ITD GROUP

PORTNOX

CORE

СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

ПРОБЛЕМАТИКА И ЗАКРЫВАЕМЫЕ РИСКИ

ПРОБЛЕМАТИКА

Сложности в идентификации и аутентификации устройств разных производителей.

Разнородность и ограниченность устройств в организации не позволяет просто решить задачу идентификации и авторизации абсолютно всех устройств в сети.

Portnox, применяя более **20** типов аутентификации для конечных устройств и прямое подключения без необходимости установки агентов позволяет выполнить идентификации и аутентификацию всех возможных типов устройств в организации, включая неуправляемые.

РИСКИ

- неконтролируемый доступ к внутренней информационной среде сторонних устройств несёт в себе многочисленные **риски получения доступа к информации сторонними лицами**, следствием чего могут стать **утечки ценной информации**, включая персональные данные, данные об активах информационной инфраструктуры, **подготовка и выполнение направленных атак** на инфраструктуру, нанесение вреда ключевым объектам;

- необходимость установки агентов для выполнения задач аутентификации несёт в себе **увеличение нагрузки на конечные рабочие станции**, **замедление работы**, и, как следствие, производительности сотрудников, **увеличение нагрузки на администраторов** информационных систем, связанной с обслуживанием агентов, устранения неисправностей агентов.

PORTNOX CORE

ПРОБЛЕМАТИКА

Зависимость от агентов и архитектуры.

Portnox позволяет исключить зависимость от агентов на конечных устройствах, а также от компонентов, как дополнительной точке отказа целых сегментов сети. Portnox не требует установки агентов на конечные устройства, тем самым снижая нагрузку и требования по вычислительным показателям для конечных устройств, а также значительно расширяя область покрытия неконтролируемых сегментов.

Архитектура решения состоит из малого количества компонентов (Сервер баз данных и сервер приложений) позволяет обеспечить отсутствие зависимости производительности и работоспособности всей инфраструктуры от работы серверов Portnox. В случае возникновения проблем с доступностью серверов Portnox или их работоспособностью никакого негативного влияния на корпоративную сеть не оказывается. Все критичные корпоративные процессы будут работать вне зависимости от доступности Portnox.

РИСКИ

- многокомпонентная архитектура решений **усложняет процесс обслуживания, повышает количество точек отказа**, увеличивая тем самым нагрузку на администрирование информационной среды, **увеличение расходов на обеспечение отказоустойчивой работы** каждого дополнительного компонента многомодульных систем.

- последовательное включение подобного рода систем в бизнес-процессы организации влечет за собой **усложнение процедуры восстановления работы инфраструктуры** во время сбоев, **увеличение расходов человеческих и ИТ-ресурсов** на поддержание непрерывной работы процессов.

PORTNOX CORE

ПРОБЛЕМАТИКА

Сложность в контроле всех существующих типов устройств. Невозможность покрыть единой политикой все существующие типы устройств.

Portnox закрывает данную задачу функционалом профилирования. Формирование профилей для разного набора устройств в организации для возможности проводить авторизацию устройств и контроль, что обеспечивает полную видимость всех сегментов корпоративной сети и всех подключённых устройств, включая многочисленные типы и группы неуправляемых устройств.

Увеличенные затраты на выполнение рутинных задач при использовании внутренних регламентов обслуживания сети.

Portnox предоставляет инструменты для построения процесса контроля соответствия профилям периферийных устройств, в случаях манипуляций с последними в виде замены/переноса принтеров, IP-телефонов, IP-камер.

Portnox выполняет проверку соответствия устройств политикам после замены, перемещения в другие сегменты, а также периодический контроль уже подключённых ранее устройств для пересмотра политики соответствия требованиям корпоративных стандартов. В случае несоответствия устройства профилю организации формируется уведомление администраторам и, при необходимости, возможны активные действия – например, отключение порта или перевод в конкретный более ограниченный сегмент сети.

РИСКИ

- отсутствие контроля за периферийными устройствами несет в себе **риски бесконтрольного доступа к информационной среде** с любой точки включения конечных периферийных устройств;
- невозможность выполнять идентификацию и контроль всех устройств в сети обеспечивает отсутствие видимости всей инфраструктуры, что **увеличивает нагрузку** на поддержание в актуальном состоянии программное обеспечение конечных устройств, соответствие требованиям политик организации при периодическом их пересмотре.
- после замены любых устройств требуется выполнить идентификацию, аутентификацию и проверку на соответствие требованиям корпоративных политик безопасности, что при отсутствии автоматического процесса приводит к необходимости периодического **вовлечения административного персонала на выполнения рутинных задач контроля, устранения несоответствий** в зависимости от количества проверяемых атрибутов по требованиям.

PORTNOX CORE

ПРОБЛЕМАТИКА

Сложность в обработке событий с разных каналов.

Portnox упрощает работу администраторов сети, предоставляя возможность дополнения процесса инвентаризации автоматизацией процесса сбора данных о конечных устройствах, а также о процессах, версиях ПО и пр.

Portnox в процессе опроса устройств собирает данные по каждому конечному устройству, что позволяет выгружать их для обработки и сравнения с имеющимися данными обо всех устройствах, с текущим статусом состояния программной оболочки устройств в актуальный момент времени. Таким образом качественно дополняя и упрощая задачу по инвентаризации резерва и использованию оборудования.

РИСКИ

- отсутствие централизованного и автоматизированного сбора данных о конечных устройствах **усложняет процесс инвентаризации, реагирования и обслуживания**, что прямым образом **требует увеличения штата сотрудников** для обслуживания инфраструктуры в зависимости от количества конечных устройств;

- невозможность оперативного автоматического реагирования на события безопасности несет в себе все вышеуказанные риски, связанные с возможностью удалённого **проникновения в пределы информационной среды злоумышленников и распространения вредоносного программного обеспечения**;

- привлечение для выполнения неавтоматизированных задач по обнаружению несоответствий и ручного перемещения устройств в карантинные участки информационной сети требуют **увеличения штата сотрудников в соответствии с размером штата устройств и требуемого времени реагирования на инциденты.**

PORTNOX CORE

ПРОБЛЕМАТИКА

Сложность в поддержании непрерывного контроля соответствия корпоративным политикам безопасности.

Portnox выполняет автоматизированный периодический контроль соответствия политикам различных устройств в соответствии со специализированными унифицированными профилями. В зависимости от построенных процессов в первом действии после процесса аутентификации устройств выполняется проверка наличия, например, установленного антивируса и агента DLP (возможны вариации проверок запущенных служб, наличия конкретных ключей реестре, файлов в файловой системе и пр.). В рамках проверки осуществляется исследование рабочих станций на наличие запущенных соответствующих служб и наличия установленного требуемого корпоративными стандартами ПО.

В случае, если выполняются следующие условия (на примере антивируса Касперского и агента DLP).
В рамках проверки наличия антивирусного ПО «Касперский»:

- служба avp.exe находится в состоянии «остановлена»,

«не запущено»;

- отсутствует файл C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows\avp.exe
- отсутствует папка C:\Program Files (x86)\Kaspersky Lab\NetworkAgent

В рамках проверки наличия агента DLP:

- служба <DLP_Service> находится в состоянии «остановлена», «не запущено»;
- отсутствует файл: C:\Program Files (x86)\<DLP_Agent_dir>\<DLP_Agent_exe_file>

устройство автоматически направляется в «карантинный» сегмент сети,

Portnox уведомляет администраторов безопасности о событии и предоставляет возможность для выполнения нескольких сценариев работы с «нарушителем», такие как намеренная установка недостающего ПО на «карантинную» машину, ограничение сетевого доступа, полная изоляция от корпоративной сети (отключение сетевого порта на коммутаторе).

Кроме вышеуказанных проверок Portnox обеспечивает возможности для просмотра актуальных обновлений ОС, наличия специфических для компании артефактов на конечных станциях и пр. В случае несоответствия предлагается предусмотреть различные варианты реакции. Например, автоматический запуск процесса установки актуальных обновлений ОС, антивирусных баз и пр. Процесс можно выполнять также с переносом устройства в отдельный VLAN, как пример возможности автоматизации процесса без привлечения персонала с уведомлением последнего о выполняемых системой шагах для полного информирования ответственных сотрудников.

PORTNOX CORE

РИСКИ

- невозможность своевременно обеспечивать контроль выполнения соответствия конечных устройств политикам безопасности несёт в себе **риск вирусного заражения всей инфраструктуры**, **возможность утечек ценной информации** за пределы организации, **проникновения злоумышленников в пределы закрытых сегментов информационной инфраструктуры и получение конфиденциальной информации;**

- отсутствие автоматизации в выполнении контроля за соответствием устройств информационной инфраструктуры несёт **значительное увеличение нагрузки на администраторов соответствующих подразделений** для выполнения ручного контроля выполнения соответствующих задач.

ПРОБЛЕМАТИКА

Сложность формирования маршрута устройств.

Portnox успешно решает задачу отслеживания перемещения устройства в сети. В процессе администрирования и обслуживания, а также штатных изменений в структуре организации, оборудование периодически перемещается администраторами инфраструктуры.

Для отслеживания истории перемещения и быстрого поиска устройства в случае возникновения информационных инцидентов, **Portnox** предоставляет инструменты журналирования истории перемещения устройства в организации. При необходимости можно быстро найти конечное устройство, определить сетевое устройство и порт, к которому подключено конечное устройство, определить к какому оборудования оно было подключено на предыдущих этапов существования его в организации.

РИСКИ

- расследование инцидентов без возможности выявить маршрут перемещения конечных устройств в сети **увеличивает время на получение важной информации для расследования** на порядки в зависимости от количества изменений расположений в сети устройств;

- процесс инвентаризации требует **увеличения штата сотрудников** в соответствии с размером штата устройств и требованиями по времени выполнения процедуры при отсутствии автоматизированного средств отслеживания перемещения устройств в организации.

PORTNOX CORE

ПРИМЕРЫ КЕЙСОВ

ТЕЛЕКОМ

ЦЕЛЬ И ЗАДАЧИ

Выстраивание процесса идентификации и аутентификации устройств разных производителей.

РЕШЕНИЕ

Разнородность и ограниченность устройств в организации не позволяет просто решить задачу идентификации и авторизации абсолютно всех устройств в сети. **Portnox**, применяя более 20 типов аутентификации для конечных устройств и прямое подключения без необходимости установки агентов позволяет выполнить идентификации и аутентификацию всех возможных типов устройств в организации, включая неуправляемые устройства.

РЕЗУЛЬТАТ

Сформирован и внедрен процесс идентификации и аутентификации всех новых подключаемых в различные сегменты корпоративной сети устройств. Обеспечивается периодическая повторная идентификация уже подключенных устройств в соответствии с политиками безопасности организации. Все не прошедшие аутентификацию устройства помещаются в отдельный изолированный сегмент сети.

ФИНАНСОВЫЕ ОРГАНИЗАЦИИ

ЦЕЛЬ И ЗАДАЧИ

Обеспечить распространение всех политик безопасности на все сегменты организации и устройства. Обеспечить независимость устройств от необходимости устанавливать дополнительное ПО.

РЕШЕНИЕ

Portnox позволяет исключить зависимость от дополнительных агентов на конечных устройствах, а также от дополнительных компонентов, как дополнительной точке отказа целых сегментов сети. **Portnox** не требует установки агентов на конечные устройства, тем самым снижая нагрузку и требования по вычислительным показателям для конечных устройств, а также значительно расширяя область покрытия неконтролируемых сегментов.

РЕЗУЛЬТАТ

Удалось обеспечить применение всех политик информационной безопасности организации для всех устройств без необходимости установки дополнительных агентов на конечные устройства. Благодаря специфике архитектуры решения, удалось обеспечить независимость производительности и работоспособности всей инфраструктуры от работы серверов **NAC**. Все критичные корпоративные процессы работают вне зависимости от доступности **Portnox**.