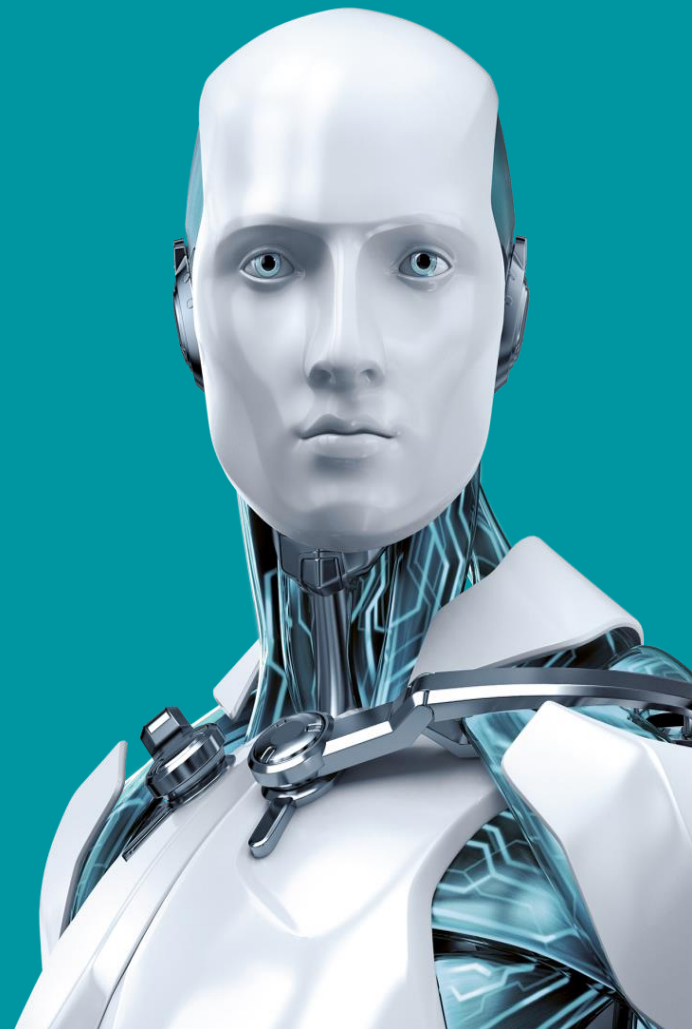
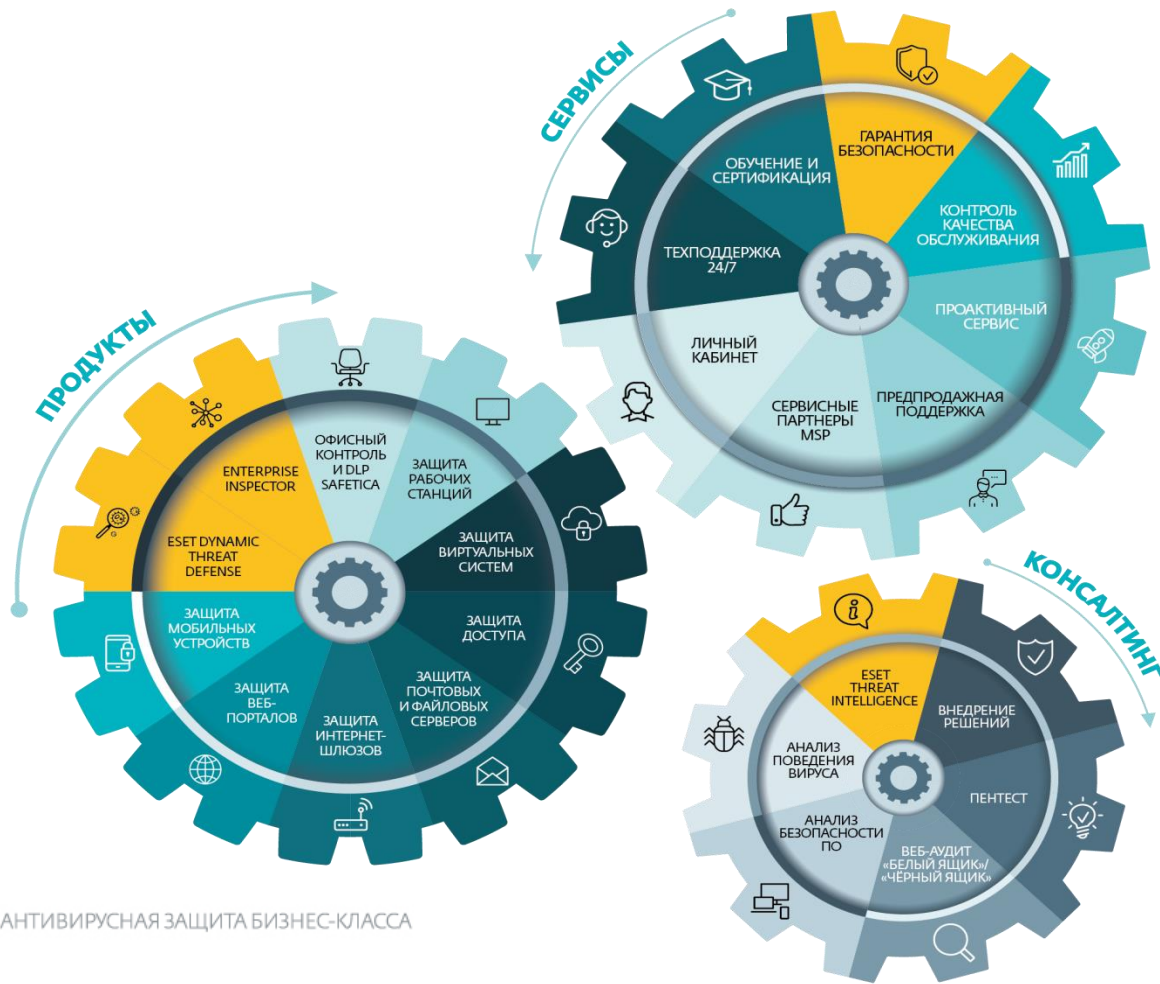


# ESET-не только антивирус

Бойков Иван  
Региональный представитель  
на территории ЦФО

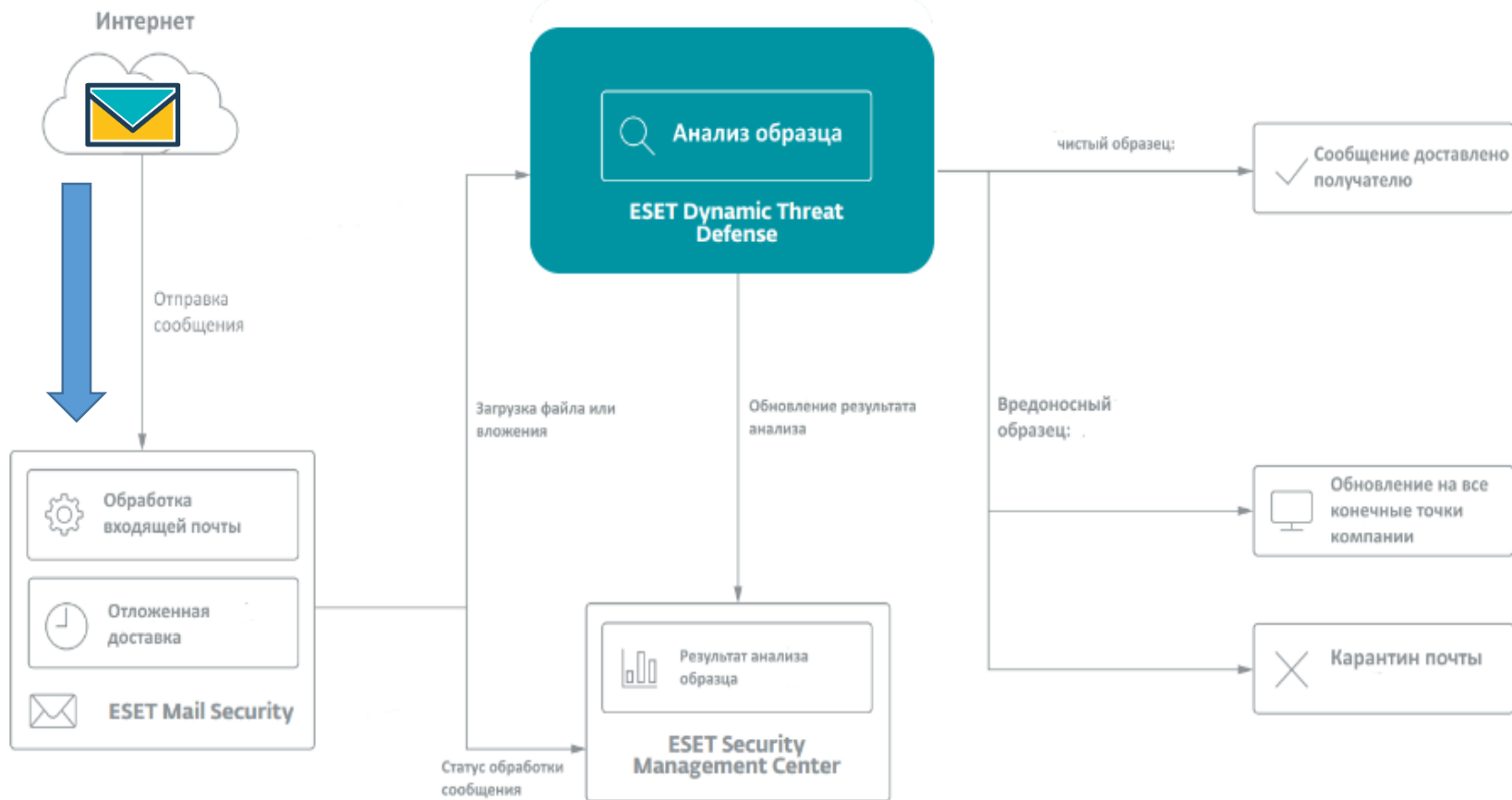


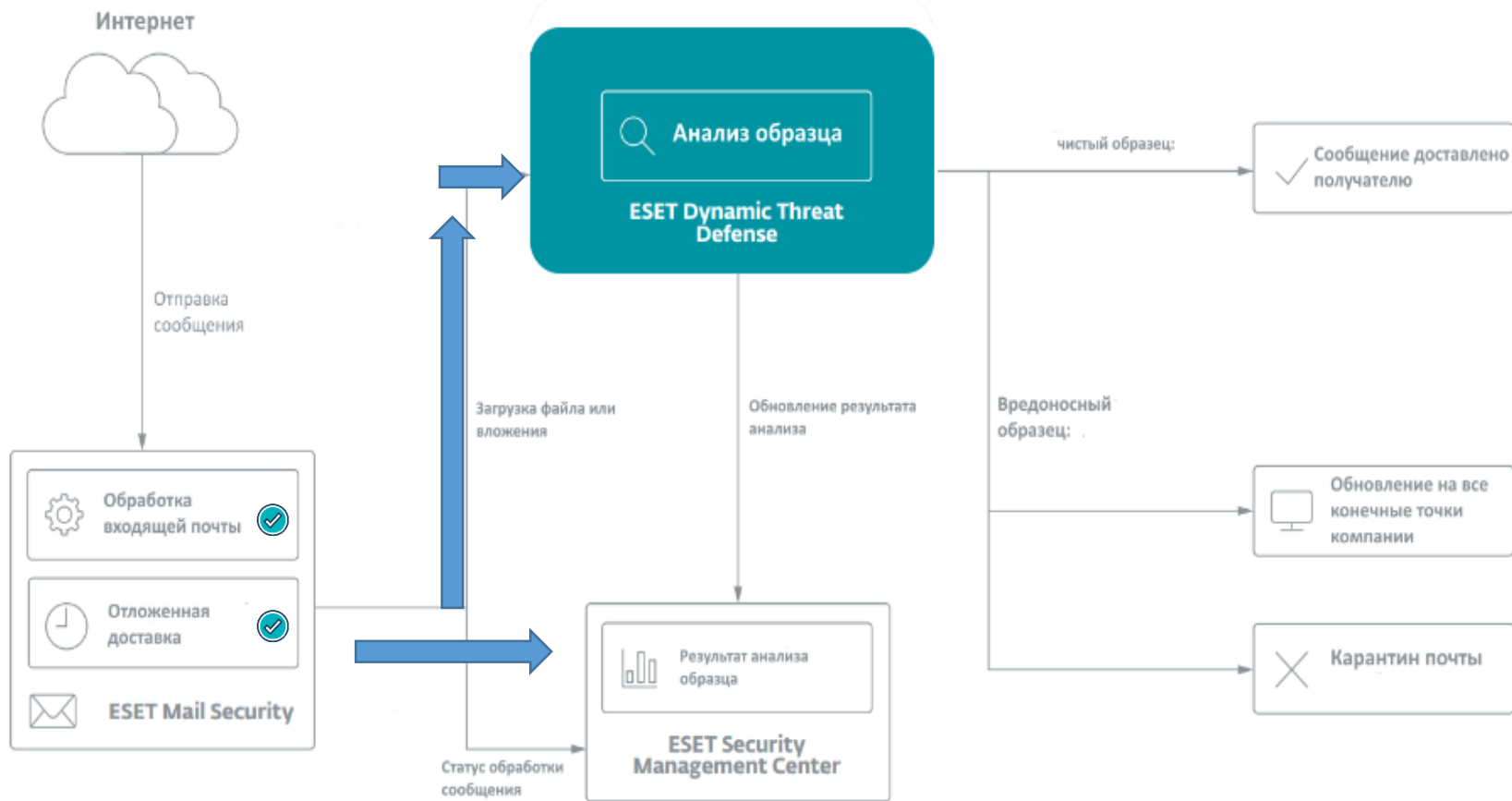
# ПРОДУКТЫ, СЕРВИСЫ И КОНСАЛТИНГ

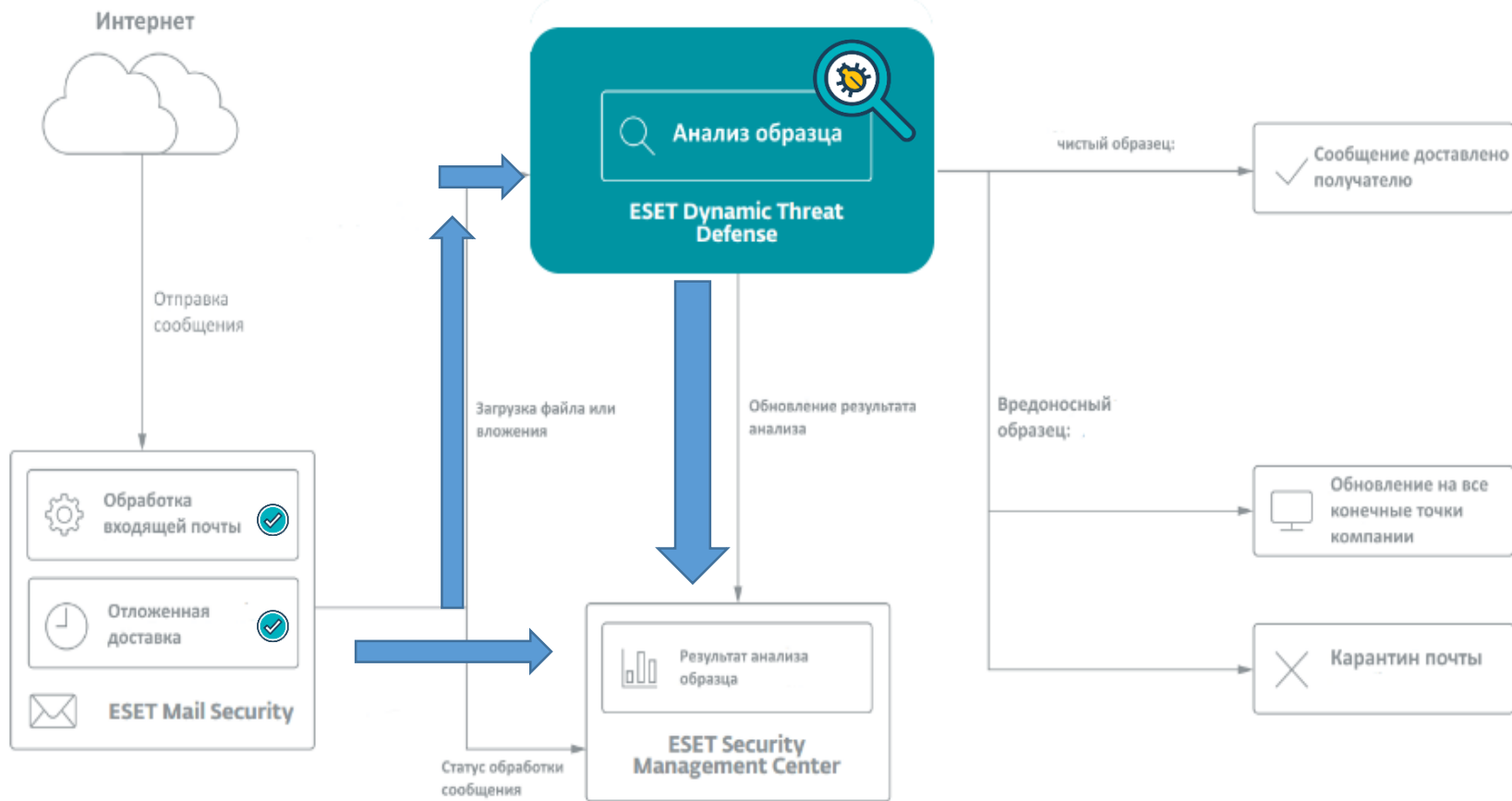


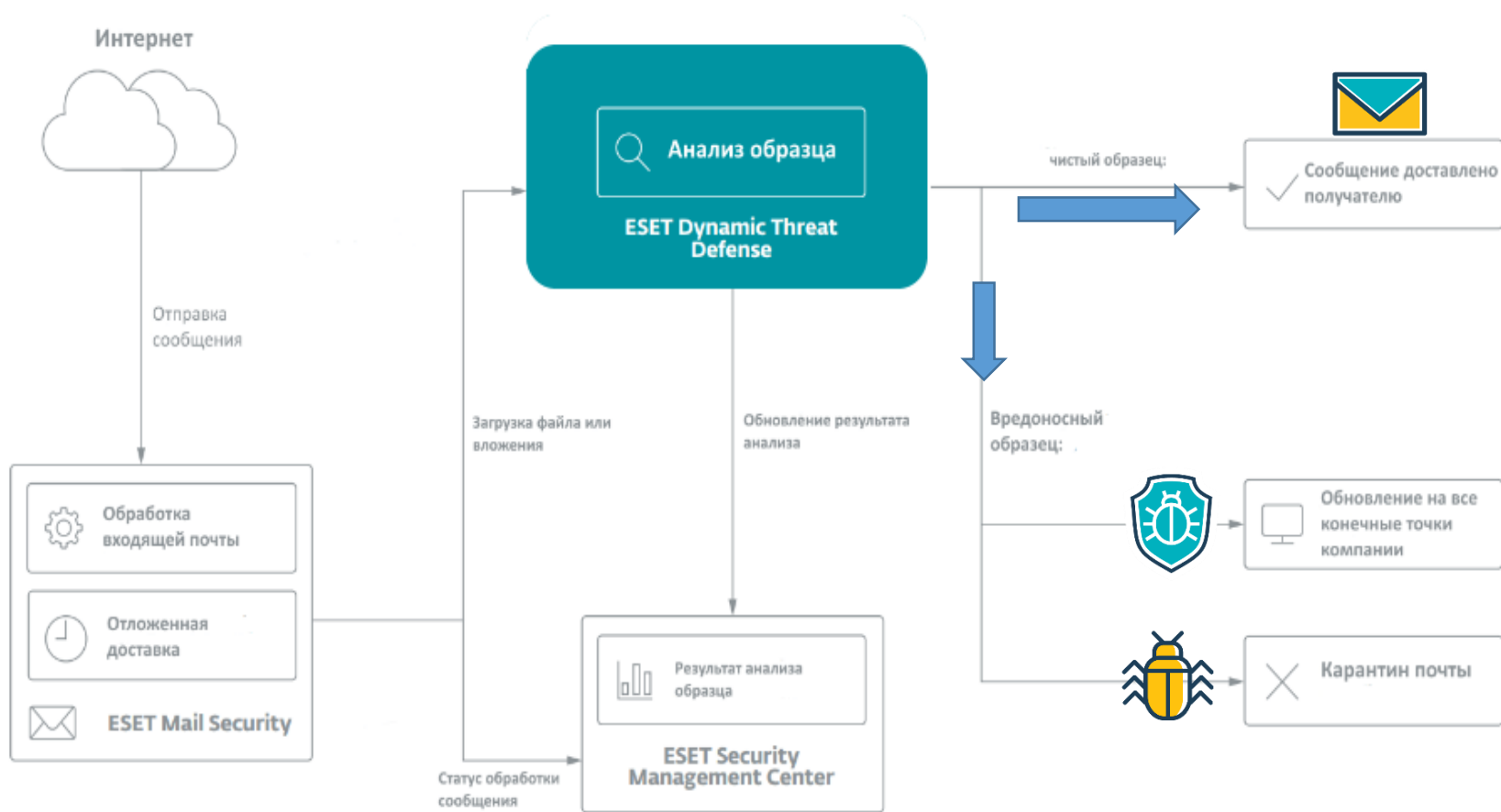


DYNAMIC THREAT DEFENSE









Лицензии

СОСТОЯНИЕ



<input type="checkbox"/> ЛИЦЕНЗИЯ	ПРОДУКТ	ВЛАДЕЛЕЦ	СОСТОЯНИЕ	
<input type="checkbox"/>		@esetnod32.ru		
<input type="checkbox"/>		iv@esetnod32.ru		

## Добавить лицензию

Лицензионный ключ содержится в письме с подтверждением, которое вы получаете по электронной почте сразу после покупки. Если вы купили продукт в магазине, ключ находится на лицензионной карточке.

## Лицензионный ключ

Если у вас уже есть имя пользователя и пароль для продукта ESET, вы можете [преобразовать их в лицензионный ключ](#).

ПРОДОЛЖИТЬ

ОТМЕНА

+ ДОБАВИТЬ ЛИЦЕНЗИЮ

УДАЛИТЬ



- Группы
- Шаблоны динамических групп
- Отправленные файлы
- Карантин
- 1** Управление лицензиями
- ПРАВА ДОСТУПА
- Пользователи
- Наборы разрешений
- СЕРТИФИКАТЫ

Управление лицензиями

Кем активи... ГРУППА... Вы...

- Влада Сидорова**
- ESET Enterprise Inspector MTA
- ESET Enterprise Inspector MTA

Лицензии ДОБАВИТЬ ФИЛЬТР ПРЕДУСТАНОВКИ

ОТКРЫТЫЙ ИДЕНТИФИКАТОР	ИМЯ ПРОДУКТА	СОСТ.	МОДУЛИ	ПОДМОДУЛИ	СРОК ДЕЙСТВИЯ:
3AD-N94-4M8	ESET Dynamic Threat Defense for ...	Ⓜ	0/10 (0 в а...		2018 июля 20 15:00:00
3AD-N94-4M8	Использовать лицензию для активации	✓			2018 дек. 31 15:00:00

- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 1** ... >

### Изменить клиентскую задачу

Клиентские задачи > Изменить клиентскую задачу

- Основное
- Параметры
- Сводка**

### Основное

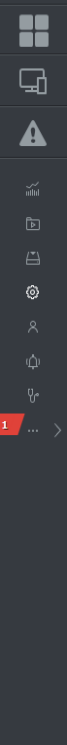
**Имя**  
Активация EDTD

**Описание**

**Тип задачи**  
Активация программы

### Настройки активации программы

**Лицензия ESET**  
ESET Dynamic Threat Defense for Mail Security, открытый идентификатор — 3AD-N94-4M8, влад 15:00:00



## Изменить политику

Политики &gt; Изменить политику

Основное

Параметры

Назначение

Сводка

## ESET Endpoint for Windows

Введите текст для поиска...



## МОДУЛЬ ОБНАРУЖЕНИЯ 14

Защита файловой системы в режиме реального времени

## Облачная защита 14

Процессы сканирования вредоносных программ

NIPS

ОБНОВЛЕНИЕ

ЗАЩИТА СЕТИ

## + ОБЛАЧНАЯ ЗАЩИТА 12

## - ESET DYNAMIC THREAT DEFENSE 2

Порог обнаружения

≥ 7.0

Подозрительные

Действие по обнаружении

≥ 7.0

Завершить активный проц

## Новая политика

Политики &gt; Новая политика

Основное

Параметры

Назначение

Сводка

ESET Mail Security for Microsoft Exchange (V6+)

Введите текст для поиска...



СЕРВЕР

## КОМПЬЮТЕР 3

Защита файловой системы в режиме реального времени

## Облачная защита 3

Процессы сканирования вредоносных программ

Сканирование Hyper-V

## + ОБЛАЧНАЯ ЗАЩИТА

## - ESET DYNAMIC THREAT DEFENSE 3

Порог обнаружения

≥ 7.0

Очень подозрительные

Действие по обнаружении

≥ 7.0

Завершить активный проц

Максимальное время ожидания результатов анализа (мин)

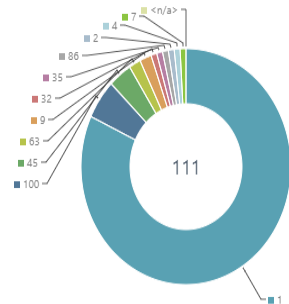
≥ 7.0

5

## Dashboard

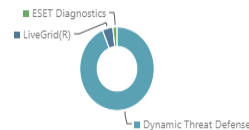
Overview Incidents Overview Computers Security Management Center Server Antivirus threats Firewall threats ESET applications ETD

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...



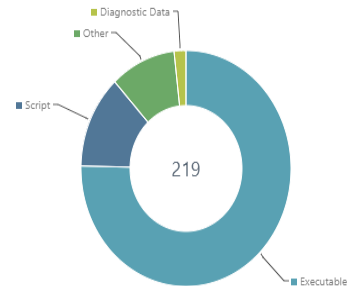
Generated 0 minutes ago

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 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...



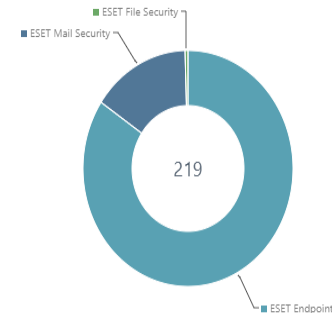
Generated 0 minutes ago

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...
F9D3BEAF78D...	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...
A585F3A172EB...	Executable	Automatic	Finished	1	2018 Mar 16 1...
49521A5A03BE...	Executable	Automatic	Finished	45	2018 Mar 16 1...
1E4A48BEC5E4...	Script	Automatic	Finished	1	2018 Mar 15 1...
0DA78D177B9...	Script	Automatic	Finished	1	2018 Mar 15 1...
3F37A08C29E6...	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...
C1680CADA1...	Executable	Automatic	Finished	1	2018 Mar 14 1...

Generated 0 minutes ago

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



Generated 0 minutes ago

## Отправленные файлы



ДОБАВИТЬ ФИЛЬТР

ПРЕДУСТАНОВКИ

ФАЙЛ	ХЭШ	СТАТУС	СОСТОЯНИЕ	ПОСЛЕДНЯЯ ОБРАБ	ПОЛЬЗОВАТЕЛИ	ПРИЧИНА	ПОЛУЧАТЕЛЬ	КАТЕГОРИЯ	КОМПЬЮТЕР
file:///C:/Prog...metryClient.dll	9A556E9E2C37C505325C80F853754DD03416F050					Автоматически...	LiveGrid(R)	Исполняемый файл	
file:///C:/Prog...yDataShared.dll	60E730AA282C849C047BCBE08BAEE0EED5D14DE2					Автоматически...	LiveGrid(R)	Исполняемый файл	
file:///4FB79F...D05692420ECD0FE	5804A4926689E6F11DC33D6A180E7DADEE867D3					Автоматически...	LiveGrid(R)	Исполняемый файл	
file:///222289...57805576DF12268	9DDF98144C07DE9D9F818038489210559AA3A237					Автоматически...	LiveGrid(R)	Исполняемый файл	
file:///C:/Wind...32/vmbuses.dll	842F1E3C2D92266E681A249DE43879252878C8D2C			2018 июня 20 12:37:30	ESET\vsobolev	Вручную	Dynamic Threat Defense	Исполняемый файл	
http://ftp.nod..._suspicious.bat	F02C2C66C43953E0A88257DF3C4A017268798233			2018 июля 20 00:13:50		Автоматически...	Dynamic Threat Defense	Сценарий	
http://ftp.nod..._t_malicious.bat	1322926A4998C7A3A2B231F865CD378F80D562ED			2018 июля 20 00:13:49		Автоматически...	Dynamic Threat Defense	Сценарий	
http://ftp.nod..._suspicious.bat	36C38333CDE5E2154C5F78AC1A79EFD2EF4C92			2018 июля 20 00:13:49		Автоматически...	Dynamic Threat Defense	Сценарий	
http://t1.daum..._ayerSetup64.exe	A7A7F0D1665EB1703F74A3C311F8535F5728107			2018 июня 20 15:18:49		Автоматически...	Dynamic Threat Defense	Исполняемый файл	
file:///C:/Prog...nuget/MyGet.ps1	E0881DA8E82A267DA0810EE4AE5897D14AEDC656			2018 июля 23 15:37:50	NT AUTHORITY\сис...	Автоматически...	Dynamic Threat Defense	Сценарий	
file:///C:/Wind...F-BE1615FC8B9F	986808DCFE80A936D033F83DC858087D66EB362			2018 июня 20 16:31:08	ESET\vsobolev	Автоматически...	Dynamic Threat Defense	Исполняемый файл	
file:///C:/Wind...F-8AA039D8FF31	74C77C6FADED016369F596EE2523257D9C9217			2018 июня 20 16:34:32	ESET\vsobolev	Автоматически...	Dynamic Threat Defense	Исполняемый файл	
file:///C:/Wind...2-372608D9C16E	62FA001137E66C8E3E8272844E82D7FA68A9020			2018 июня 21 09:23:00	ESET\vsobolev	Автоматически...	Dynamic Threat Defense	Исполняемый файл	
file:///C:/Wind...ler/MSID9D8.tmp	A50D9B617EA460205A959E09B3C5978411C7E82			2018 июня 21 09:27:36	NT AUTHORITY\сис...	Автоматически...	Dynamic Threat Defense	Исполняемый файл	
file:///C:/Wind...3-E3AFF5EBD7E5	472E117F79F6C8EED0419F6DC271D54FF6D89AF7			2018 июня 21 09:26:56	ESET\vsobolev	Автоматически...	Dynamic Threat Defense	Исполняемый файл	
file:///C:/User...eractiveRes.ps1	2DEF8B5A2758AF744E3DD8AF3A4A4153A28E4713			2018 июля 19 12:38:37	ESET\vsobolev	Автоматически...	Dynamic Threat Defense	Сценарий	
file:///C:/User...eractiveRes.ps1	49044724698E6964DC93ACF5BEE2A778BEAD4133			2018 июля 19 12:38:36	ESET\vsobolev	Автоматически...	Dynamic Threat Defense	Сценарий	
file:///C:/User...ticsResolve.ps1	D7745A4817748A46CFFAAC350F939D5B379F898			2018 июня 21 09:40:12	ESET\vsobolev	Автоматически...	Dynamic Threat Defense	Сценарий	
file:///C:/User...roubleshoot.ps1	7008E759C8478F74A4EA4C0911DE158EF00ACE84			2018 июня 21 09:40:11	ESET\vsobolev	Автоматически...	Dynamic Threat Defense	Сценарий	
file:///C:/User...sticsVerify.ps1	4658484E0E3AC8626E67D54617422787C8899408			2018 июня 21 09:37:06	ESET\vsobolev	Автоматически...	Dynamic Threat Defense	Сценарий	
file:///C:/User...dPSPService.ps1	0C95DD05514D062354C0EECC9AE8D4371233058B			2018 июля 16 18:05:17	ESET\vsobolev	Автоматически...	Dynamic Threat Defense	Сценарий	
file:///C:/User...ityFirewall.ps1	78F2CBC39821DADEDE63EA553488AEF8A45663A00			2018 июня 21 09:40:11	ESET\vsobolev	Автоматически...	Dynamic Threat Defense	Сценарий	
file:///C:/User...tyFunctions.ps1	FB35AF68329D6080EC92E24230EAFCE812B0A9F9			2018 июня 21 09:40:11	ESET\vsobolev	Автоматически...	Dynamic Threat Defense	Сценарий	

ДОБАВИТЬ ИСКЛЮЧЕНИЕ В ПОЛИТИКУ

∞

< НАЗАД Отправленные файлы > http://ftp.no...uspicious.bat — сведения о файле

## 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.ba  
**Размер** 150 Б (150 байт)

ЗАКРЫТЬ ПРОСМОТРЕТЬ ПОВЕДЕНИЕ ДОБАВИТЬ ИСКЛЮЧЕНИЕ В ПОЛИТИКУ

# ОТЧЕТ О ПОВЕДЕНИИ ФАЙЛОВ



<b>СТАТУС</b>	Подозрительный
<b>SHA-1</b>	36C3B3332CDE52E154C5F78AC1A79EFED2EF4C92
<b>РАЗМЕР</b>	150Б
<b>КАТЕГОРИЯ</b>	Сценарий

## Обнаруженное поведение

<b>ПОВЕДЕНИЕ</b>	Проанализированный образец скопирован.
<b>ОБЪЯСНЕНИЕ</b>	Образец был скопирован в другое расположение.
<b>ПОЛЕЗНЫЕ ДЕЙСТВИЯ</b>	Это стандартное поведение для некоторых установщиков.
<b>ВРЕДОНОСНЫЕ ДЕЙСТВИЯ</b>	Вредоносная программа попыталась скрыть свое наличие.

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

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

<b>ПОВЕДЕНИЕ</b>	Сетевые подключения.
<b>ОБЪЯСНЕНИЕ</b>	Образец пытался обмениваться данными с другим компьютером через сеть или прослушивать подключения других компьютеров.
<b>ПОЛЕЗНЫЕ ДЕЙСТВИЯ</b>	Чистые образцы используют сетевые подключения для загрузки контента.

# ВЫВОД



ПРОСТОЙ В ИСПОЛЬЗОВАНИИ



ЛЁГКИЙ ДЛЯ СИСТЕМЫ

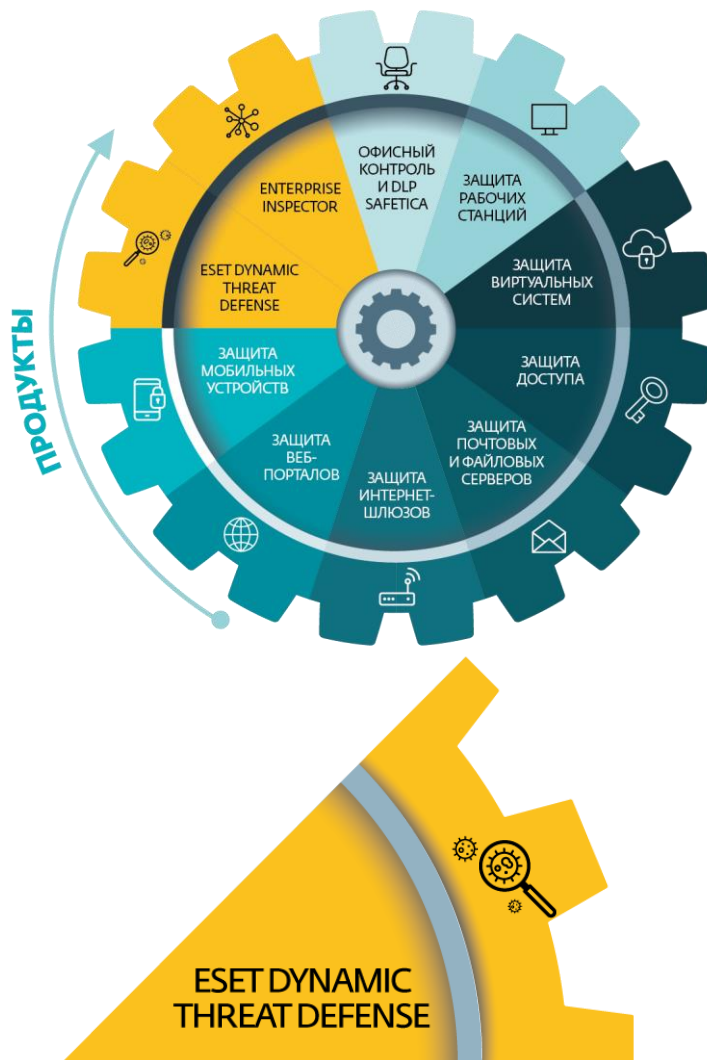


БЫСТРАЯ НАСТРОЙКА



ДОПОЛНИТЕЛЬНАЯ ЗАЩИТА

**eSet** АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

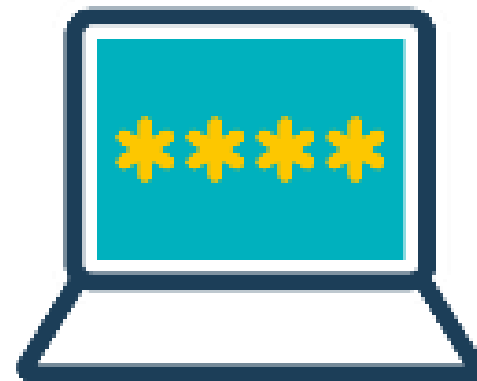




SECURE AUTHENTICATION

# ДЛЯ ЧЕГО НАМ НУЖНЫ ПАРОЛИ?

- Для подключения к ресурсам компании
- К облачным сервисам Microsoft Office 365
- К веб-приложениям Microsoft, например, Outlook Web Access (OWA)
- При подключении к Exchange Control Panel 2010 & Exchange Administrator Center 2013
- Для VPN и VDI систем
- ...





# w#hN02v)b56

1234567890

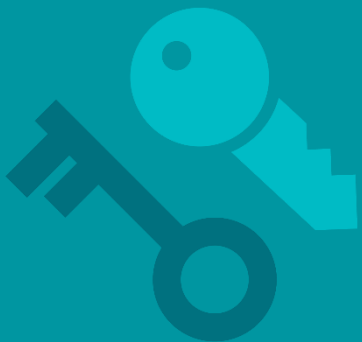
0987654321

Password123

Marina1990



# Двухфакторная аутентификация



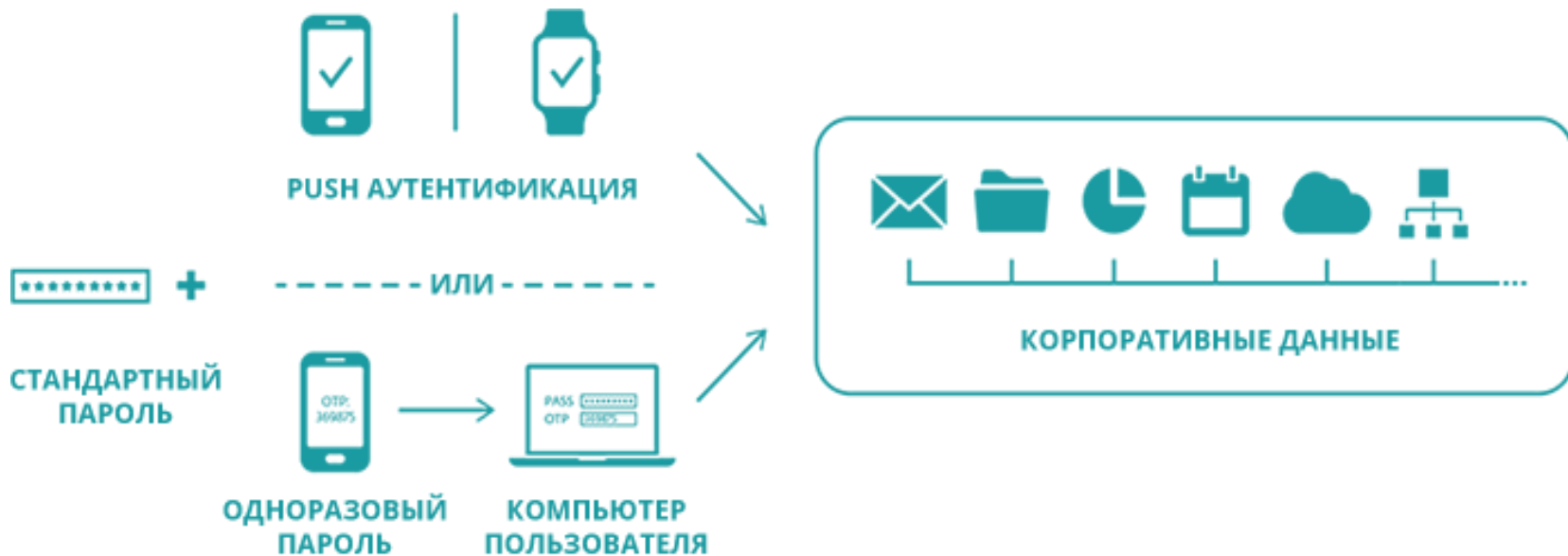
Требует от пользователя наличия двух типов учетных данных, прежде чем он сможет получить доступ к аккаунту:

**то, что он знает**, например, пароль или персональный идентификационный номер (PIN-код)

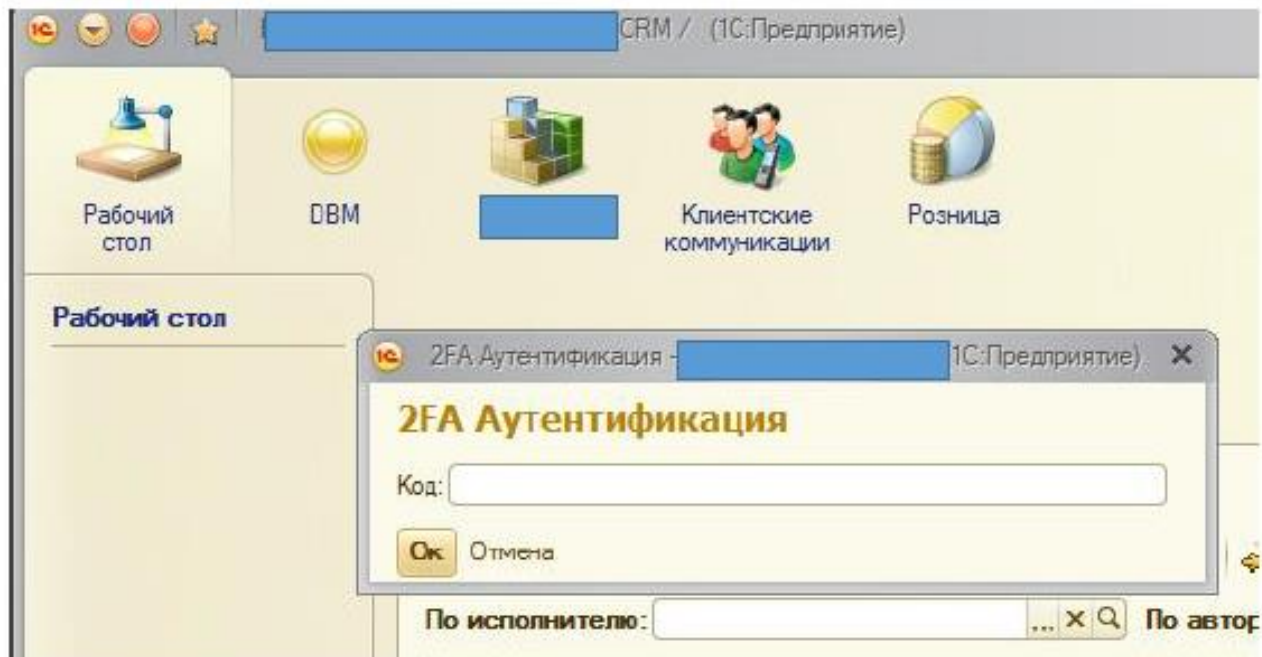
**то, что у него есть**, например, телефон, банковская карта, брелок

Комбинация этих элементов значительно повышает безопасность доступа к конфиденциальной информации.

# КАК РАБОТАЕТ СИСТЕМА



# ИНТЕГРАЦИЯ С 1С



ДОСТУПЕН:

- NFR
- ДЕМО СТЕНД



# ВЫВОД



ПРОСТОЙ В ИСПОЛЬЗОВАНИИ



ЛЁГКИЙ ДЛЯ СИСТЕМЫ



РЕШЕНИЕ ДЛЯ УДАЛЁННЫХ СОТРУДНИКОВ

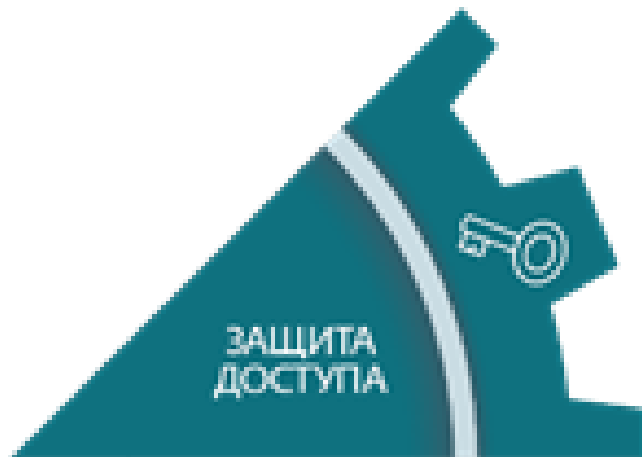
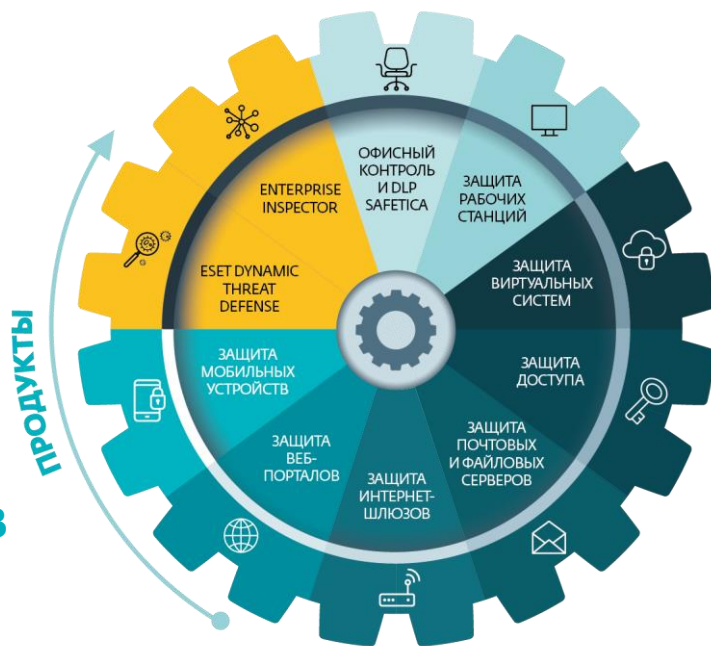


ДОПОЛНИТЕЛЬНАЯ ЗАЩИТА



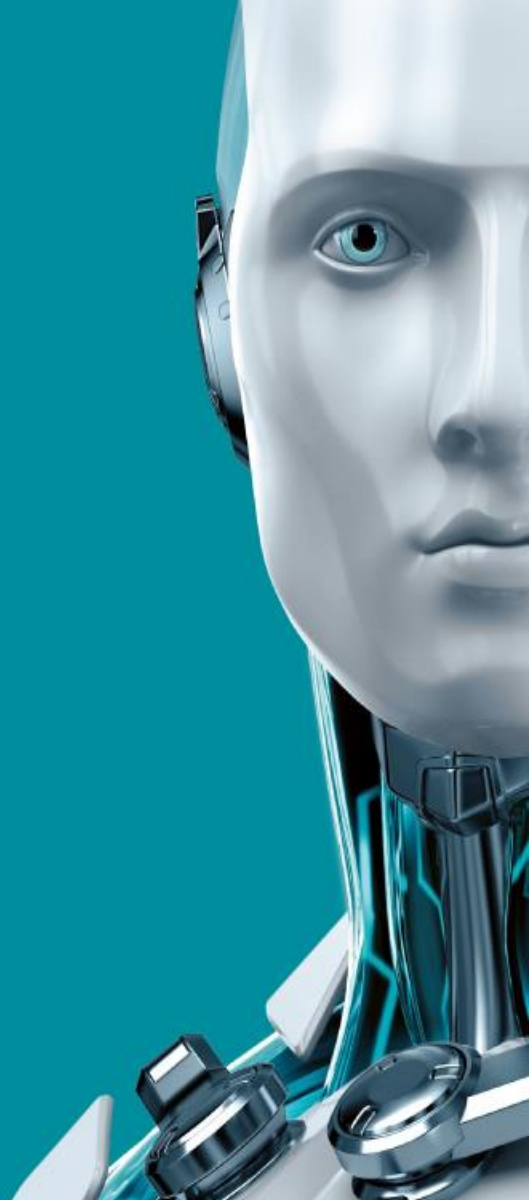
ГОТОВ К РАБОТЕ

**eSet** АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА



# ОФИСНЫЙ КОНТРОЛЬ И DLP safetica

 TECHNOLOGY ALLIANCE



# О КОМПАНИИ

## SAFETICA TECHNOLOGIES

- › Чешская компания, основана в **2009** году, команда **70+**
- › Клиенты в более чем **95** странах
- › Продукт входит в **TOP 5 DLP** - в рейтинге журнала SC Magazine
- › DLP решение для любого типа бизнеса - по версии **Gartner**
- › Входит в **ESET Technology Alliance** с 2016 года



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

# УТЕЧКА ДАННЫХ

## ПОЧЕМУ ЭТО ПРОИСХОДИТ?

- › Создание собственной компании на базе уникальных данных
- › Продажа информации конкурентам
- › Использование данных для устройства на новую работу
- › Чтобы просто навредить компании или людям в ней
- › «Я создавал это, значит это мои данные!» (Нет, это не так...)
- › Другие причины, которые кажутся сотрудникам логичными



## УТЕЧКА ДАННЫХ КАК ЭТО ПРОИСХОДИТ?

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



# ПРИНЦИПИАЛЬНЫЕ РАЗЛИЧИЯ DLP



## СЕТЕВЫЕ

АППАРАТНЫЙ ИЛИ ВИРТУАЛЬНЫЙ ШЛЮЗ



## КОНТЕНТНЫЙ ФИЛЬТР

ПРИНЯТИЕ РЕШЕНИЯ НА ОСНОВЕ АНАЛИЗА  
СОДЕРЖИМОГО



## АГЕНТНЫЕ

АГЕНТЫ DLP НА КОНЕЧНЫХ ТОЧКАХ



## КОНТЕКСТНЫЙ ФИЛЬТР

ПРИНЯТИЕ РЕШЕНИЯ ПО ФОРМАЛЬНЫМ  
ПРИЗНАКАМ



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

# 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)



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



› Контроль приложений



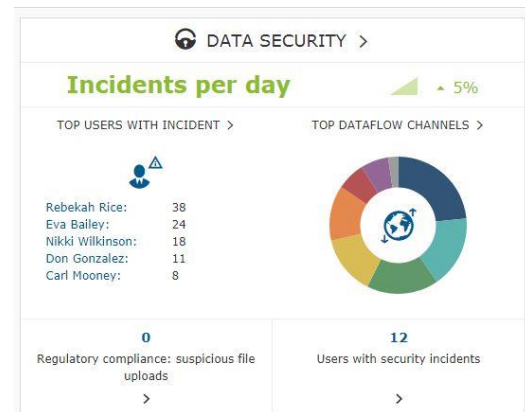
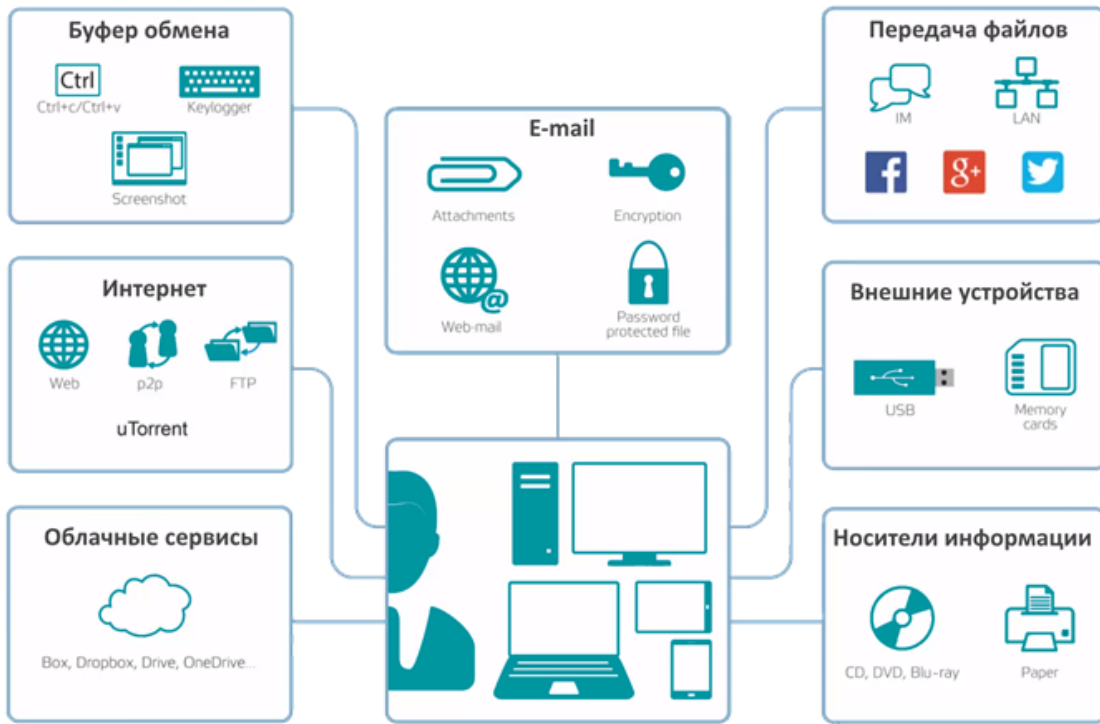
› Контроль печати



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

# ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ

## МОДУЛЬ DLP



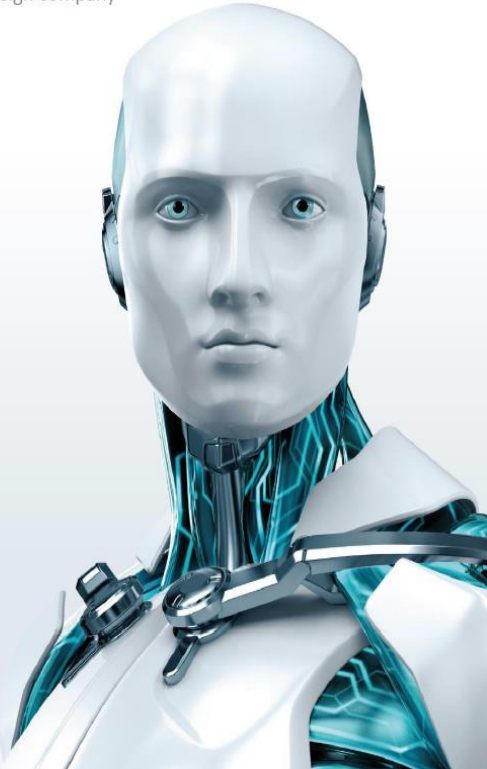
# РЕЗУЛЬТАТЫ ВНЕДРЕНИЯ

**eSet** ОФИСНЫЙ КОНТРОЛЬ И DLP

**Safetica**

АНАЛИЗ РЕЗУЛЬТАТОВ

Industrial design company



## ✓ ПРОИЗВОДИТЕЛЬНОСТЬ:

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

## ✓ РАБОТА С ДАННЫМИ:

- *Отсутствие утечки данных из компании*
- *Отсутствие нежелательные действия с данными*

## ✓ ИСПОЛЬЗОВАНИЕ ИТ-РЕСУРСОВ:

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

# Спасибо за внимание! Вопросы?

Бойков Иван

Региональный представитель компании ESET в ЦФО

тел: +7 961 615 17 13

e-mail: [iboykov@esenod32.ru](mailto:iboykov@esenod32.ru)



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА