

IBM Proventia Desktop Endpoint Security: мощная, многоуровневая защита для рабочих станций

Подразделение IBM Internet Security Systems (ISS) помогает повысить уровень безопасности всего предприятия за счет мощных средств защиты рабочих станций

Решение IBM Proventia Desktop Endpoint Security (Proventia Desktop), разработанное подразделением IBM Internet Security Systems (ISS), помогает реализовать превентивный подход к обеспечению безопасности рабочих станций. Это современное программное обеспечение своевременно защищает персональные компьютеры и мобильные устройства от известных и неизвестных угроз и других несанкционированных действий. Proventia Desktop предоставляет эффективное, рентабельное и стандартизированное решение для обеспечения безопасности самых важных и часто используемых ИТ-ресурсов предприятия.

Угрозы, направленные на рабочие станции, крайне важны для любой организации, т.к. очень быстро меняются. Заинтересованные в прибыли злоумышленники выпускают скрытые эксплойты, которые не обнаруживаются устаревшими средствами безопасности. Особенно неприятные атаки, например, с использованием троянских программ, невозможно предотвратить только с помощью антивирусного программного обеспечения. Благодаря популярности атак с использованием вредоносного кода злоумышленники продолжают использовать уязвимости типа "zero-hour", с которыми не могут справиться традиционные средства безопасности, такие как антивирусы и брандмауэры. Даже если бы эти решения и могли предотвращать атаки, временные и экономические затраты специалистов ИТ-отделов и отделов обеспечения безопасности, связанные с управлением ими, нивелируют все преимущества.

Многоуровневое решение Proventia Desktop представляет собой надежное и эффективное решение для обеспечения безопасности для рабочих станций. Оно включает в себя персональный брандмауэр, антивирусное ПО, контроль приложений и "spyware" с технологиями упреждающего действия, такими как система защиты от переполнения буфера, технология блокирование конкретной уязвимости и патентованная система IBM ISS Virus Prevention System (VPS) для борьбы с вирусами.*

Proventia Desktop позволяет устранить простои, перебои в работе и сократить число обращений в службу поддержки. Это решение легко интегрируется в ИТ-инфраструктуру и поддерживает как локальное, так и централизованное управление. Proventia Desktop является частью платформы обеспечения безопасности IBM, которая предоставляет средства превентивной защиты для ИТ-среды в целом – продукты и службы, которые обеспечивают оценку уязвимостей и предотвращение угроз.

Почему для рабочих станций нужны особые средства обеспечения безопасности?

Брандмауэры и антивирусное ПО не могут справиться с современными угрозами

Современные гибридные угрозы и изощренные способы атак позволяют без особых трудностей обходить традиционные системы защиты. Многие компании пострадали и понесли ощутимые убытки от сетевых атак, несмотря на наличие брандмауэров и установленного антивирусного ПО. Например, некоторые системы могут выявлять атаки с использованием технологии переполнения буфера, но не могут остановить их до самого запуска. Традиционные антивирусные решения, использующие вирусные сигнатуры, могут блокировать известные вирусы, но не обеспечивают никакой защиты от новых, неизвестных вирусов.

Появление новых пользователей и устройств значительно усложняет задачу обеспечения соответствия нормативным требованиям

Новые настольные и портативные компьютеры, используемые сотрудниками дома и в поездках, в корпоративных офисах и филиалах компаний, порождают проблемы, связанные с соответствием нормативным требованиям, и представляют собой новый источник сетевых угроз. Периметр корпоративной сети надежен настолько, насколько надежно самое уязвимое конечное устройство.

Неразбериха с обновлениями безопасности

Критические обновления безопасности для настольных операционных систем и приложений могут повысить уровень защищенности, но велика вероятность того, что сотрудники ИТ-отдела и службы поддержки будут слишком заняты и не смогут оперативно устанавливать такие обновления. Ситуация осложняется еще и тем, что установка обновлений часто приводит к проблемам намного более серьезным, чем те, которые они призваны устранять.

Никакая система обеспечения безопасности, реагирующая во время атаки, не сможет предотвратить потери данных

Даже самые современные средства обеспечения безопасности, например, антивирусное ПО, реагируют только во время атаки – слишком поздно, чтобы избежать простоев, сохранить все транзакции, избежать компрометации конфиденциальной информации и возможного нарушения других обязательств.

Почему именно Proventia Desktop? Каковы преимущества этого решения?

Защита с помощью единого агента

Решение Proventia Desktop обеспечивает защиту еще до возникновения угрозы, помогая снизить общий уровень уязвимости вычислительной среды предприятия. Являясь интегрированным агентом для конечного устройства, оно исключает снижение производительности и расходы на подписку, которые характерны для ситуации с использованием нескольких агентов. Proventia Desktop интегрирует все необходимые средства обеспечения безопасности в рамках одного продукта.

Более низкая совокупная стоимость владения

Решение Proventia Desktop отличается экономичностью использования и вместе с тем позволяет избежать дорогостоящих процедур по внедрению обновлений и исправлений. Многоуровневая защита, реализованная в виде единого агента, сокращает затраты на лицензирование и подписку и помогает сократить число обращений в службу поддержки и исправлений на уровне клиента.

Proventia Desktop обеспечивает широкие возможности по настройке и управлению на основе политик. С помощью IBM Proventia Management SiteProtector администраторы могут управлять внедрением в масштабе предприятия с помощью единой консоли.

Как работает многоуровневая защита?

Она блокирует угрозы на уровне приложения и сети.

Защита от угроз на уровне приложений

Атаки с помощью файлов, например, с помощью вирусов и троянских программ, – это угроза для настольных компьютеров на уровне приложений. Proventia Desktop противодействует угрозам на уровне приложений с помощью системы VPS, антивирусного ПО, контроля приложений, и антишпионского ПО.

Virus Prevention System – Технология предотвращения вирусных атак на основе сигнатур удаляет вредоносные программы с конечных устройств, однако не может являться единственным элементом системы обеспечения безопасности конечного устройства. В Proventia Desktop традиционные средства антивирусной защиты дополняются патентованной системой VPS, которая обнаруживает и блокирует шпионское ПО и более 95 процентов новых и неизвестных вирусов и программ-червей без использования обновляемой базы и ложных срабатываний. Вместо использования сигнатур система VPS анализирует “поведение” исполняемого файла и выявляет семейства вредоносного кода. VPS запускает код в виртуальной среде, безопасно отслеживает его выполнение, а затем проверяет наличие вредоносного содержимого. Это позволяет гарантировать, что реальные угрозы будут блокированы, а обмен безопасными данными будет проходить без помех.

Контроль приложений – Proventia Desktop позволяет разрешать или запрещать установку определенных приложений на конечном устройстве.

Антивирусное и антишпионское ПО – Proventia Desktop содержит механизм Bit Defender, предназначенный для сканирования серверов и удаления вредоносного ПО.

Предотвращение сетевых атак

Персональный брандмауэр – Брандмауэр, встроенный в Proventia Desktop, блокирует несанкционированный доступ к портам, IP-адресам и сервисам, защищая от таких атак, как IP-спуфинг, чтобы предотвратить перехват сессий протоколов и сервисов.

Система предотвращения вторжений на основе уязвимостей – Proventia Desktop включает в себя технологию Proventia Intrusion Prevention, защищающую уязвимости, на которые направлены атаки, вместо того чтобы использовать сигнатуры для выявления известного вредоносного кода. Для блокирования известного вредоносного ПО и его модификаций используется анализ на основе сигнатур и протоколов.

Система защиты от переполнения буфера – Proventia Desktop помогает предотвратить проблемы, связанные с переполнением буфера. Атаки с переполнением буфера коварны, поскольку от них нельзя защититься, просто не открывая вложенные в электронные письма файлы. Благодаря системе защиты от переполнения буфера решение Proventia Desktop эффективно предотвращает такие виды атак с помощью предустановленной конфигурации.

Руководство по выбору решения для обеспечения безопасности рабочей станции
Для эффективной оценки решений по обеспечению безопасности рабочей станции необходимо принимать во внимание следующие особенности:

- *Профилактический подход к обеспечению безопасности*
- *Различные методы анализа, используемые для блокирования угроз на уровне приложений и сети*
- *Анализ содержимого на основе уязвимостей, осуществляемый лидером в области исследований технологий безопасности*
- *Эффективная политика обеспечения безопасности по умолчанию*
- *Автоматическое, готовое к использованию средство обеспечения безопасности*
- *Широкие возможности централизованного управления*
- *Высочайшая оперативность реагирования.*

Воспользуйтесь преимуществами IBM ISS уже сегодня

Узнайте, как IBM Proventia Desktop поможет защитить вашу компанию от сетевых угроз. Обязательно выясните, может ли ваша компания воспользоваться 30-дневной пробной версией программного обеспечения. Для демонстрации на месте обратитесь в ближайшее представительство IBM Internet Security Systems. Адреса представительств и дополнительные сведения о продукте можно найти на сайте:

ibm.com/services/us/iss



IBM EE/A

123 317 Москва, Краснопресненская наб. 18
тел. 775 8800
факс 258-6347

Адрес домашней страницы IBM:

ibm.com

IBM, логотип IBM, ibm.com, Proventia и SiteProtector – товарные знаки International Business Machines Corporation в США и/или других странах.

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

В данной брошюре могут содержаться ссылки или указания на продукты и услуги IBM, которые компания IBM не планирует предоставлять в некоторых странах.

Все данные по производительности, представленные в этой публикации, были получены в определенной операционной среде и при указанных выше условиях и приведены только в демонстрационных целях. Результаты, полученные при других условиях, могут отличаться от заявленных. Заказчикам рекомендуется проводить собственное тестирование.

* U.S. Patent No. 7,093,239.

Произведено в Соединенных Штатах
Америки
04-07

© Copyright IBM Corporation 2007
Все права защищены.