

КАК ОБЕСПЕЧИТЬ ЗАЩИТУ КОМПАНИИ ОТ ВНЕШНИХ И ВНУТРЕННИХ УГРОЗ?

Дмитрий Самойленко
ESET ЮФО/СКФО/ЦФО

СОДЕРЖАНИЕ

1. УГРОЗЫ
2. АДАПТИВНАЯ ЗАЩИТА
3. 7Е ПОКОЛЕНИЕ ПРОДУКТОВ ESET
4. EDTD + EEI
5. ESET CLOUD ADMINISTRATOR
6. ЗАЩИТА ОТ ВНУТРЕННИХ УГРОЗ
7. ESA
8. ESET THREAT INTELLIGENCE



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

СТАТИСТИКА ИНСТИТУТА AV-TEST

ИЗВЕСТНЫЕ УГРОЗЫ

Total malware



х3 с 2014г

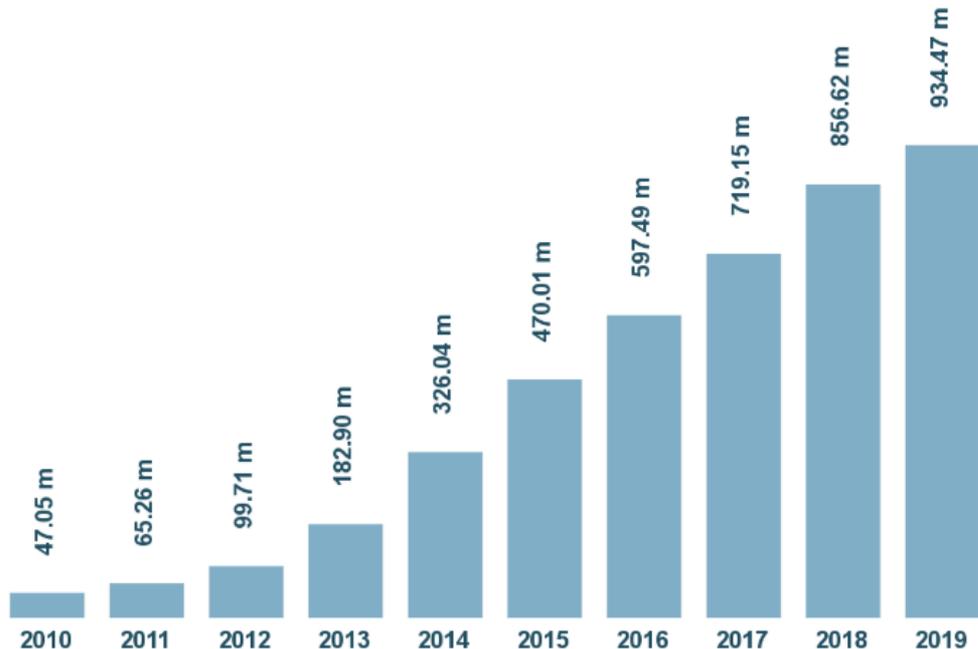
- **390 000 шт. в день**

Новых образцов

вредоносных программ каждый день

- **Новые способы**

Новые способы обхода обнаружения



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Last update: August 26, 2019

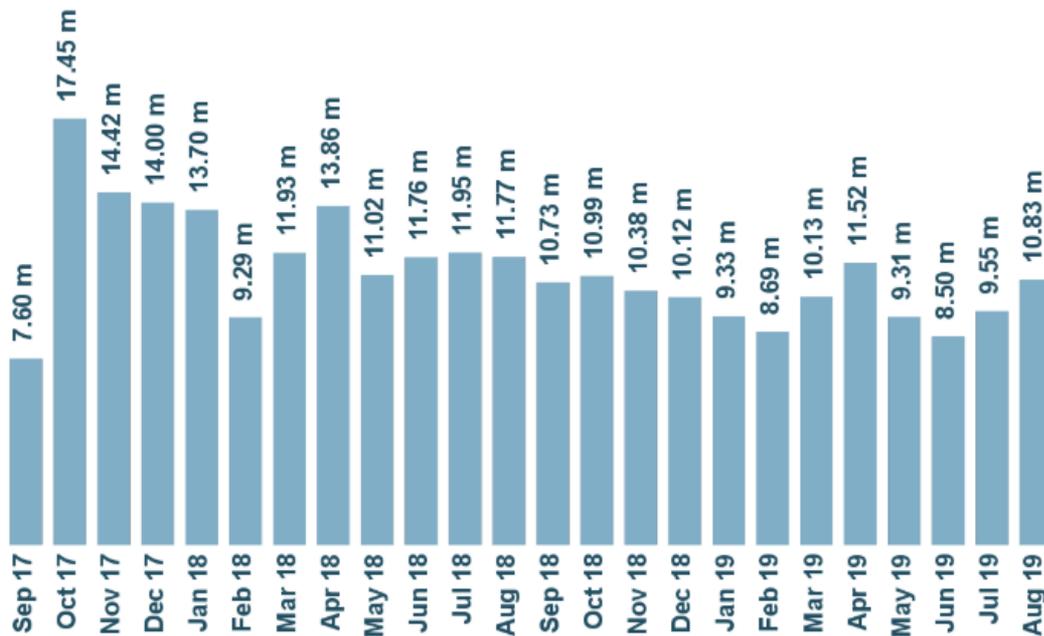
Copyright © AV-TEST GmbH, www.av-test.org

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

УГРОЗЫ ПРОГРЕССИРУЮТ И СТАНОВЯТСЯ СЛОЖНЕЕ



Новые угрозы



Last update: August 26, 2019

Copyright © AV-TEST GmbH, www.av-test.org



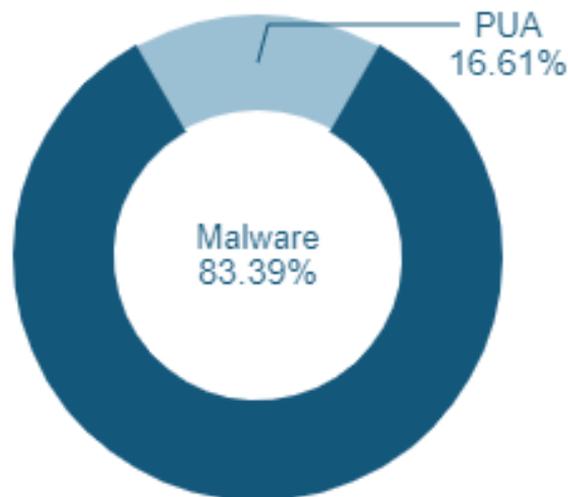
АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

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

РАСПРЕДЕЛЕНИЕ УГРОЗ ЗА 12 МЕСЯЦЕВ

Total distribution of threats
over the last 12 months

AVTEST



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

Человеческий фактор

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

** PwC, 2016*

- › **47% пересылают рабочие файлы**
на личную почту
- › **44% устанавливают приложения**
на компьютер в корпоративной сети
- › **56% открывают любые сайты**
без ограничений



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ESET Russia, 2017, 750 респондентов

КАК ОБЕСПЕЧИТЬ ЗАЩИТУ ОТ ВНЕШНИХ УГРОЗ?



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Архитектура адаптивной защиты

ПРОГНОЗИРОВАНИЕ

Оценка риска по приоритетам

Предвидение угрозы/атаки

Базовые системы и положения безопасности

Устранение последствий

Корректировка политик безопасности

Расследование инцидентов, ретроспективный анализ

РЕАГИРОВАНИЕ

ПРЕДОТВРАЩЕНИЕ

Упрочнение систем

Изолирование систем

Предотвращение атак

Обнаружение инцидентов

Подтверждение и приоритизация рисков

Содержание инцидентов

ОБНАРУЖЕНИЕ



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

Замкнутый контур

ESET Security Management Center

NEW ESET Enterprise Inspector

NEW ESET Dynamic Threat Defense

ESET Endpoint Security/ESET Endpoint Antivirus

ESET Security Management Center

ESET Enterprise Inspector **NEW**

ESET Dynamic Threat Defense **NEW**

РЕАГИРОВАНИЕ

ОБНАРУЖЕНИЕ

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**

НАДЕЖНОСТЬ! 7-ОЕ ПОКОЛЕНИЕ

МНОГОУРОВНЕВАЯ ЗАЩИТА ТЕХНОЛОГИЯМИ ESET

АКТИВНЫ ПОСТОЯННО



ОБНАРУЖЕНИЕ
И БЛОКИРОВАНИЕ
ПО ПОВЕДЕНИЮ (HIPS)



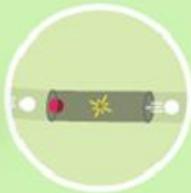
ESET LIVE GRID



МАШИННОЕ ОБУЧЕНИЕ



СКАНЕР UEFI



ЗАЩИТА
ОТ СЕТЕВЫХ АТАК



РЕПУТАЦИЯ
И КЭШ



ПЕСОЧНИЦА



ДНК СИГНАТУРЫ



РАСШИРЕННОЕ
СКАНИРОВАНИЕ
ПАМЯТИ



ЗАЩИТА ОТ
ШИФРАТОРОВ



ЗАЩИТА
ОТ ЭКСПЛОЙТОВ



ОБЛАЧНАЯ СИСТЕМА
ЗАЩИТЫ



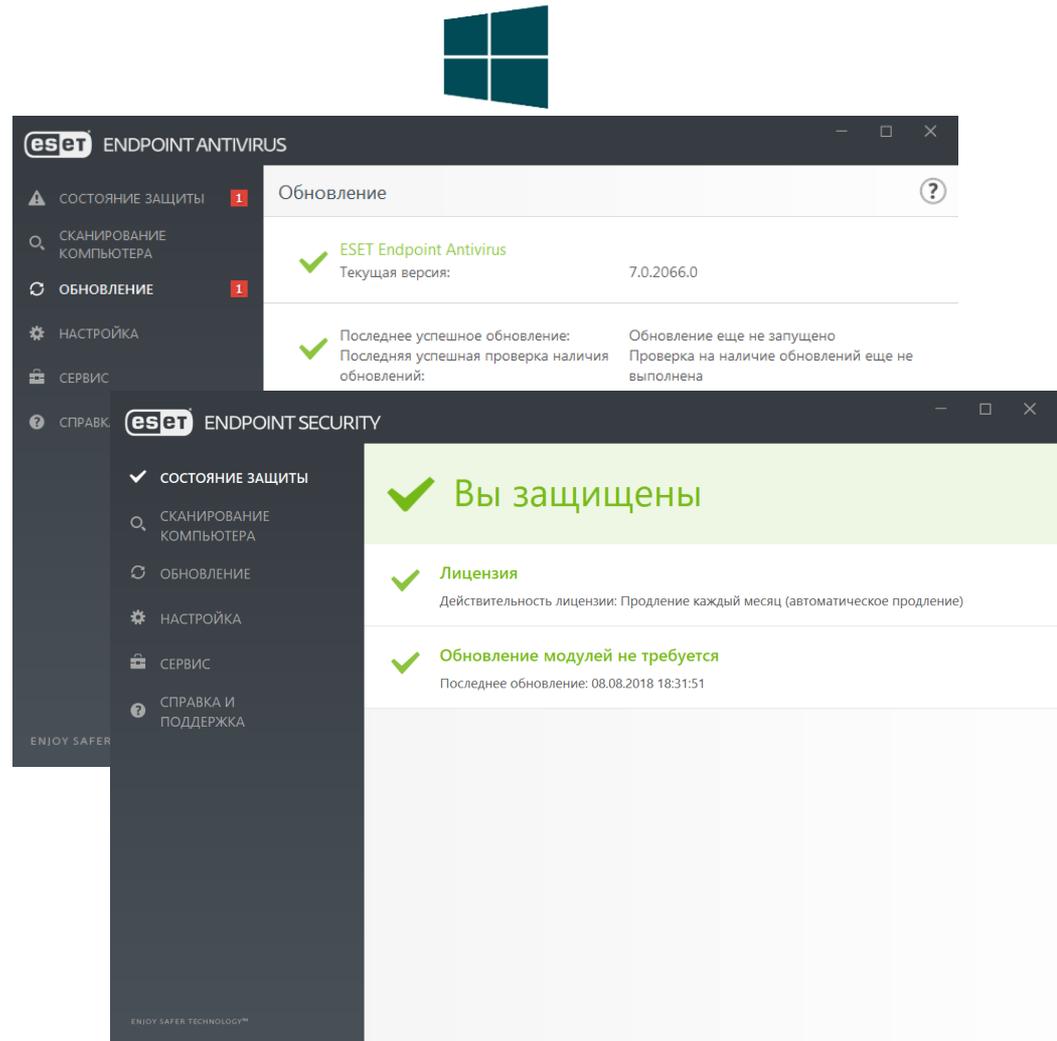
ЗАЩИТА
ОТ БОТНЕТОВ

ДО ВЫПОЛНЕНИЯ УГРОЗЫ

ПОСЛЕ ВЫПОЛНЕНИЯ УГРОЗЫ

ESET ENDPOINT SECURITY ESET ENDPOINT ANTIVIRUS

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



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

The screenshot displays the ESET File Security for Microsoft Windows Server interface. The main status bar at the top indicates "Вы защищены" (You are protected) with a green checkmark. Below this, three key status items are listed:

- Лицензия** (License): Действительность лицензии: 14.03.2019
- Обновление модулей не требуется** (Module update not required): Последнее обновление: 08.08.2018 20:22:26

A section titled "Статистика защиты файловой системы" (File system protection statistics) provides the following data:

Заражено:	0
Очищено:	0
Не заражено:	2 279
Всего:	2 279

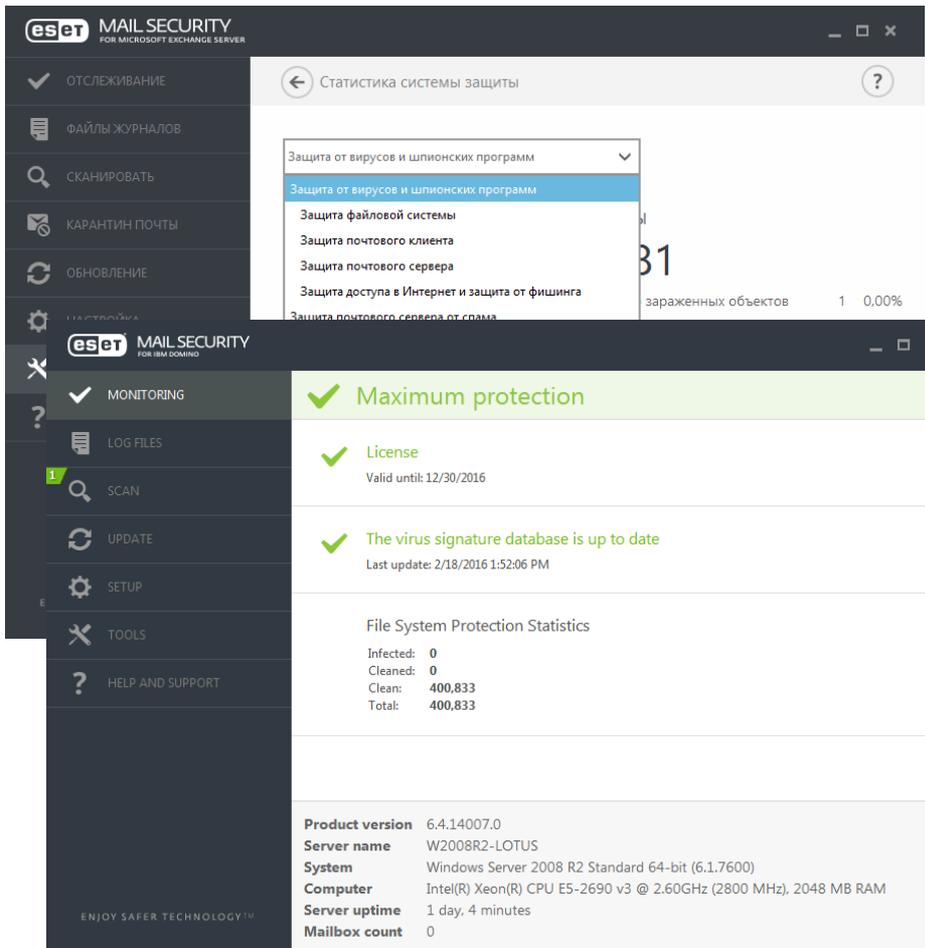
At the bottom, system information is displayed:

Версия продукта	7.0.12012.0
Имя сервера	WIN-TK16S21N282
Система	Windows Server 2012 R2 Standard 64-bit (6.3.9600)
Компьютер	Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz (2712 MHz), 7640 MB RAM
Время работы сервера	3 мин.

The left sidebar contains navigation options: ОТСЛЕЖИВАНИЕ, ФАЙЛЫ ЖУРНАЛА, СКАНИРОВАТЬ, ОБНОВЛЕНИЕ, НАСТРОЙКА, СЕРВИС, СПРАВКА И ПОДДЕРЖКА. The ESET logo and "ENJOY SAFER TECHNOLOGY™" are visible at the bottom left of the interface.

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)*



The screenshot displays the ESET Mail Security interface for Microsoft Exchange Server. The main window shows the 'Статистика системы защиты' (System Protection Statistics) section, which includes a dropdown menu for protection types and a summary of infected objects. The interface is in Russian, but the main content area shows English text for system status and statistics.

System Protection Statistics

Category	Value
Зараженных объектов	1
Percentage	0.00%

System Status

- Maximum protection
- License: Valid until: 12/30/2016
- The virus signature database is up to date (Last update: 2/18/2016 1:52:06 PM)

File System Protection Statistics

Infected:	0
Cleaned:	0
Clean:	400,833
Total:	400,833

System Information

Product version	6.4.14007.0
Server name	W2008R2-LOTUS
System	Windows Server 2008 R2 Standard 64-bit (6.1.7600)
Computer	Intel(R) Xeon(R) CPU E5-2690 v3 @ 2.60GHz (2800 MHz), 2048 MB RAM
Server uptime	1 day, 4 minutes
Mailbox count	0

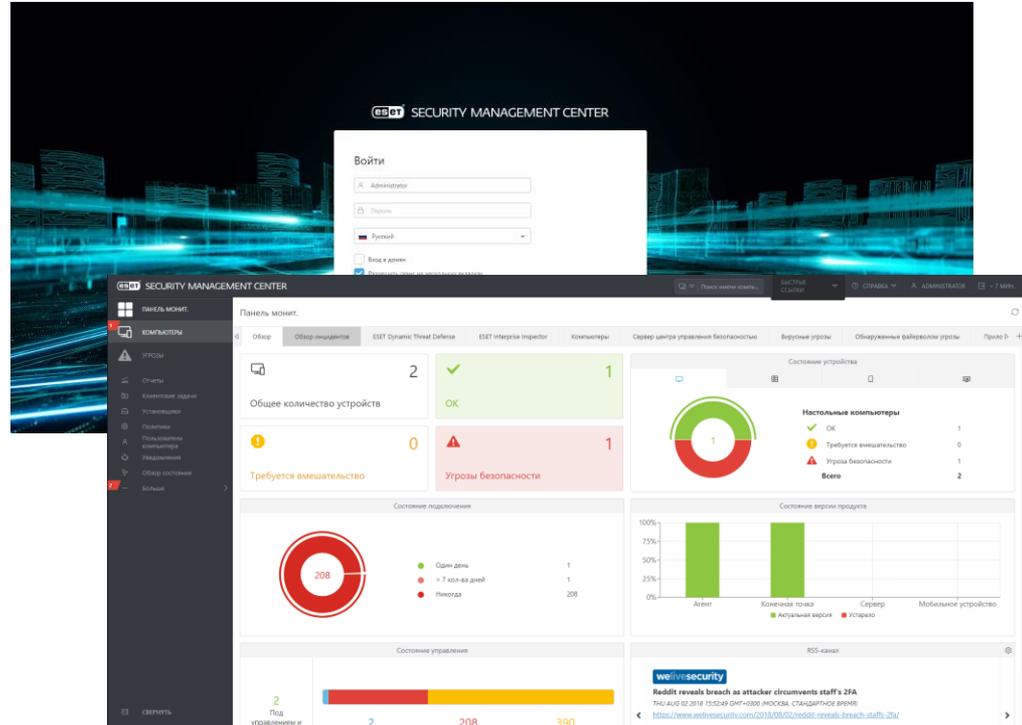


SECURITY MANAGEMENT CENTER

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

The screenshot shows the ESET Security Management Center interface. On the left is a navigation sidebar with options like 'Панель мониторинга', 'Компьютеры', 'Угрозы', 'Отчеты', 'Клиентские задания', 'Установщики', 'Политики', 'Пользователи компьютера', 'Уведомления', 'Обзор состояния', 'Больше', and 'Вернуть'. The main area is titled 'Панель мониторинга' and contains several widgets:

- Компьютеры с соответствующими сведениями:** A table listing computers with columns for name, manufacturer, device model, and serial number.
- Компьютеры со сведениями о ЦП:** A table listing computers with columns for name, manufacturer, description, and CPU number.
- Компьютеры со сведениями об ОЗУ:** A table listing computers with columns for name, manufacturer, total memory, and RAM type.
- Число компьютеров, сгруппированных по общей емкости:** A donut chart showing 4 computers grouped by total memory.

The screenshot shows the hardware details for a specific device in the ESET Security Management Center. The interface includes a navigation menu on the left and a main content area with tabs for 'Основное', 'Оборудование', and 'Продукты и лицензии'. The 'Оборудование' tab is active, displaying the following information:

- Устройство:** Lenovo 4180PUG, Serial number PBAK414.
- CPU:** Intel(R) Core(TM) i7-2640M CPU @ 2.80GHz, Base frequency 2801 MHz, Number of cores 2, Number of logical cores 4, Architecture type x64, Manufacturer GenuineIntel.
- RAM:** Capacity 8 GiB, Base frequency 1333 MHz, Manufacturer Kingston, Description Physical Memory, Architecture type Hei33ecno.
- Хранилище:** Type Physical disk drive, Description INTEL SSDSC2BW480A4 SCSI Disk Device, Capacity 447 GiB, Serial number PHDA410301PH4805GN, Manufacturer (Standard disk drives).

At the bottom, there are buttons for 'ЗАКРЫТЬ' and 'КОМПЬЮТЕР'.

Песочница

NEW

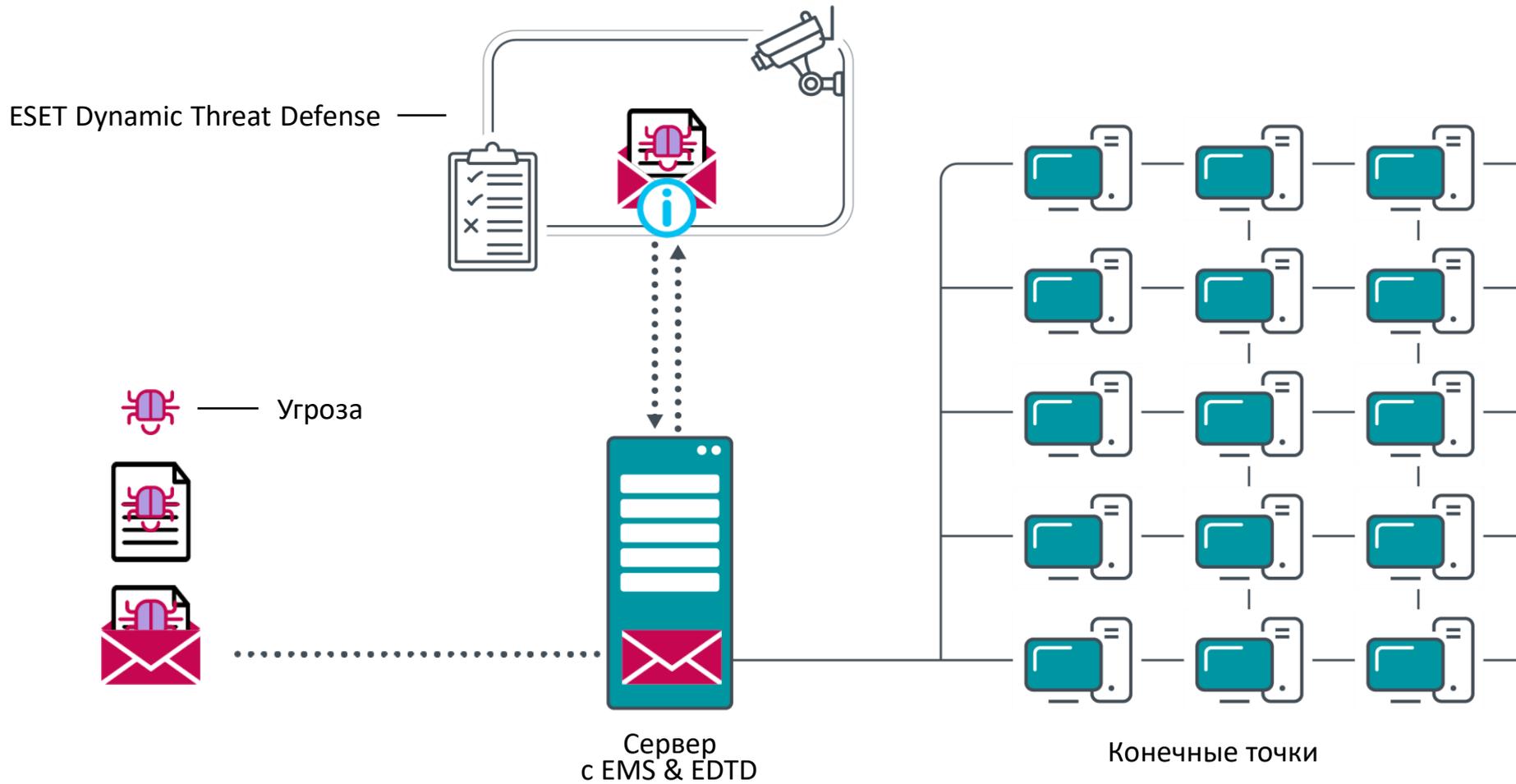


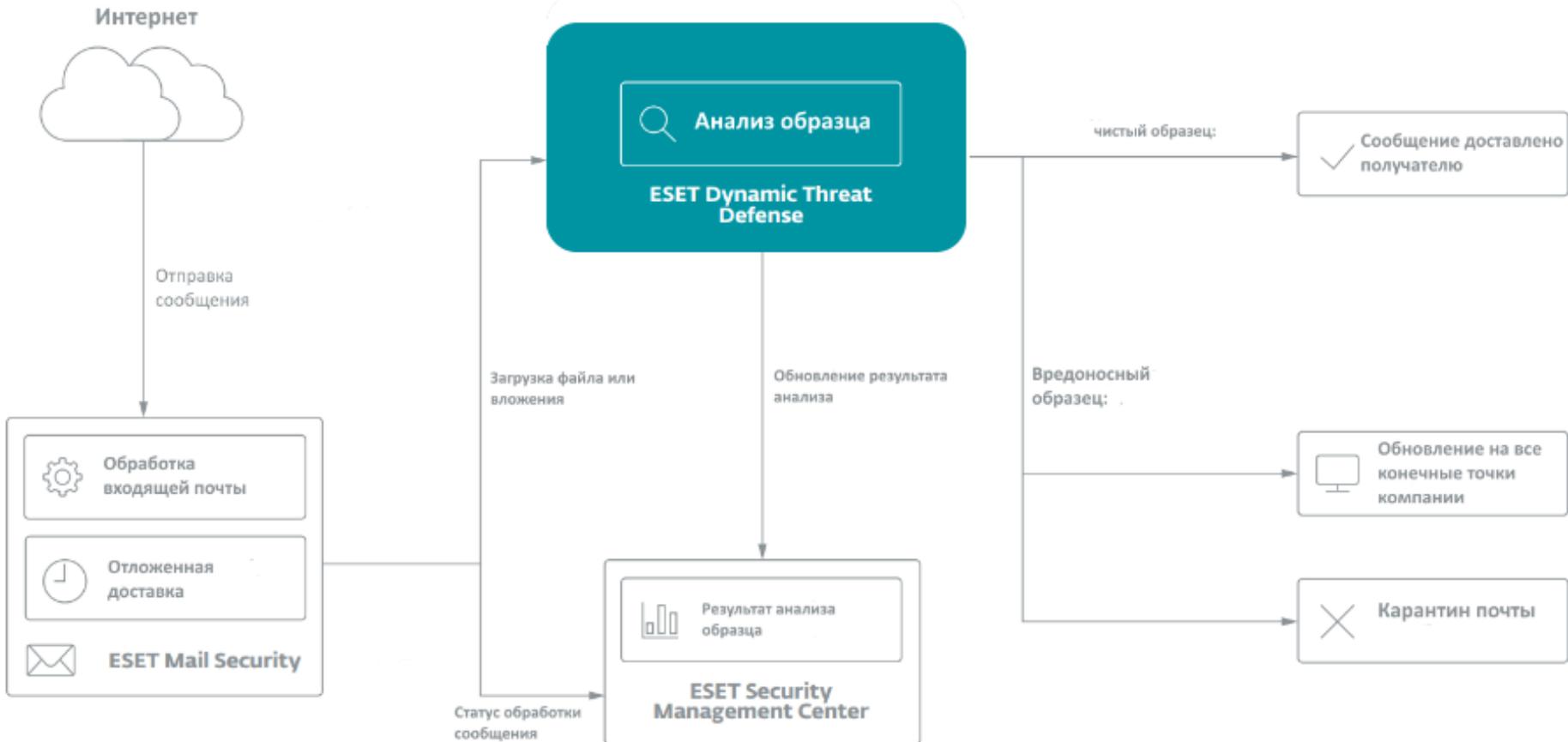
DYNAMIC THREAT DEFENSE

ESET DYNAMIC THREAT DEFENSE

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



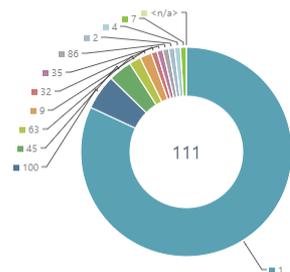




Dashboard

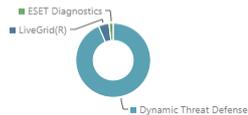
Overview Incidents Overview Computers Security Management Center Server Antivirus threats Firewall threats ESET applications EDTD ⌂ +

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



Generated 0 minutes ago

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



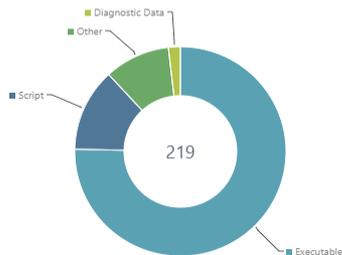
Generated 0 minutes ago

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 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...

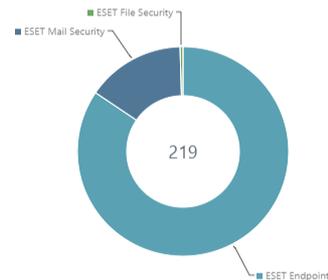


Generated 0 minutes ago

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...
F9D38EAF78D...	Executable	Automatic	Finished	1	2018 Mar 16 1...
A609359D34D...	Executable	Automatic	Finished	63	2018 Mar 16 1...
6AF5D9E8670...	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...
AS85F3A172EB...	Executable	Automatic	Finished	1	2018 Mar 16 1...
49521A5A03BE...	Executable	Automatic	Finished	45	2018 Mar 16 1...
1E4A4BBEC3E4...	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...
C31609CADA1...	Executable	Automatic	Finished	1	2018 Mar 14 1...

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



Generated 0 minutes ago

Отправленные файлы



ФАЙЛ	ХЭШ	СТАТУС	СОСТОЯНИЕ	ПОСЛЕДНЯЯ ОБРАБ	ПОЛЬЗОВАТЕЛ:	ПРИЧИНА	ПОЛУЧАТЕЛЬ	КАТЕГОРИЯ	КОМПЬЮТЕР
file:///C:/Prog...metryClient.dll	9A556E9E2C37C505325C80F853754DD03416F050					Автоматически...	LiveGrid(R)	Исполняемый файл	es...
file:///C:/Prog...yDataShared.dll	60E730AA282C849CC047BC8E08BAE0EED5D14DE2					Автоматически...	LiveGrid(R)	Исполняемый файл	es...
file:///4FB79F...D05692420ECD0FE	5804A4926E689E6F11DC33D6A180E7DADEEB67D3					Автоматически...	LiveGrid(R)	Исполняемый файл	es...
file:///222289...57805576DF12268	9DF98144C07DE9D9F818038489210559AA3A237					Автоматически...	LiveGrid(R)	Исполняемый файл	es...
file:///C:/Wind...32/vmbuses.dll	842F1E3C2D9226681A249DE4839725287BCBD2C		Завершено	2018 июня 20 12:37:30	ESET\bsobolev	Вручную	Dynamic Threat Defense	Исполняемый файл	es...
http://ftp.nod...suspicious.bat	F02C266C43953E0A88257DF3CA017268798233		Завершено	2018 июля 20 00:13:50		Автоматически...	Dynamic Threat Defense	Сценарий	es...
http://ftp.nod...t_malicious.bat	1322926A4998C7A3A28231F865CD378F80D562ED		Завершено	2018 июля 20 00:13:49		Автоматически...	Dynamic Threat Defense	Сценарий	es...
http://ftp.nod...suspicious.bat	36C383332CDE5E2154C5F78AC1A79EFED2E4FC92		Завершено	2018 июля 20 00:13:49		Автоматически...	Dynamic Threat Defense	Сценарий	es...
http://tL.daum...ayerSetup64.exe	A7A7F0D1665EB1703F74A3C111F8535FF5728107		Завершено	2018 июня 20 15:18:49		Автоматически...	Dynamic Threat Defense	Исполняемый файл	es...
file:///C:/Prog...nuget/MyGet.ps1	E0881DABEB2A267DA0810EE4AE5897D14AEDC656		Завершено	2018 июля 23 15:37:50	NT AUTHORITY\сис...	Автоматически...	Dynamic Threat Defense	Сценарий	es...
file:///C:/Wind...F-BE1615FCE89F	986808DCFE80A936D033FE3C803858087D66EB362		Завершено	2018 июня 20 16:31:08	ESET\bsobolev	Автоматически...	Dynamic Threat Defense	Исполняемый файл	es...
file:///C:/Wind...F-BAA039D8FF31	74C77C6FAD0E016369F596EE2523257D9CC9217		Завершено	2018 июня 20 16:34:32	ESET\bsobolev	Автоматически...	Dynamic Threat Defense	Исполняемый файл	es...
file:///C:/Wind...2-372608D9C16E	62FA001137E66C8E3E38272844E82D7FA68A9020		Завершено	2018 июня 21 09:23:00	ESET\bsobolev	Автоматически...	Dynamic Threat Defense	Исполняемый файл	es...
file:///C:/Wind...ler/MSID9D8.tmp	A50D98617EA480205A9559E0983C5978411C7E82		Завершено	2018 июня 21 09:27:36	NT AUTHORITY\сис...	Автоматически...	Dynamic Threat Defense	Исполняемый файл	es...
file:///C:/Wind...3-E3AFF5EBD7E5	472E117F79F6C8EED0419F6DC271D54FF8D89AF7		Завершено	2018 июня 21 09:26:56	ESET\bsobolev	Автоматически...	Dynamic Threat Defense	Исполняемый файл	es...
file:///C:/User...eractiveRes.ps1	2DEFB85A2758AF744E3DD8AF3AAA153A2E4713		Завершено	2018 июля 19 12:38:37	ESET\bsobolev	Автоматически...	Dynamic Threat Defense	Сценарий	es...
file:///C:/User...eractiveRes.ps1	49044724698E6964DC93ACF5BEE2A7788EAD4133		Завершено	2018 июля 19 12:38:36	ESET\bsobolev	Автоматически...	Dynamic Threat Defense	Сценарий	es...
file:///C:/User...bcsResolve.ps1	D7745A4817748A466FFAAC350F939D58379F898		Завершено	2018 июня 21 09:40:12	ESET\bsobolev	Автоматически...	Dynamic Threat Defense	Сценарий	es...
file:///C:/User...roubleshoot.ps1	7008E759CB47BF744A4E4CD911DE158EF00AC84		Завершено	2018 июня 21 09:40:11	ESET\bsobolev	Автоматически...	Dynamic Threat Defense	Сценарий	es...
file:///C:/User...sticsVerify.ps1	4658484E0E3AC862667D54617422787C8899408		Завершено	2018 июня 21 09:37:06	ESET\bsobolev	Автоматически...	Dynamic Threat Defense	Сценарий	es...
file:///C:/User...tDPSService.ps1	0C9DD05514D062354C0ECC9AEBD4371233058B		Завершено	2018 июля 16 18:05:17	ESET\bsobolev	Автоматически...	Dynamic Threat Defense	Сценарий	es...
file:///C:/User...ityFirewall.ps1	78F2C8C39821DADE6E3EA553488AEF845663A00		Завершено	2018 июня 21 09:40:11	ESET\bsobolev	Автоматически...	Dynamic Threat Defense	Сценарий	es...
file:///C:/User...tyFunctions.ps1	FB35AF68329D60B0EC92E24230EAFCE8E1280A9F9		Завершено	2018 июня 21 09:40:11	ESET\bsobolev	Автоматически...	Dynamic Threat Defense	Сценарий	es...

ДОБАВИТЬ ИСКЛЮЧЕНИЕ В ПОЛИТИКУ

OO

! Подозрительный

Статус **!** Подозрительный
Состояние **✓** Завершено
Последняя обработка 2018 июля 20 00:13:49
Отправлено 2018 июня 20 12:35:41
Поведение [Просмотреть поведение](#)

http://ftp.nod...._suspicious.bat

Компьютер esetnote25.eset.local
Пользователь
Причина Автоматически
Получатель Dynamic Threat Defense
Хэш 36C3B3332CDE52E154C5F78AC1A79EFED2EF4C92

Анализ

Статус **!** Подозрительный
Состояние **✓** Завершено
Отправлено 2018 июня 20 12:35:41
Последняя обработка 2018 июля 20 00:13:49

Источник

Компьютер esetnote25.eset.local
Пользователь
Причина Автоматически
Получатель Dynamic Threat Defense

Файл

Хэш 36C3B3332CDE52E154C5F78AC1A79EFED2EF4C92
Имя файла http://ftp.nod.sk/~mcipak/beta/ESET Dynamic Threat Defense/EDTD compatible v7 products/EDTD_test_suspicious.bat
Размер 150 Б (150 байт)

! ОТЧЕТ О ПОВЕДЕНИИ ФАЙЛОВ



СТАТУС	Подозрительный
SNA-1	36C3B3332CDE52E154C5F78AC1A79EFED2EF4C92
РАЗМЕР	150Б
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



ENTERPRISE INSPECTOR

NEW

ESET ENTERPRISE INSPECTOR: КАК РАБОТАЕТ

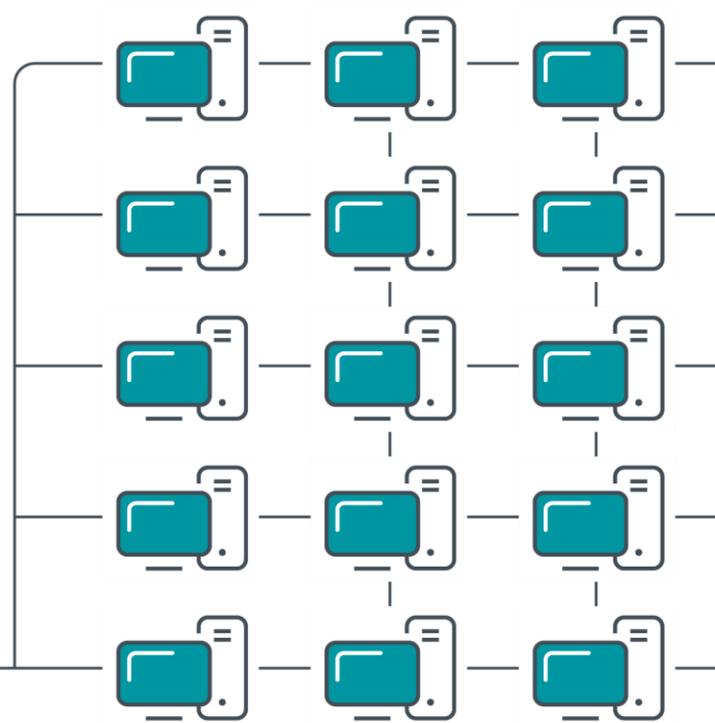


- ✓ **Собирает информацию** в режиме реального времени
- ✓ Обеспечивает **фильтрацию и сортировку**
- ✓ Позволяет создавать **собственные правила**
- ✓ Использует систему репутаций **ESET LiveGrid**

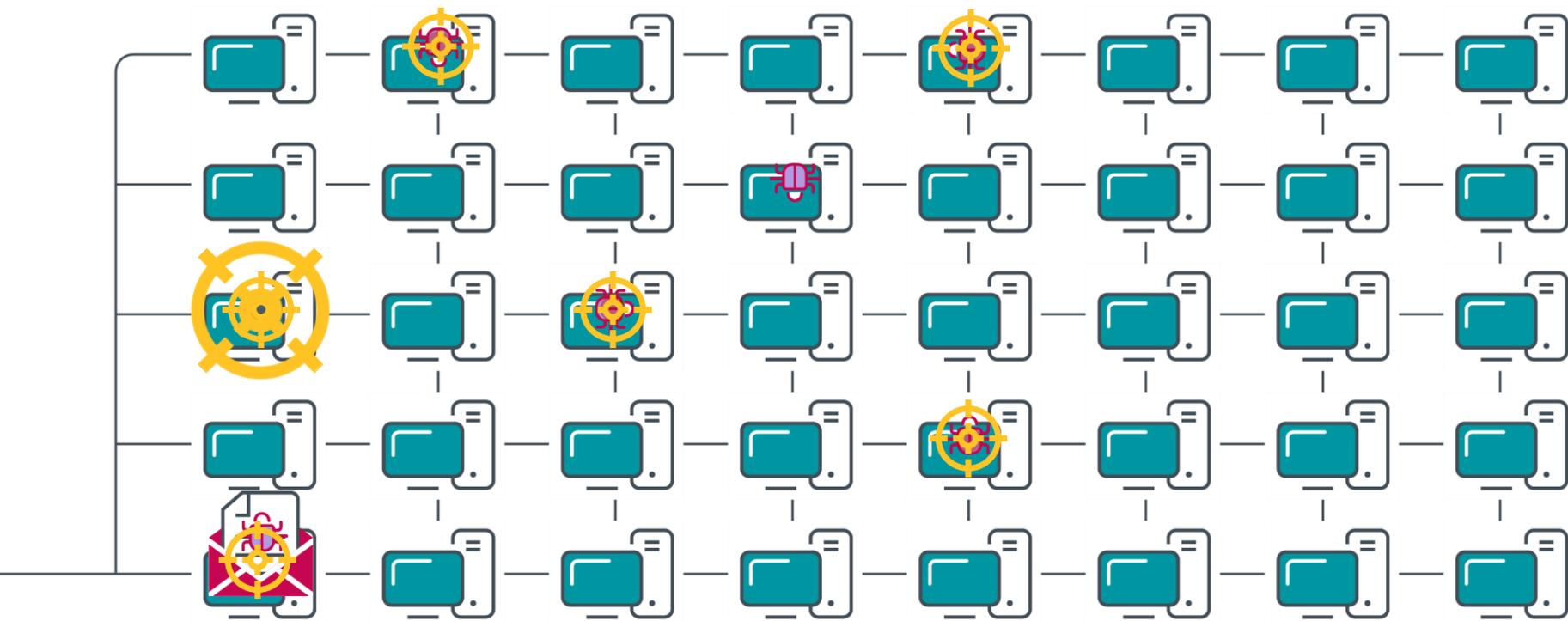
ESET Dynamic Threat Defense



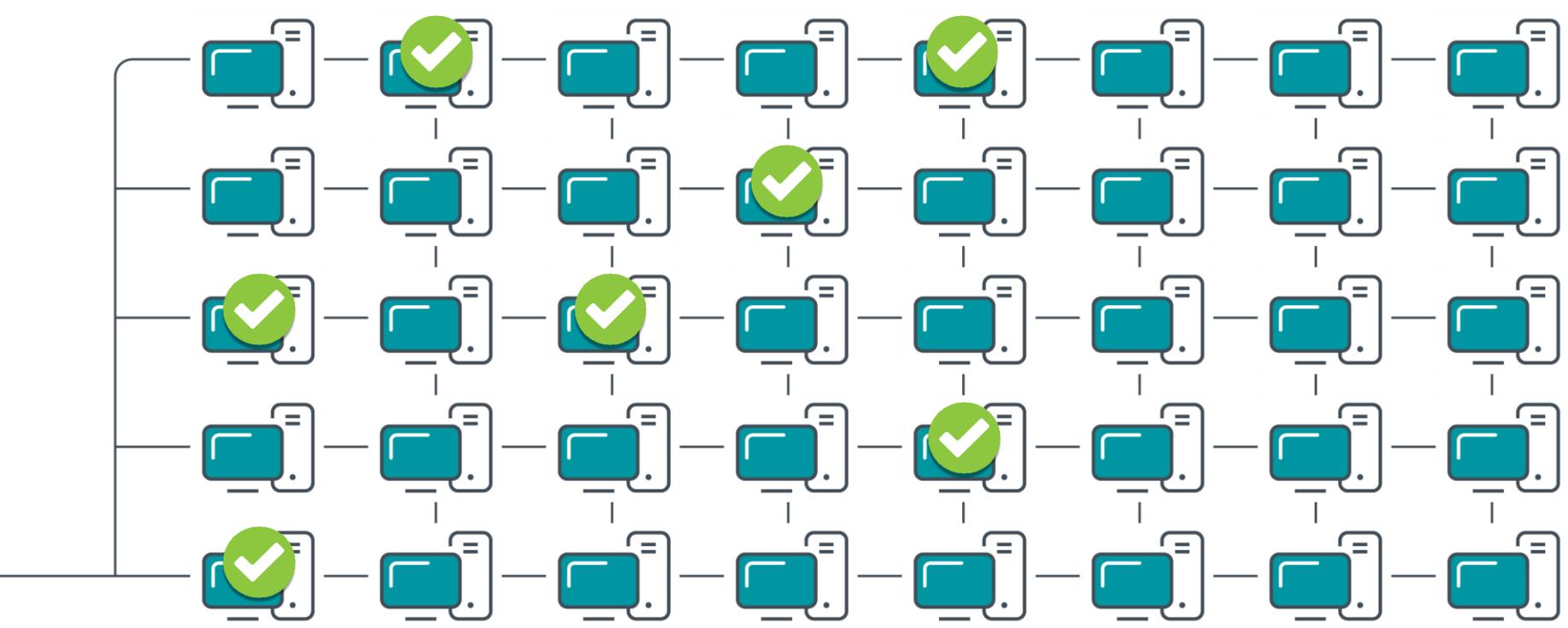
Сервер
с EMS & EDTD



Конечные точки



Конечные точки

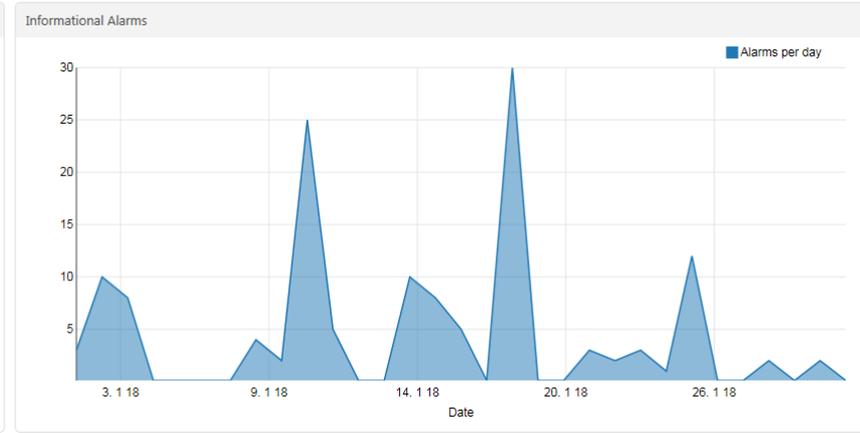
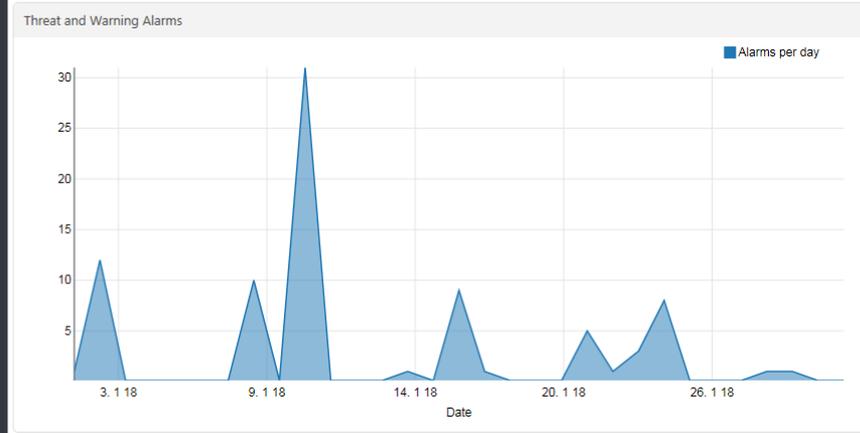
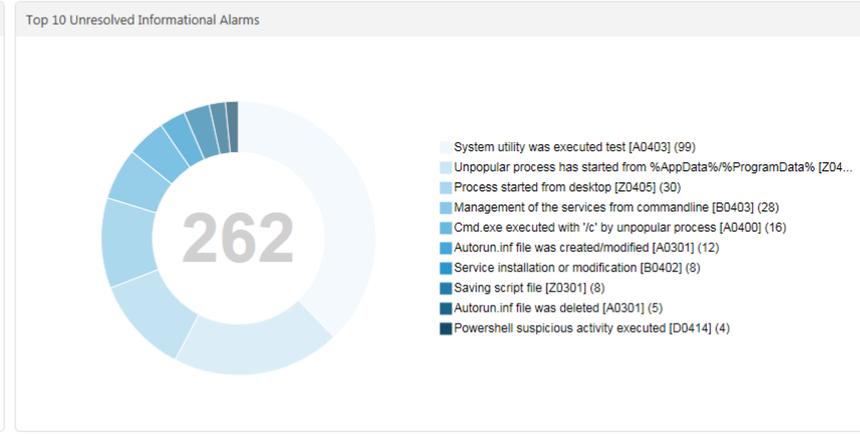
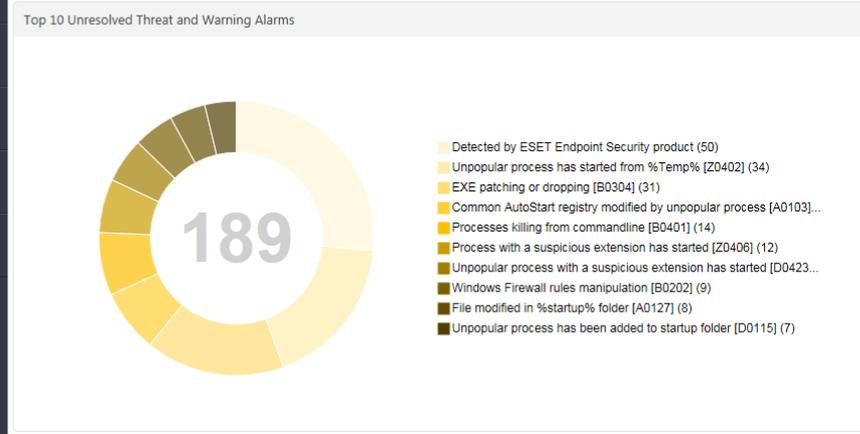


Endpoints

- DASHBOARD
- ALARMS
- EXECUTABLES
- SCRIPTS
- COMPUTERS
- ADMIN

Dashboard ADD FILTER

- Alarms
- Executables
- Computers
- More
- Server status



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



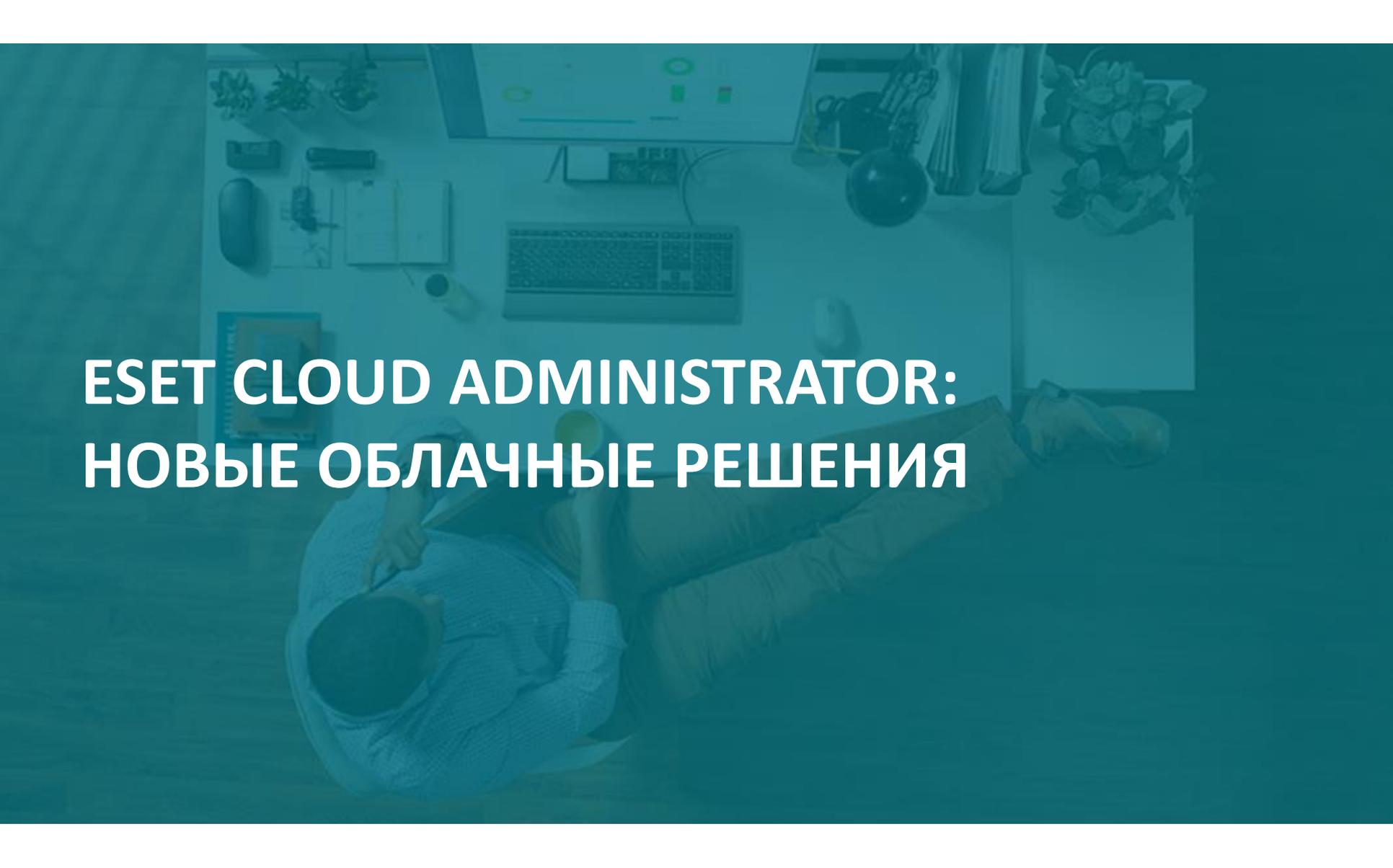
Отображение



Реагирование



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА



**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

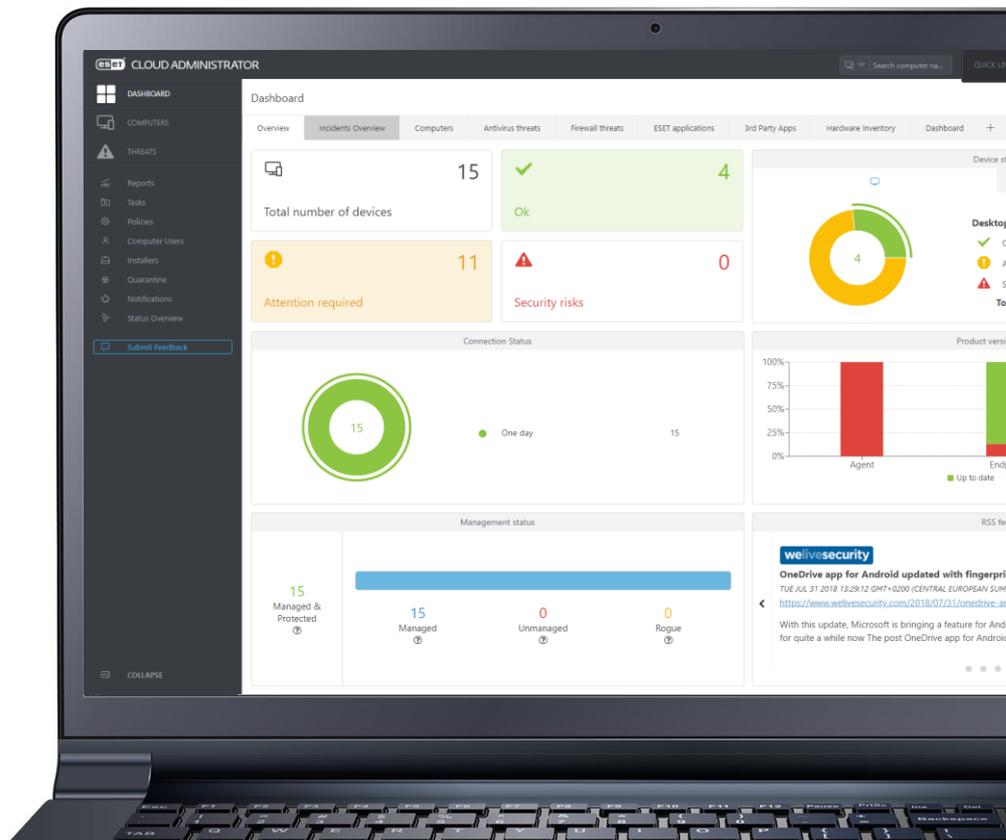


ESET Secure Business Cloud

- 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



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](#)

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

Общее количество устройств **1**

OK

0

OK

1

Требуется вмешательство

0

Угрозы безопасности

Состояние устройства

Настольные компьютеры

OK	0
Требуется вмешательство	1
Угроза безопасности	0
Всего	1

Состояние подключения

1

> 7 кол-ва дней

Состояние версии продукта

Категория	Актуальная версия	Устарело
Агент	0	100
Конечная точка	0	100
Сервер	0	0

Состояние управления

1 Под управлением и защитой	1 Управляемые	0 Неуправляемый	0 Неавторизованные
---------------------------------------	-------------------------	---------------------------	------------------------------

RSS-канал

welivesecurity

DanaBot updated with new C&C communication

TUW 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?



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



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



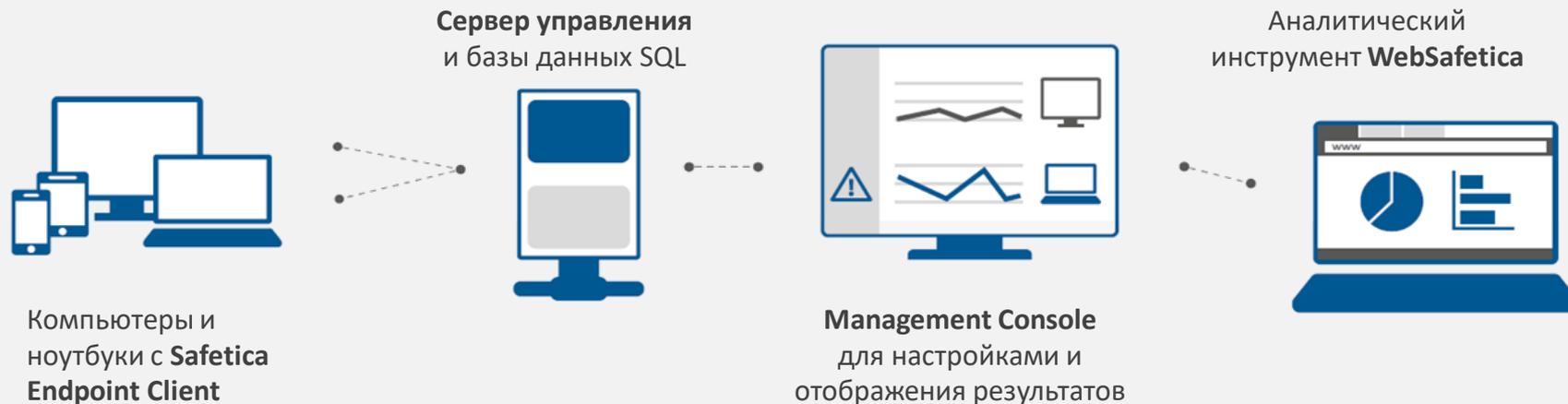
КОНТЕКСТНЫЙ ФИЛЬТР

ПРИНЯТИЕ РЕШЕНИЯ ПО ФОРМАЛЬНЫМ
ПРИЗНАКАМ

НИКАКИХ СКРЫТЫХ РАСХОДОВ

Офисный контроль и DLP “Safetica”

АРХИТЕКТУРА РЕШЕНИЯ



Клиент

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

Сервер

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

База данных (MS SQL)

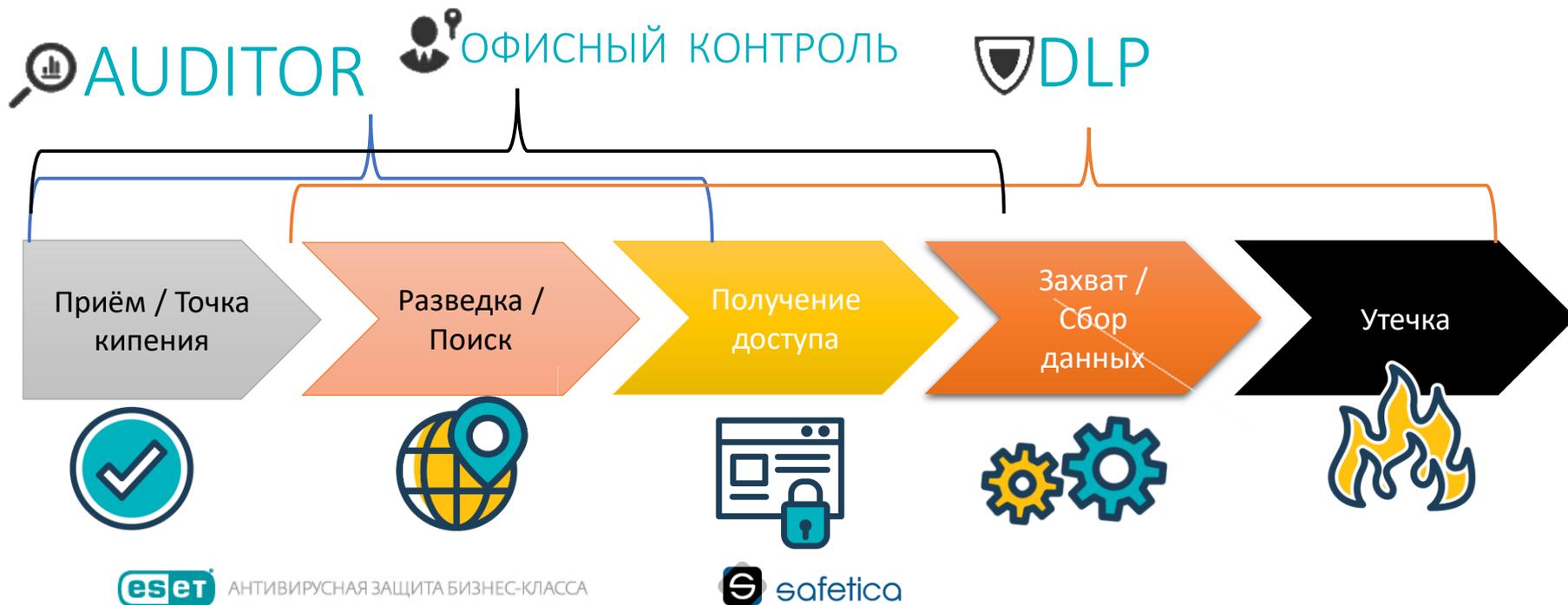
MS SQL 2008 R2 и выше,
рекомендуется MS SQL 2012 и выше
MS SQL 2012 Express включена в
установочный пакет Safetica

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



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ AUDITOR)



АУДИТ
ЧУВСТВИТЕЛЬНЫХ
ДААННЫХ КОМПАНИИ



ПРЕДСТАВЛЕНИЕ О
ТОМ, ЧТО ПРОИСХОДИТ
В КОМПАНИИ



УМЕНЬШЕНИЕ
РАСХОДОВ НА
ПЕРСОНАЛ



ПОВЫШЕНИЕ
ЭФФЕКТИВНОСТИ
СОТРУДНИКОВ



СОКРАЩЕНИЕ
РАСХОДОВ КОМПАНИИ
НА ОФИСНЫЕ НУЖДЫ



СРАВНЕНИЕ РАБОТЫ
СОТРУДНИКОВ



СОБЛЮДЕНИЕ ПОЛИТИК
БЕЗОПАСНОСТИ



ОКУПАЕМОСТЬ
ВНЕДРЕНИЯ

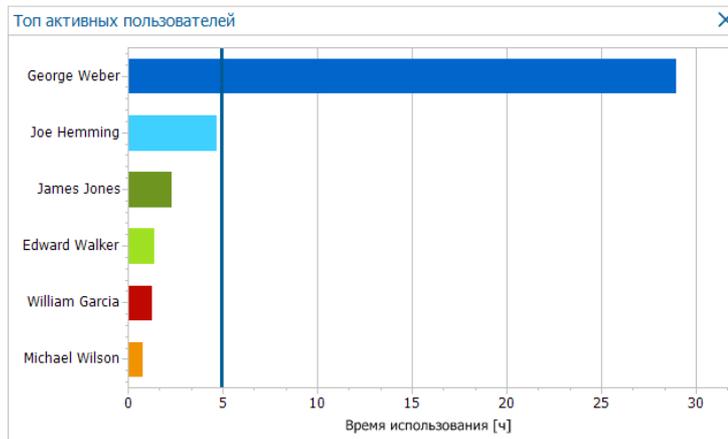
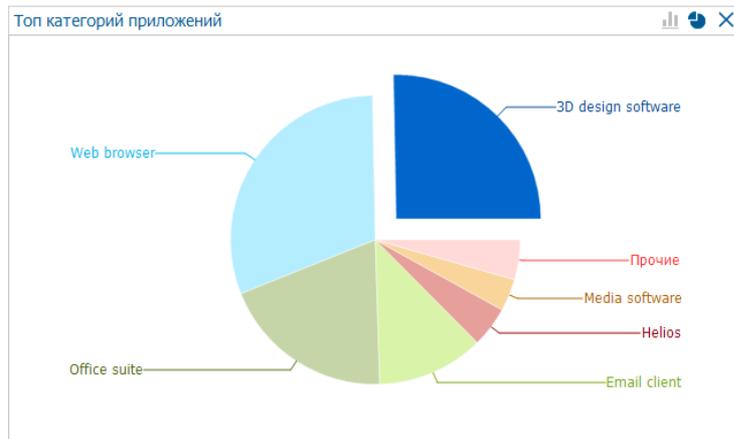


ЭФФЕКТИВНОСТЬ
ИСПОЛЬЗОВАНИЯ ПО

ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ AUDITOR)



ГРАФИКИ



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

ЗАПИСИ

Перетащите под тот текст столбцы, по которым вы хотите сгруппировать

Приложение

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

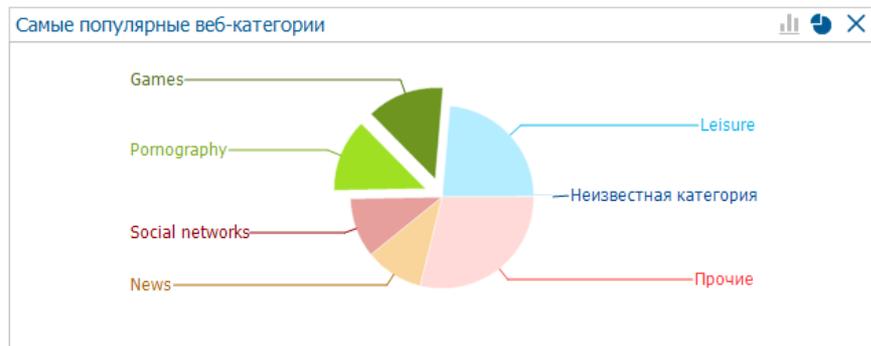
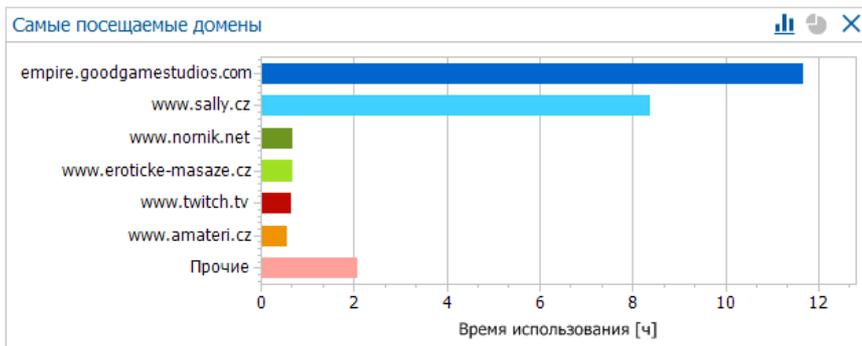
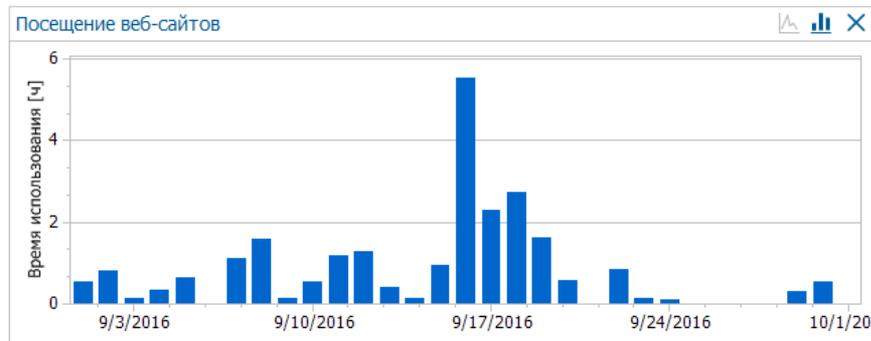
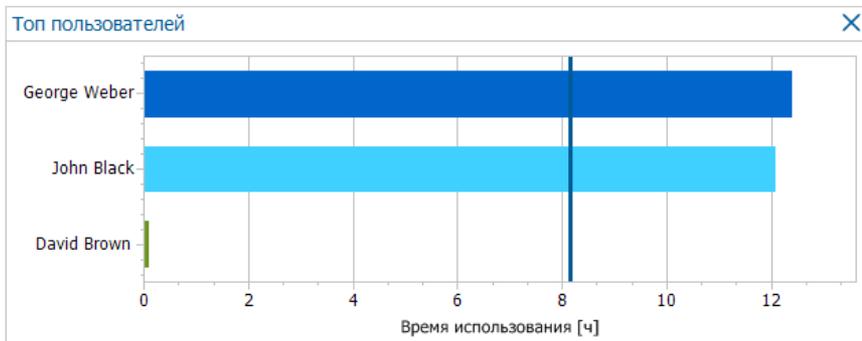
Упорядочить

Категория приложен... Y



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ AUDITOR)



ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ SUPERVISOR)



WEB-КОНТРОЛЬ

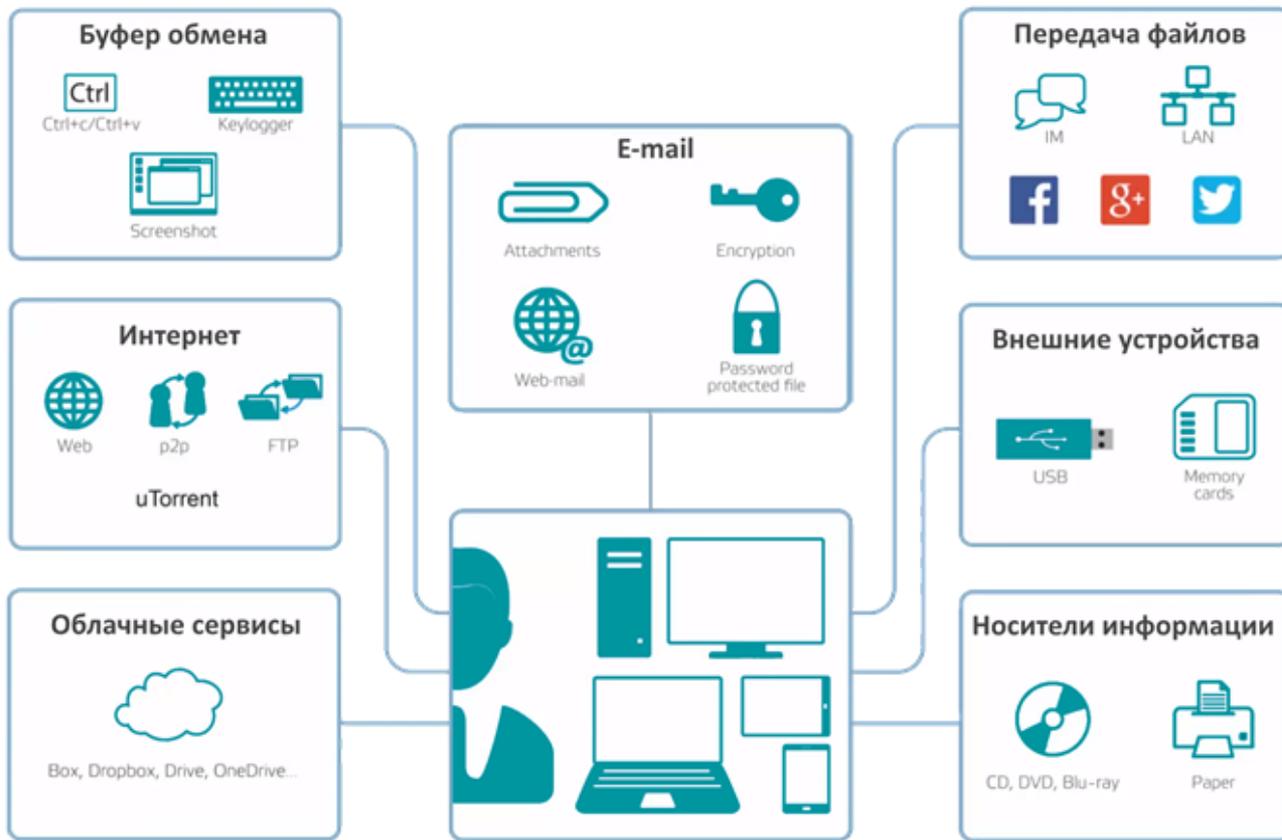


КОНТРОЛЬ ПРИЛОЖЕНИЙ



КОНТРОЛЬ ПЕЧАТИ

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (МОДУЛЬ DLP)



КОНТЕКСТНЫЙ ФИЛЬТР

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

В 12В14

ABC

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

ПРАВИЛА ПОЛИТИКИ

Шаблон политики: Пользовательский - Настроить

Загрузка в сеть: Безопасные зоны разрешены

Email: Зарегистрирован

Интернет мессенджеры: Разрешен

Внешние устройства: Безопасные зоны разрешены

Облачные хранилища: Зарегистрирован

ПРАВИЛА ПОЛИТИКИ

Шаблон политики: Встроенные: Управление к - Настроить

Загрузить в общую папку: Зарегистрирован

Загрузить на веб-почту: Зарегистрирован

Загрузка в сеть: Разрешен

Email: Разрешен

Интернет мессенджеры: Зарегистрирован

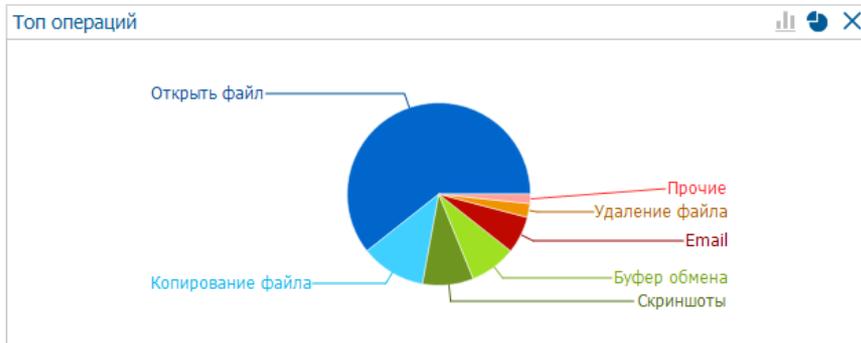
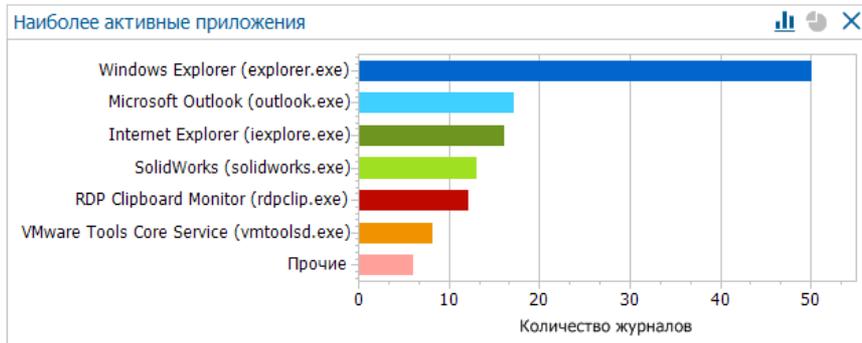
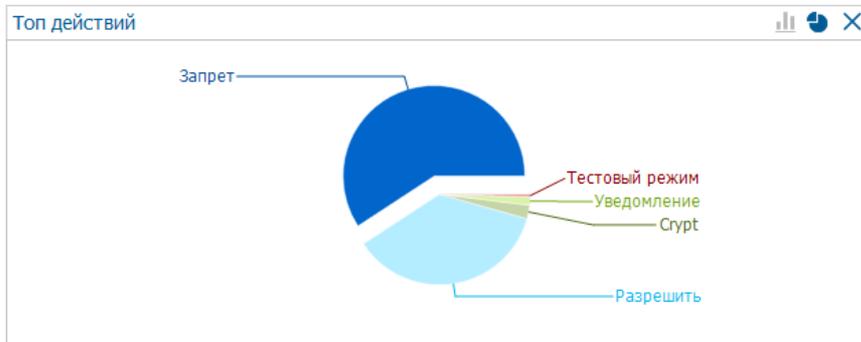
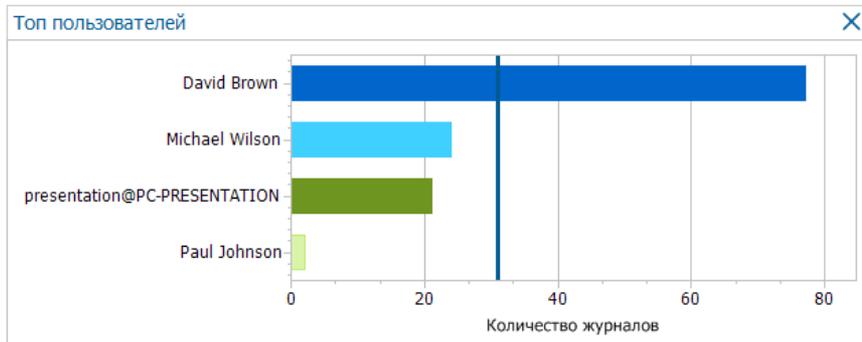
Внешние устройства: Безопасные зоны разрешены

Облачные хранилища: Пользовательский

Принтеры: Безопасные зоны разрешены

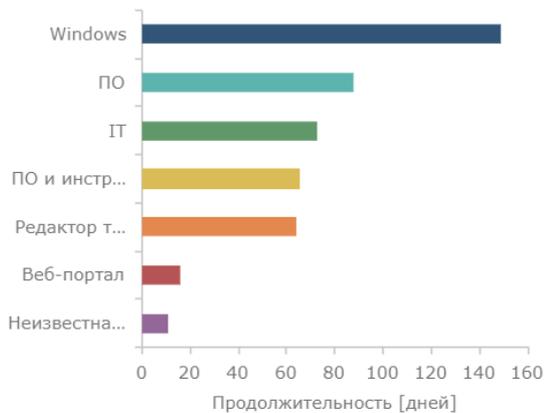


ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (МОДУЛЬ DLP)



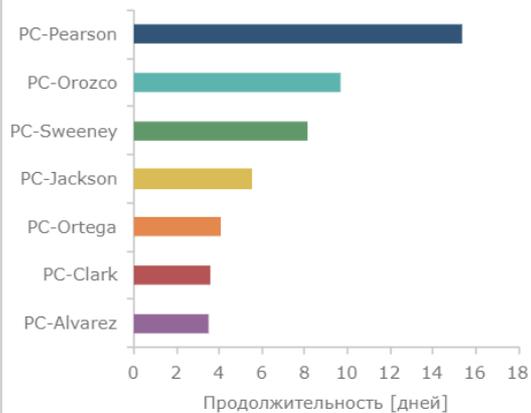
АНАЛИЗ РЕЗУЛЬТАТОВ WEBSAFETICA

КАК СОТРУДНИКИ ИСПОЛЬЗОВАЛИ С...



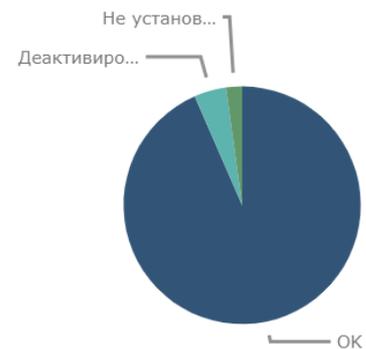
АНАЛИЗ ПОВЕДЕНИЯ >

КАКИЕ КОМПЬЮТЕРЫ БЫЛИ НАИБО...



ИСПОЛЬЗОВАНИЕ РЕСУРСОВ >

КАК ЗАЩИЩЕНА МОЯ КОМПАНИЯ?



УПРАВЛЕНИЕ >



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

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**

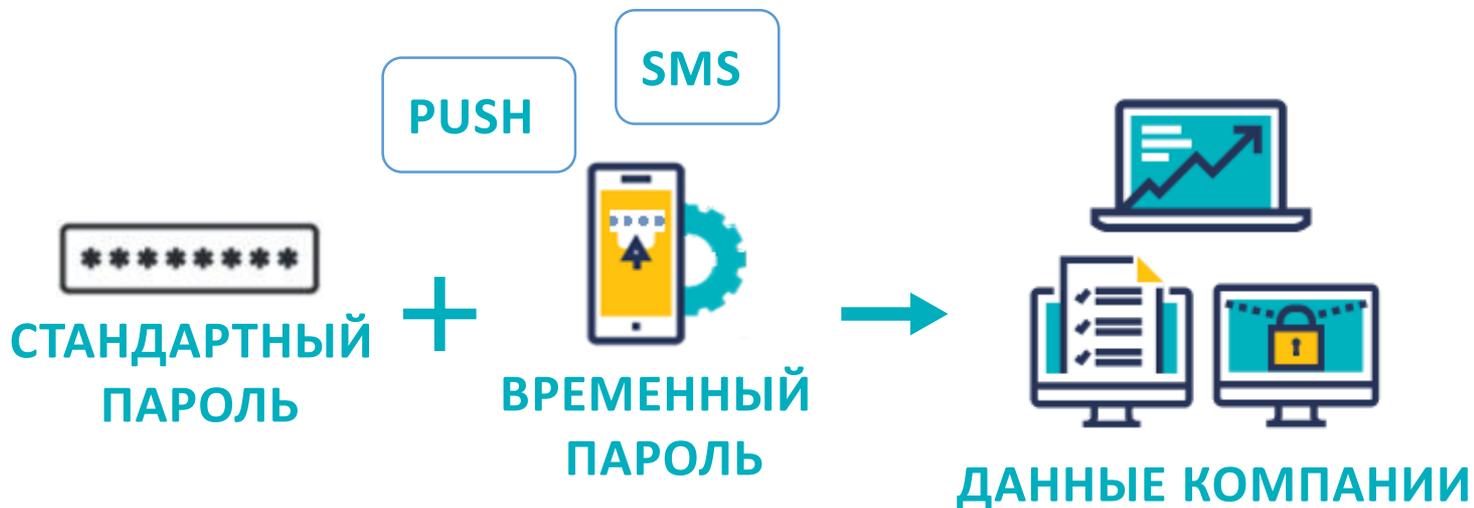


ПАРОЛИ ПИШЕМ ИЛИ ЗАПОМИНАЕМ?



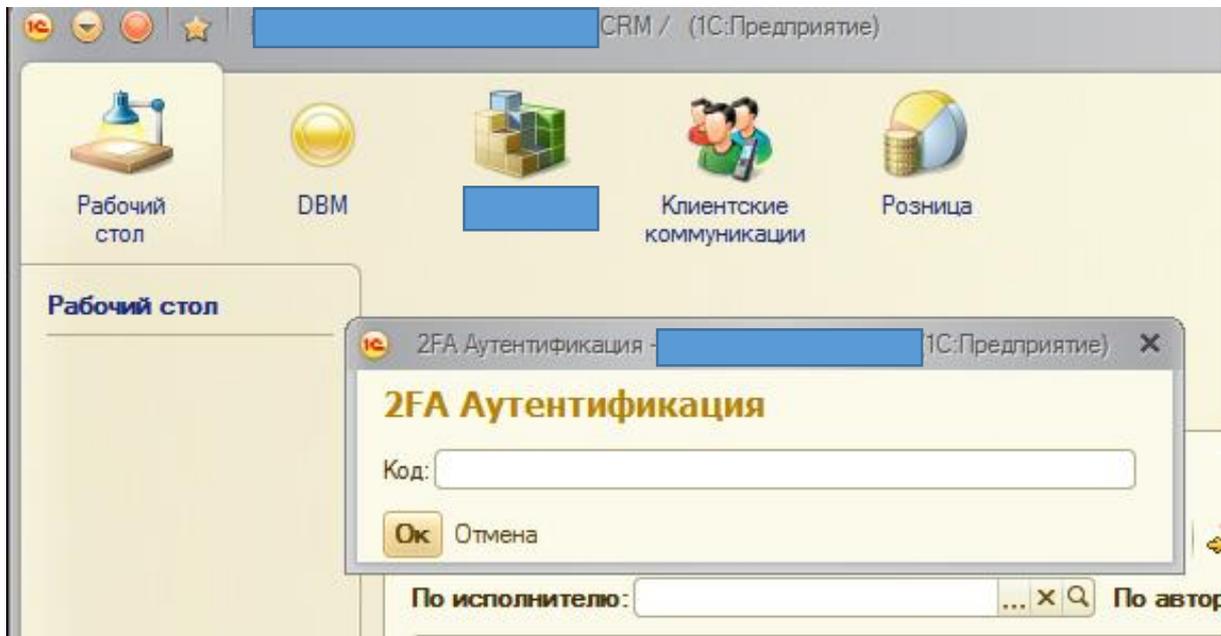
АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

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?

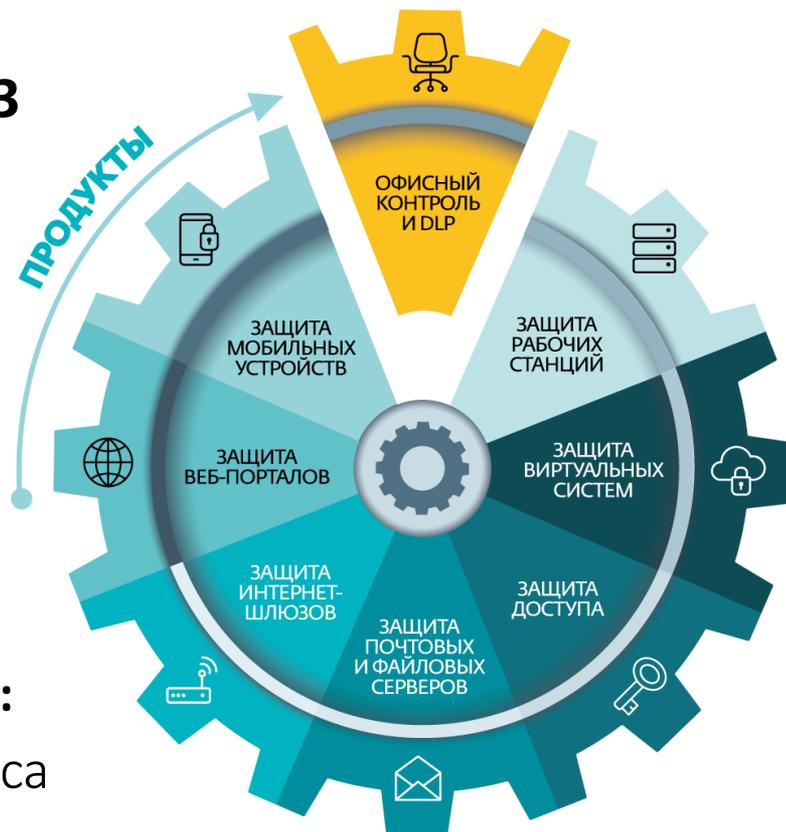
КОМПЛЕКСНЫЙ ПОДХОД:

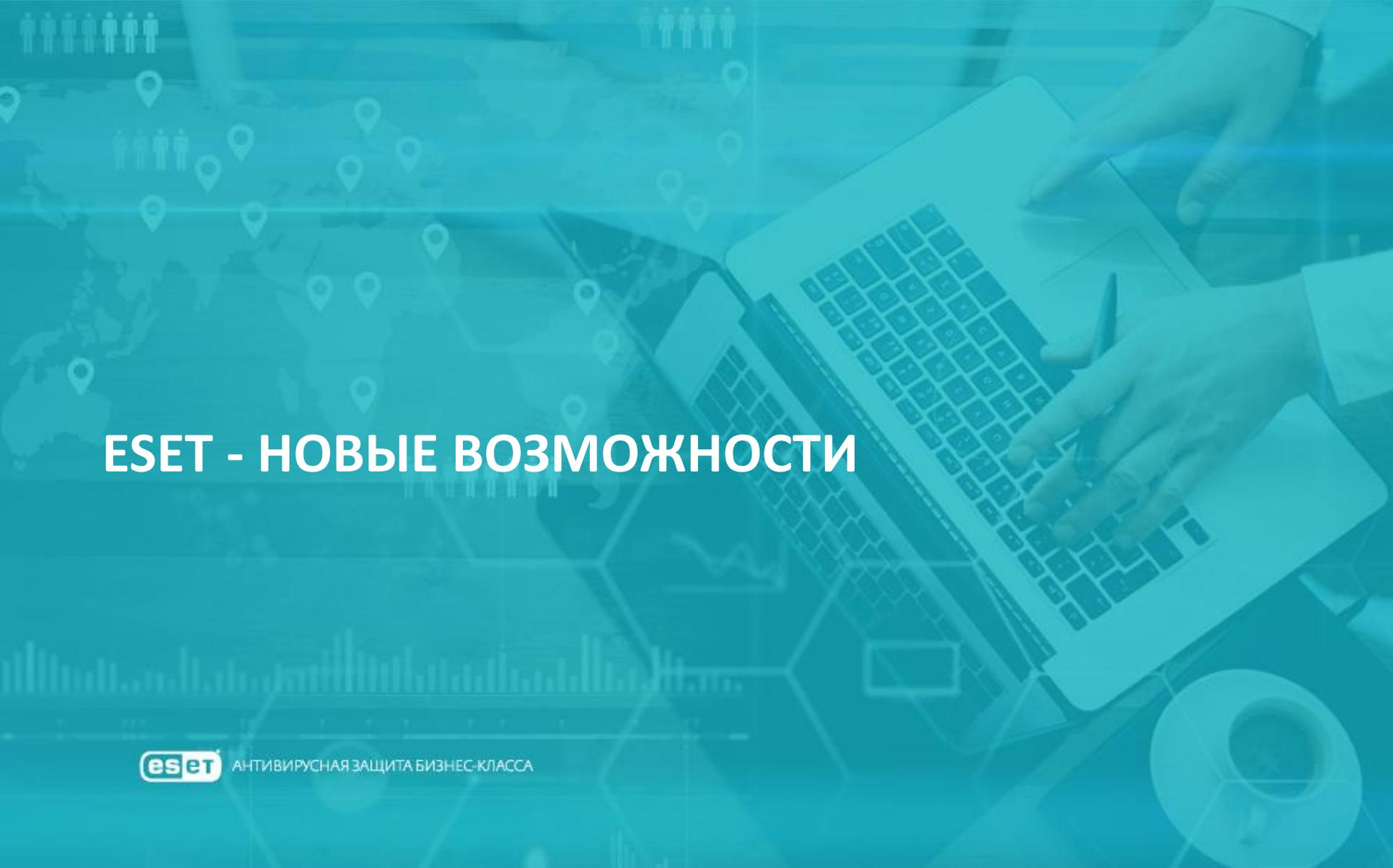
1. БЕЗОПАСНОСТЬ ОТ ВНЕШНИХ УГРОЗ

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

2. БЕЗОПАСНОСТЬ ОТ ВНУТРЕННИХ УГРОЗ:

- › Офисный контроль и DLP Safetica
- › ESA





ESET - 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



Технологии обнаружения



Защита от сетевых атак



Репутация и кеш



Расширенное сканирование памяти



Защита от программ-вымогателей

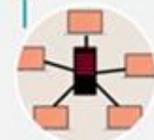
Анализ кода/Извлечение признаков /Машинное обучение/

Песочница

ДНК сигнатуры



Защита от эксплойтов



Защита от ботнетов



Отслеживание ботнетов



Облачная система защиты



Внешние источники образцов и URL



Портал ESET Threat Intelligence



Отчеты ESET Threat Intelligence



Поставка данных киберразведки



Поиск по правилам YARA

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