



Как защитить важные данные и противодействовать угрозам нулевого дня

Ланцевских Дмитрий

Инженер поддержки продаж ESET Russia

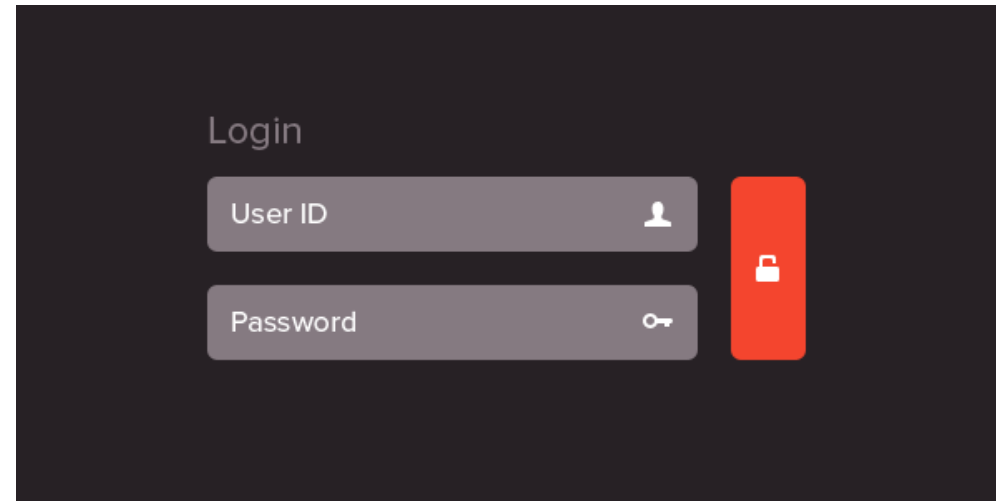
КОНФИДЕНЦИАЛЬНЫЕ ДАННЫЕ ЭТО

- › Персональные данные
- › Финансовые документы
- › Бизнес-планы
- › Ноу-хау
- › Клиентские базы
- › Прайсы
- › Юридические документы
- › ...

В любой компании есть **конфиденциальные данные!**

ГДЕ ХРАНИТСЯ ИНФОРМАЦИЯ?

- › На ПК пользователя
- › В CRM
- › В периметре компании
- › Облачные сервисы Microsoft
- › Порталы
- › ...



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 СОТРУДНИКОВ

- › Постоянные пароли
- › Простые пароли
- › Пароли содержат пользовательскую информацию
- › Одинаковые пароли



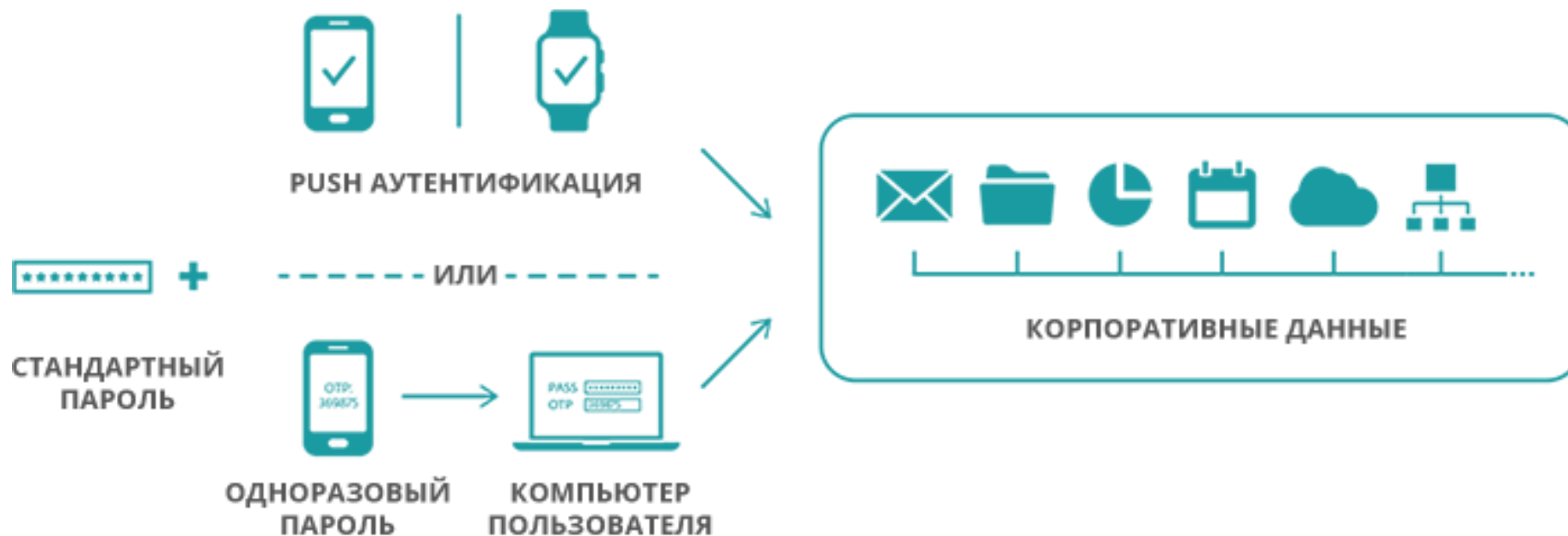


SECURE AUTHENTICATION



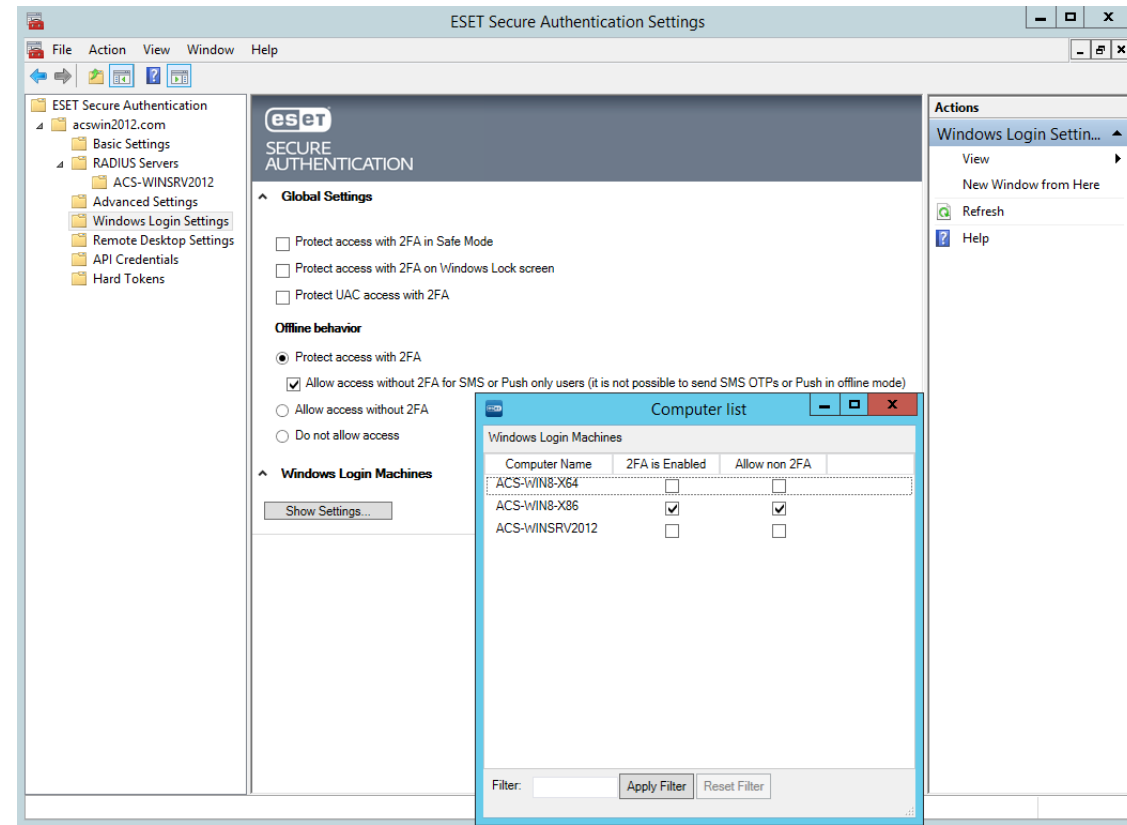
АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

КАК РАБОТАЕТ ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ



ВАРИАНТЫ ИНТЕГРАЦИИ

- › Защита входа в компьютер
- › Защита **облачных** сервисов
- › Защита **веб-приложений**
- › Защита **VPN** и **VDI** систем
- › CRM
- › Пакеты API и SDK - для внедрения в **собственные системы** аутентификации



СИСТЕМНЫЕ ТРЕБОВАНИЯ

Серверная часть

Microsoft Windows Server 2008, 2008 R2,
2012, 2012 R2, 2016, 2019
Windows Small Business Server 2008, 2011

**Установка и базовая настройка
за 10 минут**

Клиентская часть

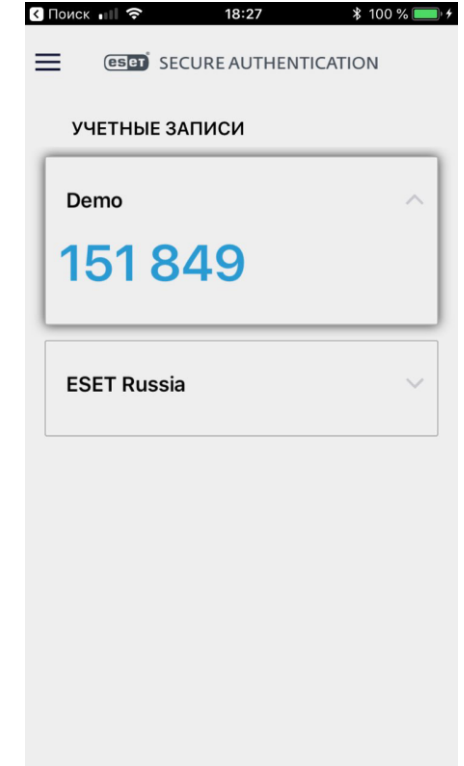
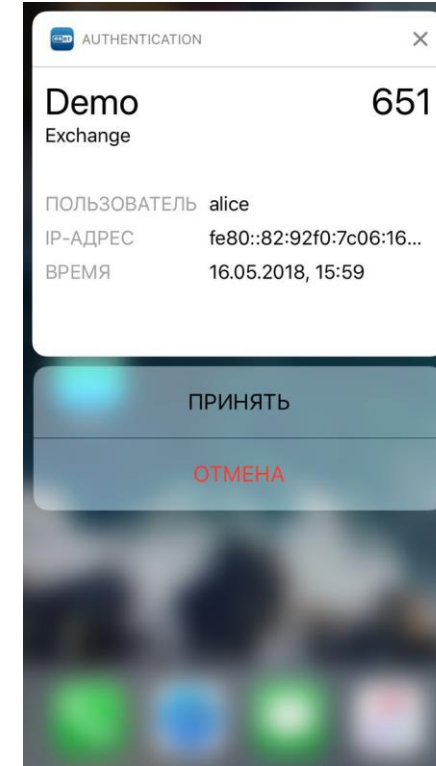
Windows 7/8/8.1/10

Apple iOS с версии 9 и выше;
Android™ с версии 4.1 и выше;
Windows Phone 8.1 по Windows 10 Mobile



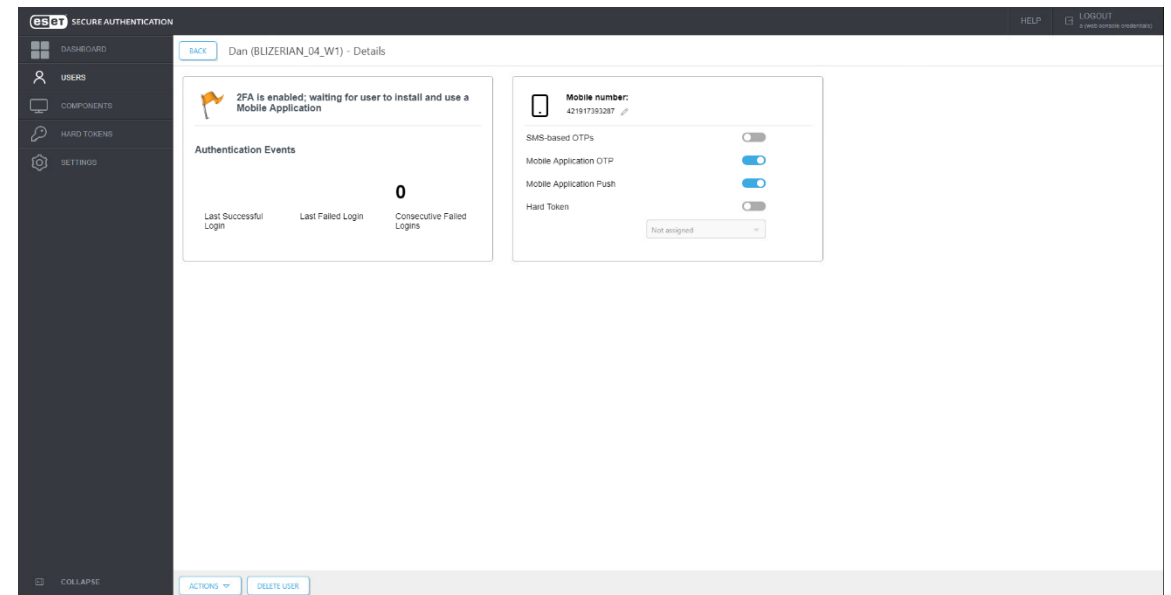
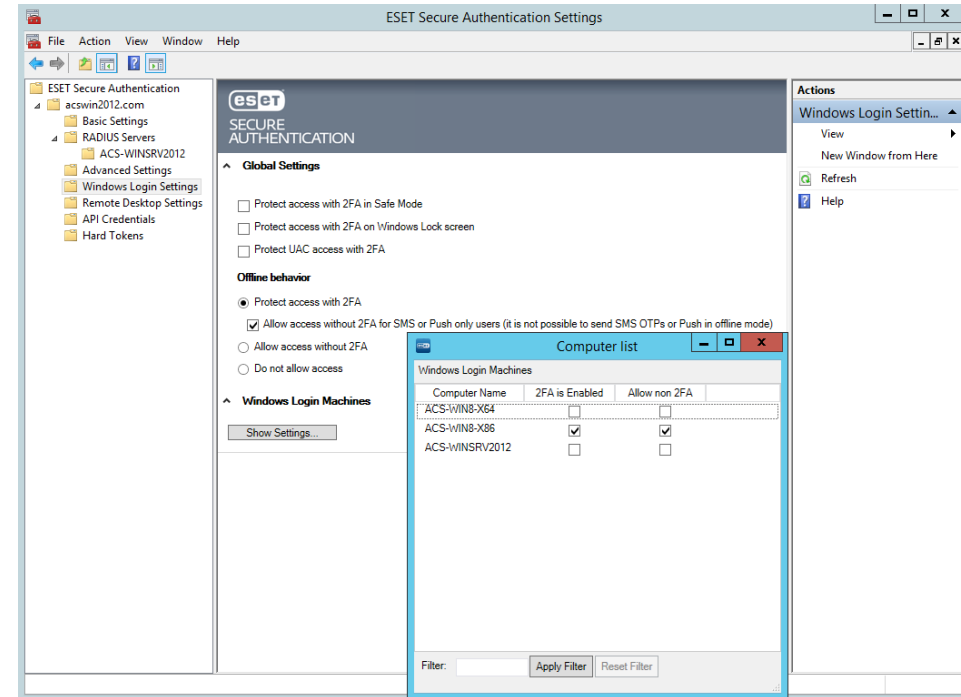
КЛИЕНТСКАЯ ЧАСТЬ

- › Совместима с любым мобильным телефоном с функцией приема SMS сообщений
- › Для выдачи временных паролей не нужна мобильная сеть и подключение к интернету
- › Мобильное приложение защищено PIN-кодом
- › Поддерживает функцию PUSH-аутентификации в устройствах на базе Windows Phone, Android и iOS
- › Поддержка временных токенов через мобильное приложение ESA

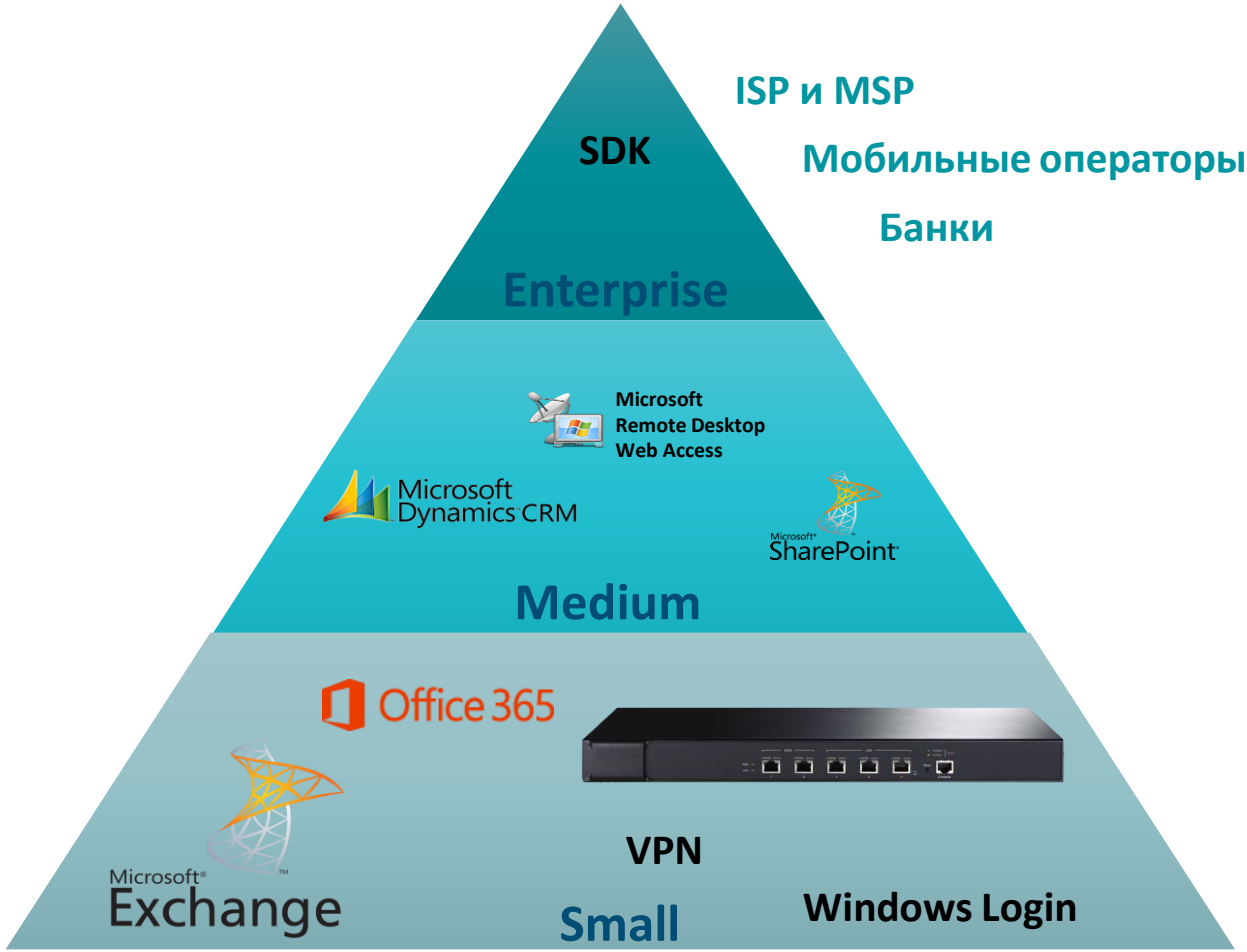


ВОЗМОЖНОСТИ АДМИНИСТРИРОВАНИЯ

- › Поддержка Microsoft Management Console (MMC)
- › Поддержка самостоятельной регистрации пользователей.
- › **ESET Secure Authentication Web Console**
- › Интеграция в Active Directory и добавление в Active Directory Users & Computers (ADUC) дополнительных параметров для настройки двухфакторной аутентификации



Применение ESA



**ДОСТУП
ПОЛУЧЕН**

Все ПОД КОНТРОЛЕМ



УТЕЧКА ДАННЫХ ЭТО РЕАЛЬНОСТЬ!

- › **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

УТЕЧКА ДАННЫХ

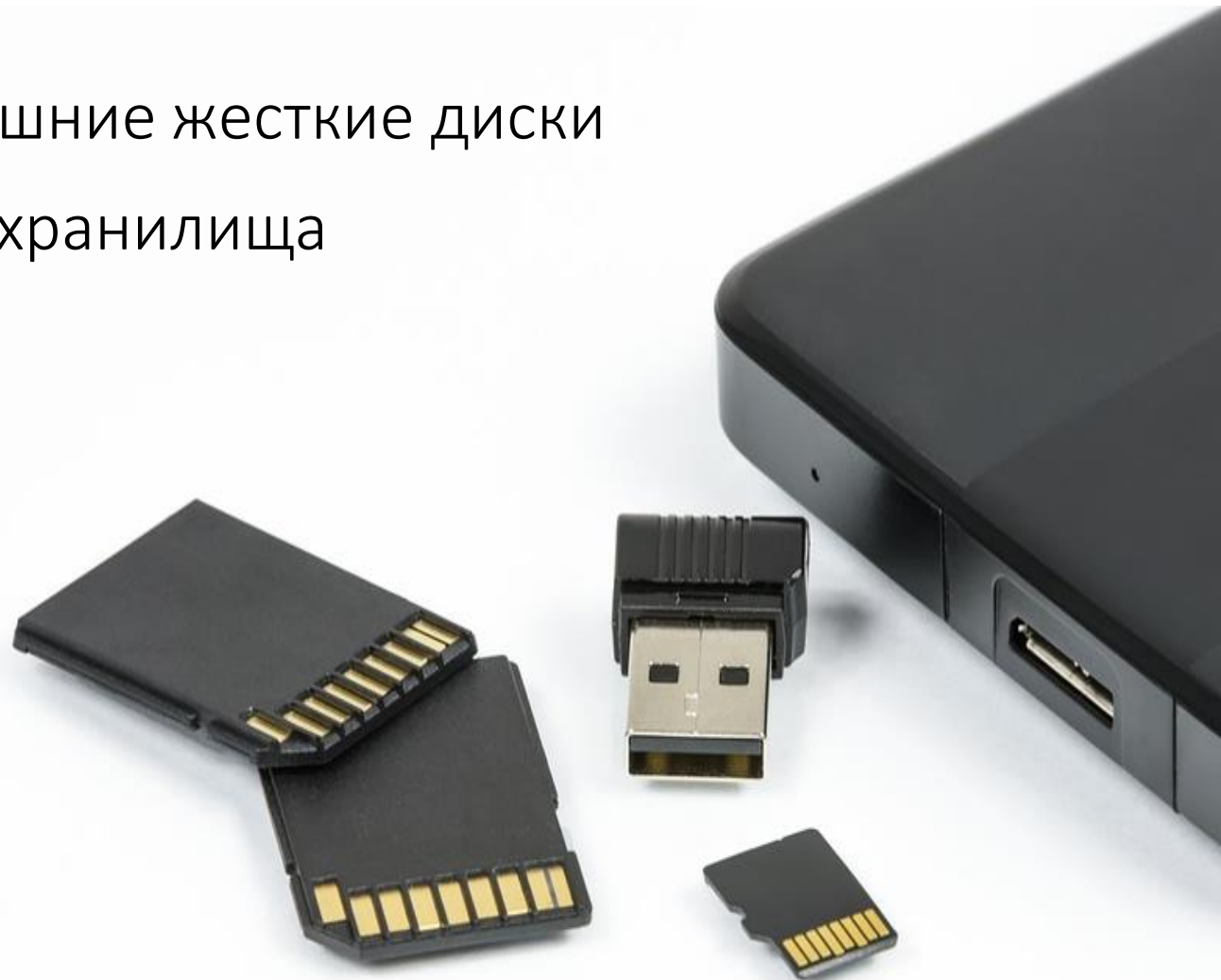
ПОЧЕМУ ЭТО ПРОИСХОДИТ?

- › Создание собственной компании на базе уникальных данных
- › Продажа информации конкурентам
- › Использование данных для устройства на новую работу
- › Отправил по невнимательности **не тому адресату**
- › Потерял флешку по дороге домой
- › Другие причины

УТЕЧКА ДАННЫХ

КАК ЭТО ПРОИСХОДИТ?

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



УТЕЧКА ДАННЫХ И НЕЭФФЕКТИВНАЯ РАБОТА - КАК ЗАЩИТИТЬСЯ?

ОФИСНЫЙ КОНТРОЛЬ И DLP SAFETICA



ОФИСНЫЙ КОНТРОЛЬ И DLP



safetica



TECHNOLOGY ALLIANCE



ПРИНЦИПИАЛЬНЫЕ РАЗЛИЧИЯ DLP СИСТЕМ



СЕТЕВЫЕ

АППАРАТНЫЙ ИЛИ ВИРТУАЛЬНЫЙ ШЛЮЗ



АГЕНТНЫЕ

АГЕНТЫ DLP НА КОНЕЧНЫХ ТОЧКАХ



КОНТЕНТНЫЙ ФИЛЬТР

ПРИНЯТИЕ РЕШЕНИЯ НА ОСНОВЕ АНАЛИЗА
СОДЕРЖИМОГО



КОНТЕКСТНЫЙ ФИЛЬТР

ПРИНЯТИЕ РЕШЕНИЯ ПО ФОРМАЛЬНЫМ
ПРИЗНАКАМ



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

АРХИТЕКТУРА РЕШЕНИЯ SAFETICA

Внедрение в 4 этапа:

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



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, с IIS 7.5 и выше

База данных (MS SQL)

MS SQL 2008 R2 и выше, рекомендуется MS SQL 2016 и выше

MS SQL 2016 Express SP1 включена в установочный пакет Safetica

КОМПЛЕКСНОЕ РЕШЕНИЕ SAFETICA



AUDITOR

РЕГИСТРАЦИЯ АКТИВНОСТИ СОТРУДНИКОВ



SUPERVISOR

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ БИЗНЕС-ПРОЦЕССОВ КОМПАНИИ



DLP

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ КОМПАНИИ

ОФИСНЫЙ КОНТРОЛЬ - МОДУЛЬ AUDITOR



ПРЕДСТАВЛЕНИЕ О ТОМ, ЧТО ПРОИСХОДИТ В КОМПАНИИ



СОБЛЮДЕНИЕ ПОЛИТИК БЕЗОПАСНОСТИ



СРАВНЕНИЕ РАБОТЫ СОТРУДНИКОВ

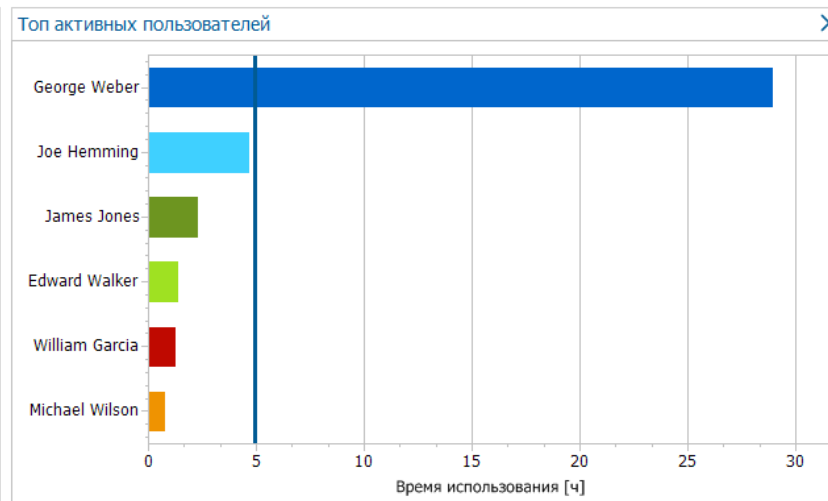
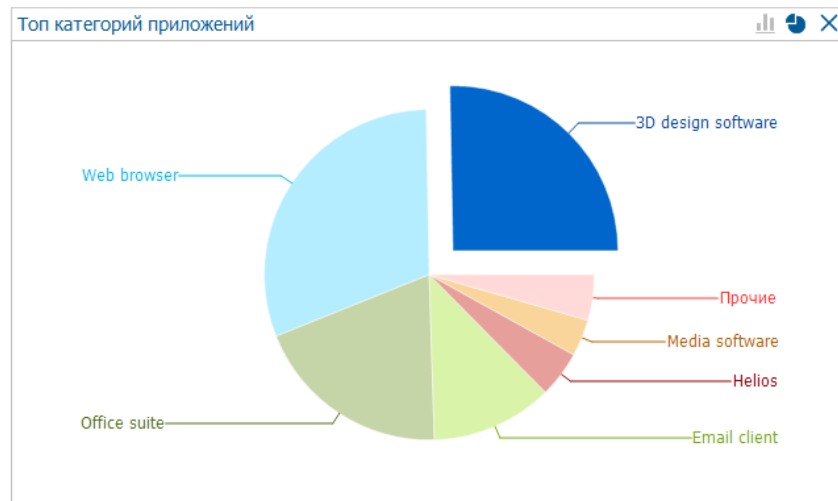


АУДИТ ЧУВСТВИТЕЛЬНЫХ ДАННЫХ КОМПАНИИ



ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ ПО

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
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 SUPERVISOR



› Web-контроль

Действие по умолчанию: Разрешено

Добавить правило

Имя	Подробнее
Блокировка по категориям	Категории: File hosting, Job search, Malware
Блокировка по IP	Категории: Pornography IP-адрес: 192.168.0
Блокировка по домену	URL: *.facebook.com/*, *.twitter.com/*



› 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



› 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

НЕЭФФЕКТИВНОСТЬ. ЧЕМ НА САМОМ ДЕЛЕ ЗАНЯТЫ СОТРУДНИКИ

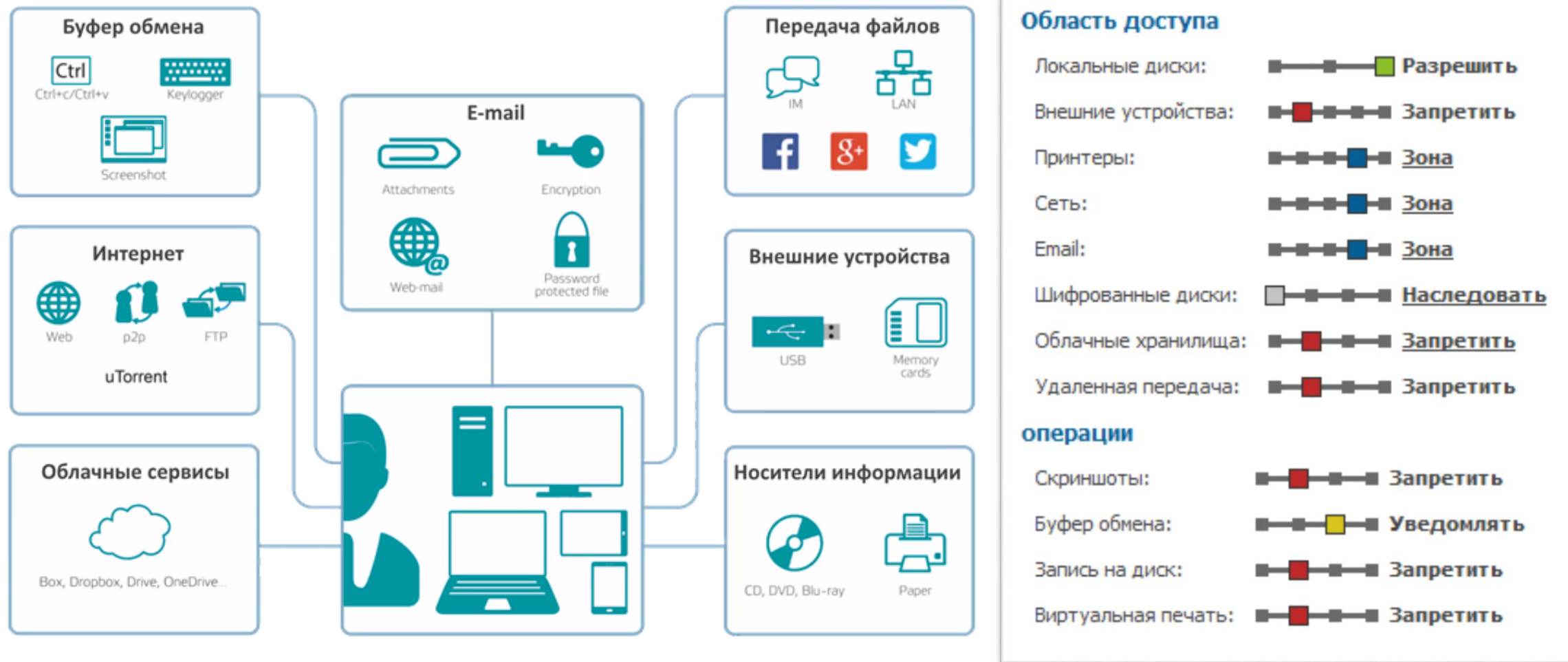
- › **28% сидят в соцсетях**
*в рабочее время (и это не SMM-менеджеры)**
- › **21% делают халтуру**
*в рабочее время**
- › **69% активно ищут новую работу**
*или открыты для предложений***

Тратят на соцсети в 2 раза
больше времени на работе,
чем дома

** Ресурсы VoucherCodesPro, 2012*



ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ - МОДУЛЬ DLP



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

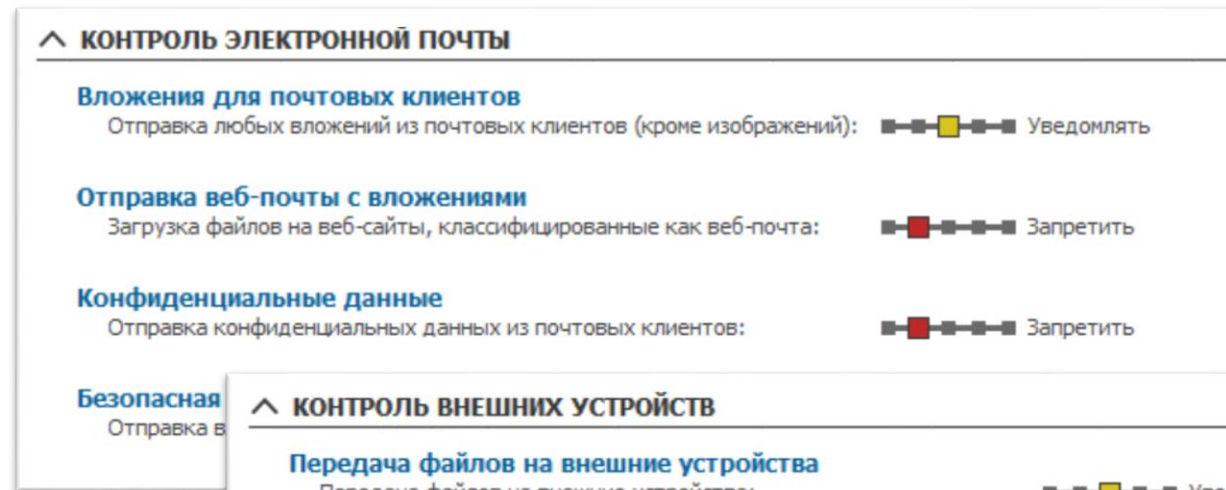
Все файлы, помещенные в определенные папки, будут автоматически получать необходимую метку.

› 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.

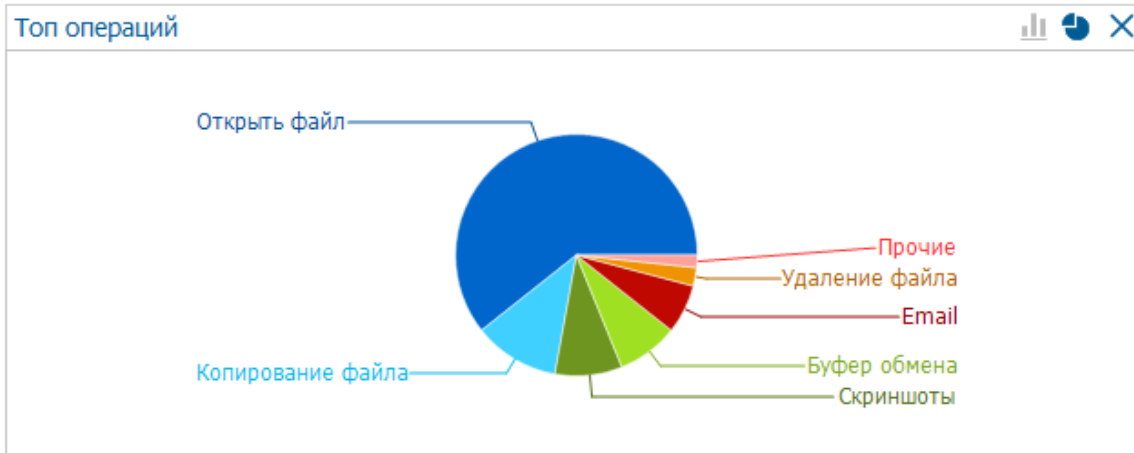
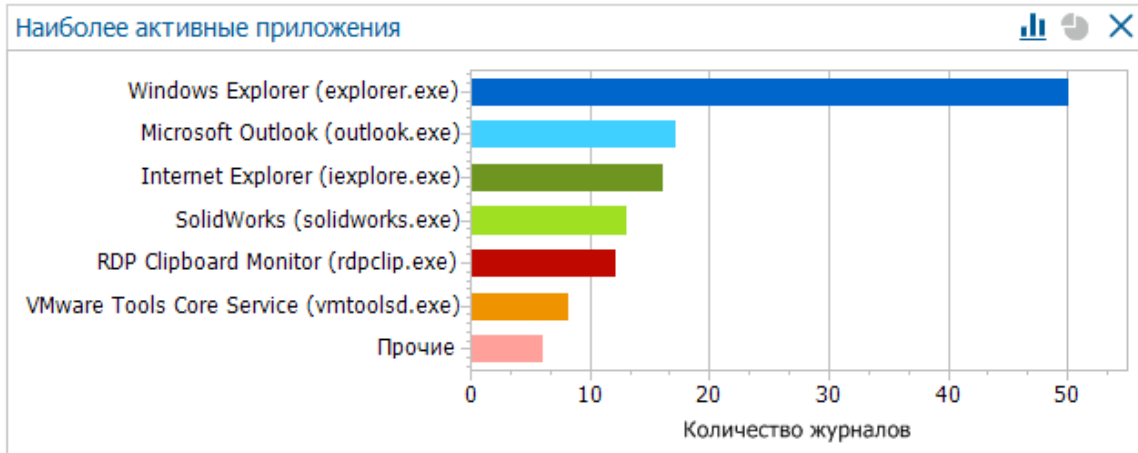
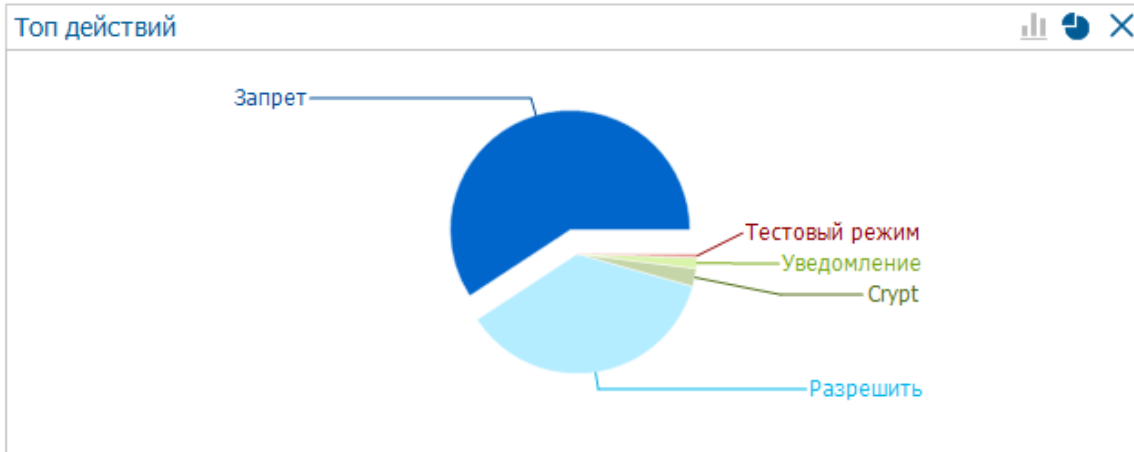
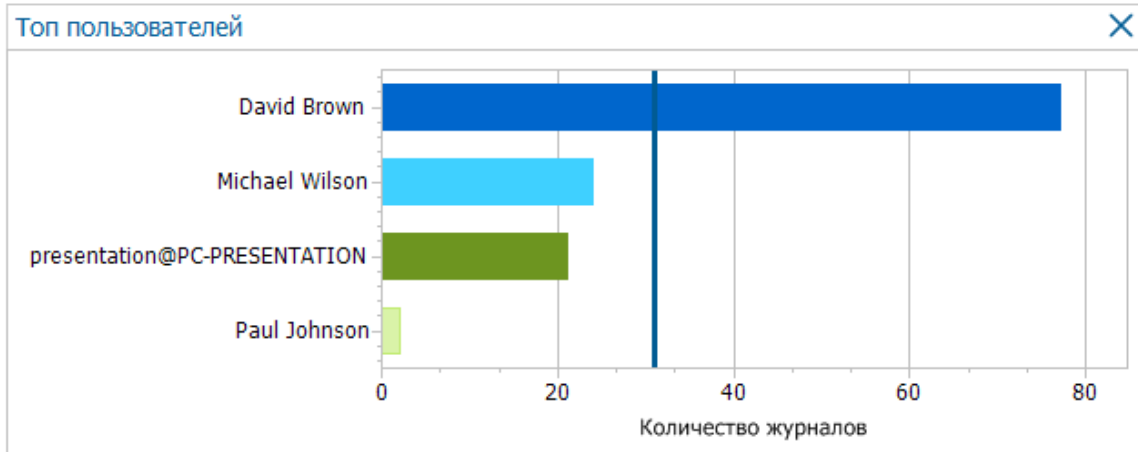
› КЛЮЧЕВЫЕ СЛОВА И РЕГУЛЯРНЫЕ ВЫРАЖЕНИЯ

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

› МЕТАДААННЫЕ СТОРОННИХ КЛАССИФИКАТОРОВ

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

АНАЛИТИКА - МОДУЛЬ DLP



ОТЧЕТНОСТЬ И БЛОКИРОВКА ДЕЯТЕЛЬНОСТИ



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	6
Auditor - Электронная почта - Наиболее активные получатели	7



Нельзя отправлять это электронное письмо

- Microsoft Outlook
- test
- @ skuznecov@esetnod32.ru



ПРЕДУПРЕЖДЕНИЯ

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



Отправить

Не отправлять



Загрузка файлов в сеть заблокирована

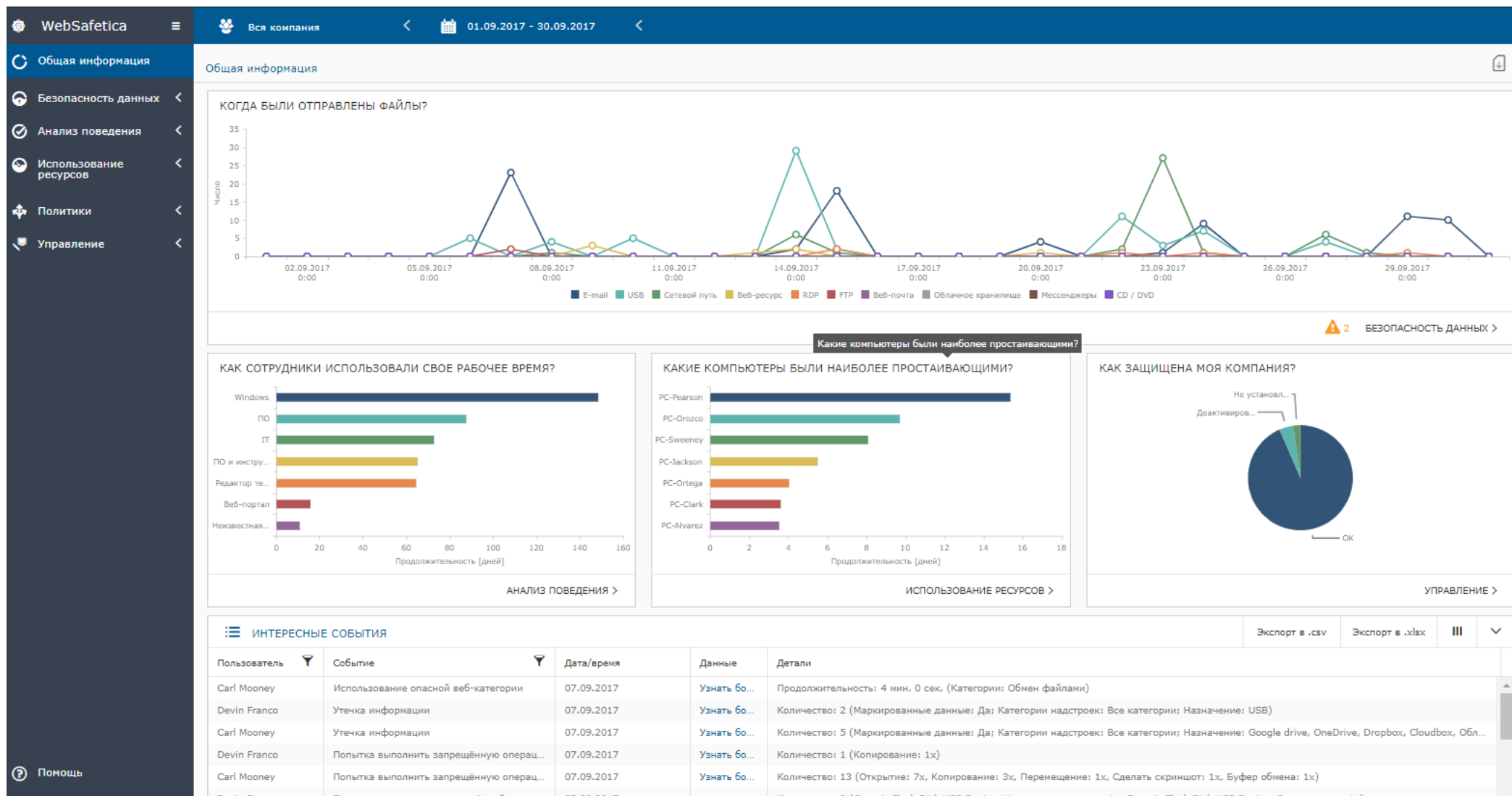
- Google Chrome
- Договор.txt
- <https://nofile.io/>

Загрузка файла **Договор.txt** для адреса **Супер Секретно**, содержащего защищенные данные (категория **Супер Секретно**) для адреса <https://nofile.io/> заблокирована.

Это действие противоречит политике безопасности и будет записано в журнал.

Close

АНАЛИЗ РЕЗУЛЬТАТОВ В ВЕБ КОНСОЛИ WEBSAFETICA



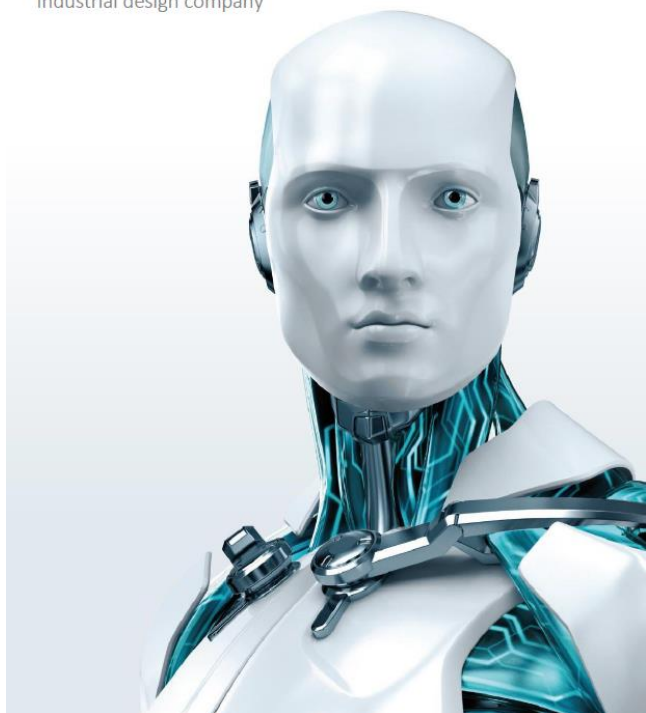
РЕЗУЛЬТАТЫ ВНЕДРЕНИЯ

eset ОФИСНЫЙ КОНТРОЛЬ И DLP

esafetica

АНАЛИЗ РЕЗУЛЬТАТОВ

Industrial design company



✓ ПОВЫШЕНИЕ ПРОИЗВОДИТЕЛЬНОСТИ:

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

✓ ЗАЩИЩЕННАЯ РАБОТА С ДАННЫМИ:

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

✓ ЭФФЕКТИВНОЕ ИСПОЛЬЗОВАНИЕ IT-РЕСУРСОВ:

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



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ЛИЦЕНЗИРОВАНИЕ И ЦЕНЫ



› АУДИТОР

SAF-AUD-NS-1-99	167 094 ₽
-----------------	-----------



› ОФИСНЫЙ КОНТРОЛЬ

SAF-SOC-NS-1-99	241 410 ₽
-----------------	-----------



› FULL DLP

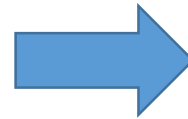
SAF-DLP-NS-1-99	371 405 ₽
-----------------	-----------

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

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%**

**УЯЗВИМОСТЬ
НУЛЕВОГО ДНЯ**



**ЭКСПЛОИТ
НУЛЕВОГО ДНЯ**



DYNAMIC THREAT DEFENSE

ESET DYNAMIC THREAT DEFENSE

ОБНАРУЖЕНИЕ УГРОЗ НУЛЕВОГО ДНЯ

- ✓ Встроенная песочница
- ✓ Машинное обучение
- ✓ Автоматическая защита
- ✓ Многоуровневое обнаружение угроз

ОТЧЕТ О ПОВЕДЕНИИ ФАЙЛОВ

СТАТУС	Очень подозрительный
SHA-1	F02C2C66C43953E0A88257DF3C4A01726B798233
РАЗМЕР	178В
КАТЕГОРИЯ	Сценарий

Обнаруженное поведение

ПОВЕДЕНИЕ	Создание службы
ОБЪЯСНЕНИЕ	Образец пытался создать новую службу. Службы — это программы, раб режиме
ПОЛЕЗНЫЕ ДЕЙСТВИЯ	Это стандартное поведение для некоторых системных служебных прог
ВРЕДОНОСНЫЕ ДЕЙСТВИЯ	Вредоносная программа пытается запуститься после перезагрузки систе

ПОВЕДЕНИЕ	Обнаружен сбрасыватель
ОБЪЯСНЕНИЕ	Образец сбросил или загрузил файл, определенный как вредоносная пр
ПОЛЕЗНЫЕ ДЕЙСТВИЯ	Чистые приложения не должны этого делать
ВРЕДОНОСНЫЕ ДЕЙСТВИЯ	Образец сбросил или загрузил вредоносное содержимое

ПОВЕДЕНИЕ	Повышение привилегий
ОБЪЯСНЕНИЕ	Образец попытался повысить собственные привилегии для получения г или доступа к системе.
ПОЛЕЗНЫЕ ДЕЙСТВИЯ	Это стандартное поведение для некоторых установщиков
ВРЕДОНОСНЫЕ	

ЦЕНТРАЛИЗОВАННЫЙ СБОР ОТЧЕТОВ И УПРАВЛЕНИЕ В ЕДИНОЙ КОНСОЛИ

eset SECURITY MANAGEMENT CENTER Search computer na... QUICK LINKS HELP ADMINISTRATOR LOGOUT

Dashboard

Overview Incidents Overview Computers Security Management Center Server Antivirus threats Firewall threats ESET applications EDTD +

Files analyzed by ESET Dynamic Threat Defense in last 30 days grouped by the resul...

Generated 0 minutes ago

Files submitted to ESET Dynamic Threat Defense and ESET LiveGrid in last 30 days g...

Generated 0 minutes ago

Files submitted to ESET Dynamic Threat Defense and ESET Live Grid in last 30 days

Group by (Hash)	Group by (File category)	Group by (Reason of submission)	Group by (State of analysis)	Group by (Score)	Maximum (Timestamp of analysis)
5B66147B4446...	Executable	Automatic	Finished	1	2018 Mar 16 1...
F9D3BEAF78D...	Executable	Automatic	Finished	1	2018 Mar 16 1...
A609359D34D...	Executable	Automatic	Finished	63	2018 Mar 16 1...
6AF5D9EB670...	Executable	Automatic	Finished	45	2018 Mar 16 1...
1FAF9DD52D6...	Executable	Automatic	Finished	45	2018 Mar 16 1...
62DD7916A86...	Executable	Automatic	Finished	1	2018 Mar 16 1...
6C16EA577433...	Executable	Automatic	Finished	45	2018 Mar 16 1...
A5B5F3A172EB...	Executable	Automatic	Finished	1	2018 Mar 16 1...
49521A5A03BE...	Executable	Automatic	Finished	45	2018 Mar 16 1...
1E4A48BEC5E4...	Script	Automatic	Finished	1	2018 Mar 15 1...
0DA7BD17789...	Script	Automatic	Finished	1	2018 Mar 15 1...
3F37A0BC29E6...	Other	Automatic	Finished	100	2018 Mar 14 1...
F5C4208E1A5...	Executable	Automatic	Finished	1	2018 Mar 14 1...
1E135AF20993...	Executable	Automatic	Finished	100	2018 Mar 14 1...
C21680CADA1...	Executable	Automatic	Finished	1	2018 Mar 14 1...

Generated 0 minutes ago

Files submitted to ESET Dynamic Threat Defense and ESET LiveGrid in last 30 days g...

Generated 0 minutes ago

Manually submitted samples to ESET Dynamic Threat Defense in last 30 days

Computer name	User name	Object URI	Time of occurrence
ESET Endpoint	EDTDPM\Administrator	file:///C:/Program Files/F...	2018 Mar 14 10:43:07

Generated 0 minutes ago

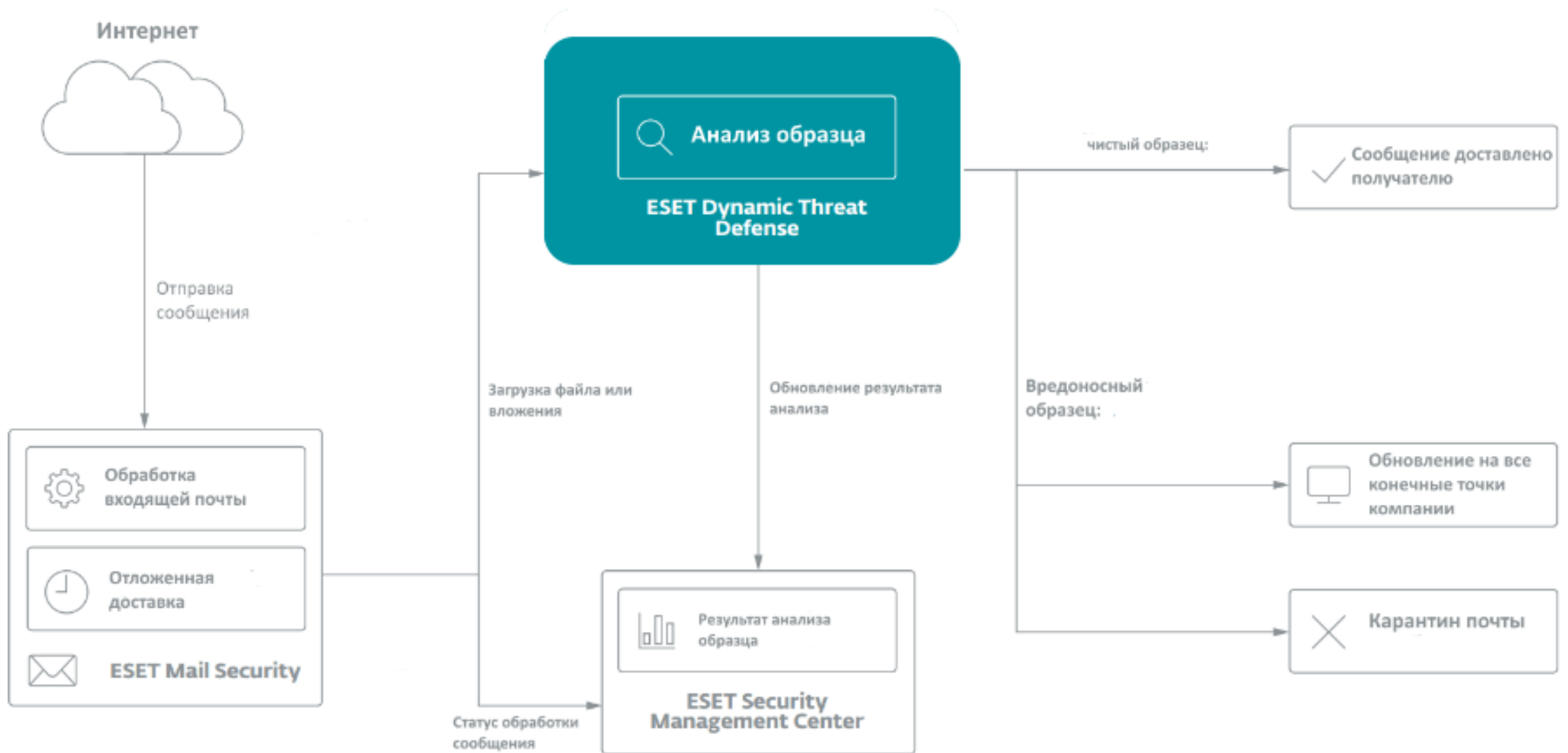
Top 10 computers with file submissions to ESET Dynamic Threat Defense and ESET L...

Generated 0 minutes ago

Files submitted to ESET Dynamic Threat Defense and ESET LiveGrid in last 30 days g...

Generated 0 minutes ago

АНАЛИЗ ОБРАЗЦОВ В РЕАЛЬНОЙ СРЕДЕ



ESET DYNAMIC THREAT DEFENSE ПОДДЕРЖИВАЕМЫЕ ПРОДУКТЫ

- ✓ ESET Endpoint Antivirus 7 для Windows
- ✓ ESET Endpoint Security 7 для Windows
- ✓ ESET File Security 7 для Windows Server
- ✓ ESET Mail Security 7 для Microsoft Exchange Server



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Спасибо! Вопросы?

