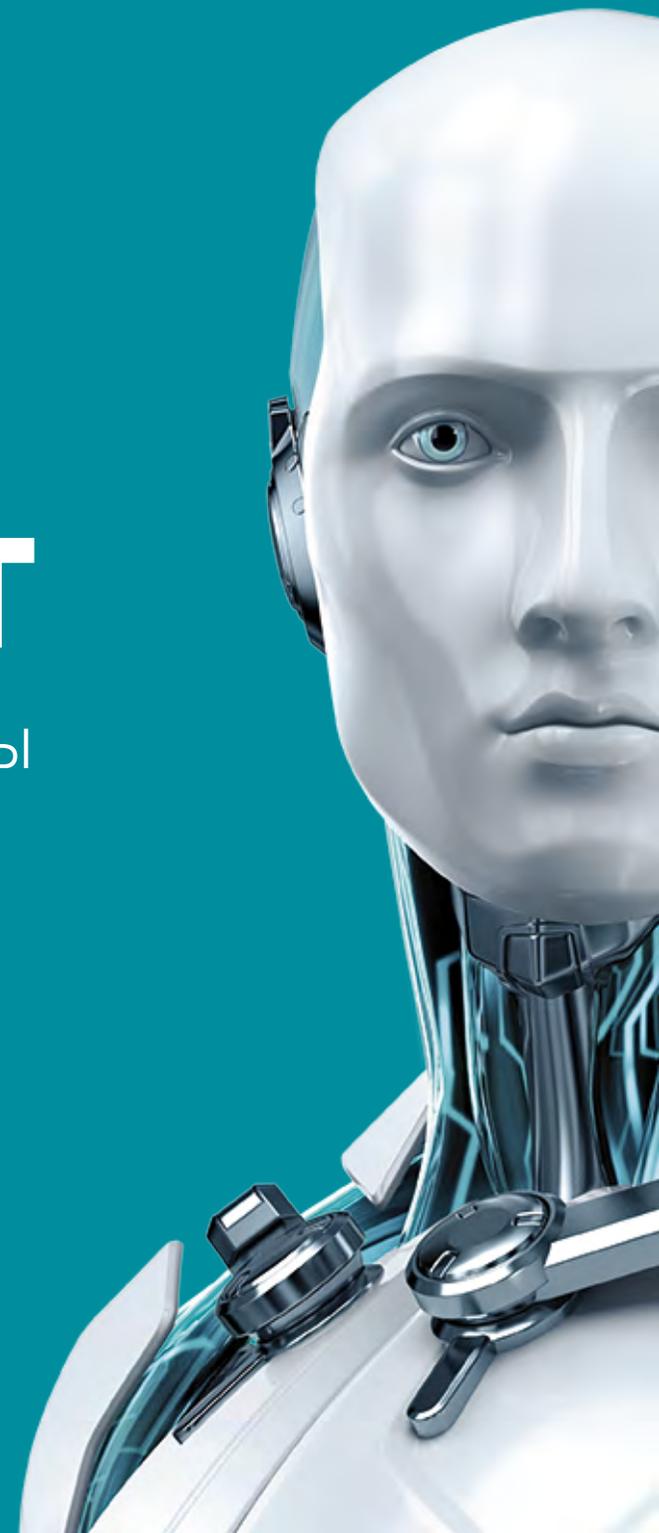


ТЕХНОЛОГИИ ESET

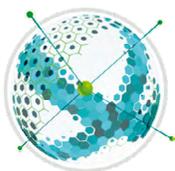
Эффективность многоуровневой защиты

 ИССЛЕДУЙ. ОТКРЫВАЙ. ОБЩАЙСЯ



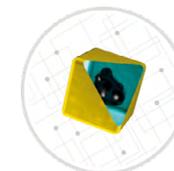
Защита от современных угроз, зачастую динамических и целенаправленных, требует многоуровневого подхода. Чем больше уровней защиты, тем меньше шансов у вредоносной программы заразить систему. Более 20 лет компания ESET внедряет проактивные и интеллектуальные технологии в свои решения. Благодаря усилиям исследовательских лабораторий ESET, мы продолжаем добавлять новые уровни защиты.

ТЕХНОЛОГИИ, СПОСОБНЫЕ ОБНАРУЖИТЬ УГРОЗУ ДО ЕЕ ВЫПОЛНЕНИЯ



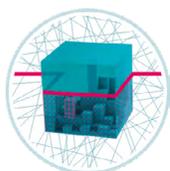
Защита от сетевых атак

Технология расширяет возможности файрвола и повышает эффективность обнаружения известных уязвимостей на сетевом уровне, для которых еще не выпущены патчи. Защита от сетевых атак позволяет оперативнее обнаруживать вредоносный трафик.



Песочница

Для определения реального поведения угрозы решения ESET используют изолированную среду – так называемую песочницу. С помощью этой технологии антивирус эмулирует различные компоненты работы системы для запуска подозрительного образца в изолированной виртуальной среде.



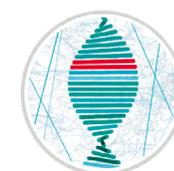
Сканер UEFI

Защищает от угроз, атакующих компьютер на более глубоком уровне – до запуска операционной системы Microsoft Windows на компьютерах с системным интерфейсом UEFI (среда предварительной загрузки). Он предназначен для контроля целостности прошивки и обнаружения попыток модификации.



Репутация и кэш

Перед сканированием наши продукты проверяют локальный кэш файла или URL-адреса на предмет связи с известными угрозами. Объект сравнивается с черными и белыми списками базы ESET. Далее из облачной системы ESET LiveGrid запрашивается информация о репутации объекта – был ли он ранее отмечен как подозрительный или классифицирован как вредоносный.



ДНК сигнатуры

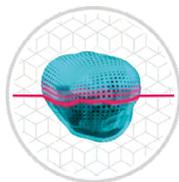
ДНК сигнатуры представляют собой совокупность характеристик вредоносного объекта и информации о его поведении. Если вредоносный код можно изменить или запутать, то поведение объекта не так просто модифицировать. Поэтому ДНК сигнатуры могут идентифицировать даже ранее неизвестные угрозы, которые содержат гены, указывающие на вредоносное поведение.

ТЕХНОЛОГИИ, СПОСОБНЫЕ ОБНАРУЖИТЬ УГРОЗУ ДАЖЕ ПОСЛЕ ЕЕ ЗАПУСКА



Облачная система защиты

Облачная система защиты построена на базе технологии ESET LiveGrid. Система отслеживает потенциальные, ранее неизвестные угрозы и передает их в облако ESET через систему обратной связи ESET LiveGrid для автоматической эмуляции в песочнице и анализа поведения.



Расширенное сканирование памяти

Расширенное сканирование памяти – новаторская технология, которая позволяет эффективно обезвреживать сложные зашифрованные вредоносные программы, попадающие на компьютер скрыто от пользователя. Функция контролирует поведение вредоносного процесса и сканирует его, как только он запускается в памяти.



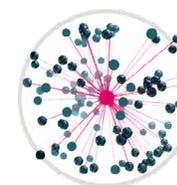
Защита от эксплойтов

Защита от эксплойтов контролирует часто эксплуатируемые приложения (веб-браузеры, PDF-редакторы, почтовые клиенты, приложения Microsoft Office, Flash, Java и т.д.). Модуль не только обращает внимание на определенные идентификаторы CVE, но и сосредотачивается на методах эксплуатации.



Защита от программ- вымогателей

Технология является дополнительным уровнем защиты от программ, блокирующих доступ или шифрующих данные пользователя и требующих выкуп за «освобождение» файлов. Защита от программ-вымогателей оценивает и контролирует все исполняемые приложения с помощью поведенческого анализа и репутационной эвристики.



Защита от ботнетов

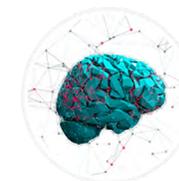
Защита от ботнетов помогает контролировать сетевую активность и находить вредоносные соединения, используемые бот-сетями. Функция блокирует каждое обнаруженное вредоносное соединение и сообщает о нем пользователю.

ТЕХНОЛОГИИ, АКТИВНЫЕ ВСЕГДА



Система предотвращения вторжений (HIPS)

Контролирует активность системы, используя набор predetermined правил для распознавания подозрительного поведения в системе. Когда подозрительная активность обнаружена, механизм самозащиты HIPS останавливает потенциально опасные действия нежелательной программы или процесса.



Машинное обучение

Компания ESET разработала собственный механизм машинного обучения, названный ESET Augur. Он использует совокупную силу нейронных сетей и группы из шести алгоритмов классификации. Технология машинного обучения позволяет правильно маркировать входящий образец как вредоносный или чистый.

ВЫСОКИЕ ОЦЕНКИ ТЕХНОЛОГИЙ ESET ОТ ЭКСПЕРТОВ БЕЗОПАСНОСТИ



ESET получает высшую награду Advanced+ в тестировании лаборатории AV-Comparatives на защиту в режиме реального времени.



ESET получает высшую награду Advanced+ в тестировании лаборатории AV-Comparatives на проактивную защиту.



Продукты ESET NOD32 участвуют в тестах независимой лаборатории Virus Bulletin с 2003 года. В конце 2016 года ESET стала первым вендором, завоевавшим сотую награду VB100.



ESET удерживает позицию лидера по обнаружению спама в тестах лаборатории Virus Bulletin.