



Минимизация инсайдерских рисков при помощи IP-guard

Меньше затрат, сложностей и риска – больше контроля

ПРОГРАММНЫЕ РЕШЕНИЯ



Инсайдеры – самая большая опасность для Вашей организации

Во время экономического кризиса Ваши данные и интеллектуальная собственность подвергаются большей опасности, чем когда-либо ранее, поскольку возрастает вероятность инсайдерского риска. Даже при хороших экономических условиях плохие люди совершают плохие поступки. При плохих же экономических условиях даже хорошие люди совершают плохие поступки. Недовольные подчиненные, бывшие сотрудники, которые перешли к конкурентам, будут нацеливаться на незащищенные данные компании. Они знают Ваш бизнес и могут действовать, преодолевая барьеры и преграды системы защиты.

Вред, причиненный инсайдерами, – многообразный и потенциально продолжительный. Результатом нарушения безопасности могут быть не только потеря интеллектуальной собственности и производительности, но также и судебные иски, штрафы и, что наиболее важно, потеря репутации.

Риски информационной безопасности следует оценивать и минимизировать с позиции экономичности бизнеса. В то время как руководители стремятся в первую очередь минимизировать прямые угрозы, им также следует рассмотреть инвестиции в безопасность ИТ как эволюционную потребность для достижения гибкости и экономической эффективности ИТ.

Меньше издержек, сложности и риска – больше контроля с IP-guard

Остерегайтесь рекламы продукции типа «Защита от утечки информации», а также рассмотрите более широкий диапазон проактивной защиты данных и технологий мониторинга. С IP-guard The Cherry Group предлагает Вам инновационное и масштабируемое решение, которое покрывает все основные подвергающиеся риску сферы информационной безопасности. Модульный подход IP-guard позволяет осуществлять в режиме реального времени групповой мониторинг всех сфер информационной безопасности, подвергающихся риску. IP-guard использует сложную технологию обнаружения нарушений безопасности и несоответствующего поведения и представляет информацию менеджменту и пользователям при помощи консолидированной системы отчетности. Благодаря использованию технологий надзора в режиме реального времени, IP-guard позволяет предотвратить большинство нарушений. Конструкция IP-guard основана на международных стандартах (ISO/IEC 27001: 2005) и уже была успешно применена в лидирующих финансовых учреждениях и компаниях Fortune-500 по всему миру, включая Россию, Украину и Казахстан.

Правильное понимание Информационной Безопасности с The Cherry Group

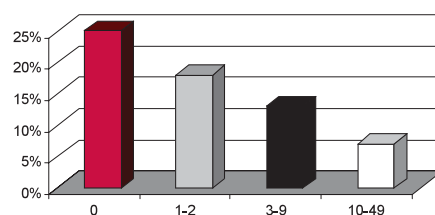
Наш профессионализм и значительный опыт позволяют нам применять сложные политики безопасности с фиксированной стоимостью в течение нескольких недель, чтобы обеспечить соответствие Вашей организации требованиям законодательства и спокойствие акционеров. Придерживаясь международных стандартов (ENISA и CISSP), наши опытные специалисты поддерживают на всех этапах процесс внедрения Системы Управления Информационной безопасностью, который работает на Вас. Ключевые компетенции The Cherry Group включают:

- Управление Информационной Безопасностью
- Управление бизнес-устойчивостью
- Соответствие законодательным и регулирующим положениям, выявление мошенничества

Факты говорят правду!

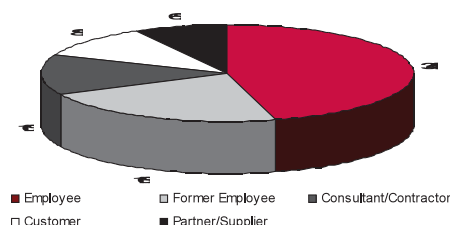
«70% всех случаев серьезных нарушений происходят с участием инсайдеров»
IDC Worldwide Security Products and services, 2008

«Сколько случаев нарушений безопасности произошло в Вашей компании в течение предыдущих 12 месяцев?»
(CIO Magazine/PwC Survey)



«85% опрошенных сотрудников сказали, что они бы использовали конфиденциальную информацию компании в своих целях в случае увольнения»
Cyber-Ark, 2009

«Как Вы считаете, что стало источником нарушения безопасности?»
(CIO Magazine/PwC survey)

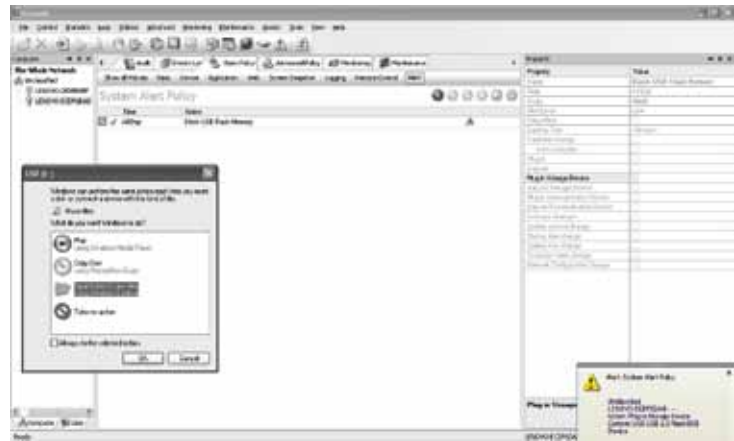


«97% респондентов считают, что наиболее вероятной причиной утечки информации послужили ненамеренные действия инсайдера или партнера по аутсорсингу либо умышленные действия инсайдера»
Ponemon Institute, 2009

IP-guard управляет инсайдерскими угрозами

Для минимизации инсайдерских рисков, организации должны ликвидировать способы и возможности, которые могут быть использованы для совершения таких преступлений. Анализируйте, контролируйте и управляйте доступом сотрудников и партнеров к Вашим информационным активам и интеллектуальной собственности.

IP-guard позволяет быстро и легко внедрить принципы «разделения обязанностей» и «наименьшего уровня привилегий» - принцип защиты системы, предусматривающий доступ сотрудников только к минимуму ресурсов для выполнения их работы. При помощи модулей «Управление приложениями» и «Управление Веб-страницами» Вы контролируете работу приложений и доступ в Интернет на уровне пользователя и рабочей станции. Доступ к данным и многочисленным приложениям увеличивает



продуктивность работы, но также и риск. Этот риск должен быть минимизирован, а не исключен. IP-guard позволяет Вам контролировать, как осуществляется доступ к данным, какие данные запрашиваются и когда. Применяя модули «Управление документооборотом», «Управление устройствами», «Управление печатью», «Управление почтой» и «Управление мгновенным обменом сообщениями», Вы сохраняете контроль над Вашими конфиденциальными данными и интеллектуальной собственностью.

Съемные устройства хранения данных обеспечивают более продуктивную работу, но также увеличивают риск утечки конфиденциальной информации. При помощи модуля «Управление съемными устройствами» Ваша организация может установить настройки, которые требуют авторизацию устройства, пользователя или машины для выполнения считывания и сохранения данных. IP-guard является наиболее гибким и эффективным решением для управления инсайдерскими рисками, при этом позволяя увеличивать продуктивность работы компании и её устойчивый рост.

IP-guard как способ управления внешними угрозами

При помощи модуля «Управление полосой пропускания» администратор легко может обнаружить любое неадекватное поведение в сети, которое может означать внешнюю угрозу, как например, «пиринговую» или FTP-загрузку. Обнаружение несанкционированного подключения к сети может быть реализовано при помощи модуля «Управление сетью». Он блокирует возможность незаконного доступа в сеть неавторизованных компьютеров и портов. IP-guard осуществляет мониторинг в режиме реального времени, и руководитель и администраторы получают уведомления в случае нарушения политики безопасности. Это позволяет им незамедлительно реагировать и адекватно минимизировать риски. В случае если требуется доступ к удаленной системе, возможно применение модуля «Управление удаленным доступом».

Исчерпывающая система управленческой отчетности и аудиторский учет от IP-guard

Модуль «Базовое управление» создан на базе IP-guard и позволяет определять основные настройки политики и системы отчетности в приложениях и активности в сети. При помощи модуля «Управление активами» Вы можете управлять всем программным и аппаратным обеспечением, включая лицензии,



обновления операционных систем и «патчи» (изменений, внесенных в программы). IP-guard ведет полный учет всей деятельности пользователя на рабочей станции. «Мониторинг экрана» может не только предоставлять доказательства нарушений, но также позволяет осуществлять мониторинг экранов в режиме реального времени. Аудиторский контроль и поддержка отчетности IP-guard соответствуют необходимым требованиям регулирующих актов, таких как «Sarbanes-Oxley Act» (SOX), «USA Patriot Act» и «Basel II».

Армения • Азербайджан • Беларусь • Грузия • Казахстан • Кыргызстан • Молдова • Таджикистан • Туркменистан • Украина • Узбекистан • Россия

www.cherrygroupcis.com

The Cherry Group CIS Ltd
Office 204
25, Aphrodite Street
1060 Nicosia
Cyprus

Контакт :
Олена В. Павлова
opavlova@cherrygroupcis.com

Эксклюзивный
дистрибутор:



Член:

