Яндекс Браузер | для организаций |

Браузер для Zero Trust

Zero Trust Access (доступ с нулевым доверием) — это концепция, предполагающая «адаптивный» подход к информационной безопасности, который учитывает изменения ландшафта рисков для защищаемого периметра.

В основе концепции — тотальное «недоверие» к любому пользователю или устройству сети, которое выражается в использовании многофакторной аутентификации, практике предоставления доступа на основе политик и регулярной проверке прав доступа пользователя к конкретному ресурсу.

В современных условиях постоянно эволюционирующих киберугроз концепция нулевого доверия обладает рядом выгодных качеств в сравнении с классической моделью безопасности.

Отличия Zero Trust от классической модели безопасности

Классическая модель	Zero Trust
• Базируется на предположении, что все пользователи и устройства внутри сети заслуживают доверия.	• Не доверяет пользователям и устройствам, вне зависимости от того, находятся они внутри сети или вне её; • Каждое действие или доступ верифицируется, даже если пользователь или устройство внутри сети.
• Предполагает защиту периметра, использует защиту от внешних вторжений (файерволы, системы предотвращения вторжений и т.д.).	• Разбивает сеть на микросегменты, защищает не периметр, а каждый конкретный ресурс внутри сети; • Пользователям предоставляется минимальный необходимый набор прав.
• Опирается на статическую аутентификацию (логин и пароль); • Может предоставлять доступ на основе роли пользователя или группы, в которой он состоит.	• Опирается на многофакторную аутентификацию; • Опирается на контекст (например, состояние устройства, местоположение пользователя, его поведение и тд.).

Главное концептуальное отличие безопасности на базе Zero Trust от классической модели заключается в том, что в Zero Trust пользователю предоставляется доступ только к той информации, которая ему нужна для работы и лишь на то время, на которое она ему нужна, в то время как в классической модели успешно аутентифицированные пользователи имеют более обширный доступ.

Модель Zero Trust приобрела актуальность в связи с развитием вредоносных техник, которые позволяют атакующим действовать не только извне, но и внутри атакованной сети. Например, одна из распространённых тактик злоумышленников заключается в получении доступа к учётным данным легитимного пользователя атакуемой сети, вход в сеть с использованием этих данных и последующее развитие атаки через вредоносные действия от имени скомпрометированного пользователя.

Классическая модель безопасности не учитывает «нетипичность» действия пользователя (поскольку он сообщил верный пароль и имеет нужные права), а модель на базе «нулевого доверия» реализацию той же тактики существенно затрудняет: требует дополнительный фактор для аутентификации, разрешает пользователю доступ в строгом соответствии с действующими политиками безопасности и динамическими условиями. Ими могут быть географическое положение пользователя, состояние устройства с которого осуществляется доступ в сеть, и др. Если устройство не соответствует установленным требованиям или его состояние изменилось после аутентификации в сети, доступ к ресурсу может быть заблокирован. Кроме того, модель Zero Trust предполагает постоянный мониторинг и анализ событий в сети.

Роль корпоративного браузера в модели Zero Trust

Одним из основных недостатков модели Zero Trust является её сложность. Подобное решение должно содержать инструменты для постоянного контроля множества приложений и пользователей. Оно должно уметь проверять и перепроверять актуальность прав пользователя на те или иные действия, а также уметь распознавать аномалии в поведении пользователей или приложений. Решение этих задач требует инвестиций в дополнительное ПО и IT-персонал.

Вместе с тем, всё больше часто используемых приложений мигрируют в веб. По разным оценкам, сегодня сотрудники организаций от 50% до 70% рабочего времени проводят в браузере. То есть большинство задач, которые раньше решались с помощью различных нативных приложений, теперь решаются через их веб-аналоги, для доступа к которым нужен только браузер. В этом контексте корпоративный браузер с развитыми функциями безопасности и управления значительно упрощает внедрение сценариев Zero Trust в корпоративную инфраструктуру, ведь вместо множества различных приложений, сотрудникам ИБ нужно уметь контролировать и защищать одно.

Функции Яндекс Браузера для организаций, подходящие для Zero Trust

Яндекс Браузер для организаций обладает функциями, позволяющими IT-службам реализовать сценарии Zero Trust в корпоративной инфраструктуре.

Политики разграничения доступа к веб-ресурсам

Яндекс Браузер для организаций поддерживает сотни политик безопасности, которые в том числе позволяют чётко разграничить, какие сотрудники к каким корпоративным ресурсам имеют доступ.
Для сотрудников из разных отделов можно создать профили, наделённые различными правами доступа в соответствии с рабочими обязанностями.

Защита от обхода контура безопасности

С помощью функции защиты от обхода контура безопасности IT-администраторы могут настроить инфраструктуру и Браузер так, чтобы доступ к корпоративным ресурсам был возможен только из Яндекс Браузера для организаций. Таким образом можно исключить возможность доступа к чувствительной информации из неконтролируемых IT-службой браузеров.

Двухфакторная аутентификация, управление авторизацией и пин-код

Сервис Яндекс ID поддерживает несколько способов мультифакторной аутентификации, а функция управления авторизацией позволит убедиться, что сотрудник авторизован в Браузере под корпоративным аккаунтом организации, а не под личным аккаунтом или аккаунтом другой организации. Функция ПИН-кода обеспечит защиту от несанкционированного физического доступа к браузеру сотрудника.

Защита от утечки данных

В Яндекс Браузере для организаций реализованы технологии защиты от утечки данных, которые позволяют тонко настроить, как и где может быть обработана конфиденциальная информация. Например, можно ограничить копирование данных в буфер обмена, использование функций захвата изображений и звука, загрузки файлов в память устройства, на внешние веб-ресурсы и т.д. В частности, функция «Цифровые водяные знаки» затруднит копирование данных с помощью сторонних записывающих изображение устройств (фото и видеокамер), а функция «Безопасное хранилище» позволит строго ограничить список устройств, на котором конфиденциальная информация будет доступна в читаемом виде.

Проверка безопасности устройств

Функция проверки безопасности устройств позволяет IT-службе провести инвентаризацию корпоративного парка устройств и обеспечить условный доступ к корпоративной инфраструктуре. Например, если на устройстве включено шифрование диска, ПИН-код и работает обновлённый до последней версии антивирус, то доступ к корпоративному ресурсу разрешён. Если же одно или несколько условий не выполнено (или перестаёт выполняться после авторизации на защищаемом ресурсе), то доступ может быть заблокирован.

Удаленная изоляция браузера

Функция удалённой изоляции браузера обеспечивает надёжную защиту критически важных корпоративных ресурсов и пользователей от любых вредоносных атак, включая атаки с помощью уязвимостей нулевого дня. В режиме удалённой изоляции сам Браузер запускается в изолированном виртуальном контейнере на сервере, а на пользовательское устройство транслируется видеопоток. В результате, даже если пользователь откроет веб-страницу с эксплойтом или случайно загрузит через Браузер файл с вредоносной программой, опасный код не покинет пределы виртуального контейнера и не навредит IT-инфраструктуре организации.

Интеграция с SIEM

Браузер способен передавать информацию о событиях безопасности в системы управления информационной безопасностью и событиями безопасности (Security Information and Event Management, SIEM), включая информацию о веб-навигации, срабатывании функций защиты от вредоносных файлов, вредоносных веб-страниц и функций защиты от утечек. Кроме того, в SIEM могут транслироваться события о состоянии безопасности устройств. Всё это позволяет службе информационной безопасности осуществлять мониторинг корпоративной сети, распознавать аномалии и вовремя реагировать на потенциальные инциденты безопасности.

Функции Яндекс Браузера для организаций на примере основных сценариев Zero Trust

Функциональность Яндекс Браузера для организаций позволяет частично или полностью реализовать основные сценарии Zero Trust в коропративной IT-инфраструктуре, где ключевые защищаемые ресурсы расположены на веб-серверах.

Классический сценарий с произвольным браузером	Zero Trust с Яндекс Браузером для организаций
Аутентификация и идентификация пользователя	
• Вход по доменным логину и паролю.	• Мультифакторная аутентификация Яндекс ID повысит вероятность верной идентификации пользователя; • Управление авторизацией исключит аутентификацию под некорпоративными учётными данными; • ПИН-код ограничит третьим лицам физический доступ к Браузеру; • Защита от обхода контура безопасности предотвратит использование альтернативных браузеров; • Доступ будет предоставлен или не предоставлен на основе данных от функции «Проверка безопасности устройств».
Предоставление доступа к ресурсам с конфиденциальной информацией и обеспечение исполнения политик безопасности	
• Безусловное доверие к прошедшим аутентификацию пользователям; • Предоставление доступа на основе прав группы, к которой принадлежит пользователь; • Возможные способы обработки информации не ограничены (можно скачивать, копировать, модифицировать); • Защита от утечек и киберугроз обеспечивается отдельными решениями внутри периметра и не всегда покрывает все используемые платформы.	• Микросегментация прав доступа с помощью политик безопасности (пользователям одной и той же группы можно назначит разный уровень доступа к одной и той же информации); • Управление доступными способами обработки конфиденциальной информацией в зависимости от уровня доступа (например: можно просматривать, но нельзя скачивать; можно скачать и редактировать, но невозможно скопировать или переслать в читаемом виде); • Удалённая изоляция веб-сессий для доступа к критическим сегментам сети или для пользователей с критическим уровнем прав; • Защита от утечек и киберугроз обеспечивается на границе сервиса или ресурса, в котором хранится конфиденциальная информация.
Постоянный мониторинг и обнаружение аномалий	
• Служба ИБ не видит события в браузере. Атаки на браузер и атаки, в которых браузер служил звеном, не обнаруживаются или обнаруживаются на более поздних стадиях; • Состояние устройств, на которых работает браузер, может не контролироваться.	• Служба ИБ получает информацию об активности в Браузере в реальном времени и имеет возможность вовремя распознавать начинающуюся атаку, например, через вредоносные расширения или фишинг; • Есть возможность автоматизировать реакцию на инцидент через SOAR/IRP-системы; • Состояние устройств, на которых работает Браузер, регулярно переоценивается. Права доступа отзываются или сохраняются на основе результатов оценки.

Используя функции Яндекс Браузера для организаций, компании, которые имеют большое количество географически распределённых филиалов, удалённых сотрудников и распределённую IT-инфраструктуру, могут надёжно защититься от кибератак и предотвратить возможные утечки конфиденциальных данных.

Яндекс Браузер | для организаций |

Наш сайт: browser.yandex.ru/corp

Telegram · Дзен · YouTube · ВК Видео

Связаться с нами: