возможность администраторам применять политики в зависимости от местоположения конечной точки, управлять сетевым трафиком на основе IP-адресов источника и получателя, регулировать взаимодействия между внутренними и внешними устройствами и при необходимости помещать их в карантин.
- **Выявление активов.** Динамический контроль изменяющихся условий в инфраструктуре с возможностью упреждающего управления, включая быструю идентификацию неуправляемых сетевых устройств для дальнейшего их изучения или для автоматической установки агентов с целью быстрого взятия таких конечных точек под контроль.

Унифицированное решение — ключ к успешному управлению

Средства контроля и управления, предоставляемые решением Tivoli Endpoint Manager, могут стать ключом к достижению успеха. Современным организациям требуются оптимальные, автоматизированные инструменты, чтобы своевременно справляться с постоянно растущими объемами данных о функционировании конечных устройств. Новые, более эффективные средства нужны для того, чтобы определять, развертывать и модифицировать политики в области безопасности, обеспечивающие защиту конечных точек и их соответствие нормативным требованиям.

Фраза «вы не можете управлять тем, чего вы не видите» как никогда справедлива в отношении безопасности. Чтобы эффективно устранять слабые места, вам, прежде всего, нужно знать, какие конечные точки подвергаются риску. Многие проверки оказываются неэффективными из-за недостаточно быстрого выявления слабостей конечных устройств. Это может быть связано с изменениями конфигурации или неспособностью быстро выполнить установку исправлений (или подтвердить их актуальность) и обновлений.

Решение на базе единой консоли позволяет организациям реализовать унифицированный подход к управлению, улучшить контроль и управляемость. Оно

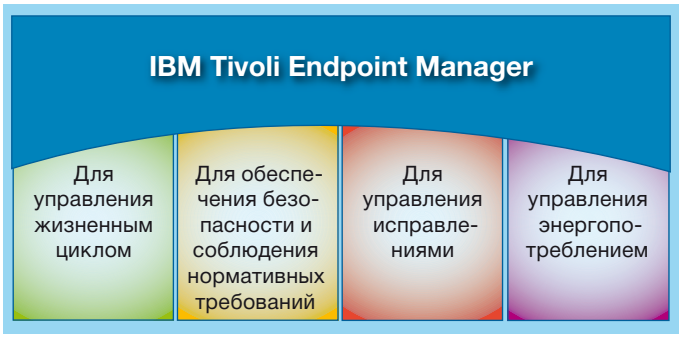
помогает, в частности, эффективно увязывать между собой процессы выработки стратегий и политик в области безопасности, исполнение этих стратегий, оперативное управление конечными точками в реальном времени, ведение отчетности в отношении безопасности и соответствия нормативным требованиям.

ПО Tivoli Endpoint Manager способно радикально улучшить ситуацию в отношении обеспечения безопасности за счет быстрого и точного внедрения изменений по всей инфраструктуре. При этом вы избавлены от нагромождения не связанных друг с другом инструментов управления, затрудняющего контроль и управление. Вы получаете единую инфраструктуру управления, позволяющую эффективно координировать действия ИТ-службы, операции настольных ПК и серверов, мероприятия в области безопасности, внесение изменений, устранение проблем, разрешение вопросов и ведение отчетности о соответствии нормативным требованиям в рамках всей организации.

ПО Tivoli Endpoint Manager позволяет снизить риски для безопасности, расходы и сложность управления, а также увеличить скорость и точность решения проблем с одновременным повышением продуктивности и степени удовлетворенности конечных пользователей. Подход на базе единого агента, единой консоли и единого управляющего сервера оптимизирует процесс и повышает надежность. Решение обеспечивает быструю окупаемость благодаря таким функциям, как управление программными исправлениями и выявление имеющихся активов, а также окупаемость в долгосрочной перспективе за счет повышения операционной эффективности, консолидации инфраструктуры управления и повышения продуктивности ИТ-службы.

Решение IBM Tivoli Endpoint Manager – это семейство продуктов, которые используют единую консоль, единый управляющий сервер и единый агент. Такой подход помогает вам консолидировать инструменты, уменьшить количество агентов и сократить расходы на управление. Для добавления сервисов достаточно просто изменить лицензионный ключ. В состав семейства IBM Tivoli Endpoint Manager входят следующие продукты:

- IBM Tivoli Endpoint Manager for Lifecycle Management;
- IBM Tivoli Endpoint Manager for Security and Compliance;
- IBM Tivoli Endpoint Manager for Patch Management;
- IBM Tivoli Endpoint Manager for Power Management.



Решение IBM Tivoli Endpoint Manager – это семейство продуктов, которые используют единую консоль, единый управляющий сервер и единый агент конечных точек.

Решения IBM для обеспечения безопасности современных организаций

ПО Tivoli Endpoint Manager является составной частью всеобъемлющего портфеля решений IBM для обеспечения безопасности. Оно помогает организациям решать проблемы защиты пользователей, информации, приложений и процессов, сетей, серверов и рабочих станций, а также физической инфраструктуры. Расширяя возможности по контролю и управлению в режиме реального времени и укрепляя безопасность конечных точек ИТ-инфраструктуры, решения IBM поддерживают современные, постоянно расширяющиеся центры обработки данных, обеспечивая рациональные, взаимосвязанные и интеллектуальные ИТ-операции.

В условиях, когда мир становится все более технически оснащенным, взаимосвязанным и интеллектуальным, решения IBM для обеспечения безопасности помогают реализовать контроль и централизованное управление в реальном времени, а также расширить функциональные возможности всей ИТ-инфраструктуры, включая глобально распределенные устройства.

Дополнительная информация

Для получения дополнительной информации о программном обеспечении IBM Tivoli Endpoint Manager свяжитесь с представителем IBM в вашем регионе или с бизнес-партнером IBM, либо посетите Web-сайт IBM по адресу: **ibm.com**/tivoli/endpoint.

О программном обеспечении IBM Tivoli

Программное обеспечение IBM Tivoli помогает организациям эффективно и действенно управлять информационно-технологическими ресурсами, задачами и процессами для удовлетворения постоянно меняющихся потребностей бизнеса и реализации гибких ИТ-сервисов при одновременном сокращении расходов. Портфель IBM Tivoli охватывает программное обеспечение для управления безопасностью, соблюдением нормативных требований, хранением данных, производительностью, готовностью, конфигурациями, операциями и жизненным циклом ИТ-активов. Программное обеспечение IBM Tivoli поддерживается сервисными службами и исследовательскими подразделениями IBM мирового уровня.

© IBM Восточная Европа /Азия
123370, Москва, Пресненская наб., 10
Тел.: +7 (495) 775-8800, факс: +7 (495) 258-6468, 258-6404

Февраль 2011 г.
Все права защищены.

IBM, логотип IBM, ibm.com, BigFix и Tivoli являются товарными знаками или зарегистрированными товарными знаками International Business Machines Corporation в США и/или других странах. Если перечисленные и другие термины IBM при их первом упоминании в настоящем тексте помечены символом товарного знака (® или ™), то эти символы указывают на то, что данные термины являются зарегистрированными или охраняемыми нормами общего права в США товарными знаками, принадлежащими IBM на момент публикации этой информации. Такие товарные знаки могут также быть зарегистрированными или охраняемыми нормами общего права товарными знаками в других странах. Текущий перечень всех товарных знаков IBM представлен на Web-странице **ibm.com**/legal/copytrade.shtml с названием Copyright and trademark information («Информация об авторском праве и товарных знаках»).

Adobe является зарегистрированным товарным знаком Adobe Systems Incorporated в США и/или других странах.

Linux является зарегистрированным товарным знаком, принадлежащим Линусу Торвальдсу, в США и/или других странах.

Microsoft, Windows и логотип Windows являются товарными знаками Microsoft Corporation в США и/или других странах.

UNIX является зарегистрированным товарным знаком The Open Group в США и/или других странах.

Java и все товарные знаки и логотипы, использующие слово Java, являются товарными знаками Sun Microsystems, Inc. в США и других странах.

Другие названия компаний, продукции и услуг могут являться товарными знаками или знаками обслуживания соответствующих компаний.

Упоминание в этой публикации продуктов или услуг корпорации IBM не означает, что IBM предполагает предоставлять их во всех странах, где она ведет свою деятельность.

Данные о продуктах актуальны на момент публикации и могут быть изменены без уведомления. Любые утверждения относительно направлений работы и перспективных планов корпорации IBM характеризуют исключительно цели и задачи компании и могут быть изменены или отозваны без уведомления.

Пользователь продукции IBM несет личную ответственность за соответствие своей деятельности требованиям законодательства. Ответственность за получение рекомендаций от компетентных государственных органов относительно применения законов и регулирующих норм, которые могут повлиять на бизнес клиента, а также за любые действия, которые могут потребоваться для соблюдения подобных законов и требований, лежит исключительно на самом клиенте. IBM не дает юридических советов или гарантий того, что ее продукты или услуги обеспечат клиенту выполнение требований законодательства или нормативных документов.

Подлежит повторной переработке

Tivoli software

TIS14081-RURU-00