# КАК ОБЕСПЕЧИТЬ ЗАЩИТУ КОМПАНИИ ОТ ВНЕШНИХ И ВНУТРЕННИХ УГРОЗ?

Дмитрий Самойленко
*ESET ЮФО/СКФО/ЦФО*

# СОДЕРЖАНИЕ



# СТАТИСТИКА ИНСТИТУТА AV-TEST

## ИЗВЕСТНЫЕ УГРОЗЫ

- **390 000 шт. в день**

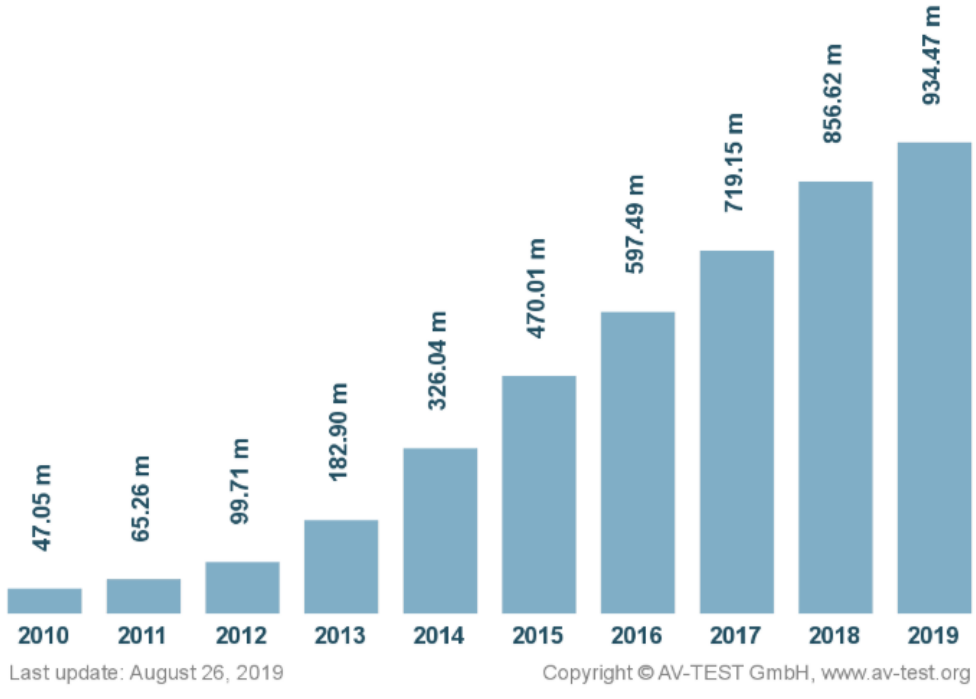
  *Новых образцов*

  *вредоносных программ  каждый день*

- **Новые способы**

  *Новые способы обхода обнаружения*

**x3 с 2014г**

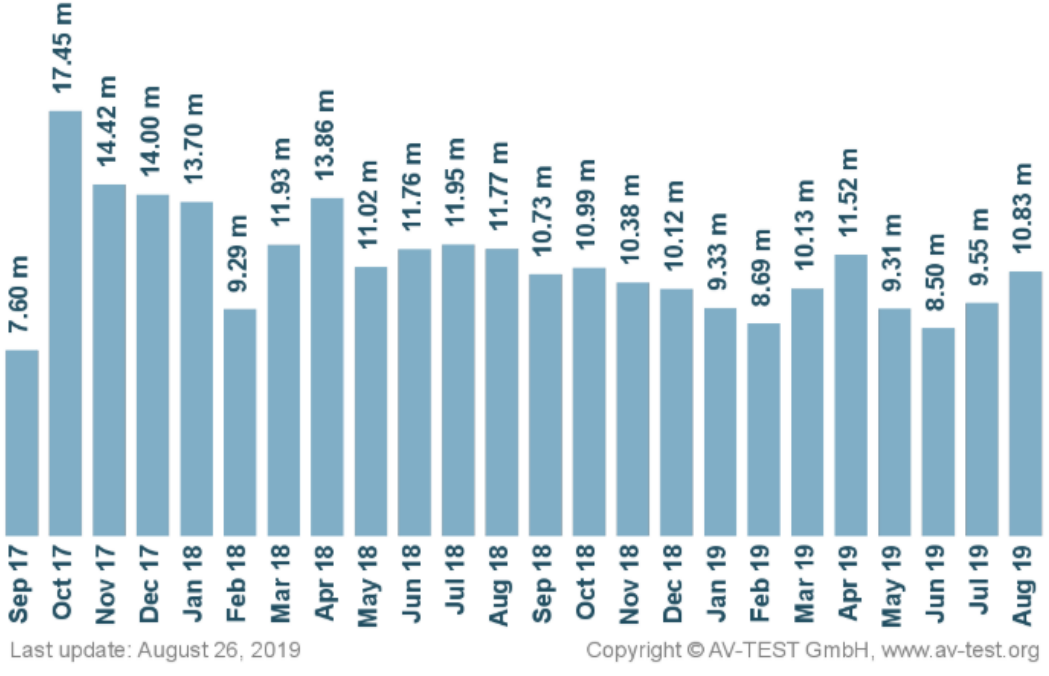



*Источник: av-test.org, статистика вредоносных программ на 26 августа 2019г.*

eset АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

# УГРОЗЫ ПРОГРЕССИРУЮТ И СТАНОВЯТСЯ СЛОЖНЕЕ

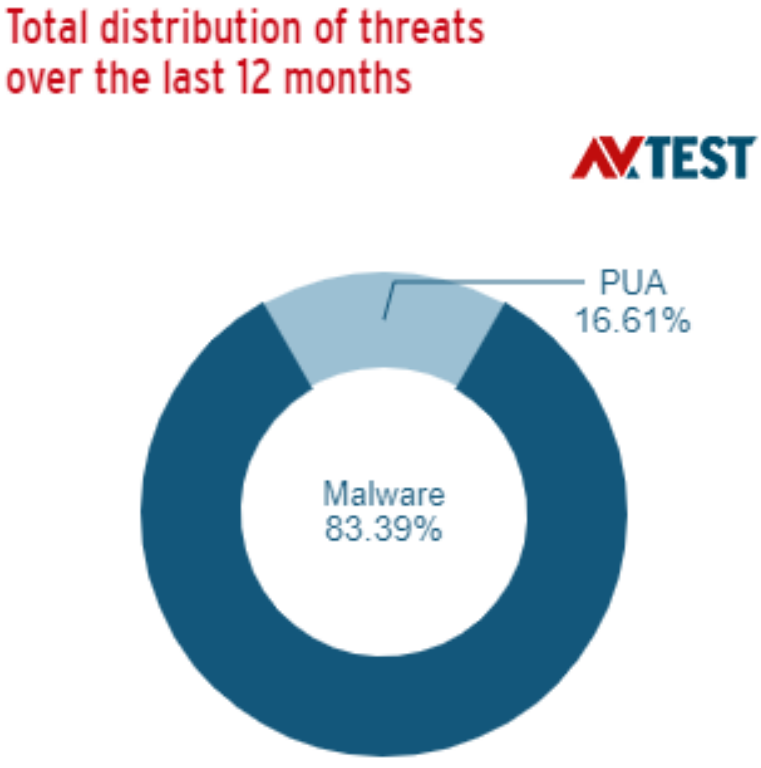
## Новые угрозы




*Источник: av-test.org, статистика вредоносных программ на 26 августа 2019г*

eset АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

# РАСПРЕДЕЛЕНИЕ УГРОЗ ЗА 12 МЕСЯЦЕВ






*Источник: av-test.org, статистика вредоносных программ на 26 августа 2019г*

# 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 ВНЕШНИХ УГРОЗ?

АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

# Архитектура адаптивной защиты

# Как ESET вписывается в адаптивную защиту


## ПРОГНОЗИРОВАНИЕ

ESET Threat Intelligence

ESET Virus Radar

WeLive Security

## ПРЕДОТВРАЩЕНИЕ

ESET Endpoint Security/ESET Endpoint Antivirus

ESET Virtualization Security

ESET Security Management Center

ESET Secure Authentication

## РЕАГИРОВАНИЕ

ESET Security Management Center

NEW ESET Enterprise Inspector

NEW ESET Dynamic Threat Defense

## ОБНАРУЖЕНИЕ

ESET Endpoint Security/ESET Endpoint Antivirus

ESET Security Management Center

ESET Enterprise Inspector NEW

ESET Dynamic Threat Defense NEW

# КОМПЛЕКСНЫЕ РЕШЕНИЯ ESET.

## 7-Е ПОКОЛЕНИЕ КОРПОРАТИВНЫХ ПРОДУКТОВ

NEW

### ESET DYNAMIC MAIL PROTECTION

NEW

### ESET ENDPOINT PROTECTION PLUS

NEW

### ESET DYNAMIC ENDPOINT PROTECTION

NEW

### ESET ENTERPRISE THREAT DEFENSE

**НАДЕЖНОСТЬ**

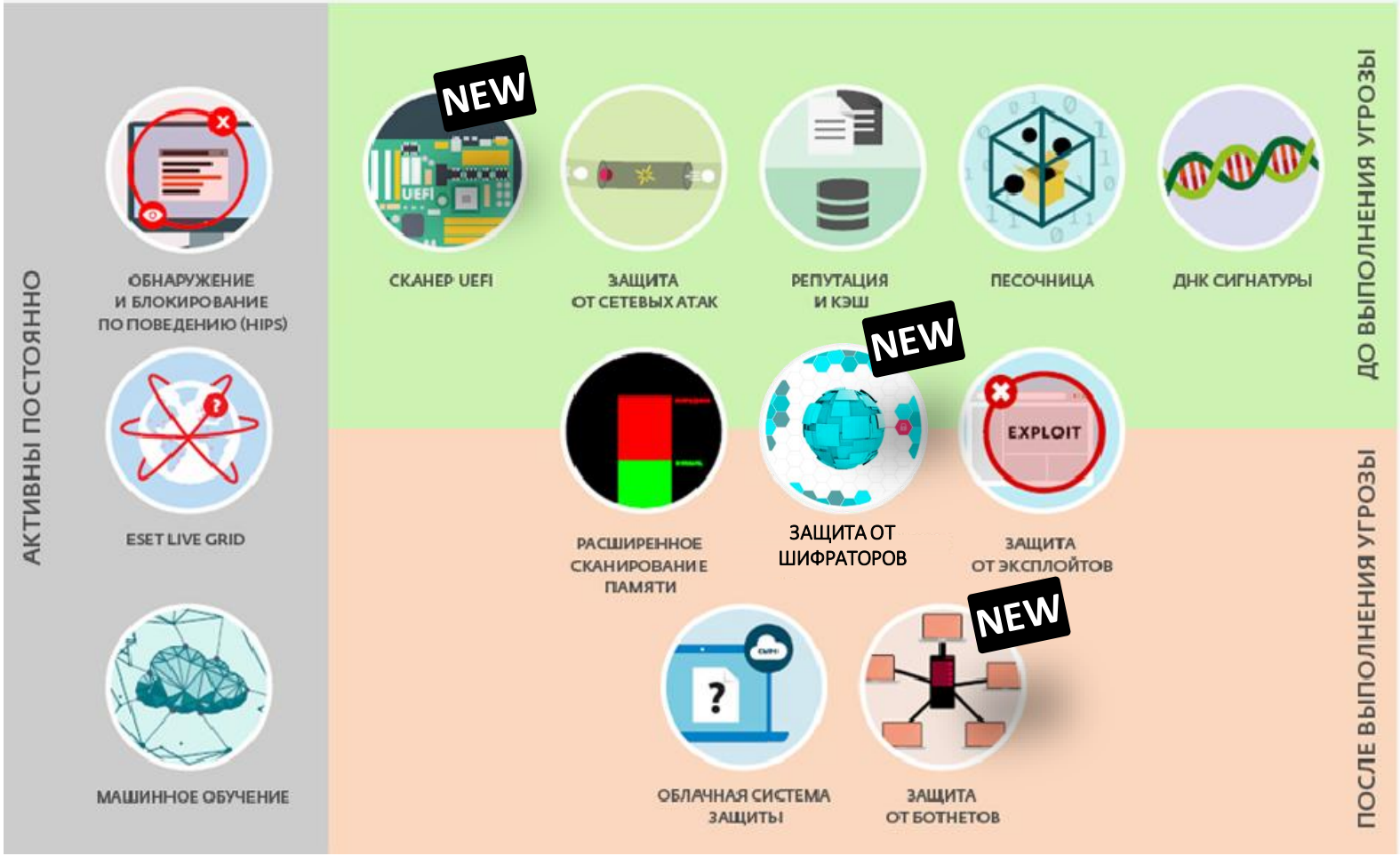
**БЫСТРОДЕЙСТВИЕ**

**УДОБСТВО В РАБОТЕ**

eset АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

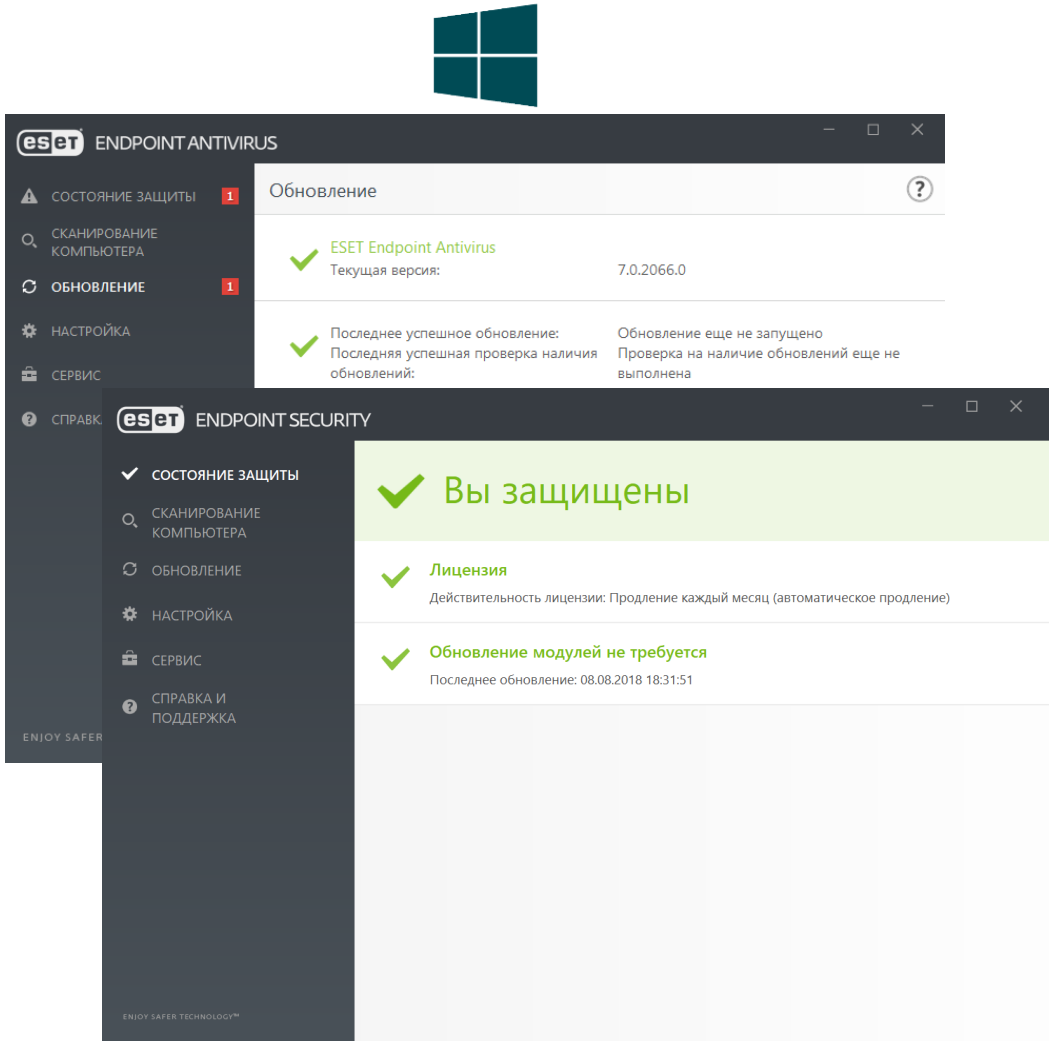
# НАДЕЖНОСТЬ! 7-ОЕ ПОКОЛЕНИЕ

## МНОГОУРОВНЕВАЯ ЗАЩИТА ТЕХНОЛОГИЯМИ ESET



# ESET ENDPOINT SECURITY
# ESET ENDPOINT ANTIVIRUS

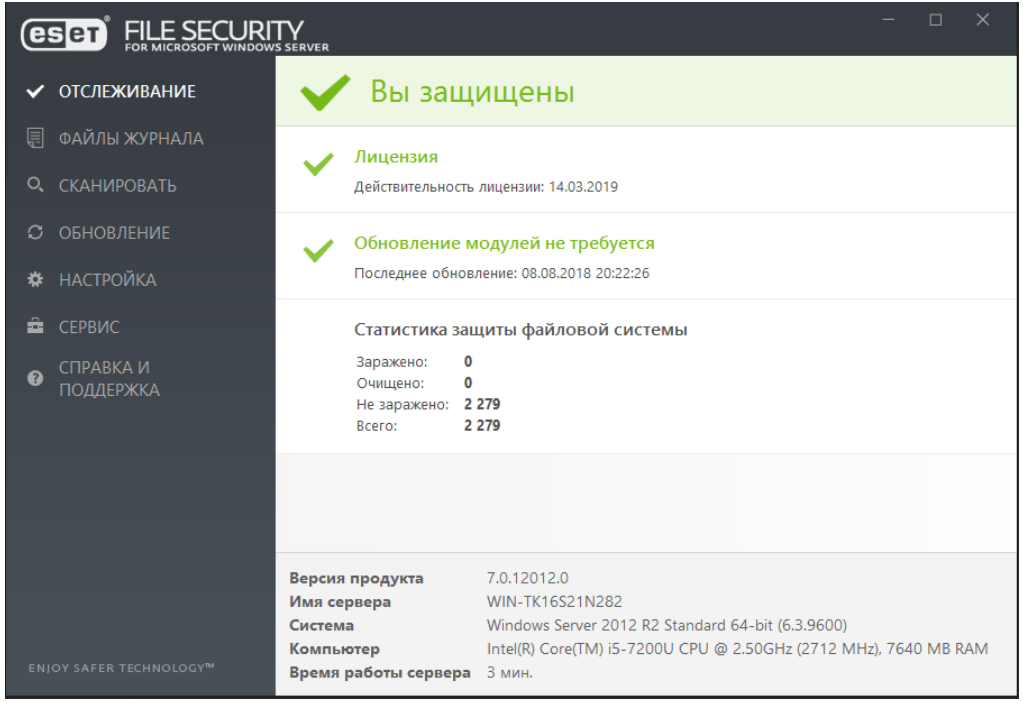
- ✓ *Поддержка **ESET Dynamic Threat Defense***
- ✓ ***Планировщик** для контроля устройств и веб-контроля*




АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

# ESET FILE SECURITY ДЛЯ WINDOWS SERVER

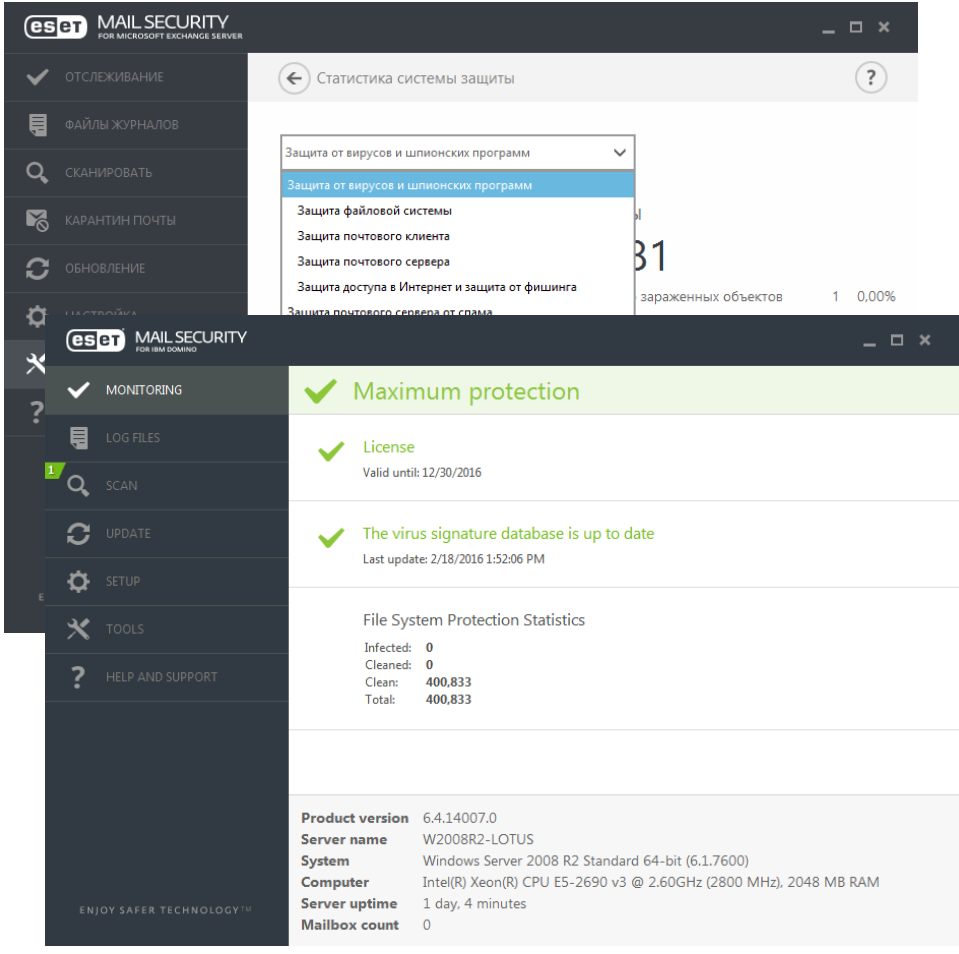
- ✓ *Поддержка Microsoft **Office 365***
- ✓ Защита от сетевых атак (IDS)
- ✓ *Поддержка **ESET Dynamic Threat Defense***
- ✓ *Добавление исключений по **хэшу файлов***
- ✓ ***64-битное** ядро сканирования*




eset АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

# ESET MAIL SECURITY ДЛЯ EXCHANGE SERVER/IBM DOMINO

- ✓ ***Уведомление администратора*** *о карантине*
- ✓ *Защита* ***Backscatter*** (D)
- ✓ *Поддержка Microsoft* ***Office 365***
- ✓ Защита от сетевых атак (IDS)
- ✓ *Поддержка* ***ESET Dynamic Threat Defense*** (D)
- ✓ ***64-битное*** *ядро сканирования* (D)



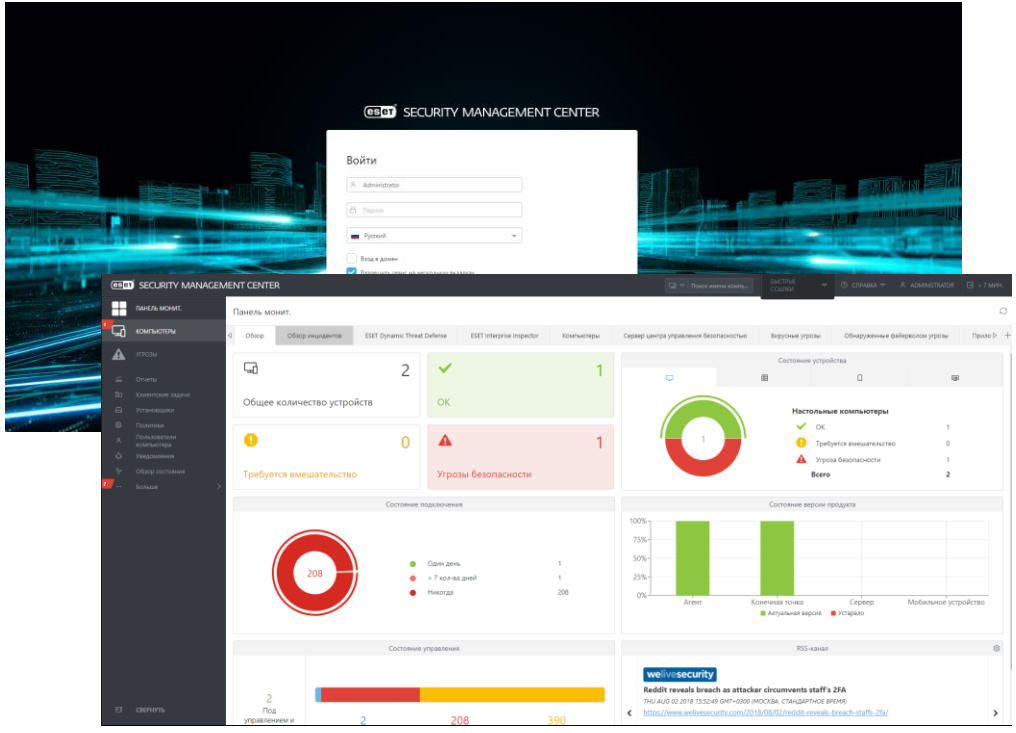

АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

# SECURITY MANAGEMENT CENTER

NEW

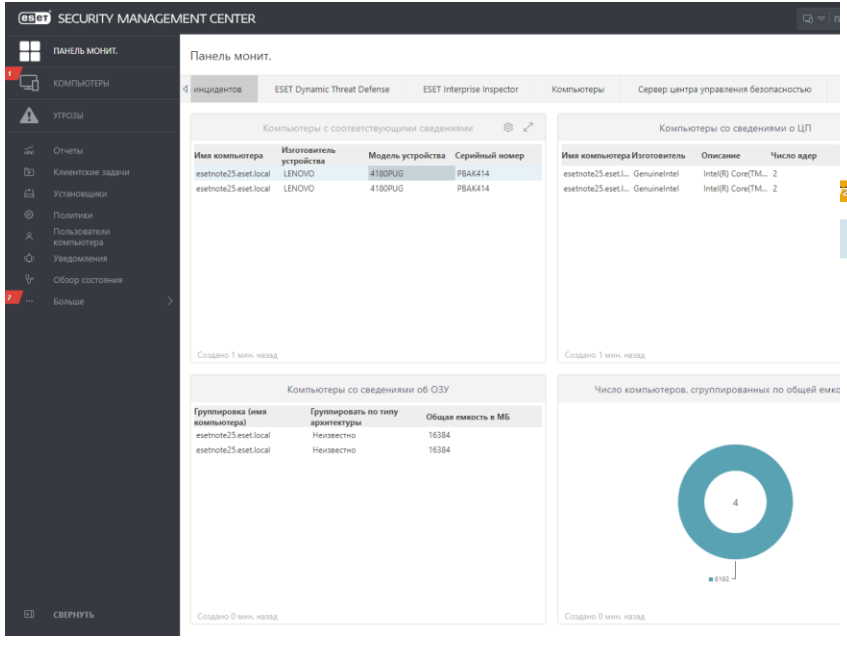
# ESET SECURITY MANAGEMENT CENTER

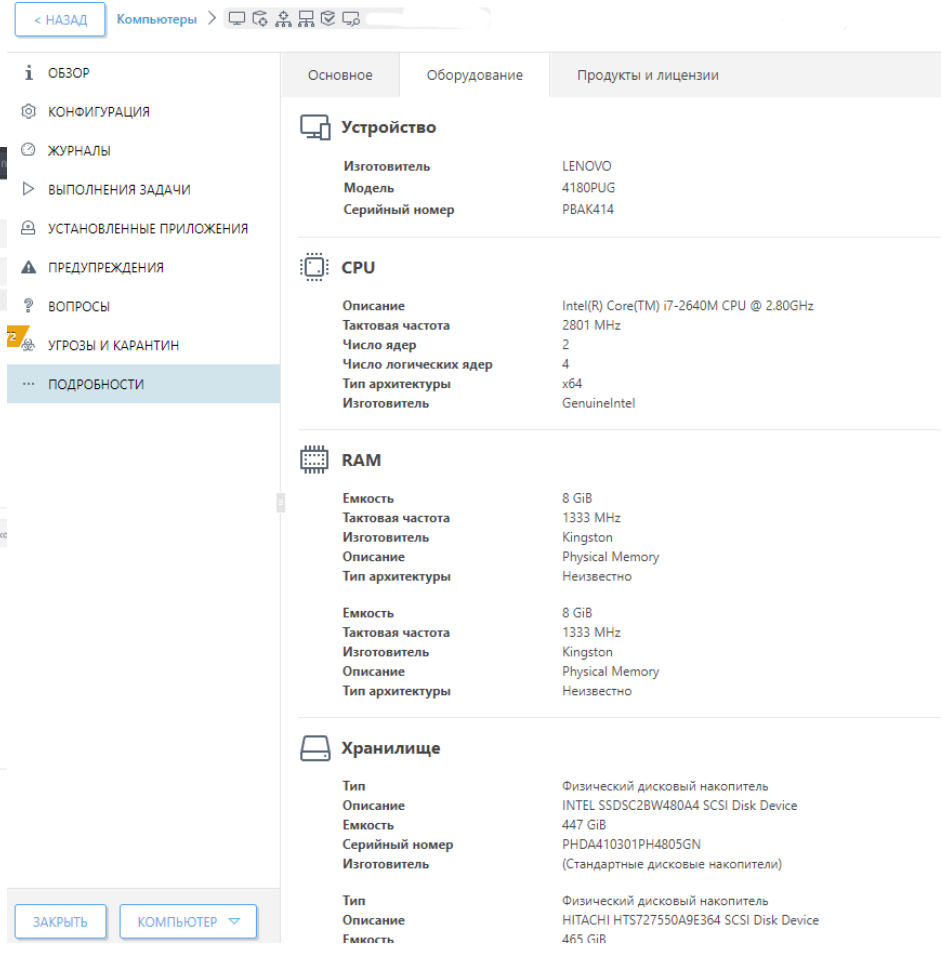
- ✓ *ESET Push Notification Service (**EPNS**)*
- ✓ *Автоматическое определение «**клонов**»*
- ✓ ***Инвентаризация** оборудования*
- ✓ *Поддержка **ESET Enterprise Inspector***
- ✓ *Поддержка **ESET Dynamic Threat Defense***



# ESET SECURITY MANAGEMENT CENTER

✓ ***Инвентаризация*** *оборудования*




eset АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

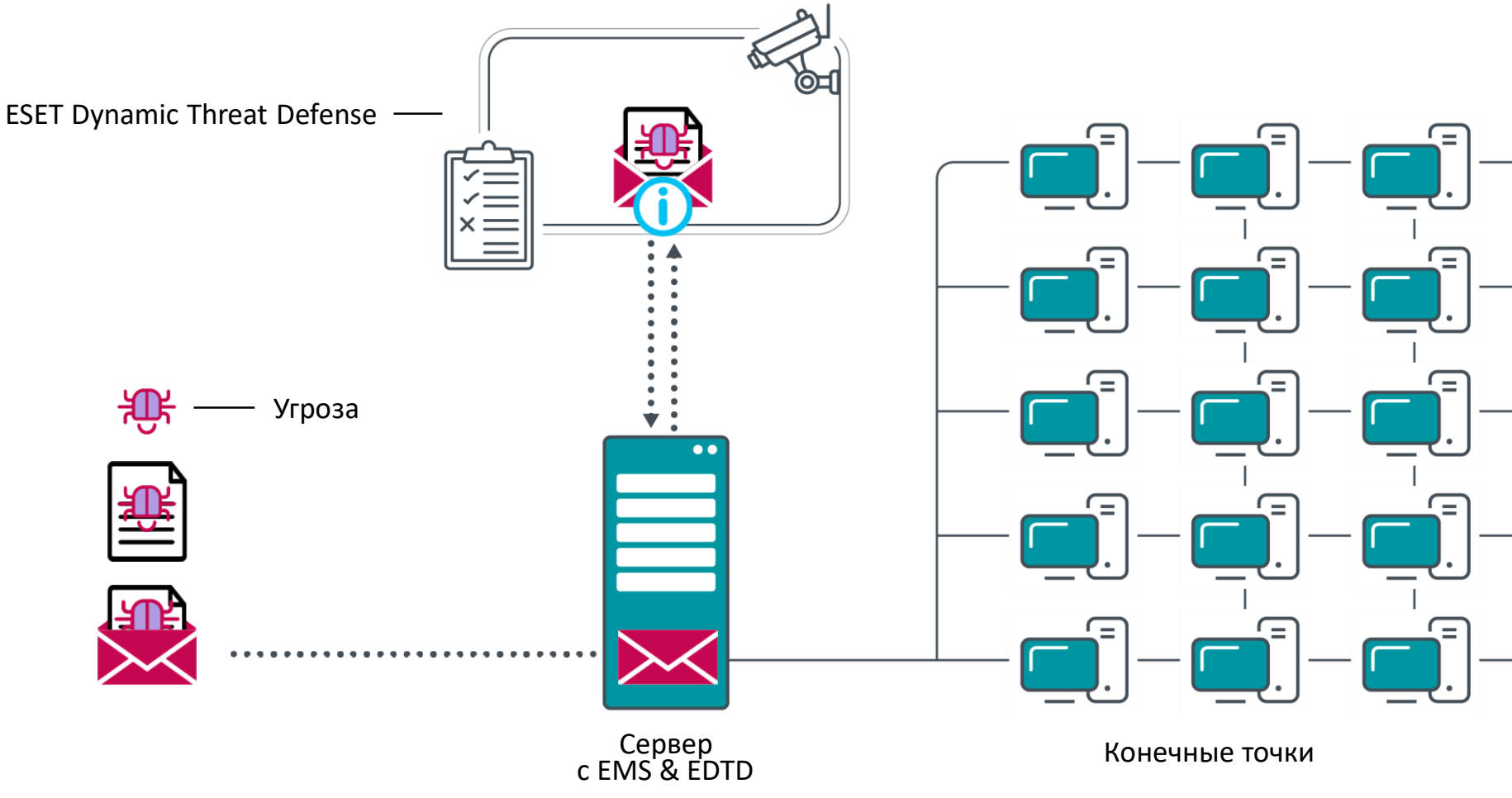
# Песочница

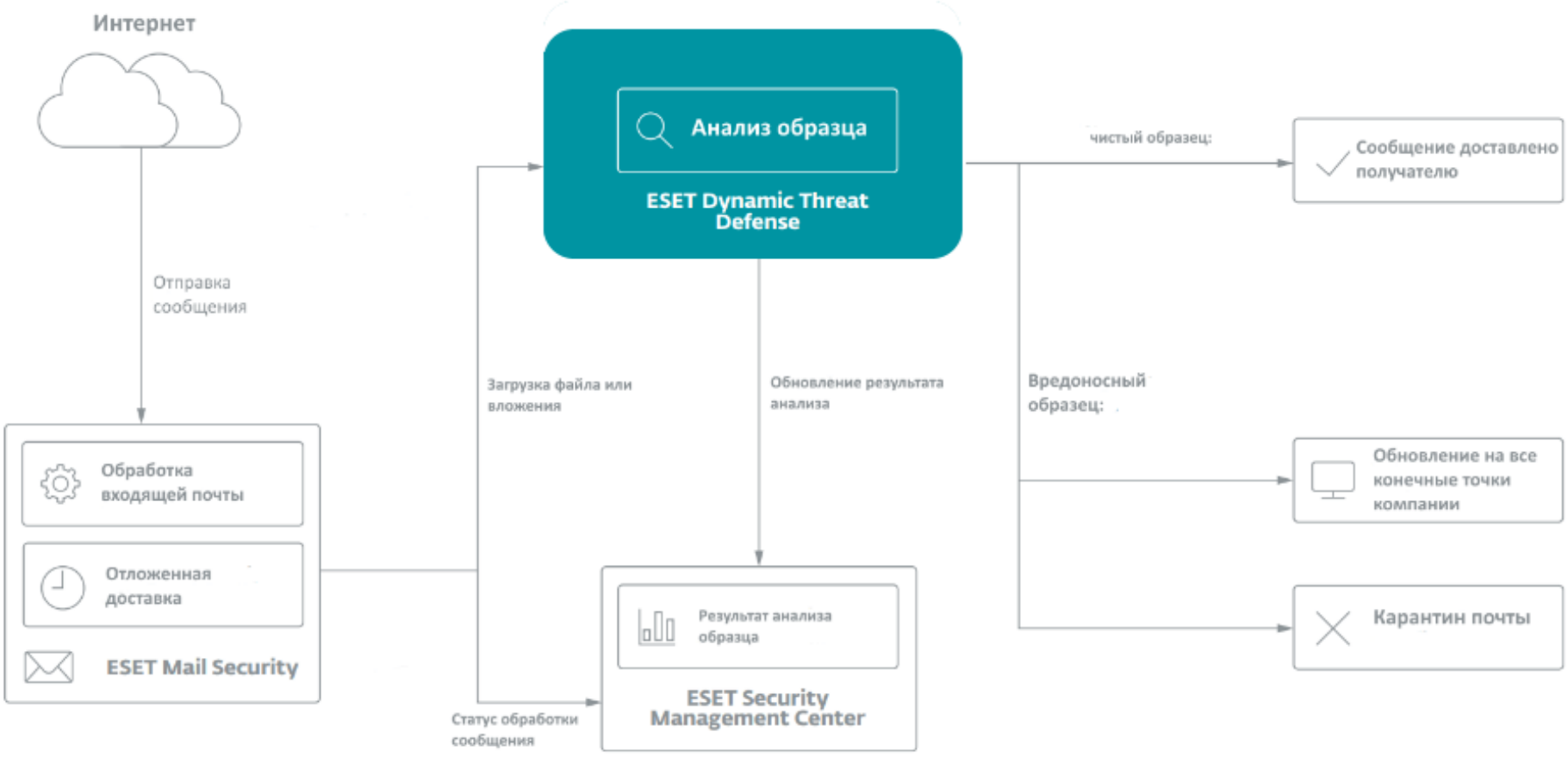
NEW

ESET DYNAMIC THREAT DEFENSE

# ESET DYNAMIC THREAT DEFENSE

- ✓ ***Облачная*** *песочница, встроенная в антивирус*
- ✓ ***Автоматическая*** *защита*
- ✓ **Многоуровневое** *обнаружение угроз*
- ✓ **Мобильность**
- ✓ **Скорость**
- ✓ **Детальный обзор**

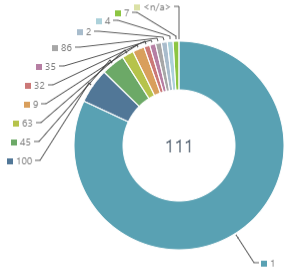

ESET Dynamic Threat Defense
Угроза
Сервер
с EMS & EDTD
Конечные точки


Интернет
Отправка сообщения
Обработка входящей почты
Отложенная доставка
ESET Mail Security
Загрузка файла или вложения
Статус обработки сообщения
Анализ образца
ESET Dynamic Threat Defense
Обновление результата анализа
Результат анализа образца
ESET Security Management Center
чистый образец:
Сообщение доставлено получателю
Вредоносный образец:
Обновление на все конечные точки компании
Карантин почты

# Dashboard

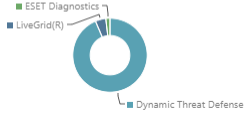


## Files analyzed by ESET Dynamic Threat Defense in last 30 days grouped by the resul...



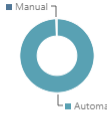

Generated 0 minutes ago

## 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 LiveGrid in last 30 days g...



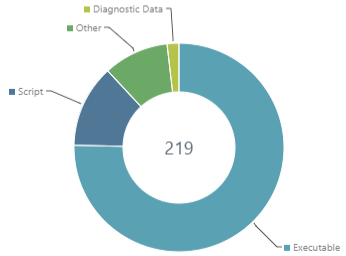

Generated 0 minutes ago

## 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... |
| 62DD7916AB6... | 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... |
| 1E4A4BBEC5E4... | Script | Automatic | Finished | 1 | 2018 Mar 15 1... |
| 0DA7BD177B9... | 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... |

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

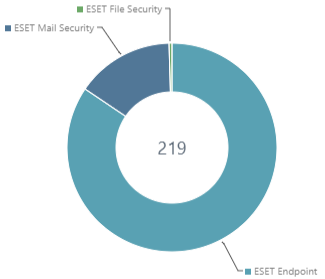
| Computer name | User name | Object URI | Time of occurrence |
|---|---|---|---|
| ESET Endpoint | EDTDPM\Administrator | file:///C:/Program Files/F... | 2018 Mar 14 10:43:07 |

Generated 0 minutes ago

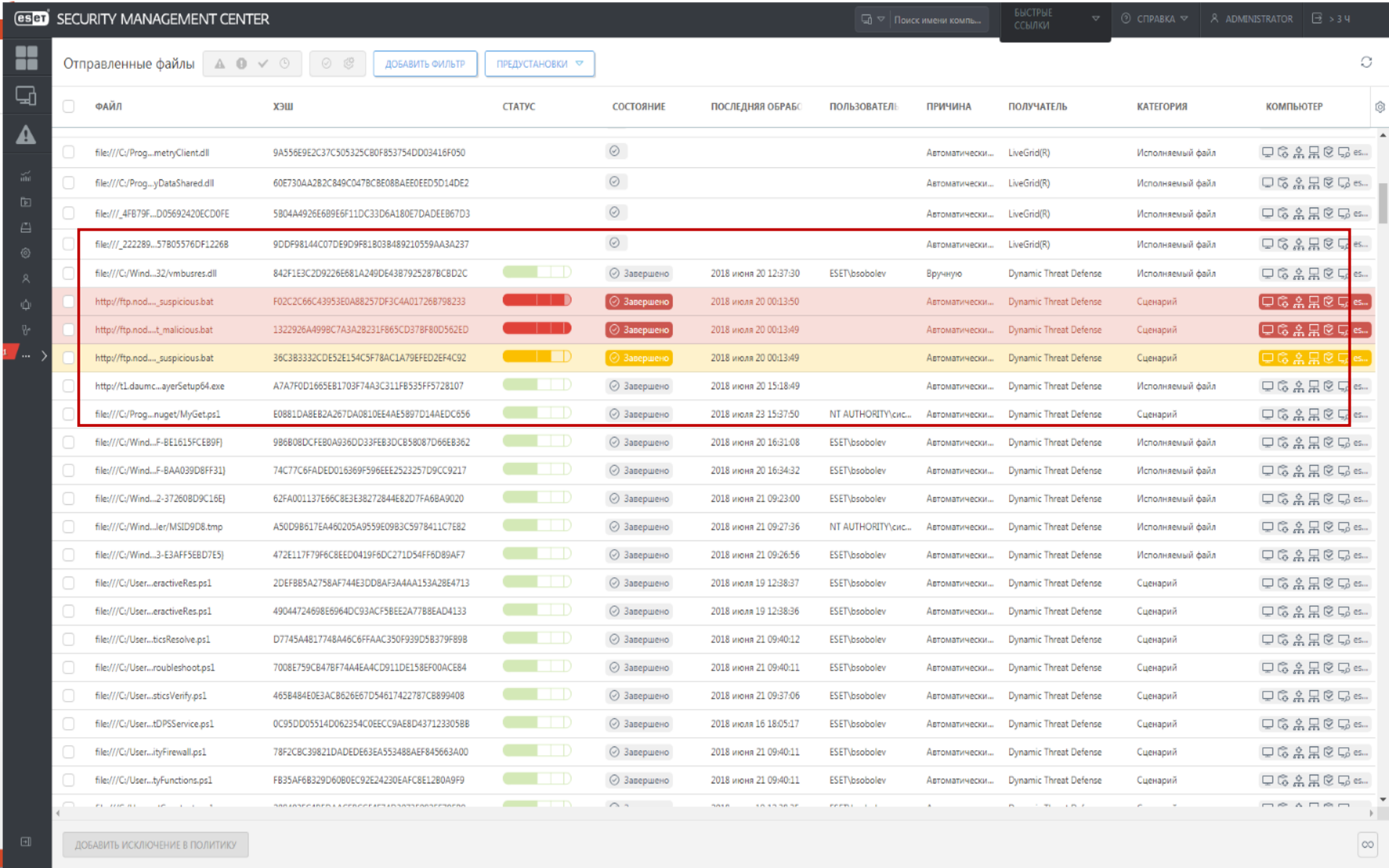
## Files submitted to ESET Dynamic Threat Defense and ESET LiveGrid in last 30 days g...

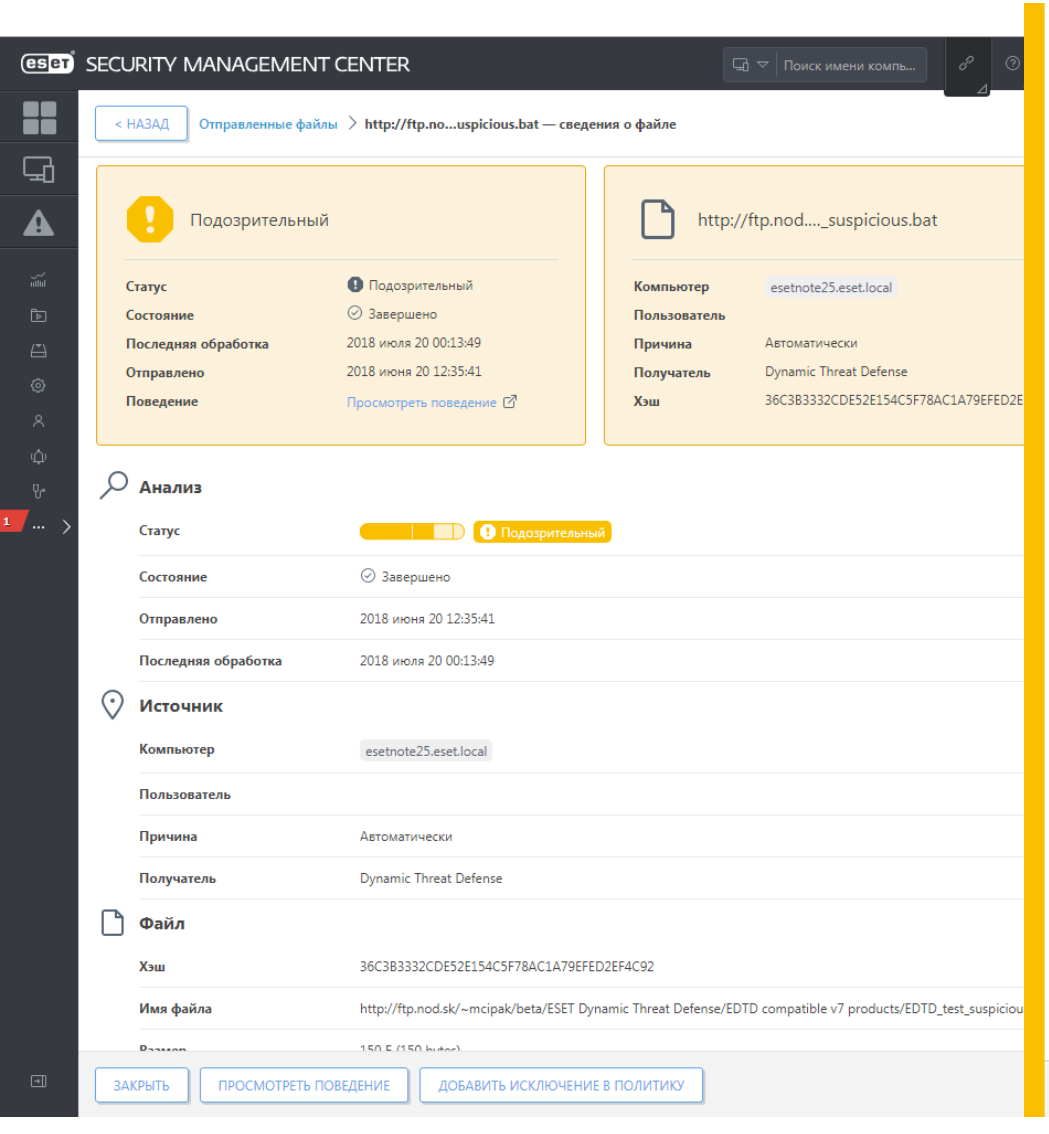

Generated 0 minutes ago

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




Generated 0 minutes ago


SECURITY MANAGEMENT CENTER
Поиск имени компь...
БЫСТРЫЕ ССЫЛКИ
СПРАВКА
ADMINISTRATOR
Отправленные файлы
ДОБАВИТЬ ФИЛЬТР
ПРЕДУСТАНОВКИ
ФАЙЛ
ХЭШ
СТАТУС
СОСТОЯНИЕ
ПОСЛЕДНЯЯ ОБРАБ
ПОЛЬЗОВАТЕЛ
ПРИЧИНА
ПОЛУЧАТЕЛЬ
КАТЕГОРИЯ
КОМПЬЮТЕР
file:///C:/Prog...metryClient.dll 9A556E9E2C37C505325CB0F853754DD03416F050 Автоматически... LiveGrid(R) Исполняемый файл
file:///C:/Prog...yDataShared.dll 60E730AA2B2C849C047BCBE08BAEE0EED5D14DE2 Автоматически... LiveGrid(R) Исполняемый файл
file:///_4FB79F...D05692420ECD0FE 5B04A4926E689E6F11DC33D6A180E7DADEEB67D3 Автоматически... LiveGrid(R) Исполняемый файл
file:///_222289...57B05576DF12268 9DDF98144C07DE9D9F81B03B489210559AA3A237 Автоматически... LiveGrid(R) Исполняемый файл
file:///C:/Wind...32/vmbusres.dll 842F1E3C2D9226E681A249DE43B7925287BCBD2C Завершено 2018 июня 20 12:37:30 ESET\bsobolev Вручную Dynamic Threat Defense Исполняемый файл
http://ftp.nod..._suspicious.bat F02C2C66C43953E0A88257DF3C4A017268798233 Завершено 2018 июля 20 00:13:50 Автоматически... Dynamic Threat Defense Сценарий
http://ftp.nod...t_malicious.bat 1322926A499BC7A3A2B231F865CD378F80D562ED Завершено 2018 июля 20 00:13:49 Автоматически... Dynamic Threat Defense Сценарий
http://ftp.nod..._suspicious.bat 36C3B3332CDE52E154C5F78AC1A79EFED2EF4C92 Завершено 2018 июля 20 00:13:49 Автоматически... Dynamic Threat Defense Сценарий
http://t1.daumc...ayerSetup64.exe A7A7F0D1665EB1703F74A3C311FB535FF5728107 Завершено 2018 июля 20 15:18:49 Автоматически... Dynamic Threat Defense Исполняемый файл
file:///C:/Prog...nuget/MyGet.ps1 E0881DA8EB2A267DA0810EE4AE5897D14AEDC656 Завершено 2018 июля 23 15:37:50 NT AUTHORITY\сис... Автоматически... Dynamic Threat Defense Сценарий
file:///C:/Wind...F-BE1615FCEB9F} 986B08DCFEB0A936DD33FEB3DCB58087D66EB362 Завершено 2018 июня 20 16:31:08 ESET\bsobolev Автоматически... Dynamic Threat Defense Исполняемый файл
file:///C:/Wind...F-BAA039D8FF31} 74C77C6FADED016369F596EEE2523257D9CC9217 Завершено 2018 июня 20 16:34:32 ESET\bsobolev Автоматически... Dynamic Threat Defense Исполняемый файл
file:///C:/Wind...2-372608D9C16E} 62FA001137E66C8E3E38272844E82D7FA6BA9020 Завершено 2018 июня 21 09:23:00 ESET\bsobolev Автоматически... Dynamic Threat Defense Исполняемый файл
file:///C:/Wind...ler/MSID9D8.tmp A50D9B617EA460205A9559E09B3C5978411C7E82 Завершено 2018 июня 21 09:27:36 NT AUTHORITY\сис... Автоматически... Dynamic Threat Defense Исполняемый файл
file:///C:/Wind...3-E3AFF5EBD7E5} 472E117F79F6C8EED0419F6DC271D54FF6D89AF7 Завершено 2018 июня 21 09:26:56 ESET\bsobolev Автоматически... Dynamic Threat Defense Исполняемый файл
file:///C:/User...eractiveRes.ps1 2DEFBB5A2758AF744E3DD8AF3A4AA153A28E4713 Завершено 2018 июля 19 12:38:37 ESET\bsobolev Автоматически... Dynamic Threat Defense Сценарий
file:///C:/User...eractiveRes.ps1 4904472469BE6964DC93ACF5BEE2A77B8EAD4133 Завершено 2018 июля 19 12:38:36 ESET\bsobolev Автоматически... Dynamic Threat Defense Сценарий
file:///C:/User...ticsResolve.ps1 D7745A4817748A46C6FFAAC350F939D5B379F89B Завершено 2018 июня 21 09:40:12 ESET\bsobolev Автоматически... Dynamic Threat Defense Сценарий
file:///C:/User...roubleshoot.ps1 7008E759CB47BF74A4EA4CD911DE158EF00ACE84 Завершено 2018 июня 21 09:40:11 ESET\bsobolev Автоматически... Dynamic Threat Defense Сценарий
file:///C:/User...sticsVerify.ps1 465B484E0E3ACB626E67D54617422787CB899408 Завершено 2018 июня 21 09:37:06 ESET\bsobolev Автоматически... Dynamic Threat Defense Сценарий
file:///C:/User...tDPSService.ps1 0C95DD05514D062354C0EECC9AE8D437123305BB Завершено 2018 июля 16 18:05:17 ESET\bsobolev Автоматически... Dynamic Threat Defense Сценарий
file:///C:/User...ityFirewall.ps1 78F2CBC39821DADEDE63EA553488AEF845663A00 Завершено 2018 июня 21 09:40:11 ESET\bsobolev Автоматически... Dynamic Threat Defense Сценарий
file:///C:/User...tyFunctions.ps1 FB35AF6B329D60B0EC92E24230EAFC8E12B0A9F9 Завершено 2018 июня 21 09:40:11 ESET\bsobolev Автоматически... Dynamic Threat Defense Сценарий
ДОБАВИТЬ ИСКЛЮЧЕНИЕ В ПОЛИТИКУ




# ОТЧЕТ О ПОВЕДЕНИИ ФАЙЛОВ

| | |
|---|---|
| **СТАТУС** | **Подозрительный** |
| **SHA-1** | 36C3B3332CDE52E154C5F78AC1A79EFED2EF4C92 |
| **РАЗМЕР** | 150B |
| **КАТЕГОРИЯ** | Сценарий |

## Обнаруженное поведение

| | |
|---|---|
| **ПОВЕДЕНИЕ** | **Проанализированный образец скопирован.** |
| **ОБЪЯСНЕНИЕ** | Образец был скопирован в другое расположение. |
| **ПОЛЕЗНЫЕ ДЕЙСТВИЯ** | Это стандартное поведение для некоторых установщиков. |
| **ВРЕДОНОСНЫЕ ДЕЙСТВИЯ** | Вредоносная программа попыталась скрыть свое наличие. |

| | |
|---|---|
| **ПОВЕДЕНИЕ** | **Выполнение ADS.** |
| **ОБЪЯСНЕНИЕ** | Образец выполнил что-то из альтернативного потока данных (ADS). |
| **ПОЛЕЗНЫЕ ДЕЙСТВИЯ** | Это необычное поведение для чистых приложений. |
| **ВРЕДОНОСНЫЕ ДЕЙСТВИЯ** | Вредоносная программа попыталась скрыть свое наличие. |

| | |
|---|---|
| **ПОВЕДЕНИЕ** | **Внедрение кода в запущенный процесс.** |
| **ОБЪЯСНЕНИЕ** | Образец пытался внедрить код в запущенный процесс. |
| **ПОЛЕЗНЫЕ ДЕЙСТВИЯ** | Это стандартное поведение для некоторых системных служебных программ. |
| **ВРЕДОНОСНЫЕ ДЕЙСТВИЯ** | Вредоносная программа попыталась скрыть свое наличие. |

| | |
|---|---|
| **ПОВЕДЕНИЕ** | **Сетевые подключения.** |
| **ОБЪЯСНЕНИЕ** | Образец пытался обмениваться данными с другим компьютером через сеть или прослушивать подключения других компьютеров. |
| **ПОЛЕЗНЫЕ ДЕЙСТВИЯ** | Чистые образцы используют сетевые подключения для загрузки контента. |

# ОТЧЕТ О ПОВЕДЕНИИ ФАЙЛОВ

| | |
|---|---|
| СТАТУС | Вредоносные программы |
| SHA-1 | 1322926A499BC7A3A2B231F865CD37BF80D562ED |
| РАЗМЕР | 225B |
| КАТЕГОРИЯ | Сценарий |

## Обнаруженное поведение

| | |
|---|---|
| ПОВЕДЕНИЕ | **Обнаружен заблокированный URL-адрес.** |
| ОБЪЯСНЕНИЕ | Образец связался с URL-адресом, заблокированным ESET. |
| ПОЛЕЗНЫЕ ДЕЙСТВИЯ | Чистые приложения не должны этого делать. |
| ВРЕДОНОСНЫЕ ДЕЙСТВИЯ | Вредоносная программа связалась с сервером злоумышленников. |

| | |
|---|---|
| ПОВЕДЕНИЕ | **Вредоносная программа обнаружена без выполнения.** |
| ОБЪЯСНЕНИЕ | Образец определен как вредоносная программа без выполнения. |
| ПОЛЕЗНЫЕ ДЕЙСТВИЯ | Чистые приложения не должны этого делать. |
| ВРЕДОНОСНЫЕ ДЕЙСТВИЯ | Вредоносная программа обнаружена модулем сканирования ESET без выполнения. |

| | |
|---|---|
| ПОВЕДЕНИЕ | **Вредоносная программа обнаружена после выполнения.** |
| ОБЪЯСНЕНИЕ | Образец определен как вредоносная программа после выполнения. |
| ПОЛЕЗНЫЕ ДЕЙСТВИЯ | Чистые приложения не должны этого делать. |
| ВРЕДОНОСНЫЕ ДЕЙСТВИЯ | Вредоносная программа обнаружена модулем сканирования ESET после выполнения. |

| | |
|---|---|
| ПОВЕДЕНИЕ | **Образец изменил запущенный процесс.** |
| ОБЪЯСНЕНИЕ | Образец вставил код в запущенный процесс надежных приложений. |
| ПОЛЕЗНЫЕ ДЕЙСТВИЯ | Это стандартное поведение для программ безопасности и контроля пользователей. |



# SAMPLE REPORT

| | |
|---|---|
| CLIENT | ESET RU |
| REPORT DATE | 2018-03-12 18:24:33 CET (UTC/GMT +01:00) |
| REPORT ID | 53553/2018 |

## Detection

| | |
|---|---|
| ESET | Win32/Filecoder.WannaCryptor.D trojan |
| Kaspersky | Trojan-Ransom.Win32.Wanna.zbu |
| McAfee | Ransom-O trojan |
| Microsoft | Ransom:Win32/WannaCrypt |
| Symantec | Ransom.Wannacry |

## ESET LiveGrid®

| | |
|---|---|
| COUNT | 10 000 to 100 000 |
| FIRST SEEN | 2017-05-12 |
| LAST SEEN | 2018-03-12 |

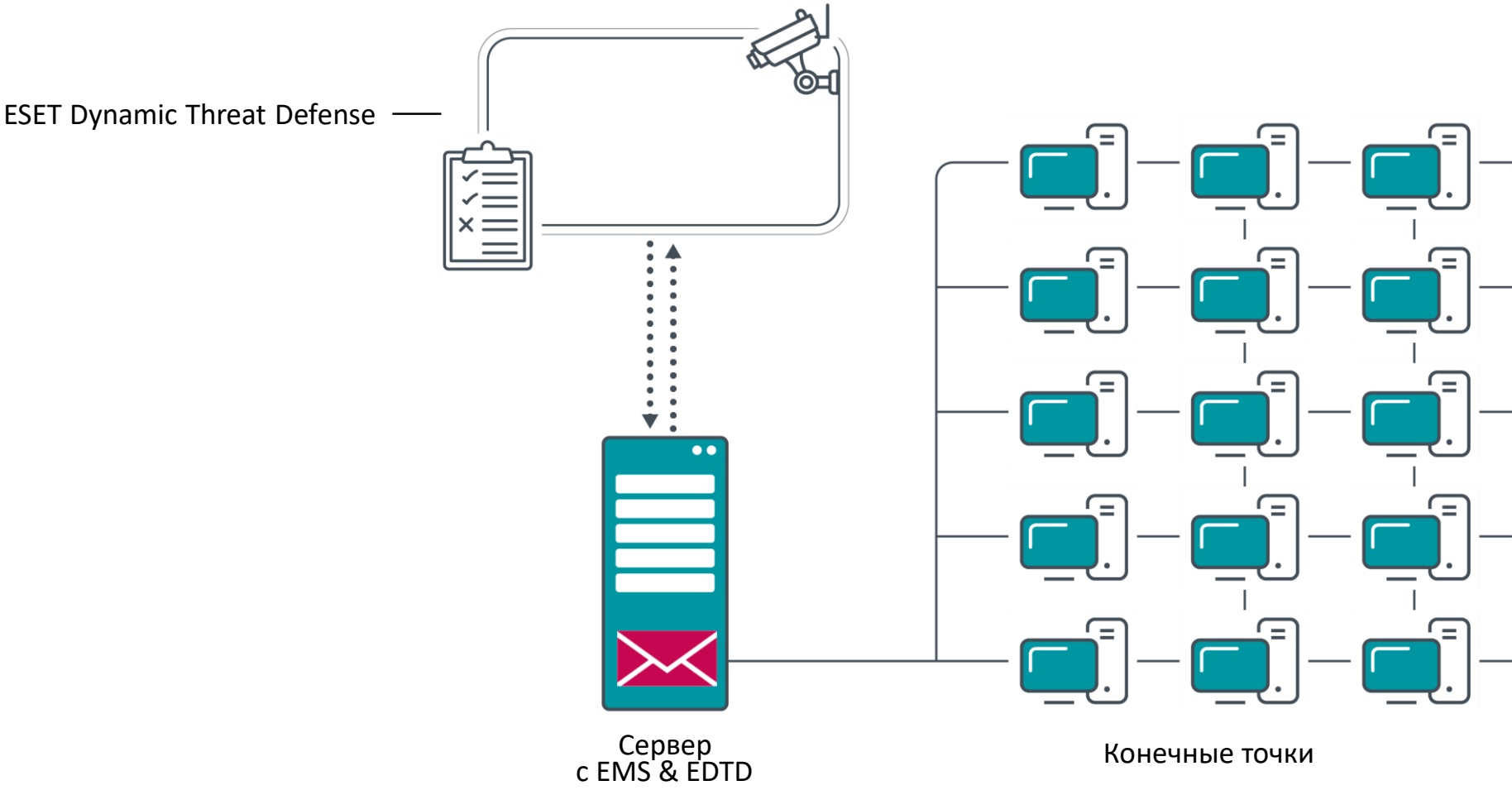
## Countries

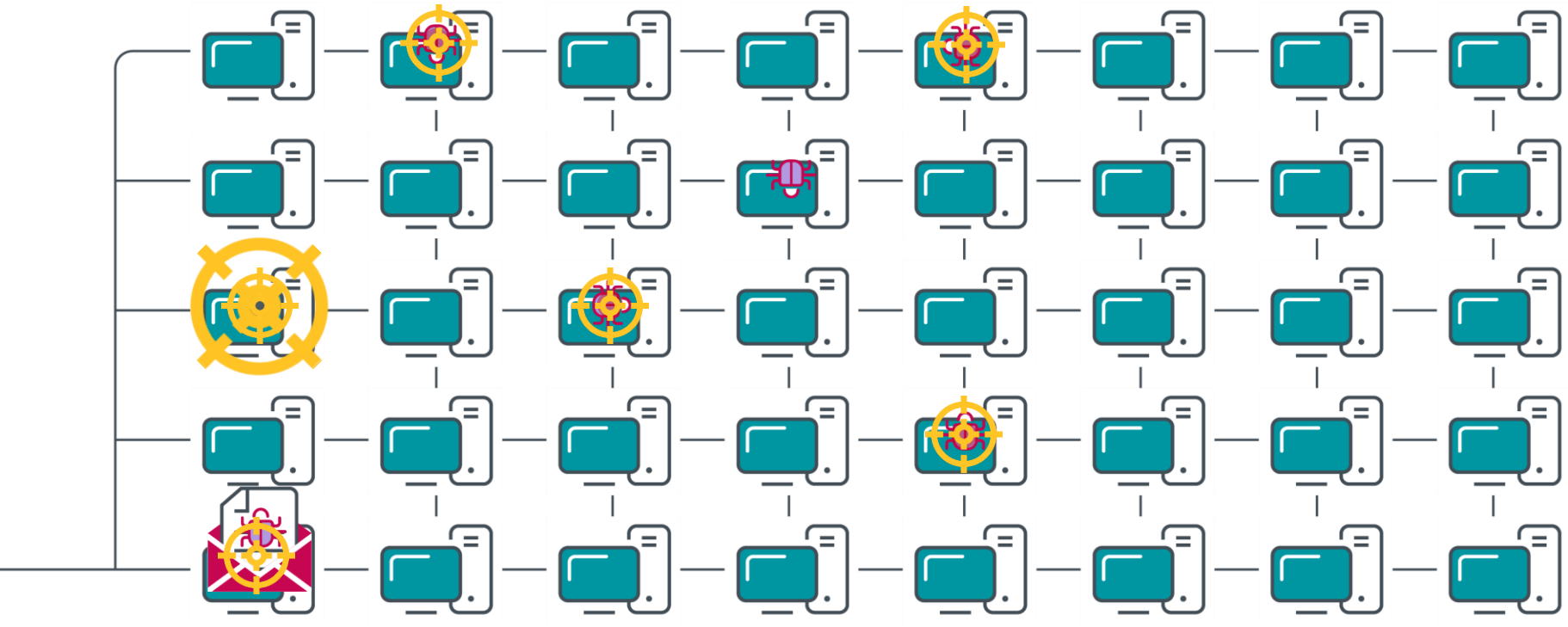
| | |
|---|---|
| Russian Federation | 10 000 to 100 000 |
| Ukraine | 1 000 to 10 000 |
| Taiwan | 1 000 to 10 000 |
| Iran | 1 000 to 10 000 |
| India | 100 to 1 000 |


NEW
ENTERPRISE INSPECTOR

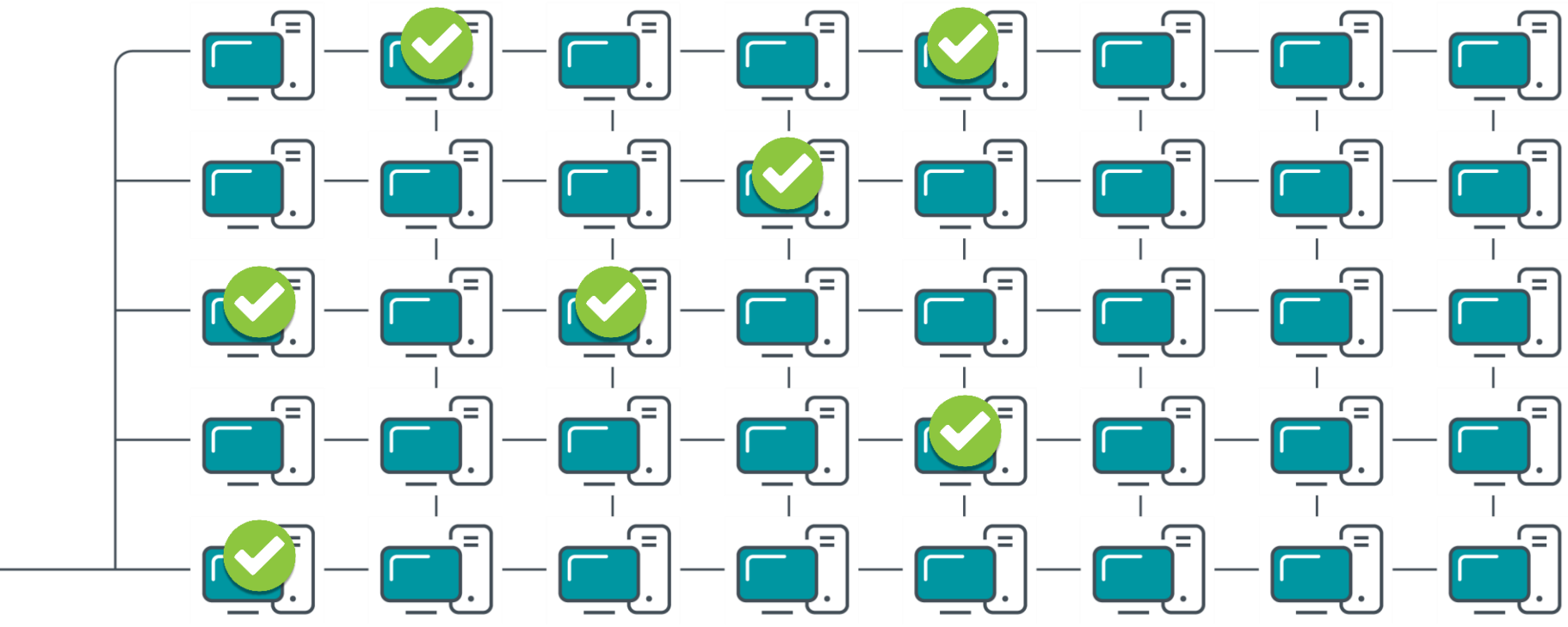
# ESET ENTERPRISE INSPECTOR: КАК РАБОТАЕТ


- ✓ **Собирает информацию** в режиме реального времени
- ✓ Обеспечивает **фильтрацию и сортировку**
- ✓ Позволяет создавать **собственные правила**
- ✓ Использует систему репутаций **ESET LiveGrid**


ESET Dynamic Threat Defense
Сервер
с EMS & EDTD
Конечные точки



Конечные точки



Endpoints

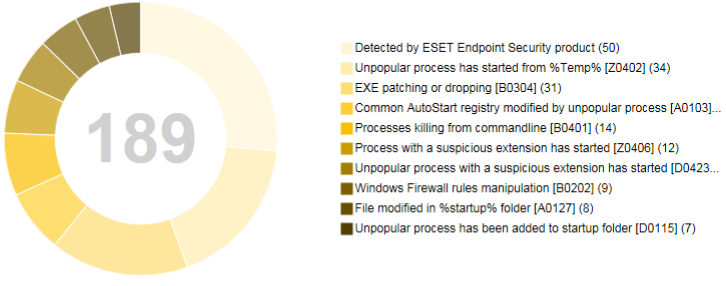
DASHBOARD
ALARMS
EXECUTABLES
SCRIPTS
COMPUTERS
ADMIN
COLLAPSE MENU

# Dashboard

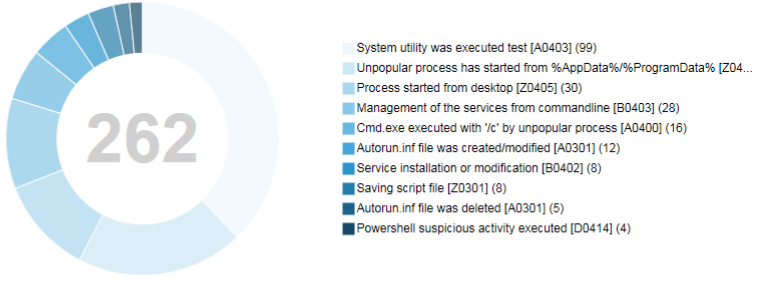
ADD FILTER

Alarms | Executables | Computers | More | Server status

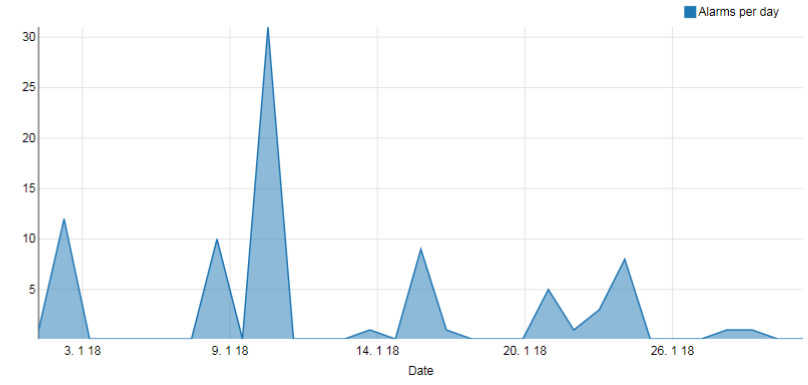
## Top 10 Unresolved Threat and Warning Alarms



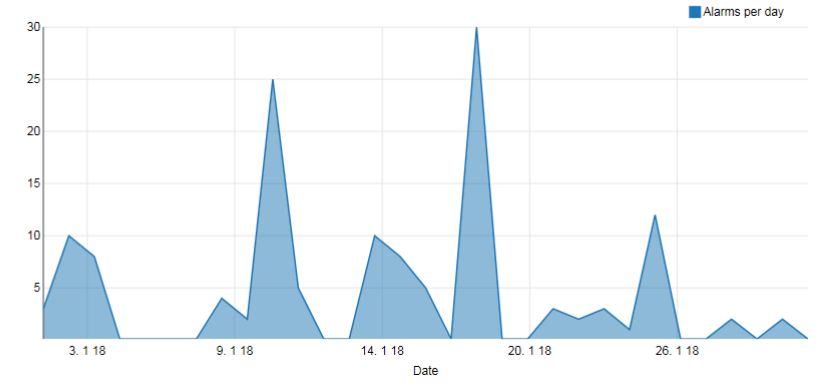

## Top 10 Unresolved Informational Alarms




## Threat and Warning Alarms




## Informational Alarms



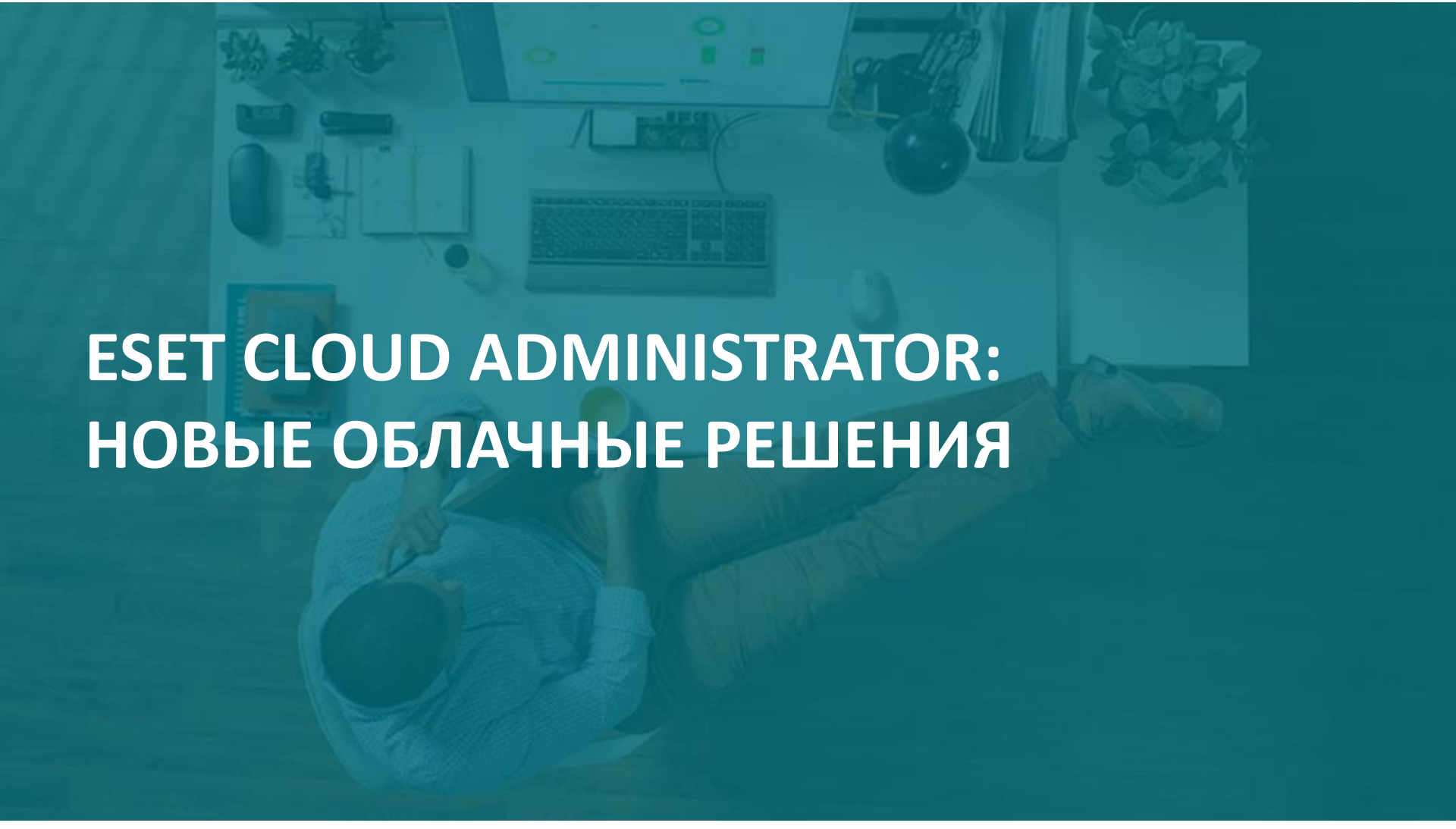
# ESET ENTERPRISE INSPECTOR: ПРЕИМУЩЕСТВА В КЛАССЕ EDR


- ✓ **Простое** внедрение, интеграция, использование
- ✓ **Проактивный** поиск и обнаружение угроз
- ✓ Сочетание **поведенческого анализа и репутационной эвристики**
- ✓ **Интуитивно понятные** уведомления и простое реагирование на инциденты
- ✓ **Многоуровневые** технологии защиты

Обнаружение

Отображение

Реагирование



# ESET CLOUD ADMINISTRATOR: НОВЫЕ ОБЛАЧНЫЕ РЕШЕНИЯ

# ESET CLOUD ADMINISTRATOR

## ОБЛАЧНЫЕ РЕШЕНИЯ

**ESET Endpoint Protection Standard Cloud**

- Защита рабочих станций
- Защита файловых серверов

**ESET Endpoint Protection Advanced Cloud**

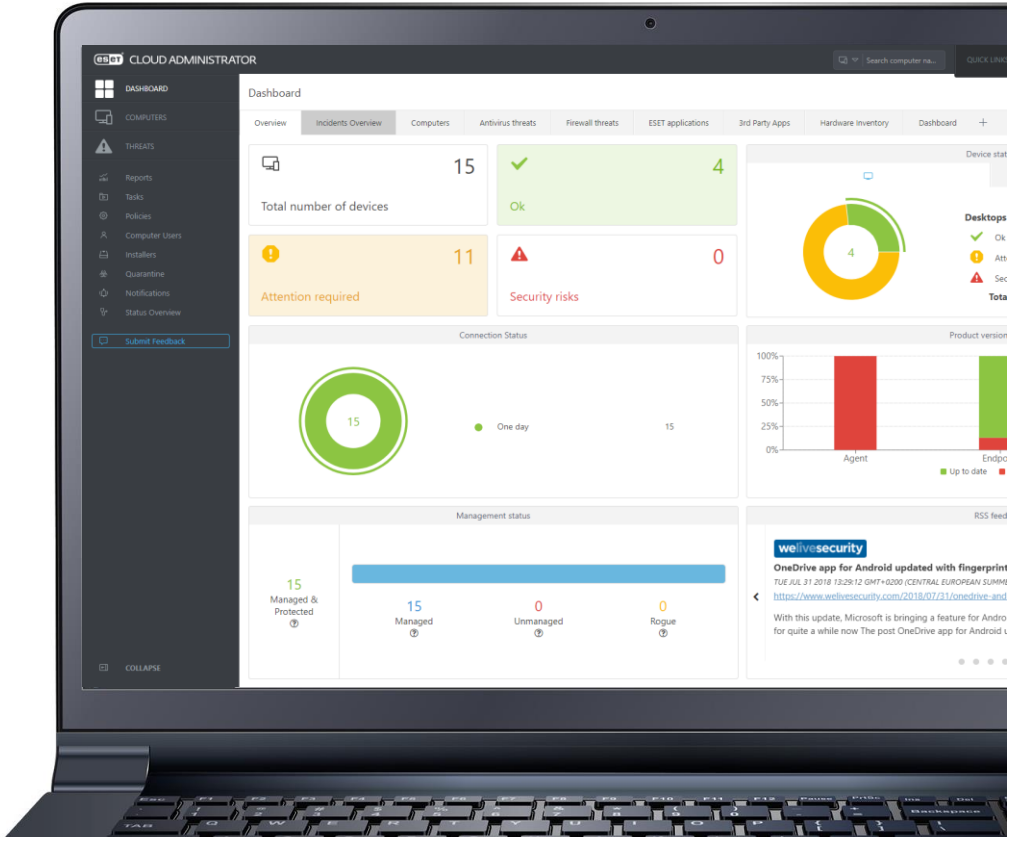
- Расширенная защита рабочих станций
- Защита файловых серверов

**ESET Secure Business Cloud**

- Расширенная защита рабочих станций
- Защита файловых серверов
- Защита почтовых серверов

# ESET CLOUD ADMINISTRATOR
## ЧТО ЭТО?

- КОНСОЛЬ УПРАВЛЕНИЯ АВ
- ПОДДЕРЖКА ДО 250 УЗЛОВ
- РАСПОЛОЖЕН В ОБЛАКЕ ESET




АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА


## Log in

LOGIN Forgotten password

## Register for free

**Manage your business security with one account**
Get real-time visibility into all your licenses and manage them from a single location.

**Get a free trial instantly in a few easy steps**
Try out our new security solutions free for 30 days on up to 25 devices.

REGISTER FOR FREE

© 1992 - 2018 ESET, spol. s r.o. - All rights reserved.

ПАНЕЛЬ МОНИТ.
КОМПЬЮТЕРЫ
УГРОЗЫ
Отчеты
Задачи
Политики
Пользователи компьютера
Установщики
Карантин
Уведомления
Обзор состояния
Отправить отзыв
СВЕРНУТЬ

# Панель монит.

Обзор | Обзор инцидентов | Computers | Antivirus threats | Firewall threats | ESET applications

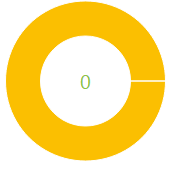
1
Общее количество устройств

0
OK

1
Требуется вмешательство

0
Угрозы безопасности

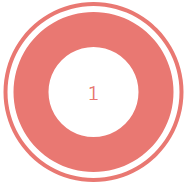
## Состояние устройства




**Настольные компьютеры**

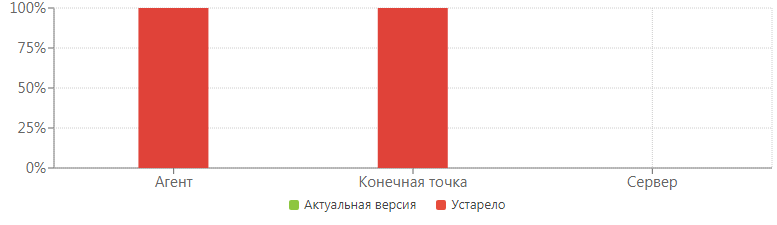
| | |
|---|---|
| OK | 0 |
| Требуется вмешательство | 1 |
| Угроза безопасности | 0 |
| **Всего** | **1** |

## Состояние подключения




> 7 кол-ва дней 1

## Состояние версии продукта




## Состояние управления

1
Под управлением и защитой

1 Управляемые
0 Неуправляемый
0 Неавторизованные

## RSS-канал

welivesecurity

**DanaBot updated with new C&C communication**

*THU FEB 07 2019 14:00:47 GMT+0300 (МОСКВА, СТАНДАРТНОЕ ВРЕМЯ)*

https://www.welivesecurity.com/2019/02/07/danabot-updated-new-cc-communication/

ESET researchers have discovered new versions of the DanaBot Trojan, updated with a more complicated protocol for C&C communication and slight modifications to architecture and campaign IDs The post

# 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
- …


eset АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

safetica

# 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

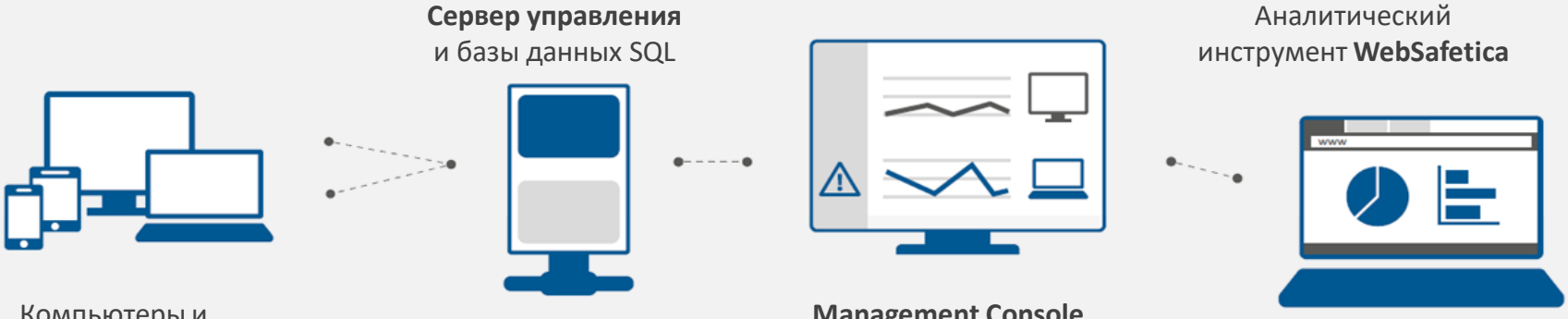
eset АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

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: четырёхядерный 2,4GHz
Оперативная память: от 4GB
Жесткий диск: от 20GB свободного места
ОС: MS Windows Server 2008 и выше, 32&64-bit

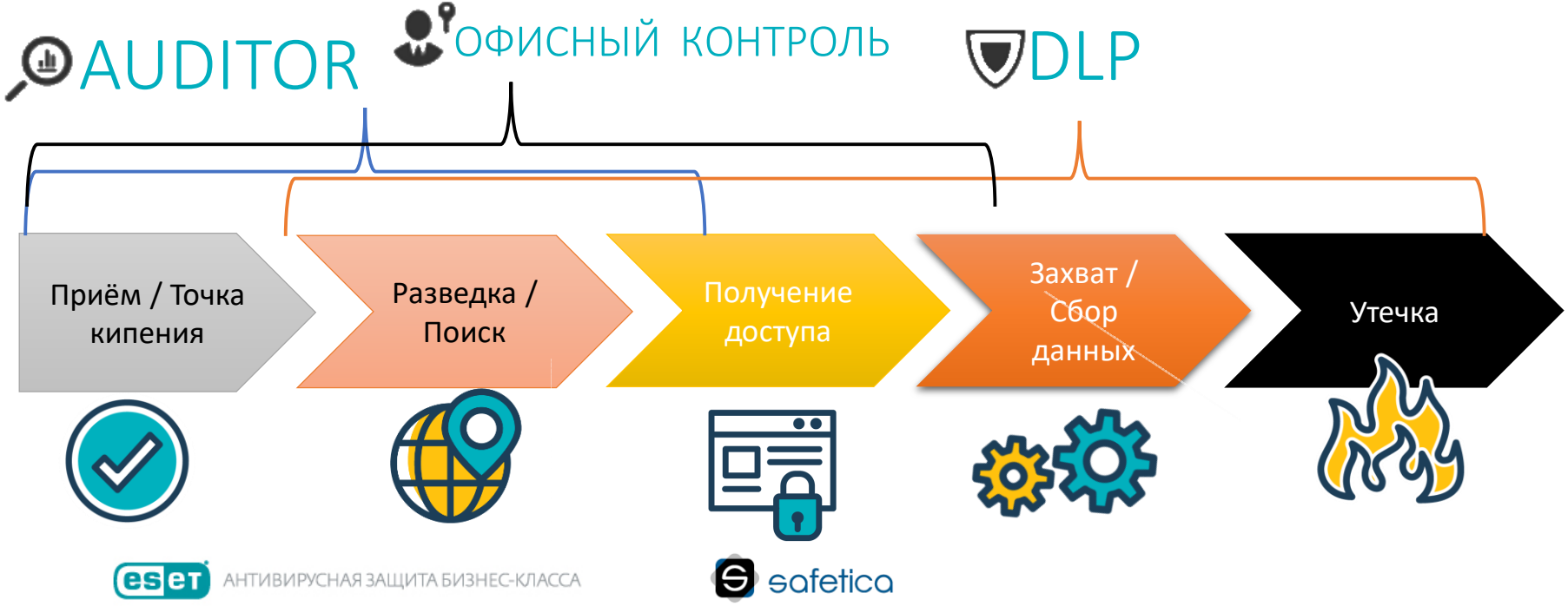
**База данных (MS SQL)**
MS SQL 2008 R2 и выше,
рекомендуется MS SQL 2012 и выше
MS SQL 2012 Express включена в
установочный пакет Safetica

# SAFETICA – КОМПЛЕКСНОЕ РЕШЕНИЕ!

**61% сотрудников**

*злоупотребляет доступом к конфиденциальным данным компании**

** Ponemon Institute, 2016*



# КОМПЛЕКСНОЕ РЕШЕНИЕ
# SAFETICA

## AUDITOR

РЕГИСТРАЦИЯ АКТИВНОСТИ СОТРУДНИКОВ

## SUPERVISOR

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

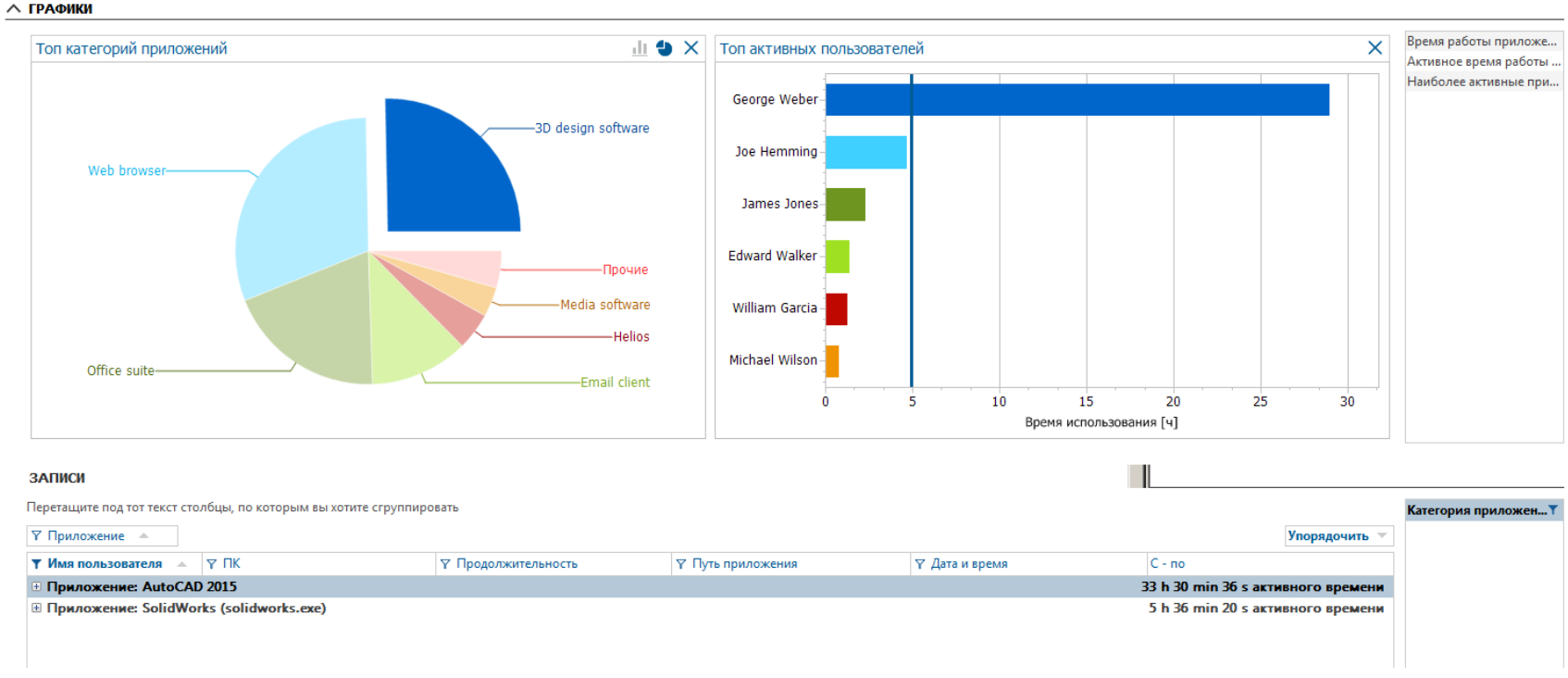
ОКУПАЕМОСТЬ ВНЕДРЕНИЯ

ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ ПО

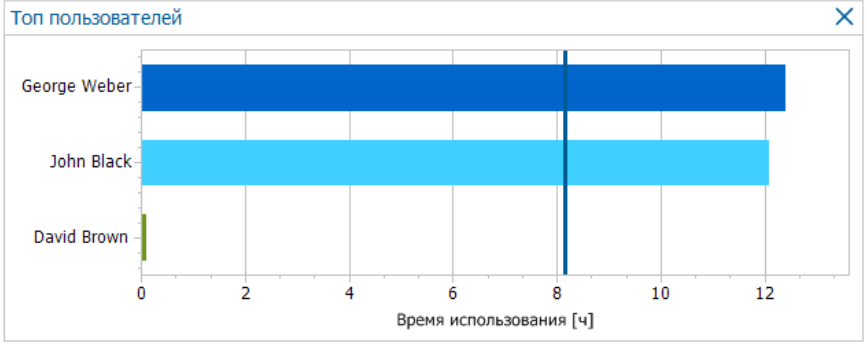
eset АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

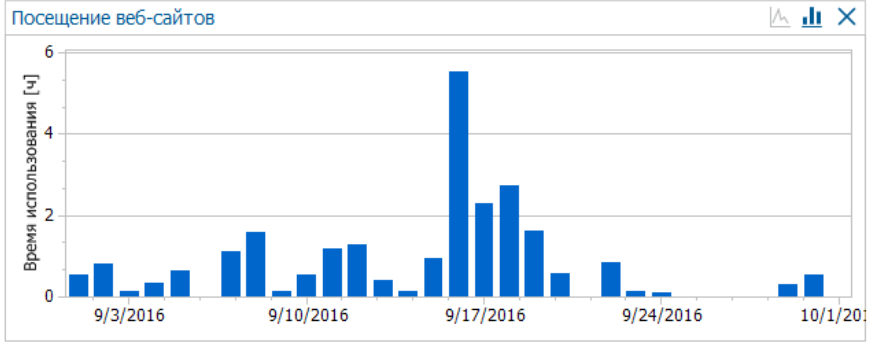
safetica

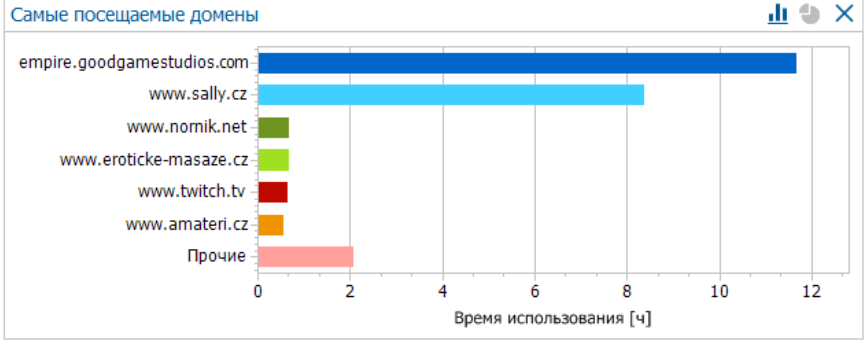
# ОФИСНЫЙ КОНТРОЛЬ
# (МОДУЛЬ AUDITOR)

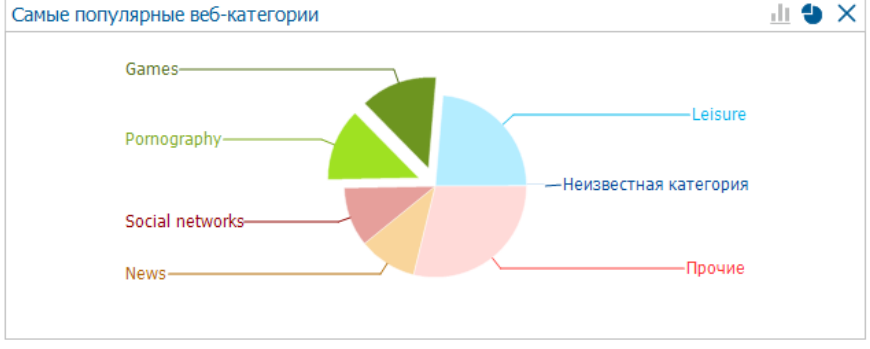


# ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ AUDITOR)

# ОФИСНЫЙ КОНТРОЛЬ
# (МОДУЛЬ SUPERVISOR)

WEB-КОНТРОЛЬ

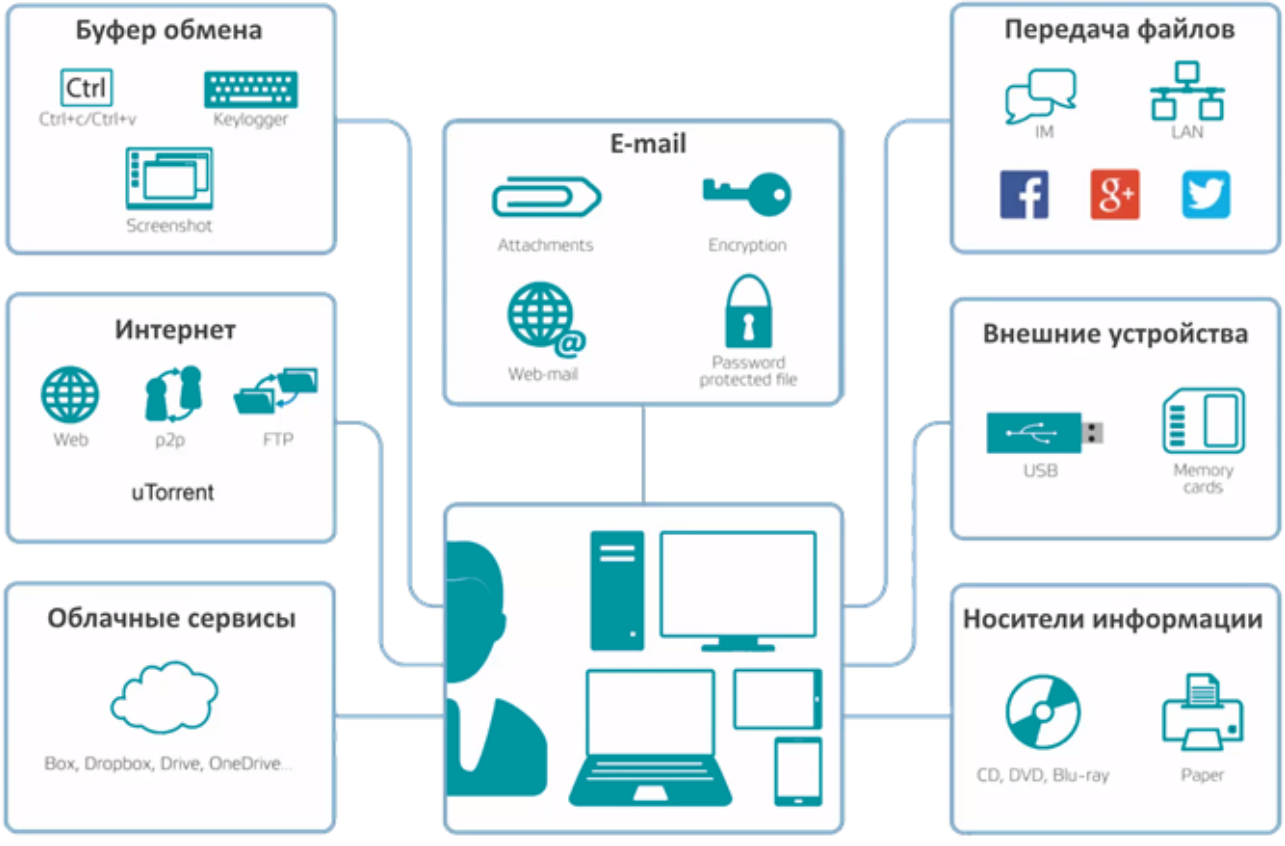
КОНТРОЛЬ ПРИЛОЖЕНИЙ

КОНТРОЛЬ ПЕЧАТИ

eset АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

safetica

# ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (МОДУЛЬ DLP)




eset АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

safetica

# 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

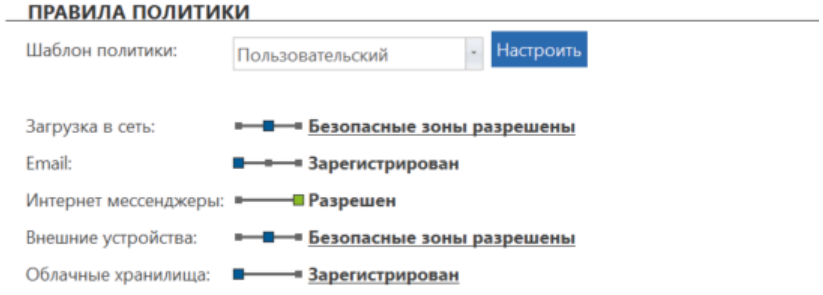
*Все файлы, помещенные в определенные папки, будут автоматически получать необходимую метку.*

## › КОНТЕНТНЫЕ ПРАВИЛА

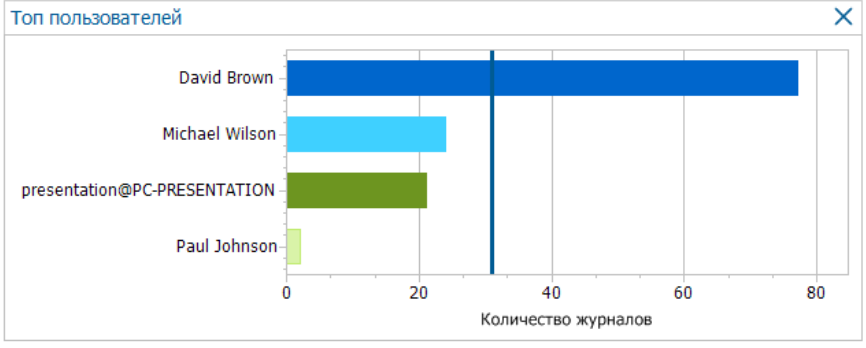
*Все файлы, содержащие определенный контент, будут автоматически получать необходимую метку.*

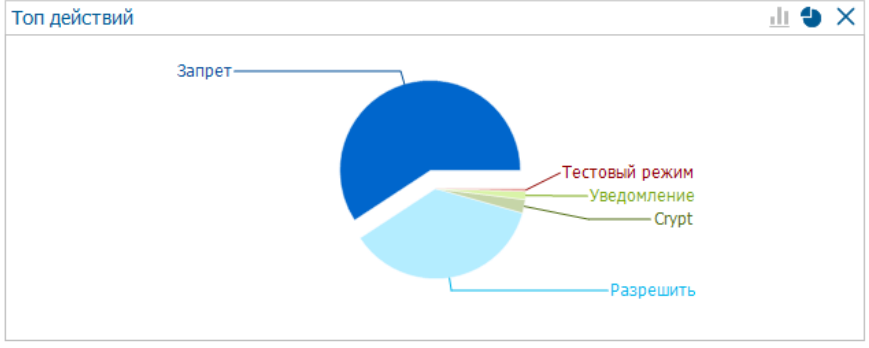
# ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (КОНТЕНТНЫЙ ФИЛЬТР)

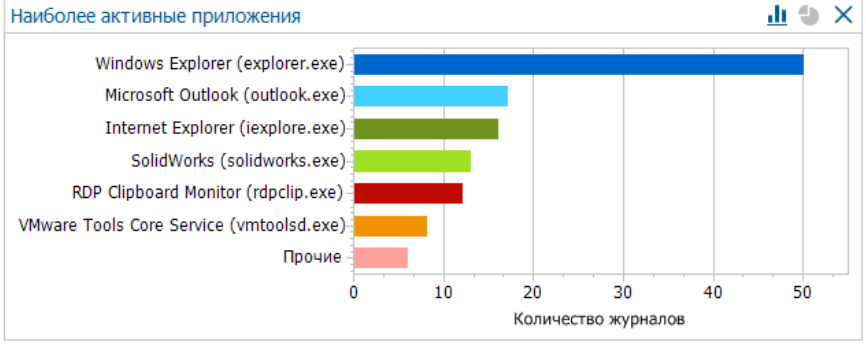
- ЭЛЕКТРОННАЯ ПОЧТА
- МЕССЕНДЖЕРЫ
- ВНЕШНИЕ УСТРОЙСТВА
- ЗАГРУЗКА ФАЙЛОВ В ИНТЕРНЕТ

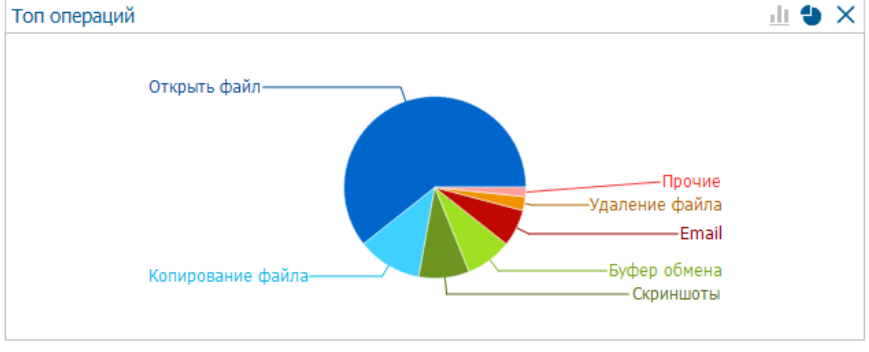



# ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (МОДУЛЬ DLP)



# АНАЛИЗ РЕЗУЛЬТАТОВ
# WEBSAFETICA



# 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**

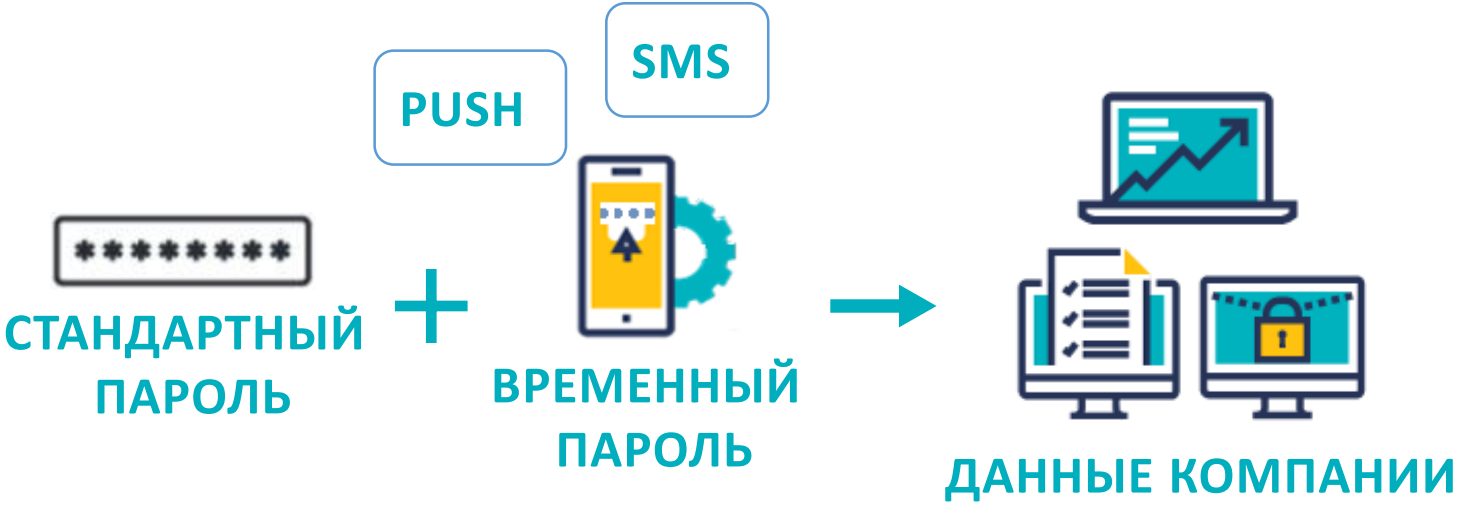
eset АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

safetica

# ПАРОЛИ ПИШЕМ ИЛИ ЗАПОМИНАЕМ?

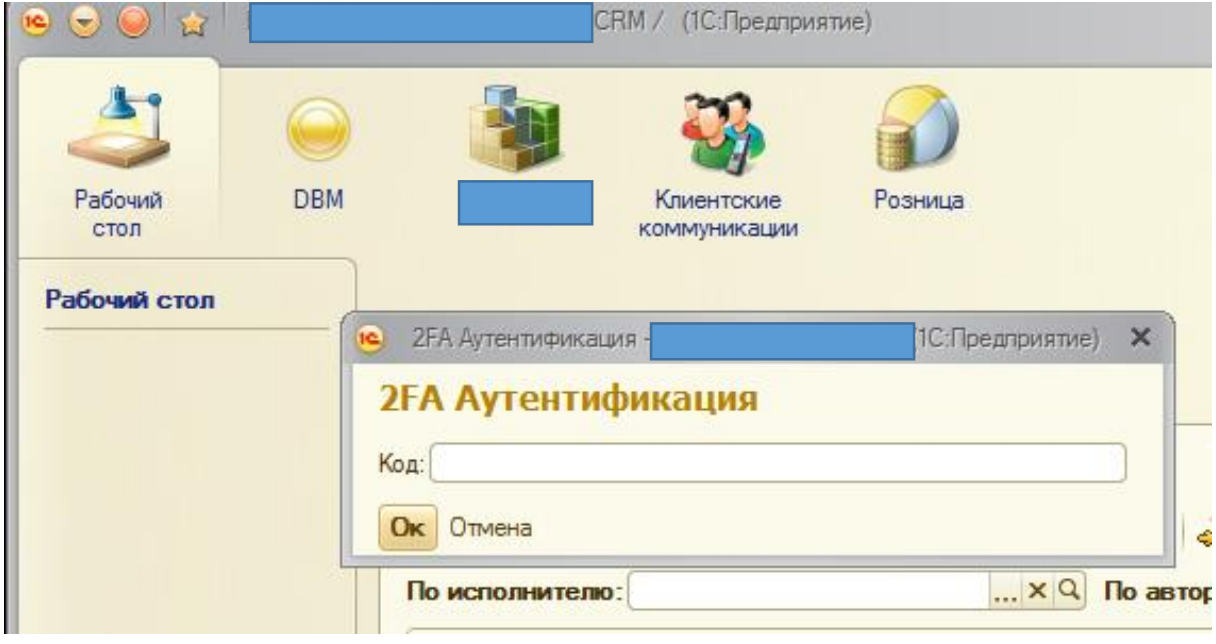
eset АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

# 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

# ИНТЕГРАЦИЯ С 1С



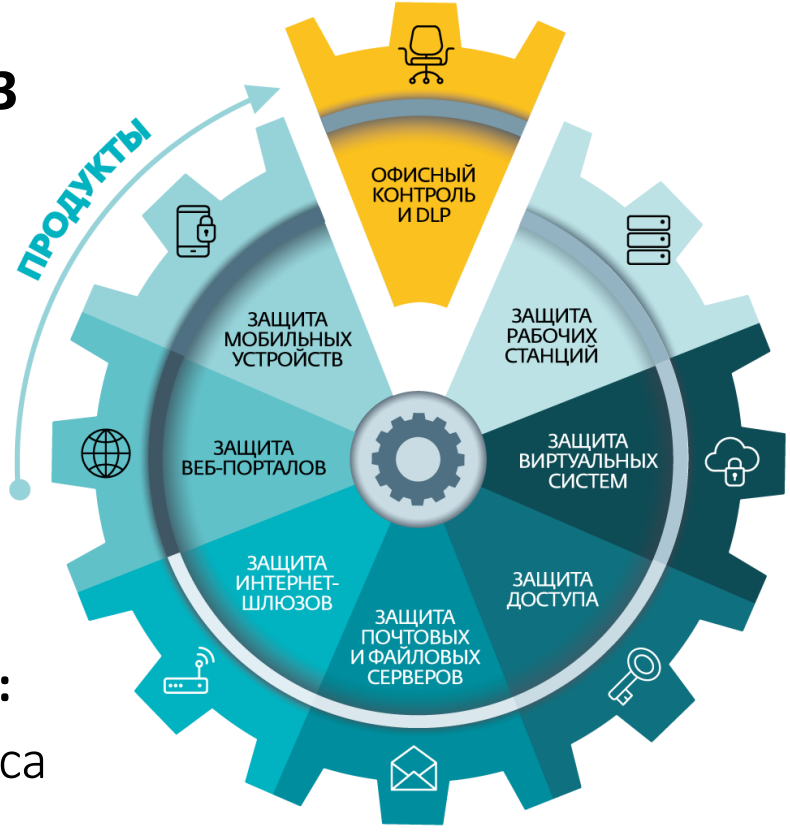

**ДОСТУПЕН:**

- **NFR**
- **ДЕМО СТЕНД**

# КАК?
# КОМПЛЕКСНЫЙ ПОДХОД:

## 1. БЕЗОПАСНОСТЬ ОТ ВНЕШНИХ УГРОЗ

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



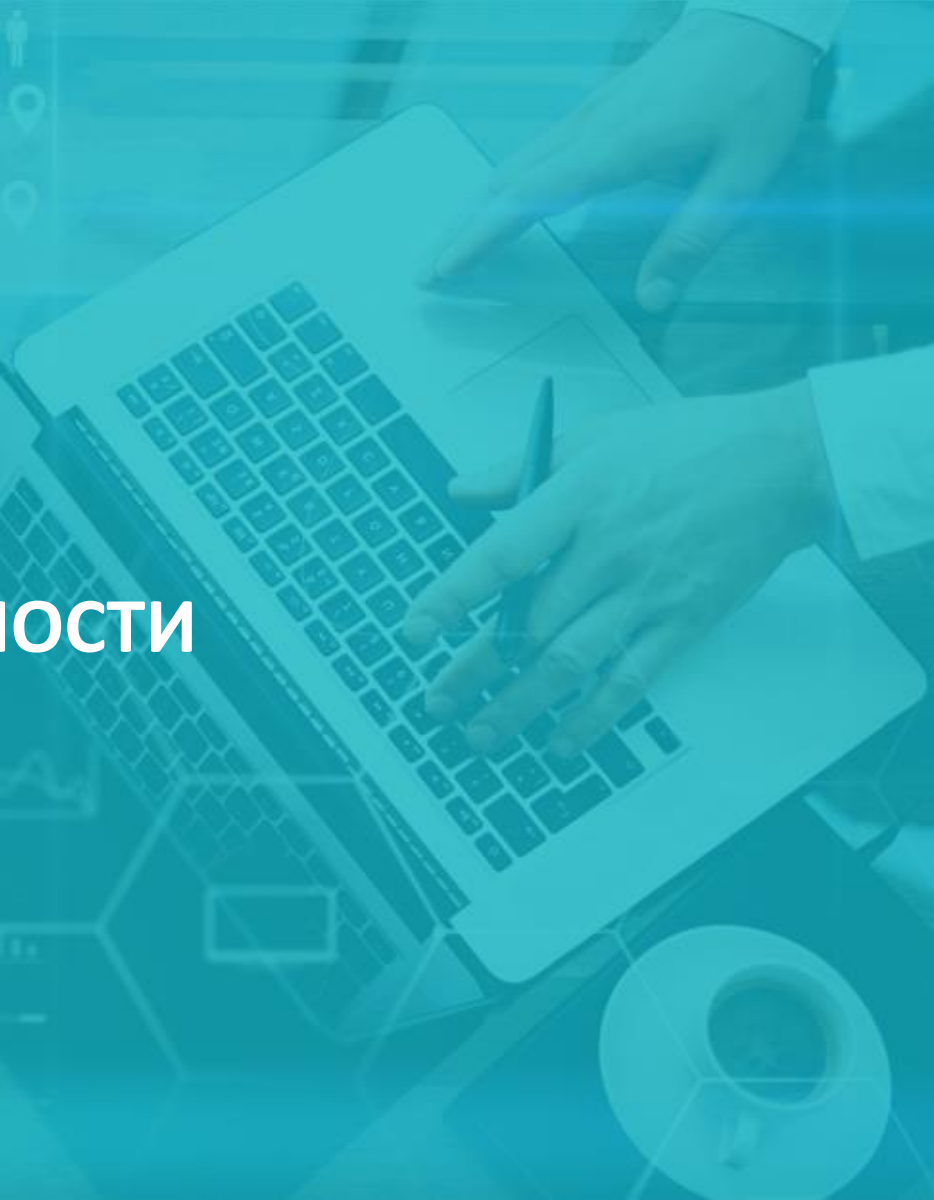

## 2. БЕЗОПАСНОСТЬ ОТ ВНУТРЕННИХ УГРОЗ:

- Офисный контроль и DLP Safetica
- ESA

eset АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

safetica

# ESET - НОВЫЕ ВОЗМОЖНОСТИ



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

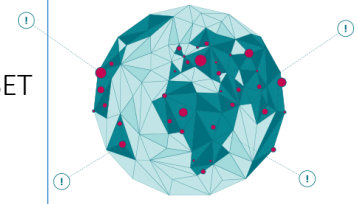
# ESET THREAT INTELLIGENCE


Сервис предоставляет статистику о новых угрозах. Помогает прогнозировать целевые атаки и адаптироваться к меняющемуся киберландшафту

- **Отчеты** о целевых вредоносных программах, активности ботнетов, фишинге
- **Анализ сэмплов**
- **Поставка данных** в SIEM-системы заказчика
- **Панель управления**
- Доступ к **ESET Threat Intelligence** с помощью API

# ИСТОЧНИКИ ДАННЫХ

- 100 миллионов сенсоров
- Облачная система ESET LiveGrid
- Песочницы ESET
- База данных ДНК сигнатур ESET
- Трекер ботнетов
- Внешние источники



# ИТОГО

- Прогнозирование целевых атак, направленных против компании
- Быстрое реагирование на киберинциденты
- Дешевле, чем устранение последствий ИБ-инцидента

# СПАСИБО
# ЗА ВНИМАНИЕ!

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