

Повышение “прозрачности” сети с помощью IBM Proventia Network Anomaly Detection System

Решения IBM ISS обеспечивает повышенную “прозрачность” и внутреннюю безопасность корпоративных сетей

Несмотря на инвестиции в средства защиты периметра и компьютеров, внутренняя сеть по-прежнему остается уязвимой для шпионского ПО, фишинга и фарминга, бот-сетей, распространения программ-червей, внутренних злоупотреблений и краж информации, а также других угроз, препятствующих достижению высокого уровня производительности и безопасности. Решение IBM Proventia Network Anomaly Detection System (ADS) дополняет и расширяет систему обеспечения безопасности, обеспечиваемую брандмауэрами и системами предотвращения вторжений. Для этого осуществляется постоянный мониторинг сети, приложений и пользовательской активности, причем этот мониторинг не вызывает появления “узких мест” и не требует перестройки сети. Возможности Proventia Network ADS основаны на знаниях и опыте экспертов подразделения IBM Internet Security Systems (ISS) в области безопасности. Одновременное использование систем обнаружения аномалий в сети и предотвращения вторжений позволяет получить следующие ключевые преимущества в области обеспечения безопасности сети и соответствия требованиям регулирующих органов.

- *Повышенная “прозрачность” сети, что обеспечивает соответствие требованиям регулирующих органов и улучшение общего состояния безопасности.*
- *Многоуровневая защита, обеспечиваемая решениями IBM ISS.*
- *Оптимизация системы предотвращения вторжений и возможность блокирования распространяющихся и внутренних угроз.*
- *Снижение общей стоимости владения (TCO) благодаря управлению безопасностью сети с помощью единой консоли.*

Почему именно Proventia Network ADS?

Proventia Network ADS представляет собой систему анализа поведения сети, которая повышает “прозрачность” сети и ее безопасность посредством сбора и анализа потоков данных, которыми обмениваются все входящие в инфраструктуру сетевые устройства. Этот программный продукт создает наглядную картину состояния и уязвимых мест сети на основе анализа сетевого поведения, оперативно обнаруживая существующие угрозы, опасную пользовательскую активность, снижение производительности сети и не соответствующие требованиям регулирующих органов действия, такие как нарушения политик безопасности и несанкционированные изменения в сети. Обеспечивая полную “прозрачность” всего потока данных в сети, Proventia Network ADS позволяет ИТ-администраторам отслеживать и защищать находящиеся под угрозой ресурсы до того, как их уязвимость будет использована для вторжения. Это позволяет поддерживать бесперебойную работу компании.

Proventia Network ADS может использоваться как автономное устройство или в сочетании с решениями IBM Proventia Network Intrusion Prevention System (IPS) и IBM Vulnerability Management Service, входящими в состав платформы обеспечения безопасности IBM Internet Security Systems. Такая интеграция обеспечивает возможность дальнейшей разработки и применения политик безопасности, соответствие требованиям регулирующих органов и повышение устойчивости сети к атакам со стороны несанкционированных приложений и служб для защиты данных и ресурсов, предназначенных для выполнения критически важных задач.

Функциональные возможности и преимущества

Повышает “прозрачность” сети

- *Включает запатентованную технологию, связанную с моделированием как поведения, так и взаимосвязей корпоративных сетей.*
- *Обеспечивает “прозрачность” проходящего через маршрутизаторы и интерфейсы потока данных в режиме реального времени и предоставляет возможность мониторинга компьютеров, служб и сетевых соединений, являющихся основной частью всего сетевого трафика.*
- *Осуществляет мониторинг портов, служб и приложений сети, выявляя аномальную активность и снижение производительности.*
- *Быстро обнаруживает проблемы в области безопасности сети, контролирует использование сетевых ресурсов и снижает риск распространения вирусов.*

Снижает риски; повышает степень соответствия требованиям регулирующих органов

- *Обнаруживает случаи несанкционированного доступа к ресурсам и поведенческие нарушения заданных политик.*
- *Составляет перечень рисков для определения хостов, представляющих наибольшую опасность для сети, и анализирует риски не только по IP-адресам, но и по отдельным пользователям.*
- *Осуществляет мониторинг активности пользователей для просмотра, поиска и экспорта этих данных за определенный период с целью контроля перемещений пользователей по сети.*
- *Блокирует сегменты и группы пользователей для предотвращения злоупотреблений со стороны инсайдеров и распространение червей, одновременно сокращая время простоя и затраты на ликвидацию последствий.*

- *Показывает, что система внутреннего контроля реализована и работает.*
- *Повышает устойчивость сети, блокируя неиспользуемые, неавторизованные порты и службы и одновременно отслеживая наиболее важные ресурсы.*
- *Обнаруживает новейшие угрозы, используя информацию службы Active Threat Feed (ATF).*
- *Дополняет решение IPS, обеспечивая поведенческий анализ сети для повышения ее защиты.*

Защита от активных угроз в масштабе предприятия

Механизмы поведенческого анализа, реализованные в Proventia Network ADS, дополняют решение IPS еще одним уровнем анализа и защиты, который постоянно пополняется информацией о новых глобальных угрозах. Используя ситуационный анализ, сетевые операторы получают информацию о взаимодействиях компьютеров благодаря оповещениям о смещениях потоков данных, переполнениях и несанкционированных подключениях. Они могут заблокировать определенные области сети до того, как угроза окажет негативное влияние на ее работу. Благодаря этому можно уменьшить риск возникновения аварий и неполадок, связанных с доступностью сети.

Обнаружение программ-червей	Обнаруживает распространение шаблонов аномального поведения
Обнаружение поведенческих аномалий	Обнаруживает потоки данных, не соответствующие поведенческим моделям
Обнаружение аномалий на основании интенсивности	Обнаруживает неожиданные отклонения от базовых уровней интенсивности потока данных с течением времени
Обнаружение сканирования сети	Обнаруживает факты медленного сканирования, быстрого сканирования, скрытого сканирования и сканирование хостов
Злоупотребления сотрудников	Обнаруживает поведенческие нарушения заданной политики безопасности
Перебои в доступности	Обнаруживает падение интенсивности потока данных через наиболее важные серверы и соединения
Отслеживание пользователей	Обнаруживает пользователей, получающих доступ к определенным ресурсам, независимо от точки их входа в систему благодаря мониторингу сети в режиме реального времени

Контроль действий сотрудников и предотвращение краж информации

В Proventia Network ADS используется ряд поведенческих моделей, предназначенных для обнаружения внутренних угроз.

Служба Active Threat Feed

Служба IBM ISS Active Threat Feed (ATF) обеспечивает не имеющую аналогов превентивную защиту, предоставляя актуальные данные о безопасности и моделях поведения сети. Пользователи Proventia Network ADS получают данные о существующих угрозах, нацеленных на их сети. После обновления данных Proventia Network ADS автоматически получает обновления от службы ATF и начинает анализ потоков данных в сети, с учетом новых моделей поведения. Именно эти данные обеспечивают значительное расширение возможностей Proventia Network ADS после первоначального внедрения. В этом заключается отличие от других базовых систем обнаружения аномального поведения, которые из-за своей статичности вынуждают администраторов систем безопасности и сетевых администраторов постоянно изучать новые модели поведения угроз, а затем самостоятельно разрабатывать и тестировать правила для обнаружения этих моделей.

Упрощенный контроль за соответствием требованиям регулирующих органов благодаря эффективной системе проверки и создания отчетов

Proventia Network ADS включает в себя возможности проверки и создания отчетов, которые позволяют упростить процедуру контроля соответствия требованиям регулирующих органов и получать точную информацию о безопасности и производительности сети. Для обеспечения соответствия требованиям регулирующих органов решение Proventia Network ADS осуществляет мониторинг важнейших ресурсов и приложений и отслеживает процедуры внесения изменений; определяет подозрительный контент и выявляет случаи несанкционированного доступа, злоупотребления сотрудниками и другие связанные с безопасностью инциденты, а также предпринимает соответствующие действия. Функции мониторинга и проверки безопасности в режиме реального времени позволяют создавать подробные и удобочитаемые отчеты, которые помогают обеспечить контроль соответствия требованиям регулирующих органов. Другие управленческие отчеты в форме графиков и таблиц содержат всестороннюю информацию о поведении сети, например информацию о взаимосвязях «клиент-сервер», статистику о потоках данных и корреляции пользователей, хостов и служб.

Интеграция решения

С помощью системы управления IBM Proventia Management SiteProtector решение Proventia Network ADS интегрируется с IBM Proventia Network Intrusion Prevention System (Proventia Network IPS) и IBM Proventia Network Enterprise Scanner (Enterprise Scanner), а также с решениями других производителей. Являясь частью многоуровневой стратегии безопасности, решения Proventia Network ADS и Proventia Network IPS работают совместно и обеспечивают эффективную защиту от угроз независимо от их источника.

Дополняет Proventia Intrusion Prevention Systems	Дополняет Proventia Network Enterprise Scanner
“Прозрачность” в масштабе сети	Пассивная оценка сети
Поведенческие методики обнаружения	Статистика работы служб
Использование сетевых ресурсов и производительность сети	Нарушения политики безопасности

Оцените преимущества

Чтобы ознакомиться с решением Proventia Network Anomaly Detection System прямо сейчас, позвоните по телефону 1 800 776-2362, отправьте электронное письмо по адресу sales@iss.net или посетите Web-сайт:

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.

Упоминание в этой публикации продуктов или услуг IBM не означает, что IBM предполагает предоставлять их во всех странах, в которых осуществляет свою деятельность.

Все результаты, представленные в данной статье, 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.

Произведено в Соединенных Штатах
Америки
04-07

© Copyright IBM Corporation 2007
Все права защищены.