Яндекс Браузер | для организаций

Яндекс Браузер для организаций: Безопасный доступ в ИТ-инфраструктуру для подрядчиков

Преимущества и риски сотрудничества с подрядчиками

Пользоваться услугами подрядчиков удобно и часто более выгодно, чем нанимать постоянный штат. Прибегая к услугам внешних контрагентов, организации оптимизируют расходы на персонал, компенсируют дефицит кадров и недостаток экспертизы нужного уровня в отдельных направлениях. Более половины компаний пользуются услугами аутсорсеров в области бухгалтерии и финансов, юриспруденции, ИТ-поддержки и др.

При этом во многих отраслях работа с подрядчиками часто предполагает необходимость предоставления доступа внешних агентов в корпоративную ИТ-инфраструктуру: к внутренним финансовым системам, системам ИТ-разработки, базам знаний и другим ресурсам, в которых может храниться конфиденциальная информация, и от работоспособности которых зависит нормальное функционирование организации.

Неконтролируемый доступ к таким ресурсам чреват рисками информационной безопасности:

- Злоумышленники могут проникнуть в сеть организации через взломанного подрядчика, нарушить работу ИТ-систем, уничтожить или похитить информацию;
- Инсайдер на стороне подрядчика может спровоцировать утечку конфиденциальных сведений организации.

Это не теоретические риски. По данным экспертов по информационной безопасности, атаки через подрядчиков являются одним из самых распространённых способов проникновения в организацию, а по оценке Европейского Агентства по Информационной Безопасности — подобные атаки останутся главной киберугрозой для организаций до 2030 года.

Утечки — ещё одна распространённая угроза. По подсчётам экспертов, каждая пятая компания сталкивается с подобными инцидентами, а средний ущерб от одной утечки составлять 5,5 млн рублей в виде прямых финансовых потерь и без учёта репутационных издержек и расходов, связанных со штрафами.

Атаки из браузера

Поскольку многие корпоративные ИТ-системы спроектированы так, чтобы взаимодействие с ними осуществлялось через веб-интерфейс, основным инструментом доступа к этим ресурсам является браузер. Это удобно, так как ИТ-администраторам не нужно заботиться об установке специализированного приложения для доступа к каждой системе на компьютер сотрудника или подрядчика. Достаточно, чтобы там стоял любой современный браузер, а у пользователя имелся логин и пароль для входа.

Однако когда речь заходит о доступе внешних агентов к внутренним системам через браузер, возникает проблема безопасности:

- Во-первых, ИБ-команда организации не имеет возможности убедиться, что подрядчик подключается к внутренним системам из безопасного окружения: обновлена ли операционная система компьютера, на котором запущен браузер подрядчика, и обновлён ли сам браузер, есть ли на компьютере защитное ПО и т.д.
- Во-вторых, ИБ-команда не может регламентировать то, как подрядчик работает с информацией, к которой он получает доступ внутри сети организации.

При такой конфигурации ИБ-службе организации остаётся уповать только на внутренние защитные инструменты, которых вполне может и хватить, чтобы предотвратить атаку вредоносную атаку через подрядчика или утечку конфиденциальных сведений, однако подключения к внутренним системам со стороны внешних агентов всегда будут неконтролируемым источником риска.

Защититься от подобной угрозы можно с помощью юридических и страховых инструментов: компанию можно застраховать от кибер-инцидентов, а в договоре с подрядчиком задекларировать его ответственность за обеспечение безопасности собственной инфраструктуры, но этим меры не снизят вероятность инцидента, а лишь частично защитят от его последствий.

Лучшим вариантом будет доступ к данным компании в контролируемых условиях, и вот как это можно сделать.

Как Яндекс Браузер для организаций помогает безопасно работать с подрядчиками

Расширенная версия Яндекс Браузера для организаций позволяет обеспечить контролируемый и защищённый доступ к внутренним ИТ-системам даже для пользователей, работающих на неконтролируемых организацией устройствах. Результат достигается с помощью пяти функций Браузера.

Аттестация устройств

Позволяет задать требования к устройству и состоянию установленного на нём ПО. Если Браузер или устройство подрядчика не соответствует ожидаемому эталону (например, ОС не обновлена до свежей версии, а антивирус отключён), то доступ к внутренним ресурсам будет заблокирован.

Обязательный браузер

При соответствующей настройке сетевой инфраструктуры организации функция позволяет сделать Яндекс Браузер для организаций единственным браузером, с помощью которого можно получить доступ к внутренним ресурсам.

Защита от утечки

Браузер обладает набором функций защиты от случайной или намеренной утечки данных через:

- функцию «Копировать/Вставить»;
- перетаскивание;
- выгрузку на внешние веб-ресурсы;
- сохранение на внешние физические носители;
- печать;
- захват звука и изображение экрана;
- скриншоты;
- фотографии и видео с помощью внешних устройств.

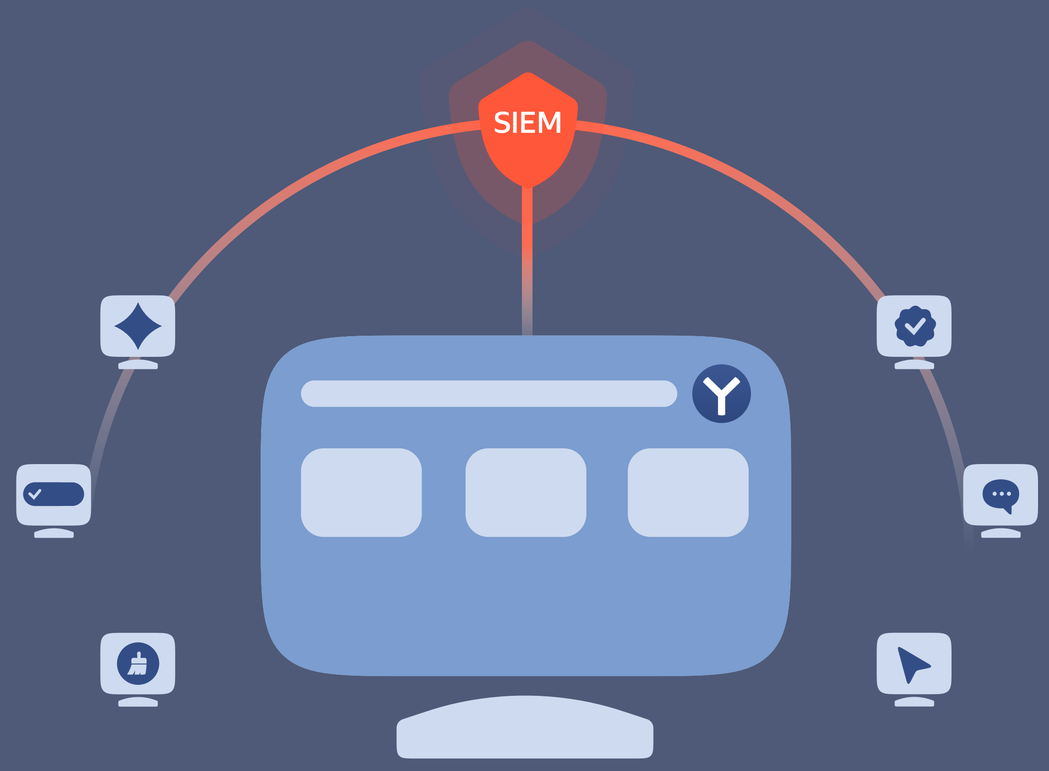
Интеграция с SIEM

Браузер способен отправлять уведомления о наступлении значимых событий безопасности в системы управления информационной безопасностью и событиями безопасности (Security information and event management, SIEM), используемые в центрах оперативной безопасности (Security Operation Center, SOC) организации. Такими событиями могут быть:

- срабатывание встроенных защитных систем Браузера (загрузка вредоносного ПО, запуск вредоносного кода, переход на фишинговую страницу и др.);
- срабатывание функций защиты от утечки;
- попытка подключения с устройства, не прошедшего аттестацию;
- и др.

Все вместе эти функции создают на устройстве подрядчика доверенную среду, из которой он сможет подключаться к внутренним ресурсам организации, не создавая серьёзных рисков вредоносной атаки или утечки конфиденциальных сведений.

Это повышает защищённость ИТ-инфраструктуры и экономит деньги, которые организации пришлось бы потратить на устранение последствий ИБ-инцидентов.



Яндекс Браузер | для организаций |

Наш сайт: browser.yandex.ru/corp

Telegram
Дзен
YouTube
ВК Видео

Связаться с нами: