Apple для работы

Безопасность платформы

Безопасность — в основе всего.

Apple уделяет максимум внимания безопасности — как безопасности пользователей, так и защите корпоративных данных. При разработке всех наших продуктов мы встраиваем в них продвинутые средства безопасности. Безопасность лежит в основе этих устройств. Это сочетается с невероятным удобством их использования, поэтому с ними можно работать так, как вам нравится. Только Apple применяет такой комплексный подход к обеспечению безопасности, поскольку мы разрабатываем и оборудование, и программное обеспечение, и сервисы.

Безопасность аппаратного обеспечения
Программное обеспечение не может быть безопасным без надёжного фундамента, предоставляемого аппаратным обеспечением. Вот почему устройства Apple под управлением iOS, iPadOS, macOS, tvOS и watchOS оснащены средствами безопасности на уровне процессора.

В их числе — специальные функции центрального процессора, обеспечивающие работу средств безопасности системы, и выделенный сопроцессор, который отвечает только за безопасность. Самым важным компонентом является сопроцессор Secure Enclave, которым оснащаются современные устройства iOS, iPadOS, watchOS и tvOS, а также все компьютеры Mac с чипом безопасности Apple T2. Secure Enclave предоставляет основу для шифрования хранящихся на устройстве данных, безопасной загрузки в macOS и работы биометрических систем.

Все современные iPhone и iPad, а также компьютеры Mac с чипом T2 имеют выделенный аппаратный модуль AES, который обеспечивает шифрование на скорости записи и чтения файлов. Благодаря этому функция защиты данных и технология FileVault защищают файлы пользователей, не раскрывая долговременные ключи шифрования центральному процессору или операционной системе.

Безопасная загрузка устройств Apple гарантирует, что программное обеспечение самых базовых уровней не является поддельным и что при запуске загружается только доверенное программное обеспечение операционной системы, разработанное Apple. На устройствах iOS и iPadOS в основе безопасной загрузки лежит постоянный код загрузочного ПЗУ, который закладывается в процессе изготовления микросхемы и называется аппаратным корнем доверия. На компьютерах Mac с чипом T2 цепочка доверия безопасной загрузки начинается с самого Secure Enclave.

Secure Enclave обеспечивает безопасную аутентификацию и сохранение конфиденциальности биометрических данных при использовании Touch ID и Face ID в устройствах Apple. Пользователи могут с лёгкостью использовать более длинные и сложные пароли и код-пароли для повышения безопасности, при этом во многих случаях аутентификация выполняется практически мгновенно.

Функции безопасности в устройствах Apple основаны на уникальном сочетании возможностей процессора, оборудования, программного обеспечения и сервисов, которые предлагает только Apple.

Безопасность системы
Средства безопасности системы дополняют уникальные возможности оборудования Apple, обеспечивая максимальную безопасность операционных систем на устройствах Apple без ущерба для удобства пользователей. Средства безопасности системы охватывают процесс загрузки, обновление программного обеспечения и текущую работу операционной системы.

В основе безопасной загрузки лежит аппаратное обеспечение, с которого начинается цепочка доверия, объединяющая все модули программного обеспечения. Прежде чем передать управление следующему звену, каждое звено убеждается в том, что следующее звено функционирует должным образом. Эта модель безопасности поддерживает не только стандартную загрузку устройств Apple, но и различные режимы восстановления и обновления на устройствах iOS, iPadOS и macOS.

Самые новые версии iOS, iPadOS и macOS являются самыми безопасными. Механизм обновления программного обеспечения не только следит за своевременным обновлением устройств Apple, но и гарантирует, что будет установлено только доверенное программное обеспечение Apple. Система обновления также предотвращает атаки через понижение версии, так что злоумышленник не может откатить устройство до более ранней версии операционной системы для кражи пользовательских данных.

Наконец, устройства Apple оснащены средствами защиты на этапах загрузки и выполнения, которые обеспечивают их целостность в процессе текущей работы. Поскольку устройства iOS, iPadOS и macOS имеют очень разные наборы возможностей и поэтому могут столкнуться с разными видами атак, их средства защиты значительно отличаются друг от друга.

Для достижения этого уровня защиты в iOS и iPadOS используются такие функции, как защита целостности ядра, защита целостности системного сопроцессора, коды аутентификации указателя и защита на уровне страниц. В macOS же должный уровень защиты обеспечивается за счёт безопасности

унифицированного расширяемого интерфейса прошивки (UEFI), режима управления системой, средств защиты прямого доступа к памяти и безопасности прошивки периферийных устройств.

Шифрование и защита данных
Устройства Apple оснащены функциями шифрования, которые защищают данные пользователя и позволяют выполнить удалённое стирание в случае потери или кражи устройства.

Безопасная последовательность загрузки, а также функции обеспечения безопасности системы и приложений помогают следить за тем, чтобы на устройстве запускались только надёжные приложения и фрагменты кода. В устройствах Apple также реализованы дополнительные функции шифрования для защиты данных пользователей даже в случае компрометации других частей системы безопасности (например, в случае пропажи устройства или запуска ненадёжного кода). Все эти функции имеют большое значение для пользователей и ИТ-администраторов, поскольку они обеспечивают постоянную защиту личной и корпоративной информации, а также предоставляют средства для мгновенного и полного удалённого стирания в случае потери или кражи устройства.

На устройствах iOS и iPadOS используется технология шифрования данных, также именуемая технологией защиты данных, а для защиты данных на компьютерах Mac используется технология шифрования томов под названием FileVault. Основой иерархии ключей в обеих моделях является специализированный процессор Secure Enclave (на устройствах, оснащённых процессором Secure Enclave). Кроме того, в обеих моделях используется выделенный модуль AES, который поддерживает шифрование на полной скорости и избавляет от необходимости предоставлять ключи шифрования ядру операционной системы или центральному процессору (где они могут быть скомпрометированы).

Безопасность приложений

Приложения являются одним из самых важных элементов современной архитектуры безопасности. Приложения значительно повышают продуктивность работы пользователей, однако, если не принять должных мер, могут негативно сказываться на безопасности системы, её стабильности и пользовательских данных. Apple реализует многоуровневую систему защиты для гарантии того, что приложения не содержат известного вредоносного программного обеспечения и не были подделаны. Дополнительные средства защиты обеспечивают тщательный контроль доступа приложений к пользовательским данным, выступая в качестве посредника.

Встроенные средства безопасности обеспечивают стабильную и надёжную платформу для приложений, что позволяет тысячам разработчиков создавать сотни тысяч приложений для iOS, iPadOS и macOS без нарушения целостности системы. А пользователи, получающие доступ к этим приложениям со своих устройств Apple, могут дополнительно защитить себя от вирусов, вредоносного кода и атак злоумышленников с помощью настроек.

Для обеспечения самого жёсткого контроля все приложения на iPhone, iPad и iPod touch могут быть получены только из App Store — и каждое работает в своей изолированной среде. Многие приложения на Mac доступны через App Store, однако пользователи Mac также загружают и используют приложения из интернета. Для безопасной загрузки из интернета в macOS предусмотрены дополнительные уровни защиты. Прежде всего, по умолчанию в macOS 10.15 и новее для запуска на Mac все приложения должны быть нотаризованы компанией Apple. Благодаря этому требованию гарантируется, что приложения не содержат известного вредоносного программного обеспечения, а разработчики получают возможность распространять такие приложения не только через App Store. Кроме того, macOS включает стандартные средства защиты от вирусов, которые предназначены для блокирования и, при необходимости, удаления вредоносного ПО.

Механизм песочниц, применяемый на всех платформах, помогает дополнительно защитить пользовательские данные от несанкционированного доступа со стороны приложений. В macOS критически важные данные сами по себе находятся в изолированной среде, так что пользователи полностью контролируют доступ к файлам на рабочем столе, в папках «Документы», «Загрузки» и других важных областях. Без согласия пользователя эти данные не доступны ни одному приложению, независимо от того, помещено оно в песочницу или нет.

Безопасность сервисов

Apple предлагает широкий набор сервисов для повышения практичности и эффективности устройств. К ним относятся Apple ID, iCloud, Вход с Apple, Apple Pay, iMessage, FaceTime, Siri и Локатор. Эти сервисы предоставляют широкие возможности для облачного хранения, синхронизации, аутентификации, оплаты, обмена сообщениями, связи и других задач, при этом обеспечивая конфиденциальность пользователей и защиту их данных.

Узнайте больше о безопасности устройств Apple.

apple.com/ru/business/it

apple.com/ru/macos/security

apple.com/ru/privacy/features

apple.com/security

Экосистема партнёров

Устройства Apple поддерживают распространённые корпоративные инструменты и службы безопасности, обеспечивая соответствие устройств и хранящихся на них данных нормативным требованиям. Каждая платформа поддерживает стандартные протоколы VPN и протоколы безопасности Wi-Fi для защиты сетевого трафика и безопасного подключения к общей корпоративной инфраструктуре.

Благодаря партнёрству с корпорацией Cisco совместное использование продуктов Apple и Cisco обеспечивает повышенную безопасность и производительность. Сети Cisco предоставляют приоритет бизнес-приложениям и обеспечивают дополнительную защиту за счёт Cisco Security Connector.