Яндекс Браузер | для организаций

Браузер для безопасности по модели SASE

Что такое SASE

В последние годы в мире корпоративных IT произошло несколько важных изменений в области использования приложений, сервисов и сетей. В частности, всё больше сотрудников работают вне офиса и всё большее их количество используют облачные сервисы, развёрнутые вне центров обработки данных, подконтрольных корпоративной службе информационной безопасности.

Одновременно растёт количество конфиденциальных данных, которые хранятся и обрабатываются не в собственном ЦОД (центре обработке данных) организации, а во внешнем облаке. Трафик из многочисленных филиалов организаций направляется не напрямую в её ЦОД, а в сторонний облачный сервис.

Интерес организаций к публичным облакам возникает, поскольку такие инфраструктуры могут быть более выгодной альтернативой IT-инфраструктуре, построенной самостоятельно. В результате IT-инфраструктура корпораций перестаёт быть централизованной, её периметр размывается и дробится.

Обратной стороной этих изменений является существенное усложнение задачи по защите конфиденциальных данных, которые теперь передаются, обрабатываются и хранятся в окружении, которое лишь частично контролируется корпоративной ИБ-службой.

SASE — это модель сетевой безопасности, которая обеспечивает быстрый и безопасный доступ к сетям и облачным приложениям в IT-инфраструктурах организаций с большим количеством филиалов и гибридным форматом работы.

Отличия SASE от традиционных моделей безопасности:

SASE	Традиционные модели безопасности
Объединяет функции безопасности и сетевые функции в одном решении. Существует в виде облачного сервиса, что упрощает масштабирование и управление.	Для безопасности и управления трафиком используются отдельные решения, которые нередко трудно интегрируются друг с другом. Обычно требуют отдельных устройств и инфраструктуры, что усложняет доступ к корпоративным ресурсам и увеличивает расходы на оборудование, ПО, их настройку и поддержку.
Использует принцип нулевого доверия (Zero Trusted Network Access), который обеспечивает доступ к данным только идентифицированным и верифицированным пользователям.	Доступ к данным предоставляется всем пользователям внутри защищаемого периметра.
Предоставляет инструменты централизованного управления и мониторинга.	Часто требуют наличия нескольких отдельных решений, что делает процесс администрирования громоздким.

SASE оптимизирует и упрощает управление передачей, обработкой и хранением корпоративных данных в распределённых IT-инфраструктурах. Эта модель предоставляет все необходимые инструменты для защиты в едином решении, в то время как традиционные модели требуют отдельных наборов оборудования и ПО для каждого филиала организации. Традиционные модели фрагментированы: они предполагают создание периметров безопасности в каждом отдельном филиале организации и при этом безусловно доверяют любому пользователю внутри этих периметров. SASE создаёт периметр безопасности там, где находятся защищаемые данные, а доступ предоставляется только тем пользователям, кто прошёл идентификацию и верификацию, — вне зависимости от того, в какой сети они находятся.

Ключевыми компонентами безопасности, организованной по модели SASE, являются:

- SD-WAN — решения, обеспечивающее централизованное программное управление корпоративными сетями вне зависимости от используемого в филиалах телекоммуникационного оборудования;
- Решения для защиты веб-трафика (Secure Web Gateway (SWG), облачный Firewall);
- Решения для управления доступом к облачным приложениям (Cloud Access Security Broker, CASB);
- Решения для управления сетевым доступом к приложениям на основе «нулевого доверия» (Zero Trust Network Access, ZTNA).

SASE может обеспечивать более удобное управление данными и их надёжную защиту в организациях:

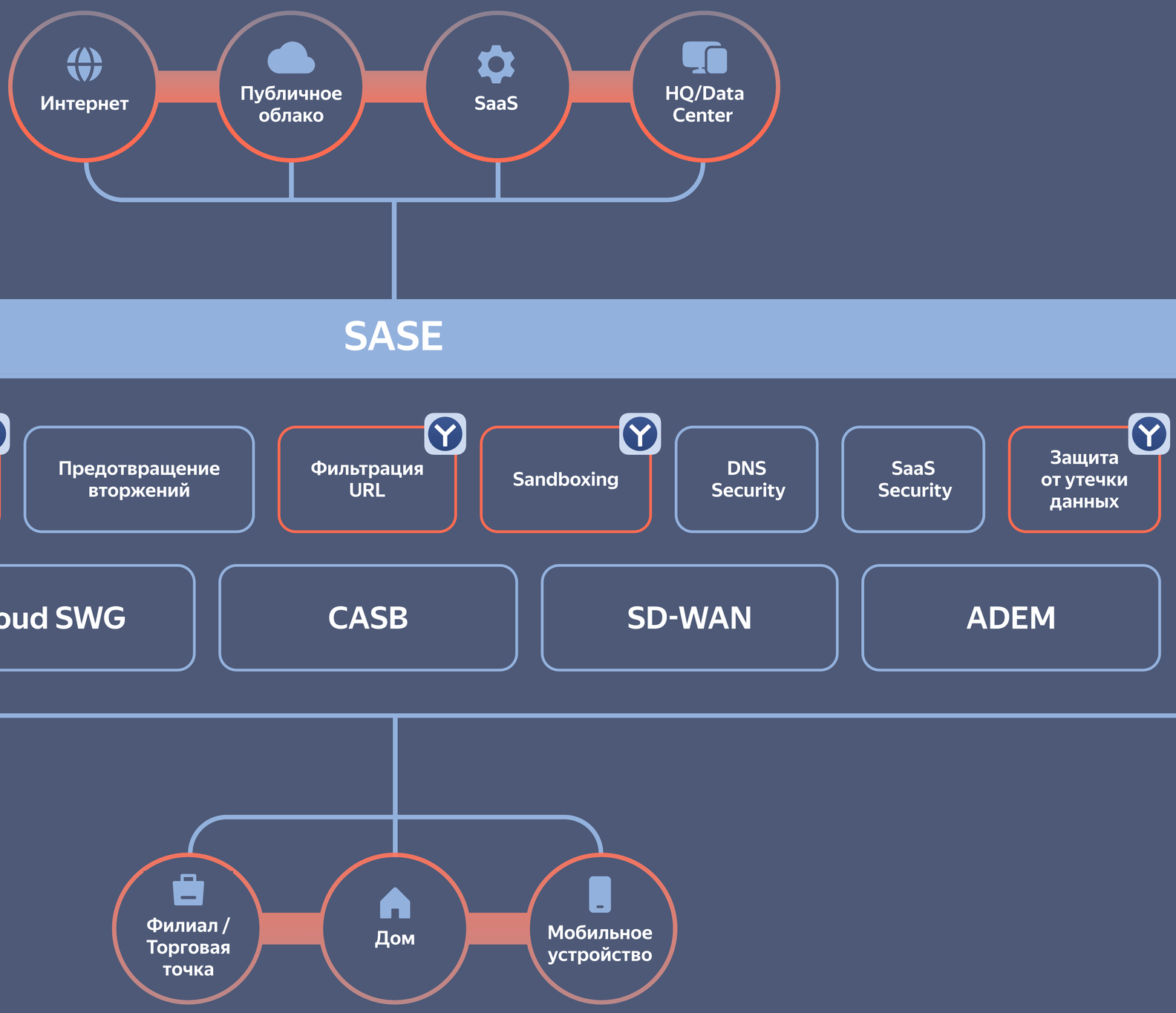
- С большим числом географически распределённых филиалов, мобильных и работающих в гибридном формате сотрудников;
- С большим числом облачных приложений, используемых для обработки конфиденциальных данных.

Почему Яндекс Браузер подходит для SASE

Важной тенденцией в корпоративных IT является активная миграция приложений в веб, в результате которой, по оценкам экспертов, около 70% рабочего времени сотрудники проводят в браузере. В этих условиях браузер становится одним из наиболее часто используемых приложений в корпоративной IT-инфраструктуре, а следовательно — и ключевым приложением, через которое происходит обмен конфиденциальной информацией и доступ к корпоративным веб-ресурсам. Другими словами, браузер становится неотъемлемым компонентом SASE-инфраструктуры.

Яндекс Браузер для организаций обладает перечнем необходимых функций, позволяющих реализовать безопасный и контролируемый доступ к корпоративной информации с любого устройства из любой сети.

Роль Яндекс Браузера для организаций в модели SASE



Защищенный корпоративный браузер

Яндекс Браузер для организаций обладает встроенной защитой от вредоносного кода (включая вредоносные расширения), фишинга и других распространённых киберугроз, а кроме того, в нём есть функция контроля собственной целостности, которая помогает выявить случаи несанкционированной модификации компонентов Браузера.

Защита от утечки данных

Яндекс Браузер для организаций позволяет строго управлять тем, к каким корпоративным данным у сотрудников есть доступ, а также тем, что с этим данными можно делать. В частности, можно ограничивать копирование данных, их сохранение в неавторизованных окружениях, выгрузку на внешние ресурсы и копирование с помощью внешних видео и фотокамер (технология цифровых водяных знаков).

Удалённая изоляция браузера

Сервис удалённой изоляции на базе Браузера позволяет организовать защищённый доступ как во внешний интернет, так и к внутренним ресурсам — извне, изолируя веб-сессии в контейнере на удалённом сервере, а на устройство пользователя транслируя лишь видеопоток.

Поскольку на устройстве сотрудника не выполняется никакой загруженный из сети код, технология защищает даже от атак через уязвимости нулевого дня — одного из самых сложных и трудно обнаруживаемых типов вредоносных атак.

Защищённое хранилище

Функция позволяет задать список веб-ресурсов (например, адреса корпоративных облачных хранилищ), файлы с которых Браузер будет скачивать в зашифрованном виде.

После скачивания такой файл можно будет открыть или отредактировать только в Браузере и только на том устройстве, на которое файл скачали.

При копировании, пересылке через почту или мессенджер, при загрузке в публичное облако файл останется зашифрованным, а значит, и недоступным для посторонних глаз.

Фильтрация URL

С помощью групповых политик Браузера можно точно определить список веб-адресов, к которым может или не может подключаться сотрудник. Кроме того, часть адресов можно настроить так, чтобы для определённых сотрудников (например, для топ-менеджмента или администраторов доменов) они открывались только в режиме удалённой изоляции браузера. Так сокращается поверхность атаки, и пользователи Браузера в модели SASE получают дополнительную защиту от угроз, которые могли быть не замечены используемыми в инфраструктуре решениями для защиты веб-трафика.

Доступ по принципу «нулевого доверия»

В Яндекс Браузере для организаций реализовано несколько технологий, позволяющих обеспечить идентификацию пользователя и доступ к корпоративным данным только из доверенных окружений. В частности, функция защиты от обхода политик безопасности позволяет настроить инфраструктуру так, чтобы корпоративные ресурсы могли принимать запросы только от Яндекс Браузера для организаций, а запросы от остальных браузеров — отклонялись. Дополнительно, функция фильтрации учётных записей, под которыми можно осуществлять вход в Браузер, защитит от ситуаций, когда сотрудники случайно или намеренно логинятся под личным Яндекс ID или корпоративным Яндекс ID, которой нет в списке одобренных.

Функция защиты экрана ПИН-кодом предотвращает несанкционированный физический доступ к Браузеру со стороны третьих лиц.

Функция «Доверенные устройства» (ранее «Аттестация устройств») позволяет настроить Браузер так, чтобы доступ к корпоративным ресурсам был возможен только, если устройство, с которого подключается сотрудник, соответствует набору предопределённых правил и политик: имеет нужный серийный номер, нужную версию ОС и Браузера, защищено паролем, антивирусным ПО и т.д. Проверка производится регулярно, и если рабочая среда сотрудника изменится в неудовлетворительную сторону, Браузер может заблокировать доступ к защищаемым ресурсам.

В совокупности с другими технологиями, такими как удалённая изоляция браузера и защита от утечек, эти функции позволяют создать условия близкие к принципу «нулевого доверия», и обеспечить тем самым безопасный доступ к корпоративным данным вне зависимости от того, находится сотрудник в доверенной корпоративной сети или вне её.

А ещё с помощью «Доверенных устройств» ИБ-служба компании может проводить регулярную инвентаризацию устройств корпоративного парка. Функцию можно настроить так, чтобы данные о рабочей среде сотрудника транслировались в системы ИБ-мониторинга, используемые в организации (например, в SIEM). Это позволит всегда точно знать общее состояние парка с точки зрения безопасности и вовремя принимать необходимые меры.

Мультиплатформенность Яндекс Браузера

Важным условием, необходимым для построения IT-инфраструктуры по модели SASE, является возможность безопасного доступа к корпоративным данным не только из разных сетей, но и с различных устройств. В традиционных моделях безопасности эти задачи решаются с помощью VPN, а также решений для виртуализации рабочих столов (VDI, Desktop-as-a-Service). Яндекс Браузер для организаций доступен на всех распространённых ОС: на Windows, Linux, MacOS, Android и iOS. Все ключевые функции безопасности и управления, позволяющие обеспечивать контролируемый и защищённый доступ к корпоративным данным, присутствуют в версиях Браузера для каждой платформы.

Яндекс Браузер для организаций обладает необходимыми инструментами для роли безопасного корпоративного браузера в IT-инфраструктурах, построенных по модели SASE (Secure Access Service Edge).

Яндекс Браузер | для организаций |

Наш сайт: browser.yandex.ru/corp

Telegram
Дзен
YouTube
ВК Видео

Связаться с нами: