Как защитить важные данные и противодействовать угрозам нулевого дня

Ланцевских Дмитрий

Инженер поддержки продаж ESET Russia

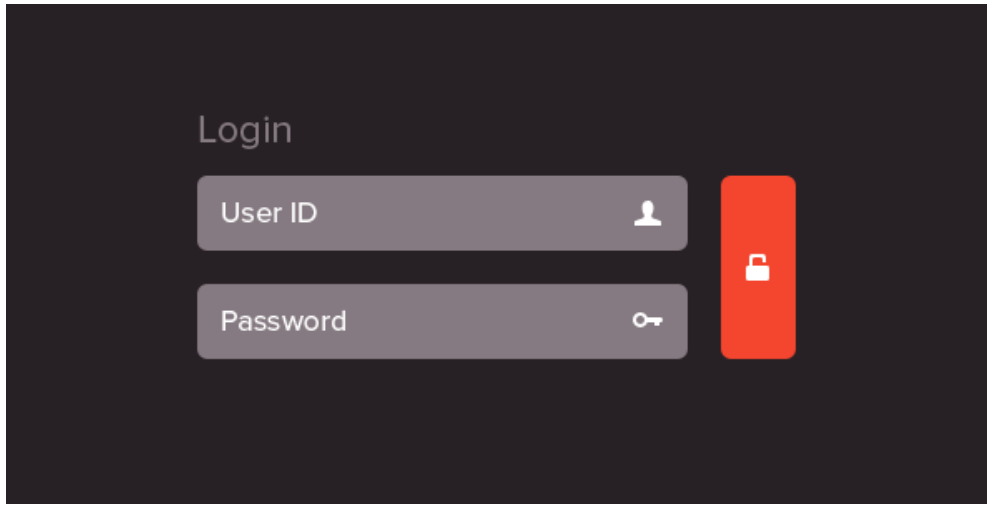
КОНФИДЕНЦИАЛЬНЫЕ ДАННЫЕ
ЭТО

- 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

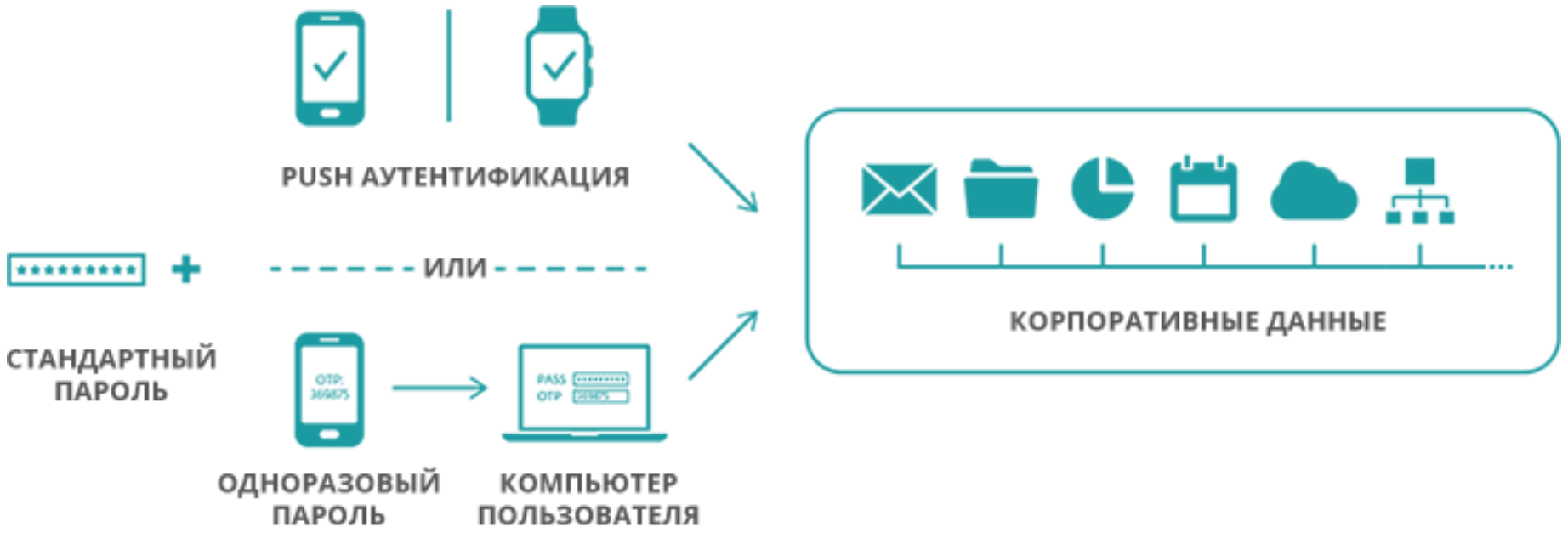
НЕКОМПЕТЕНТНОСТЬ СОТРУДНИКОВ

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

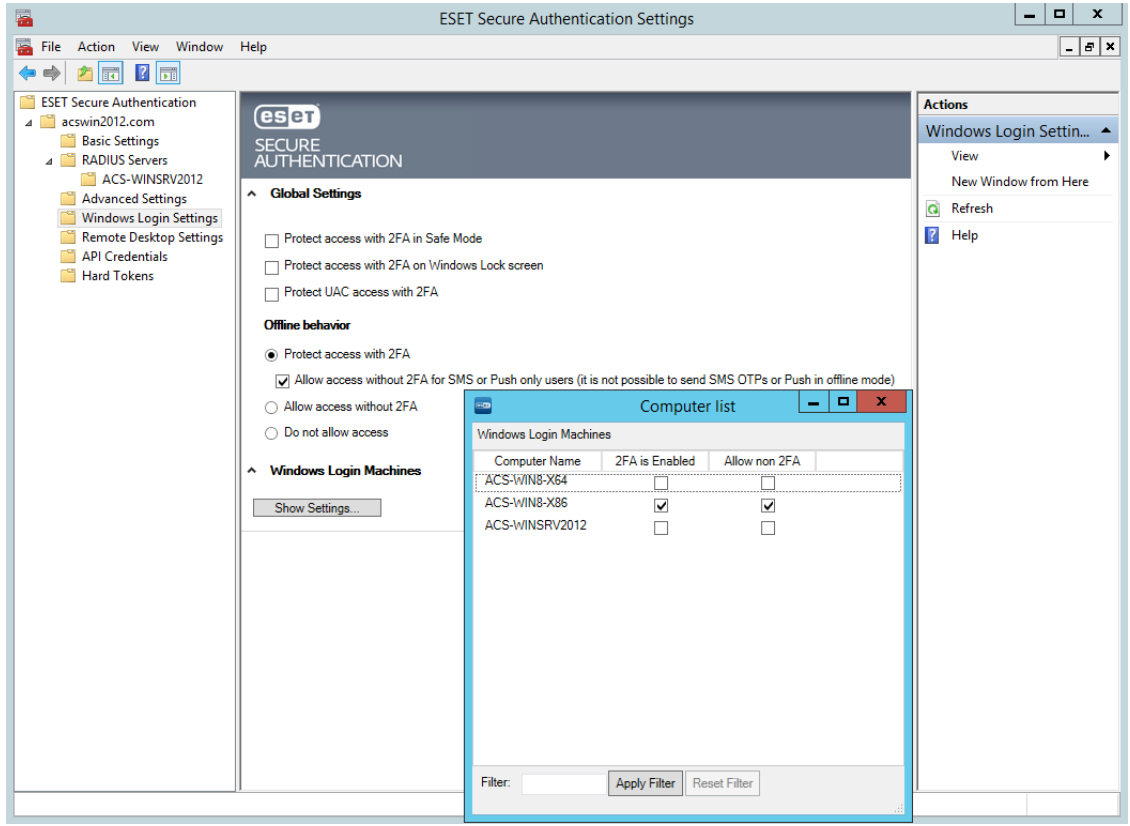
SECURE AUTHENTICATION

АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

КАК РАБОТАЕТ
ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ



ВАРИАНТЫ
ИНТЕГРАЦИИ



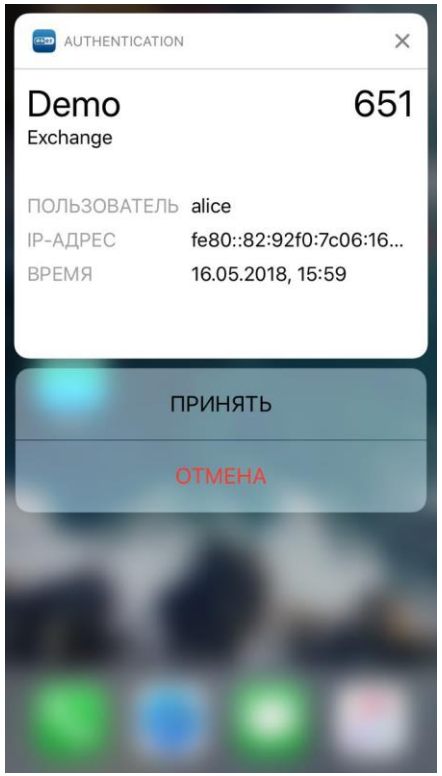
- Защита входа в компьютер
- Защита **облачных** сервисов
- Защита **веб-приложений**
- Защита **VPN** и **VDI** систем
- **CRM**
- Пакеты API и SDK - для внедрения в **собственные системы** аутентификации

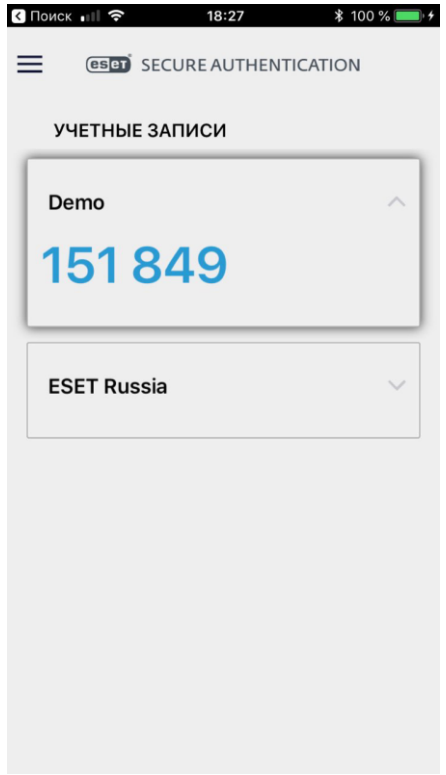
СИСТЕМНЫЕ ТРЕБОВАНИЯ

Серверная часть	Клиентская часть
Microsoft Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019 Windows Small Business Server 2008, 2011	Windows 7/8/8.1/10
Установка и базовая настройка за 10 минут	Apple iOS с версии 9 и выше; Android™ с версии 4.1 и выше; Windows Phone 8.1 по Windows 10 Mobile

КЛИЕНТСКАЯ ЧАСТЬ

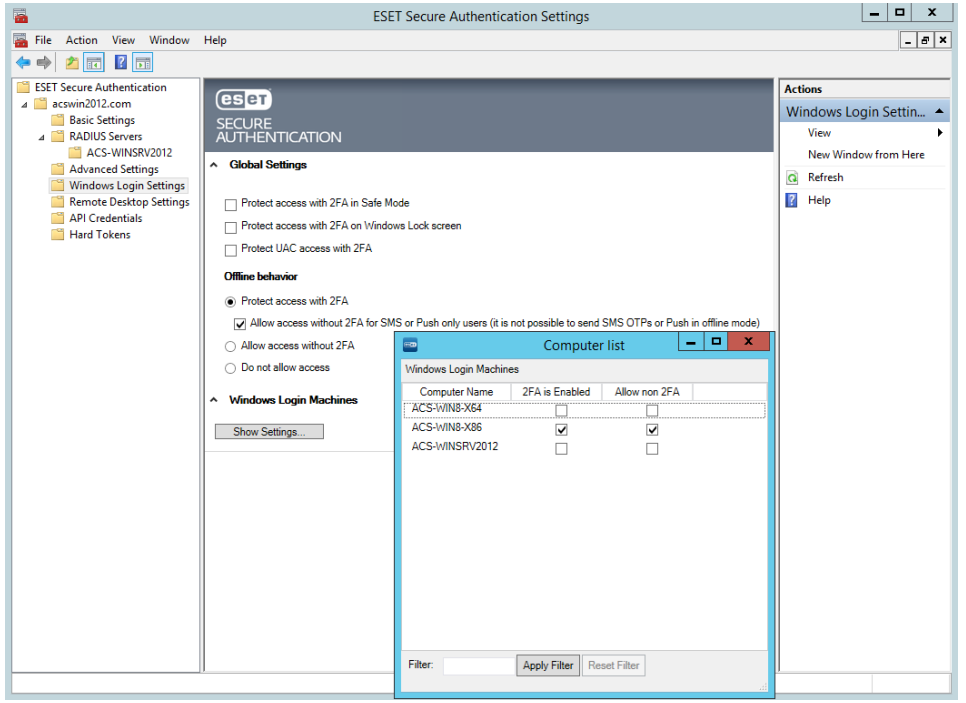
- Совместима с любым мобильным телефоном с функцией приема SMS сообщений
- Для выдачи временных паролей не нужна мобильная сеть и подключение к интернету
- Мобильное приложение защищено PIN-кодом
- Поддерживает функцию PUSH-аутентификации в устройствах на базе Windows Phone, Android и iOS
- Поддержка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

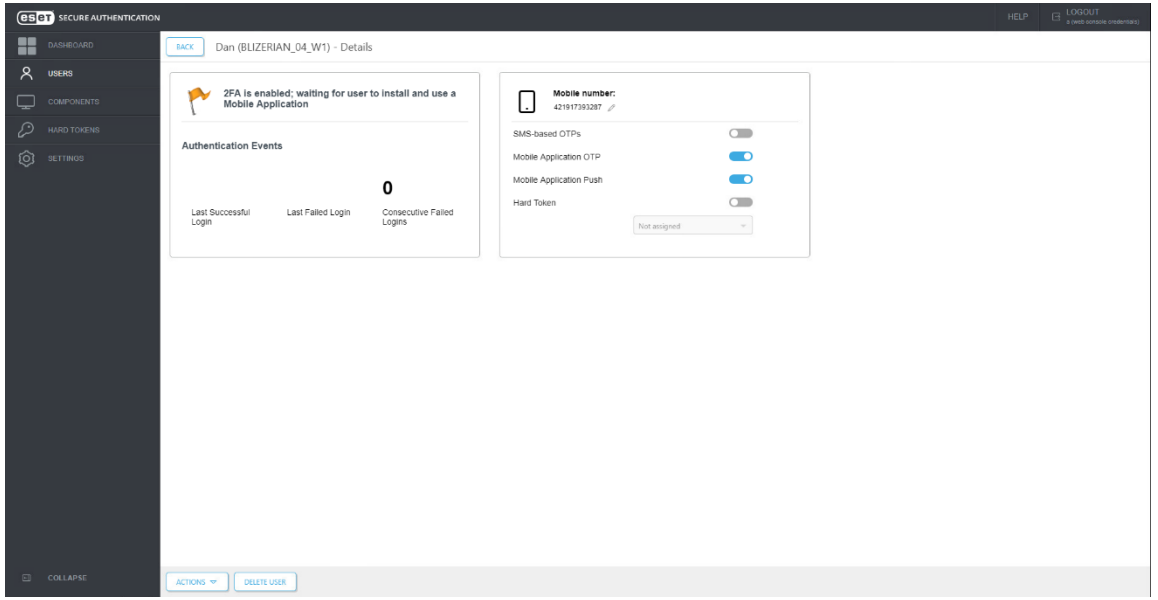




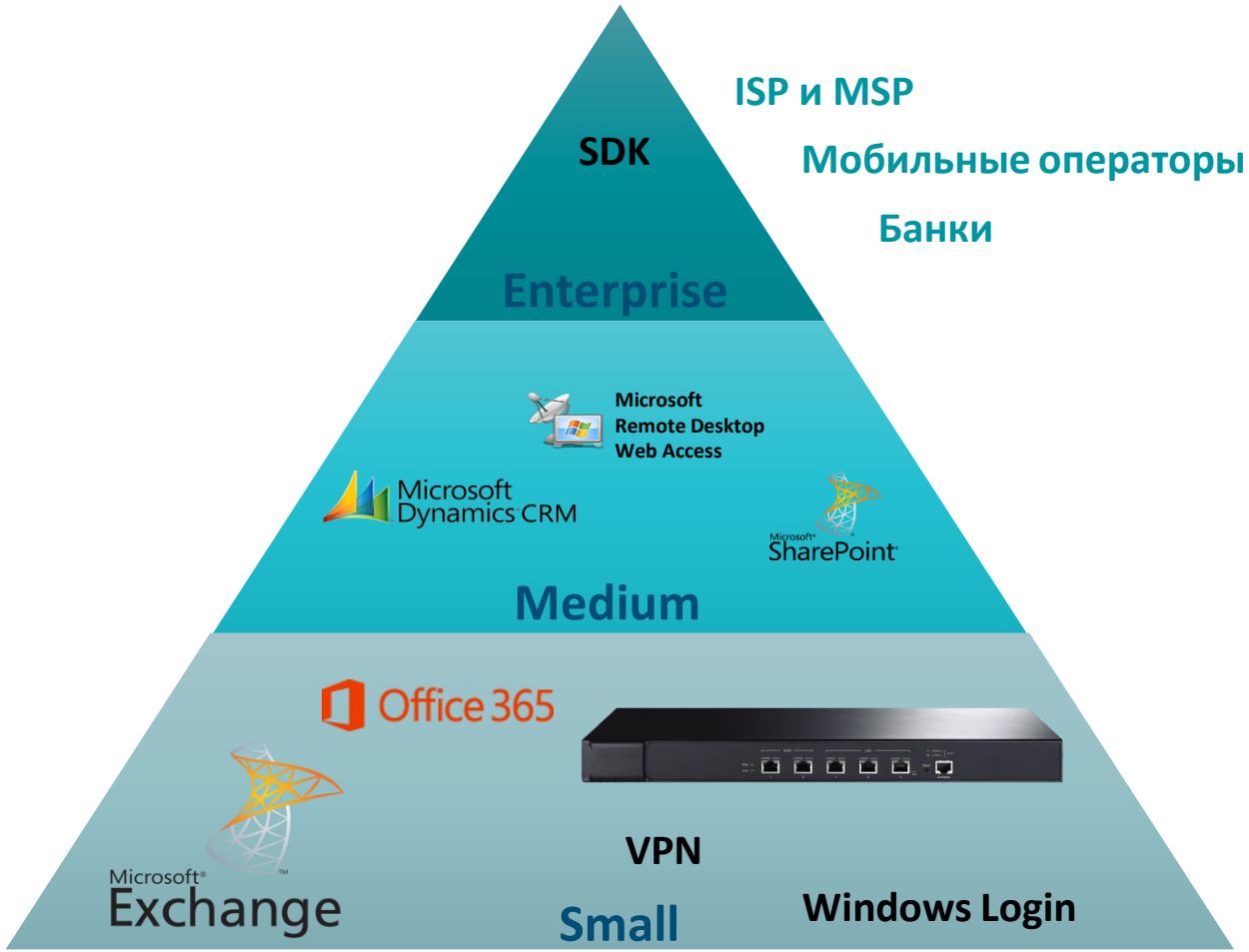
ВОЗМОЖНОСТИ АДМИНИСТРИРОВАНИЯ

- 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

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

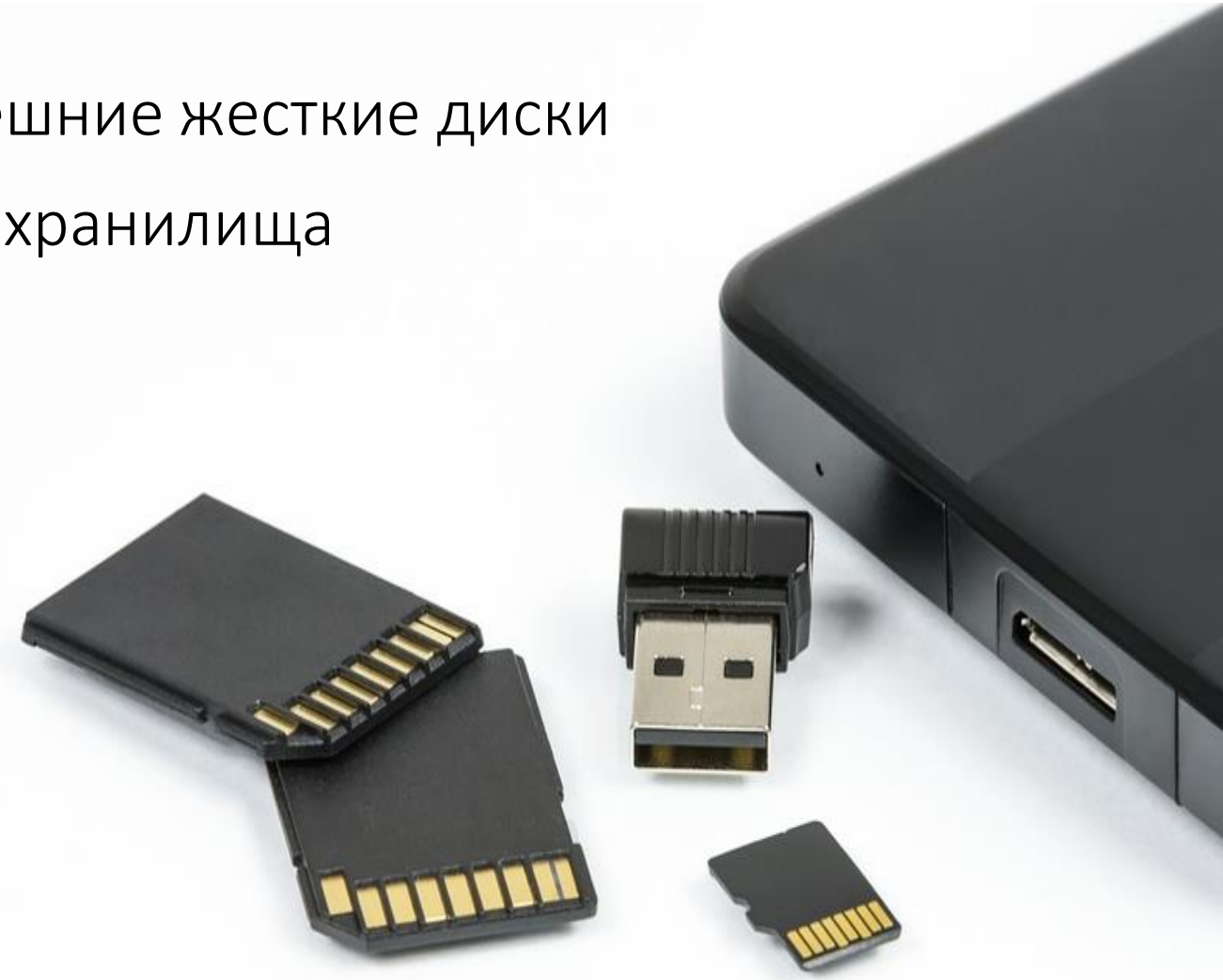
ESET Russia, 2017, 750 респондентов

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
- …



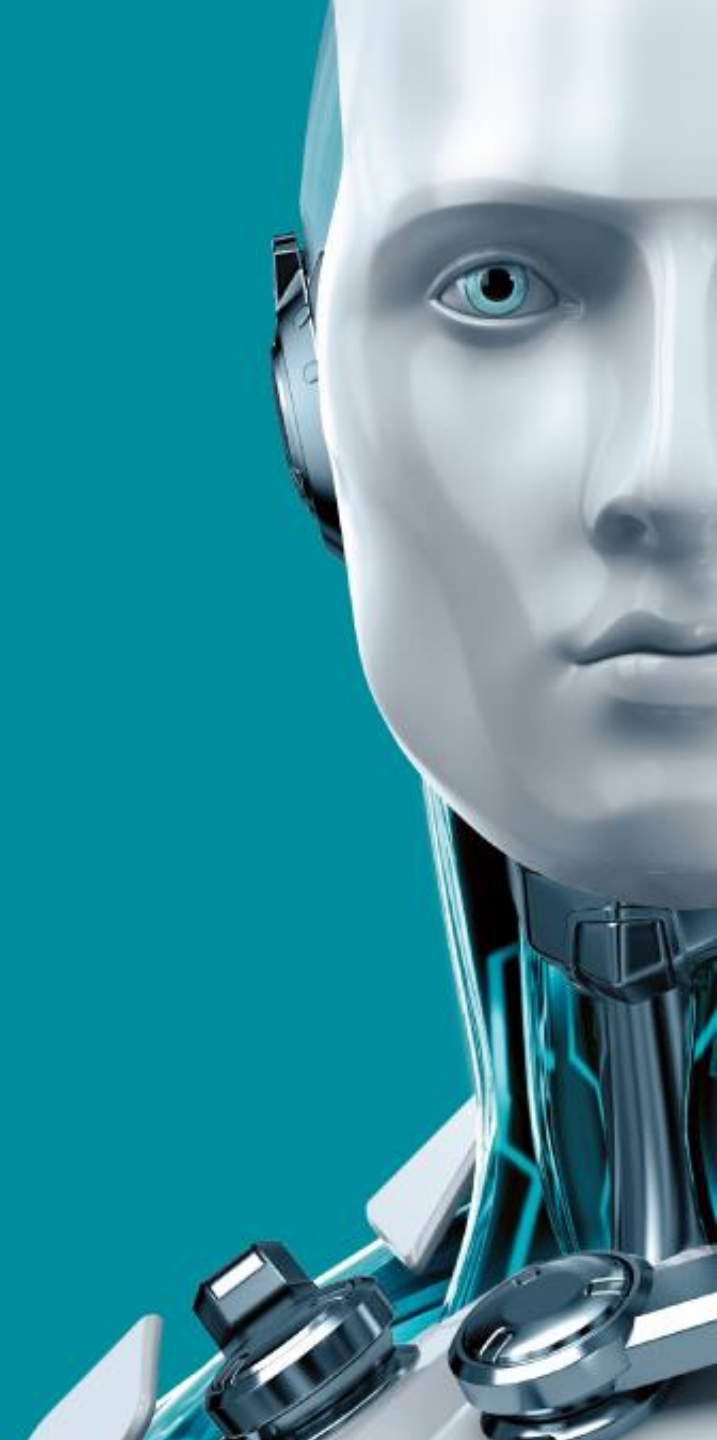
УТЕЧКА ДАННЫХ И НЕЭФФЕКТИВНАЯ РАБОТА - КАК ЗАЩИТИТЬСЯ?

ОФИСНЫЙ КОНТРОЛЬ И DLP SAFETICA

ОФИСНЫЙ КОНТРОЛЬ И DLP

safetica

ESET 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

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

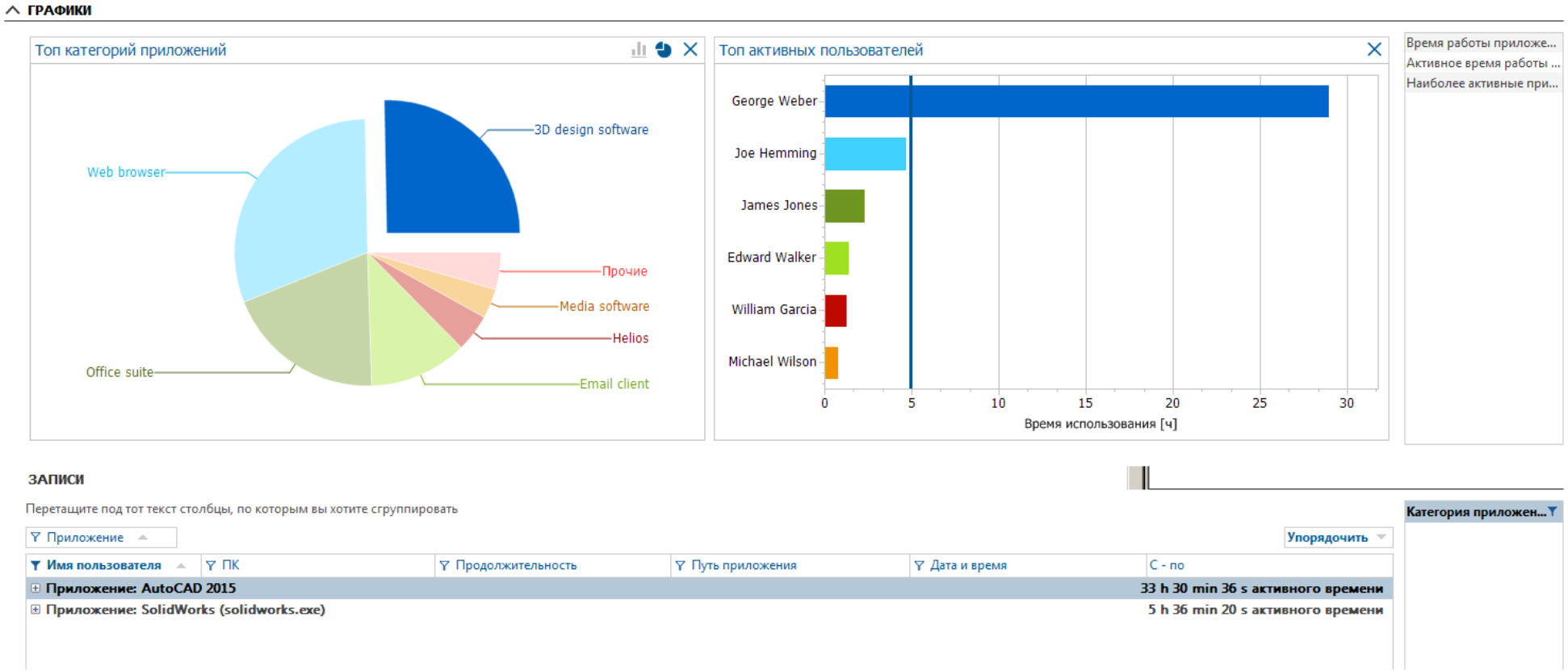
ПРЕДСТАВЛЕНИЕ О ТОМ, ЧТО ПРОИСХОДИТ В КОМПАНИИ

СОБЛЮДЕНИЕ ПОЛИТИК БЕЗОПАСНОСТИ

СРАВНЕНИЕ РАБОТЫ СОТРУДНИКОВ

АУДИТ ЧУВСТВИТЕЛЬНЫХ ДАННЫХ КОМПАНИИ

ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ ПО



ОФИСНЫЙ КОНТРОЛЬ - МОДУЛЬ SUPERVISOR

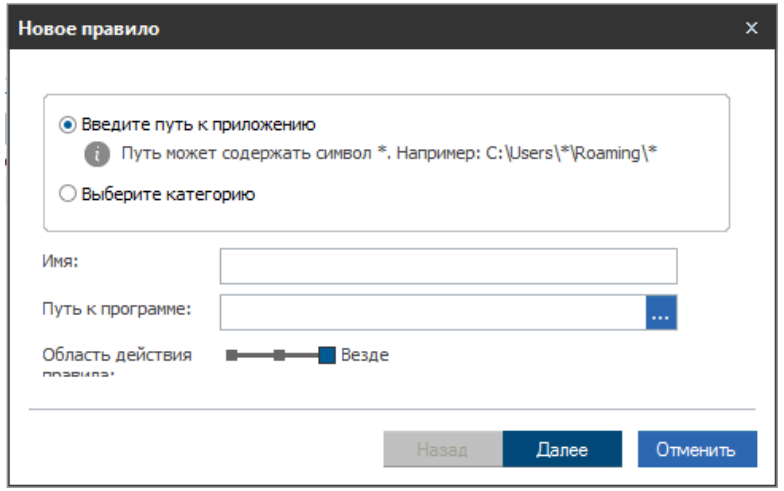
› Web-контроль

Действие по умолчанию: Разрешено

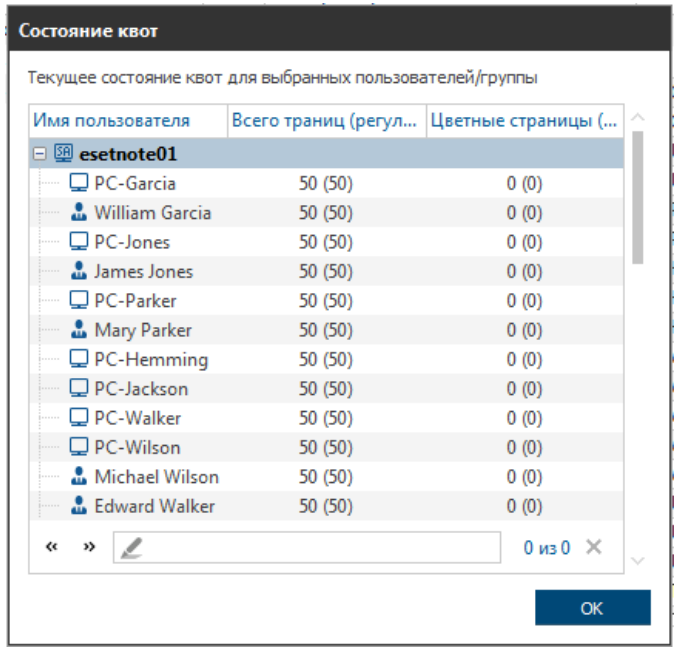
Добавить правило

Имя	Подробно
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



› Контроль печати



НЕЭФФЕКТИВНОСТЬ.
ЧЕМ НА САМОМ ДЕЛЕ ЗАНЯТЫ СОТРУДНИКИ

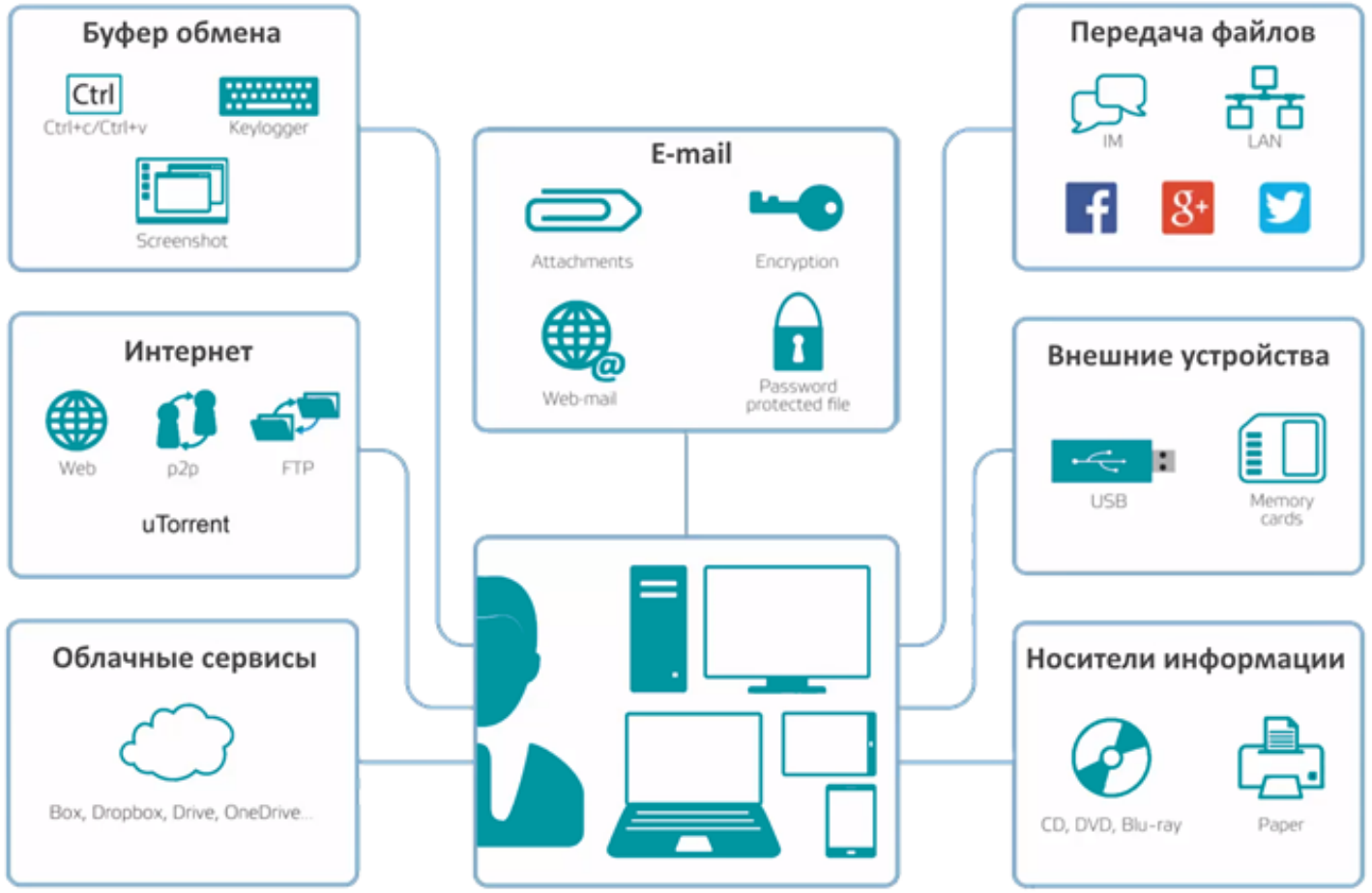
Тратят на соцсети в 2 раза больше времени на работе, чем дома

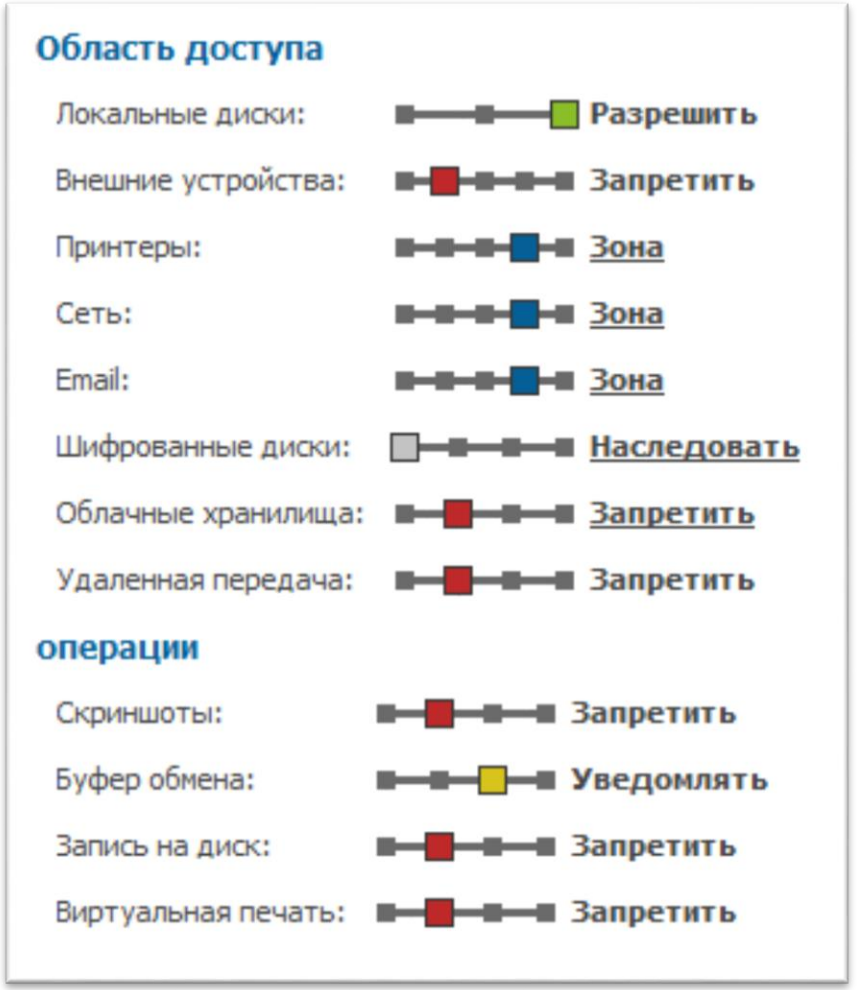
** Ресурс VoucherCodesPro, 2012*

- **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***

**ESET Russia, 2017, 750 респондентов*
*** Jobvite, 2013*

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

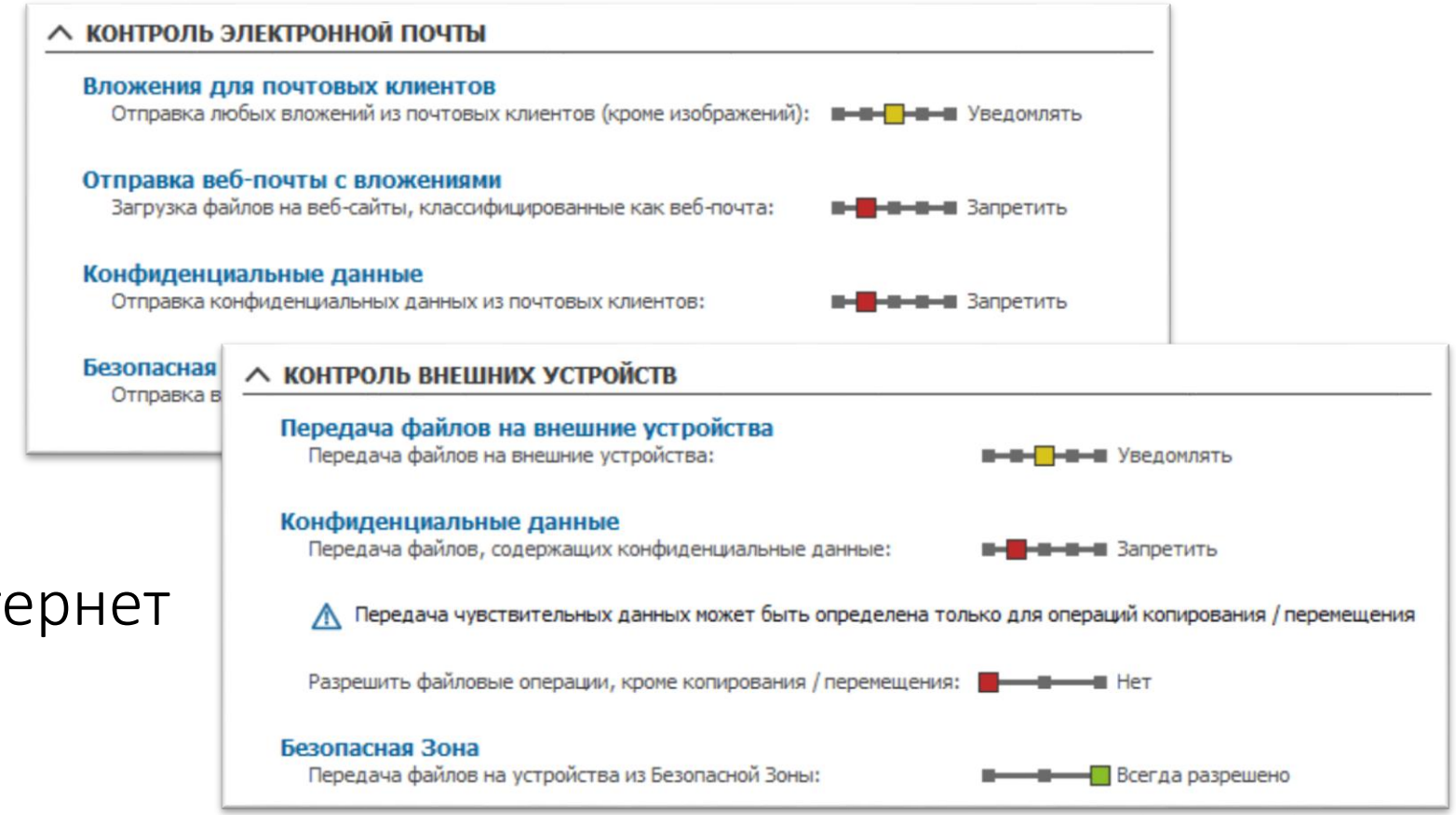
Все файлы, помещенные в определенные папки, будут автоматически получать необходимую метку.

› 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.

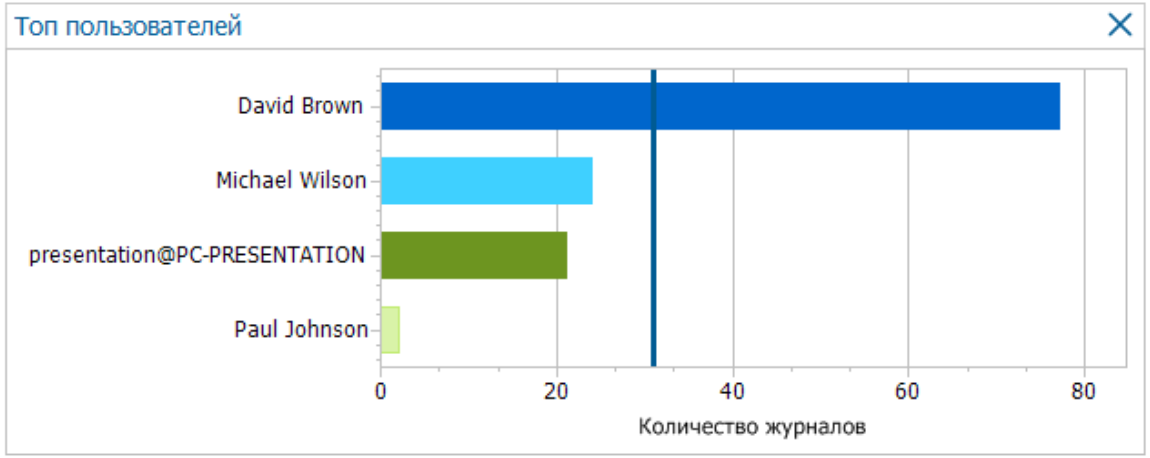
› КЛЮЧЕВЫЕ СЛОВА И РЕГУЛЯРНЫЕ ВЫРАЖЕНИЯ

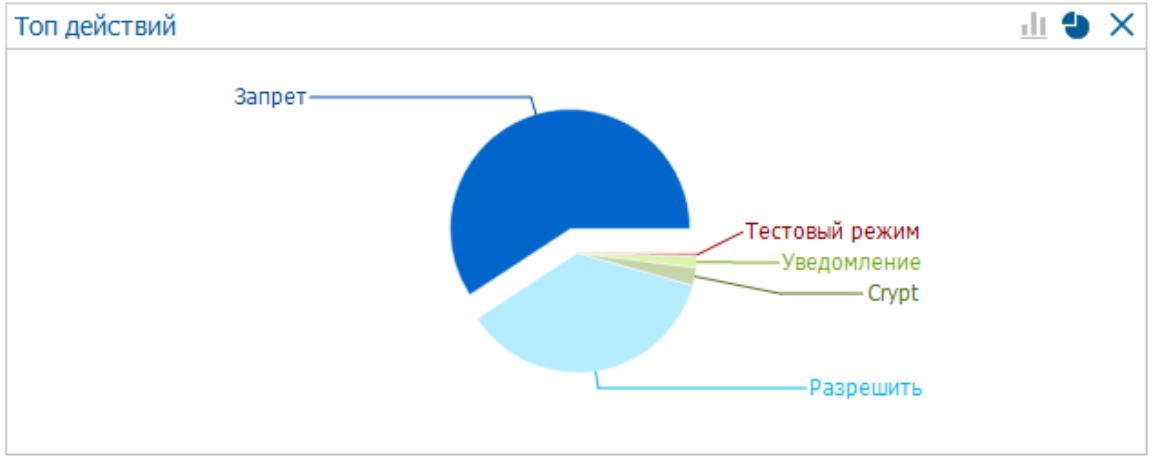
Любые слова и словосочетания, использование регулярных выражений с применением синтаксиса ECMAScript

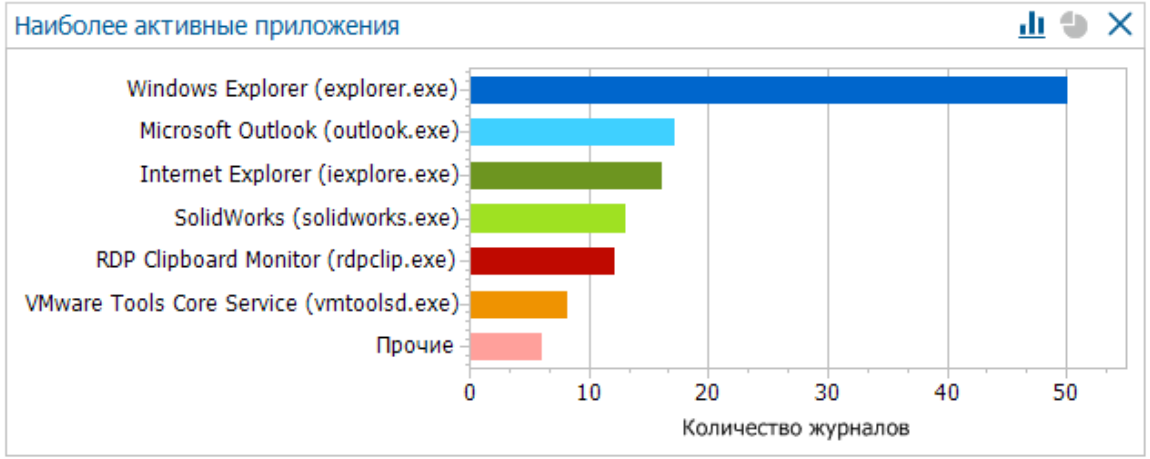
› МЕТАДАННЫЕ СТОРОННИХ КЛАССИФИКАТОРОВ

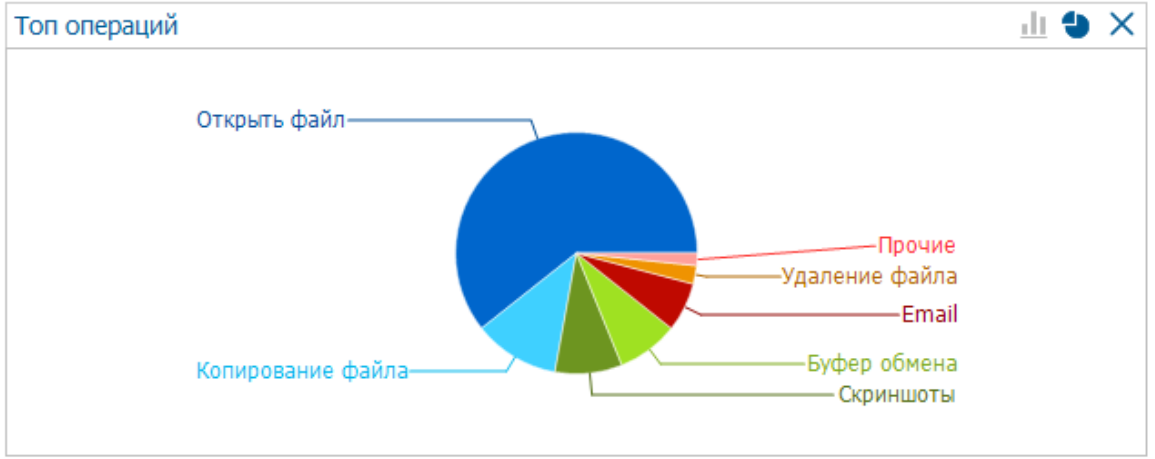
Протестирована поддержка метаданных Microsoft Azure Information Protection, Boldon James, Tukan GREENmod.

АНАЛИТИКА - МОДУЛЬ DLP

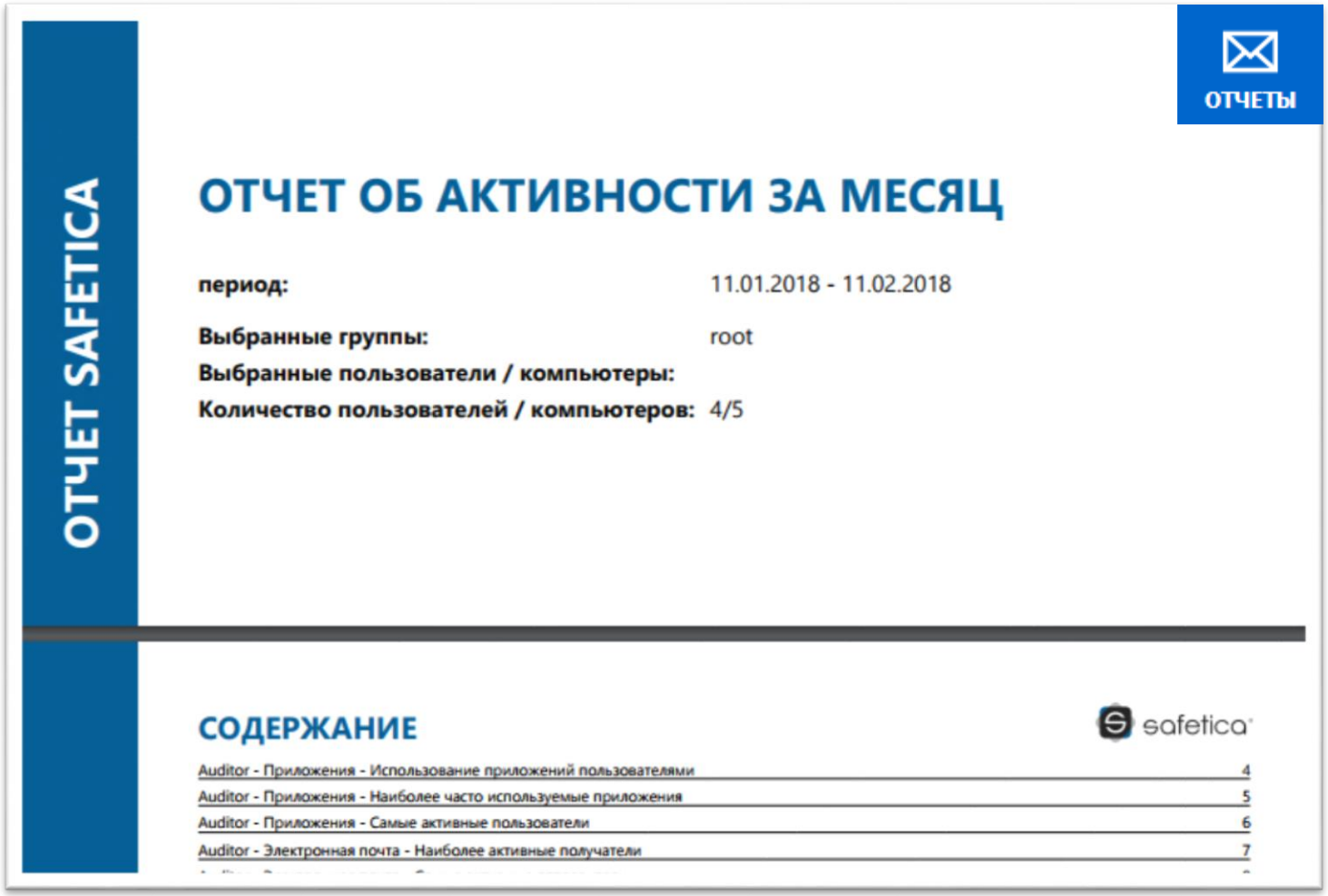


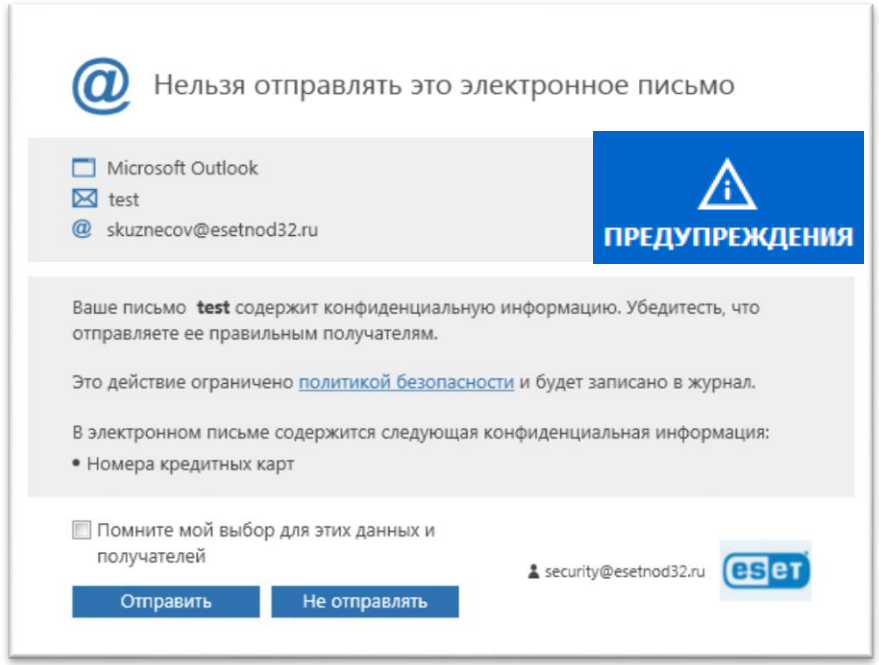


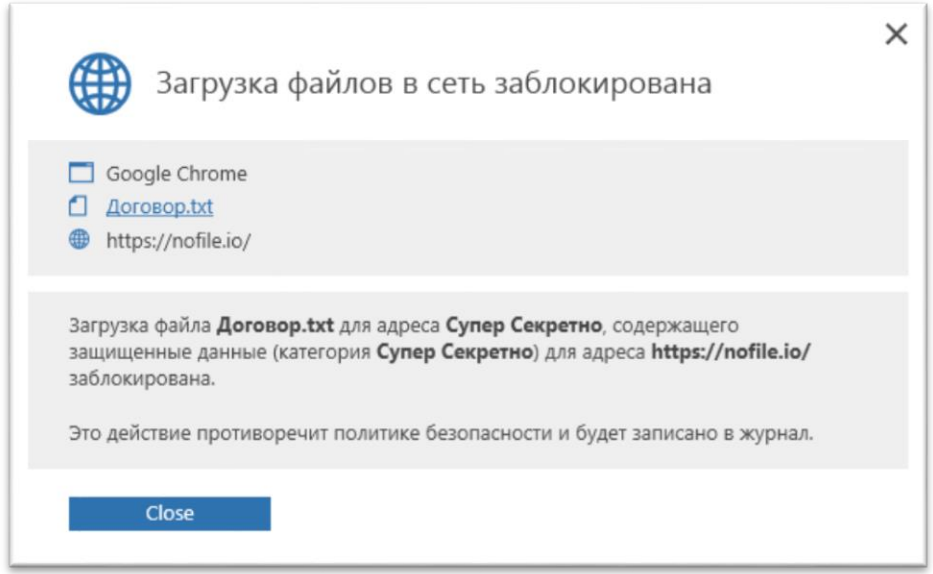




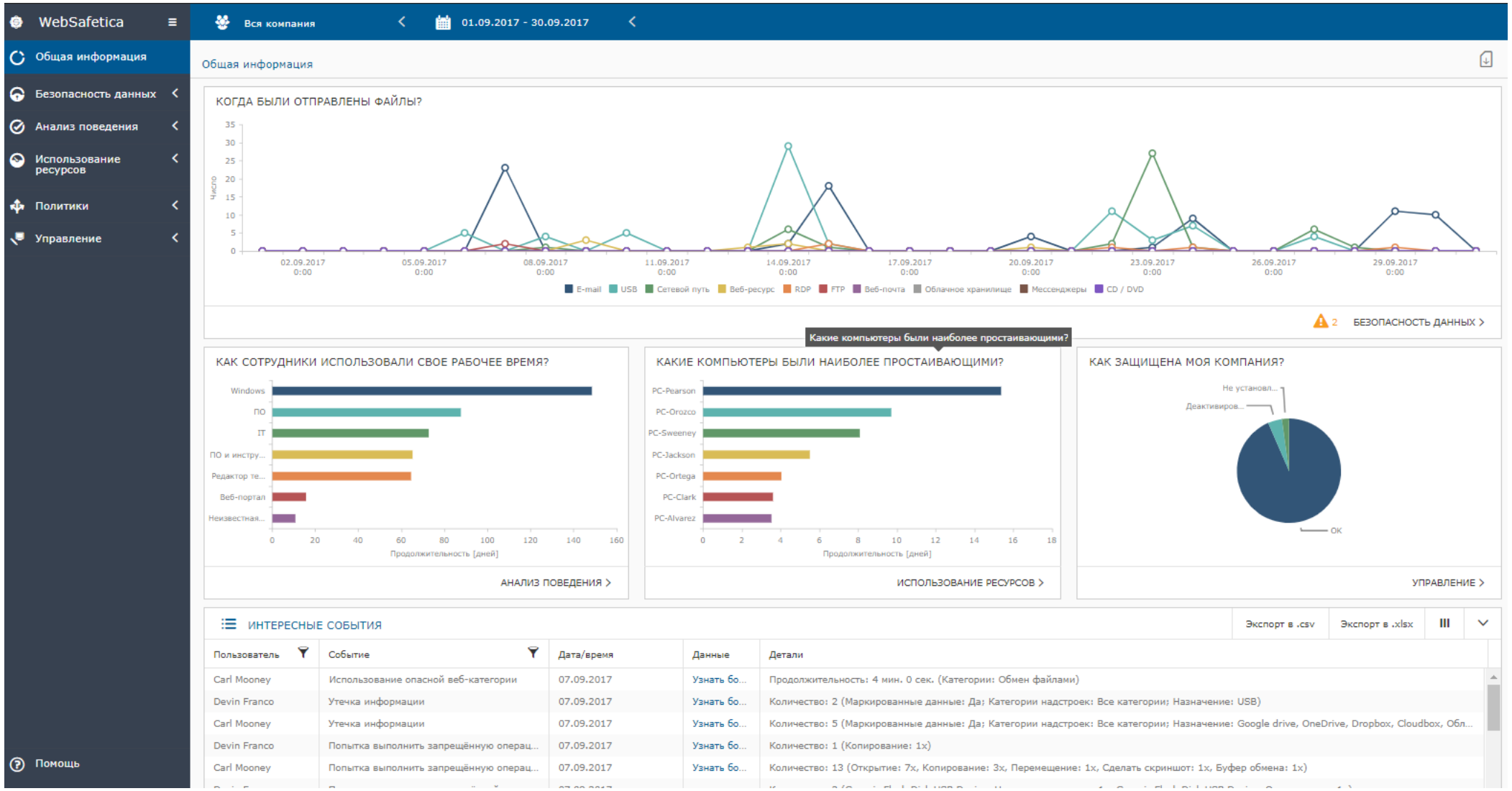
ОТЧЕТНОСТЬ И БЛОКИРОВКА ДЕЯТЕЛЬНОСТИ



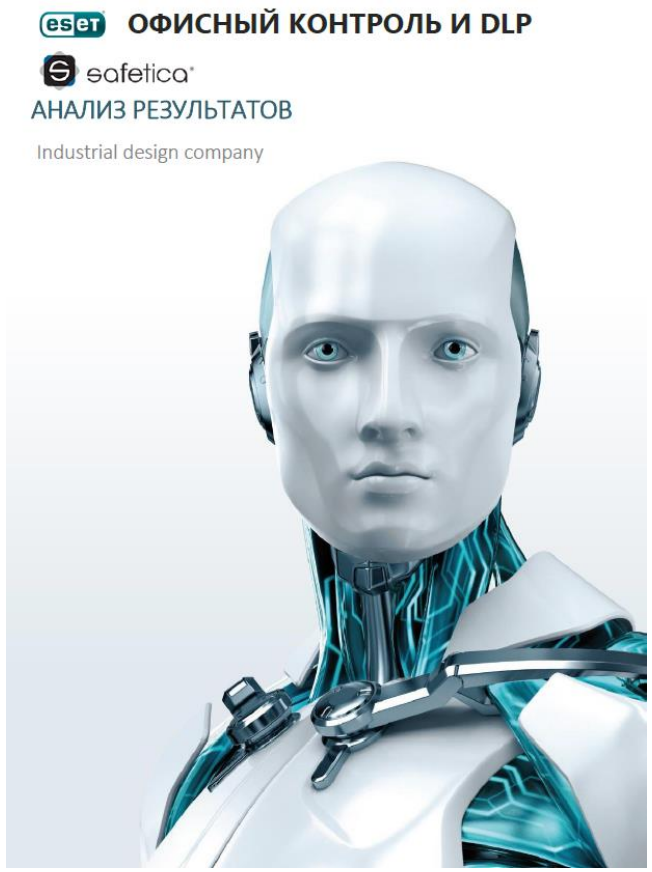




АНАЛИЗ РЕЗУЛЬТАТОВ В ВЕБ КОНСОЛИ WEBSAFETICA



РЕЗУЛЬТАТЫ ВНЕДРЕНИЯ



✓ 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*

ЛИЦЕНЗИРОВАНИЕ
И ЦЕНЫ

› АУДИТОР

SAF-AUD-NS-1-99	167 094 ₽

› ОФИСНЫЙ КОНТРОЛЬ

SAF-SOC-NS-1-99	241 410 ₽

› FULL DLP

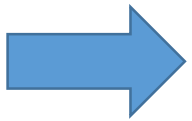
SAF-DLP-NS-1-99	371 405 ₽

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



ЭКСПЛОЙТ НУЛЕВОГО ДНЯ


eset
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	178B
КАТЕГОРИЯ	Сценарий

Обнаруженное поведение

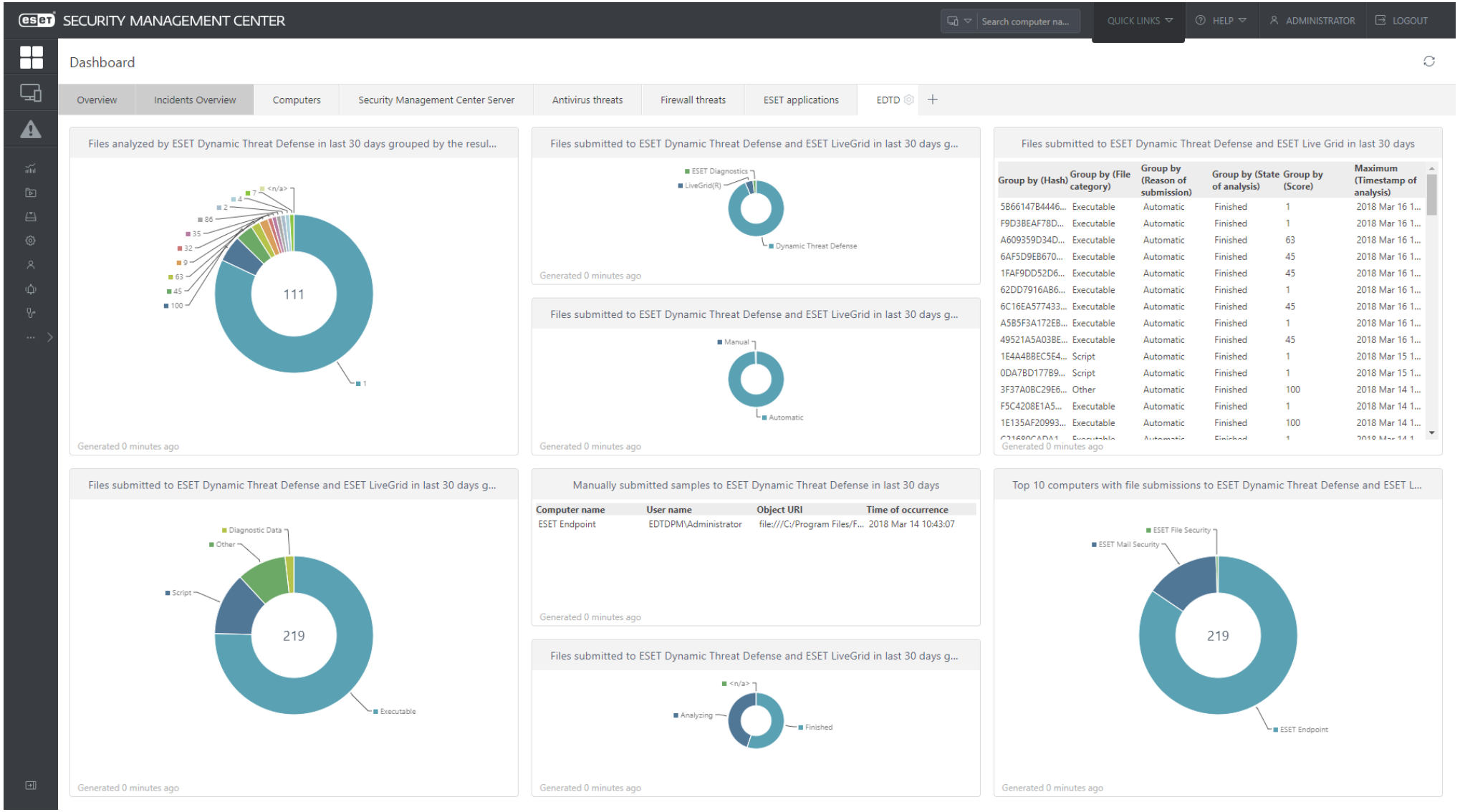
ПОВЕДЕНИЕ	**Создание службы**
ОБЪЯСНЕНИЕ	Образец пытался создать новую службу. Службы — это программы, раб режиме
ПОЛЕЗНЫЕ ДЕЙСТВИЯ	Это стандартное поведение для некоторых системных служебных прогр
ВРЕДОНОСНЫЕ ДЕЙСТВИЯ	Вредоносная программа пытается запуститься после перезагрузки систе

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

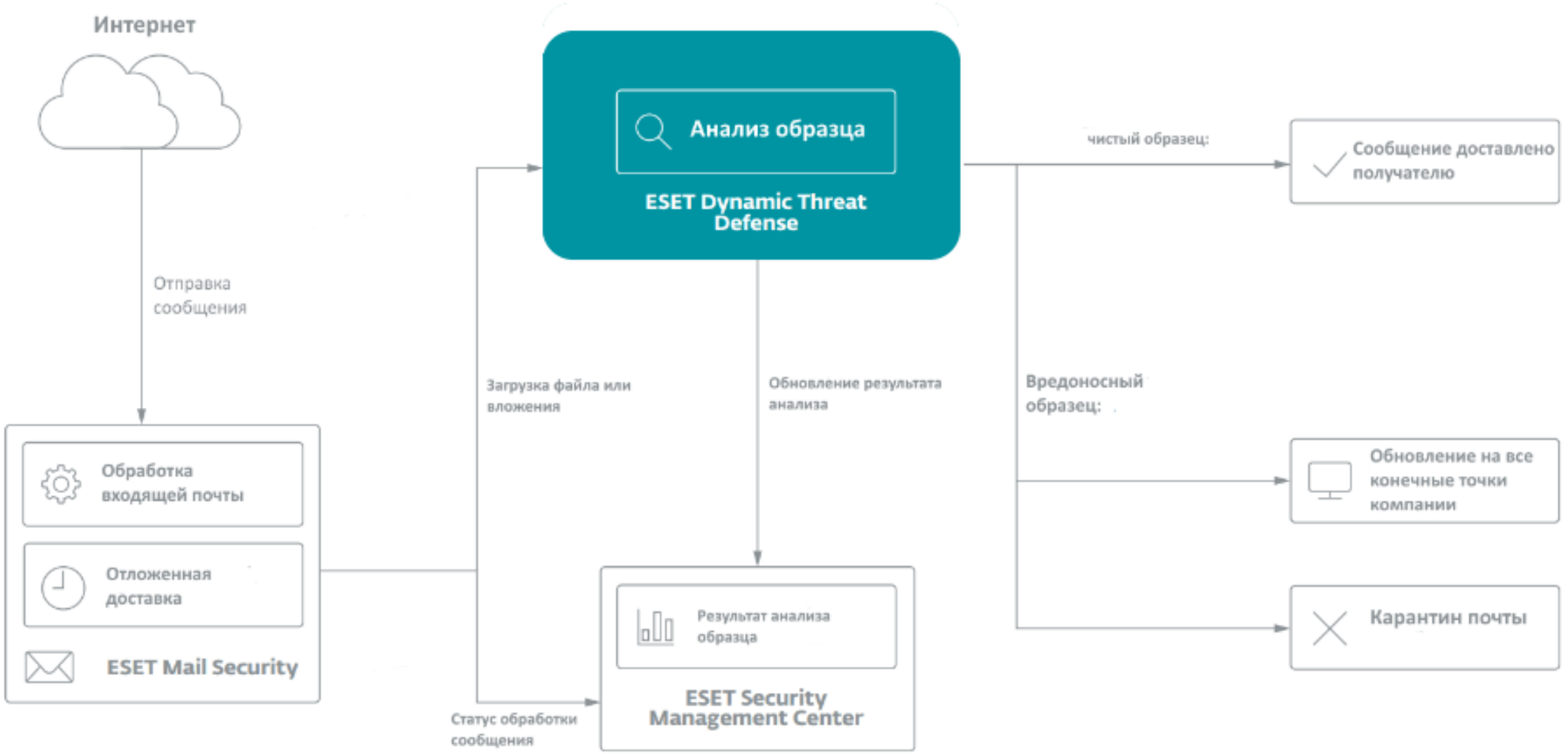
ПОВЕДЕНИЕ	**Повышение привилегий**
ОБЪЯСНЕНИЕ	Образец попытался повысить собственные привилегии для получения п или доступа к системе.
ПОЛЕЗНЫЕ ДЕЙСТВИЯ	Это стандартное поведение для некоторых установщиков
ВРЕДОНОСНЫЕ	

eset АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ЦЕНТРАЛИЗОВАННЫЙ СБОР ОТЧЕТОВ И УПРАВЛЕНИЕ В ЕДИНОЙ КОНСОЛИ



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?