ОБЗОР ПРОДУКТОВ

ЗАЩИТА МОБИЛЬНЫХ УСТРОЙСТВ

Многоуровневые технологии защиты, машинное обучение и опыт экспертов, представленные глобальным игроком рынка информационной безопасности.

АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

30 РАЗВИВАЕМ ТЕХНОЛОГИИ БЕЗОПАСНОСТИ УЖЕ 30 ЛЕТ

Что предлагает ESET для защиты мобильных устройств?

Продукты для защиты мобильных устройств можно разделить на две категории: безопасность и управление.

Функциональность для безопасности включает защиту от вредоносных программ и фишинга, проверку всех приложений, файлов и папок в режиме реального времени, ограничение доступа к незащищенным соединениям.

Решения для управления позволяют удалять конфиденциальную информацию на устройстве, ограничивать установку приложений, определять политики безопасности для пользователей и многое другое.

Отметим, что некоторые функции безопасности недоступны в мобильных устройствах на iOS и iPadOS, что связано с ограничениями Apple для сторонних разработчиков приложений.

Зачем нужна защита для мобильных устройств?

ПРОГРАММЫ-ВЫМОГАТЕЛИ

Программы-вымогатели – известная угроза для компьютеров и файловых серверов, но не стоит полагать, что мобильные устройства не страдают от этих атак. Еще в 2014 году мы обнаружили Simplocker – первый вымогатель для Android, шифрующий данные пользователя и требующий выкуп за восстановление доступа к файлам. Сегодня вирусописатели совершенствуют шифраторы для Android и методы заражения, а пострадавшие нередко вынуждены оплачивать выкуп, чтобы вернуть важную информацию из памяти устройств.

ESET Endpoint Security для Android своевременно распознает и блокирует атаки программ-вымогателей до того, как мобильному устройству будет нанесен ущерб. Проактивная защита необходима компаниям, чтобы сохранить работоспособность устройств и конфиденциальные данные в их памяти.

КРАЖА ИЛИ ПОТЕРЯ УСТРОЙСТВ

Многие компании перевели сотрудников на удаленный режим работы. При всех известных преимуществах это решение приносит новые риски – кражи или потери мобильных устройств, имеющих доступ к корпоративным ресурсам и конфиденциальные данные в памяти. Утечка этой информации может нанести ущерб деловой репутации компании.

ESET Endpoint Security для Android и ESET MDM для iOS & iPadOS предлагают организациям возможность контроля корпоративных устройств.
Если устройство потеряется или сотрудник покинет компанию, продукт ESET предотвратит утечку данных благодаря удаленной очистке памяти и блокировке устройства.

УПРАВЛЕНИЕ УСТРОЙСТВАМИ

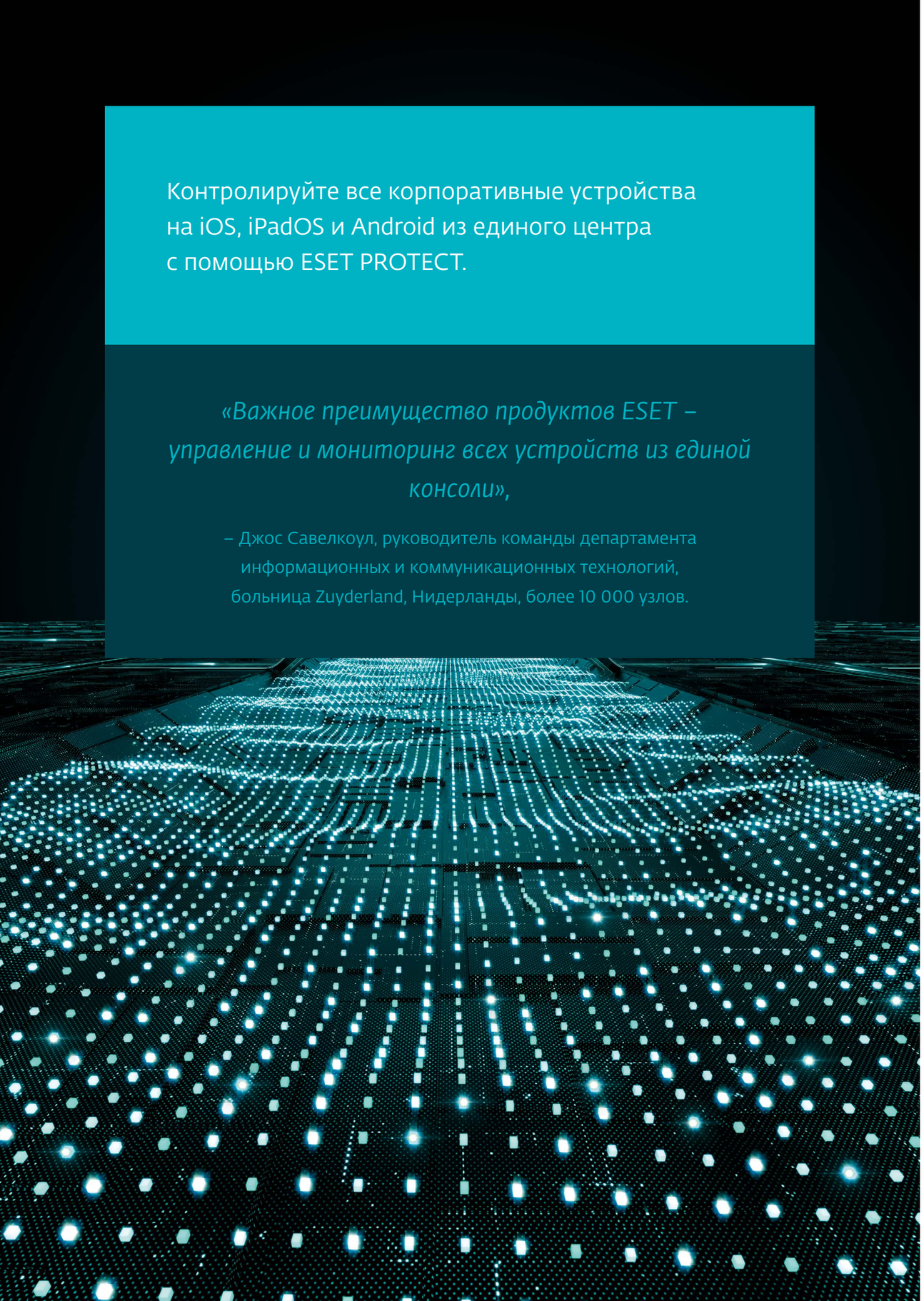
Выдавая сотрудникам корпоративные мобильные устройства, компании нередко запрещают их использование в личных целях, что связано с рисками безопасности и эффективности труда. Дополнительный повод для беспокойства – риски при подключении к общедоступным Wi-Fi сетям и использовании других функций.

Продукты ESET для мобильных платформ позволяют компаниям ограничить доступ сотрудников к небезопасным приложениям, вызовам, камере, Wi-Fi и Bluetooth. Администратор может настроить политики работы с устройствами, блокируя часть функций только в рабочее время.

Еще в 2014 году мы обнаружили Simplocker – первый шифратор для Android.

«Удаленка» приносит новые риски – кражи или потери мобильных устройств с рабочими документами и информацией, утечка которой может нанести ущерб деловой репутации компании.

Проактивная защита необходима компаниям, чтобы сохранить работоспособность мобильных устройств и конфиденциальные данные в их памяти.



Контролируйте все корпоративные устройства на iOS, iPadOS и Android из единого центра с помощью ESET PROTECT.

«Важное преимущество продуктов ESET – управление и мониторинг всех устройств из единой консоли»,

– Джос Савелкоул, руководитель команды департамента информационных и коммуникационных технологий, больница Zuyderland, Нидерланды, более 10 000 узлов.

Преимущества ESET

ЭФФЕКТИВНО И ЭКОНОМИЧНО

Контролируйте все корпоративные устройства на iOS, iPadOS и Android из единой консоли ESET PROTECT. Покупать дополнительные продукты для мобильной безопасности не потребуется.

ПРОВЕРЕННАЯ ЗАЩИТА

ESET уже более 30 лет работает в сфере информационной безопасности. Мы продолжаем развивать наши технологии, чтобы оставаться на шаг впереди самых новых угроз. Нам доверяют более 100 миллионов пользователей по всему миру.

МНОГОУРОВНЕВАЯ ЗАЩИТА

ESET сочетает многоуровневые технологии защиты, машинное обучение и опыт экспертов, чтобы предоставить клиентам наивысший уровень безопасности. Наши технологии непрерывно совершенствуются, сохраняя оптимальный баланс обнаружения угроз, производительности и отсутствия ложных срабатываний.

НЕПРЕРЫВНАЯ ПРОИЗВОДИТЕЛЬНОСТЬ

Распространенная проблема клиентов – влияние антивирусных решений на производительность мобильных устройств. Продукты ESET минимально влияют на производительность, что подтверждают тесты независимых лабораторий.

ОБЛАЧНАЯ СИСТЕМА ESET LIVEGRID

Каждый раз, когда обнаруживается угроза нулевого дня, например, программа-вымогатель, вредоносный файл отправляется в облачную систему защиты ESET LiveGrid. Угроза запускается в песочнице для контроля поведения. В течение нескольких минут результаты проверки будут отправлены на конечные точки по всему миру без каких-либо обновлений.

МИРОВОЕ ПРИСУТСТВИЕ

Наша компания представлена более чем в 200 странах. В мире действует 22 офиса и 13 центров исследований и разработки. Обширная география позволяет снабжать наших клиентов актуальной информацией обо всех последних тенденциях и угрозах независимо от страны или региона.

«Решения безопасности ESET защитили компанию Primoris и предупредили ИТ-департамент о многочисленных случаях серьезных атак и заражений, а самое главное – об атаках программ-вымогателей»,

— Джошуа Коллинз, менеджер центра обработки данных, корпорация Primoris Services, США, более 4 000 узлов.

Примеры использования

Программы-вымогатели

Программы-вымогатели – известная угроза как для компьютеров и файловых серверов, так и для мобильных устройств. Проактивная защита от подобных атак – необходимость для компаний.

РЕШЕНИЕ

- ✓ Установите ESET Endpoint Security для Android на корпоративных мобильных устройствах, чтобы обеспечить надежную защиту от любого типа вредоносных программ.
- ✓ Ограничьте установку приложений из неизвестных источников.

Утечки данных

Компании обеспокоены риском кражи или потери корпоративных устройств, а также возможностью утечки данных после увольнения сотрудника.

РЕШЕНИЕ

- ✓ Установите политики безопасности, включая шифрование мобильных устройств.
- ✓ Внедрите использование сложных паролей и PIN-кодов на всех устройствах.
- ✓ В случае необходимости удаленно заблокируйте устройство и удалите данные в его памяти.

Соответствие правилам безопасности

Политики безопасности использования мобильных устройств различаются в каждой компании, поэтому для администраторов сети важно убедиться, что настройки соответствуют всем требованиям.

РЕШЕНИЕ

- ✓ Определите список приложений, которые будут установлены на устройстве.
- ✓ Ограничьте доступ к незащищенным сетям Wi-Fi.
- ✓ Убедитесь, что функции защиты мобильных устройств включены.

ESET ENDPOINT SECURITY ДЛЯ ANDROID

ESET MDM ДЛЯ iOS & iPADOS

«Централизованное управление безопасностью на всех рабочих станциях, серверах и мобильных устройствах было для нас ключевым преимуществом»,

— IT-менеджер Diamantis Masoutis S.A., Греция, 6000 узлов.

Компании обеспокоены риском кражи или потери корпоративных устройств, а также возможностью утечки данных после увольнения сотрудника.

Технические особенности

Android/iOS/iPadOS

АНТИВОР

Удаленная блокировка учетной записи, очистка памяти, мониторинг местоположения. Отправка сообщения на потерянное устройство и настройка данных на заблокированном экране, упрощающая возврат смартфона пользователю.

КОНТРОЛЬ ПРИЛОЖЕНИЙ

Позволяет администратору сети контролировать установку приложений, блокировать доступ к ним, а также предлагать пользователю удалить конкретное приложение.

ПОЛИТИКА БЕЗОПАСНОСТИ

Большинство пользователей не сможет выбрать оптимальные настройки безопасности мобильного устройства. Поэтому ESET позволяет администратору задавать политики: сложность пароля, таймер блокировки экрана, шифрование и др.

КОНСОЛЬ УПРАВЛЕНИЯ

Продукты для мобильных устройств полностью управляются из единой консоли, которую можно установить на Windows или Linux.

Android

МНОГОУРОВНЕВАЯ ЗАЩИТА

Для обнаружения новых, ранее неизвестных угроз недостаточно одной технологии обнаружения. Поэтому все продукты ESET способны детектировать вредоносное ПО на разных этапах атаки – до, в ходе или после выполнения, не снижая при этом производительность мобильного устройства.

МАШИННОЕ ОБУЧЕНИЕ

Начиная с 1997 года во всех продуктах ESET используется машинное обучение в дополнение к остальным уровням защиты. Совокупная сила нейронных сетей и алгоритмов позволяет маркировать входящие образцы как чистые, потенциально нежелательные или вредоносные.

АНТИФИШИНГ

Предотвращает переход пользователей на потенциально опасные сайты, созданные для перехвата паролей, банковских реквизитов и другой конфиденциальной информации.

АУДИТ ПРИЛОЖЕНИЙ

Отслеживает приложения и их доступ к персональным данным и конфиденциальной информации компании, отсортированной по категориям.

iOS & iPadOS

APPLE IOS MANAGEMENT FRAMEWORK

Воспользуйтесь преимуществами Apple iOS Management Framework и контролируйте безопасность корпоративных iOS-устройств из единой консоли ESET PROTECT. Приобретать дополнительные продукты не придется.

УДАЛЕННАЯ НАСТРОЙКА УЧЕТНОЙ ЗАПИСИ

Задайте настройки Wi-Fi, VPN и Exchange.

УПРАВЛЕНИЕ МОБИЛЬНЫМИ УСТРОЙСТВАМИ

Если текущие настройки устройства не соответствуют корпоративным политикам безопасности, пользователь и администратор сети получат автоматические уведомления и варианты изменений.

Доступность функций зависит от системных ограничений Android/iOS/iPadOS и версии операционной системы.

Управление из единой консоли

ЦЕНТР АДМИНИСТРИРОВАНИЯ ESET PROTECT ОБЕСПЕЧИВАЕТ ПОЛНЫЙ ОБЗОР ПРОДУКТОВ БЕЗОПАСНОСТИ ESET В КОРПОРАТИВНОЙ СЕТИ.

О компании ESET

Более 30 лет компания ESET разрабатывает передовое программное обеспечение и сервисы в области информационной безопасности, обеспечивая комплексную защиту от киберугроз для компаний и домашних пользователей по всему миру.

ESET является частной компанией, не зависящей от государственных и политических решений. Компания обладает финансовой свободой и делает максимум для защиты всех клиентов.

ESET В ЦИФРАХ

110 млн пользователей по всему миру

400 тыс. корпоративных клиентов

200+ стран присутствия

13 центров исследований

НАШИ КЛИЕНТЫ

HONDA

С 2011 года под защитой ESET.
Лицензия продлевалась трижды и была расширена в два раза

GREENPEACE

С 2018 года под защитой ESET.
После продления лицензия расширена в 10 раз

Canon

С 2016 года под защитой ESET.
Более 14 000 рабочих станций

T

ISP-партнер по безопасности с 2008 года.
База клиентов – 2 миллиона

ESET соответствует требованиям международного стандарта в области менеджмента информационной безопасности ISO/IEC 27001:2013.

MITRE ATT&CK™

ESET активно участвует в проекте MITRE ATT&CK, пополняя глобальную базу знаний о тактиках и техниках кибератак, чтобы обеспечить лучшую защиту сообщества и своих пользователей.

НАШИ НАГРАДЫ

AV comparatives CERTIFIED ATP Enterprise DEC 2019

SE Labs AAA ENTERPRISE ENDPOINT PROTECTION JAN-MAR 2020

AV-TEST 2019 AWARD Best Usability ESET Endpoint Security

G2 Leader SPRING 2020

Gartner peerinsights customers' choice 2019

Canalys CYBERSECURITY CHAMPION 2019

ПРИЗНАНИЕ ЭКСПЕРТОВ

Gartner

ESET – единственный «Претендент» (Challenger) в рейтинге разработчиков платформ для защиты конечных точек Gartner.

FORRESTER®

ESET вошла в категорию сильнейших разработчиков (Strong Performers) по данным исследования The Forrester Wave™: Endpoint Security Suites.

The Radicati Group, Inc. A TECHNOLOGY MARKET RESEARCH FIRM

ESET названа лучшим игроком (Top Player) в рейтинге Radicati Endpoint Security, заслужив высшие оценки функциональности и стратегического видения.

АНТИВИРУСНАЯ ЗАЩИТА
БИЗНЕС-КЛАССА