



IP-guard

Предотвращение потери данных и выстраивание бизнеса

IP-guard

Вы беспокоитесь о том, что:

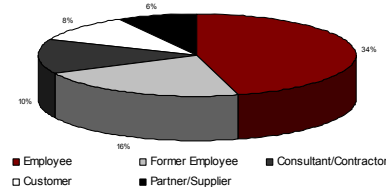
Дизайн вашего продукта незаметно похищен, клиентская база попала в руки Вашему конкуренту, финансовые данные намеренно украдены?
Ваши работники злоупотребляют корпоративными сетевыми ресурсами, увлекаются интернет играми, просматривают сайты не относящиеся к работе, «чатятся» и отправляют или принимают личную почту в рабочее время?
Ваш системный администратор тратит много времени и ресурсов на управление активами и обслуживание системы при низкой эффективности?

Преимущества IP-guard

[Предотвращение потери данных (DLP) и повышенная безопасность информации]

IP-guard фиксирует детали различных операций с электронными документами, выполненных Вашими работниками. Это защищает конфиденциальную информацию компании от незаконной передачи через сеть или внешние устройства. Кроме этого, продукт может автоматически шифровать информацию так, что она будет доступна только лицам, авторизованным компанией. IP-guard помогает компаниям в определении и блокировании незаконных операций, обеспечивая тем самым лучшую информационную безопасность и защиту данных .

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



[Стандартизация операций рабочих станций и увеличение продуктивности]

IP-guard предоставляет детальную запись и полные аналитические отчеты об использовании приложений работниками, включая работу с веб-браузером. Ограничения могут быть установлены для приложений и веб-страниц по категориями и/ или по времени, чтобы увеличить продуктивность работы сотрудников.

[Распределение ресурсов системы и оптимизация использования ресурсов]

IP-guard позволяет управлять пропускной способностью канала, чтобы не допустить скачивания работниками фильмов, музыки или других файлов, которые занимают значительный объем полосы пропускания. Также продукт позволяет осуществлять мониторинг таких операций, как печать файлов и запись компакт-дисков для оптимизации планирования ресурсов предприятий.

[Управление ИТ активами и снижение издержек на обслуживание]

IP-guard автоматически собирает данные о программном и аппаратном обеспечении. Автоматизироваться может также установка «патчей» и поиск уязвимостей. Функция внедрения программного обеспечения позволяет распространять «софт» третьих сторон на все или выбранные компьютеры с агентами. Эта опция предоставляет ИТ-администратору удобный способ управления ИТ-активами предприятия.

[Гибкая системная среда уровня предприятия для достижения корпоративного контроля]

IP-guard является чрезвычайно гибким и универсальным продуктом. Он может быть адаптирован к различным сетевым структурам, поддерживает удаленный контроль, помогая транснациональным организациям управлять заграничными подразделениями.

Управление инсайдерским риском

Предотвращение несанкционированного копирования документов на переносные устройства или путем передачи по сети. Блокирует соединение компьютера с внешними источниками (например, с переносными устройствами хранения данных, такими как гибкие диски, пишущие CD-приводы, USB, а также с устройствами для установки соединения – портами, модемами, разъемами USB, bluetooth, инфракрасными портами и пр.) для предотвращения незаконного копирования или перемещения данных.

Мониторинг и управление приложениями

Запись и ведение статистики использования приложений работниками для оценки эффективности их работы. В случае использования неавторизованного программного обеспечения появляется уведомление, а работа такого программного обеспечения блокируется IP-guard.

Мониторинг и контроль работы в интернете

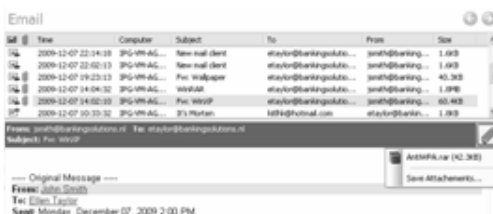
Запись веб-страниц, посещенных пользователями, и анализ данных об использовании интернет.

Журнал событий

Запись операций компьютера для отслеживания и анализа поведения работника.

Мониторинг почты

Запись содержимого исходящих и входящих почтовых сообщений и вложенных файлов.



Контроль отправки мгновенных сообщений

Мониторинг истории разговоров всех агентов обмена мгновенными сообщениями, а также передачи файлов с помощью таких агентов.



«70% всех случаев серьезных нарушений происходят с участием инсайдеров»

IDC Worldwide Security Products and services, 2008

Контроль пропускной способности канала и портов

Путем анализа данных о передаче и загрузке информации, формируется распределение пропускной способности канала. IP-guard также может контролировать сетевые коммуникации по IP-портам и IP-адресам для ограничения таких действий, как сетевые игры, просмотр фильмов, чаты, торрент-загрузки и передача информации за пределы организации.

Мгновенный снимок экрана

Снимок экрана компьютера в режиме реального времени с функцией записи экрана. Любое незаконное поведение может быть отслежено на экране.



Управление системами



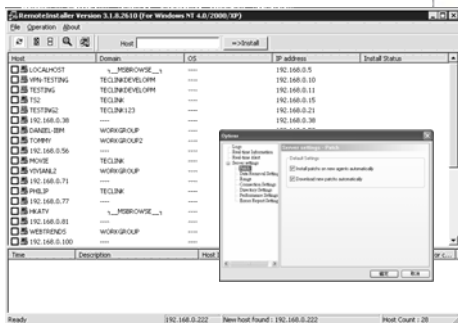
Внедрение программного обеспечения

Установка программного обеспечения

Обеспечение установки на каждый компьютер в корпоративной сети такого программного обеспечения, как ERP системы, бизнес-программы и другие офисные «патчи»

Распространение документов

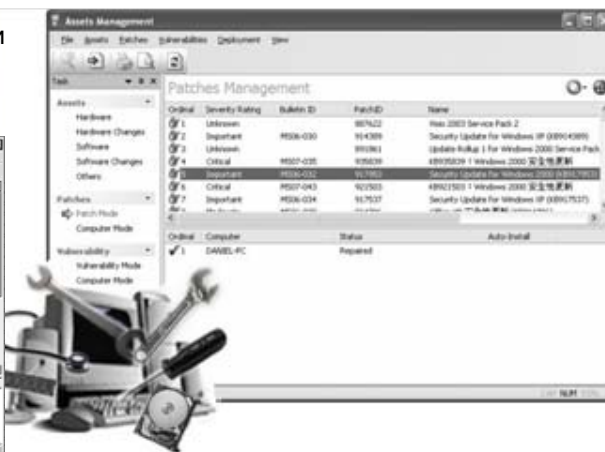
Рассылка документов и уведомлений выбранным агентам для минимизации рабочей нагрузки администратора и увеличения эффективности работы



Управление активами

Автоматический сбор информации о программном и аппаратном обеспечении

Детальная запись информации о программном и аппаратном обеспечении каждой рабочей станции. Дополнительная информация, относящаяся к устройствам: производитель, спецификации, авторское право и т.д.



Управление «патчами» и сканирование уязвимостей

Управление патчами Windows

Периодическое сканирование и загрузка «патчей» защиты, а также их распространение и автоматическая установка в сети

Сканирование уязвимостей

Периодическое сканирование, анализ и устранение системных уязвимостей

Отслеживание изменений программного и аппаратного обеспечения

Отслеживание изменений в аппаратных устройствах, установке и удалении программ. Уведомление о любых изменениях в статусе активов.

Запрос об активах и статистика

Автоматическое обобщение и сбор статистики об аппаратном и программном обеспечении

Удаленное обслуживание

Проверка информации в режиме реального времени

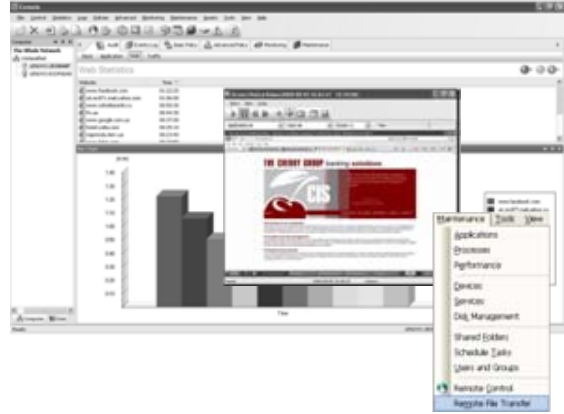
Администратор может проверять информацию удаленно в режиме реального времени, например, получать сервисный отчет об использовании CPU, анализировать и устранять ошибки на удаленных рабочих станциях

Удаленный рабочий стол

Администратор может установить соединение с любым агентом IP-guard через интернет и управлять компьютером при помощи мышки и клавиатуры

Передача файлов

Администратор может передавать файлы на и получать файлы с удаленных рабочих станций, что облегчает трансфер инструментов диагностики и файлов журнала



Информационная безопасность

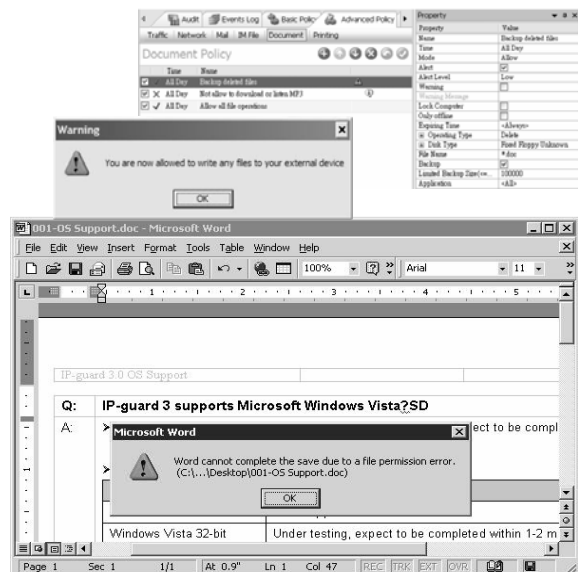
Конфиденциальная информация (например, коды источников, ключевые научные формулы, дизайнерские разработки и т.д.) хранится в электронных файлах. Безопасность файлов является основой информационной безопасности. IP-guard производит мониторинг доступа ко всем файлам и, в то же время, контролируя чтение и запись файлов на переносные устройства хранения данных, а также использование внешних устройств и интернета, позволяет предотвратить утечку конфиденциальной информации.

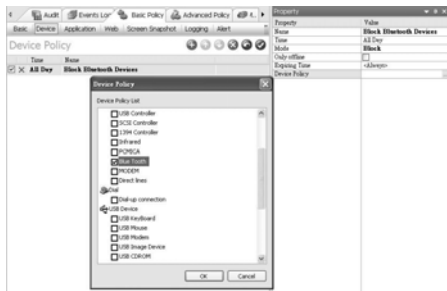
Мониторинг операций с документами

Запись всех операций с документами в деталях. Система заблокирует любые незаконные операции и уведомит об этом администратора.

Предотвращение утечки информации через переносные устройства хранения данных и сеть

Предотвращает несанкционированное копирование документов на переносные устройства хранения данных или через сеть. Блокирует соединение компьютера с внешними источниками (например, с переносными устройствами хранения данных, такими как гибкие диски, пишущие CD-приводы, USB, а также с устройствами для установки соединения – портами, модемами, разъемами USB, bluetooth, инфракрасными портами и пр.) для предотвращения незаконного копирования или перемещения данных.



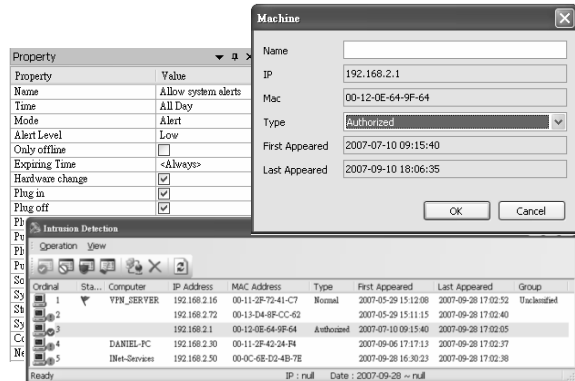


Предотвращает утечку важных файлов через интернет

Контроль передачи файлов по электронной почте, FTP, через приложения P2P и агенты обмена мгновенными сообщениями для предотвращения передачи конфиденциальной информации через интернет.

Предотвращает незаконный доступ к внутренней сети

Неавторизованные компьютеры не могут получить доступ в сеть, связываться и обмениваться информацией с другими компьютерами, даже если они подключены к внутренней сети, что позволяет эффективно устранить возможность несанкционированного копирования внутренней информации.



IP-guard включает в себя сервер, консоль, агент и свитч

[**Сервер**] собирает и хранит данные, автоматически распространяет политики

[**Консоль**] формирует политики, проверяет данные, обеспечивает статистический учет и анализ

[**Агент**] записывает данные и выполняет политики

[**Свитч**] обеспечивает соединение серверов, консолей и агентов из разных доменов

Системные требования IP-guard

[операционные системы]

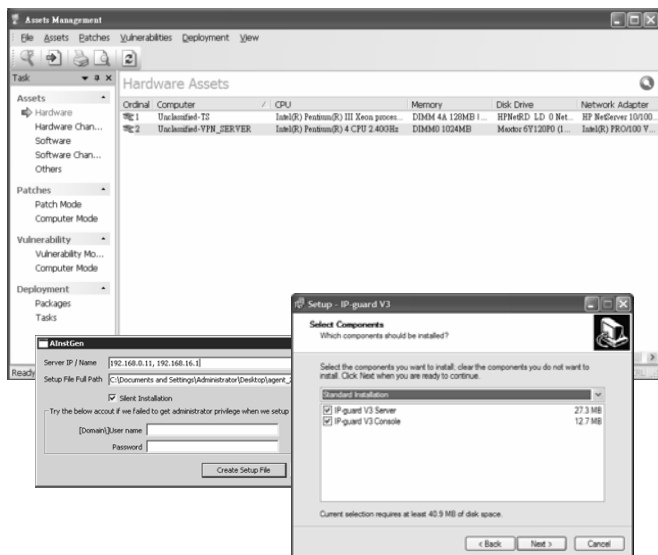
Microsoft Windows 95 OSR2 / 98 / ME / NT4 / 2000 / XP / 2003 / Vista

[минимальные требования к аппаратному обеспечению]

Сервер: P500 / 128MB / 10GB HD
 Консоль: P166 / 64MB / 10MB HD
 Агент: P166 / 32MB / 10MB HD
 Свитч: P166 / 32MB / 10MB HD

[сетевые требования]

Поддержка TCP/IP протокола



IP-guard Modules

Select only the modules you need to create a solution that works for you

The modular build-up of IP-guard allows you to select only the modules that you need to meet your exact requirements. This way, you will only pay for functionality that really benefits your organization. Basic Management is a mandatory module and provides the core of IP-guard's functionality.

Module name	Module description
Основное Управление	<ul style="list-style-type: none"> - Настройка и установка политик IP-guard - Базовые средства управления, такие как доступ к панели управления - Мощный механизм поиска и функциональность импорта/экспорта
Управление приложениями	<ul style="list-style-type: none"> - Предотвращение использования неавторизованных приложений - Детальные лог-файлы приложений и профили пользователей - Незамедлительные сообщения о нарушениях безопасности в программных системах
Управление документами	<ul style="list-style-type: none"> - Детальное логирование всех операций (редакт., удаление, копирование и т.д.) - Мощные возможности шифрования внутренних и внешних хранилищ данных - Автоматическое резервирование всех изменяемых файлов
Управление IM	<ul style="list-style-type: none"> - Поддержка всех известных Интернет-пейджеров, таких как: Skype, ICQ, MSN и другие - Запись всех переговоров и сообщений - Возможность логирования и резервного копирования всех пересылаемых файлов
Управление почтой	<ul style="list-style-type: none"> - Поддержка всех типов электронной почты: POP/SMTP mail / Outlook / Notes / webmail и т.д. - Ограничение отправляемых сообщений по разным параметрам (адресат / тема / размер прикрепленного файла и т.д.) - Логирование и легкий поиск всех сообщений и прикрепленных файлов
Управление печатью	<ul style="list-style-type: none"> - Контроль прав доступа к принтеру во всей организации - Возможность резервного копирования всех печатаемых файлов - Детальное логирование использования всех типов принтеров: локальных, сетевых и виртуальных
Управление экраном	<ul style="list-style-type: none"> - Мониторинг активности экранов в режиме реального времени - Возможность мониторинга 16 экранов одновременно с возможностью видеть их на одном экране - Возможность записи экранной истории в видео-файле
Управление веб	<ul style="list-style-type: none"> - Контроль доступа к веб с использованием опций черного или белого списков - Незамедлительные сообщения для руководства о нарушениях политики безопасности пользования Интернетом - Детальное логирование всех действий в Интернет
Управление съёмными накопителями	<ul style="list-style-type: none"> - Авторизация использования съёмных носителей - Шифрование дисков и съёмных носителей на уровне файлов - Авторизованный доступ к зашифрованным данным
Управление оборудованием	<ul style="list-style-type: none"> - Полная инвентаризация и управление программным и аппаратным обеспечением - Сканирование защищенности и автоматическое обновление Windows - Быстрое и эффективное средство установки корпоративного программного обеспечения
Управление полосой пропускания	<ul style="list-style-type: none"> - Контроль над использованием пропускной способности на уровне пользователей или структурных единиц - Контроль трафика на уровне портов и IP адресов - Ограничение скорости загрузки на уровне рабочих станций
Управление устройствами	<ul style="list-style-type: none"> - Легкий контроль доступа к аппаратным устройствам - Возможность запуска новой политики безопасности в режиме реального времени без перезагрузки - Детальное логирование и незамедлительные сообщения о нарушении политики безопасности аппаратных устройств
Управление сетью	<ul style="list-style-type: none"> - Полный контроль над сетевым трафиком на уровне портов и IP адресов - Предотвращение несанкционированного доступа на уровне сети - Незамедлительные сообщения для администраторов при нарушении политики сетевой безопасности
Удалённое техобслуживание	<ul style="list-style-type: none"> - Удаленные отчеты о состоянии рабочих станций - Обеспечение поддержки удаленных систем во всем мире - Удаленная транспортировка файлов

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

The Cherry Group CIS Ltd

25, Aphrodite Street

1060 Nicosia

Cyprus

Тел +357 22 02267-2

Факс: +357 22 02267-9

E-mail: info@cherrygroupcis.com

Наш партнер :

Эксклюзивный дистрибутор:



www.cherrygroupcis.com