PRODUCT BRIEF

В ОБЩИХ ЧЕРТАХ

Symantec® Zero Trust Network Access (ZTNA) является важнейшим компонентом комплексного решения SASE.

АРХИТЕКТУРА НУЛЕВОГО ДОВЕРИЯ ИСКЛЮЧАЕТ УЯЗВИМОСТЬ ПРИЛОЖЕНИЙ

- Доступ с наименьшими привилегиями сокращает площадь атаки.
- Связь на уровне приложений между аутентифицированными пользователями и приложениями.
- Отсутствие входящих соединений с сетью скрывает приложения от злоумышленников.

ЛЮБОЕ УСТРОЙСТВО, ЛЮБОЕ МЕСТОПОЛОЖЕНИЕ, ЛЮБОЕ ОБЛАКО

- Безагентный доступ для всех типов приложений (web, SSH, RDP, TCP) с любого устройства, в любом месте, в любом облаке.

Symantec® Zero Trust Network Access

Доступ к облачным или локальным приложениям в любое время, в любом месте и с любого устройства

Необходимость обеспечения безопасного доступа с нулевым уровнем доверия к облачным и локальным приложениям

Обеспечение доступа авторизованных пользователей к корпоративным приложениям и сервисам было простым делом, когда все находилось в крупных корпоративных центрах обработки данных, а пользователи располагались в предсказуемых местах и использовали корпоративные устройства. Внутри периметра сети пользователи имели полный доступ к приложениям и сервисам. За пределами межсетевого экрана они использовали такие средства как VPN для получения доступа к корпоративной сети,а затем и к приложениям, необходимым для работы.

Облачное поколение навсегда изменило способы доступа сотрудников к информации, и ИТ-специалистам пришлось идти в ногу со временем. Перенос приложений в "облако" без ущерба для мобильности пользователей и возможности доступа в любое место является первостепенной задачей. Такая трансформация создала значительные сложности и выявила уязвимости в системе безопасности, существующие в традиционных методах VPN-доступа.Эти проблемы включают в себя следующие уязвимости:

- **Атаки с широкой сетевой поверхностью:** Сканирование уязвимостей и другие методы раскрывают всю сеть и отображают доступные приложения. В традиционных решениях часто отсутствует привилегированный доступ "точно в срок", что дает полный доступ к ненужным ресурсам.
- **Латеральное перемещение:** Создание прямого соединения с сеткой сервисов и клиентов значительно увеличивает вероятность латерального перемещения.
- **Отсутствие видимости:** Действия, выполняемые пользователями, подключающимися к приложениям, крайне затрудняют сквозную трассировку.
- **Сложные проблемы обслуживания и масштабирования:** Развертывание нескольких шлюзов для поддержки всех возможных вариантов транзита трафика требует настройки DMZ и межсетевых экранов, что является дорогостоящим и сложным процессом.
- **Неудовлетворительная работа пользователей:** Невозможность поддержки сторонних подрядчиков с их собственными устройствами снижает производительность. Транспортировка трафика приводит к увеличению задержек, неудобствам и плохой работе пользователей.

Современная динамичная бизнес-среда, изощренные угрозы и кибератаки создают уникальные проблемы, требующие нового подхода, который позволяет отказаться от устаревшего подхода, основанного на периметре, подвергающего опасности корпоративные сети и приложения и не рассчитанного на эпоху облачных вычислений.

В ОБЩИХ ЧЕРТАХ (ПРОДОЛЖЕНИЕ) ЛЕГКОЕ АДМИНИСТРИРОВАНИЕ

• Быстрое введение в эксплуатацию с помощью Zero Touch Provisioning.

• Управление доступом к любым размещенным приложениям в любых облачных и локальных центрах обработки данных.

• Полный аудиторский контроль действий пользователей в приложении.

УПРАВЛЕНИЕ И ЗАЩИТА ДАННЫХ

• Тонкие политики, основанные на идентификации, местоположении, состоянии устройства, действиях, доступе к ресурсам и уровне соответствия данных.

• **Symantec Advanced Threat Protection и Content Analysis** для глубокой проверки.

• Соблюдение требований к данным с помощью облачной проверки **Symantec Data Loss Prevention Cloud** .

Symantec Zero Trust Network Access

Symantec Zero Trust Network Access (ZTNA) – это облачный сервис, обеспечивающий высокозащищенное управление доступом к корпоративным приложениям, развернутым в облаках IaaS и локальных центрах обработки данных. Symantec ZTNA исключает входящие соединения с сетью, создает программно определяемый периметр между пользователями и корпоративными приложениями и устанавливает доступ на уровне приложений на основе политик. Этот сервис обеспечивает полную маскировку всех корпоративных приложений и сервисов и их невидимость для злоумышленников, решая весь комплекс задач, с которыми сталкиваются традиционные решения.

По сравнению с традиционными решениями, основанными на периметре,Symantec ZTNA обладает следующими функциональными возможностями:

• Обеспечивает обязательный компонент SASE для обеспечения безопасности доступа к приложениям, как отмечают отраслевые аналитики.

• Устраняет атаки на поверхность сети, маскируя приложения от неавторизованных пользователей и предотвращая боковое перемещение авторизованных пользователей за пределы разрешенного им приложения.

• Интегрируясь с любым существующим поставщиком идентификационных данных, ZTNA непрерывно повторно авторизует доступ и действия пользователя в режиме реального времени в рамках контекстного подхода,основанного на наименьших привилегиях, проверяя каждый запрос по широкому набору параметров безопасности.

• Обеспечивает полный контроль и мониторинг данных для применения политик разрешенных действий, а также поточный контроль данных для обеспечения соответствия нормативным требованиям и защиты от вредоносных программ.

• Смена парадигмы безопасности позволяет полностью решить современные проблемы безопасности.

Symantec ZTNA обеспечивает лучший в своем классе пользовательский опыт, максимально быстро передавая трафик приложения от конечного пользователя непосредственно к приложению, независимо от его местонахождения. Symantec ZTNA обеспечивает следующие преимущества:

• Будучи облачным сервисом, он оптимизирует маршрут доступа к приложениям, избегая ненужных задержек, вызванных архитектурой транзита сетевого трафика.

• Symantec ZTNA использует инфраструктуру Google Cloud, обходя перегруженные маршруты публичного Интернета, что повышает удобство доступа пользователей к приложениям организации.

• Безагентный доступ к приложениям обеспечивает гибкость доступа пользователей к приложениям с любого устройства.

• Бесшовный доступ без шлюза к любому приложению (IaaS, PaaS, web или внутреннему).

В отличие от традиционных решений, основанных на периметре, для Symantec ZTNA исчезают проблемы обслуживания и масштабирования. Отпадает необходимость в сложном развертывании и обслуживании специализированных шлюзов безопасности.

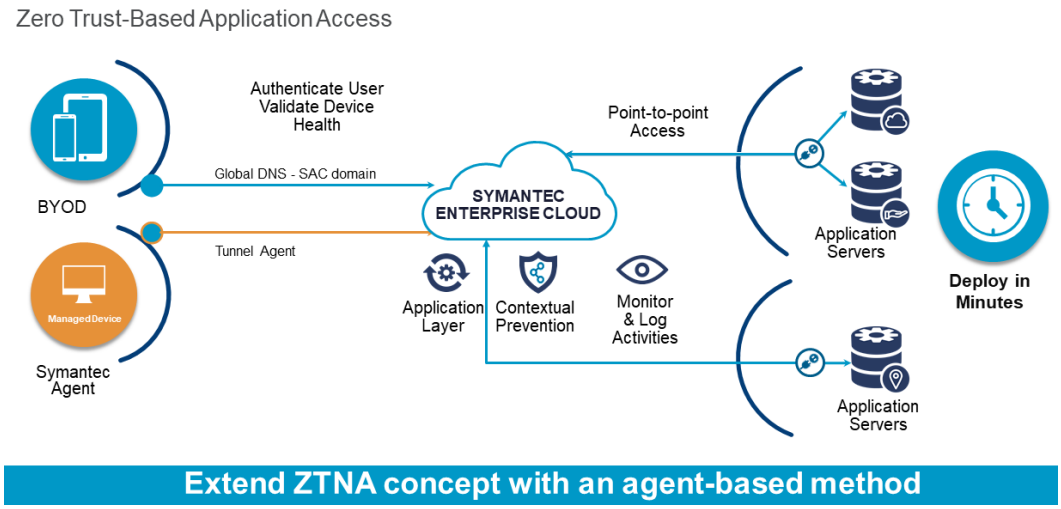
Быстрое внедрение

Symantec ZTNA снижает уровень сложности за счет простого развертывания без использования агентов, не требующего внесения изменений в существующие конфигурации безопасности. Оно легко интегрируется с существующими решениями по управлению идентификацией и доступом. Авторизованные пользователи могут подключаться из любой точки мира, используя любое устройство. Подключение позволяет им получить безопасный доступ к любому размещенному приложению в распределенных центрах обработки данных, как в частном или общедоступном облаке, так и в локальных центрах обработки данных.

Принцип работы

Когда аутентифицированный пользователь запрашивает удаленный доступ к корпоративному ресурсу, Symantec ZTNA создает и постоянно контролирует временное защищенное соединение между пользователем и запрашиваемым ресурсом. Двунаправленное HTTPS-соединение устанавливается на уровне приложений и исключает необходимость допуска пользователей во всю корпоративную сеть. Соединение является временным и автоматически разрывается, как только пользователь завершает свою задачу. С помощью Symantec ZTNA пользователи получают доступ только к тем приложениям и ресурсам, для которых они авторизованы. Решение обеспечивает полную видимость, управление и контекстное исполнение действий пользователей, а также мониторинг и протоколирование каждой операции для упрощения аудита и отчетности.

Access with ZTNA



Примеры использования

Защита доступа к корпоративным приложениям, переносимым в облако

По мере миграции корпоративных приложений в "облако" ИТ-специалисты должны обеспечить пользователям безопасный и беспрепятственный доступ к ресурсам, необходимым для их продуктивной работы. Решение должно исключить сложную настройку и обслуживание инструментов, которые не были разработаны для решения задач безопасности и соответствия нормативным требованиям в условиях отсутствия периметра.

Symantec ZTNA обеспечивает быстрый, свободный от агентов, безопасный доступ к корпоративным приложениям и ресурсам, расположенным как в облаке, так и в локальных центрах обработки данных. Гранулярные политики определяют контроль доступа на основе идентификации пользователя, состояния устройства, чувствительности приложения и выполняемых пользователем операций. Пользователям никогда не предоставляется широкий доступ на уровне сети, вместо этого они получают ограниченный доступ к конкретным приложениям на основе профиля доверия пользователя.

Защита доступа для персональных устройств и сторонних пользователей

Мобильность пользователей и BYOD стали новой нормой. Сотрудники должны иметь возможность легко и быстро получать доступ к корпоративным приложениям независимо от их местонахождения и используемого устройства. Современная динамичная бизнес-экосистема часто требует предоставления третьим лицам, например партнерам или поставщикам, доступа к корпоративным ресурсам или системам, не подвергая организацию атакам. Symantec ZTNA обеспечивает аутентифицированный доступ к корпоративным ресурсам с нулевым уровнем доверия без предоставления доступа к сети. Удаленные пользователи и сотрудники партнеров могут получать доступ к определенным приложениям на основе их идентификационных данных и характеристик устройств, а специалисты по безопасности могут в режиме реального времени принимать меры по блокированию нежелательной и подозрительной активности.

Повышение производительности после слияния или поглощения

Объединение ИТ-операций после таких событий, как слияние или поглощение, – сложный и рискованный процесс, поскольку он предполагает объединение двух или более различных архитектур безопасности и потенциальное подвергание конфиденциальных данных новым угрозам. Пользователи часто страдают от плохого или отсутствующего подключения к необходимым ресурсам, низкой производительности и громоздких шагов для того, чтобы добраться до приложения. Решение Symantec ZTNA предназначено для обеспечения безопасного, бесперебойного и мгновенного доступа к внутренним ресурсам после завершения процесса слияния и поглощения. Простая настройка – все, что требуется для безопасного предоставления приложений пользователям новой организации для немедленного доступа и повышения производительности, без необходимости развертывания и управления VPN.

Защита доступа к средам DevOps

Командам DevOps требуется доступ как к производственным средам, так и к средам разработки. Защита этих сред от нежелательных лиц и неавторизованных пользователей имеет решающее значение для обеспечения безопасной работы организации. Symantec ZTNA автоматически предоставляет или удаляет доступ к VM, рабочим нагрузкам PaaS и приложениям за считанные секунды, используя облачное решение, основанное на API и не требующее вмешательства агентов. Оно обеспечивает аутентификацию доступа к средам DevOps, его своевременное предоставление на основе принципа наименьших привилегий, а также полный аудит и регистрацию.

Соответствие требованиям организации

Краеугольным камнем эффективной системы SASE является защита данных в соответствии с установленными политиками управления, которые разрабатывались годами. Обеспечение соблюдения правил для множества приложений, размещенных в различных облачных центрах обработки данных, может оказаться сложной задачей. По мере того, как организации переносят приложения в облако, обеспечивая защиту данных с помощью поставщика SASE, обладающего опытом в области предотвращения потери данных в облаке (DLP) (например, Broadcom), службы безопасности могут обеспечить соблюдение правил DLP в облаке как часть маршрута передачи данных ZTNA внутри облака.

Преимущества Symantec ZTNA

В следующей таблице приведены преимущества, отличающие Symantec ZTNA от традиционных решений.

Symantec ZTNA Отличия и преимущества

Отличия	Преимущества
Простое лицензирование	Symantec Network Protection предусматривает простое лицензирование на одного пользователя, включающее Symantec ZTNA, а также другие критически важные компоненты SASE, в том числе облачный защищенный веб-шлюз (SWG), расшифровку TLS/SSL, облачный брандмауэр, глубокую проверку содержимого и другие.
Интеграция DLP	Symantec ZTNA интегрируется с Symantec Data Loss Prevention, что позволяет организациям применять политики управления данными.
Безагентный доступ для BYOD	Поддержка персональных устройств мобильных пользователей, сторонних партнеров или консультантов для обеспечения безопасного доступа к корпоративным ресурсам и приложениям.
Поддержка DevOps	Доступ к средам DevOps, таким как виртуальные машины, рабочие нагрузки PaaS и приложения, предоставляется или прекращается в считанные секунды на основе наименьших привилегий.
Служба Symantec Threat Intelligence Service	Symantec предоставляет крупнейшую сеть разведки угроз и обеспечивает расширенную проверку на угрозы всего трафика через защищенное решение ZTNA.
Единый агент для управляемых устройств	Клиенты Symantec могут использовать клиент Symantec Endpoint или Cloud Secure Web Gateway для быстрого внедрения ZTNA, чтобы предоставить пользователям безопасный доступ к корпоративным ресурсам с минимальными операционными усилиями.
Облачно-нативное решение	Созданное в "облаке", решение Symantec ZTNA использует возможности Google Cloud для обеспечения максимальной производительности и масштабируемости независимо от размера организации.

Symantec by Broadcom Software

О компании Broadcom® Software

Broadcom Software – мировой лидер в области разработки критически важного для бизнеса программного обеспечения, которое модернизирует, оптимизирует и защищает самые сложные гибридные среды в мире. Благодаря своей культуре, ориентированной на инженерные разработки, Broadcom Software создает обширный портфель лучшего в отрасли программного обеспечения для инфраструктуры и безопасности, включая AIOps, кибербезопасность, управление потоком создания стоимости, DevOps, мэйнфреймы и безопасность платежей. Портфель программного обеспечения обеспечивает масштабируемость, гибкость и безопасность для крупнейших глобальных компаний мира.

Oberig it

Компания Oberig IT
является официальным дистрибьютором **Symantec** на территории Украины, Молдовы, Казахстана.
info.ua@oberig-it.com
www.oberig-it.com

www.oberig-it.com