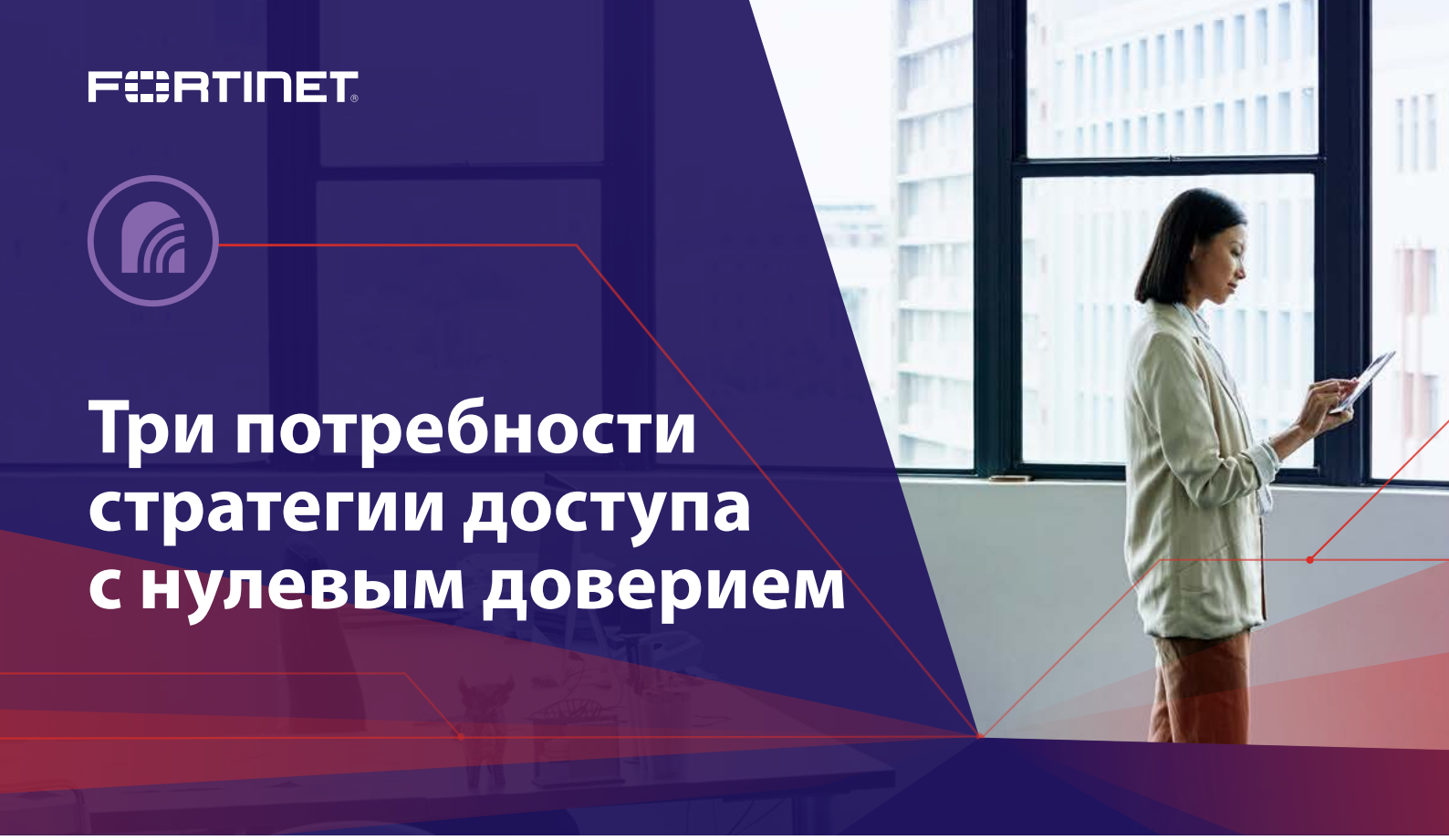

Три потребности стратегии доступа с нулевым доверием

Традиционные модели обеспечения безопасности исходят из предположения, что сети организации следует доверять. Однако автоматическое распространение доверия на все устройства или пользователей подвергает организацию риску в случае намеренной или случайной компрометации какого-либо устройства или пользователя. Именно поэтому многие руководители служб безопасности переходят к принципу доступа с нулевым доверием (ZTA) при идентификации, проверке подлинности и мониторинге пользователей и устройств как в сети, так и вне ее.

Цифровые инновации дают беспрецедентный рост продуктивности, однако они же создают новые риски для кибербезопасности. Злоумышленники, вредоносное ПО и зараженные устройства, не подвергающиеся проверке на границе сети, часто имеют свободный доступ к ее внутренним сегментам.

Поэтому организации больше не могут доверять пользователям и устройствам независимо от того, находятся они за пределами или внутри сети. Руководители служб безопасности должны исходить из того, что каждое устройство в сети может быть заражено, а каждый пользователь может намеренно или случайно скомпрометировать критически важные ресурсы. Стратегия доступа к сети с нулевым доверием меняет фундаментальную парадигму открытых сетей, построенных на принципе доверия по умолчанию, на структуру с нулевым доверием, которая реализуется внедрением строгого контроля доступа к сети.

Стратегия ZTA контролирует сетевые подключения и выполняет три важные функции.

С развитием доступности подключений, практик совместной работы и количества устройств расширяется и спектр угроз. В связи с этим требуется комплексный подход с нулевым доверием, позволяющий распознавать и контролировать каждого пользователя и каждое устройство в вашей сети.

1. ЧТО: знай каждое устройство в своей сети

Обилие приложений и устройств расширяет периметр сетей, создавая миллиарды границ, которые требуют управления и защиты. Перегруженные IT-специалисты изо всех сил стремятся удержать под контролем волну новых устройств, которая возникает в результате внедрения Интернета вещей (IoT), политик работы на личных устройствах (BYOD) и просто по мере развития корпоративной среды.

Первый шаг к внедрению стратегии ZTA — обнаружение и идентификация всех устройств в сети, включая телефоны и ноутбуки конечных пользователей, сетевые серверы, принтеры или устройства IoT без монитора, такие как контроллер системы отопления, вентиляции и кондиционирования, или устройство считывания пропусков. Благодаря такому отслеживанию сотрудники отдела безопасности получают сведения о типе, функциях и назначении каждого устройства, присутствующего в сети. Исходя из этой информации, они могут настроить целесообразные средства контроля доступа для таких устройств. Когда такой контроль реализован, в рамках доступа с нулевым

доверием ведется постоянный мониторинг с получением ответов от устройств, чтобы выявлять проблемы и устранять соответствующие устройства до того, как они заразят другие устройства или системы в сети.

2. КТО: знай каждого пользователя в своей сети

Удостоверение пользователей — критически важный элемент эффективной политики ZTA. Организации должны знать каждого пользователя, который пытается получить доступ к сети. Это сотрудник? Подрядчик? Гость? Поставщик? Для удостоверения пользователя требуются имя пользователя и многофакторная проверка подлинности; пароли обычно бывают слабыми, и их часто похищают. Также следует использовать сертификаты для принудительного удостоверения. Они могут быть связаны с контролем доступа на основе ролей (RBAC), чтобы пользователь, прошедший проверку подлинности, получал доступ к определенным возможностям и службам.

После того как личность пользователя удостоверена, политики доступа определяются его ролью в организации. Можно использовать политику максимально ограниченного доступа, предоставляя пользователю доступ только к тем ресурсам, которые необходимы для его роли или должности, и открывая доступ к дополнительным ресурсам лишь в случае непосредственной необходимости.

По мере распространения модели с нулевым доверием в организации руководители отделов безопасности могут начать внедрять средства контроля, которые будут давать пользователям необходимый доступ к сети из любого места. Возможность определить доступ на основе ролей для всех пользователей сети обеспечивает высокий уровень сетевой безопасности, что хорошо как для самой организации, так и для всех ее контрагентов (партнеров, поставщиков, подрядчиков).

3. ВНУТРИ и СНАРУЖИ: знай, как защитить ресурсы внутри сети и за ее пределами

Согласно недавнему отчету, 63% компаний не могут контролировать конечные точки за пределами своей сети и более половины не в состоянии определить, соответствуют ли устройства в таких конечных токах установленным требованиям.[1] Одна из основных проблем, приводящих к этому, — увеличение мобильности рабочих мест в сочетании с распространением практики удаленной работы.

Используя стратегию ZTA, организации могут решить проблему защиты устройств за пределами сети, повышая уровень отслеживания конечных точек. Критически важными элементами стратегии ZTA являются проверка на уязвимости, надежные политики развертывания исправлений и Web Filtering. В дополнение к этому подход с нулевым доверием позволяет реализовать надежный удаленный доступ к сетевым ресурсам при помощи подключения к виртуальной частной сети (VPN). Это позволяет специалистам по безопасности видеть, контролировать и защищать устройства независимо от того, находятся они внутри сети или за ее пределами.

Рекомендации по переходу на следующий этап

Эффективная система с нулевым доверием обеспечивает идентификацию, сегментацию и непрерывный мониторинг всех устройств, позволяя организациям гарантировать безопасность внутренних ресурсов, надлежащую защиту данных, приложений и интеллектуальной собственности и упрощение сетевых операций и функций обеспечения безопасности в целом.

[1] Отчет «The Cost of Insecure Endpoints», Ponemon Institute, 2019 г.

Возможности стратегии ZTA для устройств:

- Идентификация, профилирование и проверка на наличие уязвимостей всех устройств
- Установление и поддержание текущего контроля сети
- Обеспечение автоматического реагирования и настройки сети

Возможности стратегии ZTA для пользователей:

- Удостоверение пользователей при помощи имени пользователя, многофакторной проверки подлинности и сертификатов
- Поддержка ролей для предоставления информации от источника проверки подлинности привилегированным пользователям
- Дополнительные функции безопасности и менее утомительная работа для конечного пользователя благодаря проверке подлинности с единым входом

ноября 22, 2020 7:49 ПП

696154-0-1-RU