



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ОПЕРЕЖАЮЩАЯ ЗАЩИТА ОТ КИБЕРУГРОЗ И ШИФРАТОРОВ

Кудров Максим

Presale engineer ESET Russia



СОДЕРЖАНИЕ

1. Компания и технологии
2. Централизованное управление
3. Защита рабочих станций и мобильных устройств
4. Защита серверов и шлюзов
5. Встроенная песочница
6. Решение класса EDR
7. Награды, тесты и кейсы



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

О КОМПАНИИ



РАЗВИВАЕМ
ТЕХНОЛОГИИ
БЕЗОПАСНОСТИ
УЖЕ 30 ЛЕТ

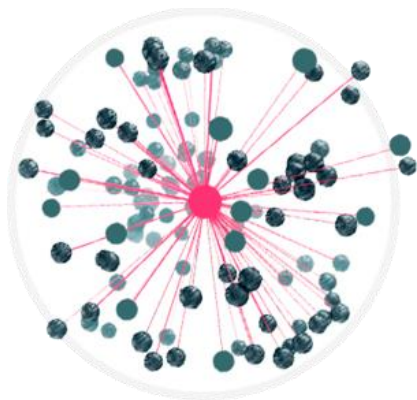


ПЕРВЫЙ ВЕНДОР,
ЗАВОЕВАВШИЙ
100 НАГРАД
VIRUS BULLETIN

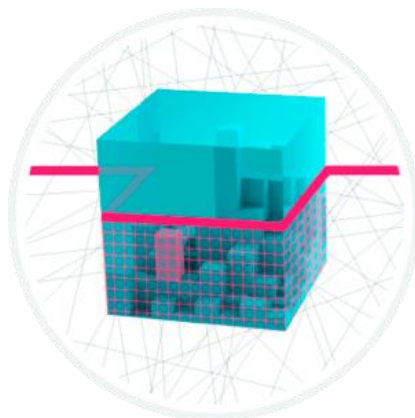


АНТИВИРУСНЫЙ
ВЕНДОР №4
В КОРПОРАТИВНОМ
СЕКТОРЕ В МИРЕ*

НОВЫЕ ТЕХНОЛОГИИ В ПРОДУКТАХ ESET ДЛЯ БИЗНЕСА



ЗАЩИТА ОТ
БОТНЕТОВ



СКАНЕР
UEFI



ЗАЩИТА ОТ
ШИФРАТОРОВ



АНТИВИРУСНАЯ ЗАЩИТА СО ВСТРОЕННЫМ ФАЙЕРВОЛОМ И ЗАЩИТОЙ ОТ ШИФРАТОРОВ



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ТЕХНОЛОГИИ ESET

ЭВОЛЮЦИЯ ЗАЩИТЫ

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



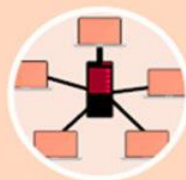
ЗАЩИТА ОТ ПРОГРАММ-
ВЫМОГАТЕЛЕЙ



ЗАЩИТА
ОТ ЭКСПЛОЙТОВ



ОБЛАЧНАЯ СИСТЕМА
ЗАЩИТЫ



ЗАЩИТА
ОТ БОТНЕТОВ

ДО ВЫПОЛНЕНИЯ УГРОЗЫ

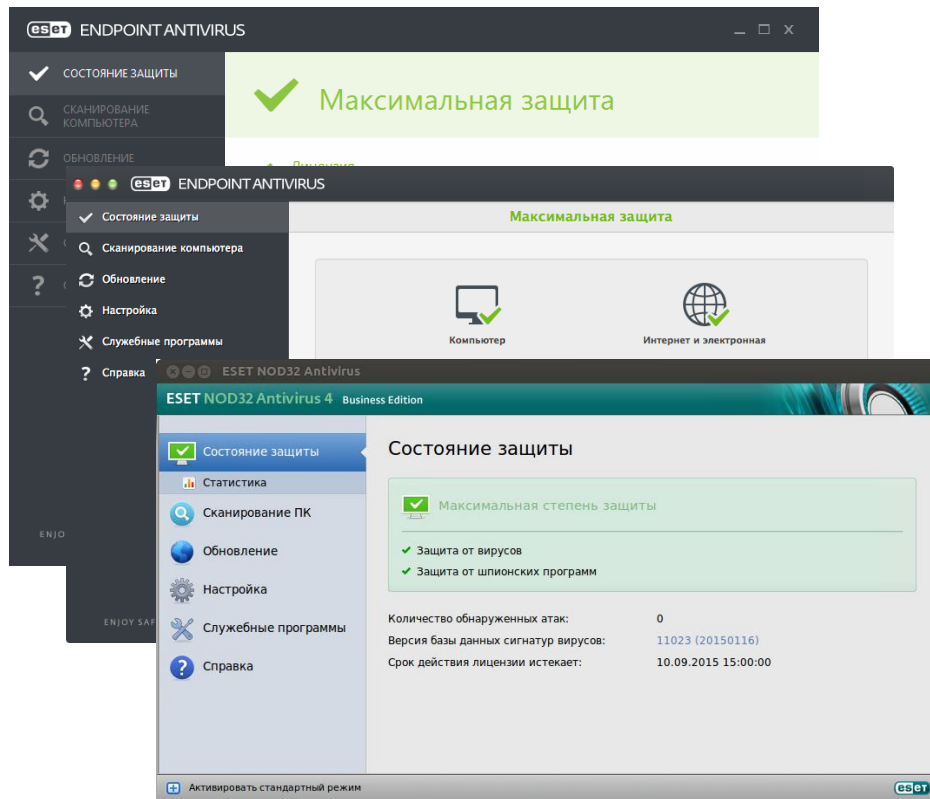
ПОСЛЕ ВЫПОЛНЕНИЯ УГРОЗЫ

ESET ENDPOINT ANTIVIRUS

ЗАЩИТА РАБОЧИХ СТАНЦИЙ



- ✓ *Защита* рабочих станций на Microsoft Windows, macOS, Linux
- ✓ *Минимальное влияние* на систему
- ✓ *Централизованное* управление

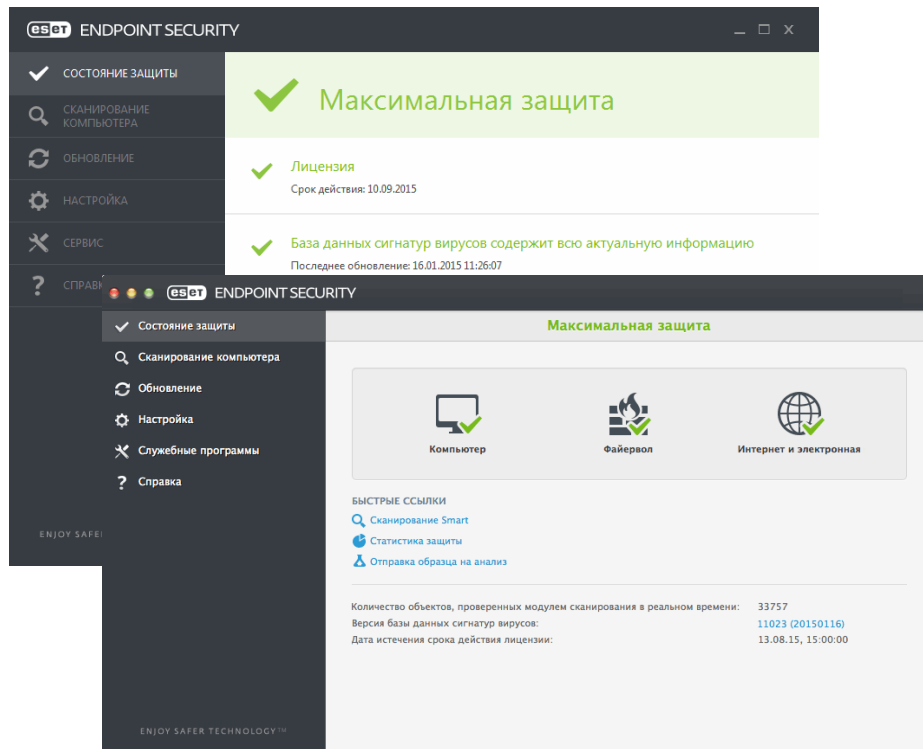


ESET ENDPOINT SECURITY

РАСШИРЕННАЯ ЗАЩИТА РАБОЧИХ СТАНЦИЙ



- ✓ *Защита рабочих станций на Microsoft Windows и macOS*
- ✓ *Контроль пользователя*
- ✓ *Защита сети*
- ✓ *Выбор компонентов для установки*



СРАВНЕНИЕ ФУНКЦИЙ



Расширенная защита
рабочих станций
(ESET Endpoint Security)



Защита рабочих станций
(ESET Endpoint Antivirus)



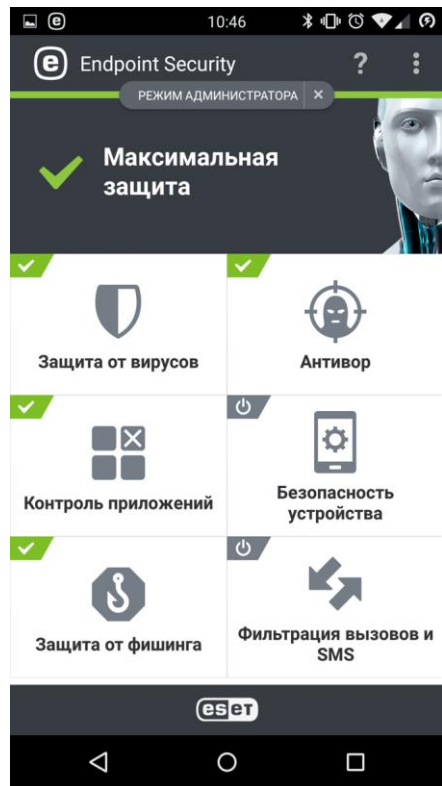
Антивирус	●	●
Антишпион	●	●
Антифишинг	●	●
Файервол	●	●
Защита от сетевых атак	●	●
Антиспам	●	●
Контроль устройств	●	●
Веб-контроль	●	●
HIPS	●	●
Защита от ботнетов	●	● new
Защита от эксплойтов	●	●
Защита от шифраторов	● new	● new
Сканер UEFI	● new	● new

ESET ENDPOINT SECURITY ДЛЯ ANDROID

ЗАЩИТА МОБИЛЬНЫХ УСТРОЙСТВ



- ✓ *Защита мобильных устройств на Android*
- ✓ *Контроль устройства*
- ✓ *Контроль приложений*
- ✓ *Модуль «Антивор»*
- ✓ *Централизованное управление*

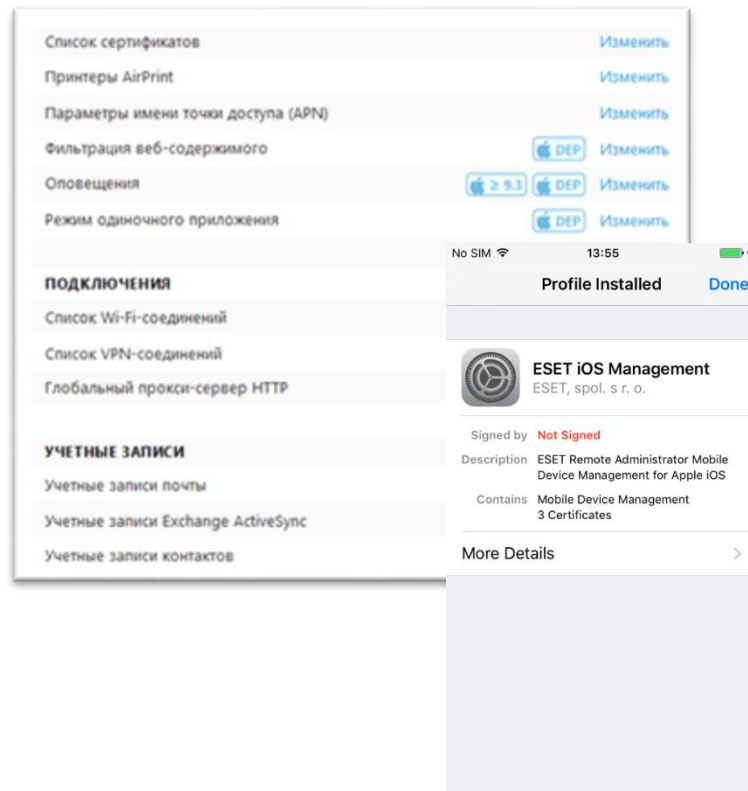


ESET MOBILE DEVICE MANAGEMENT

УПРАВЛЕНИЕ IOS УСТРОЙСТВАМИ



- ✓ «Антивор»
- ✓ «Белый» и «Черный» списки приложений
- ✓ Фильтрация веб-контента
- ✓ Удаленное управление параметрами Exchange, Wi-Fi и VPN
- ✓ Настройка времени автоматической блокировки, сложности пароля



ЗАЩИТА СЕРВЕРОВ



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ESET FILE SECURITY ДЛЯ WINDOWS



- ✓ Оптимизация работы в *серверной среде*
- ✓ Поддержка *кластерной* структуры
- ✓ *Многопоточное сканирование* без снижения производительности
- ✓ Сканирование *Hyper-V*

The screenshot displays the ESET File Security for Microsoft Windows Server interface. The left sidebar contains navigation options: ОТСЛЕЖИВАНИЕ (selected), ФАЙЛЫ ЖУРНАЛОВ, СКАНИРОВАТЬ, ОБНОВЛЕНИЕ, НАСТРОЙКА, СЕРВИС, and СПРАВКА И ПОДДЕРЖКА. The main area shows a green status bar with 'Максимальная защита' and three green checkmarks indicating 'Лицензия' (valid until 10.09.2015) and 'База данных сигнатур вирусов содержит всю актуальную информацию' (last updated 16.01.2015 14:19:48). Below this is a 'Статистика защиты файловой системы' section with the following data:

Заражено:	0
Очищено:	0
Очистить:	18992
Всего:	18992

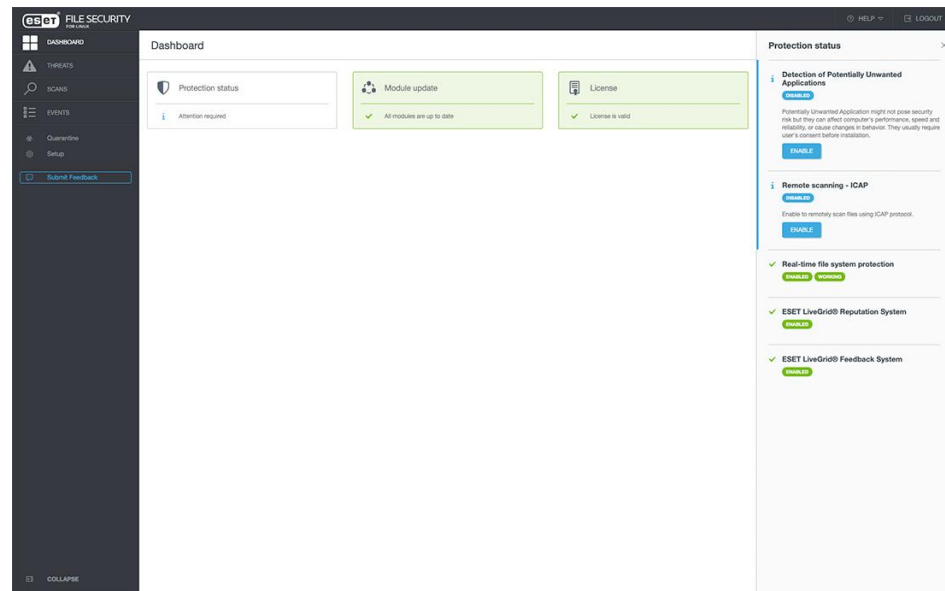
At the bottom, system information is provided:

Версия продукта:	6.0.12025.1
Имя сервера:	WIN-U7OR9A7EUC3.eset.test
Система:	Windows Server 2012 Standard Evaluation 64-bit (6.2.9200)
Компьютер:	Intel(R) Core(TM) i7-2640M CPU @ 2.80GHz (2791 MHz), 2000 MB RAM
Время работы сервера:	28 мин.

ESET FILE SECURITY ДЛЯ LINUX



- ✓ *Защита файловой системы в режиме реального времени*
- ✓ *Мультисервисная архитектура*
- ✓ *Сканирование сетевого хранилища*
- ✓ *Поддержка SELinux*



ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ

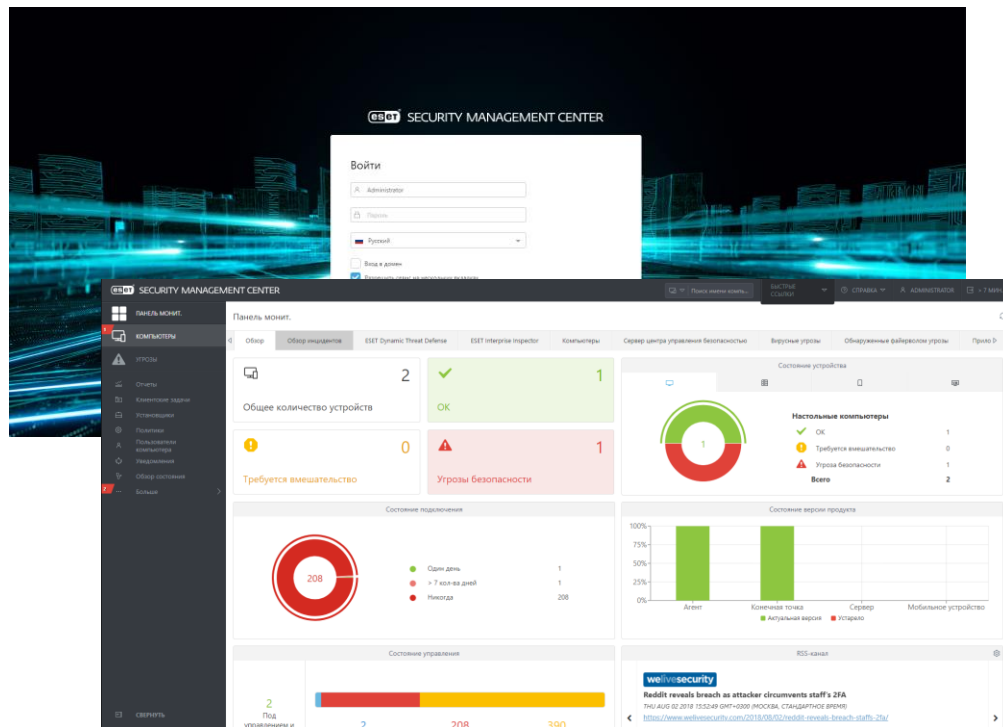


АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ESET SECURITY MANAGEMENT CENTER

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ

- ✓ ESET Push Notification Service (EPNS)
- ✓ Автоматическое определение «КЛООНОВ»
- ✓ Инвентаризация оборудования
- ✓ Поддержка ESET Dynamic Threat Defense
- ✓ Возможность управления мобильными устройствами MDC



ESET SECURITY MANAGEMENT CENTER

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ

✓ *Инвентаризация оборудования*

SECURITY MANAGEMENT CENTER

Панель мониторинга

Компьютеры

Угрозы

Отчеты

Конфигурация

Журналы

Выполнения задачи

Установленные приложения

Предупреждения

Вопросы

Угрозы и карантин

Подобности

Свернуть

Панель мониторинга

Инциденты

ESET Dynamic Threat Defense

ESET Interprise Inspector

Компьютеры

Сервер центра управления безопасностью

Компьютеры с соответствующими сведениями

Имя компьютера	Изготовитель устройства	Модель устройства	Серийный номер
esetnote25.eset.local	LENOVO	4180PUG	PBAK414
esetnote25.eset.local	LENOVO	4180PUG	PBAK414

Создано 1 мин. назад

Компьютеры со сведениями о ЦП

Имя компьютера	Изготовитель	Описание	Число ядер
esetnote25.eset.local	GenuineIntel	Intel(R) Core(TM) i7-2640M	2
esetnote25.eset.local	GenuineIntel	Intel(R) Core(TM) i7-2640M	2

Создано 1 мин. назад

Компьютеры со сведениями об ОЗУ

Группировка (без компьютера)	Группировать по типу архитектуры	Общая емкость в МБ
esetnote25.eset.local	Неизвестно	16384
esetnote25.eset.local	Неизвестно	16384

Создано 0 мин. назад

Число компьютеров, сгруппированных по общей емкости

4

■ 8192

Создано 0 мин. назад

< НАЗАД Компьютеры >

ОБЗОР

КОНФИГУРАЦИЯ

ЖУРНАЛЫ

ВЫПОЛНЕНИЯ ЗАДАЧИ

УСТАНОВЛЕННЫЕ ПРИЛОЖЕНИЯ

ПРЕДУПРЕЖДЕНИЯ

ВОПРОСЫ

УГРОЗЫ И КАРАНТИН

ПОДРОБНОСТИ

Основное Оборудование Продукты и лицензии

Устройство

Изготовитель: LENOVO
 Модель: 4180PUG
 Серийный номер: PBAK414

CPU

Описание: Intel(R) Core(TM) i7-2640M CPU @ 2.80GHz
 Тактовая частота: 2801 MHz
 Число ядер: 2
 Число логических ядер: 4
 Тип архитектуры: x64
 Изготовитель: GenuineIntel

RAM

Емкость: 8 GiB
 Тактовая частота: 1333 MHz
 Изготовитель: Kingston
 Описание: Physical Memory
 Тип архитектуры: Неизвестно

Емкость: 8 GiB
 Тактовая частота: 1333 MHz
 Изготовитель: Kingston
 Описание: Physical Memory
 Тип архитектуры: Неизвестно

Хранилище

Тип: Физический дисковый накопитель
 Описание: INTEL SSDSC2BW480A4 SCSI Disk Device
 Емкость: 447 GiB
 Серийный номер: PHDA410301PH4805GN
 Изготовитель: (Стандартные дисковые накопители)

Тип: Физический дисковый накопитель
 Описание: HITACHI HTS727550A9E364 SCSI Disk Device
 Емкость: 465 GiB

ЗАКРЫТЬ КОМПЬЮТЕР

ESET BUSINESS ACCOUNT

ОБЛАЧНЫЙ ПОРТАЛ ДЛЯ КОРПОРАТИВНЫХ КЛИЕНТОВ

✓ *Управление лицензиями корпоративных продуктов и пользователями*

✓ *Входная точка для подключения облачных решений*

The screenshot displays the ESET Business Account web portal. The interface is divided into several sections:

- Top Bar:** Includes the ESET logo, "BUSINESS ACCOUNT", and user information (ANDREY ERMOLOV).
- Left Sidebar:** Contains navigation options: "ПАНЕЛЬ МОНИТОРИНГА", "ПРЕДУПРЕЖДЕНИЯ", "ЛИЦЕНЗИИ", "Активированные устройства", "Управление пользователями", "Журнал аудита", "Подробности", "Параметры", and "Отправить отзыв".
- Main Content Area:**
 - Лицензии (Licenses):** A table with columns: "ЛИЦЕНЗИЯ", "ПРОДУКТ", "ВЛАДЕЛЕЦ". It lists licenses such as "ESET Secure Enterprise", "ESET Endpoint Security + File Security", and "ESET Dynamic Threat Defense".
 - Активированные устройства (Activated Devices):** A table with columns: "УСТРОЙСТВО", "ИМЯ РАБОЧЕГО МЕСТА", "ПРОДУКТ", "ВЕРСИЯ", "КЕМ АКТИВИРОВАНО". It shows a device with IP "gateway.mydomain.local" and "ESET Dynamic Threat Defense for Endpoint Security + File Security" version "7.0.12016.0".
- Bottom Bar:** Includes buttons for "ДОБАВИТЬ ЛИЦЕНЗИЮ", "УДАЛИТЬ", "ЭКСПОРТ AS CSV", and "20" items.

ВСТРОЕННАЯ ПЕСОЧНИЦА

Защита от угроз «нулевого дня»
с помощью встроенной песочницы



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ESET DYNAMIC THREAT DEFENSE

ОБНАРУЖЕНИЕ УГРОЗ НУЛЕВОГО ДНЯ

- ✓ *Встроенная песочница*
- ✓ *Машинное обучение*
- ✓ *Автоматическая защита*
- ✓ *Многоуровневое обнаружение угроз*

The screenshot displays the ESET Security Management Center interface. The main window shows a file analysis report for a file named 'http://ftp.nod... suspicious.bat'. The report is categorized as 'Подозрительный' (Suspicious) and 'Завершено' (Completed). The analysis details include the file's hash, name, and the reason for detection: 'Автоматически' (Automatically). The report also lists the source computer as 'esetnote25.eset.local' and the destination as 'Dynamic Threat Defense'.

The right-hand pane shows a detailed report titled 'ОТЧЕТ О ПОВЕДЕНИИ ФАЙЛОВ' (FILE BEHAVIOR REPORT). It lists several detected behaviors with their explanations and actions:

СТАТУС	Подозрительный
СТАТУС	Подозрительный
РАЗМЕР	150В
КАТЕГОРИЯ	Сценарий

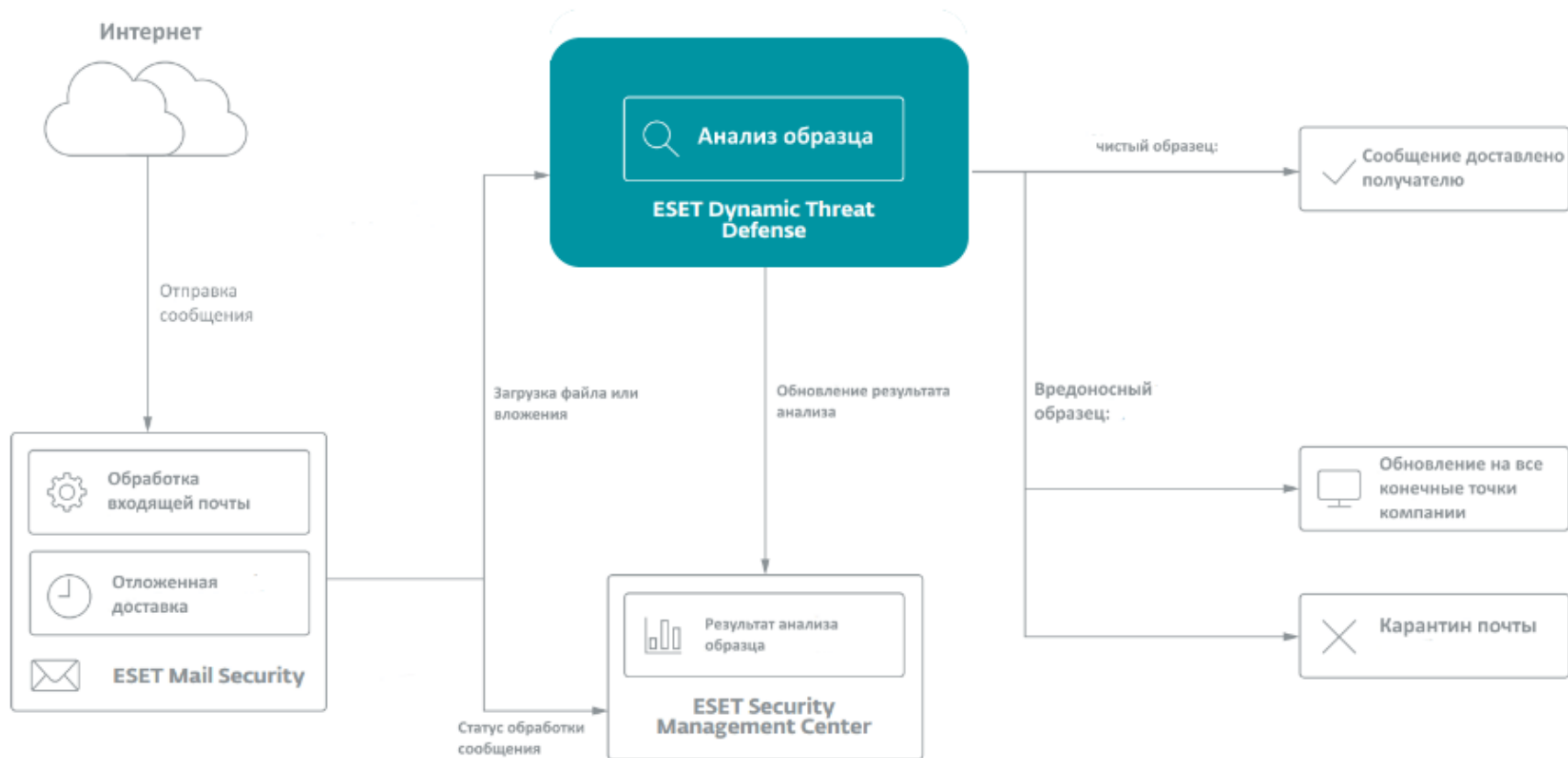
Обнаруженное поведение

ПОВЕДЕНИЕ	Объяснение	Полезные действия	Вредоносные действия
Проанализированный образец скопирован.	Образец был скопирован в другое расположение.	Это стандартное поведение для некоторых установщиков.	Вредоносная программа попыталась скрыть свое наличие.
Выполнение ADS.	Образец выполнил что-то из альтернативного потока данных (ADS).	Это необходимое поведение для чистых приложений.	Вредоносная программа попыталась скрыть свое наличие.
Внедрение кода в запущенный процесс.	Образец пытался внедрить код в запущенный процесс.	Это стандартное поведение для некоторых системных служебных программ.	Вредоносная программа попыталась скрыть свое наличие.
Сетевые подключения.	Образец пытался обмениваться данными с другим компьютером через сеть или прослушивать подключения других компьютеров.	Чистые образцы используют сетевые подключения для загрузки контента.	

At the bottom of the interface, there are buttons for 'ЗАКРЫТЬ' (Close), 'ПРОСМОТРЕТЬ ПОВЕДЕНИЕ' (View Behavior), and 'ДОБАВИТЬ ИСКЛЮЧЕНИЕ В ПОЛИТИКУ' (Add Exception to Policy).

ESET DYNAMIC THREAT DEFENSE

ОБНАРУЖЕНИЕ УГРОЗ НУЛЕВОГО ДНЯ



ESET DYNAMIC THREAT DEFENSE

ПОДДЕРЖИВАЕМЫЕ ПРОДУКТЫ

- ✓ *ESET Endpoint Antivirus 7* для Windows
- ✓ *ESET Endpoint Security 7* для Windows
- ✓ *ESET File Security 7* для Windows Server
- ✓ *ESET Mail Security 7* для Microsoft Exchange Server



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

РЕШЕНИЕ КЛАССА EDR

Анализ данных об инцидентах
и блокировка угроз



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ESET ENTERPRISE INSPECTOR

РЕШЕНИЕ КЛАССА EDR



Обнаружение

Поиск
вредоносных
аномалий



Отображение

Что затронуто?
Когда это произошло?
Как это произошло?



Реагирование

Блокировать
Удалить



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ESET ENTERPRISE INSPECTOR

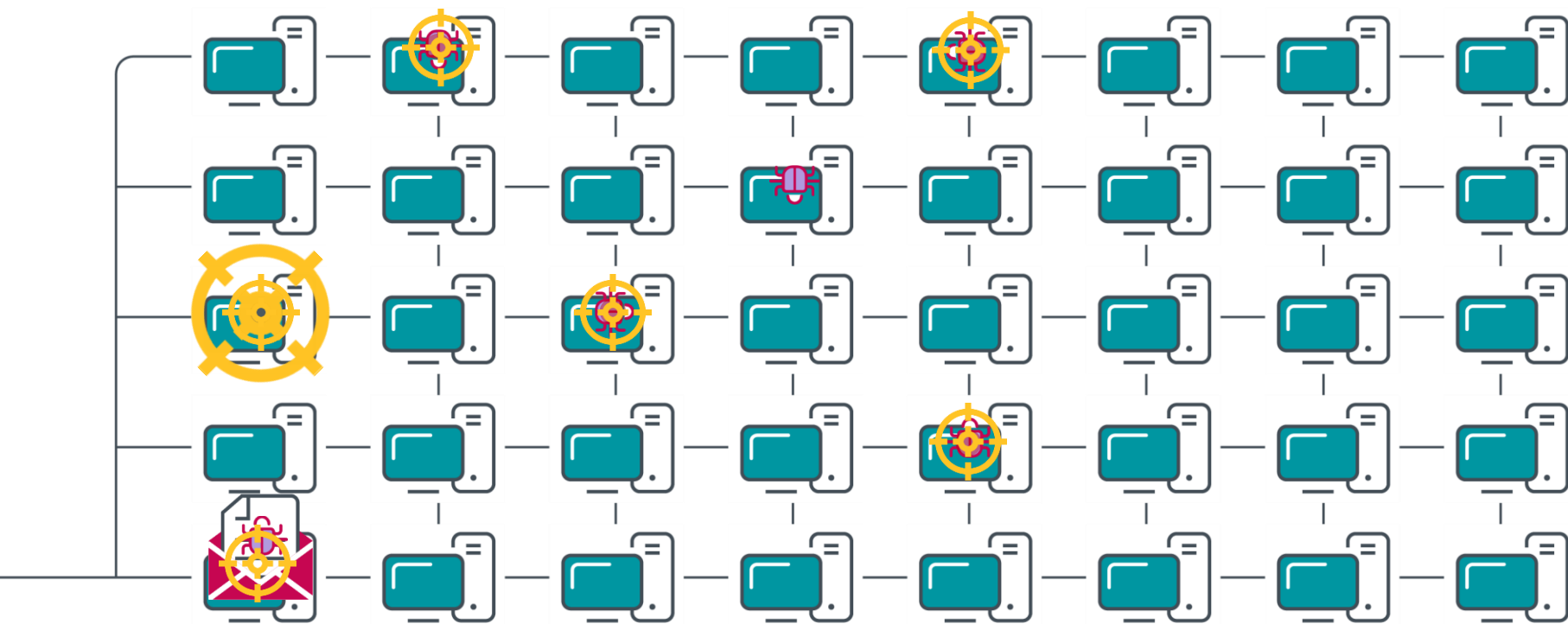
КАК ЭТО РАБОТАЕТ

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



ESET ENTERPRISE INSPECTOR

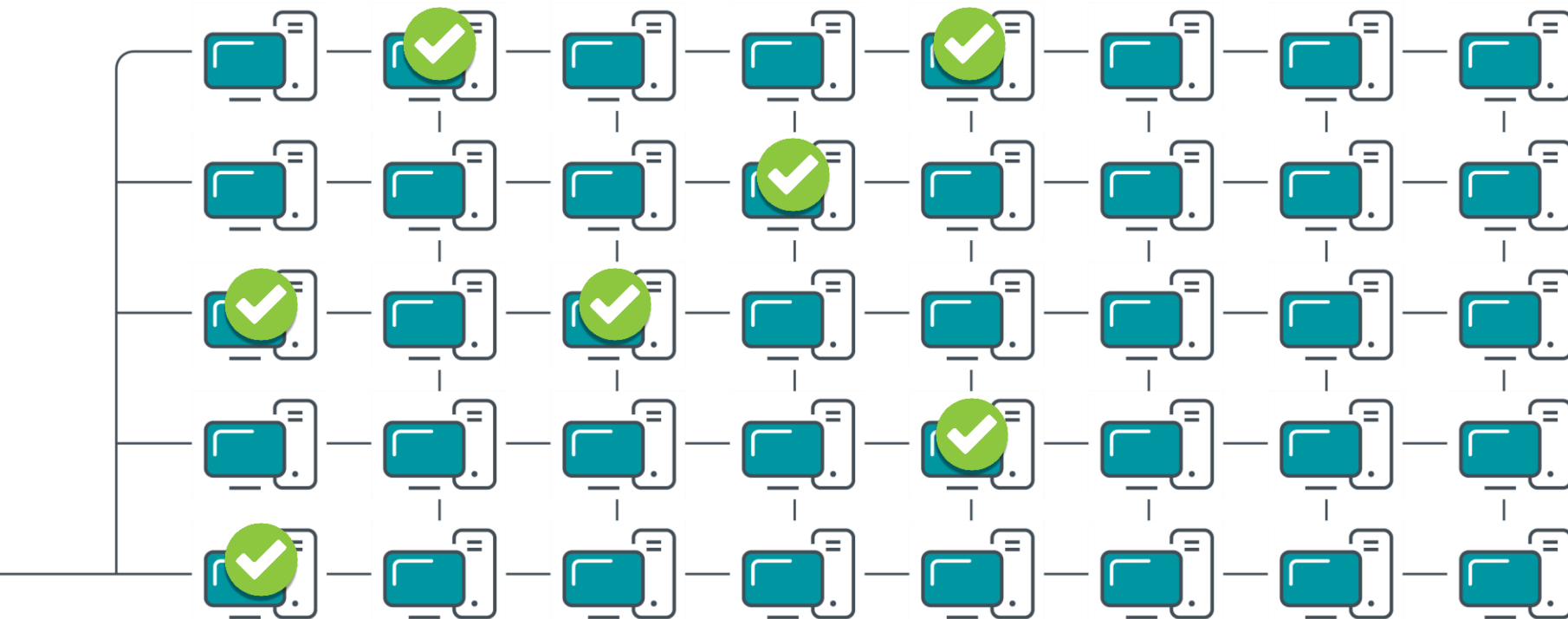
КАК ЭТО РАБОТАЕТ



Endpoints

ESET ENTERPRISE INSPECTOR

КАК ЭТО РАБОТАЕТ



Endpoints

ESET ENTERPRISE INSPECTOR

ENTERPRISE INSPECTOR Dashboard

Alarms Executables Computers More Server status

Executable popularity

ENTERPRISE INSPECTOR Dashboard

Alarms Executables Computers More Server status

Top 10 Unresolved Threat and Warning Alarms

189

- 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 [AD103]...
- 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

262

- 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

Executable status

16682

- Ok (16623)
- Info (30)
- Warning (27)
- Threat (2)

Problematic Executables

EXECUTABLE (BY SHA-1) (78)	UNRESOLVED ALARMS (UNIQUE) *	UNRESOLVED ALARMS
exe.exe	7	9
epic.exe	5	38
ransim.exe	5	38
esl_demo.exe	4	36
executor.exe	3	25
estest.exe	2	19
64.0.1282.138_chrome_instaler...	2	2
setuphost.exe	2	3
googleupdate.exe	2	2
httpclienttester.exe	2	6
esl_demo.exe	2	2

НАГРАДЫ, ТЕСТЫ И КЕЙСЫ



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ОЦЕНКА ЗАЩИТЫ И БЫСТРОДЕЙСТВИЯ



Лидирующие позиции в рейтингах Virus Bulletin

Технологии ESET NOD32 завоевали больше наград VB100, чем программы любого другого вендора в области безопасности.



Лучшие результаты по защите почты от спама

Специалисты лаборатории Virus Bulletin говорят: «С того момента, как компания ESET начала принимать участие в тестах «VBSpam», ее программы постоянно занимали высокие позиции в рейтинге».



Антивирус неуязвим – самозащита на 100%

Антивирусное ПО ESET надежно защищает не только систему и данные от киберугроз, но и собственные модули от взлома. Это подтверждают результаты тестирования независимой лаборатории AV-Test.



Самые низкие показатели ложных срабатываний

По итогам исследований на количество ложных срабатываний компании AV-Comparatives продукты ESET признаны лучшими среди ведущих антивирусных решений.



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ПОТРЕБЛЕНИЕ СЕТЕВОГО ТРАФИКА В МОМЕНТ ПРОСТОЯ



НАМ ДОВЕРЯЮТ

ESET ОФИЦИАЛЬНЫЙ ЗАЩИТНИК GOOGLE CHROME

○○○

600mil.



chrome



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

НАМ ДОВЕРЯЮТ



SONY



Canon



re:Store



ВЫВОДЫ



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

РАССКАЖИТЕ ВСЕМ, ЧТО ПРОДУКТЫ ESET ДЛЯ БИЗНЕСА ЭТО:

- ✓ *Выгодное комплексное кроссплатформенное решение*
- ✓ *Защита **каждого узла** корпоративной сети*
- ✓ *Решение класса EDR – **ESET Enterprise Inspector***

СПАСИБО
ЗА ВНИМАНИЕ!



www.vkontakte.ru/nod32



www.facebook.com/ESETNOD32Russia



www.club.esetnod32.ru



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

