



Secret Net Studio 8.13

Средство защиты данных и контроля безопасности конечных точек



Сокращение издержек на администрирование СЗИ и обучение персонала



Быстрая централизованная настройка защиты в соответствии с требованиями законодательства РФ



Высокая масштабируемость, поддержка распределенных инфраструктур



Централизованное управление клиентами SNS для Linux/ Secret Net LSP

Основные заказчики



ИТ и телеком



Энергетика



Наука и НПО



Финансы



Органы
государственной
власти



Обработывающие
производства

Задачи

- Защита рабочих станций и серверов от вирусов и вредоносных программ.
- Защита от сетевых атак.
- Защита от подделки и перехвата сетевого трафика внутри локальной сети.
- Защита информации от несанкционированного доступа.
- Контроль утечек и каналов распространения защищаемой информации.
- Защита от действий инсайдеров.
- Разграничение доступа к конфиденциальной информации и ресурсам.
- Защита от кражи информации при утере носителей.
- Соответствие требованиям регуляторов к защите персональных данных, государственных информационных систем, автоматизированных систем управления и государственной тайны.
- Защита объектов критической информационной инфраструктуры (КИИ).

Возможности Secret Net Studio



Возможности

Защита от несанкционированного доступа

- Дискреционное и мандатное управление доступом к файлам.
- Усиленный вход в систему.
- Поддержка схем аутентификации пользователя.
- Теневое копирование.
- Контроль печати.
- Затирание данных.
- Замокнутая программная среда и контроль целостности данных.

Антивирусная защита и обнаружение вторжений

- Сигнатурные и эвристические методы поиска вредоносного ПО.
- Постоянная защита, сканирование из контекстного меню и по расписанию.
- «Белые» списки директорий и файлов.
- Выбор профилей сканирования.
- Локальные серверы обновлений.
- Эвристический и сигнатурный анализ входящего сетевого трафика.
- Автоматическая временная блокировка атакующих хостов.
- Команда оперативного снятия блокировки.
- Песочница.
- Почтовый антивирус.
- Удаление вредоносных файлов, занятых другими процессами.

Шифрование данных

- Шифрование контейнеров произвольного размера.
- Хранение ключевой информации на электронных ключах или съемных дисках.
- Резервное копирование ключей.
- Настраиваемые права доступа к данным в контейнере.
- Полнодисковое шифрование.
- Совместимость с ПАК «Соболь».
- Регистрация изменений статусов защиты диска сторонними средствами.

Защита сетевого взаимодействия

Межсетевой экран

- Фильтрация трафика на L3, L4 и L7.
- Настройка реакции на срабатывание правил.
- Возможность задать действие правил по дням недели и времени суток.
- Шаблоны для различных сетевых служб.
- Добавление возможности экспортировать/импортировать правила МЭ.
- Поддержка настройки SPI через Программу управления.

Авторизация сетевых соединений

- Разграничение доступа для терминальных серверов.
- Защита от атак Man-in-the-middle.
- Программная сегментация сети без изменения сетевой топологии.
- Сокращение сетевого трафика.

Централизованное управление и мониторинг

- Шаблоны настроек для приведения системы в соответствие требованиям законодательства РФ.
- Централизованное развертывание, установка исправлений и обновлений.
- Централизованное управление клиентами SNS для Linux/Secret Net LSP через сервер безопасности SNS.
- Иерархические политики для управления настройками защитных компонентов.
- Получение журналов из ПАК «Соболь».
- Оповещение о событиях ИБ в панели управления и по e-mail.
- Централизованное управление безопасностью в несвязанных доменах Active Directory.
- Детализированный аудит применения эффективных политик безопасности.
- Идентификация действий администратора в системе.
- Передача парольных политик в ПАК «Соболь».
- Поддержка экспорта/импорта списка рабочих станций.
- Централизованное управление сессиями пользователей и питанием компьютера.
- Возможность отправки журналов на сторонний syslog сервер.
- Возможность создания и распространения легковесного автономного пакета развертывания.
- **new** Централизованное управление с помощью Security Code Orchestrator:
 - Управление клиентами SNS и SNS для Linux.
 - Возможность совместного режима работы сервера безопасности SNS и Security Code Orchestrator.

Контроль устройств

- Дискреционное и полномочное управление доступом к устройствам.
- Контроль по группам, классам, моделям и отдельным устройствам.
- Иерархическое наследование настроек.
- Контроль подключения и отключения устройств.
- Управление перенаправлением устройств в терминальных подключениях.
- Защита от подмены VID и PID подключаемого устройства.

Устойчивость к атакам

- Внешний контроль целостности защитных процессов СЗИ.
- Внешний контроль целостности драйверов в системе.
- Защита системы управления от действий локального администратора.
- **new** Возможность интеграции со сторонними песочницами.

Лицензирование



По уровню защиты

Подсистема	Максимальная защита	Оптимальная защита	Постоянная защита	Дополнительная защита*
Защита от НСД	●	●	●	-
Контроль устройств	●	●	●	-
Защита диска и шифрование контейнеров	●	-	●	-
Персональный межсетевой экран	●	-	●	-
Антивирус	●	●	-	●
Обнаружение и предотвращение вторжений	●	●	-	●
Песочница	●	-	●	-
Полнодисковое шифрование	●	-	●	-
Срок лицензии	1 или 3 года	1 или 3 года	Бессрочно	1 или 3 года

* Пакет «Дополнительная защита» может быть приобретен только в дополнение к другому набору лицензий.

Сертификаты

Secret Net Studio 8.10, 8.13

ФСТЭК России

- СВТ 5
- СКН 4
- САВЗ 4
- МЭ 4 тип «В»
- СОВ 4
- УД 4

Secret Net Studio 8.10

ФСБ России

- СЗИ от НСД класса АК3/АК5

О компании «Код Безопасности»

Компания «Код Безопасности» – лидирующий российский разработчик сертифицированных программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов.

+7 (495) 982-30-20

info@securitycode.ru

www.securitycode.ru

