

# 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. ЗАЩИТА ОТ ВНУТРЕННИХ УГРОЗ
6. ESA



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

# СТАТИСТИКА ИНСТИТУТА AV-TEST

## ИЗВЕСТНЫЕ УГРОЗЫ

Total malware



# х3 с 2014г

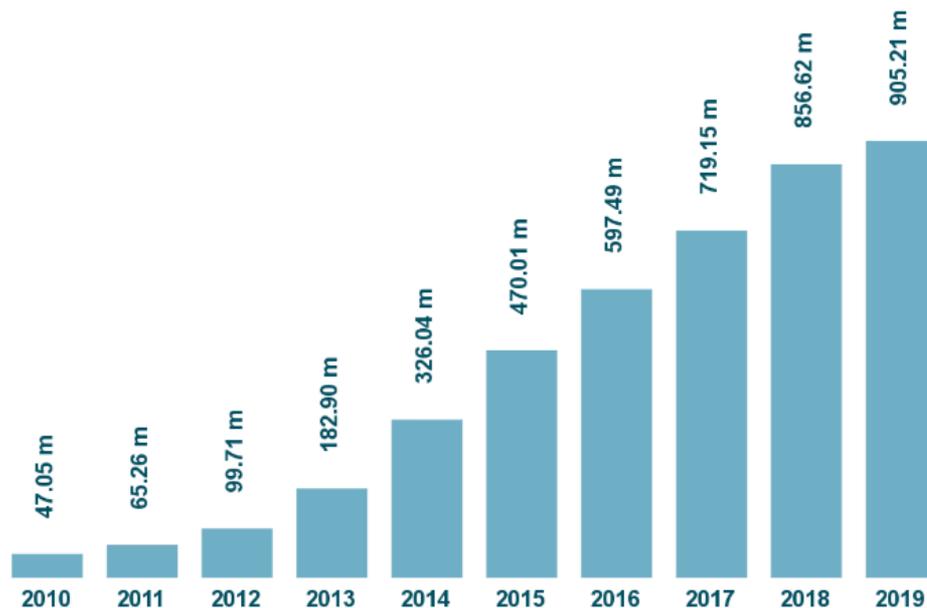
- **390 000 шт. в день**

*Новых образцов*

*вредоносных программ каждый день*

- **Новые способы**

*Новые способы обхода обнаружения*



Last update: May 30, 2019

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



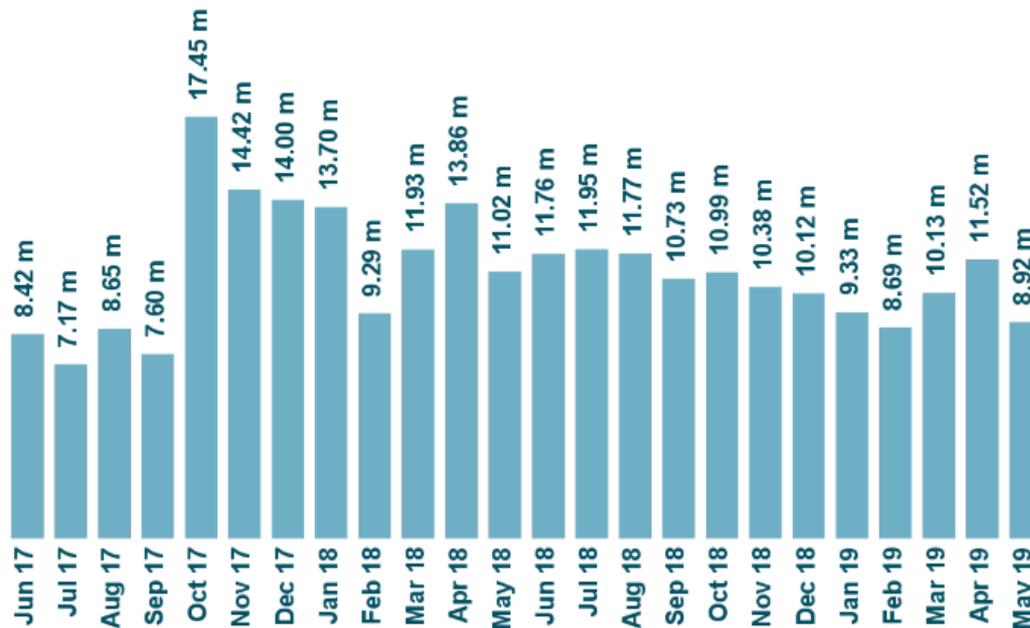
АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

*Источник: av-test.org, статистика вредоносных программ на 30 Мая 2019г.*

# УГРОЗЫ ПРОГРЕССИРУЮТ И СТАНОВЯТСЯ СЛОЖНЕЕ



## Новые угрозы



Last update: May 30, 2019

Copyright © AV-TEST GmbH, [www.av-test.org](http://www.av-test.org)

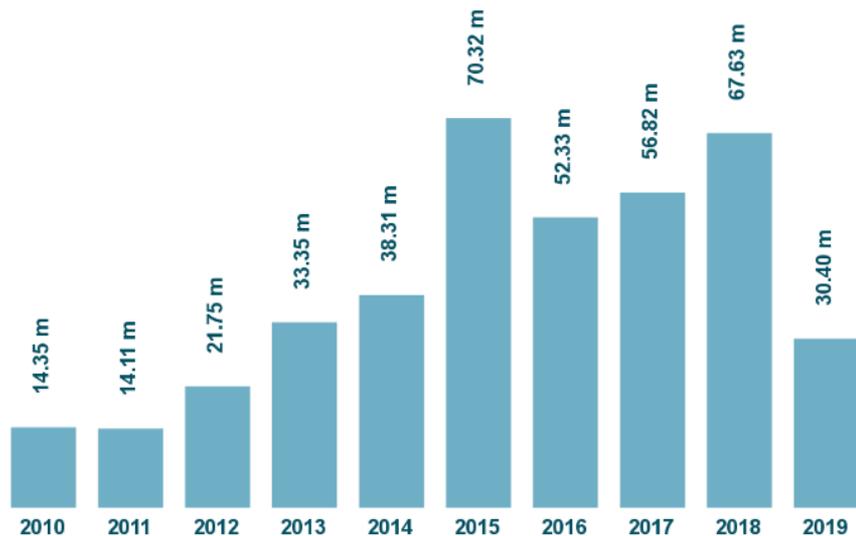


АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Источник: [av-test.org](http://av-test.org), статистика вредоносных программ на 30 мая 2019г

# УГРОЗЫ ДЛЯ WINDOWS

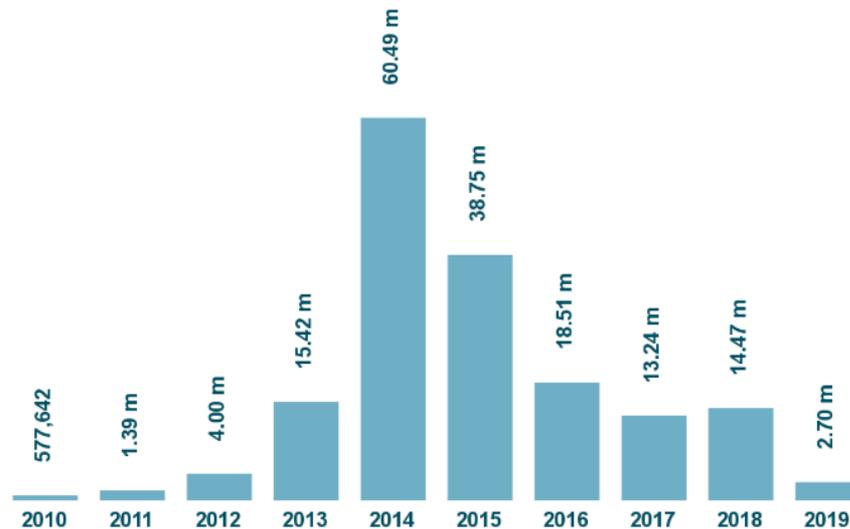
## Development of Windows malware



Last update: May 30, 2019

Copyright © AV-TEST GmbH, [www.av-test.org](http://www.av-test.org)

## Development of PUA for Windows



Last update: May 30, 2019

Copyright © AV-TEST GmbH, [www.av-test.org](http://www.av-test.org)

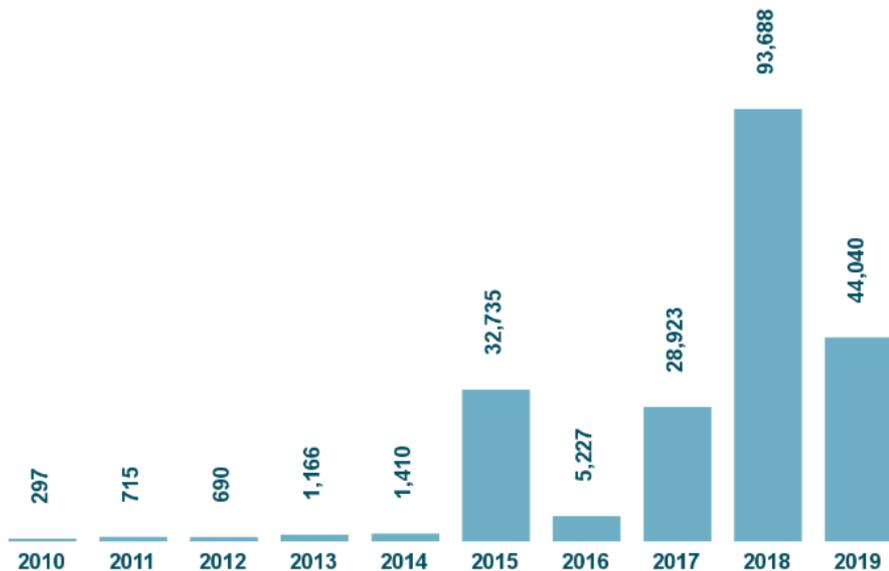


АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Источник: [av-test.org](http://av-test.org), статистика вредоносных программ на 30 мая 2019г

# УГРОЗЫ ДЛЯ MACOS

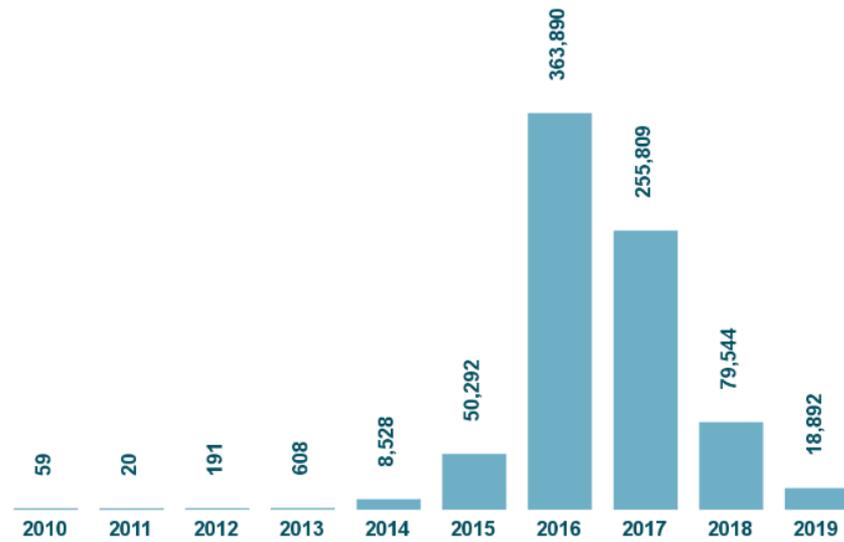
## Development of MacOS malware



Last update: May 30, 2019

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

## Development of PUA for MacOS



Last update: May 30, 2019

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



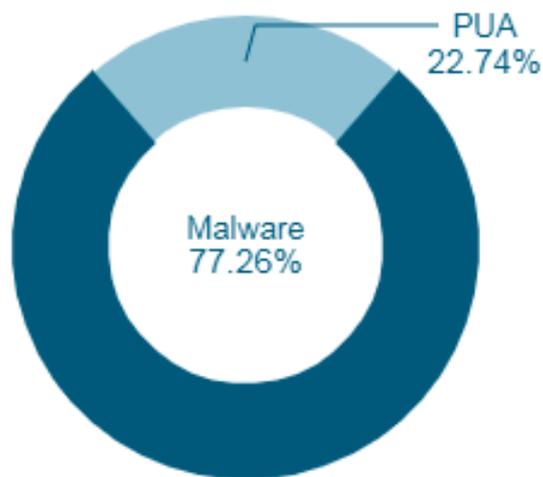
АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Источник: av-test.org, статистика вредоносных программ на 30 мая 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\**

*\* PricewaterhouseCoopers, 2016*

- › **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*



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

# КАК ОБЕСПЕЧИТЬ ЗАЩИТУ?



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

Непрерывный  
мониторинг  
и анализ

# 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



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**

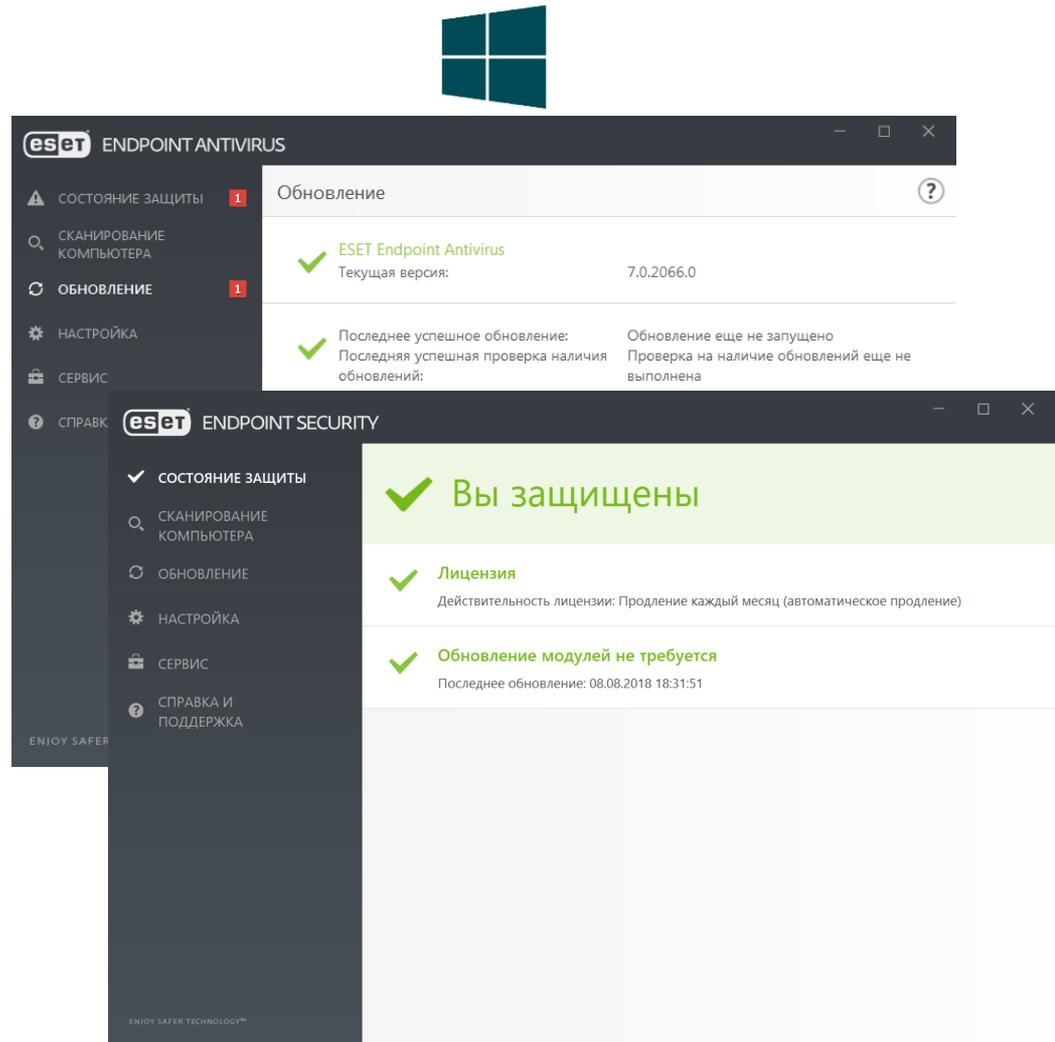
ESET Dynamic Threat Defense **NEW**

## РЕАГИРОВАНИЕ

## ОБНАРУЖЕНИЕ

# ESET ENDPOINT SECURITY ESET ENDPOINT ANTIVIRUS

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



# ESET FILE SECURITY ДЛЯ WINDOWS SERVER

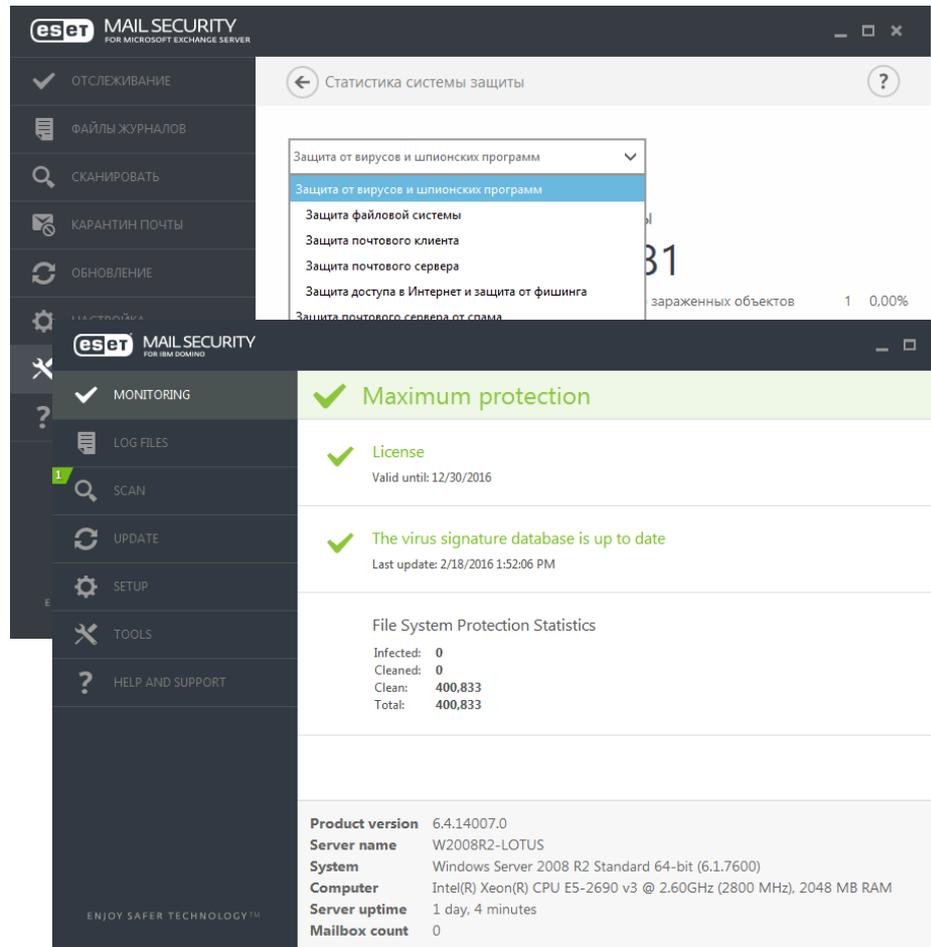
- ✓ Поддержка Microsoft **Office 365**
- ✓ Защита от сетевых атак (IDS)
- ✓ Поддержка **ESET Dynamic Threat Defense**
- ✓ Добавление исключений по хэшу файлов
- ✓ **64-битное** ядро сканирования

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 green checkmarks confirm the license status, update requirements, and protection statistics. The statistics section shows 0 infected files, 0 cleaned files, and 2,279 files not infected out of a total of 2,279 files. The bottom section provides system information including the product version (7.0.12012.0), server name (WIN-TK16S21N282), operating system (Windows Server 2012 R2 Standard 64-bit), and server uptime (3 minutes).

eset FILE SECURITY FOR MICROSOFT WINDOWS SERVER	
✓ ОТСЛЕЖИВАНИЕ	✓ Вы защищены
📁 ФАЙЛЫ ЖУРНАЛА	✓ Лицензия Действительность лицензии: 14.03.2019
🔍 СКАНИРОВАТЬ	✓ Обновление модулей не требуется Последнее обновление: 08.08.2018 20:22:26
🔄 ОБНОВЛЕНИЕ	Статистика защиты файловой системы
⚙️ НАСТРОЙКА	Заражено: 0
🛠️ СЕРВИС	Очищено: 0
❓ СПРАВКА И ПОДДЕРЖКА	Не заражено: 2 279
	Всего: 2 279
	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.
ENJOY SAFER TECHNOLOGY™	

# 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 IBM Domino. The left sidebar contains navigation options: ОТСЛЕЖИВАНИЕ, ФАЙЛЫ ЖУРНАЛОВ, СКАНИРОВАТЬ, КАРАНТИН ПОЧТЫ, ОБНОВЛЕНИЕ, НАСТРОЙКИ, МОНИТОРИНГ, LOG FILES, SCAN, UPDATE, SETUP, TOOLS, and HELP AND SUPPORT. The main window shows the 'Статистика системы защиты' (Protection System Statistics) page. A dropdown menu is open, listing protection modules: Защита от вирусов и шпионских программ (selected), Защита файловой системы, Защита почтового клиента, Защита почтового сервера, Защита доступа в Интернет и защита от фишинга, and Защита почтового сервера от спама. The main content area displays a green banner for 'Maximum protection' and a 'License' section indicating validity until 12/30/2016. Below this, it states 'The virus signature database is up to date' with a last update of 2/18/2016 1:52:06 PM. A 'File System Protection Statistics' section shows 0 infected, 0 cleaned, and 400,833 total objects. At the bottom, system information is provided: 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, and Mailbox count 0.

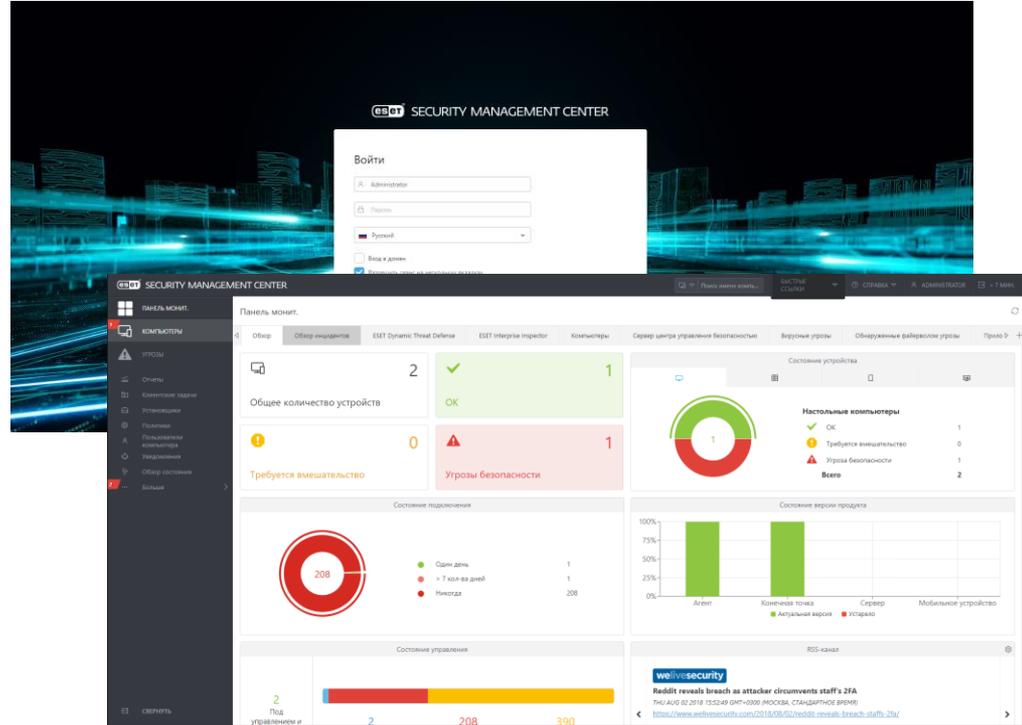


SECURITY MANAGEMENT CENTER

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. The left sidebar contains navigation options: ПАНЕЛЬ МОНИТ., КОМПЬЮТЕРЫ, УГРОЗЫ, Отчеты, Контекстные задачи, Установщики, Политики, Пользователи компьютера, Уведомления, Обзор состояния, Больше, and СВЕРНУТЬ. The main area is titled "Панель мониторинга" and displays several data panels:

- 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 Number of Cores.
- Компьютеры со сведениями об ОЗУ:** A table listing computers with columns for Grouping (by architecture), Grouping (by type), and Total Capacity in MB.
- Число компьютеров, сгруппированных по общей емкости:** A donut chart showing 4 computers grouped by total capacity.

The screenshot shows the hardware details for a specific device in the ESET Security Management Center. The navigation menu includes: ОБЗОР, КОНФИГУРАЦИЯ, ЖУРНАЛЫ, ВЫПОЛНЕНИЯ ЗАДАЧИ, УСТАНОВЛЕННЫЕ ПРИЛОЖЕНИЯ, ПРЕДУПРЕЖДЕНИЯ, ВОПРОСЫ, УГРОЗЫ И КАРАНТИН, and ПОДРОБНОСТИ. The main area displays hardware details for a device:

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

# Песочница

NEW

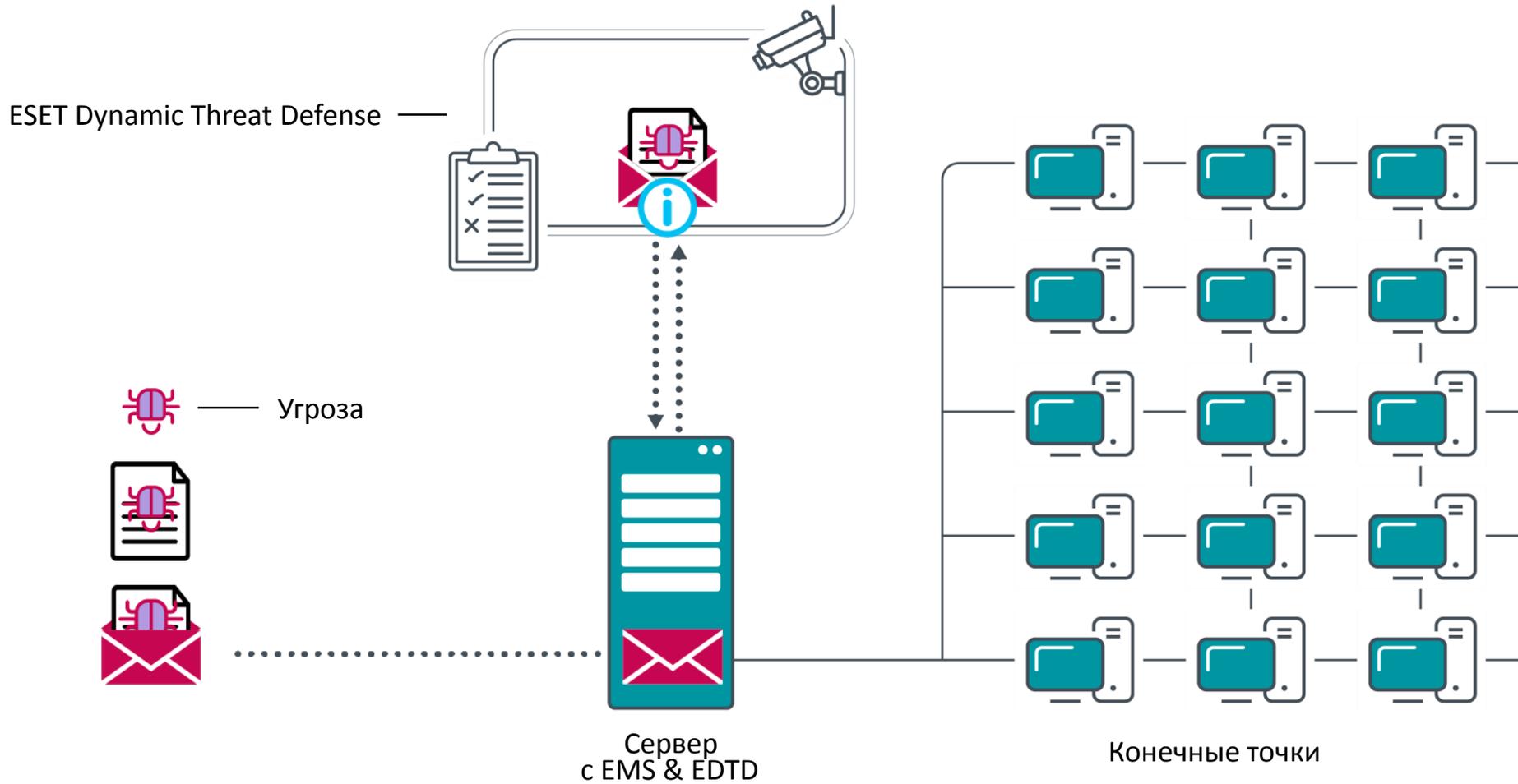


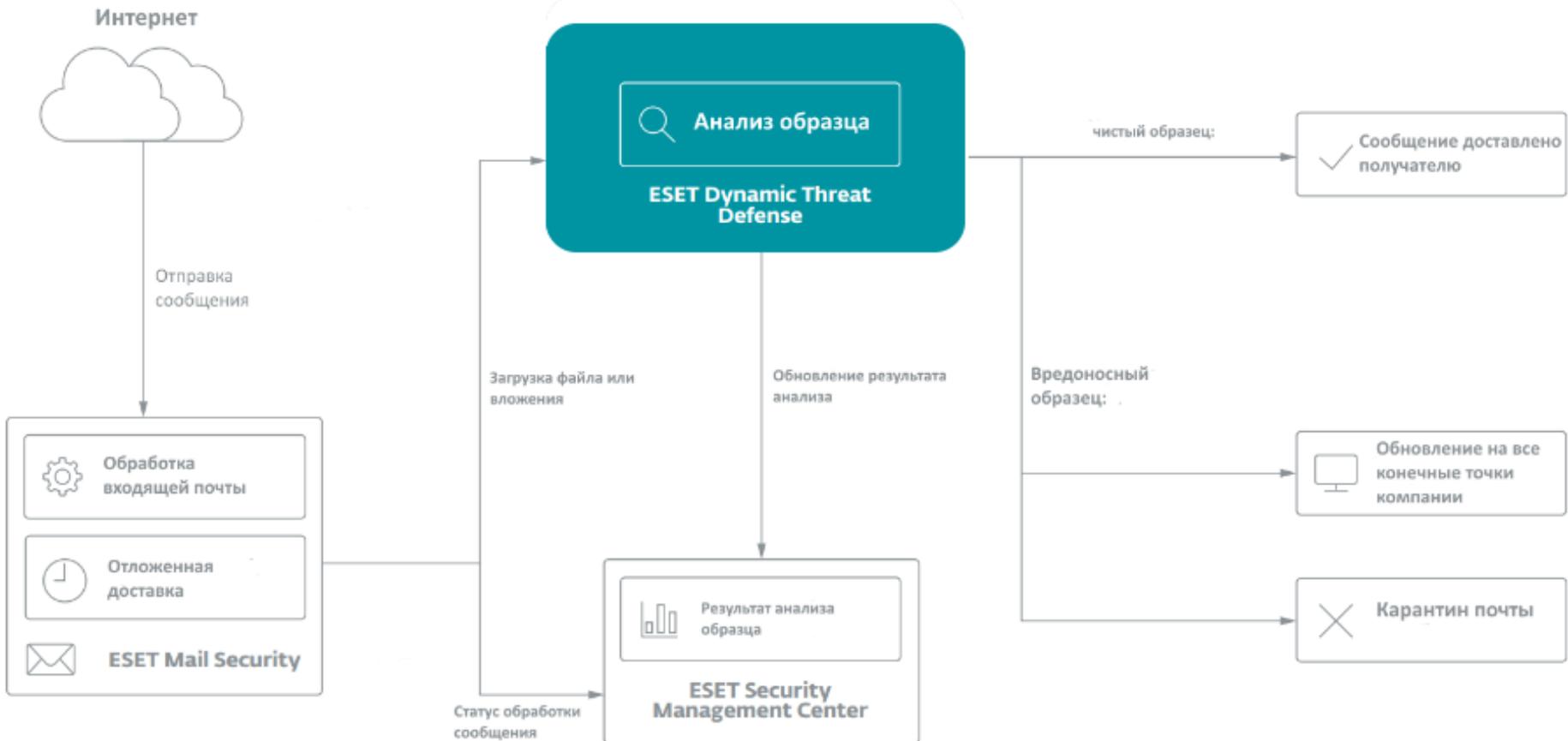
DYNAMIC THREAT DEFENSE

# ESET DYNAMIC THREAT DEFENSE

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



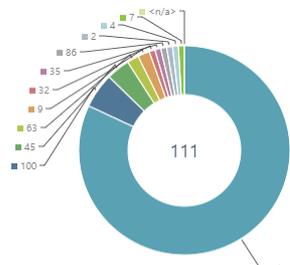




## Dashboard

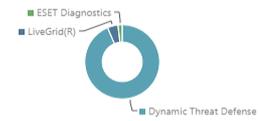
- Overview
- Incidents Overview
- Computers
- Security Management Center Server
- Antivirus threats
- Firewall threats
- ESET applications
- EDTD

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



Generated 0 minutes ago

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



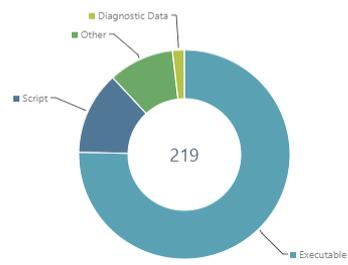
Generated 0 minutes ago

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...

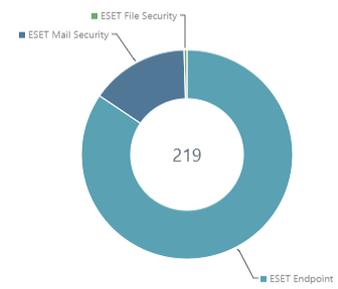


Generated 0 minutes ago

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)
586614784446...	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...
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...
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...
0DA78D17789...	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...
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	ПОЛЬЗОВАТЕЛИ	ПРИЧИНА	ПОЛУЧАТЕЛЬ	КАТЕГОРИЯ	КОМПЬЮТЕР
file:///C:/Prog...metryClient.dll	9A556E9E2C37C505325C80F853754DD03416F050					Автоматически...	LiveGrid(R)	Исполняемый файл	es...
file:///C:/Prog...yDataShared.dll	60E730AA282C849C047BC8E08BAE0EED5D14DE2					Автоматически...	LiveGrid(R)	Исполняемый файл	es...
file:///4F879F...D05692420ECCDOFE	5804A4926E689E6F11DC33D6A180E7DAD8EE867D3					Автоматически...	LiveGrid(R)	Исполняемый файл	es...
file:///222289...57805576DF12268	9DDF98144C07DE9D9F818038489210559AA3A237					Автоматически...	LiveGrid(R)	Исполняемый файл	es...
file:///C:/Wind...32/vmbuses.dll	842F1E3CD9226E681A249DE4387925287BCBD2C					Вручную	Dynamic Threat Defense	Исполняемый файл	es...
http://ftp.nod..._suspicious.bat	F02C266C43953E0A88257DF3C4A017268798233	Завершено		2018 июля 20 00:13:50	ESET\bsobolev	Автоматически...	Dynamic Threat Defense	Сценарий	es...
http://ftp.nod..._malicious.bat	1322926A4998C7A3A28231F865CD378F80D562ED	Завершено		2018 июля 20 00:13:49		Автоматически...	Dynamic Threat Defense	Сценарий	es...
http://ftp.nod..._suspicious.bat	36C383332CDE5E2154C5F78AC1A79FEFED2EF4C92	Завершено		2018 июля 20 00:13:49		Автоматически...	Dynamic Threat Defense	Сценарий	es...
http://t1.daum...ayerSetup64.exe	A7A7F0D1665EB1703F74A3C11FB535FF5728107	Завершено		2018 июня 20 15:18:49		Автоматически...	Dynamic Threat Defense	Исполняемый файл	es...
file:///C:/Prog...nugot/MyGet.ps1	E0881DA8EB2A267DA0810EE4AE5897D14AEDC656	Завершено		2018 июля 23 15:37:50	NT AUTHORITY\сис...	Автоматически...	Dynamic Threat Defense	Сценарий	es...
file:///C:/Wind...F-BE1615FCE89F)	986808DCF80A936D033FE38C858087D66EB362	Завершено		2018 июня 20 16:31:08	ESET\bsobolev	Автоматически...	Dynamic Threat Defense	Исполняемый файл	es...
file:///C:/Wind...F-BAA039D8FF31)	74C77C6FADED016369F596EE2523257D9CC9217	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	A50D98617EA460205A9559E0983C5978411C7E82	Завершено		2018 июня 21 09:27:36	NT AUTHORITY\сис...	Автоматически...	Dynamic Threat Defense	Исполняемый файл	es...
file:///C:/Wind...3-E3AFF5EBD7E5)	472E117F79F6C8EED0419F6DC271D54FF6D89AF7	Завершено		2018 июня 21 09:26:56	ESET\bsobolev	Автоматически...	Dynamic Threat Defense	Исполняемый файл	es...
file:///C:/User...eractiveRes.ps1	2DEFB85A2758AF744E8DF3A4AAA153A284E713	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...ticsResolve.ps1	D7745A4817748A46C6FFAAC350F939D58379F89B	Завершено		2018 июня 21 09:40:12	ESET\bsobolev	Автоматически...	Dynamic Threat Defense	Сценарий	es...
file:///C:/User...roubleshoot.ps1	7008E759CB478F744A4E4CD911DE158EF00AC8E4	Завершено		2018 июня 21 09:40:11	ESET\bsobolev	Автоматически...	Dynamic Threat Defense	Сценарий	es...
file:///C:/User...sticsVerify.ps1	465B484E0E3ACB62667D54617422787C8899408	Завершено		2018 июня 21 09:37:06	ESET\bsobolev	Автоматически...	Dynamic Threat Defense	Сценарий	es...
file:///C:/User...tDPSService.ps1	0C95DD05514D062354C0ECC9A88D4371233058B	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	FB35AF68329D6080EC9E24230EAF8E1280A9F9	Завершено		2018 июня 21 09:40:11	ESET\bsobolev	Автоматически...	Dynamic Threat Defense	Сценарий	es...

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	<a href="#">Просмотреть поведение</a>

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

Компьютер	esetnote25.eset.local
Пользователь	
Причина	Автоматически
Получатель	Dynamic Threat Defense
Хэш	36C3B3332CDE52E154C5F78AC1A79EFED2E...

### Анализ

Статус	<div style="width: 100%; height: 10px; background: linear-gradient(to right, #ccc, #ccc); border: 1px solid #ccc; display: inline-block;"></div> <span style="background-color: #ffc107; padding: 2px 5px; border-radius: 3px;">Подозрительный</span>
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...
Размер	150 К (150 000 байт)

ЗАКРЫТЬ
ПРОСМОТРЕТЬ ПОВЕДЕНИЕ
ДОБАВИТЬ ИСКЛЮЧЕНИЕ В ПОЛИТИКУ

# ОТЧЕТ О ПОВЕДЕНИИ ФАЙЛОВ

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

## Обнаруженное поведение

<b>ПОВЕДЕНИЕ</b>	<b>Проанализированный образец скопирован.</b>
<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>	<b>Выполнение ADS.</b>
<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>	<b>Внедрение кода в запущенный процесс.</b>
<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>	<b>Сетевые подключения.</b>
<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.

<b>СТАТУС</b>	<b>Вредоносные программы</b>
SHA-1	1322926A499BC7A3A2B231F865CD37BF80D562ED
РАЗМЕР	225B
КАТЕГОРИЯ	Сценарий

## Обнаруженное поведение

<b>ПОВЕДЕНИЕ</b>	<b>Обнаружен заблокированный URL-адрес.</b>
<b>ОБЪЯСНЕНИЕ</b>	Образец связался с URL-адресом, заблокированным ESET.
<b>ПОЛЕЗНЫЕ ДЕЙСТВИЯ</b>	Чистые приложения не должны этого делать.
<b>ВРЕДОНОСНЫЕ ДЕЙСТВИЯ</b>	Вредоносная программа связалась с сервером злоумышленников.
<b>ПОВЕДЕНИЕ</b>	<b>Вредоносная программа обнаружена без выполнения.</b>
<b>ОБЪЯСНЕНИЕ</b>	Образец определен как вредоносная программа без выполнения.
<b>ПОЛЕЗНЫЕ ДЕЙСТВИЯ</b>	Чистые приложения не должны этого делать.
<b>ВРЕДОНОСНЫЕ ДЕЙСТВИЯ</b>	Вредоносная программа обнаружена модулем сканирования ESET без выполнения.
<b>ПОВЕДЕНИЕ</b>	<b>Вредоносная программа обнаружена после выполнения.</b>
<b>ОБЪЯСНЕНИЕ</b>	Образец определен как вредоносная программа после выполнения.
<b>ПОЛЕЗНЫЕ ДЕЙСТВИЯ</b>	Чистые приложения не должны этого делать.
<b>ВРЕДОНОСНЫЕ ДЕЙСТВИЯ</b>	Вредоносная программа обнаружена модулем сканирования ESET после выполнения.
<b>ПОВЕДЕНИЕ</b>	<b>Образец изменил запущенный процесс.</b>
<b>ОБЪЯСНЕНИЕ</b>	Образец вставил код в запущенный процесс надежных приложений.
<b>ПОЛЕЗНЫЕ ДЕЙСТВИЯ</b>	Это стандартное поведение для программ безопасности и контроля пользователей.

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

## Detection

<b>ESET</b>	<a href="#">Win32/Filecoder.WannaCryptor.D trojan</a>
<b>Kaspersky</b>	Trojan-Ransom.Win32.Wanna.zbu
<b>McAfee</b>	Ransom-O trojan
<b>Microsoft</b>	Ransom:Win32/WannaCrypt
<b>Symantec</b>	Ransom.Wannacry

## ESET LiveGrid®

<b>COUNT</b>	10 000 to 100 000
<b>FIRST SEEN</b>	2017-05-12
<b>LAST SEEN</b>	2018-03-12

## Countries

<b>Russian Federation</b>	10 000 to 100 000
<b>Ukraine</b>	1 000 to 10 000
<b>Taiwan</b>	1 000 to 10 000
<b>Iran</b>	1 000 to 10 000
<b>India</b>	100 to 1 000



ENTERPRISE INSPECTOR

NEW

# EDR РЕШЕНИЯ ESET ENTERPRISE INSPECTOR



«Вы не можете в равной степени защитить всё...мы должны найти способ, чтобы контролировать только то, что имеет значение».

Эрл Перкинс, Вице-президент Gartner по исследованиям

# ESET ENTERPRISE INSPECTOR: КАК РАБОТАЕТ

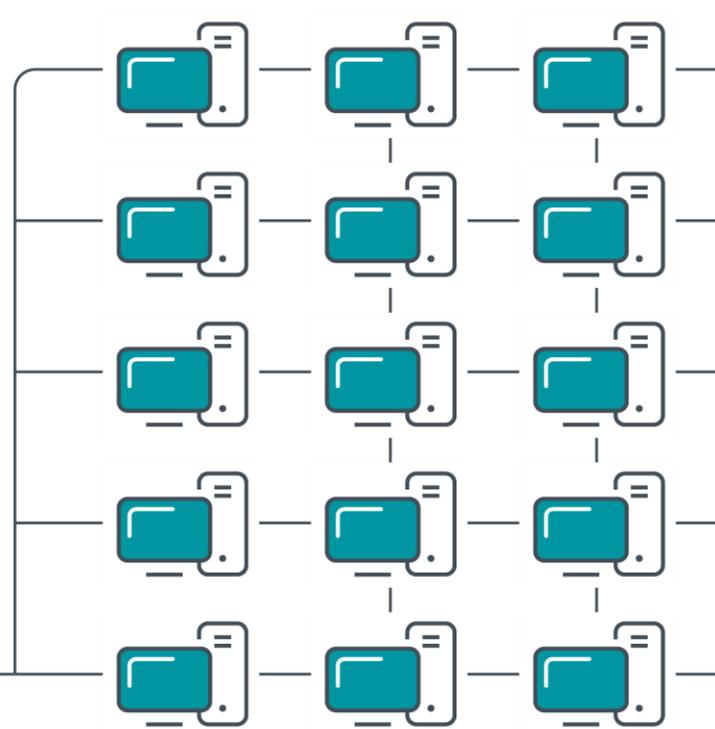


- ✓ **Собирает информацию** в режиме реального времени
- ✓ Обеспечивает **фильтрацию и сортировку**
- ✓ Позволяет создавать **собственные правила**
- ✓ Использует систему репутаций **ESET LiveGrid**

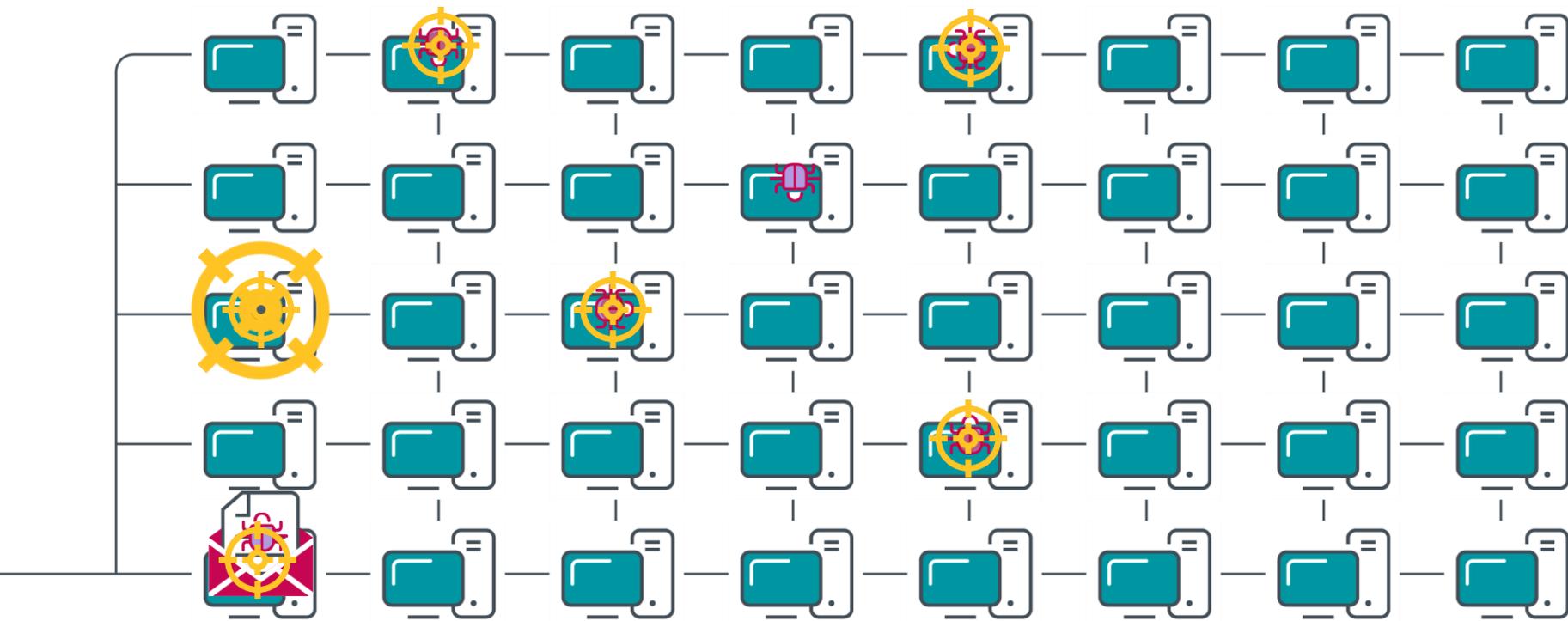
ESET Dynamic Threat Defense



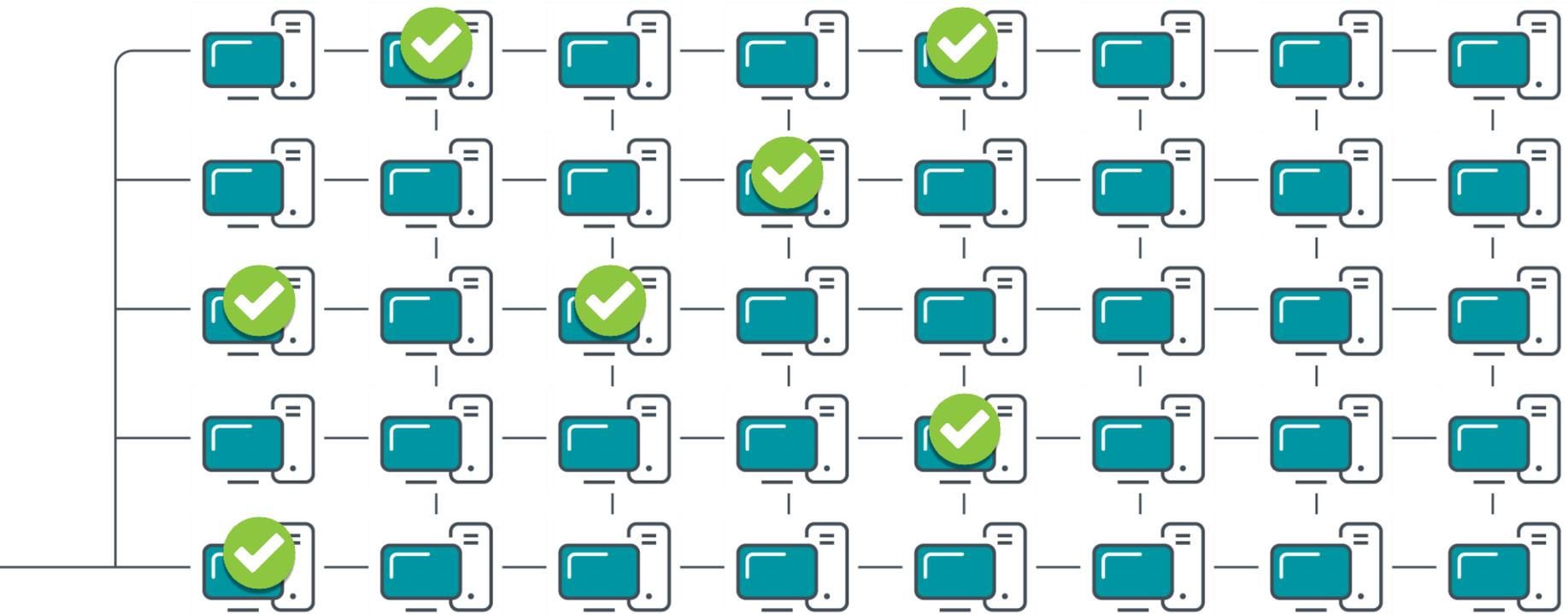
Сервер  
с EMS & EDTD



Конечные точки



Конечные точки



Endpoints

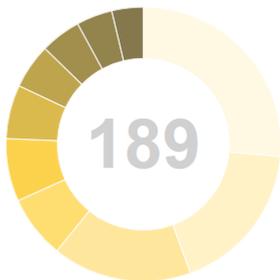
DASHBOARD

Dashboard

ADD FILTER

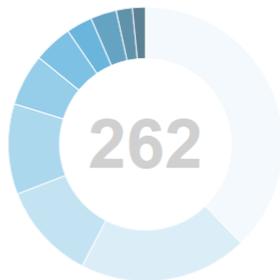
Alarms Executables Computers More Server status

Top 10 Unresolved Threat and Warning Alarms



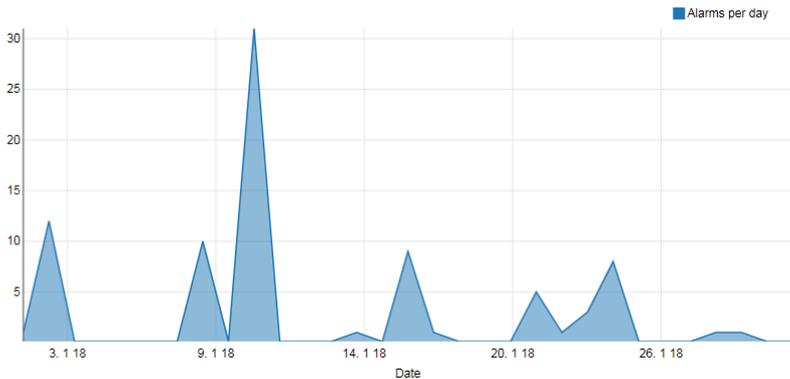
- Detected by ESET Endpoint Security product (50)
- Unpopular process has started from %Temp% [Z0402] (34)
- EXE patching or dropping [B0304] (31)
- Common AutoStart registry modified by unpopular process [A0103]...
- Processes killing from commandline [B0401] (14)
- Process with a suspicious extension has started [Z0406] (12)
- Unpopular process with a suspicious extension has started [D0423]...
- Windows Firewall rules manipulation [B0202] (9)
- File modified in %startup% folder [A0127] (8)
- Unpopular process has been added to startup folder [D0115] (7)

Top 10 Unresolved Informational Alarms

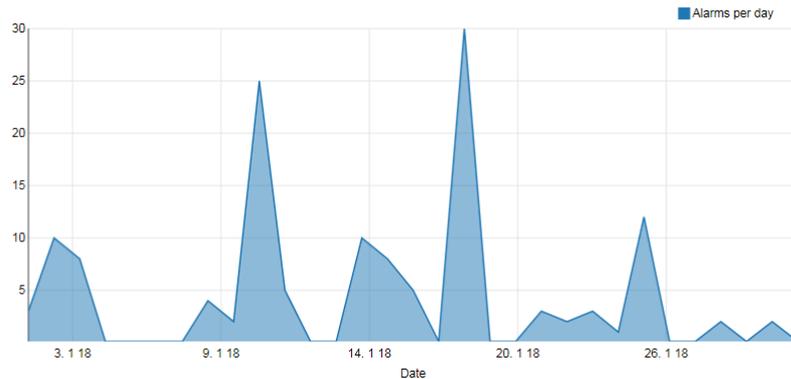


- System utility was executed test [A0403] (99)
- Unpopular process has started from %AppData%\%ProgramData% [Z04...
- Process started from desktop [Z0405] (30)
- Management of the services from commandline [B0403] (28)
- Cmd.exe executed with '/c' by unpopular process [A0400] (16)
- Autorun.inf file was created/modified [A0301] (12)
- Service installation or modification [B0402] (8)
- Saving script file [Z0301] (8)
- Autorun.inf file was deleted [A0301] (5)
- Powershell suspicious activity executed [D0414] (4)

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

# 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

# АРХИТЕКТУРА РЕШЕНИЯ SAFETICA

## В четыре шага

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



# НИКАКИХ СКРЫТЫХ РАСХОДОВ

## Сервер

Процессор: четырёхядерный 2,4GHz

Оперативная память: от 2GB

Жесткий диск: от 3GB свободного места (от 100GB с БД)

ОС: MS Windows Server 2008 и выше, 32&64-bit

## База данных (MS SQL)

MS SQL 2008 R2 и выше, рекомендуется MS SQL 2012 и выше

MS SQL 2016 Express включена в установочный пакет Safetica



# 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  
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

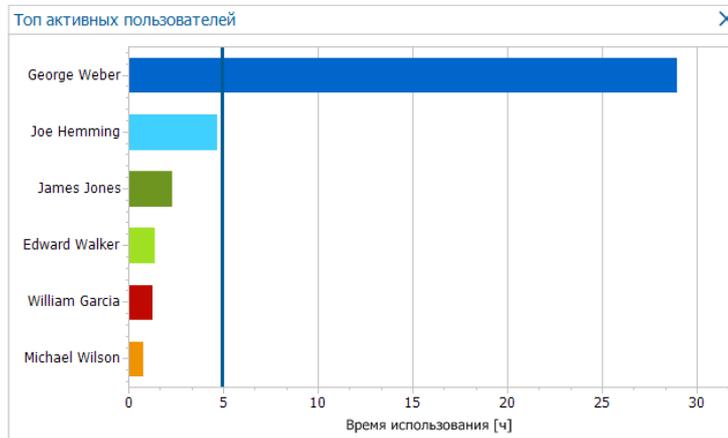
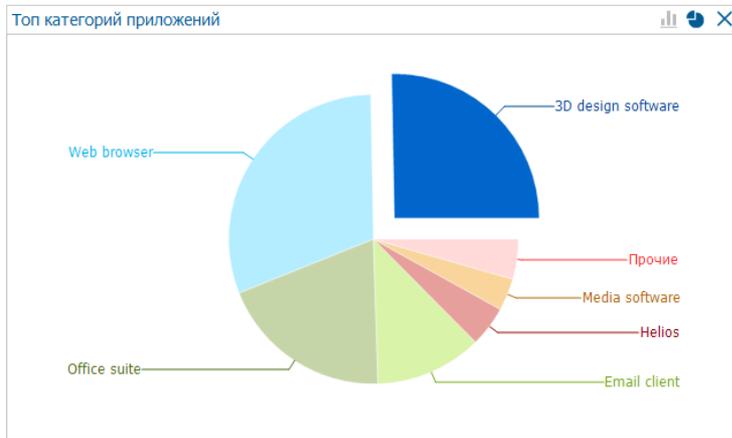


ЭФФЕКТИВНОСТЬ  
ИСПОЛЬЗОВАНИЯ ПО

# 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

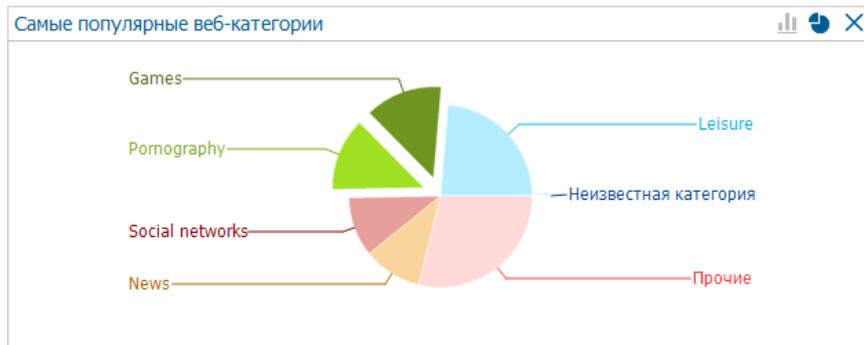
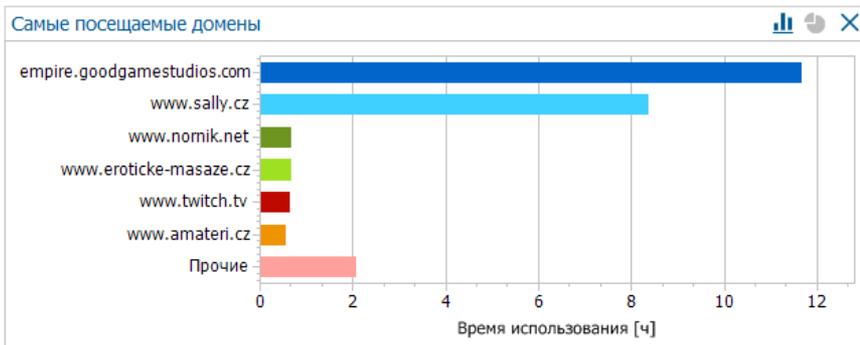
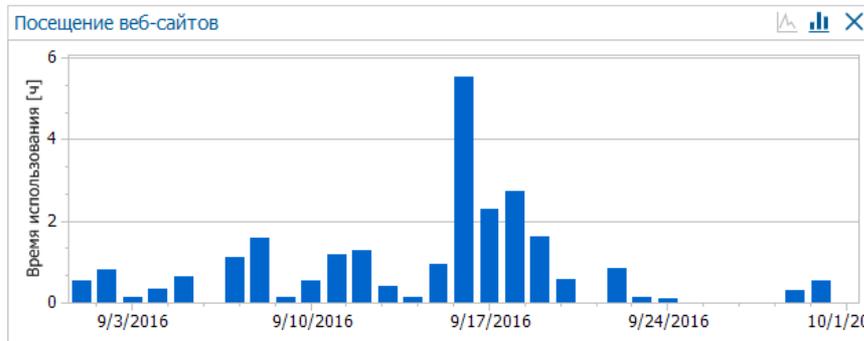
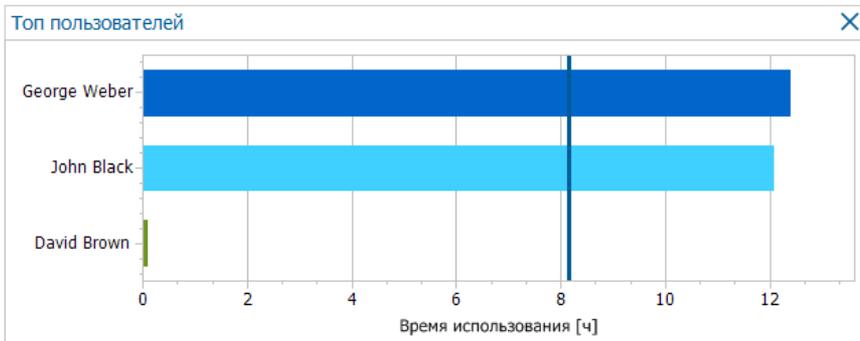
Упорядочить

Категория приложен... Y

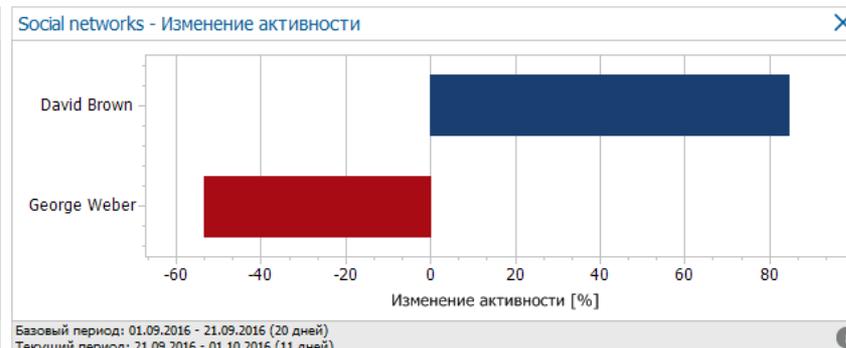
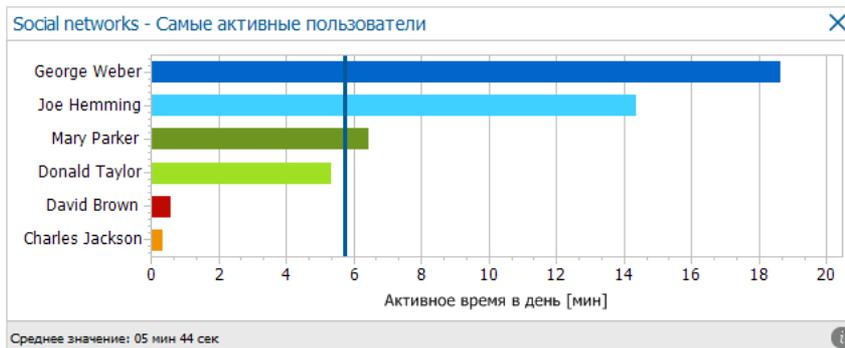
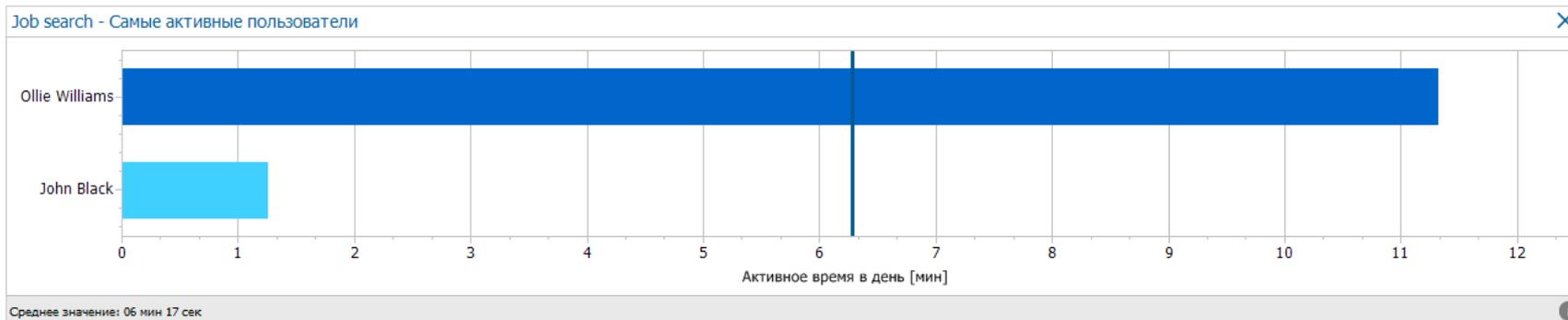


АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

# ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ AUDITOR)



# ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ AUDITOR)



# ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ AUDITOR)

- › **Дополнительная мотивация сотрудников**  
*по итогам оценки эффективности труда*
- › **Обоснование для расширения штата**  
*на основе объективной информации о загруженности*
- › **Снижение нагрузки на сотрудника/отдел**  
*и справедливое распределение обязанностей внутри рабочей группы*



# ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ SUPERVISOR)



WEB-КОНТРОЛЬ



КОНТРОЛЬ ПРИЛОЖЕНИЙ



КОНТРОЛЬ ПЕЧАТИ

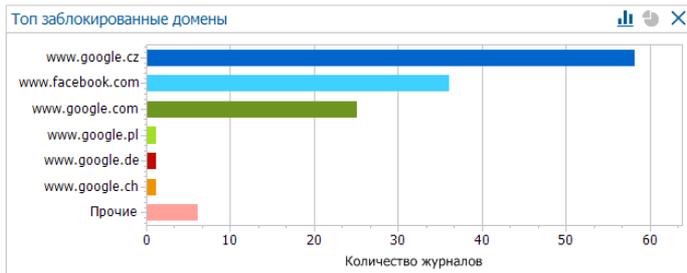
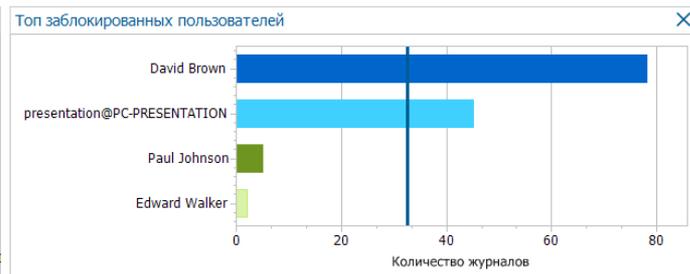
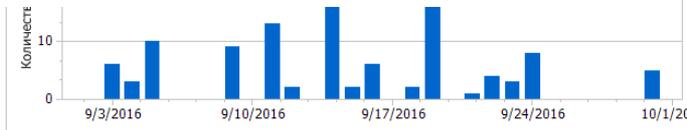
# ОФИСНЫЙ КОНТРОЛЬ (WEB-КОНТРОЛЬ)



Действие по умолчанию:  —  Разрешено

Добавить правило

Имя	Подробнее
Блокировка по категориям	Категории: File hosting, Job search, Malware, Pornography, ...
Блокировка по IP	Категории: Pornography IP-адрес: 192.168.0.5, 192.168.0.15 - ...
Блокировка по домену	URL: *.facebook.com/*, *.twitter.com/*



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

# ОФИСНЫЙ КОНТРОЛЬ (КОНТРОЛЬ ПРИЛОЖЕНИЙ)



Новое правило

Введите путь к приложению  
Путь может содержать символ \*. Например: C:\Users\\*\(Roaming)\*

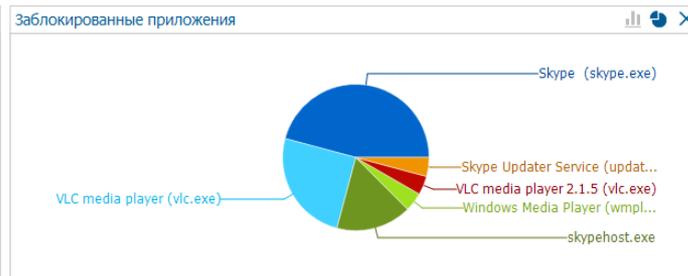
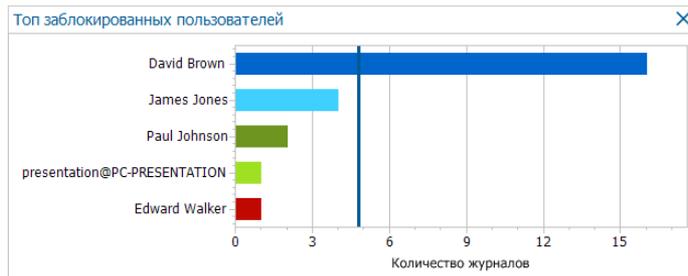
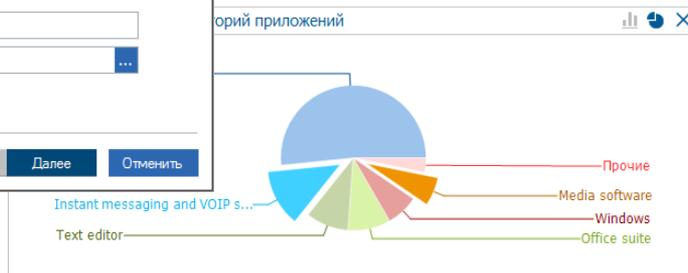
Выберите категорию

Имя:

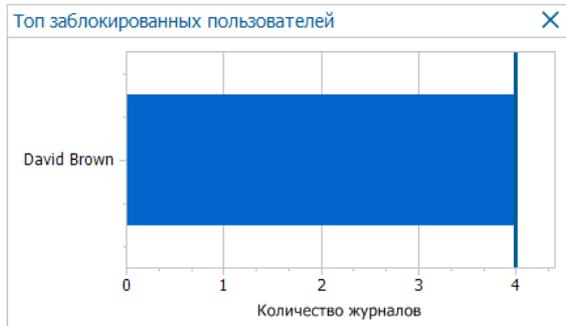
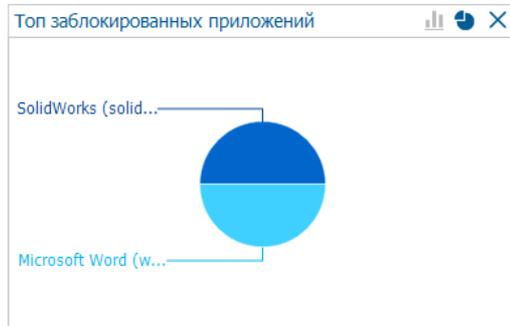
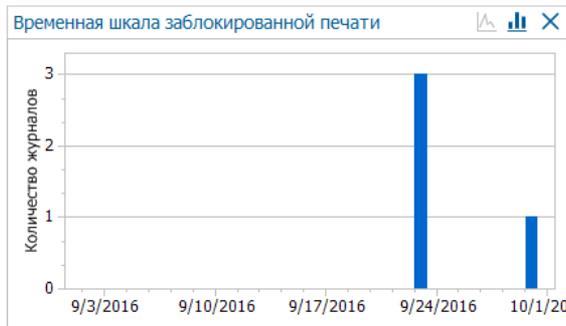
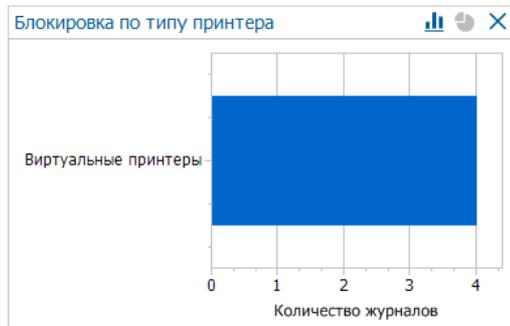
Путь к программе:

Область действия:  Везде

Назад Далее Отменить



# ОФИСНЫЙ КОНТРОЛЬ (КОНТРОЛЬ ПЕЧАТИ)



Состояние квот

Текущее состояние квот для выбранных пользователей/группы

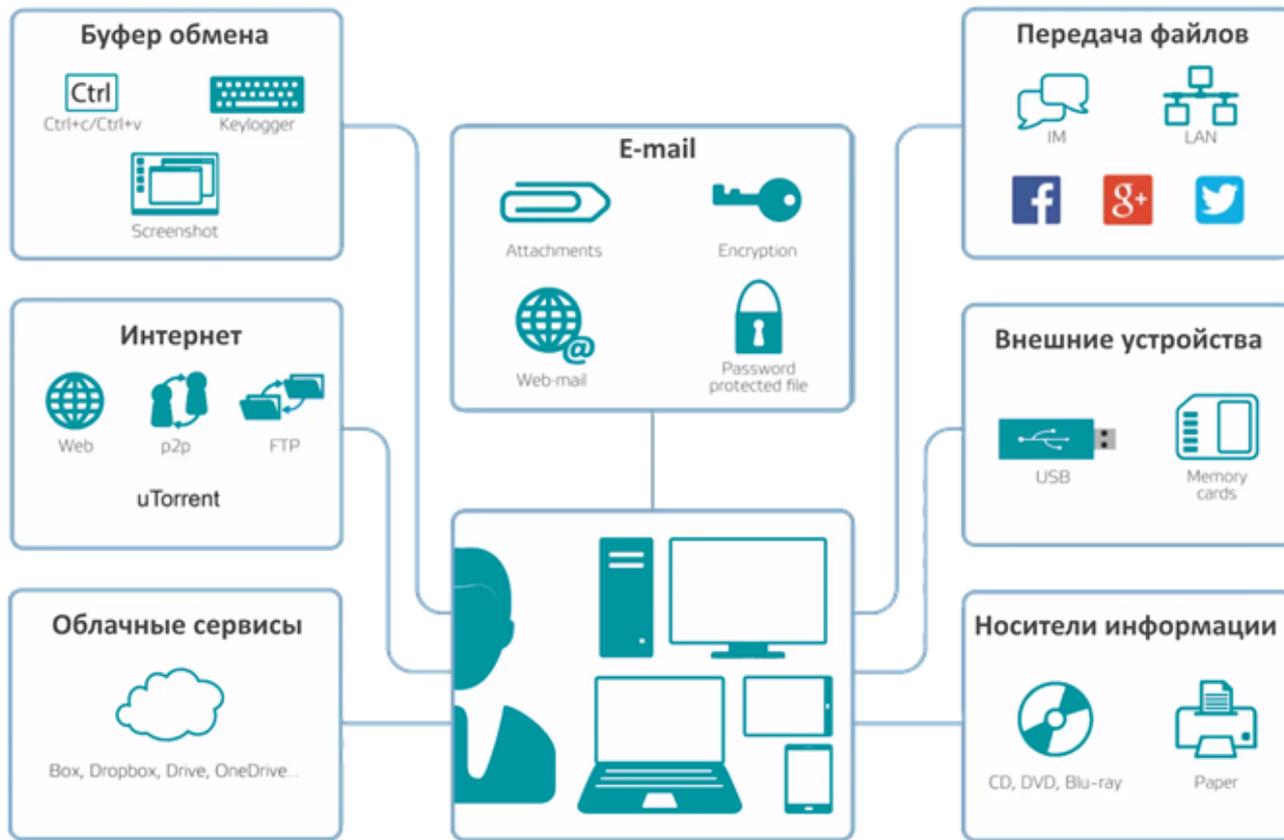
Имя пользователя	Всего страниц (регул...	Цветные страницы (...)
esetnote01		
PC-Garcia	50 (50)	0 (0)
William Garcia	50 (50)	0 (0)
PC-Jones	50 (50)	0 (0)
James Jones	50 (50)	0 (0)
PC-Parker	50 (50)	0 (0)
Mary Parker	50 (50)	0 (0)
PC-Hemming	50 (50)	0 (0)
PC-Jackson	50 (50)	0 (0)
PC-Walker	50 (50)	0 (0)
PC-Wilson	50 (50)	0 (0)
Michael Wilson	50 (50)	0 (0)
Edward Walker	50 (50)	0 (0)

0 из 0

OK



# ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (МОДУЛЬ DLP)



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА



safetica

# 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 (КОНТЕНТНЫЙ ФИЛЬТР)

## › ПРЕДУСТАНОВЛЕННОЕ СОДЕРЖИМОЕ

*Идентификационные номера и номера социального страхования различных стран, номера кредитных карт, номера банковских счетов.*

## › КЛЮЧЕВЫЕ СЛОВА И РЕГУЛЯРНЫЕ ВЫРАЖЕНИЯ

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

## › МЕТАДАННЫЕ СТОРОННИХ КЛАССИФИКАТОРОВ

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



# ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ

## ПРЕДУСТАНОВЛЕННЫЕ ПРАВИЛА

### ^ ОСНОВНАЯ ИНФОРМАЦИЯ

Политики DLP настраивают безопасность данных в вашей среде. Политики управляют общим потоком данных, конкретными данными или приложениями и предлагают действия DLP, от автоматической регистрации событий до строгой блокировки. Чтобы ознакомиться с политиками DLP, посетите [базу знаний Safetica](#).

#### Новая политика безопасности

△ Применяется первое соответствующее правило политики.

Политика	Тип	Режим		
↓ Patients + ...	TopSecret	Блокирова...	<a href="#">Изменить</a>	<a href="#">Удалить</a>
↓ Patients + ...	TopSecret	Уведомить	<a href="#">Изменить</a>	<a href="#">Удалить</a>
↓ Patients + ...	TopSecret	Блокирова...	<a href="#">Изменить</a>	<a href="#">Удалить</a>
↓ Patients + ...	TopSecret	Уведомить	<a href="#">Изменить</a>	<a href="#">Удалить</a>
↓ Financial Fil...	Sensitive	Уведомить	<a href="#">Изменить</a>	<a href="#">Удалить</a>
↓ Financial Fil...	Sensitive	Уведомить	<a href="#">Изменить</a>	<a href="#">Удалить</a>
↓ Multimedia...	Multimedia	Зарегистр...	<a href="#">Изменить</a>	<a href="#">Удалить</a>
↓ Multimedia...	Multimedia	Зарегистр...	<a href="#">Изменить</a>	<a href="#">Удалить</a>
↓ Patients + ...	Insurance - ...	Блокирова...	<a href="#">Изменить</a>	<a href="#">Удалить</a>
↓ Patients + ...	Insurance - ...	Уведомить	<a href="#">Изменить</a>	<a href="#">Удалить</a>
↓ Patients + ...	Insurance - ...	Блокирова...	<a href="#">Изменить</a>	<a href="#">Удалить</a>
↓ Patients + ...	Insurance - ...	Уведомить	<a href="#">Изменить</a>	<a href="#">Удалить</a>
↓ Design dat...	CAD softw...	Блокирова...	<a href="#">Изменить</a>	<a href="#">Удалить</a>
↓ MS Office ...	Office suite	Блокирова...	<a href="#">Изменить</a>	<a href="#">Удалить</a>
↓ MS Office ...	Office suite	Уведомить	<a href="#">Изменить</a>	<a href="#">Удалить</a>
↓ MS Office ...	Office suite	Уведомить	<a href="#">Изменить</a>	<a href="#">Удалить</a>
↓ Channel co...	Sensitive d...	Уведомить	<a href="#">Изменить</a>	<a href="#">Удалить</a>

### ^ ПОДРОБНОСТИ ПОЛИТИКИ

Имя политики: **Patients + Design Files policy - TopSecret - zone settings - notifying**

Описание политики: **Please see the manual.**

Тип политики: **Данные: TopSecret**

Режим политики: **Зарегистрировать и уведомить**

Политика применяется к: **Safetica**

### ^ ПРАВИЛА ПОЛИТИКИ

Загрузка в сеть: **Настройки пользовательской зоны**

Email: **Настройки пользовательской зоны**

Облачные хранилища: **Различающиеся настройки**

Буфер обмена (не регистрировать): **Уведомлен**

Создание скришота (не регистрировать): **Уведомлен**

Запись на диск: **Уведомлен**

Сеть (эксперт): **Настройки пользовательской зоны**

Локальные диски (эксперт): **Настройки пользовательской зоны**



# ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (МОДУЛЬ DLP)

## ^ ИНТЕГРАЦИЯ В ПРИЛОЖЕНИЯ

[Сбросить к настройкам по умолчанию](#)

Приложение	Активно в режиме	Состояние интеграции
Microsoft Edge (microsof...	Расширенный монитор...	<input checked="" type="checkbox"/> Активно
Microsoft OneDrive for B...	Расширенный монитор...	<input checked="" type="checkbox"/> Активно
Microsoft OneNote Quic...	Расширенный монитор...	<input checked="" type="checkbox"/> Активно
Firefox (firefox.exe)	Расширенный монитор...	<input checked="" type="checkbox"/> Активно
Thunderbird (thunderbir...	Расширенный монитор...	<input checked="" type="checkbox"/> Активно
Send to OneNote Tool (O...	Расширенный монитор...	<input checked="" type="checkbox"/> Активно
Microsoft OneNote (ONE...	Расширенный монитор...	<input checked="" type="checkbox"/> Активно
Microsoft Outlook (outlo...	Расширенный монитор...	<input checked="" type="checkbox"/> Активно
Microsoft Edge Content ...	Расширенный монитор...	<input checked="" type="checkbox"/> Активно
Yandex (browser.exe)	Расширенный монитор...	<input checked="" type="checkbox"/> Активно
Browser_Broker (browser_...	Расширенный монитор...	<input checked="" type="checkbox"/> Активно
Microsoft Word (WINWO...	Расширенный монитор...	<input checked="" type="checkbox"/> Активно
Runtime Broker (runtime...	Расширенный монитор...	<input checked="" type="checkbox"/> Активно

## ^ ИНТЕГРИРОВАННЫЕ ТЕХНОЛОГИИ

- Сетевой уровень:  Активировать
- Расширение MAPI:  Активировать
- Контекстное меню:  Активировать

## ^ ДРАЙВЕРЫ

 Для завершения деактивации требуется перезагрузить компьютер.

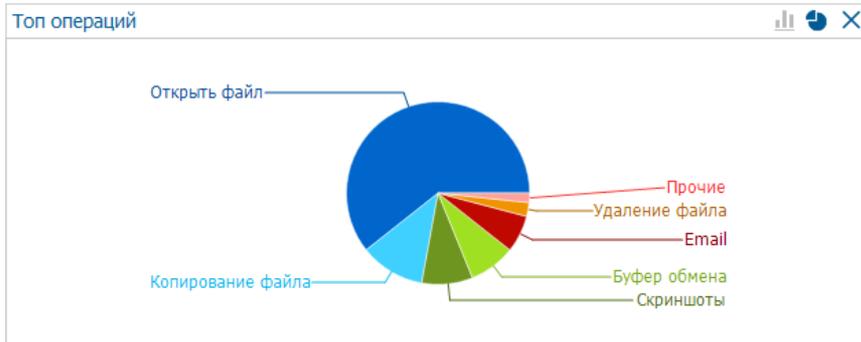
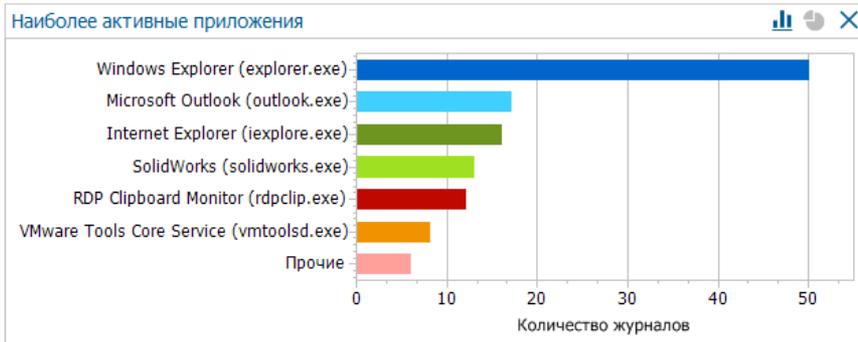
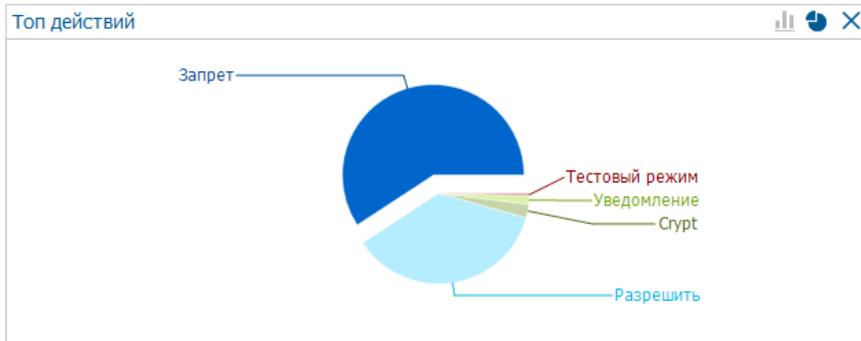
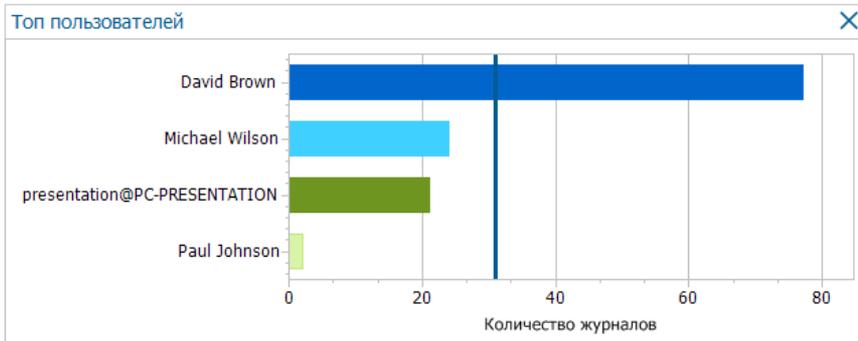
- Драйвер диска Safetica:  Активировать
- Драйвер шифрования Safetica:  Наследовать
- Safetica device driver:  Наследовать

## ^ СЕРВИСЫ

- Safetica net monitor service:  Активировать
- Safetica DLP service:  Активировать
- Служба мониторинга файлов Safetica:  Активировать
- Служба классификации Safetica:  Активировать
- Служба приложений Safetica:  Активировать
- Обслуживание устройств Safetica:  Наследовать

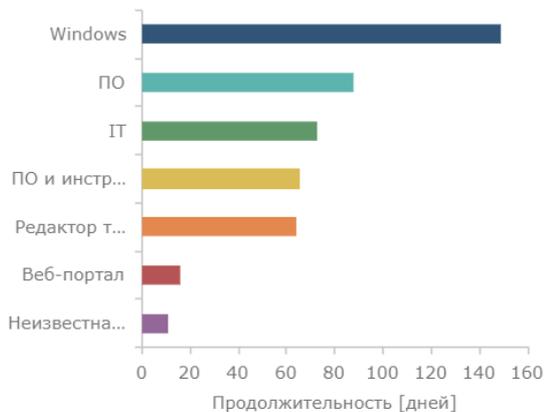


# ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (МОДУЛЬ DLP)



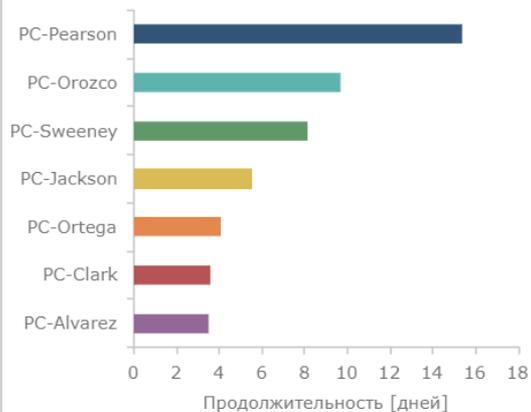
# АНАЛИЗ РЕЗУЛЬТАТОВ WEBSAFETICA

## КАК СОТРУДНИКИ ИСПОЛЬЗОВАЛИ С...



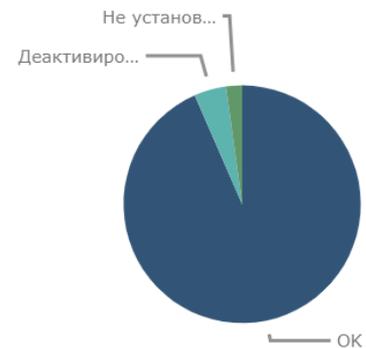
АНАЛИЗ ПОВЕДЕНИЯ >

## КАКИЕ КОМПЬЮТЕРЫ БЫЛИ НАИБО...



ИСПОЛЬЗОВАНИЕ РЕСУРСОВ >

## КАК ЗАЩИЩЕНА МОЯ КОМПАНИЯ?



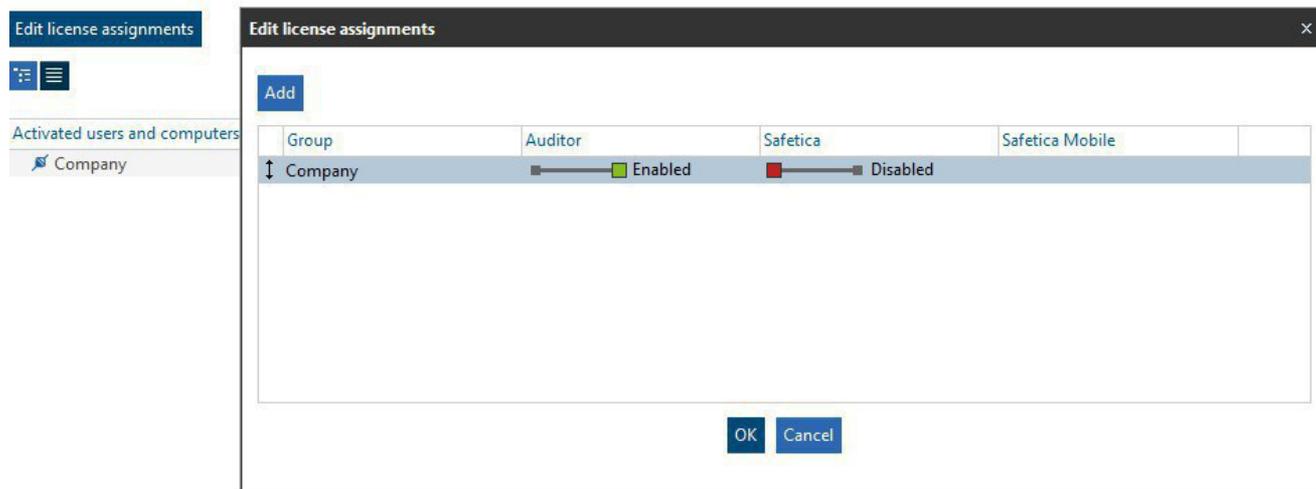
УПРАВЛЕНИЕ >



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

# УПРАВЛЕНИЕ ЛИЦЕНЗИЕЙ РАСПРЕДЕЛЕНИЕ МОДУЛЕЙ

Активируйте необходимые модули



# 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

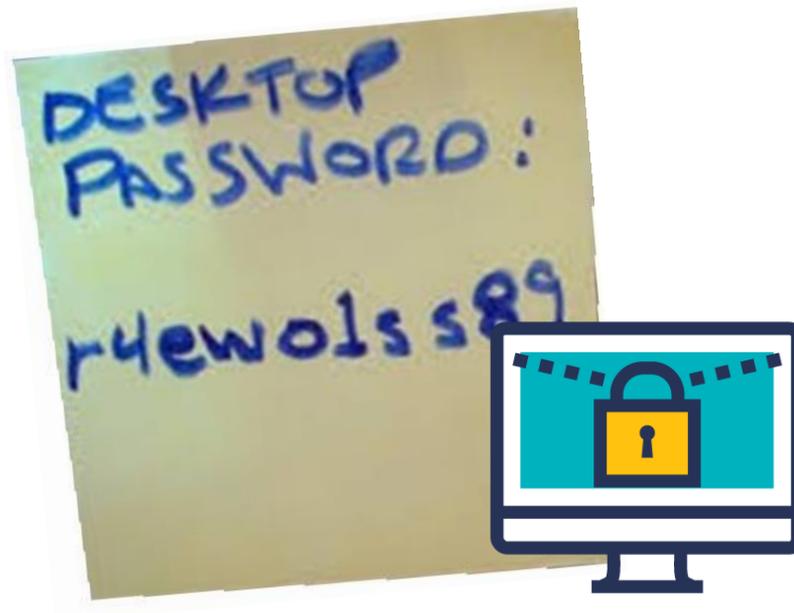
# w#hN02v)b56

1234567890

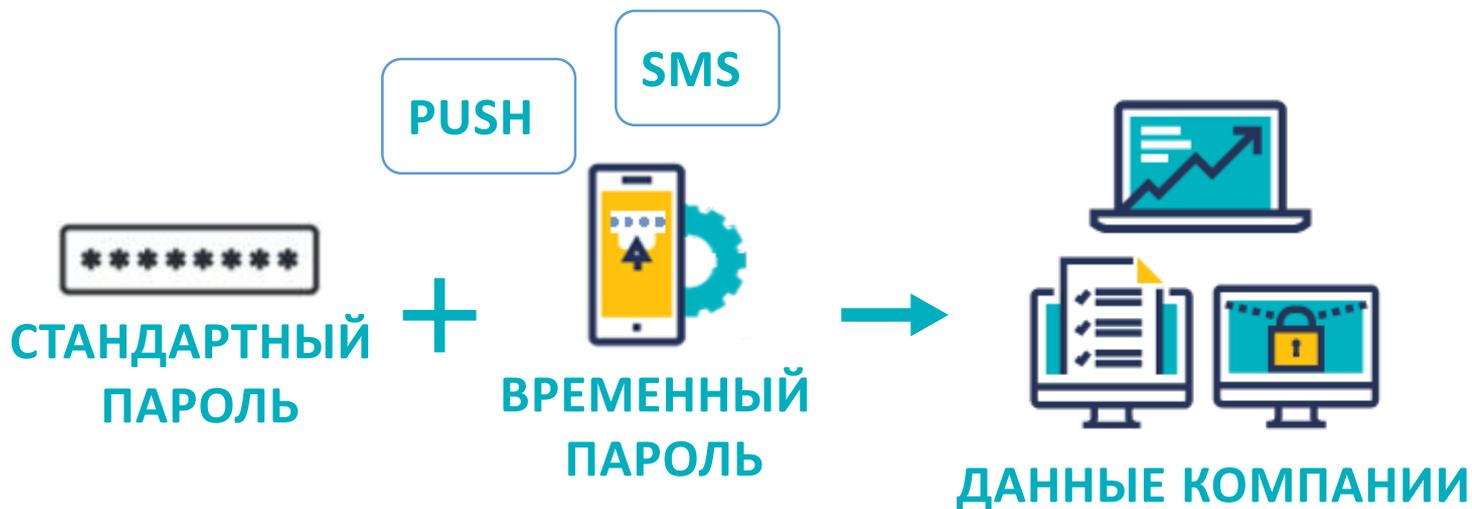
0987654321

Password123

Marina1990

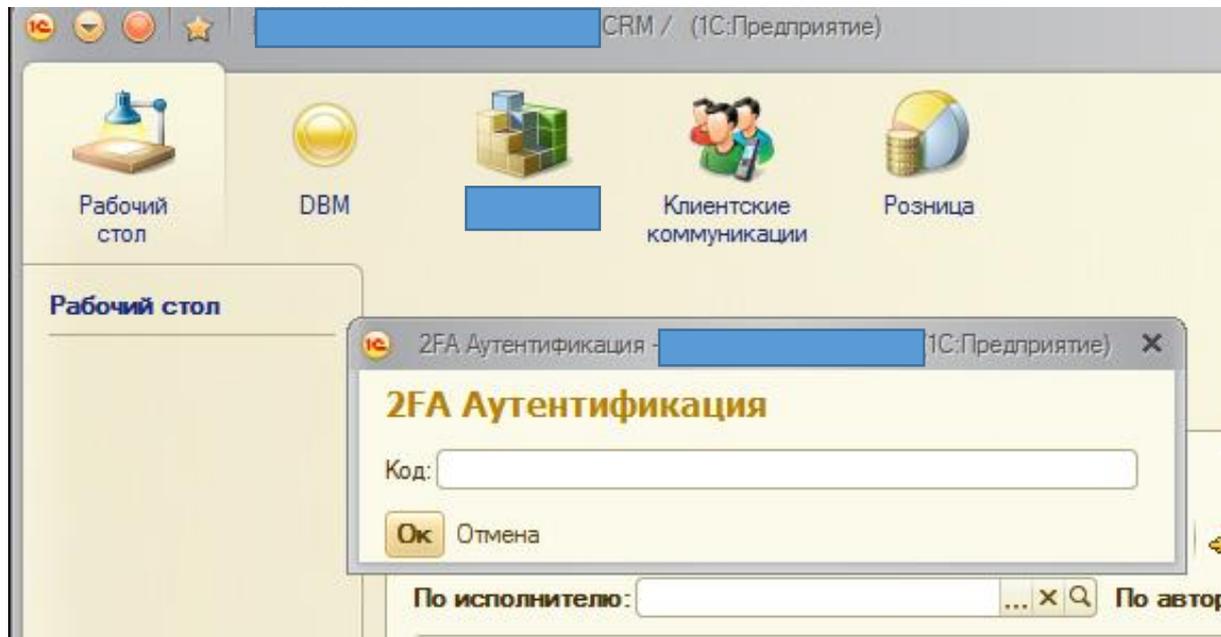


# ESET Secure Authentication



- **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?

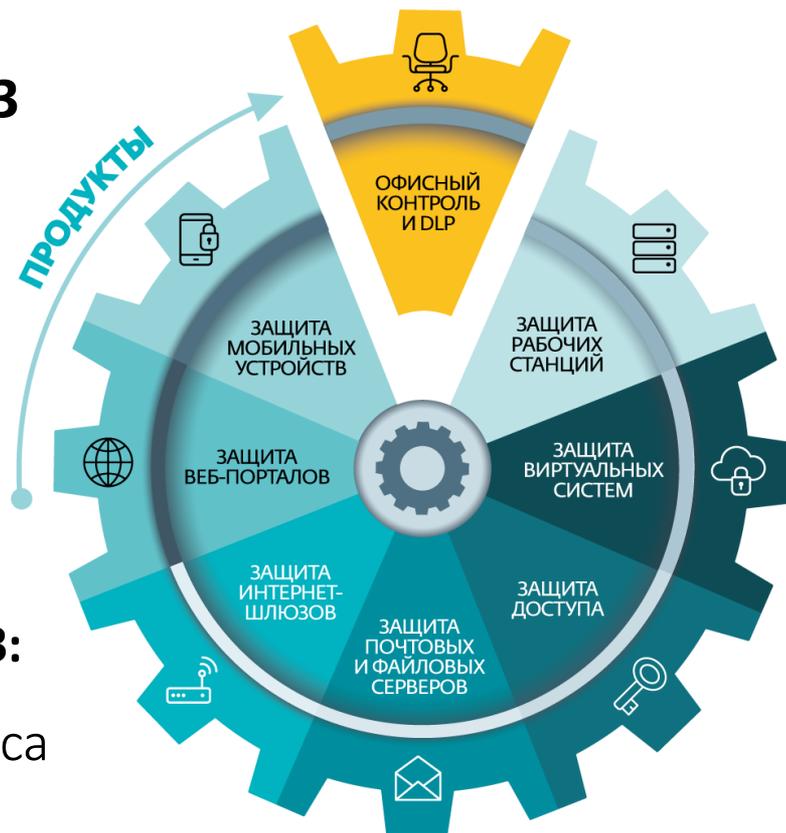
## КОМПЛЕКСНЫЙ ПОДХОД:

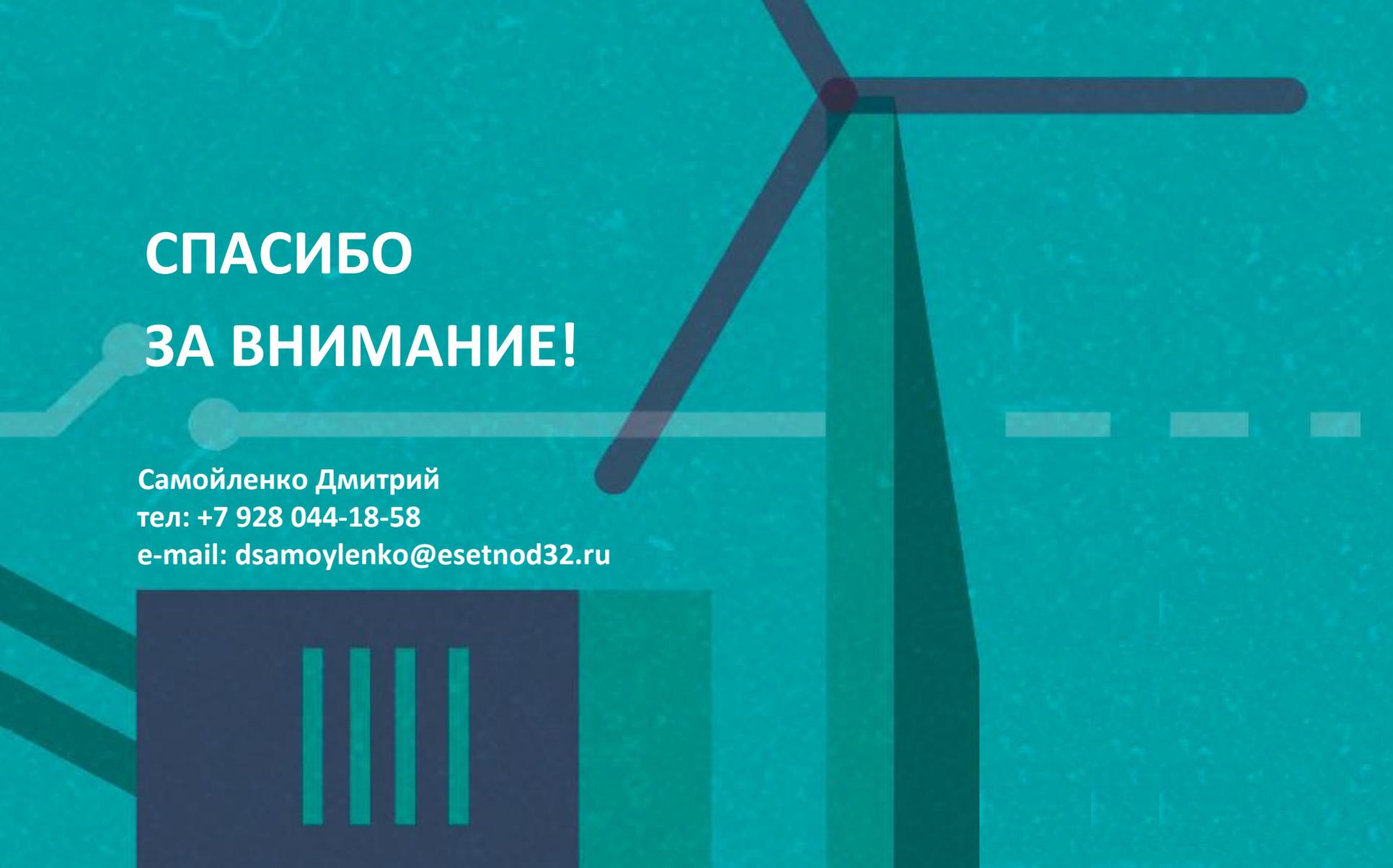
### 1. БЕЗОПАСНОСТЬ ОТ ВНЕШНИХ УГРОЗ

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

### 2. БЕЗОПАСНОСТЬ ОТ ВНУТРЕННИХ УГРОЗ:

- › Офисный контроль и DLP Safetica
- › ESA





**СПАСИБО**

**ЗА ВНИМАНИЕ!**

Самойленко Дмитрий

тел: +7 928 044-18-58

e-mail: [dsamoylenko@esetnod32.ru](mailto:dsamoylenko@esetnod32.ru)