

ОФИСНЫЙ КОНТРОЛЬ И DLP safetica

Иван Иванов, технический консультант

 TECHNOLOGY ALLIANCE



О КОМПАНИИ

SAFETICA TECHNOLOGIES

- › Чешская компания, основана в 2009 году, команда 70+
- › Клиенты в более чем 95 странах
- › Продукт входит в TOP 5 DLP - в рейтинге журнала SC Magazine
- › DLP решение для любого типа бизнеса - по версии Gartner
- › Входит в ESET Technology Alliance с 2016 года

УТЕЧКА ДАННЫХ

ПОЧЕМУ ЭТО ПРОИСХОДИТ?

- › Создание собственной компании на базе уникальных данных
- › Продажа информации конкурентам
- › Использование данных для устройства на новую работу
- › Чтобы просто навредить компании или людям в ней
- › «Я создавал это, значит это мои данные!» (Нет, это не так...)
- › Другие причины, которые кажутся сотрудникам логичными

УТЕЧКА ДАННЫХ

КАК ЭТО ПРОИСХОДИТ?

- › USB-флешки / телефоны / внешние жесткие диски
- › DropBox / и другие облачные хранилища
- › Электронная почта
- › Различные приложения
- › Мессенджеры
- › Bluetooth
- › ...



УТЕЧКА ДАННЫХ ЭТО РЕАЛЬНОСТЬ!

- › **67% сотрудников распечатывают**
любые корпоративные документы
- › **47% копируют документы**
или делают скриншоты
- › **73% подключают флешки**
и другие внешние носители к рабочим ПК

Человеческий фактор

*63% инцидентов информационной безопасности в компаниях связано с бывшими и действующими сотрудниками**

** PricewaterhouseCoopers, 2016*

- › **47% пересылают рабочие файлы**
на личную почту
- › **44% устанавливают приложения**
на компьютер в корпоративной сети
- › **56% открывают любые сайты**
без ограничений

УТЕЧКА ДАННЫХ КАК ЗАЩИТИТЬСЯ?

ОФИСНЫЙ КОНТРОЛЬ И DLP SAFETICA



ПРИНЦИПИАЛЬНЫЕ РАЗЛИЧИЯ



СЕТЕВЫЕ

АППАРАТНЫЙ ИЛИ ВИРТУАЛЬНЫЙ ШЛЮЗ



КОНТЕНТНЫЙ ФИЛЬТР

ПРИНЯТИЕ РЕШЕНИЯ НА ОСНОВЕ АНАЛИЗА
СОДЕРЖИМОГО



АГЕНТНЫЕ

АГЕНТЫ DLP НА КОНЕЧНЫХ ТОЧКАХ



КОНТЕКСТНЫЙ ФИЛЬТР

ПРИНЯТИЕ РЕШЕНИЯ ПО ФОРМАЛЬНЫМ
ПРИЗНАКАМ



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

АРХИТЕКТУРА РЕШЕНИЯ SAFETICA

В четыре шага

- › Анализ – 1 неделя
- › Установка – 2 недели
- › Обучение (входит в остальные этапы)
- › Настройка – 4 недели



КОМПЛЕКСНОЕ РЕШЕНИЕ SAFETICA



AUDITOR

РЕГИСТРАЦИЯ АКТИВНОСТИ СОТРУДНИКОВ



SUPERVISOR

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ БИЗНЕС-ПРОЦЕССОВ КОМПАНИИ



DLP

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ КОМПАНИИ



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

НИКАКИХ СКРЫТЫХ РАСХОДОВ

Сервер

Процессор: четырёхядерный 2,4GHz

Оперативная память: от 2GB

Жесткий диск: от 3GB свободного места (от 100GB с БД)

ОС: MS Windows Server 2008 и выше, 32&64-bit

База данных (MS SQL)

MS SQL 2008 R2 и выше, рекомендуется MS SQL 2012 и выше

MS SQL 2016 Express включена в установочный пакет Safetica



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ AUDITOR)



ПРЕДСТАВЛЕНИЕ О ТОМ, ЧТО
ПРОИСХОДИТ В КОМПАНИИ



СОБЛЮДЕНИЕ ПОЛИТИК
БЕЗОПАСНОСТИ



СРАВНЕНИЕ РАБОТЫ
СОТРУДНИКОВ



АУДИТ ЧУВСТВИТЕЛЬНЫХ
ДАННЫХ КОМПАНИИ



ЭФФЕКТИВНОСТЬ
ИСПОЛЬЗОВАНИЯ ПО



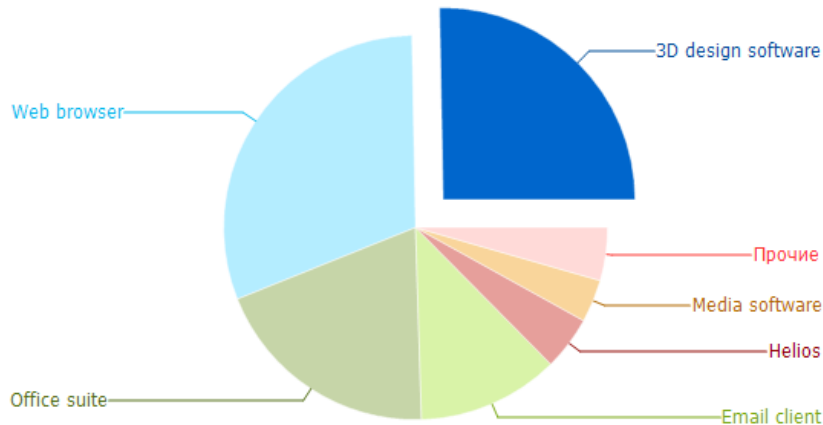
АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ AUDITOR)

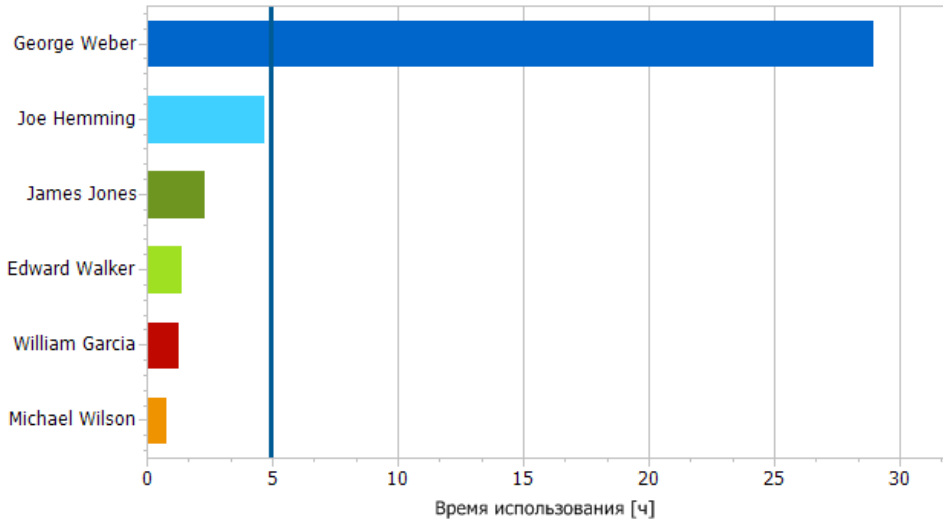


ГРАФИКИ

Топ категорий приложений



Топ активных пользователей



Время работы приложе...
Активное время работы ...
Наиболее активные при...

ЗАПИСИ

Перетащите под тот текст столбцы, по которым вы хотите сгруппировать

Приложение

Имя пользователя	ПК	Продолжительность	Путь приложения	Дата и время	С - по
Приложение: AutoCAD 2015					33 h 30 min 36 s активного времени
Приложение: SolidWorks (solidworks.exe)					5 h 36 min 20 s активного времени

Упорядочить

Категория приложен...

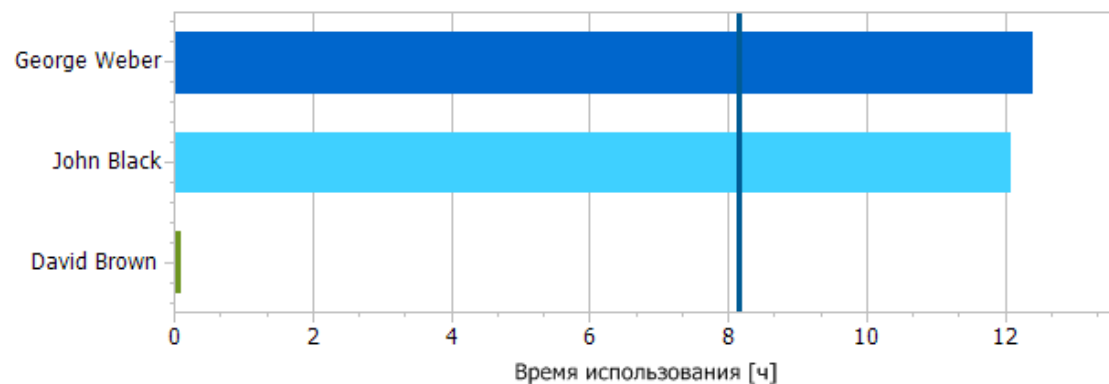


АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

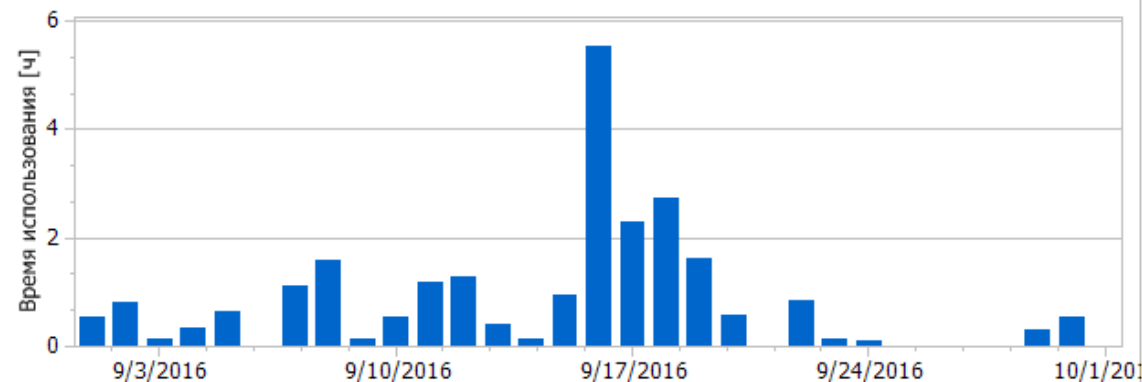
ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ AUDITOR)



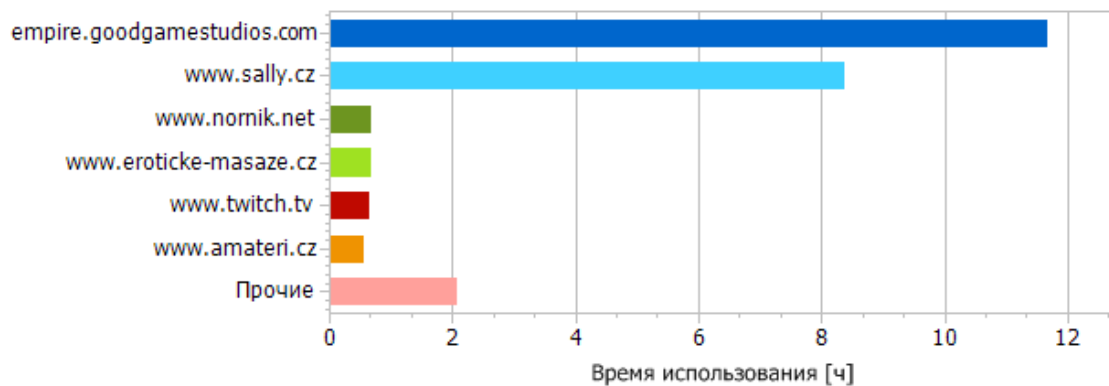
Топ пользователей



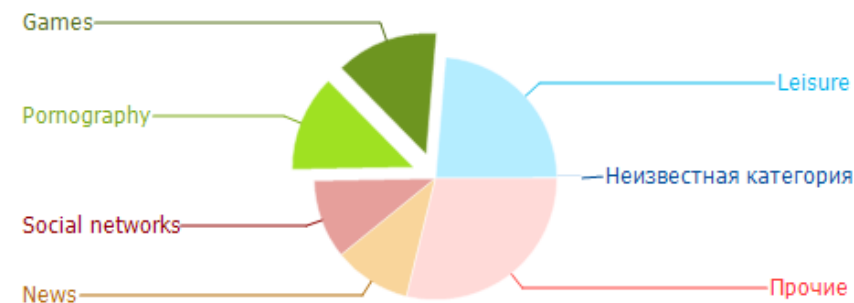
Посещение веб-сайтов



Самые посещаемые домены



Самые популярные веб-категории

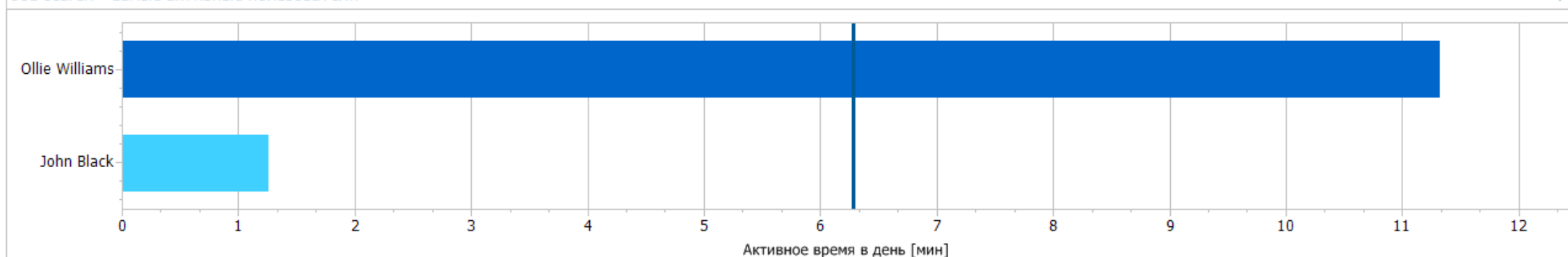


АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ AUDITOR)

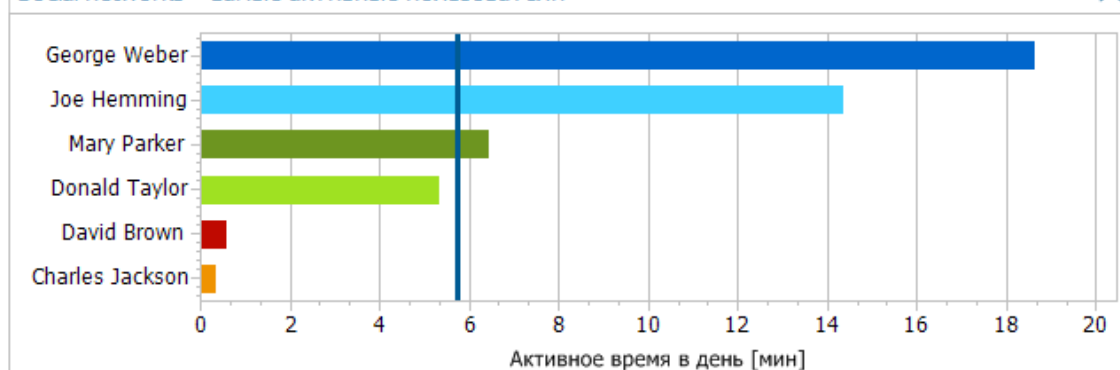


Job search - Самые активные пользователи



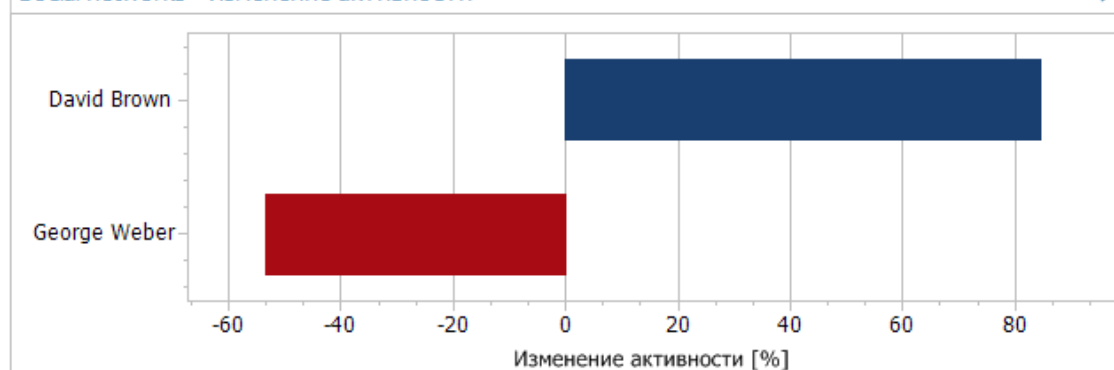
Среднее значение: 06 мин 17 сек

Social networks - Самые активные пользователи



Среднее значение: 05 мин 44 сек

Social networks - Изменение активности



Базовый период: 01.09.2016 - 21.09.2016 (20 дней)
Текущий период: 21.09.2016 - 01.10.2016 (11 дней)



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ AUDITOR)

- › **Дополнительная мотивация сотрудников**

по итогам оценки эффективности труда

- › **Обоснование для расширения штата**

на основе объективной информации о загруженности

- › **Снижение нагрузки на сотрудника/отдел**

и справедливое распределение обязанностей внутри рабочей группы

- › **Ваш вариант**



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ SUPERVISOR)



› Web-контроль



› Контроль приложений



› Контроль печати



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

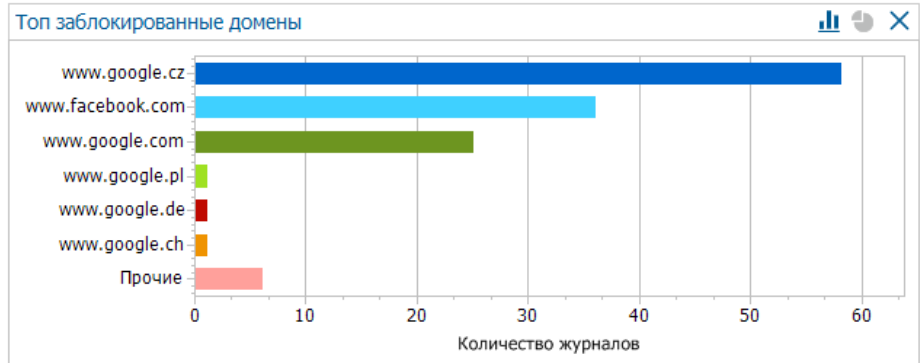
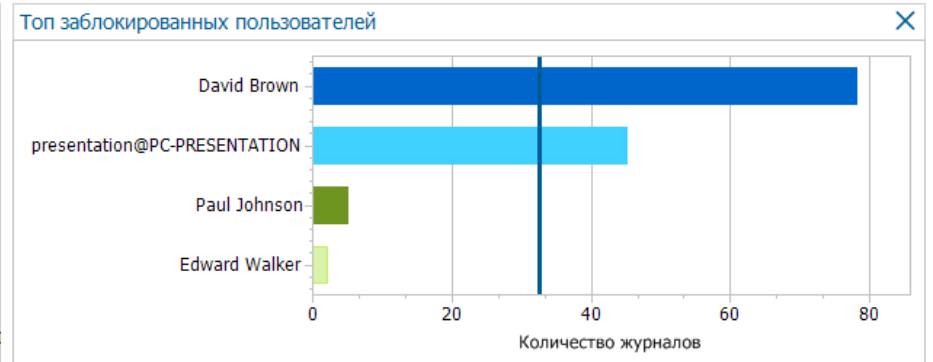
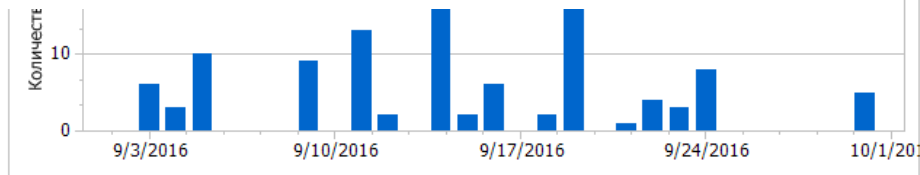
ОФИСНЫЙ КОНТРОЛЬ (WEB-КОНТРОЛЬ)



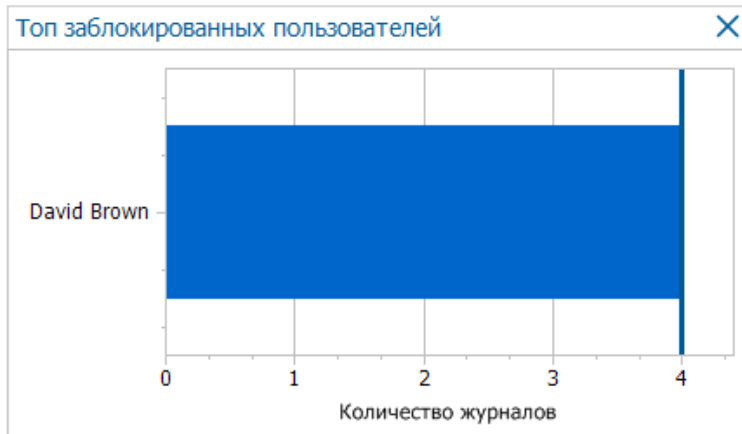
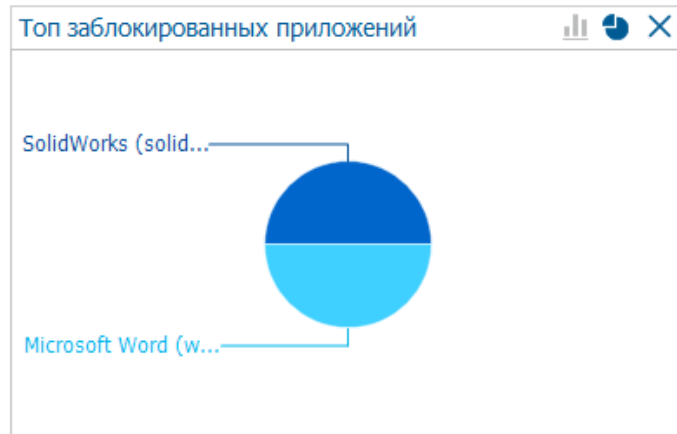
Действие по умолчанию: Разрешено

Добавить правило

Имя	Подробнее
Блокировка по категориям	Категории: File hosting, Job search, Malware, Pornography, ...
Блокировка по IP	Категории: Pornography IP-адрес: 192.168.0.5, 192.168.0.15 - ...
Блокировка по домену	URL: *.facebook.com/*, *.twitter.com/*



ОФИСНЫЙ КОНТРОЛЬ (КОНТРОЛЬ ПЕЧАТИ)



Состояние квот

Текущее состояние квот для выбранных пользователей/группы

Имя пользователя	Всего страниц (регул...	Цветные страницы (...)
esetnote01		
PC-Garcia	50 (50)	0 (0)
William Garcia	50 (50)	0 (0)
PC-Jones	50 (50)	0 (0)
James Jones	50 (50)	0 (0)
PC-Parker	50 (50)	0 (0)
Mary Parker	50 (50)	0 (0)
PC-Hemming	50 (50)	0 (0)
PC-Jackson	50 (50)	0 (0)
PC-Walker	50 (50)	0 (0)
PC-Wilson	50 (50)	0 (0)
Michael Wilson	50 (50)	0 (0)
Edward Walker	50 (50)	0 (0)

« » 0 из 0

OK



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ОФИСНЫЙ КОНТРОЛЬ (КОНТРОЛЬ ПРИЛОЖЕНИЙ)



Новое правило

☒ Введите путь к приложению
Путь может содержать символ *. Например: C:\Users*\Roaming*

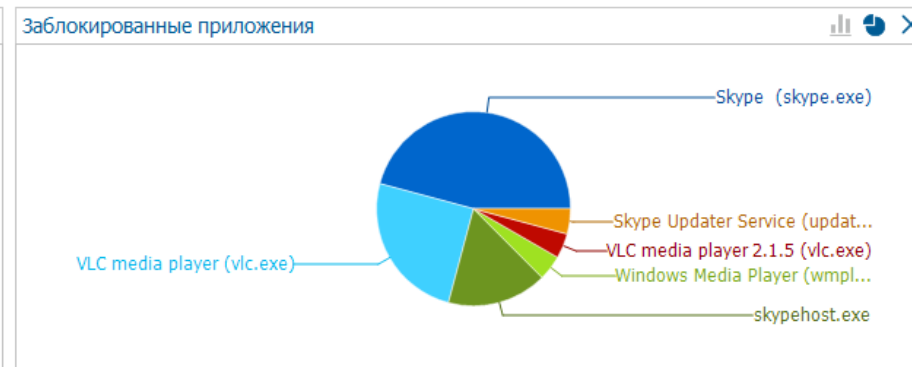
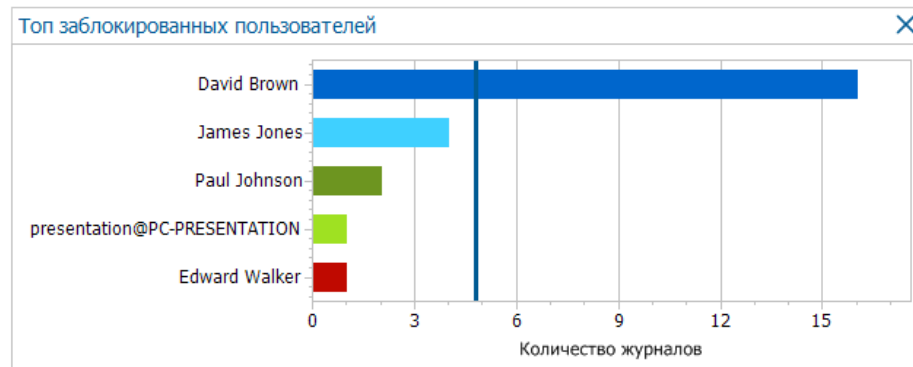
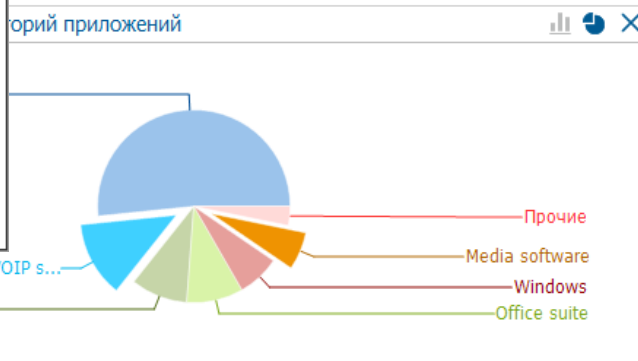
☐ Выберите категорию

Имя:

Путь к программе:

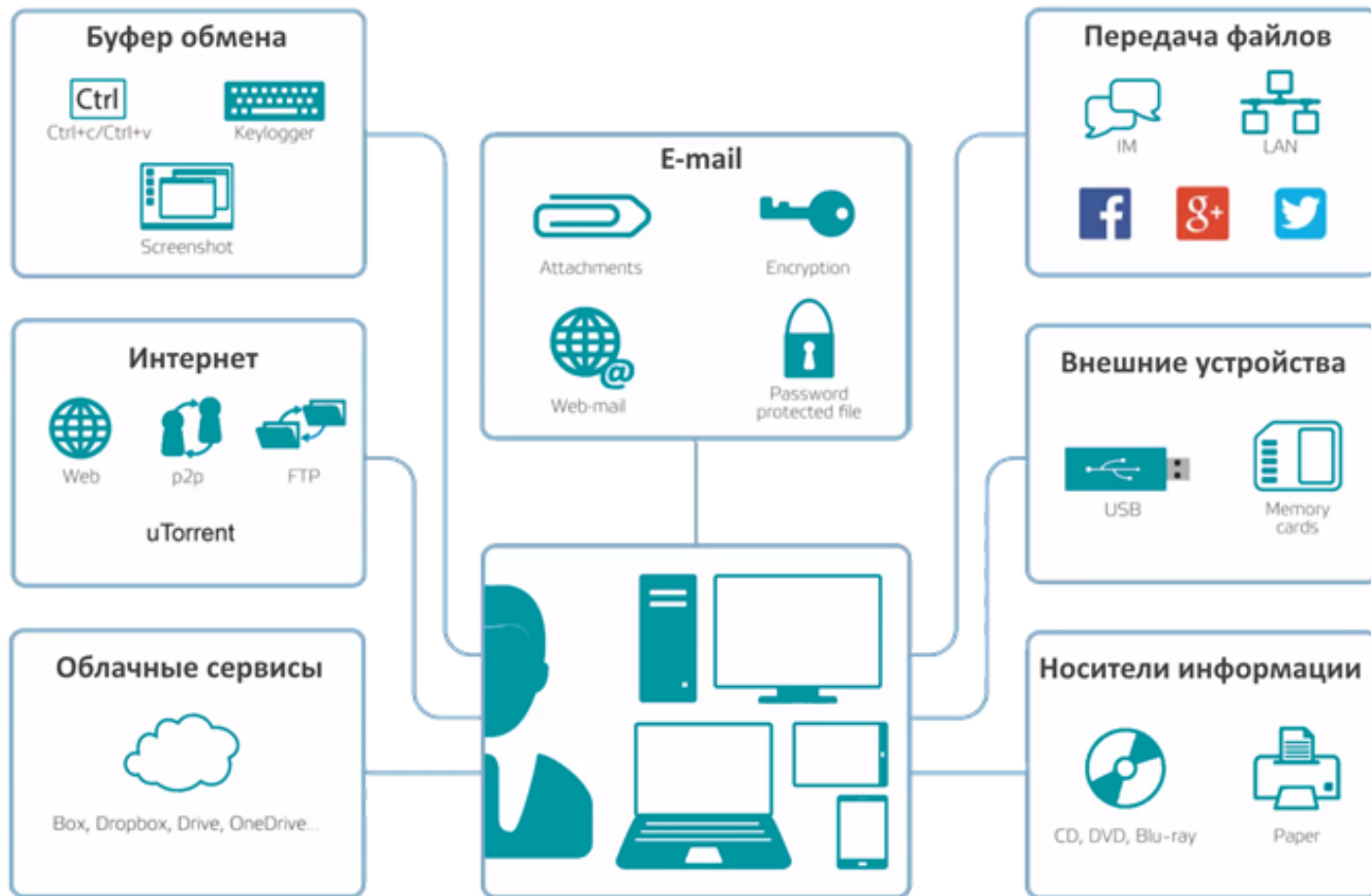
Область действия: ☒ Везде

Назад Далее Отменить



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (МОДУЛЬ DLP)



Область доступа

Локальные диски:		Разрешить
Внешние устройства:		Запретить
Принтеры:		<u>Зона</u>
Сеть:		<u>Зона</u>
Email:		<u>Зона</u>
Шифрованные диски:		<u>Наследовать</u>
Облачные хранилища:		<u>Запретить</u>
Удаленная передача:		Запретить
операции		
Скриншоты:		Запретить
Буфер обмена:		Уведомлять
Запись на диск:		Запретить
Виртуальная печать:		Запретить

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (КОНТЕКСТНЫЙ ФИЛЬТР)

› ПРАВИЛА ПРИЛОЖЕНИЙ

Определение приложений и категорий приложений, в которых выходные файлы должны быть помечены выбранной категорией данных

› ВЕБ ПРАВИЛА

Веб-правила могут использоваться для установки меток на файлы, загруженные с определенных доменов или доменов из определенной категории

› ПРАВИЛА ПО ПУТИ

Все файлы, помещенные в определенные папки, будут автоматически получать необходимую метку.

› КОНТЕНТНЫЕ ПРАВИЛА

Все файлы, содержащие определенный контент, будут автоматически получать необходимую метку.



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (КОНТЕНТНЫЙ ФИЛЬТР)

- › Электронная почта
- › Мессенджеры
- › Внешние устройства
- › Загрузка файлов в Интернет

ПРАВИЛА ПОЛИТИКИ

Шаблон политики: Пользовательский - Настроить

Загрузка в сеть: ☒ Безопасные зоны разрешены

Email: ☒ Зарегистрирован

Интернет мессенджеры: ☒ Разрешен

Внешние устройства: ☒ Безопасные зоны разрешены

Облачные хранилища: ☒ Зарегистрирован

ПРАВИЛА ПОЛИТИКИ

Шаблон политики: Встроенные: Управление к - Настроить

Загрузить в общую папку: ☒ Зарегистрирован

Загрузить на веб-почту: ☒ Зарегистрирован

Загрузка в сеть: ☒ Разрешен

Email: ☒ Разрешен

Интернет мессенджеры: ☒ Зарегистрирован

Внешние устройства: ☒ Безопасные зоны разрешены

Облачные хранилища: ☒ Пользовательский

Принтеры: ☒ Безопасные зоны разрешены



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (КОНТЕНТНЫЙ ФИЛЬТР)

› ПРЕДУСТАНОВЛЕННОЕ СОДЕРЖИМОЕ

Идентификационные номера и номера социального страхования различных стран, номера кредитных карт, номера банковских счетов.

› КЛЮЧЕВЫЕ СЛОВА И РЕГУЛЯРНЫЕ ВЫРАЖЕНИЯ

Любые слова и словосочетания, использование регулярных выражений с применением синтаксиса ECMAScript

› МЕТАДААННЫЕ СТОРОННИХ КЛАССИФИКАТОРОВ

Протестирована поддержка метаданных Microsoft Azure Information Protection, Boldon James, Tukan GREENmod.

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ

ПРЕДУСТАНОВЛЕННЫЕ ПРАВИЛА

^ ОСНОВНАЯ ИНФОРМАЦИЯ

Политики DLP настраивают безопасность данных в вашей среде. Политики управляют общим потоком данных, конкретными данными или приложениями и предлагают действия DLP, от автоматической регистрации событий до строгой блокировки. Чтобы ознакомиться с политиками DLP, посетите [базу знаний Safetica](#).

Новая политика безопасности

⚠ Применяется первое соответствующее правило политики.

Политика	Тип	Режим		
↓ Patients + ...	TopSecret	Блокирова...	Изменить	Удалить
↓ Patients + ...	TopSecret	Уведомить	Изменить	Удалить
↓ Patients + ...	TopSecret	Блокирова...	Изменить	Удалить
↓ Patients + ...	TopSecret	Уведомить	Изменить	Удалить
↓ Financial Fil...	Sensitive	Уведомить	Изменить	Удалить
↓ Financial Fil...	Sensitive	Уведомить	Изменить	Удалить
↓ Multimedia...	Multimedia	Зарегистр...	Изменить	Удалить
↓ Multimedia...	Multimedia	Зарегистр...	Изменить	Удалить
↓ Patients + ...	Insurance -...	Блокирова...	Изменить	Удалить
↓ Patients + ...	Insurance -...	Уведомить	Изменить	Удалить
↓ Patients + ...	Insurance -...	Блокирова...	Изменить	Удалить
↓ Patients + ...	Insurance -...	Уведомить	Изменить	Удалить
↓ Design dat...	CAD softw...	Блокирова...	Изменить	Удалить
↓ MS Office ...	Office suite	Блокирова...	Изменить	Удалить
↓ MS Office ...	Office suite	Уведомить	Изменить	Удалить
↓ MS Office ...	Office suite	Уведомить	Изменить	Удалить
↓ Channel co...	Sensitive d...	Уведомить	Изменить	Удалить

^ ПОДРОБНОСТИ ПОЛИТКИ

Имя политики: **Patients + Design Files policy - TopSecret - zone settings - notifying**

Описание политики: **Please see the manual.**

Тип политики: **Данные: TopSecret**

Режим политики: **Зарегистрировать и уведомить**

Политика применяется к: **Safetica**

^ ПРАВИЛА ПОЛИТИКИ

Загрузка в сеть: **Настройки пользовательской зоны**

Email: **Настройки пользовательской зоны**

Облачные хранилища: **Различающиеся настройки**

Буфер обмена (не регистрировать): **Уведомлен**

Создание скришота (не регистрировать): **Уведомлен**

Запись на диск: **Уведомлен**

Сеть (эксперт): **Настройки пользовательской зоны**

Локальные диски (эксперт): **Настройки пользовательской зоны**



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (МОДУЛЬ DLP)

^ ИНТЕГРАЦИЯ В ПРИЛОЖЕНИЯ

[Сбросить к настройкам по умолчанию](#)

Приложение	Активно в режиме	Состояние интеграции
Microsoft Edge (microsof...	Расширенный монитор...	☒ Активно
Microsoft OneDrive for B...	Расширенный монитор...	☒ Активно
Microsoft OneNote Quic...	Расширенный монитор...	☒ Активно
Firefox (firefox.exe)	Расширенный монитор...	☒ Активно
Thunderbird (thunderbir...	Расширенный монитор...	☒ Активно
Send to OneNote Tool (O...	Расширенный монитор...	☒ Активно
Microsoft OneNote (ONE...	Расширенный монитор...	☒ Активно
Microsoft Outlook (outlo...	Расширенный монитор...	☒ Активно
Microsoft Edge Content ...	Расширенный монитор...	☒ Активно
Yandex (browser.exe)	Расширенный монитор...	☒ Активно
Browser_Broker (browser_...	Расширенный монитор...	☒ Активно
Microsoft Word (WINWO...	Расширенный монитор...	☒ Активно
Runtime Broker (runtime...	Расширенный монитор...	☒ Активно

^ ИНТЕГРИРОВАННЫЕ ТЕХНОЛОГИИ

- Сетевой уровень: ☒ Активировать
- Расширение MAPI: ☒ Активировать
- Контекстное меню: ☒ Активировать

^ ДРАЙВЕРЫ

 Для завершения деактивации требуется перезагрузить компьютер.

- Драйвер диска Safetica: ☒ Активировать
- Драйвер шифрования Safetica: ☐ Наследовать
- Safetica device driver: ☐ Наследовать

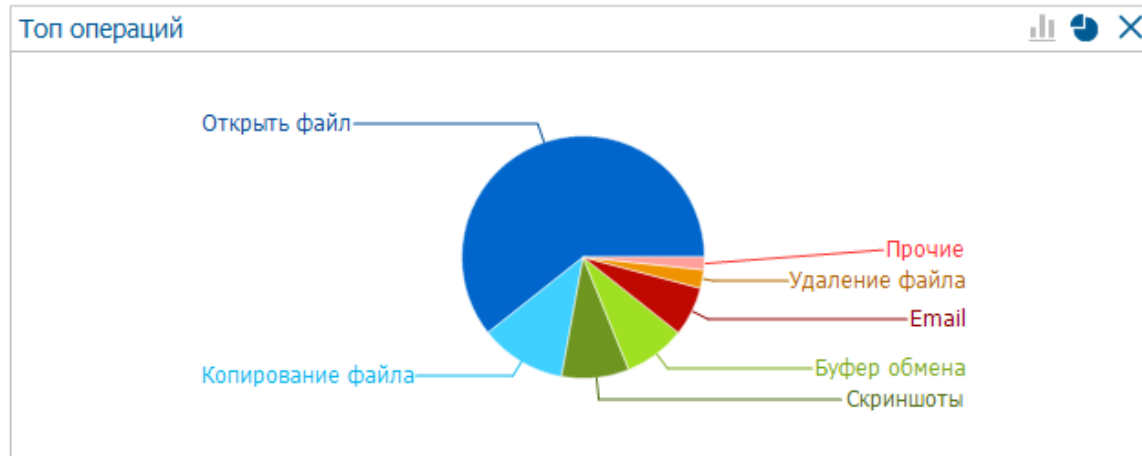
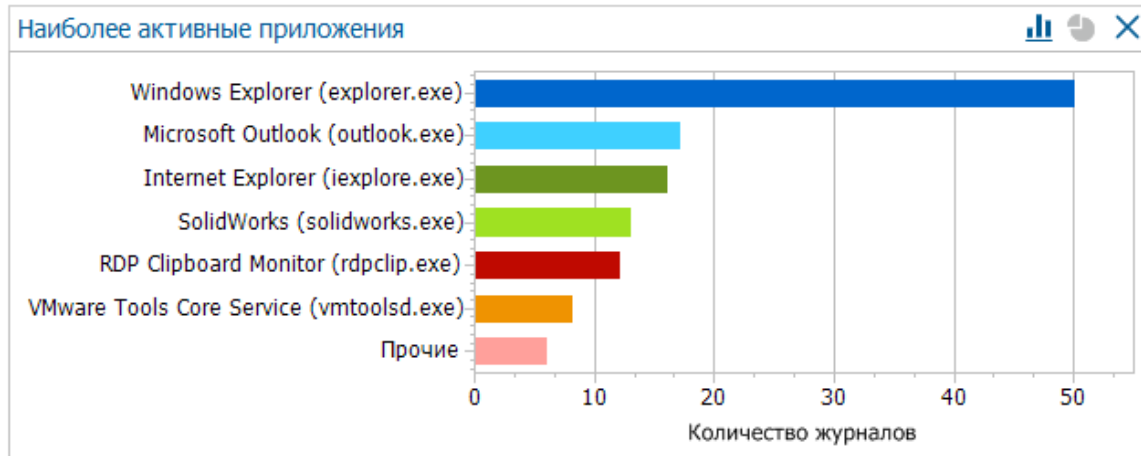
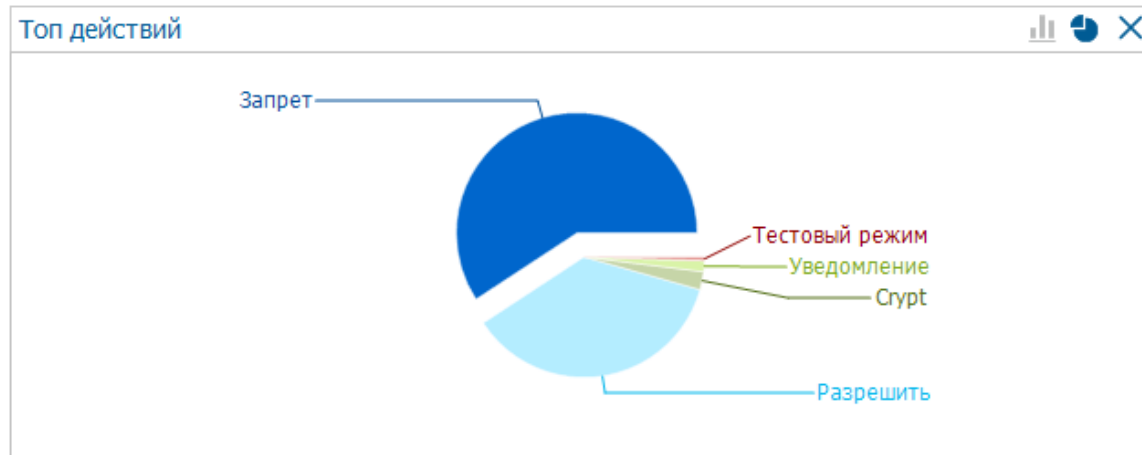
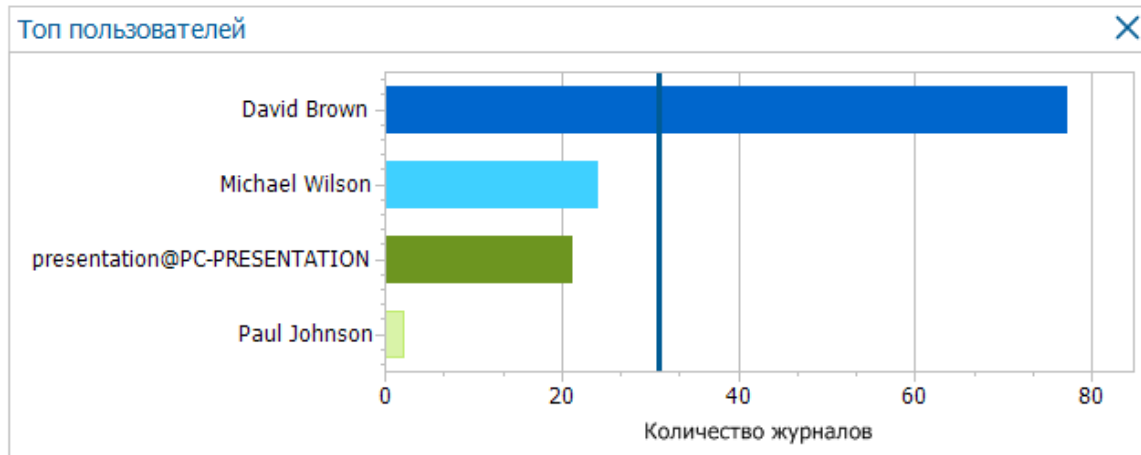
^ СЕРВИСЫ

- Safetica net monitor service: ☒ Активировать
- Safetica DLP service: ☒ Активировать
- Служба мониторинга файлов Safetica: ☒ Активировать
- Служба классификации Safetica: ☒ Активировать
- Служба приложений Safetica: ☒ Активировать
- Обслуживание устройств Safetica: ☐ Наследовать



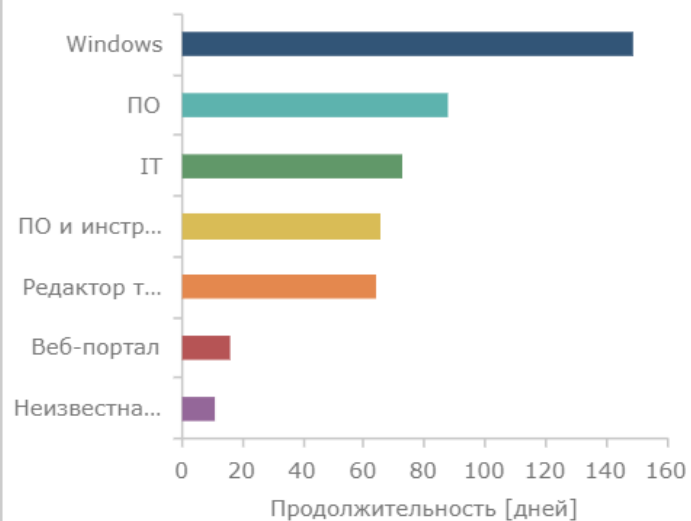
АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (МОДУЛЬ DLP)



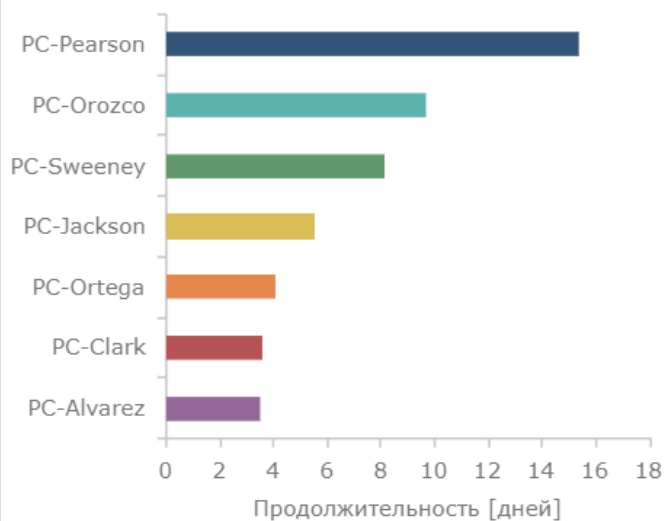
АНАЛИЗ РЕЗУЛЬТАТОВ WEBSAFETICA

КАК СОТРУДНИКИ ИСПОЛЬЗОВАЛИ С...



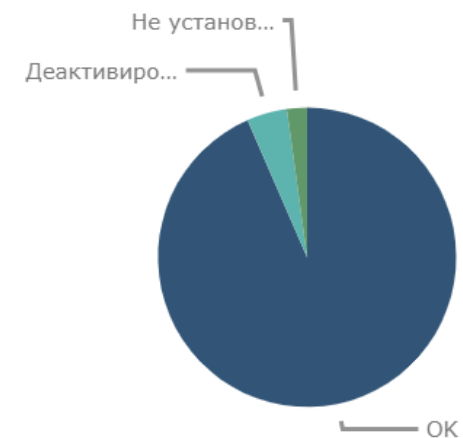
АНАЛИЗ ПОВЕДЕНИЯ >

КАКИЕ КОМПЬЮТЕРЫ БЫЛИ НАИБО...



ИСПОЛЬЗОВАНИЕ РЕСУРСОВ >

КАК ЗАЩИЩЕНА МОЯ КОМПАНИЯ?



УПРАВЛЕНИЕ >



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ОТЧЕТНОСТЬ И БЛОКИРОВКА ДЕЯТЕЛЬНОСТИ

ОТЧЕТ SAFETICA

ОТЧЕТЫ

ОТЧЕТ ОБ АКТИВНОСТИ ЗА МЕСЯЦ

период: 11.01.2018 - 11.02.2018

Выбранные группы: root

Выбранные пользователи / компьютеры:

Количество пользователей / компьютеров: 4/5

СОДЕРЖАНИЕ

Auditor - Приложения - Использование прил

Auditor - Приложения - Наиболее часто испо

Auditor - Приложения - Самые активные пол

Auditor - Электронная почта - Наиболее акти

Загрузка файлов в сеть заблокирована

☐ Google Chrome

☐ Договор.txt

☐ https://nofile.io/

Загрузка файла **Договор.txt** защищенные данные (категор) заблокирована.

Это действие противоречит п

Close

Нельзя отправлять это электронное письмо

☐ Microsoft Outlook

☒ test

@ skuznecov@esetnod32.ru

Ваше письмо **test** содержит конфиденциальную информацию. Убедитесь, что отправляете ее правильным получателям.

Это действие ограничено [политикой безопасности](#) и будет записано в журнал.

В электронном письме содержится следующая конфиденциальная информация:

- Номера кредитных карт

☐ Помните мой выбор для этих данных и получателей

Отправить

Не отправлять

security@esetnod32.ru

Предупреждения

Safetica <noreply@safetica.com>

кому: [REDACTED]

Safetica зарегистрировала новые предупреждения. Обратите внимание на следующие события:

* Снимок экрана заблокирован. Категории данных: Супер Секретно. (Правила: утечка) - Администратор [REDACTED] - [REDACTED] (12.02)

УПРАВЛЕНИЕ ЛИЦЕНЗИЕЙ

РАСПРЕДЕЛЕНИЕ МОДУЛЕЙ

Активируйте необходимые модули

Edit license assignments

Activated users and computers

Company

Edit license assignments

Add

Group	Auditor	Safetica	Safetica Mobile
Company	Enabled	Disabled	

OKCancel

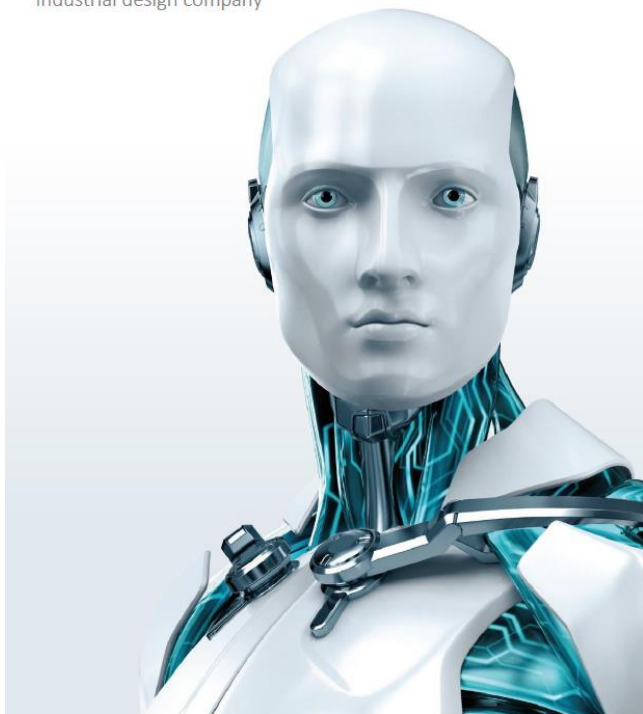
РЕЗУЛЬТАТЫ ВНЕДРЕНИЯ

eset ОФИСНЫЙ КОНТРОЛЬ И DLP

esafetica

АНАЛИЗ РЕЗУЛЬТАТОВ

Industrial design company



✓ ПРОИЗВОДИТЕЛЬНОСТЬ:

- *Использование приложений*
- *Посещенные сайты*
- *Поиск работы*
- *Общее время непродуктивной деятельности*

✓ РАБОТА С ДАННЫМИ:

- *Утечка данных из компании*
- *Нежелательные действия с данными*

✓ ИСПОЛЬЗОВАНИЕ IT-РЕСУРСОВ:

- *Использование рабочих станций*
- *Печать*
- *Дорогие лицензии*



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ЛИЦЕНЗИРОВАНИЕ И ЦЕНЫ



› АУДИТОР



› ОФИСНЫЙ КОНТРОЛЬ



› FULL DLP

Лицензия на один, два или три года
Количество узлов в лицензии: от **10** до **N**



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ЛИЦЕНЗИРОВАНИЕ И ЦЕНЫ

- › Продление на 1 год: скидка 40%
- › Миграция (с аналогичного продукта конкурента): скидка 20%
- › Отраслевая скидка для образования: 50%
- › Отраслевая скидка для медицины: 30%

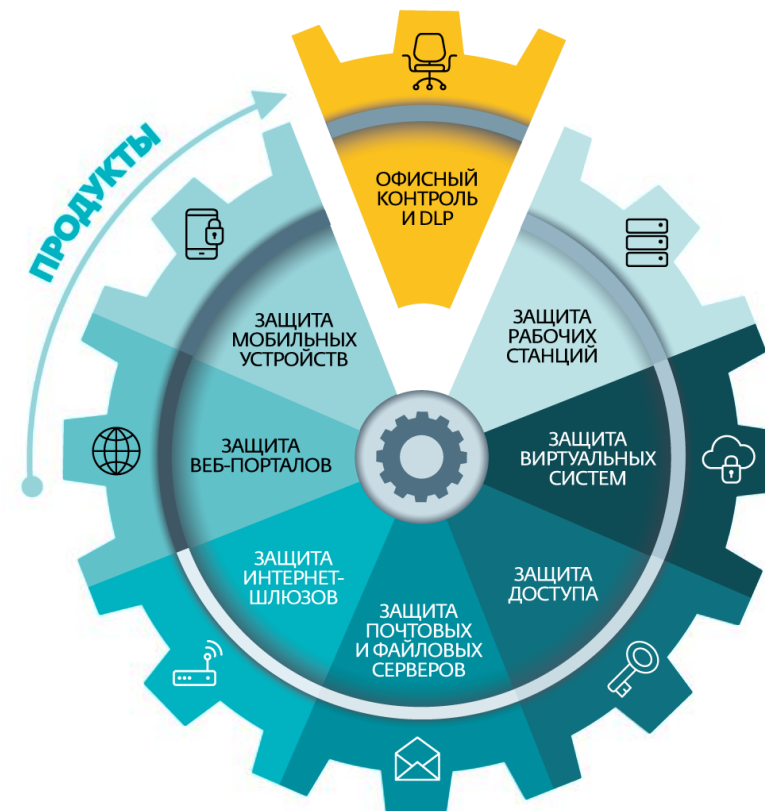
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

КОМПЛЕКСНЫЙ ПОДХОД

У компании есть:

- › Антивирус
- › Файервол
- › Антиспам
- › Защита от сетевых атак
- › ...

Офисный контроль и DLP – это недостающий уровень безопасности!



ДЛЯ ЛЮБОЙ КОМПАНИИ

Офисный контроль и DLP Safetica

Закрывает распространенные проблемы, связанные с человеческим фактором в компании любого размера

✓ КОМПЛЕКСНОЕ РЕШЕНИЕ

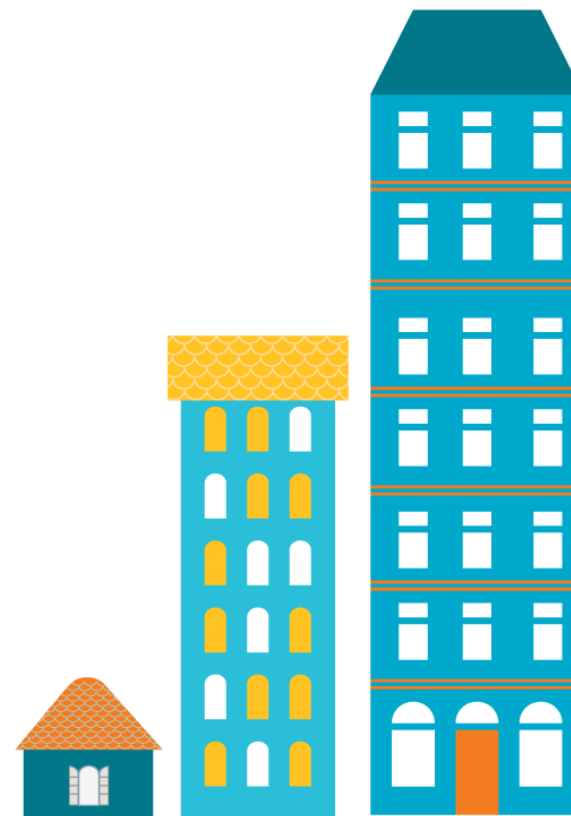
- *Аудит активности пользователей*
- *Ограничение деятельности сотрудников*
- *Предотвращение утечки данных*

✓ ЛЕГКОЕ ВНЕДРЕНИЕ

- *Независимость от структуры и языка документов*
- *Поддержка любых типов файлов*
- *Не требуется составления словарей*

✓ БЕЗ ДОПОЛНИТЕЛЬНЫХ ВЛОЖЕНИЙ

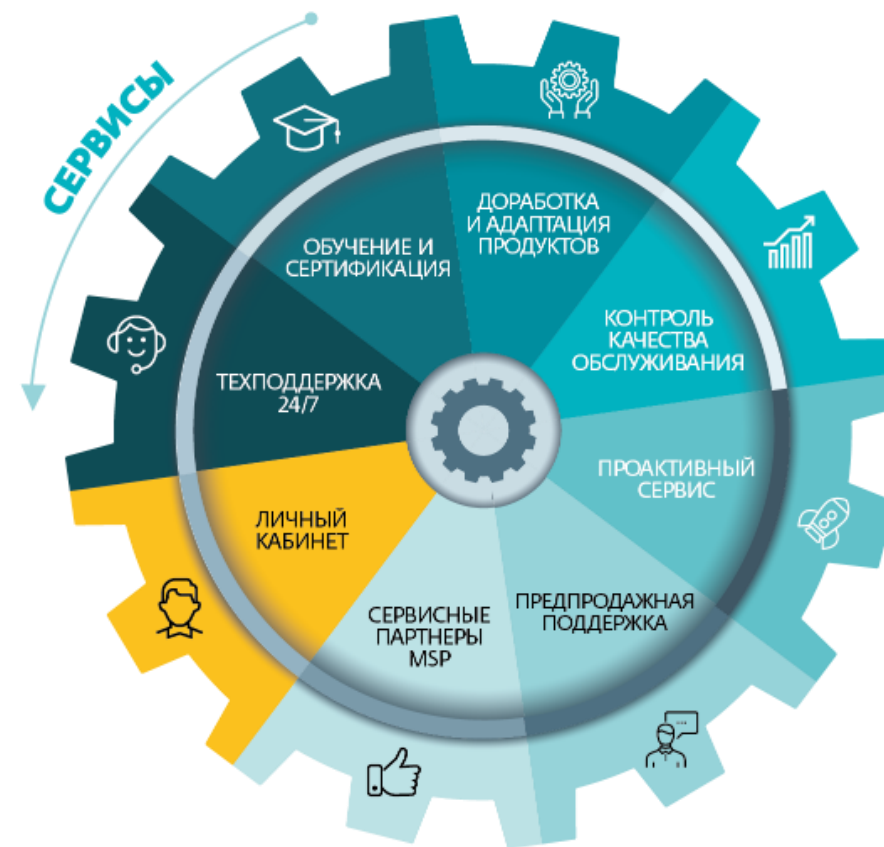
- *Стоимость проекта = стоимость лицензии*



СЕРВИСЫ ESET

ПОМОЖЕМ ВАМ В ЛЮБОЙ СИТУАЦИИ

- ✓ *Предпродажная поддержка*
- ✓ *Доработка и адаптация продуктов*
- ✓ *Техническая поддержка 24/7*
- ✓ *Контроль качества обслуживания*
- ✓ *Обучение и сертификация*



СЕРВИСЫ ESET

ПОДТВЕРЖДЕННОЕ КАЧЕСТВО

ESET – победитель номинаций российского конкурса клиентского сервиса CX Awards:

- ✓ «Лучшее вовлечение персонала»
- ✓ «Лучшие клиентоориентированные организации»





АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Спасибо! Вопросы?

