



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ESET – ЗАЩИТА ОТ ВНУТРЕННИХ УГРОЗ

*Дмитрий Самойленко, региональный
представитель ESET в ЮФО/СКФО*



ESET В РОССИИ И МИРЕ: СВЕЖИЕ НОВОСТИ

30

РАЗВИВАЕМ
ТЕХНОЛОГИИ
БЕЗОПАСНОСТИ
УЖЕ 30 ЛЕТ



9 ЦЕНТРОВ
ИССЛЕДОВАНИЙ



>110 млн
КОРПОРАЦИИ, СРЕДНИЙ
И МАЛЫЙ БИЗНЕС,
ДОМАШНИЕ
ПОЛЬЗОВАТЕЛИ ПО
ВСЕМУ МИРУ



ПЕРВЫЙ ВЕНДОР,
ЗАВОЕВАВШИЙ
100 НАГРАД
VIRUS BULLETIN



АНТИВИРУСНЫЙ
ВЕНДОР №4
В КОРПОРАТИВНОМ
СЕКТОРЕ В МИРЕ*

ESET RUSSIA



С 2005 года

Более 150 сотрудников

7 офисов в России и странах СНГ

• Более 15 миллионов пользователей в России

• Более 500 компаний-партнеров

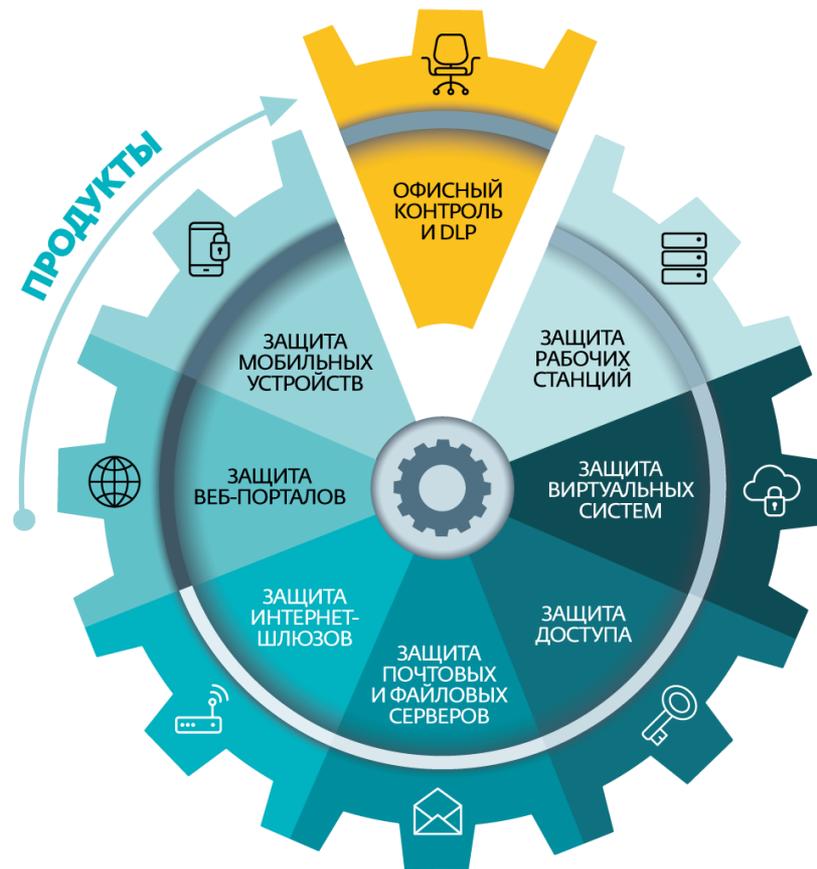
• 25-30% – доля российского рынка



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

НЕ ПРОСТО АНТИВИРУС

ОФИСНЫЙ КОНТРОЛЬ И SAFETICA DLP



О КОМПАНИИ SAFETICA TECHNOLOGIES



- › Чешская компания, основана в 2009 году, команда 70+
- › Клиенты в более чем 50 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

УТЕЧКА ДАННЫХ

КАК ЭТО ПРОИСХОДИТ?

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



СЛАБОЕ ЗВЕНО

Человеческий фактор

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

** PwC, 2016*



НЕКОМПЕТЕНТНОСТЬ

Нарушение правил информационной безопасности, утечка конфиденциальных данных, ошибки в работе в сети



ЗЛОНАМЕРЕННЫЕ ДЕЙСТВИЯ

Кража информации в пользу конкурентов, уничтожение ПО, переписки или документов, публикация конфиденциальных данных



ПРОБЛЕМЫ ЭФФЕКТИВНОСТИ

Непродуктивное использование времени, ПО и компьютеров; падение производительности; поиск новой работы

НЕКОМПЕТЕНТНОСТЬ. УТЕЧКА ДАННЫХ ЭТО РЕАЛЬНОСТЬ!

61% сотрудников

*злоупотребляет доступом к конфиденциальным
данным компании**

** Ponemon Institute, 2016*

› **67% сотрудников распечатывают**

любые корпоративные документы

› **47% копируют документы**

или делают скриншоты

› **73% подключают флэшки**

и другие внешние носители к рабочим ПК

› **47% пересылают рабочие файлы**

на личную почту

› **44% устанавливают приложения**

на компьютер в корпоративной сети

› **56% открывают любые сайты**

без ограничений

ЗЛОНАМЕРЕННЫЕ ДЕЙСТВИЯ. КАК МСТЯТ СОТРУДНИКИ

- › **20% копировали**
*рабочие материалы при увольнении,
чтобы использовать на новой работе*
- › **7% пользовались**
*удаленным доступом к почте
и другим ресурсам после увольнения*
- › **5% уничтожили**
*ценные документы, переписку или ПО,
уходя из компании*
- › **2% опубликовали**
*конфиденциальные данные
бывшего работодателя*



НЕЭФФЕКТИВНОСТЬ. ЧЕМ НА САМОМ ДЕЛЕ ЗАНЯТЫ СОТРУДНИКИ

- › **28% сидят в соцсетях**
*в рабочее время (и это не SMM-менеджеры)**
- › **21% делают халтуру**
*в рабочее время**
- › **69% активно ищут новую работу**
*или открыты для предложений***

**Тратят на соцсети в 2 раза
больше времени**

на работе, чем дома

** Pесурс VoucherCodesPro, 2012*



ЧЕЛОВЕЧЕСКИЙ ФАКТОР КАК ЗАЩИТИТЬСЯ?

ОФИСНЫЙ КОНТРОЛЬ И DLP SAFETICA



ПРИНЦИПИАЛЬНЫЕ РАЗЛИЧИЯ

ДОРОГО И ДОЛГО



СЕТЕВЫЕ

АППАРАТНЫЙ ИЛИ ВИРТУАЛЬНЫЙ ШЛЮЗ



КОНТЕНТНЫЙ ФИЛЬТР

ПРИНЯТИЕ РЕШЕНИЯ НА ОСНОВЕ АНАЛИЗА
СОДЕРЖИМОГО

БЫСТРО И БЕЗ ЛИШНИХ ЗАТРАТ



АГЕНТНЫЕ

АГЕНТЫ DLP НА КОНЕЧНЫХ ТОЧКАХ



КОНТЕКСТНЫЙ ФИЛЬТР

ПРИНЯТИЕ РЕШЕНИЯ ПО ФОРМАЛЬНЫМ
ПРИЗНАКАМ

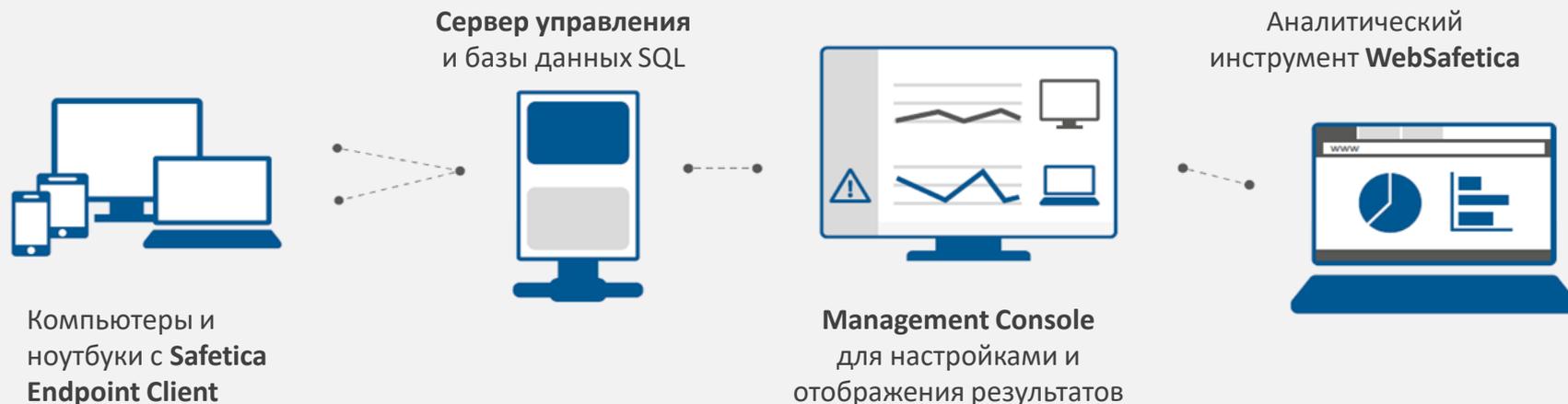
АРХИТЕКТУРА РЕШЕНИЯ SAFETICA



НИКАКИХ СКРЫТЫХ РАСХОДОВ

Офисный контроль и DLP “Safetica”

АРХИТЕКТУРА РЕШЕНИЯ



Клиент

Процессор: двухъядерный 2,4 GHz
Оперативная память: 2 GB
Жесткий диск: 2 GB свободного места
ОС: MS Windows XP и выше, 32&64-bit

Сервер

Процессор: четырёхъядерный 2,4GHz
Оперативная память: от 4GB
Жесткий диск: от 20GB свободного места
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 2012 Express включена в
установочный пакет Safetica

КОМПЛЕКСНОЕ РЕШЕНИЕ SAFETICA



AUDITOR

РЕГИСТРАЦИЯ АКТИВНОСТИ СОТРУДНИКОВ



ОФИСНЫЙ КОНТРОЛЬ

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ БИЗНЕС-ПРОЦЕССОВ КОМПАНИИ



DLP

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ КОМПАНИИ

ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ AUDITOR)



АУДИТ
ЧУВСТВИТЕЛЬНЫХ
ДАННЫХ КОМПАНИИ



ПРЕДСТАВЛЕНИЕ О
ТОМ, ЧТО ПРОИСХОДИТ
В КОМПАНИИ



УМЕНЬШЕНИЕ
РАСХОДОВ НА
ПЕРСОНАЛ



ПОВЫШЕНИЕ
ЭФФЕКТИВНОСТИ
СОТРУДНИКОВ



СОКРАЩЕНИЕ
РАСХОДОВ КОМПАНИИ
НА ОФИСНЫЕ НУЖДЫ



СРАВНЕНИЕ РАБОТЫ
СОТРУДНИКОВ



СОБЛЮДЕНИЕ ПОЛИТИК
БЕЗОПАСНОСТИ



ОКУПАЕМОСТЬ
ВНЕДРЕНИЯ

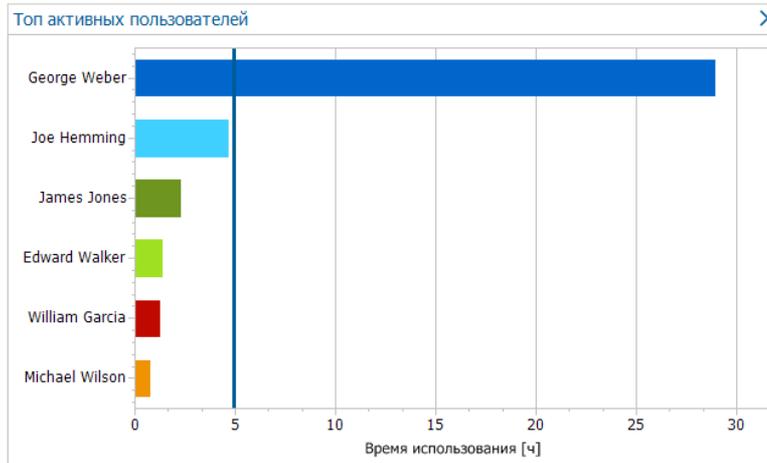
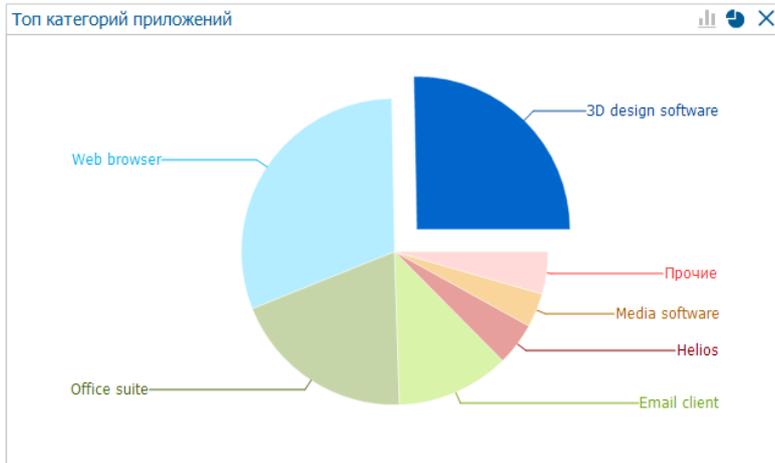


ЭФФЕКТИВНОСТЬ
ИСПОЛЬЗОВАНИЯ ПО

ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ AUDITOR)



ГРАФИКИ



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

ЗАПИСИ

Перетащите под тот текст столбцы, по которым вы хотите сгруппировать

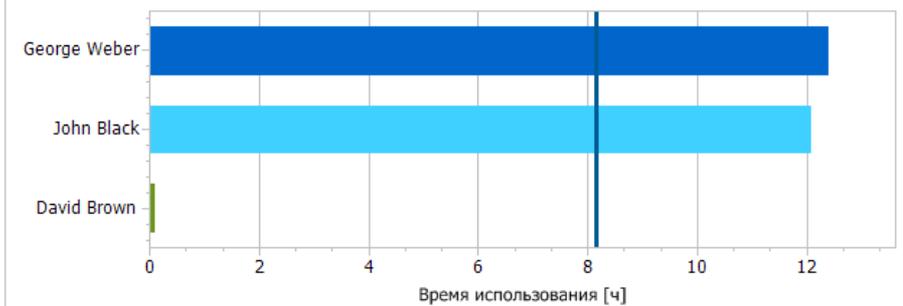
Приложение	Имя пользователя	ПК	Продолжительность	Путь приложения	Дата и время	С - по	Упорядочить
Приложение: AutoCAD 2015						33 h 30 min 36 s активного времени	
Приложение: SolidWorks (solidworks.exe)						5 h 36 min 20 s активного времени	

Категория приложен...Y

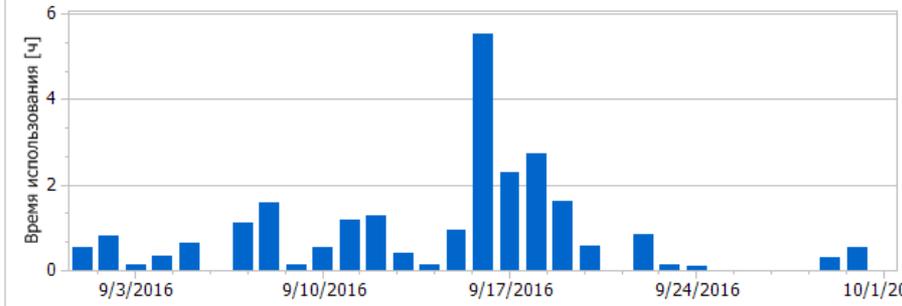
ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ AUDITOR)



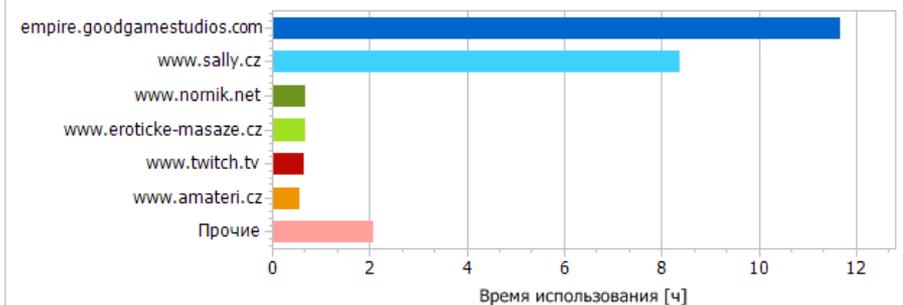
Топ пользователей



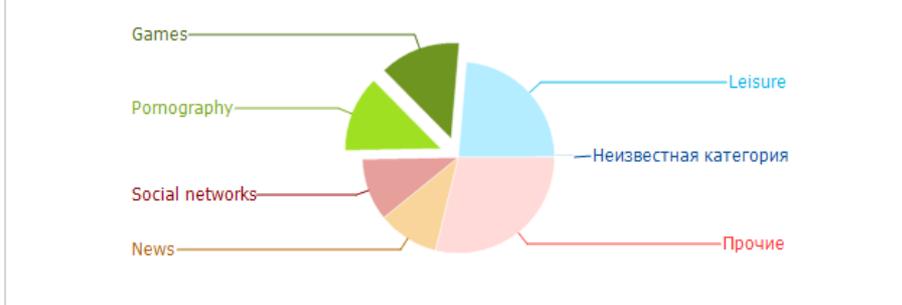
Посещение веб-сайтов



Самые посещаемые домены



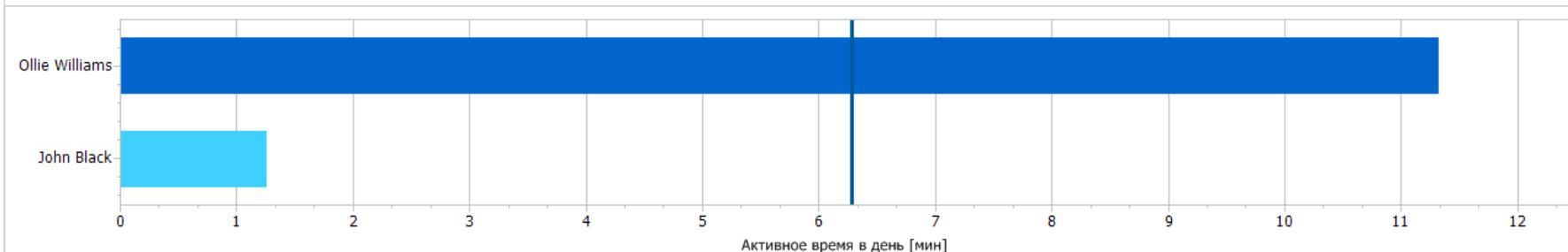
Самые популярные веб-категории



ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ AUDITOR)

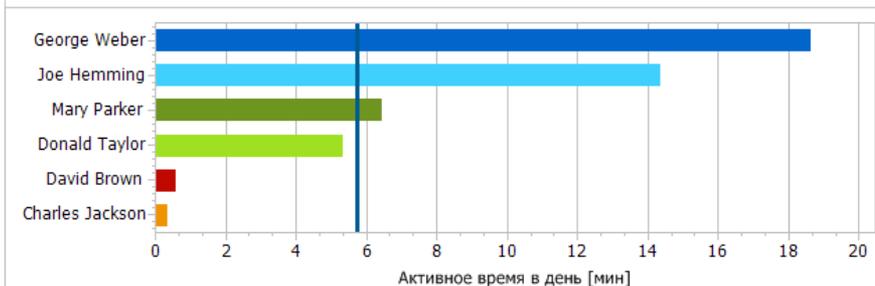


Job search - Самые активные пользователи



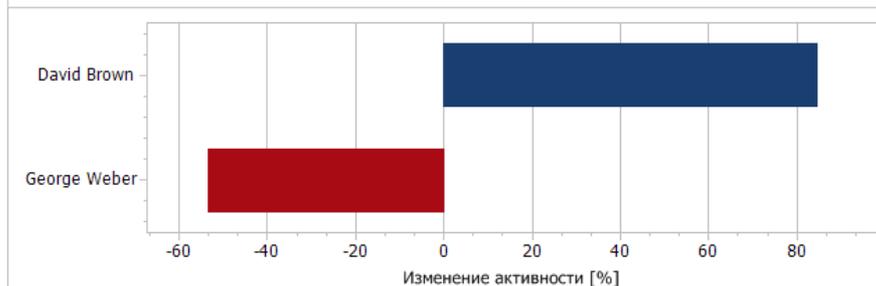
Среднее значение: 06 мин 17 сек

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)

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



ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ SUPERVISOR)



› Web-контроль



› Контроль приложений



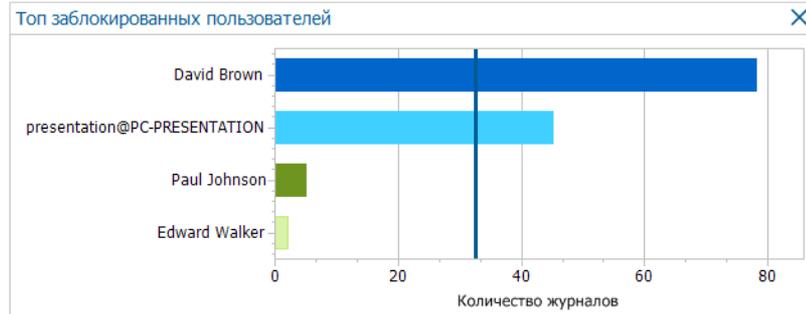
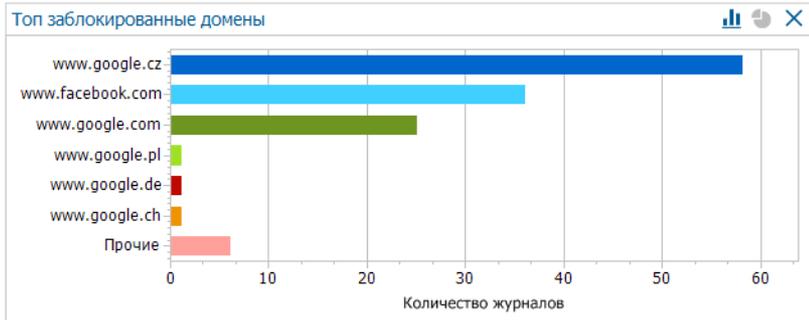
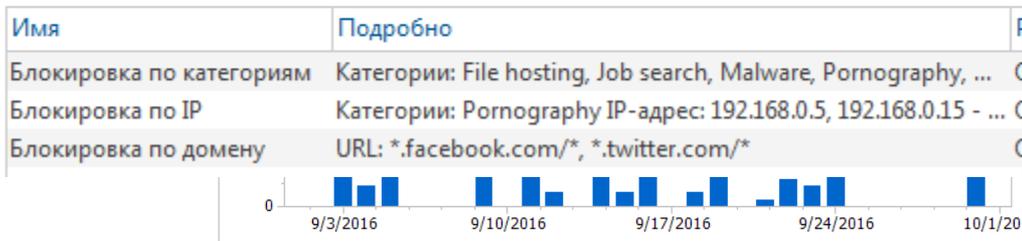
› Контроль печати

ОФИСНЫЙ КОНТРОЛЬ (WEB-КОНТРОЛЬ)



Действие по умолчанию: Разрешено

Добавить правило



ОФИСНЫЙ КОНТРОЛЬ (КОНТРОЛЬ ПРИЛОЖЕНИЙ)



Новое правило

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

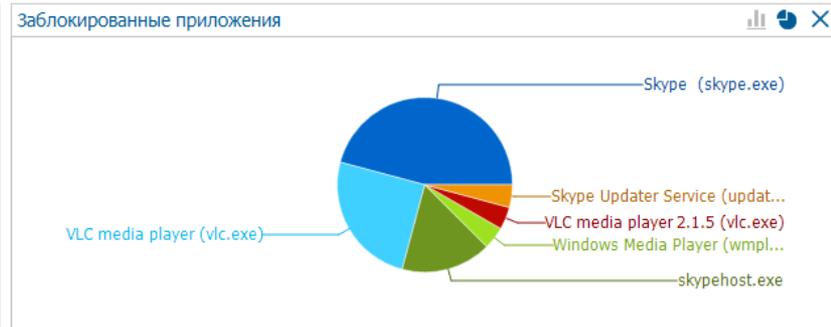
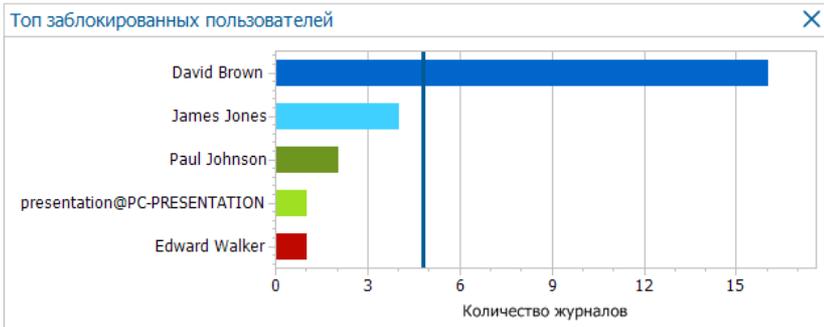
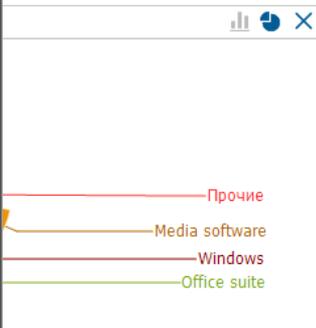
Выберите категорию

Имя:

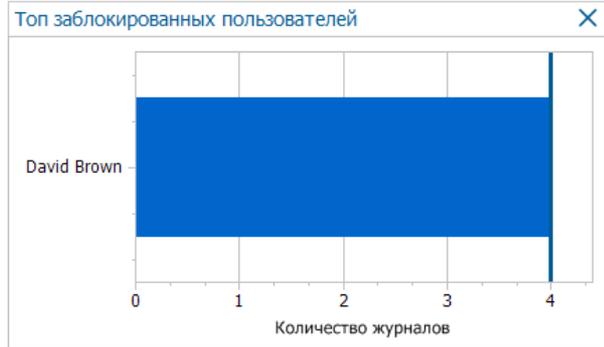
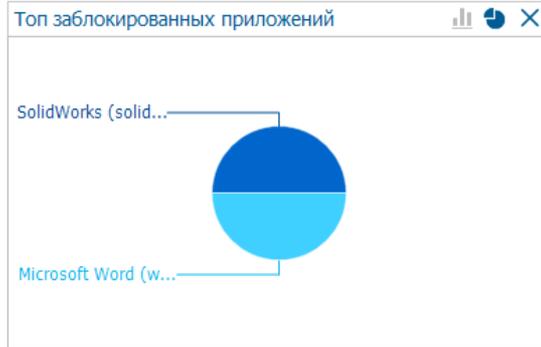
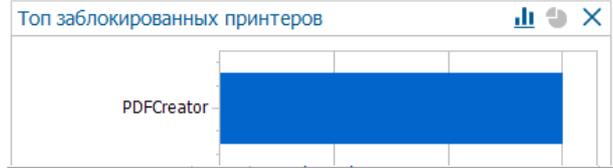
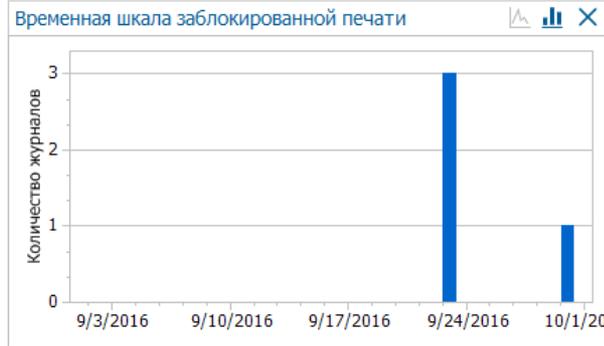
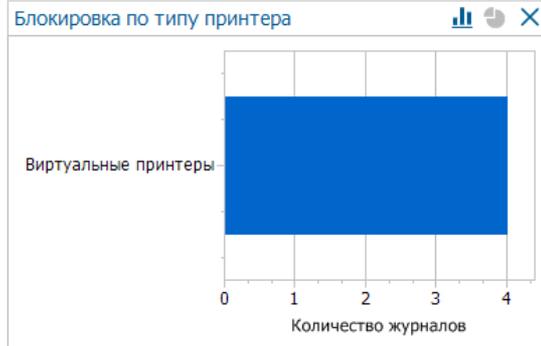
Путь к программе:

Область действия правила: Везде

Назад Далее Отменить



ОФИСНЫЙ КОНТРОЛЬ (КОНТРОЛЬ ПЕЧАТИ)



Состояние квот

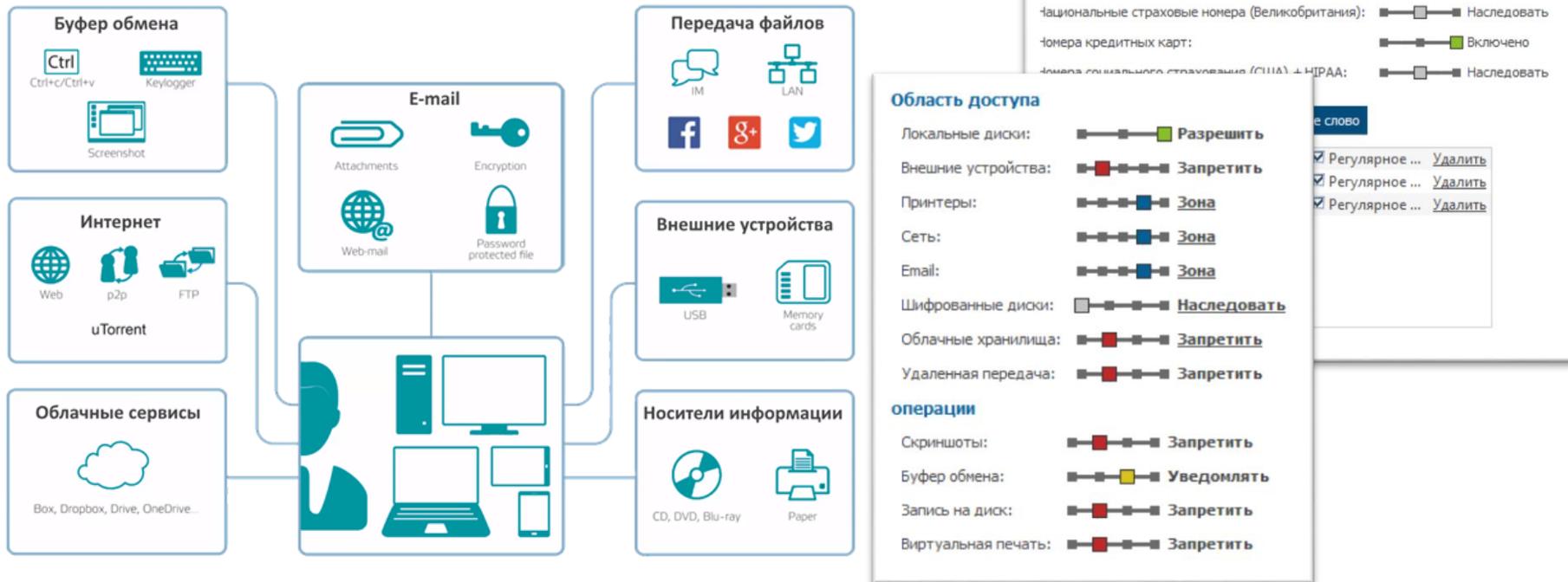
Текущее состояние квот для выбранных пользователей/группы

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 X

OK

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (МОДУЛЬ DLP)



ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (МОДУЛЬ DLP)

› ПРАВИЛА ПРИЛОЖЕНИЙ

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

› ПРАВИЛА ПО ПУТИ

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

› ВЕБ ПРАВИЛА

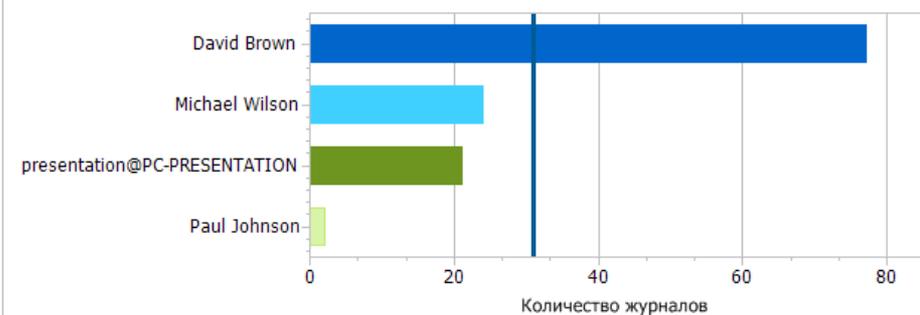
Веб-правила могут использоваться для установки меток на файлы, загруженные с определенных доменов или доменов из определенной категории

› КОНТЕНТНЫЕ ПРАВИЛА

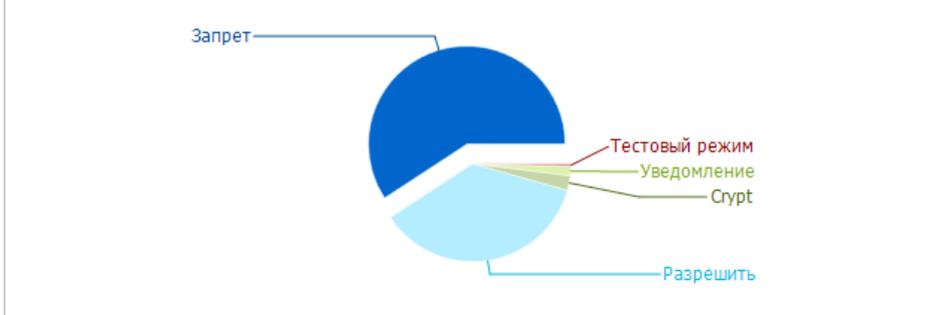
Все файлы, содержащие определенный контент, будут автоматически получать необходимую метку. (раз в день, два дня, неделю, месяц)

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (МОДУЛЬ DLP)

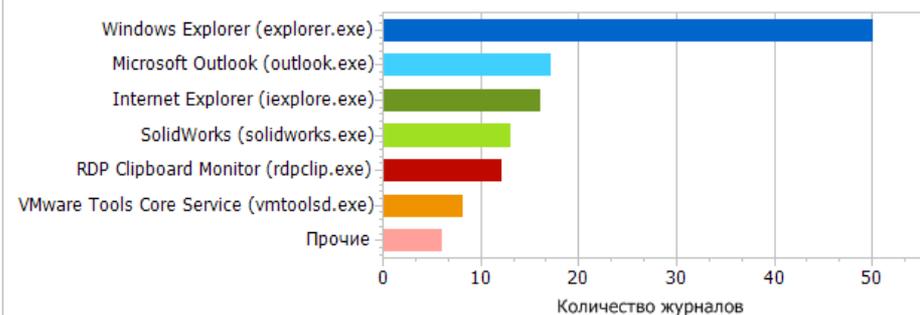
Топ пользователей



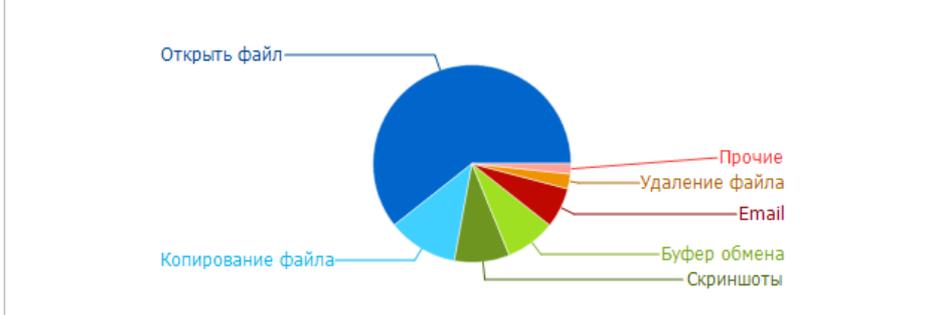
Топ действий



Наиболее активные приложения



Топ операций



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 приложений пользователями 4
- Auditor - Приложения - Наиболее часто используемые приложения 5
- Auditor - Приложения - Самые активные пользователи 5
- Auditor - Электронная почта - Наиболее активные пользователи 5



Загрузка файла

- Google Chrome
- Договор.txt
- https://nofile.io/

Загрузка файла **Договор.txt** для отправки защищенные данные (категория: Супер Секретно) заблокирована.

Это действие противоречит политике безопасности.

Microsoft Outlook

test

@ skuznecov@esetnod32.ru

Нельзя отправлять это электронное письмо

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

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] (12.0)

АНАЛИЗ РЕЗУЛЬТАТОВ WEBSAFETICA

DATA SECURITY >

Incidents per day  ▲ 5%

TOP USERS WITH INCIDENT >

TOP DATAFLOW CHANNELS >



Rebekah Rice:	38
Eva Bailey:	24
Nikki Wilkinson:	18
Don Gonzalez:	11
Carl Mooney:	8



0

Regulatory compliance: suspicious file uploads



12

Users with security incidents



PRODUCTIVITY >

82 %  ▲ 81%

TOP UNPRODUCTIVE USERS >

USERS ACTIVITIES >



Rebekah Rice:	8 h 44 min 31 s
Eva Bailey:	5 h 30 min 59 s
Nikki Wilkinson:	2 h 12 min 22 s
Devin Franco:	1 h 6 min 0 s
Erika Vargas:	1 h 3 min 19 s



4

Users looking for job



47.0 %

Of online time is unproductive



IT UTILIZATION >

48 %  ▼ 11%

TOP INACTIVE COMPUTERS >

COMPUTERS ACTIVITIES >



PC-Pearson:	15 days 9 h 2 min 2...
PC-Orozco:	9 days 16 h 47 min ...
PC-Sweeney:	8 days 2 h 22 min 1...
PC-Jackson:	5 days 12 h 16 min ...
PC-Ortega:	4 days 1 h 1 s



1397 h 50 min

Computer inactivity time



11

Printed pages



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА



safetico

БЫСТРОЕ ВНЕДРЕНИЕ

Контекстный фильтр

В четыре шага

› Любые типы файлов

› Независимость от языка документа

› Независимость от кодировок

› Не требуется составление словарей

› Меньшая ресурсоёмкость

› Меньше ложных срабатываний

› Мгновенный результат

› Анализ – 1 неделя

› Установка – 2 недели

› Обучение (входит в остальные этапы)

› Настройка – 4 недели

РЕЗУЛЬТАТЫ ВНЕДРЕНИЯ

eset ОФИСНЫЙ КОНТРОЛЬ И DLP

safetica

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



safetica

ЛИЦЕНЗИРОВАНИЕ И ЦЕНЫ



› АУДИТОР

Аудитор

1 572 РУБЛЕЙ В ГОД ЗА 1 РАБОЧУЮ СТАНЦИЮ



› ОФИСНЫЙ КОНТРОЛЬ

Аудитор + Супервайзер

2 271 РУБЛЕЙ В ГОД ЗА 1 РАБОЧУЮ СТАНЦИЮ



› FULL DLP

Full DLP (Аудитор + Супервайзер + DLP)

3 493 РУБЛЕЙ В ГОД ЗА 1 РАБОЧУЮ СТАНЦИЮ

- Лицензия на один, два или три года (с даты выписки, от 10 узлов)
- По числу компьютеров с установленным Safetica Endpoint Client
- Серверные компоненты не подлежат лицензированию



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА



safetica

ЛИЦЕНЗИРОВАНИЕ И ЦЕНЫ

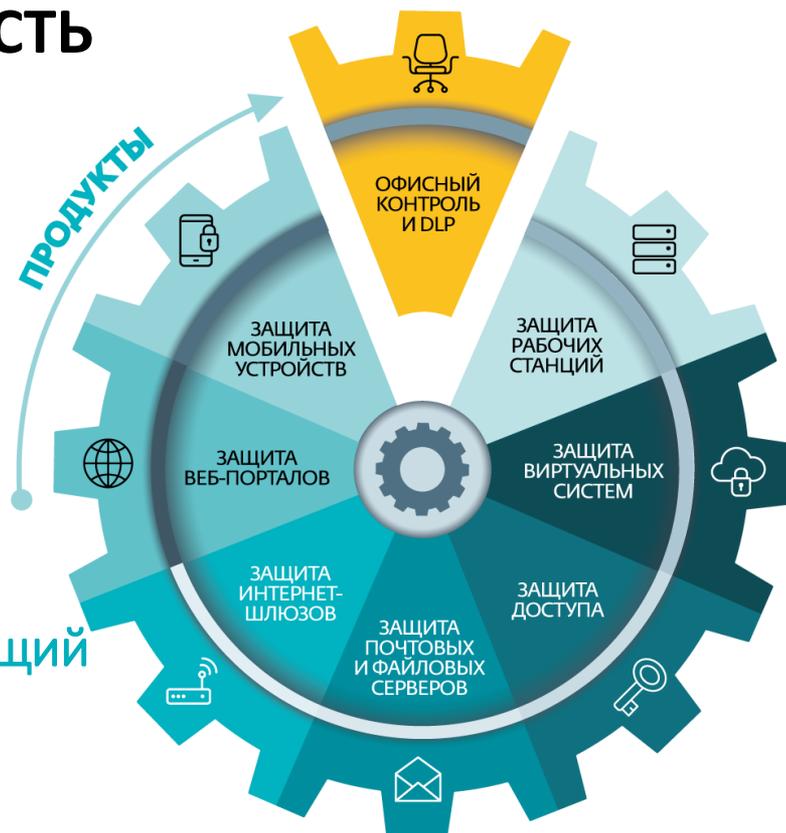
- ✓ Продление на 1 год: скидка 20%
- ✓ Миграция (с аналогичного продукта конкурента): скидка 20%
- ✓ Отраслевая скидка для образования: 50%
- ✓ Отраслевая скидка для медицины: 30%

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

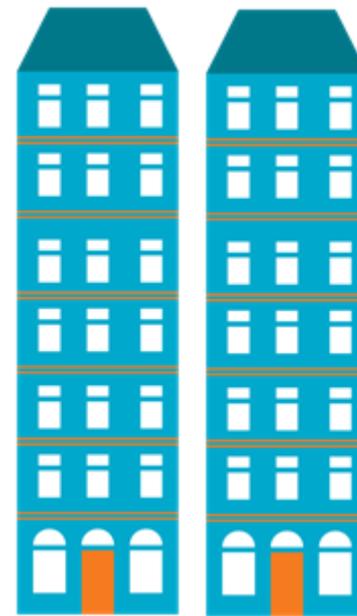
МАЛЫЙ БИЗНЕС



СРЕДНИЙ БИЗНЕС



КРУПНЫЙ БИЗНЕС





safetica - полнота, гибкость и удобство

✓ 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

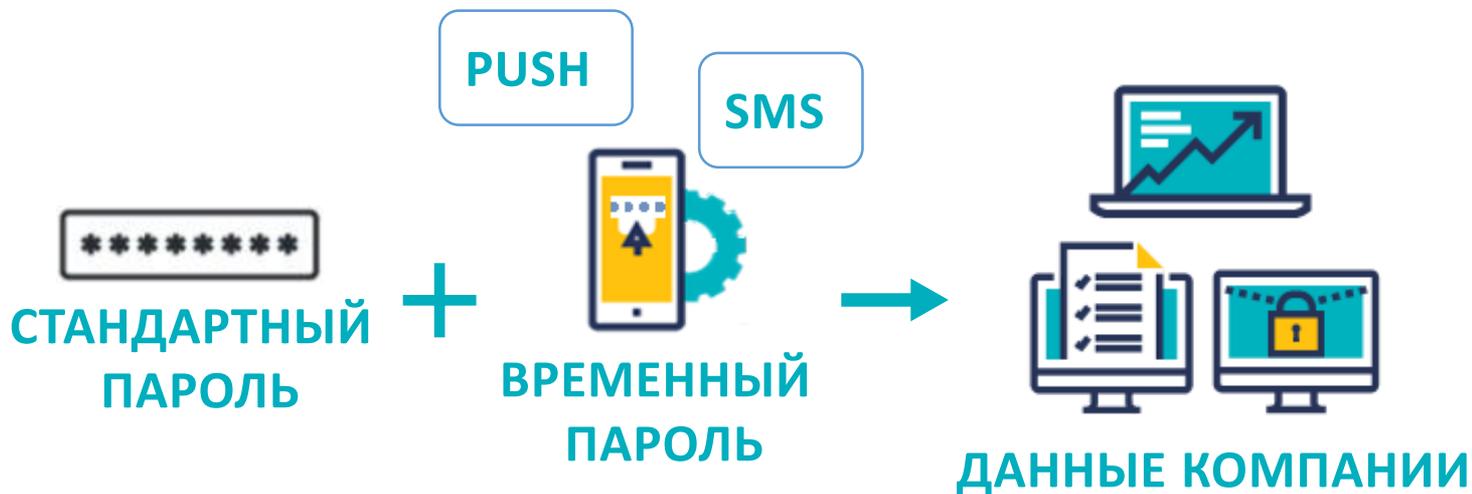
✓ БЕЗ ДОПОЛНИТЕЛЬНЫХ ВЛОЖЕНИЙ

- Стоимость проекта = стоимость лицензии

✓ ПРОСТОЕ ЛИЦЕНЗИРОВАНИЕ

- Аудитор; Аудитор + Супервизор; Full DLP (Аудитор + Супервизор + DLP)

ESET Secure Authentication



- Уникальные пароли при каждом подключении для предотвращения утечки конфиденциальных данных
- Двухфакторный разовый пароль аутентификации (2FA OTP) — решение на базе мобильных устройств
- Только программное обеспечение — нет необходимости в дополнительном управлении аппаратными устройствами
- Никаких дополнительных затрат на аппаратное обеспечение — интегрируется в существующую инфраструктуру

ВАРИАНТЫ ИНТЕГРАЦИИ

ОС Microsoft Windows, Linux, macOS

Поддержка MS AD Federation Services (AD FS 3.0)

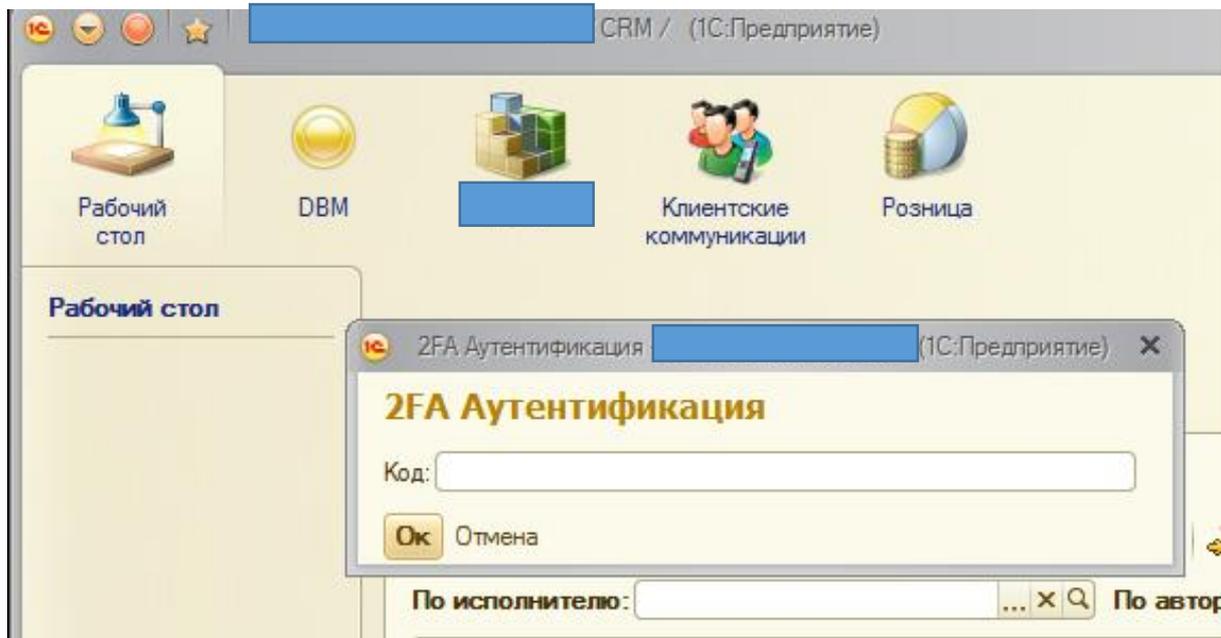
Exchange, OWA, SharePoint, Dynamics CRM и Remote Desktop

VPN и VDI - интеграция в RADIUS-системы, в том числе: Cisco ASA, VMware Horizon View и Citrix XenApp и др.

API и SDK - для внедрения в собственные системы

ИНТЕГРАЦИЯ С 1С

Разработан шаблон и инструкция



**СПАСИБО
ЗА ВНИМАНИЕ!**

Самойленко Дмитрий
тел: +7 928 044-18-58
e-mail: dsamoylenko@esetnod32.ru



www.vkontakte.ru/nod32



www.facebook.com/ESETNOD32Russia



www.club.esetnod32.ru



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

