# IBM Tivoli Endpoint Manager for Security and Compliance

*Единое решение для управления безопасностью конечных точек ИТ-инфраструктуры предприятия*

## Ключевые моменты

- Обеспечивает представление актуальных данных и средства контроля с помощью единой консоли управления.
- Использует единый, многоцелевой интеллектуальный агент, который позволяет оценить и решать проблемы, гарантируя непрерывное соблюдение нормативных требований и стратегии безопасности.
- Позволяет управлять сотнями тысяч физических и виртуальных устройств независимо от их местоположения, типа соединения и состояния.
- Автоматически управляет исправлениями для разных операционных систем и приложений.

Количество конечных точек ИТ-инфраструктуры и угрожающих им опасностей растет беспрецедентными темпами. Обеспечить унифицированное представление и защиту всей сложной и распределенной среды в режиме реального времени позволяет решение IBM Tivoli® Endpoint Manager for Security and Compliance.

Пакет Tivoli Endpoint Manager for Security and Compliance призван гарантировать безопасность конечных точек всей ИТ-инфраструктуры организации. Он помогает защитить устройства и предоставить регулирующим органам доказательства того, что все стандарты безопасности соблюдаются. Это простое в управлении и развертывании решение обеспечивает высокий уровень защищенности в среде с большим числом разнообразных устройств – от серверов до настольных ПК. Данное решение поддерживает ноутбуки, работающие через интернет-соединение, и специализированные устройства, такие как кассовые терминалы (POS), банкоматы и киоски самообслуживания.

Tivoli Endpoint Manager for Security and Compliance обеспечивает высокую гибкость бизнеса, а также скорость и точность восстановления данных. Это решение способствует уменьшению стоимости и сложности управления ИТ-средой. Кроме того, обеспечивая повышение производительности труда и более комфортные условия работы пользователей, это решение мало влияет на функционирование самих устройств. Где бы ни находилось устройство, Tivoli Endpoint Manager for Security and Compliance помогает уменьшить риск и усилить контроль, непрерывно обеспечивая соблюдение нормативных требований.

## Решение проблем безопасности в масштабах организации

Tivoli Endpoint Manager for Security and Compliance решает проблемы безопасности, связанные с рабочими станциями и распределенной средой. Обеспечивая в рамках единого решения управление конечными точками ИТ-инфраструктуры и их защиту, это ПО помогает гарантировать полную безопасность и соблюдение нормативных требований. Например, оно может существенно сократить число пробелов в защите, распространяя исправления для программного обеспечения за считанные минуты. Помимо этого, сокращается разрыв между функциями, которые определяют и реализуют стратегию и политику безопасности, управляют устройствами в режиме реального времени и генерируют отчеты по безопасности и нормативно-правовому соответствию.

В число возможностей Tivoli Endpoint Manager for Security and Compliance входят:

- предоставление точной и актуальной информации о конфигурации устройств и исправлениях, а также непрерывный контроль за соблюдением правил безопасности;
- централизованное управление сторонними средствами защиты от вредоносного ПО и межсетевыми экранами;
- практические рекомендации по соблюдению базовых параметров для компьютеров федеральных учреждений США (FDCC) и требований Руководства по техническому обеспечению безопасности Агентства защиты информационных систем Министерства обороны США (DISA STIG);
- поддержка протокола Security Content Automation (SCAP); Tivoli Endpoint Manager – это первый продукт, сертифицированный Национальным институтом стандартов и технологии (NIST) США как для оценки, так и для устранения угроз;
- надежная передача в устройства инструкций в соответствии с сертификатами NIAP CCEVS EAL3 и FIPS 104-2 уровня 2;
- поддержка стандарта распространения открытых и общедоступных материалов по безопасности Open Vulnerability and Assessment Language (OVAL);
- прием сообщений об уязвимостях и рисках для безопасности, публикуемых Институтом SANS, и реагирование на них;
- демонстрация тенденций и анализ изменений конфигурации безопасности с помощью передовых инструментов отчетности.

Дополнительные возможности, предоставляемые всеми продуктами семейства Tivoli Endpoint Manager на основе технологии BigFix®:

- обнаружение конечных точек ИТ-инфраструктуры, о которых организация могла не знать: в некоторых случаях доля таких устройств достигает 30%;
- единая консоль для управления функциями настройки, обнаружения ресурсов и безопасности, упрощающая работу;
- специальные действия, нацеленные на устройства с конфигурацией или пользователями определенного типа, а также применение по отношению к ним практически любого аппаратного или программного обеспечения;
- использование единой инфраструктуры управления для координации работы ИТ-инфраструктуры, службы безопасности, настольных ПК и серверов;
- поддержка многофункциональных конечных точек ИТ-инфраструктуры независимо от их местоположения, типа соединения или состояния с комплексным управлением для всех основных операционных систем, приложений и исправлений на основе принятых политик.

Tivoli Endpoint Manager for Security and Compliance обеспечивает автоматизированные, ориентированные на конкретные результаты процессы, которые гарантируют контроль, прозрачность и быстрое выполнение изменений, а также отчетность по соблюдению нормативных требований. Устранение угроз происходит молниеносно: проблемы вредоносных программ и вирусов решаются с помощью быстродействующих инструментов управления обновлениями.

## Широкий спектр мощных функций безопасности

Tivoli Endpoint Manager for Security and Compliance обеспечивает перечисленные ниже ключевые функции и предоставляет возможность по мере необходимости легко добавлять другие возможности без усложнения инфраструктуры и накладных расходов.

### Управление исправлениями

Функции управления исправлениями обеспечивают широкие возможности по распространению патчей для Microsoft® Windows®, UNIX®, Linux® и Mac OS, а также для Adobe®, Mozilla, Apple, Java™ и других приложений

среди распределенных устройств, независимо от их местонахождения, типа соединения или состояния. Один сервер управления исправлениями способен поддерживать до 250 000 устройств, сокращая время установки исправлений без ущерба для функциональности устройств даже по сети с низкой пропускной способностью или территориально распределенной сети. Отчеты, составляемые в режиме реального времени, содержат информацию о том, когда и кем были развернуты исправления, а также автоматическое подтверждение того, что исправления установлены. Таким образом, формируется полное решение для развертывания исправлений с обратной связью.

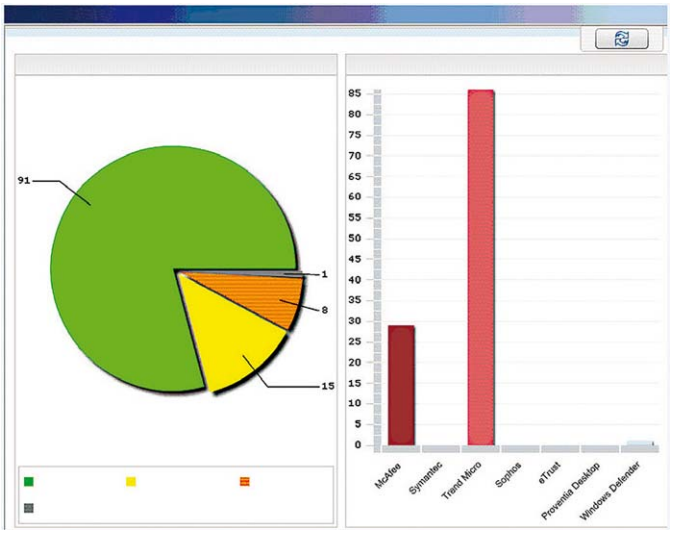
## Управление параметрами безопасности

Содержащиеся в решении средства для управления параметрами безопасности, сертифицированные Национальным институтом стандартов и технологий США, представляют собой обширную библиотеку технических элементов управления, которые помогают соблюдать требования по безопасности, определяя и исправляя параметры настройки безопасности системы. Библиотеки поддерживают непрерывное соблюдение основных правил безопасности, обеспечивают сигнализацию, восстановление и подтверждение восстановления не соответствующих правилам безопасности устройств. Они также гарантируют проверку всех конечных точек ИТ-инфраструктуры в режиме реального времени.

Эта функция доставляет полезную информацию о состоянии и степени безопасности устройств независимо от их местонахождения, операционной системы, типа соединения (включая компьютеры, подсоединенные к кабельной сети, и периодически подключаемые ноутбуки), а также об установленных на них приложениях. Это помогает консолидировать и унифицировать жизненный цикл устройств, сокращая время их настройки и восстановления.

## Управление уязвимостями

Средства управления уязвимостями позволяют обнаруживать, оценивать и устранять уязвимости, прежде чем возникнет угроза безопасности системы. Они оценивают системы в соответствии со стандартными определениями уязвимостей, написанными на языке




Tivoli Endpoint Manager for Security and Compliance составляет отчеты, которые помогают организациям выявить проблемы, влияющие на эффективность усилий по обеспечению безопасности и соблюдению нормативных требований.

Open Source Security Language (OVAL). При этом в режиме реального времени составляются отчеты о неудовлетворительных политиках обеспечения безопасности. Результатом становится улучшенный контроль и полная интеграция на каждом шаге всего процесса – от обнаружения и оценки угроз до их устранения и формирования отчетов.

ИТ-персонал может выявлять и устранять известные уязвимости – с помощью автоматических процедур или вручную – по всем конечным точкам ИТ-инфраструктуры. Применяя единый инструмент для обнаружения и устранения уязвимостей, администраторы могут повысить скорость и точность, сократив время развертывания исправлений и обновлений программного обеспечения. Администраторы могут также распространить управление безопасностью на мобильные устройства, подключенные или не подключенные к сети, настроив сигнализацию для быстрого выявления устройств-нарушителей и их восстановления или удаления.

## Обнаружение ресурсов

При наличии Tivoli Endpoint Manager for Security and Compliance задача выявления ИТ-ресурсов перестает быть «упражнением в арифметике». Решение предоставляет готовую динамическую ситуационную информацию об изменении условий в инфраструктуре. Возможность частого сканирования всей корпоративной сети обеспечивает полную прозрачность и контроль, помогая гарантировать быстрое выявление с минимальной нагрузкой на сеть всех компьютеров и других IP-адресуемых виртуальных машин, а также сетевых и периферийных устройств, таких как принтеры, сканеры, маршрутизаторы и коммутаторы. Эта функция помогает следить за всеми конечными точками ИТ-инфраструктуры предприятия, включая ноутбуки за пределами корпоративной сети.

## Управление средствами безопасности от разных поставщиков

Эта функция предоставляет администраторам возможность централизованного управления сторонними клиентскими решениями безопасности от таких поставщиков, как Computer Associates, McAfee, Sophos, Symantec и Trend Micro. Благодаря такому централизованному управлению организации могут повысить масштабируемость, быстродействие и надежность системы защиты. Решение осуществляет контроль состояния устройств, гарантируя постоянную работу клиентов защиты конечных точек и своевременное обновление антивирусных баз. В дополнение к единому представлению разнородных технологий это облегчает перевод устройств с одного решения на другое, позволяя удалять и переустанавливать программное обеспечение одним нажатием клавиши. Проверка с обратной связью, в том числе проверка отключенных от сети устройств через Интернет, гарантирует, что установка обновлений и других изменений будет выполнена полностью.

## Автоматический карантин

Tivoli Endpoint Manager for Security and Compliance автоматически оценивает устройства на наличие необходимых настроек для соблюдения правил безопасности и в случае выявления несоответствия может поместить устройство в сетевой карантин. Сервер Tivoli Endpoint Manager получит доступ к такому устройству в целях управления, но всем остальным доступ будет перекрыт.

## Служба антивируса и защиты Web-репутации (опция)

Глубокая интеграция с продуктом Core Protection Module (CPM) компании Trend Micro предоставляет возможности по защите устройств от вирусов, троянских коней, червей, шпионских программ, руткитов, новых вариантов вредоносного ПО и вредоносных Web-сайтов. Защита обеспечивается с помощью обращения в режиме реального времени к размещенной в облачной среде базе данных об угрозах, что практически полностью исключает необходимость в загрузке файлов антивирусных баз в защищаемое устройство. Технология защиты Web-репутации предотвращает посещение пользователями вредоносных Web-сайтов по их собственной инициативе или в результате скрытых автоматических действий вредоносных программ.

## Семейство Tivoli Endpoint Manager

Дальнейшая консолидация инструментов позволяет уменьшить число агентов для разных устройств и сократить затраты на управление за счет расширения инвестиций в Tivoli Endpoint Manager for Security and Compliance с добавлением других компонентов семейства Tivoli Endpoint Manager. Так как управление всеми функциями производится с помощью единой консоли, единого управляющего сервера и единого агента устройств, добавление дополнительных служб – это вопрос простой замены лицензионного ключа.

- **Tivoli Endpoint Manager for Power Management –** позволяет обеспечить соблюдение стратегии экономии энергии в масштабах всей организации с детализацией, необходимой для применения данной стратегии к каждому компьютеру.
- **Tivoli Endpoint Manager for Lifecycle Management –** всеобъемлющий и эффективный подход к объединению ИТ-функций путем отображения в режиме реального времени состояния устройств и предоставления администраторам дополнительных возможностей по управлению конечными точками ИТ-инфраструктуры.

## Tivoli Endpoint Manager: основан на технологии BigFix

За всеми функциями Tivoli Endpoint Manager стоит уникальный подход единой инфраструктуры, при котором принятие решений распределено между устройствами, что обеспечивает выдающиеся преимущества для всего семейства решений со следующими возможностями:

- **Интеллектуальный агент.** Tivoli Endpoint Manager использует передовой подход, при котором в каждой конечной точке ИТ-инфраструктуры размещается интеллектуальный агент. Этот единый агент выполняет несколько функций, включая непрерывную самооценку и контроль за соблюдением правил, но при этом оказывает минимальное влияние на производительность системы. В отличие от традиционной архитектуры «клиент – сервер», когда все указания поступают из центра управления, этот агент самостоятельно принимает решения, отправляя сообщения на центральный сервер и извлекая исправления, конфигурации и другую информацию, необходимую для реализации соответствующей стратегии. В результате управляющему серверу всегда известно о ситуации с соблюдением нормативных требований и изменениях состояния устройств, что позволяет быстро составлять актуальные отчеты по нормативно-правовому соответствию.
- **Отчетность**. Единая, унифицированная консоль, встроенная в Tivoli Endpoint Manager, обеспечивает полную информацию, в том числе непрерывную отчетность в режиме реального времени и анализ, выполняемый интеллектуальными агентами в конечных точках ИТ-инфраструктуры организации.
- **Возможности связи.** Масштабируемая и легкая архитектура Tivoli Endpoint Manager позволяет любому агенту настроиться на работу в качестве связующего звена между другими агентами и консолью. Такая функция связи позволяет использовать существующие серверы или рабочие станции для распространения пакетов программного обеспечения по сети, уменьшая потребность в серверах.
- **IBM Fixlet®-сообщения.** Fixlet Relevance Language – это опубликованный командный язык, который позволяет заказчикам, бизнес-партнерам и разработчикам создавать настраиваемые стратегии и службы для устройств, управляемых посредством Tivoli Endpoint Manager.

## Расширение возможностей Tivoli по обеспечению безопасности

Tivoli Endpoint Manager for Security and Compliance является частью всеобъемлющего семейства решений IBM для обеспечения безопасности. Это ПО помогает справляться с проблемами безопасности в масштабах всей организации. Поддерживая отлаженные, взаимосвязанные и интеллектуальные ИТ-операции, решения IBM для обеспечения безопасности помогают информировать соответствующих специалистов в режиме реального времени, централизованно управлять и повышать безопасность всей ИТ-инфраструктуры, включая территориально распределенные устройства.

### Семейство Tivoli Endpoint Manager – требования к системе

**Требования к серверу:**

- Microsoft SQL Server 2005/2008
- Microsoft Windows Server 2003/2008/2008 R2

**Требования к консоли:**

- Microsoft Windows XP/2003/Vista/2008/2008 R2/7

**Платформы, поддерживаемые агентом:**

- Microsoft Windows, including X P, 2000, 2003, Vista, 2008, 2008 R2, 7, CE, Mobile, XP Embedded and Embedded Point-of-Sale
- Mac OS X
- Solaris
- IBM AIX®
- Linux on IBM System z®
- HP-UX
- VMware ESX Server
- Red Hat Enterprise Linux
- SUSE Linux Enterprise
- Oracle Enterprise Linux
- CentOS Linux
- Debian Linux
- Ubuntu Linux

## Дополнительная информация

Для получения дополнительной информации о программном обеспечении IBM Tivoli Endpoint Manager for Security and Compliance 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.



Tivoli software

TID14075-USEN-00