ОФИСНЫЙ КОНТРОЛЬ И DLP SAFETICA

Дмитрий Самойленко
Руководитель представительства
ESET на территории ЮФО, СКФО

СОДЕРЖАНИЕ

СТАТИСТИКА ИНСТИТУТА AV-TEST

ИЗВЕСТНЫЕ УГРОЗЫ

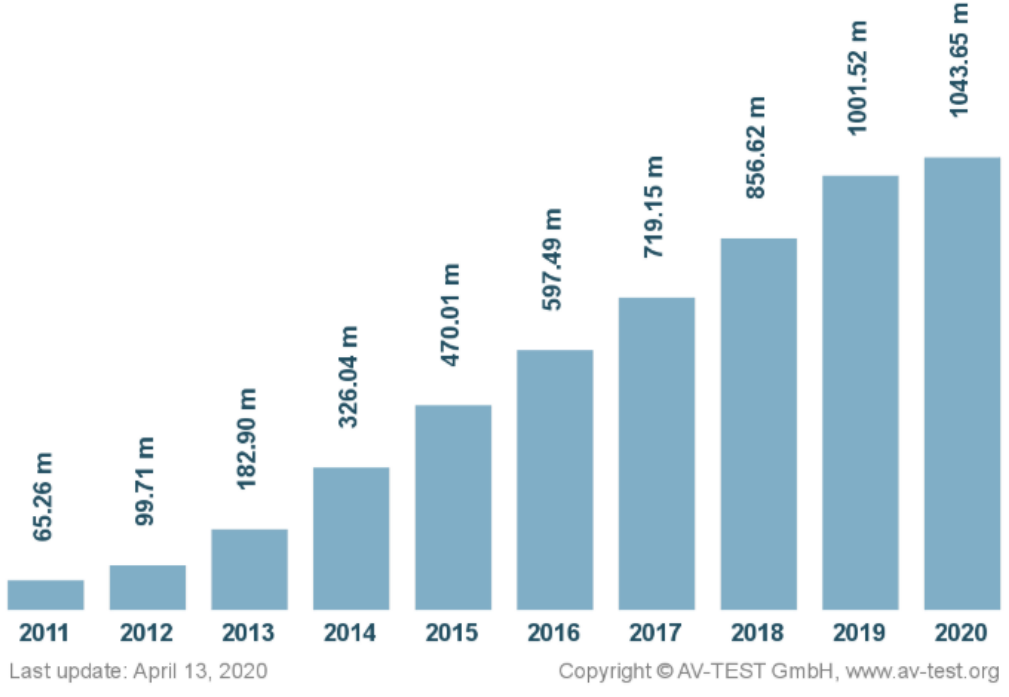
- **390 000 шт. в день**

  Новых образцов

  вредоносных программ каждый день

- **Новые способы**

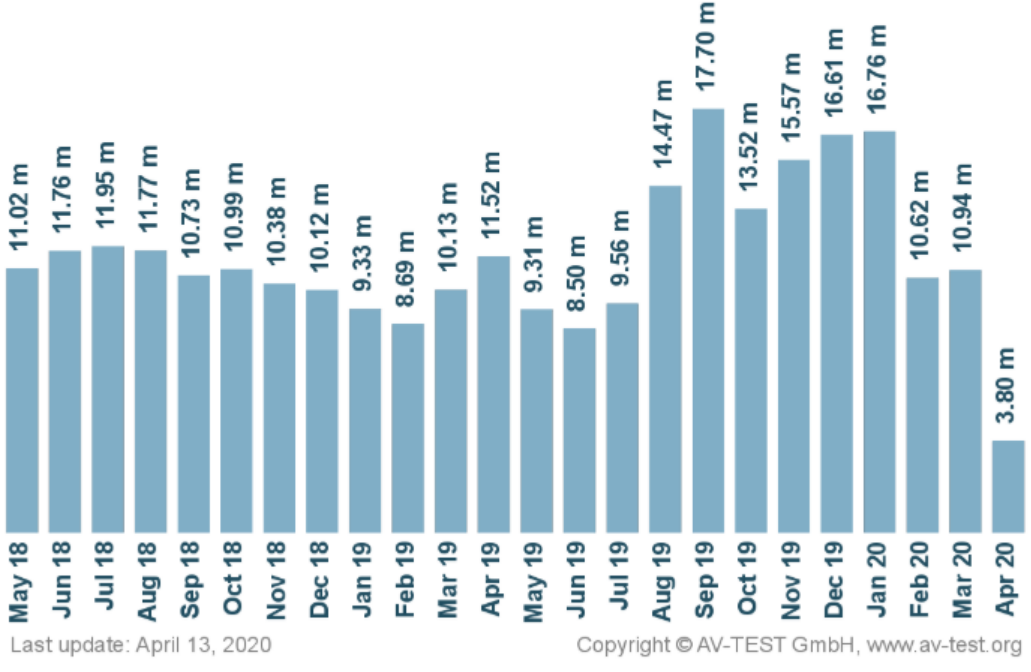
  Новые способы обхода обнаружения



Источник: av-test.org, статистика вредоносных программ на 13 Апреля 2020 г.

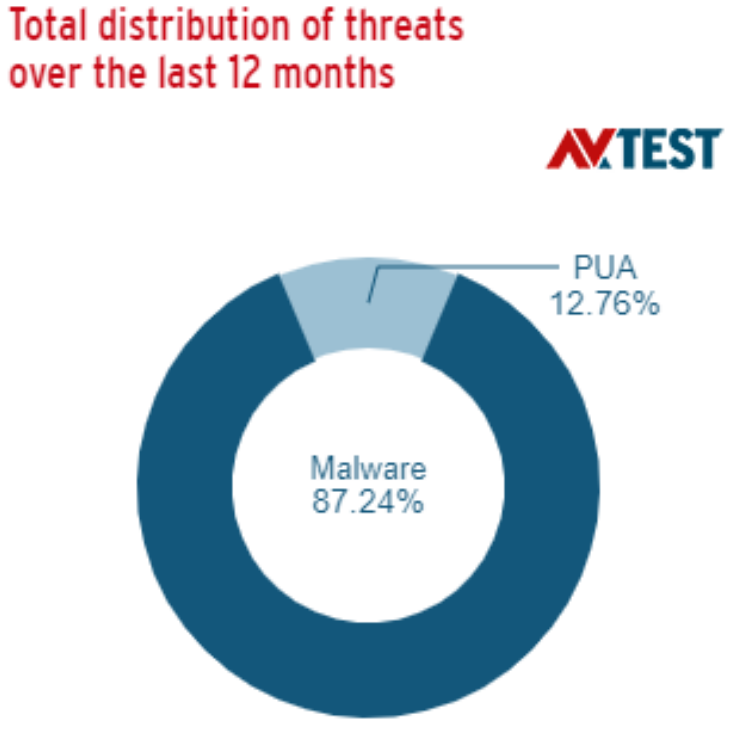
УГРОЗЫ ПРОГРЕССИРУЮТ И СТАНОВЯТСЯ СЛОЖНЕЕ

Новые угрозы



Источник: av-test.org, статистика вредоносных программ на 13 Апреля 2020 г.

РАСПРЕДЕЛЕНИЕ УГРОЗ ЗА 12 МЕСЯЦЕВ



Источник: av-test.org, статистика вредоносных программ на 13 Апреля 2020 г

УТЕЧКА ДАННЫХ
ЭТО РЕАЛЬНОСТЬ!

Человеческий фактор

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

** PwC, 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

ESET Russia, 2017, 750 респондентов

КАК ОБЕСПЕЧИТЬ ЗАЩИТУ ОТ ВНУТРЕННИХ УГРОЗ?

ESET АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ЧЕЛОВЕЧЕСКИЙ ФАКТОР

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

УТЕЧКА ДАННЫХ
КАК ЭТО ПРОИСХОДИТ?

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

РЕШЕНИЕ
ОФИСНЫЙ КОНТРОЛЬ И DLP SAFETICA

- ST-Чешская компания, основана в 2009 году
- DLP решение для любого типа бизнеса - по версии Gartner
- Входит в ESET Technology Alliance с 2016 года

eset АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

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

КОНТЕНТНЫЙ ФИЛЬТР

АРХИТЕКТУРА РЕШЕНИЯ SAFETICA

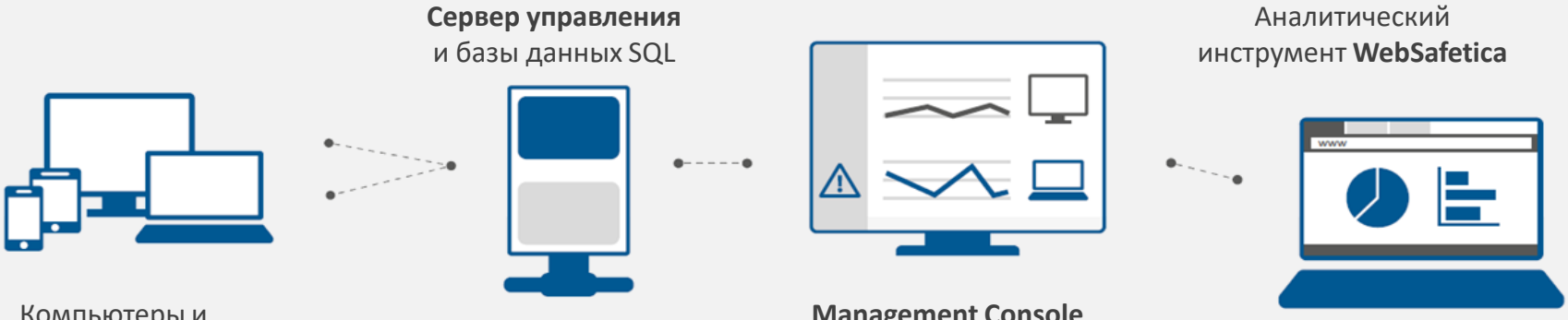
В четыре шага

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

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 7 SP1 и выше; MAC OS 10.10 и более новые* (*Auditor)

Сервер
Процессор: четырёхядерный 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 2016 Express включена в установочный пакет Safetica

КОМПЛЕКСНОЕ РЕШЕНИЕ
SAFETICA

AUDITOR

РЕГИСТРАЦИЯ АКТИВНОСТИ СОТРУДНИКОВ

SUPERVISOR

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ БИЗНЕС-ПРОЦЕССОВ КОМПАНИИ

DLP

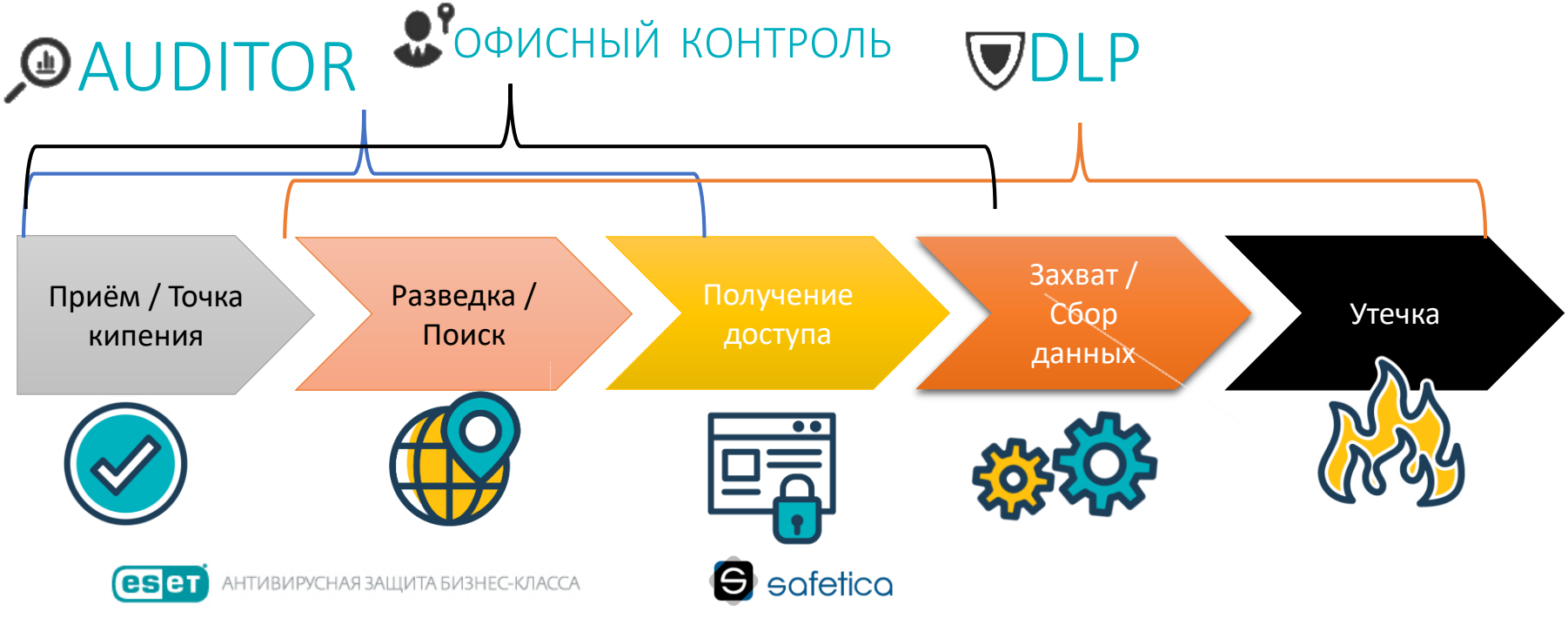
ПРЕДОТВРАЩЕНИЕ УТЕЧКИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ КОМПАНИИ

SAFETICA – КОМПЛЕКСНОЕ РЕШЕНИЕ!

61% сотрудников

*злоупотребляет доступом к конфиденциальным данным компании**

** Ponemon Institute, 2016*



ОФИСНЫЙ КОНТРОЛЬ
(МОДУЛЬ AUDITOR)

АУДИТ ЧУВСТВИТЕЛЬНЫХ ДАННЫХ КОМПАНИИ

ПРЕДСТАВЛЕНИЕ О ТОМ, ЧТО ПРОИСХОДИТ В КОМПАНИИ

УМЕНЬШЕНИЕ РАСХОДОВ НА ПЕРСОНАЛ

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ СОТРУДНИКОВ

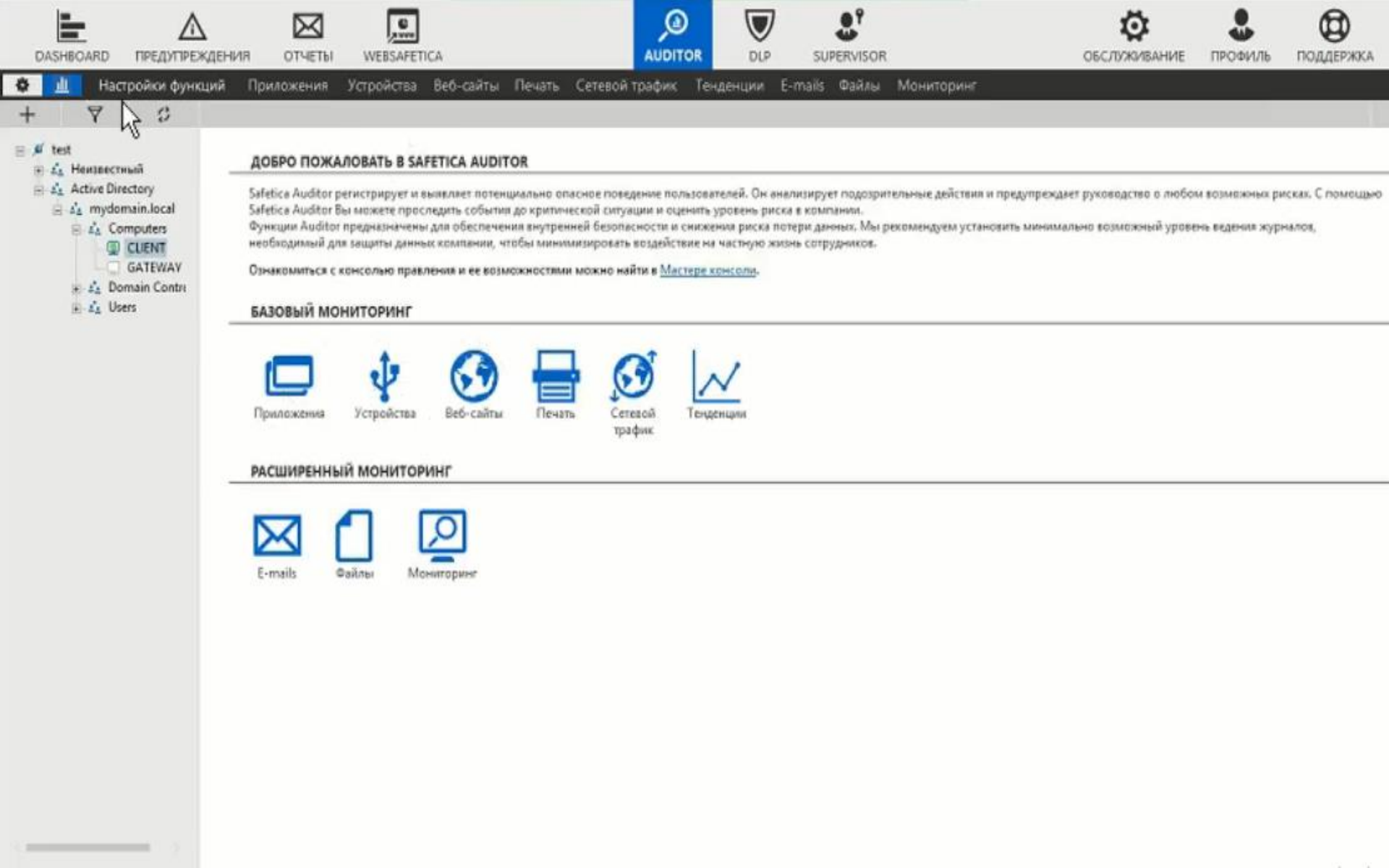
СОКРАЩЕНИЕ РАСХОДОВ КОМПАНИИ НА ОФИСНЫЕ НУЖДЫ

СРАВНЕНИЕ РАБОТЫ СОТРУДНИКОВ

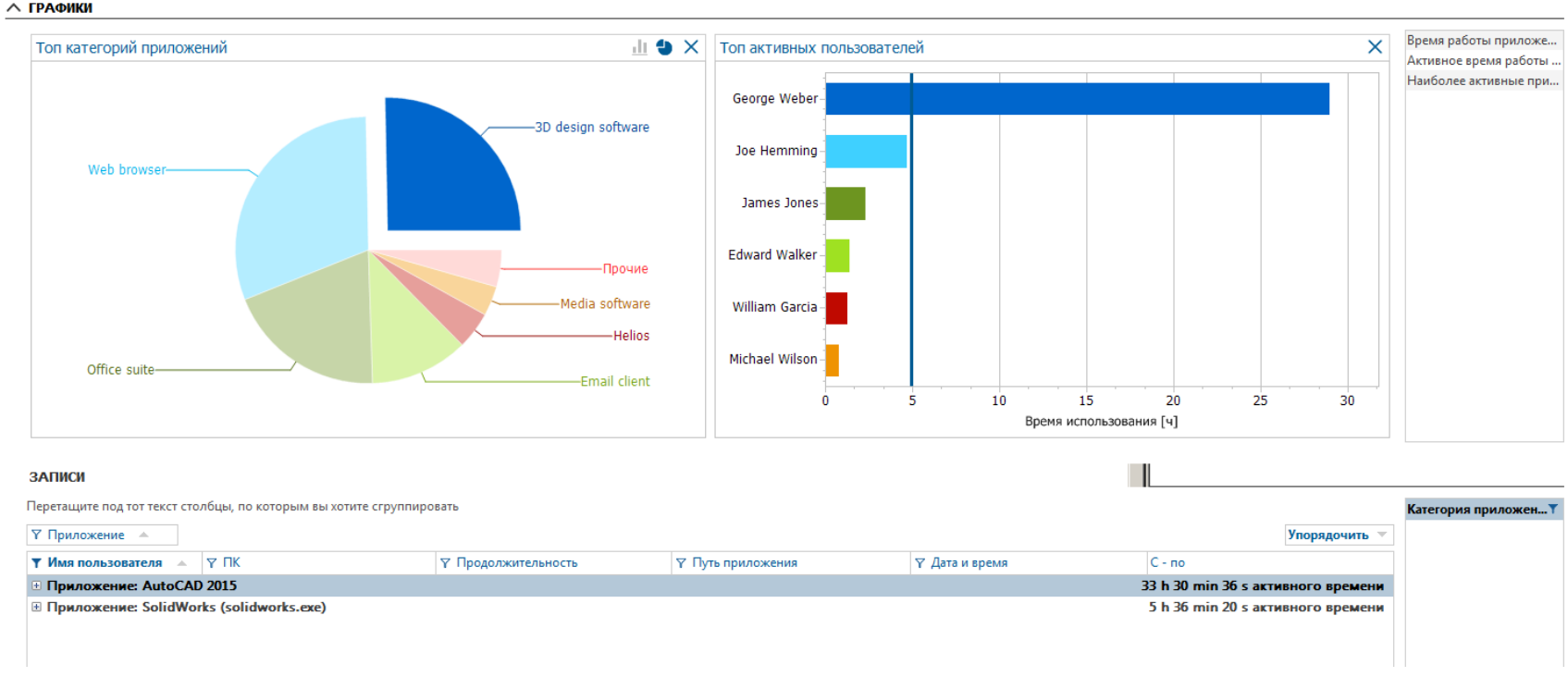
СОБЛЮДЕНИЕ ПОЛИТИК БЕЗОПАСНОСТИ

ОКУПАЕМОСТЬ ВНЕДРЕНИЯ

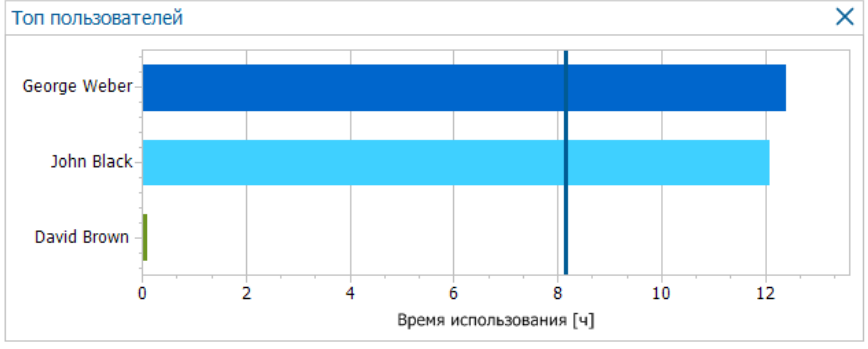
ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ ПО

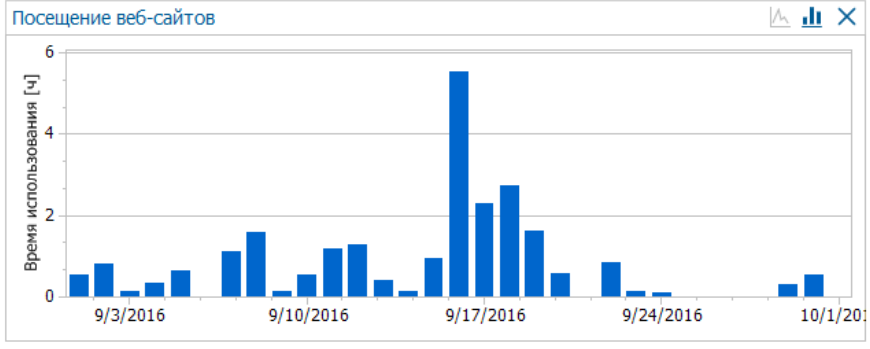

DASHBOARD
ПРЕДУПРЕЖДЕНИЯ
ОТЧЕТЫ
WEBSAFETICA
AUDITOR
DLP
SUPERVISOR
ОБСЛУЖИВАНИЕ
ПРОФИЛЬ
ПОДДЕРЖКА
Настройки функций
Приложения
Устройства
Веб-сайты
Печать
Сетевой трафик
Тенденции
E-mails
Файлы
Мониторинг
test
Неизвестный
Active Directory
mydomain.local
Computers
CLIENT
GATEWAY
Domain Contr
Users
ДОБРО ПОЖАЛОВАТЬ В SAFETICA AUDITOR
Safetica Auditor регистрирует и выявляет потенциально опасное поведение пользователей. Он анализирует подозрительные действия и предупреждает руководство о любом возможных рисках. С помощью Safetica Auditor Вы можете проследить события до критической ситуации и оценить уровень риска в компании.
Функции Auditor предназначены для обеспечения внутренней безопасности и снижения риска потери данных. Мы рекомендуем установить минимально возможный уровень ведения журналов, необходимый для защиты данных компании, чтобы минимизировать воздействие на частную жизнь сотрудников.
Ознакомиться с консолью правления и ее возможностями можно найти в Мастере консоли.
БАЗОВЫЙ МОНИТОРИНГ
Приложения
Устройства
Веб-сайты
Печать
Сетевой трафик
Тенденции
РАСШИРЕННЫЙ МОНИТОРИНГ
E-mails
Файлы
Мониторинг

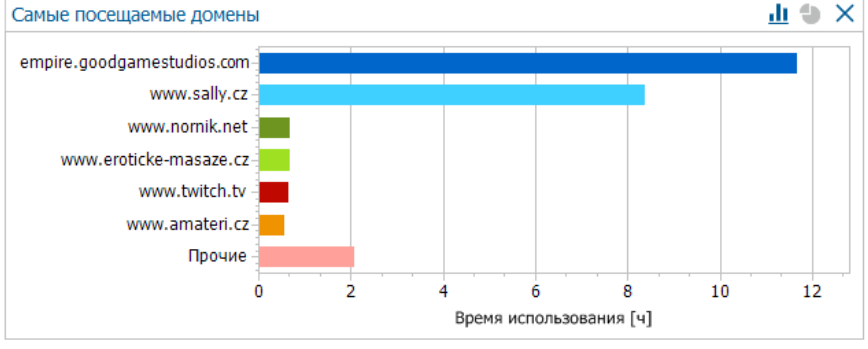
ОФИСНЫЙ КОНТРОЛЬ
(МОДУЛЬ AUDITOR)

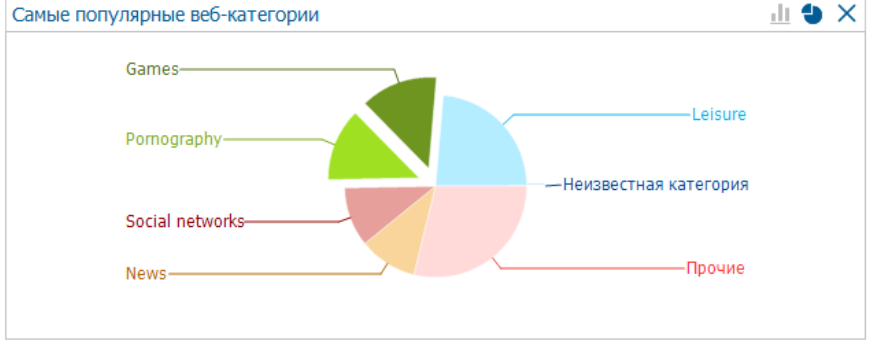


ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ AUDITOR)









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)

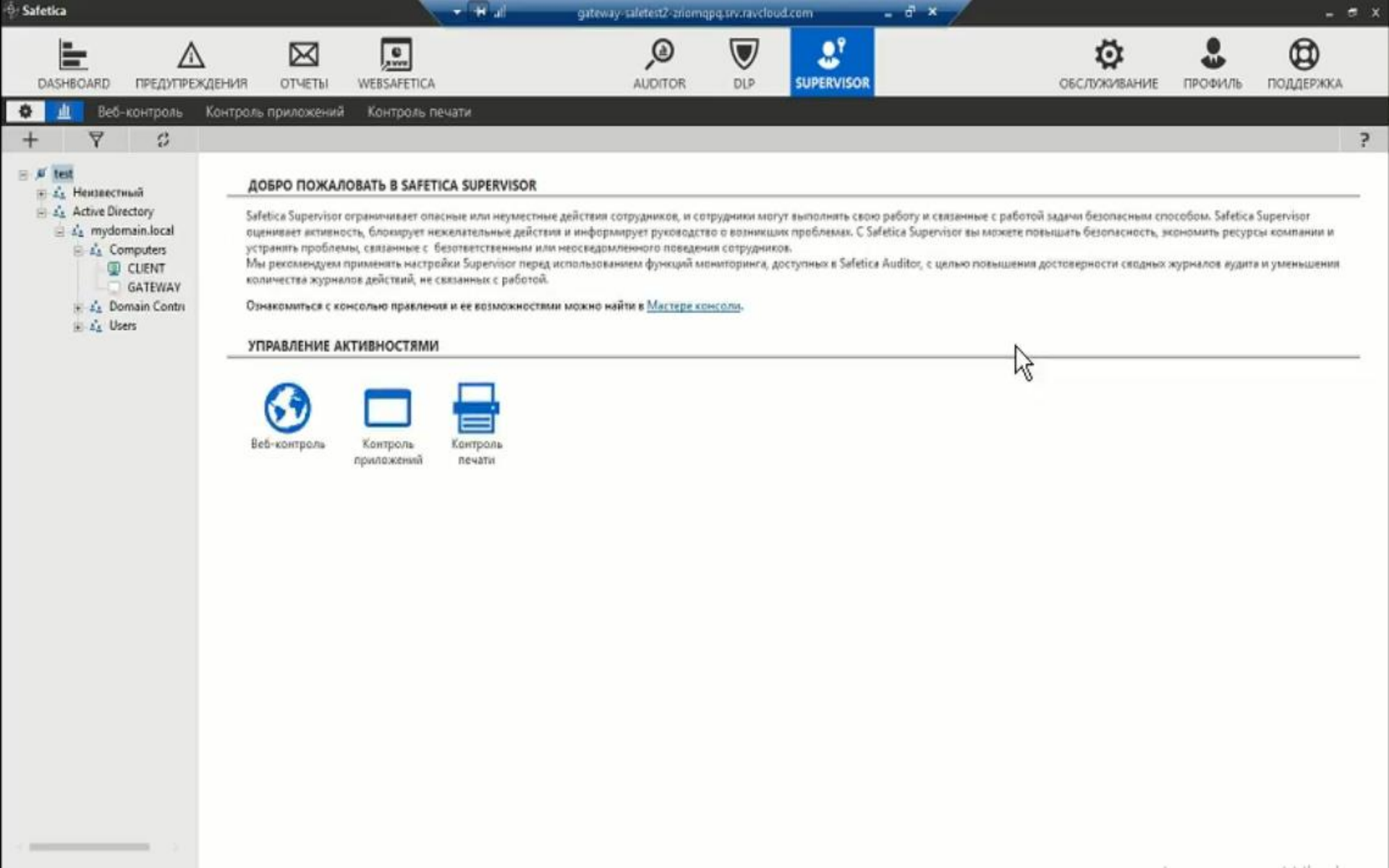
WEB-КОНТРОЛЬ

КОНТРОЛЬ ПРИЛОЖЕНИЙ

КОНТРОЛЬ ПЕЧАТИ

eset АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

safetica

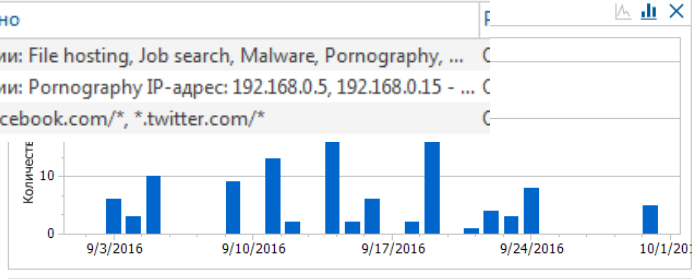

Safetica
gateway-saletest2-zriomqpq.srv.ravcloud.com
DASHBOARD
ПРЕДУПРЕЖДЕНИЯ
ОТЧЕТЫ
WEBSAFETICA
AUDITOR
DLP
SUPERVISOR
ОБСЛУЖИВАНИЕ
ПРОФИЛЬ
ПОДДЕРЖКА
Веб-контроль
Контроль приложений
Контроль печати
test
Неизвестный
Active Directory
mydomain.local
Computers
CLIENT
GATEWAY
Domain Contr
Users
ДОБРО ПОЖАЛОВАТЬ В SAFETICA SUPERVISOR
Safetica Supervisor ограничивает опасные или неуместные действия сотрудников, и сотрудники могут выполнять свою работу и связанные с работой задачи безопасным способом. Safetica Supervisor оценивает активность, блокирует нежелательные действия и информирует руководство о возникших проблемах. С Safetica Supervisor вы можете повышать безопасность, экономить ресурсы компании и устранять проблемы, связанные с безответственным или неосведомленного поведения сотрудников.
Мы рекомендуем применять настройки Supervisor перед использованием функций мониторинга, доступных в Safetica Auditor, с целью повышения достоверности сводных журналов аудита и уменьшения количества журналов действий, не связанных с работой.
Ознакомиться с консолью правления и ее возможностями можно найти в Мастере консоли.
УПРАВЛЕНИЕ АКТИВНОСТЯМИ
Веб-контроль
Контроль приложений
Контроль печати

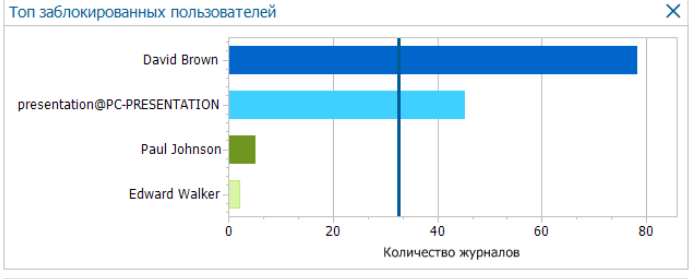
ОФИСНЫЙ КОНТРОЛЬ
(WEB-КОНТРОЛЬ)

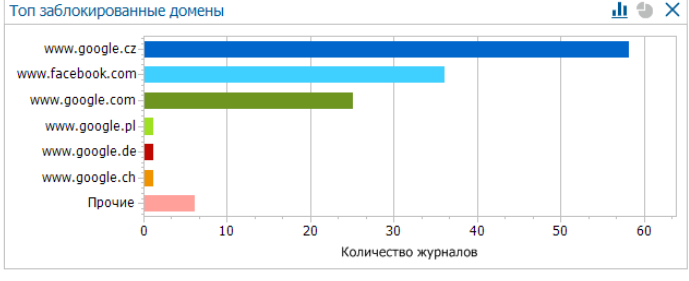
Действие по умолчанию: Разрешено

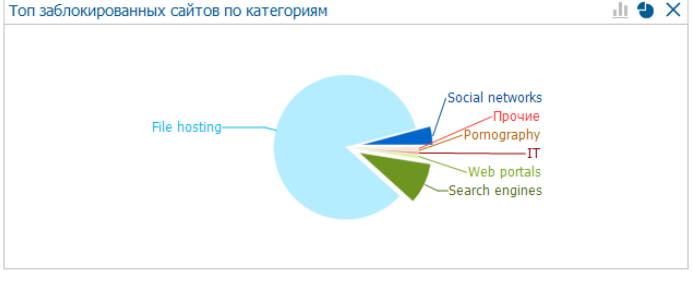
Добавить правило

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

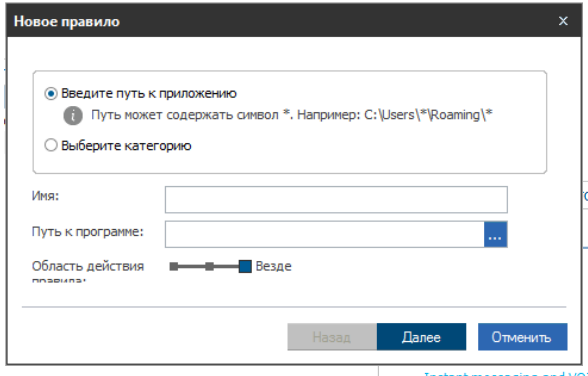


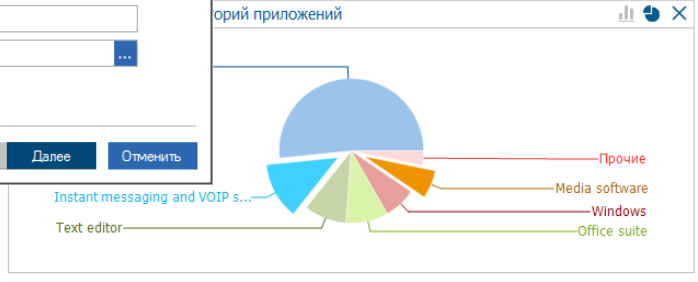


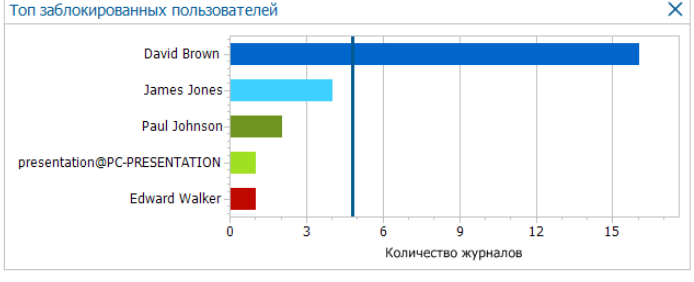


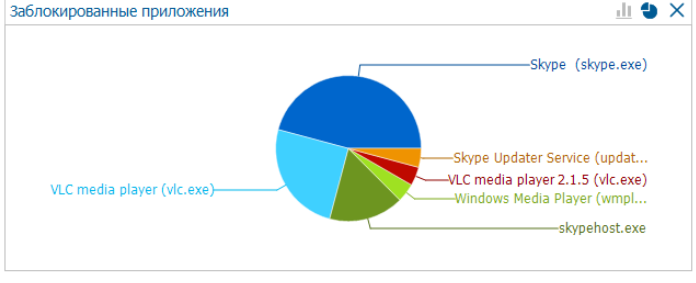


ОФИСНЫЙ КОНТРОЛЬ
(КОНТРОЛЬ ПРИЛОЖЕНИЙ)





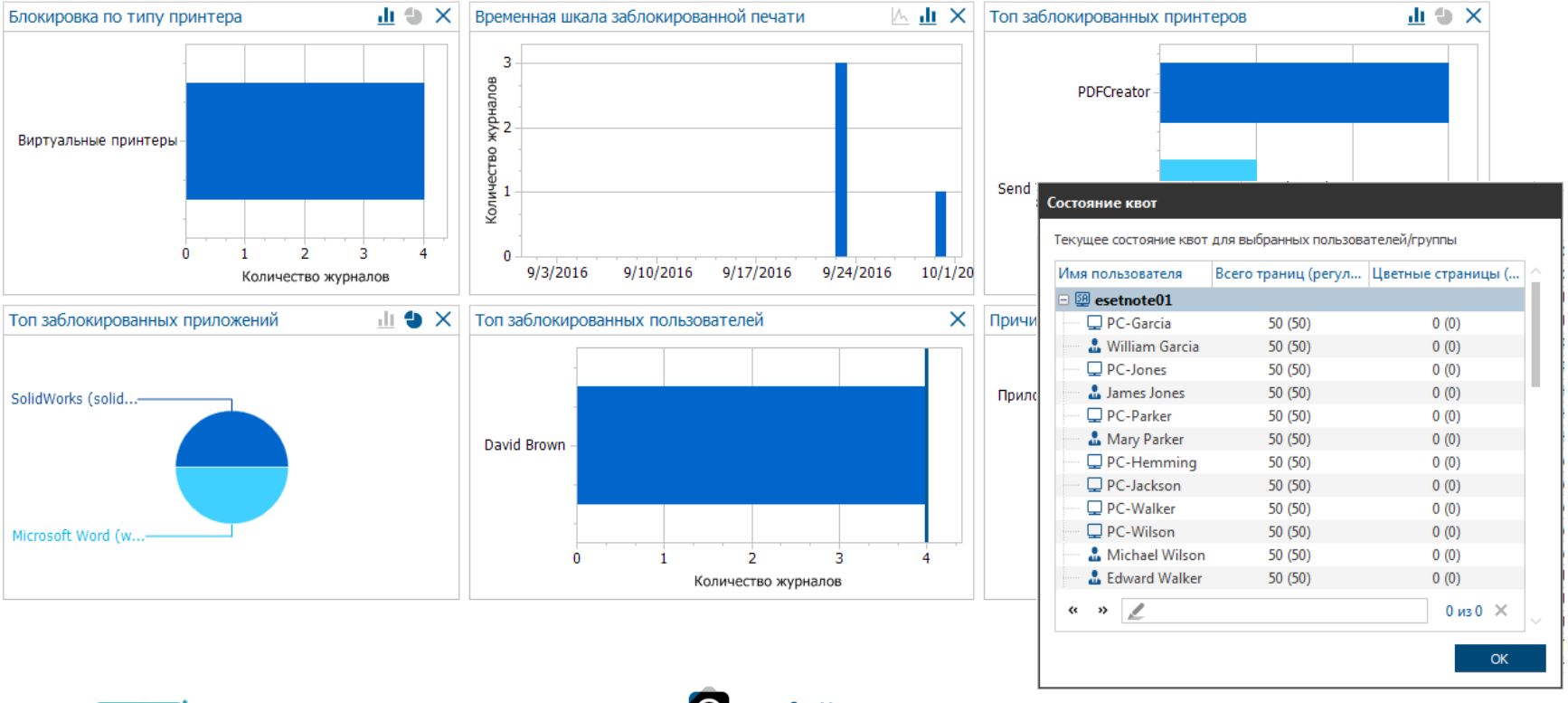




eset АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

safetica

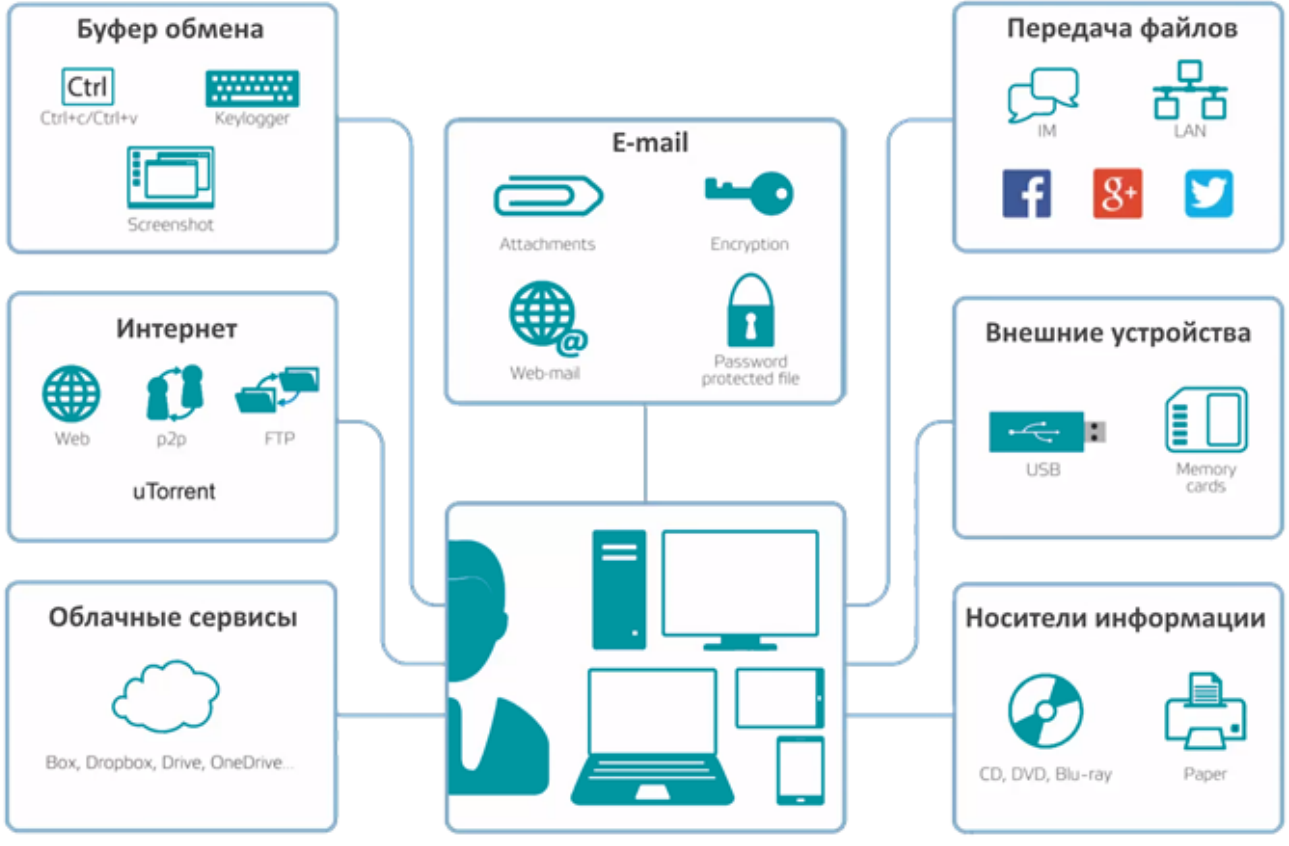
ОФИСНЫЙ КОНТРОЛЬ
(КОНТРОЛЬ ПЕЧАТИ)



ESET АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

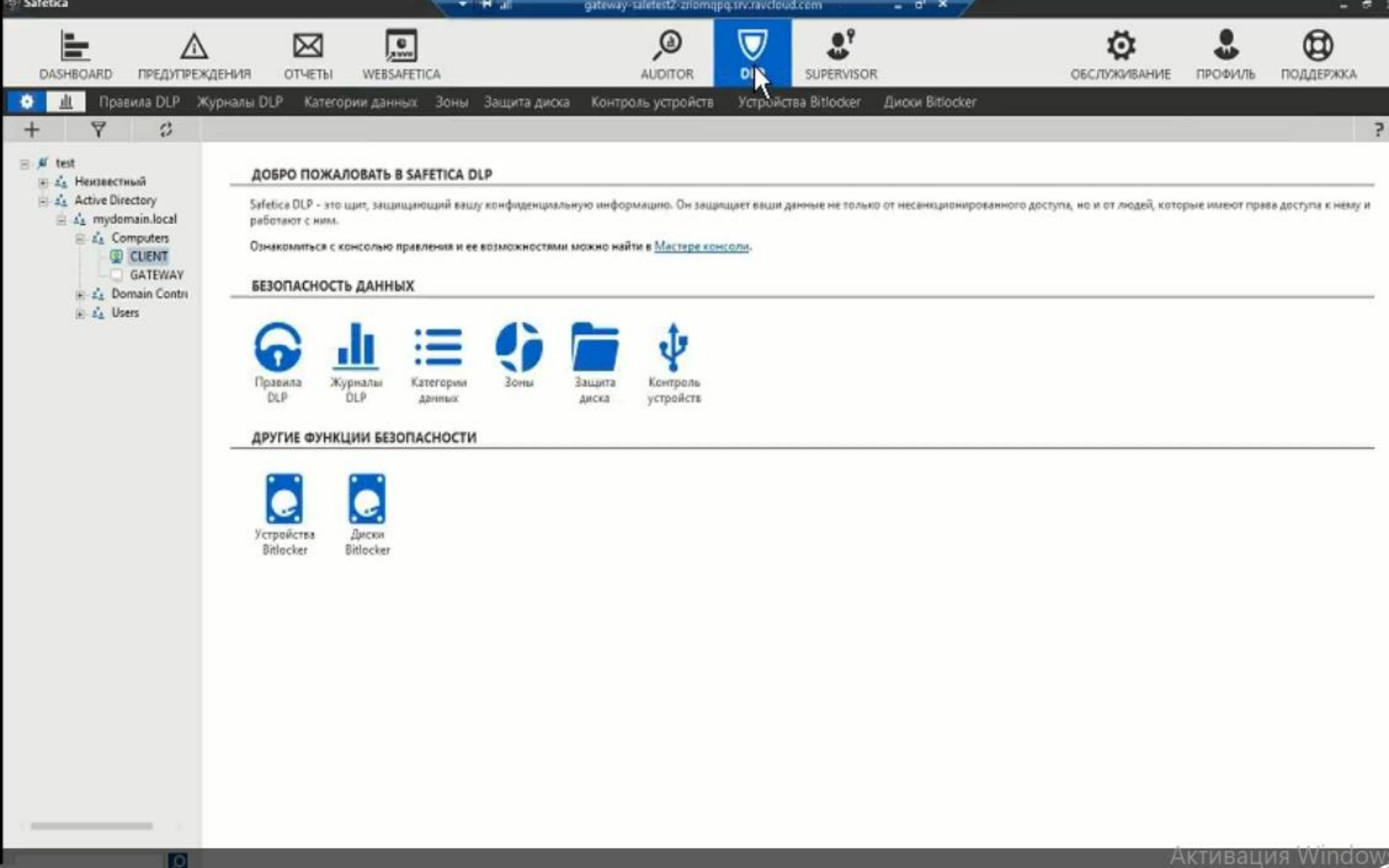
safetica

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (МОДУЛЬ DLP)



eset АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

safetica


DASHBOARD
ПРЕДУПРЕЖДЕНИЯ
ОТЧЕТЫ
WEBSAFETICA
AUDITOR
DLP
SUPERVISOR
ОБСЛУЖИВАНИЕ
ПРОФИЛЬ
ПОДДЕРЖКА
Правила DLP
Журналы DLP
Категории данных
Зоны
Защита диска
Контроль устройств
Устройства Bitlocker
Диски Bitlocker
test
Неизвестный
Active Directory
mydomain.local
Computers
CLIENT
GATEWAY
Domain Contr
Users
ДОБРО ПОЖАЛОВАТЬ В SAFETICA DLP
Safetica DLP - это щит, защищающий вашу конфиденциальную информацию. Он защищает ваши данные не только от несанкционированного доступа, но и от людей, которые имеют права доступа к нему и работают с ним.
Ознакомиться с консолью правления и ее возможностями можно найти в Мастере консоли.
БЕЗОПАСНОСТЬ ДАННЫХ
Правила DLP
Журналы DLP
Категории данных
Зоны
Защита диска
Контроль устройств
ДРУГИЕ ФУНКЦИИ БЕЗОПАСНОСТИ
Устройства Bitlocker
Диски Bitlocker

КОНТЕКСТНЫЙ
ФИЛЬТР

1. ЭФФЕКТИВНО И ПРОСТО
2. БЕЗ ЛОЖНЫХ СРАБАТЫВАНИЙ
3. ЗАЩИЩАЕТ ДОКУМЕНТ ПО РАСШИРЕНИЮ, А НЕ ПО СОДЕРЖИМОМУ

eset АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

safetica

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

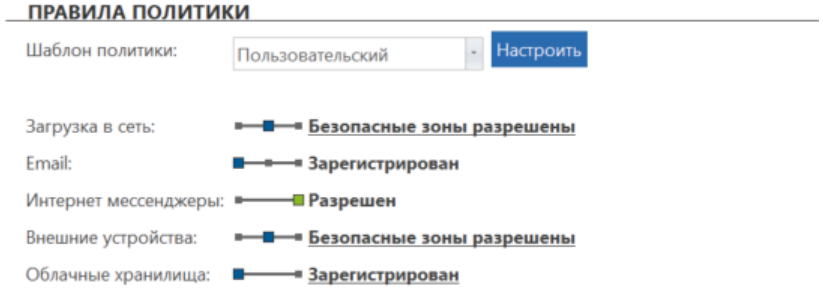
Все файлы, помещенные в определенные папки, будут автоматически получать необходимую метку.

› КОНТЕНТНЫЕ ПРАВИЛА

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

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (КОНТЕНТНЫЙ ФИЛЬТР)

- ЭЛЕКТРОННАЯ ПОЧТА
- МЕССЕНДЖЕРЫ
- ВНЕШНИЕ УСТРОЙСТВА
- ЗАГРУЗКА ФАЙЛОВ В ИНТЕРНЕТ



ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (КОНТЕНТНЫЙ ФИЛЬТР)

› ПРЕДУСТАНОВЛЕННОЕ СОДЕРЖИМОЕ

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

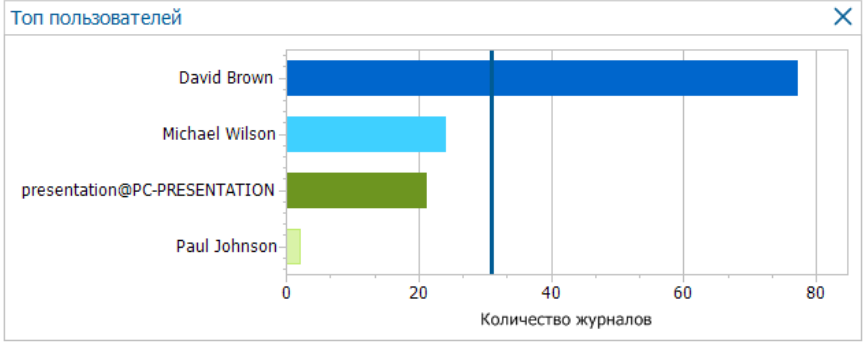
› КЛЮЧЕВЫЕ СЛОВА И РЕГУЛЯРНЫЕ ВЫРАЖЕНИЯ

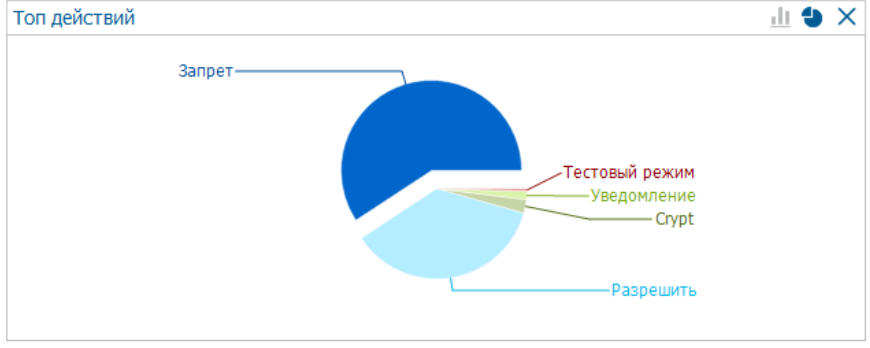
Любые слова и словосочетания, использование регулярных выражений с применением синтаксиса ECMAScript

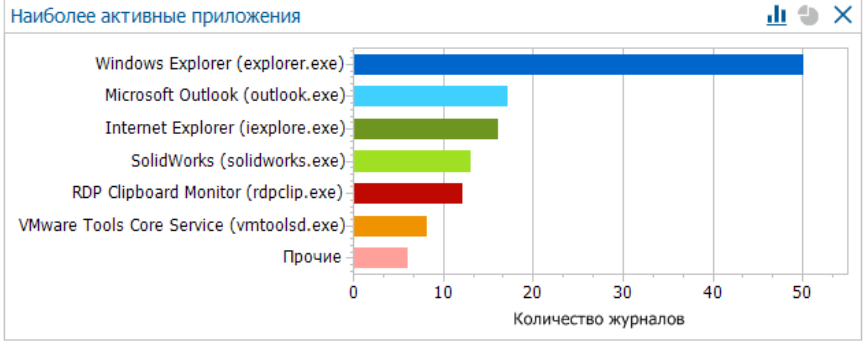
› МЕТАДАННЫЕ СТОРОННИХ КЛАССИФИКАТОРОВ

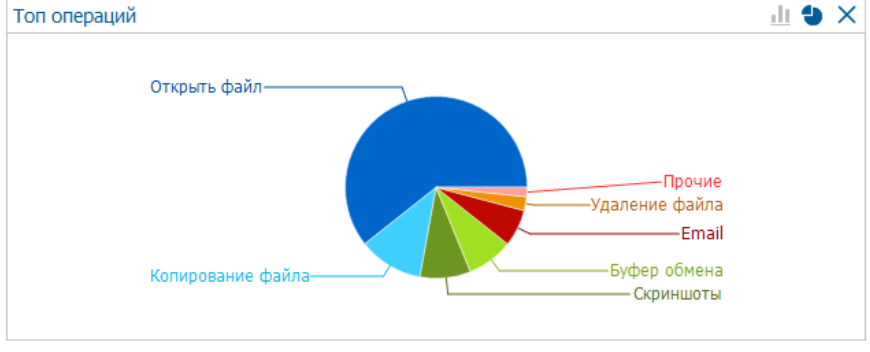
Протестирована поддержка метаданных Microsoft Azure Information Protection, Boldon James, Tukan GREENmod.

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (МОДУЛЬ DLP)





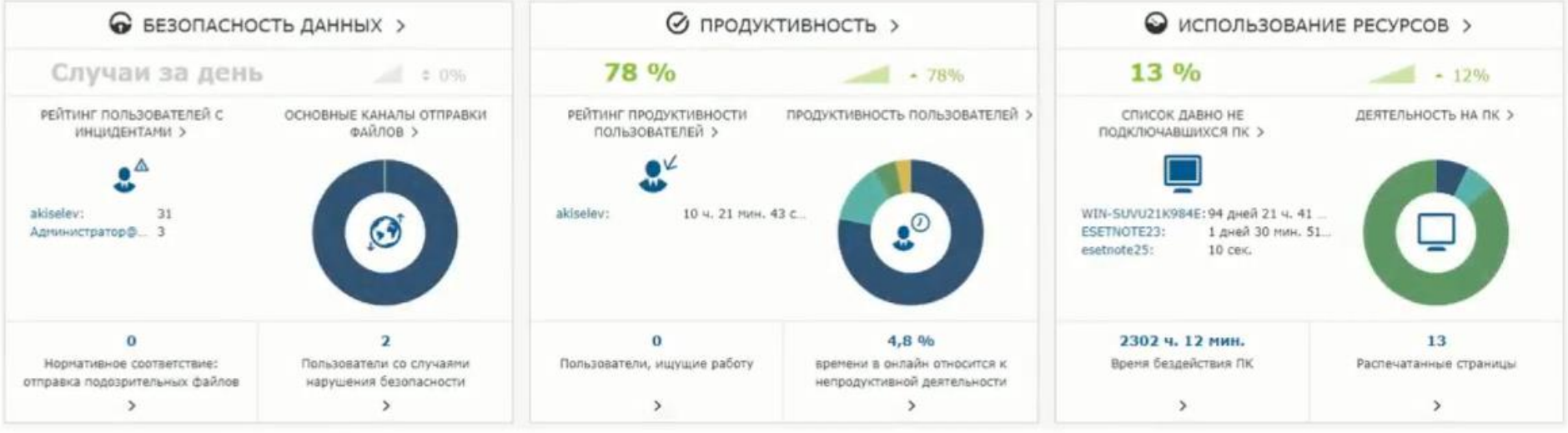




eset АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

safetica

АНАЛИЗ РЕЗУЛЬТАТОВ
WEBSAFETICA

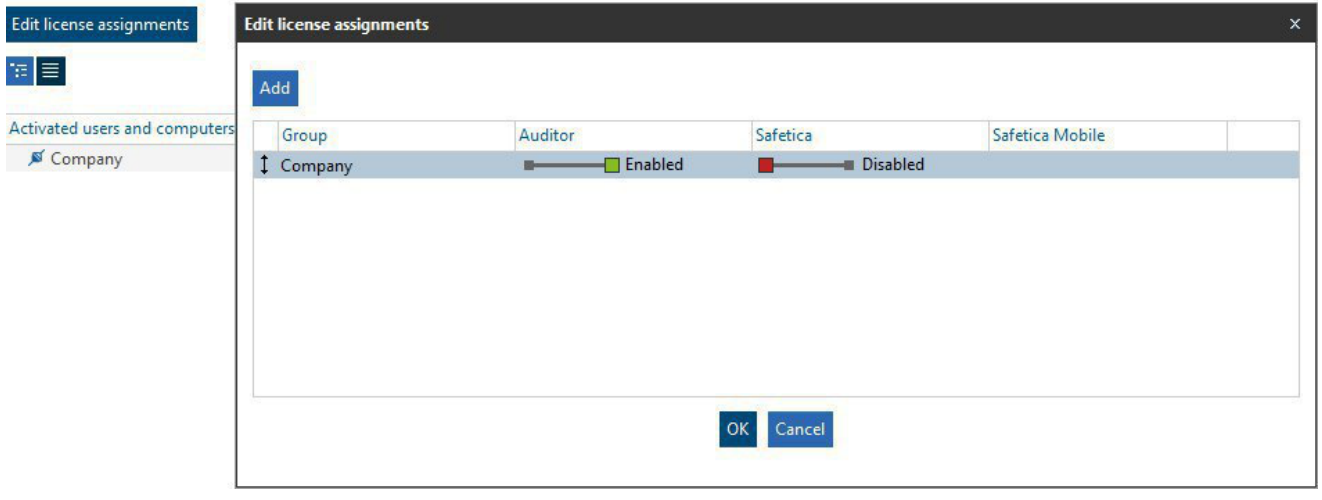


eset АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

safetica

УПРАВЛЕНИЕ ЛИЦЕНЗИЕЙ
РАСПРЕДЕЛЕНИЕ МОДУЛЕЙ

Активируйте необходимые модули

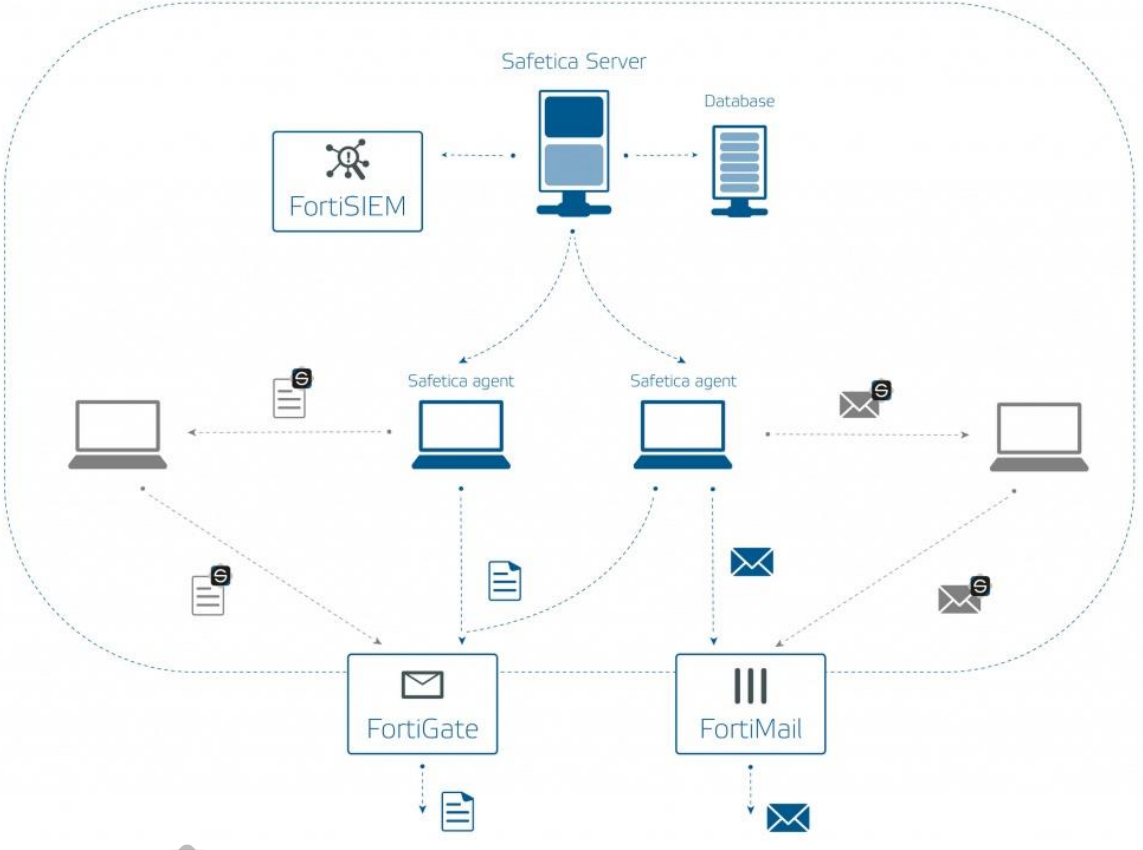


НОВАЯ ВЕРСИЯ 9.5
НОВЫЙ УЛУЧШЕННЫЙ ФУНКЦИОНАЛ

1. Интеграция с Office 365. (Можно внедрять политики DLP для электронной почты Exchange Online.)
2. Улучшена поддержка веб-приложений использующих сквозное шифрование. (Telegram, WhatsApp)
3. Интеграция с FortiNet
4. Поддержка macOS (Auditor)
5. Использование пользовательских словарей
6. И др.

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ
ИНТЕГРАЦИЯ С FORTINET

1. FORTIMAIL
2. FORTIGATE
3. FORTISIEM



КЕЙСЫ

ПРОЕКТЫ!

- ПРОИЗВОДСТВО
- НЕФТЬ И ГАЗ
- СТРАХОВАНИЕ
- ЛОГИСТИКА
- ФИНАНСОВЫЙ СЕКТОР
- ГОСУДАРСТВЕННЫЙ СЕКТОР
- ПРОЕКТИРОВАНИЕ
- МЕДИЦИНА
- ТОРГОВЛЯ

ESET АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

safetica

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% (гос)

ОФИСНЫЙ КОНТРОЛЬ И
DLP SAFETICA

НАШИ ПРЕИМУЩЕСТВА:

1. **Внедрение решения** от несколько дней до 8 недель
2. **Выявление инсайдеров благодаря модульной структуре** продукта на всех этапах работы с информацией (Auditor, Supervisor, DLP)
3. **Полноценное DLP решение с агентной архитектурой**
4. **Не требуются серверов** с высокими вычислительными мощностями
5. **Проводит оценку** эффективности сотрудников
6. **Успешно прогнозирует** инциденты безопасности
7. **Точный мониторинг времени**
8. **Оптимальная стоимость**

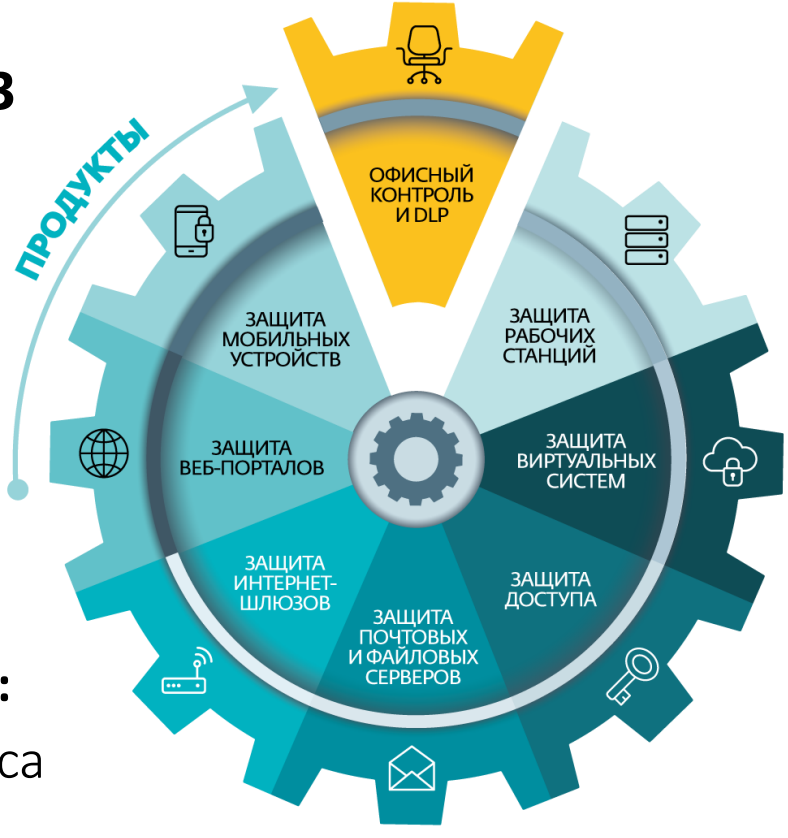
eset АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

safetica

КАК?
КОМПЛЕКСНЫЙ ПОДХОД:

1. БЕЗОПАСНОСТЬ ОТ ВНЕШНИХ УГРОЗ

- Антивирус
- EMS
- EVS
- Защита от сетевых атак
- EDTD
- EEI
- ESET Cloud

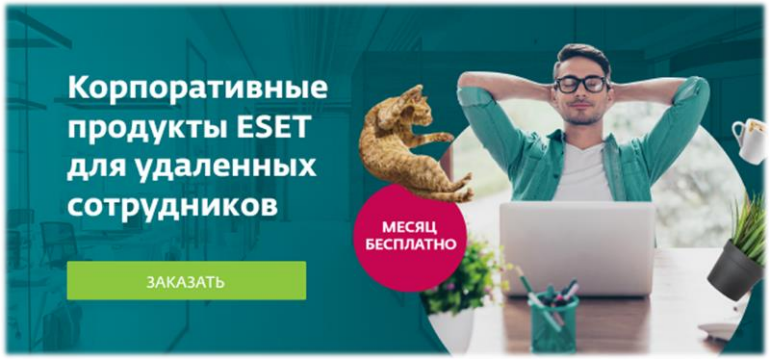


2. БЕЗОПАСНОСТЬ ОТ ВНУТРЕННИХ УГРОЗ:

- Офисный контроль и DLP Safetica
- ESA

eset АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

safetica



Комплект первой помощи

Тестовые версии трех продуктов предоставляется бесплатно сроком на 1 месяц

СРОК ДЕЙСТВИЯ
НЕ ОГРАНИЧЕН

- **ESET Secure Authentication** – надежное средство двухфакторной аутентификации для безопасного доступа к IT-инфраструктуре компании.
- **Auditor Safetica** – часть решения «Офисный контроль и DLP Safetica» для выявления потенциальных рисков безопасности и мониторинга эффективности работы сотрудника из дома.
- **ESET NOD32 Smart Security Business Edition** – комплексное бизнес-решение для оперативного сканирования и распознавания всех типов угроз. Содержит расширенный функционал безопасности и контроля работы пользователей.

СПАСИБО
ЗА ВНИМАНИЕ!

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