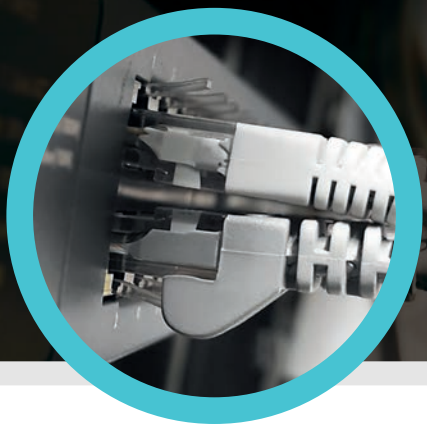
portnox™

Solutions Overview

# Portnox CORE

## On-Premise



*«Мы с гордостью присуждаем Portnox нашу премию за стратегию, новаторское решение и лидерство 2016 года в области Network Access Control»*

Joe Fristensky. Партнер и вице-президент. Frost & Sullivan

## Наша технология

Portnox обеспечивает полный контроль доступа к сети независимо от типа подключения: проводное, беспроводное, VPN, виртуальные сети и даже облачные ресурсы. В отличие от большинства других решений, Portnox для своей работы не требует дополнительных аппаратных устройс¬тв, программ-агентов, 802.1x или перестроения существующей сетевой инфраструктуры, TAP/SPAN портов. Данное решение поддерживает любую сетевую топологию и обладает уникальной способностью взаимодействовать напрямую с огромным спектром сетевых устройств с различным уровнем поддержки IP практически всех производителей.

Portnox CORE – это программное решение на платформе Windows Server, которое напрямую связано со всеми элементами сетевой инфраструктуры и обеспечивает непрерывный мониторинг всех устройств, подключенных к сети. Portnox поддерживает множество способов взаимодействия с сетевым оборудованием, включая SNMP, telnet, SSH и т. д. Таким образом, Portnox всегда обеспечивает полную и точную картину сети (в конце концов, устройства могут избежать обнаружения при сканирования диапазона IP-адресов, но не ARP-таблицы). После обнаружения Portnox может опросить каждое подключенное устройство с целью проверки его типа, уровня соответствия корпоративным стандартам, подлинности и даже личности пользователя. Все это делается без использования программ-агентов. Вместо этого используется более двадцати пяти различных методов профилирования и аутентификации, начиная от WMI, удаленного реестра и именованных каналов для устройств Windows, SSH и Telnet для устройств MacOS и Linux и многих других - для IoT, VoIP и прочих не-ПК устройств, составляющих значительную часть любой сегодняшней сети. Затем решение Portnox сопоставляет все найденные им данные и принимает решение о возможности подключения каждого конкретного устройства, с определенным уровнем соответствия принятым стандартам, конкретным пользователем к конкретной локации и конкретному порту или точке доступа.

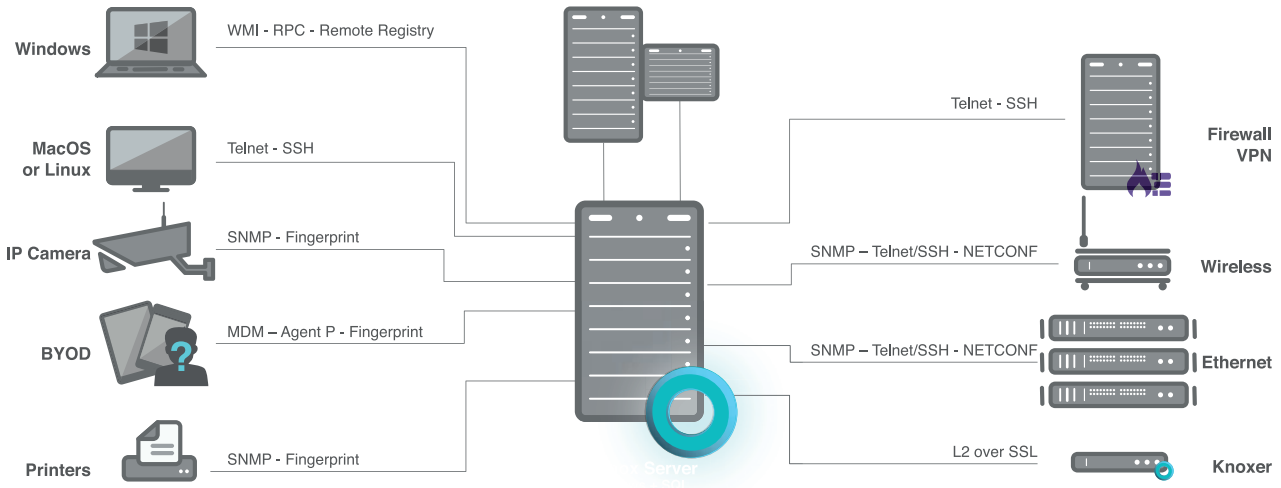
## СОДЕРЖАНИЕ



## КРАТКИЙ ОБЗОР

- Централизованное управление
- Без агентов
- Без изменений инфраструктуры
- Без необходимости 802.1x
- Охватывает все типы подключений
- Охватывает все устройства
- В режиме реального времени/событийно-управляемый
- Масштабируемый
- Легкий в управлении и внедрении
- Гибкие настройки и сценарии использования

# Краткий обзор архитектуры Portnox




В отличие от многих традиционных решений NAC, которые полагаются на анализе трафика с зеркалированных портов, сканирование диапазонов IP-адресов, инвентарный каталог или какие-либо другие пассивные методы, которые не обеспечивают обнаружение устройств в режиме реального времени, Portnox напрямую подключается через нативные протоколы к Вашей сетевой инфраструктуре (коммутаторы, WLC, VPN, виртуальные коммутаторы и т.п.), что обеспечивает немедленное обнаружение всех изменений в сети в режиме реального времени. Например, к управляемым коммутаторам Portnox обычно подключается через SNMP – это гарантирует, что Portnox сразу же узнает об изменениях на уровне L2. Когда новое устройство подключается к порту, Portnox уже его «видит», часто даже до того, как оно получит IP-адрес! Затем решение Portnox может подключаться к предварительно настроенным «IP-помощникам» (маршрутизатор/брандмауэр/IP PBX/AD) для получения IP-адреса и другой дополнительной информации о новых устройствах. Используя эту информацию и профиль устройства, Portnox выполняет аутентификацию устройства, чтобы подтвердить, что это легитимное корпоративное устройство, или определить устройство как неавторизованное.

Такая схема работы не позволяет ни одному устройству «спрятаться» от Portnox – если устройство подключено к сети, Portnox узнает об этом, даже если эти устройства подключены к неуправляемым коммутаторам! Portnox – это программное решение, которое развертывается в среде Windows Server 2008/2012 R2/2016 (физической или виртуальной). Portnox развертывается централизованно, один экземпляр сервера может обеспечить контроль сети крупного предприятия (20 000 портов). Если специфика бизнеса или схема сети требуют распределенного развертывания, решение Portnox обеспечивает это без какой-либо дополнительной платы.

## ОСОБЕННОСТИ АРХИТЕКТУРЫ

- Использует нативные протоколы для подключения к сети
- Без агентов
- Не зависит от 802.1x
- Событийно-управляемый
- Работа в режиме реального времени
- Полностью программное решение
- Централизованная или распределенная архитектура без дополнительных затрат.

# Обнаружение устройств – непрерывно, в режиме реального времени

Portnox начинает работать уже на канальном уровне. Подключаясь непосредственно к Вашей проводной, беспроводной и виртуальной инфраструктуре, Portnox обеспечивает непрерывное, событийное обнаружение в реальном времени всех устройств, которые подключаются к Вашей сети.

Более того, Portnox не перестает работать после успешной первоначальной проверки устройства в момент подключения. Решение с заданной периодичностью осуществляет повторные проверки уже подключенных устройств, чтобы обеспечить постоянное соответствие принятым корпоративным стандартам безопасности.

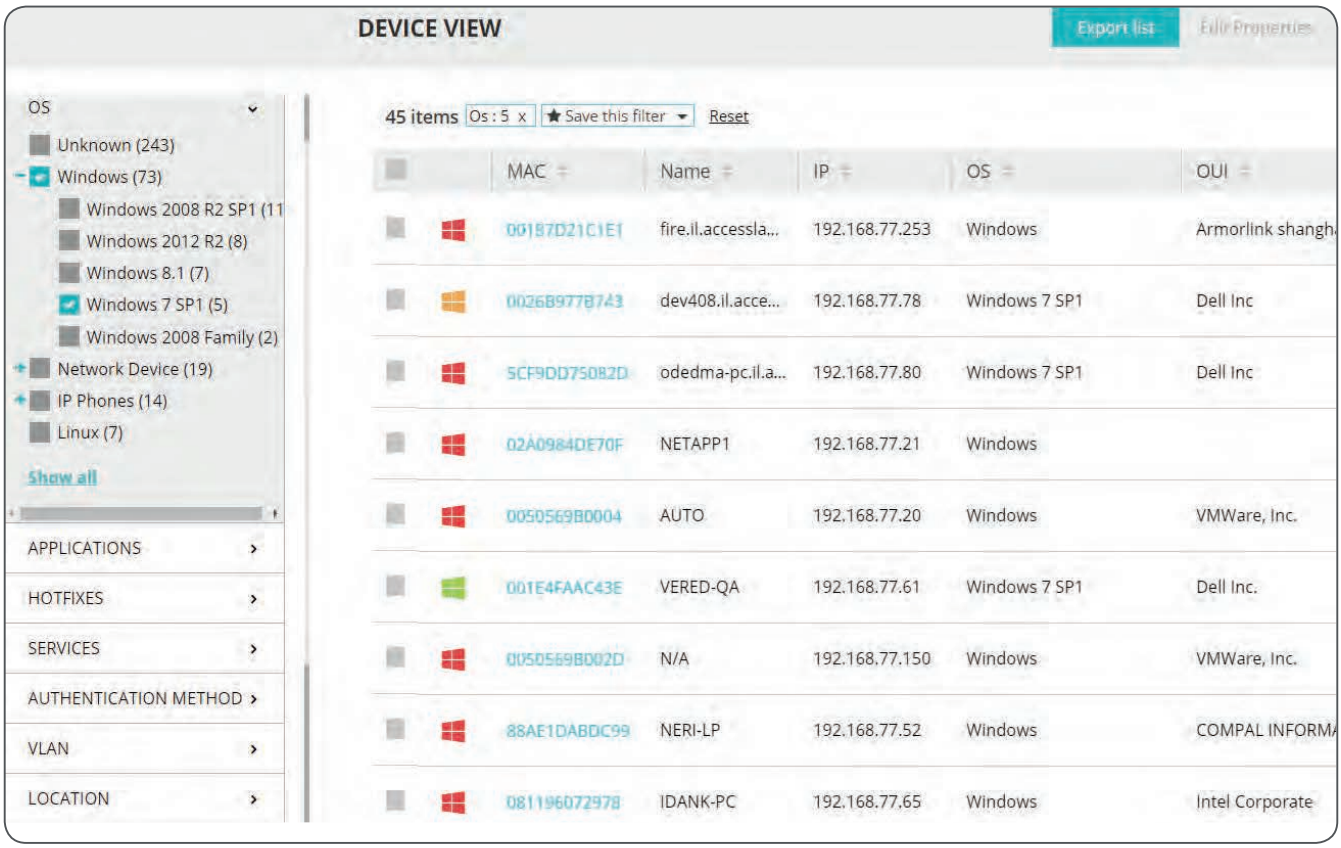
Конвергентные VoIP устройства? Нет проблем! Portnox автоматически обнаружит, определит и проверит отдельно VoIP-телефоны и отдельно – подключенные к ним устройства.

Неавторизованные концентраторы или точки доступа? Нет проблем! Portnox обнаруживает, уведомляет и может принимать меры против несанкционированных концентраторов или точек доступа.

Portnox предлагает множество удобных настраиваемых информационных панелей, с богатыми возможностями поиска, фильтрации по множеству параметров, например, тип ОС, приложения, службы, методы аутентификации, состояние безопасности, сервисы, патчи и т. д. Хотите увидеть все подключенные устройства под управлением Windows 7 SPI – просто щелкните, просмотрите и, если необходимо, экспортируйте!

## МЫ ВИДИМ ВСЕ

- Обнаружение начинается на канальном уровне
- В режиме реального времени
- Событийно-управляемое
- Непрерывное
- Без сканирования диапазона IP-адресов и анализа копий трафика
- Легкое создание настраиваемых представлений на основании множества атрибутов устройств, включая OS, приложения, расположение, статус безопасности и др.



# Device Authentication

| | | | | |
|---|---|---|---|---|
| **Win32** | [kerberos] | [ntlm2] | [registry] | [workgroup] |
| **Unix & Linux** | User Pass [ssh] | Key Auth [ssh] | SSHD FP | [telnet*] |
| **Printers** | [snmp] | [Oil lookup] | http | 3D |
| **Fingerprint** | [proprietary] | [dhcp] | [syn/arp] | [salt] |
| **VoIP** | pbx | VMware | VPN | Geo IP |
| **Interactive user** | [portal] | [chaperone] | [voucher] | [guests] |

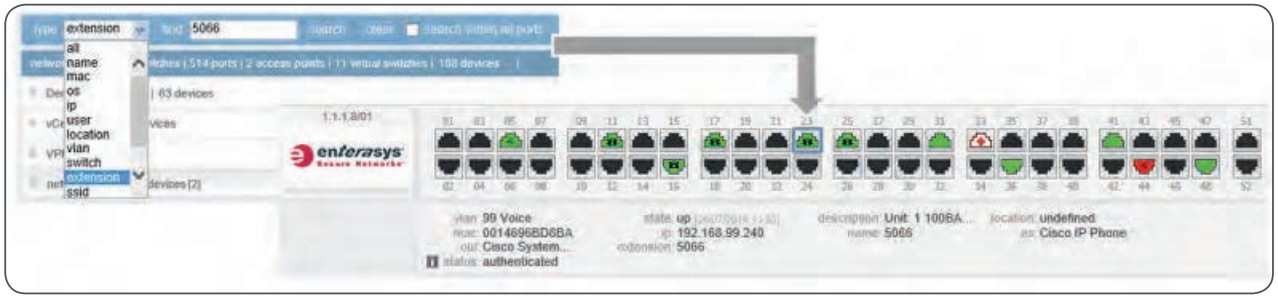
*Пример методов аутентификации устройств*

Следующий этап после обнаружения – это аутентификация. Так же как и в случае с прямой связью с сетевой инфраструктурой, решение Portnox аутентифицирует и корпоративные устройства, используя только нативные протоколы, без установки каких либо агентов, сапплликантов и т.п. Portnox поддерживает более 25 методов проверки подлинности и обеспечивает гарантию того, что к корпоративной сети смогут подключиться только легитимные устройства, включая и полноценную аутентификацию IoT-устройств. Спектр возможностей очень широк: от проверки состояния входа в домен в самом простом случае – до SNMP, SSH, OSFP – отпечатка устройства.

802.1x или другие решения на основе агентов всегда имеют проблему ограниченной поддержки устройств. В результате для подключения многих устройств, включая растущий сегмент IoT, придется создавать списки разрешенных MAC-адресов. Это порождает значительную дополнительную административную нагрузку при том, что с точки зрения обеспечения безопасности эта мера – чуть лучше чем не делать совсем ничего! Большинство IoT- устройств содержат MAC-адрес на видимой метке, и даже самый неопытный «хакер» может легко узнать его и подделать. Поэтому остерегайтесь любого решения, которое базируется на списках MAC-адресов.
В среде VoIP Portnox идет еще дальше и обеспечивает не только надежную аутентификацию (как правило, через SNMP или OSFP), но и интегрируется с VoIP PBX для получения дополнительной информации об устройстве VoIP, включая добавочный номер. Эта информация затем становится доступной для поиска. Хотите знать, где подключен VoIP-номер 5066? С помощью Portnox для этого вам необходимо сделать всего один клик!

## АУТЕНТИФИКАЦИЯ

- 25+ Методов аутентификации
- Без агентов
- Без сапплликантов
- Строгая, безопасная\ аутентификация для IoT устройств
- Ваучеры на ограниченную по времени аутентификацию устройства

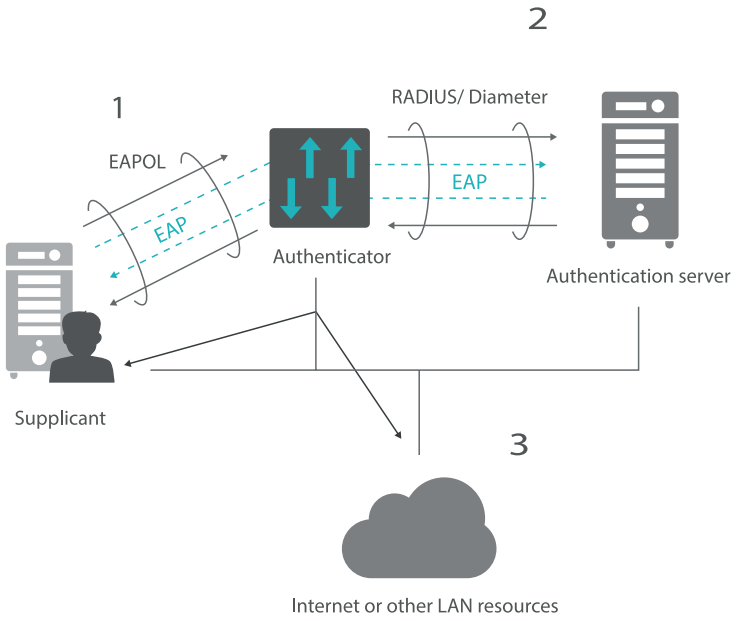
# Активные меры защиты и проверки соответствия

Честно говоря, существует множество различных решений и методов обнаружения устройств, подключенных к сети. Основная ценность NAC-решения заключается в способности про-активно принимать меры защиты в отношении нелегитимных устройств или устройств, которые нарушают принятые стандарты безопасности. Проблема заключается в том, что большинство традиционных решений NAC не работают в режиме реального времени, не обладают достаточной гибкостью и поэтому не могут эффективно функционировать в автоматическом режиме. У многих CIO/CISO есть печальный опыт эксплуатации NAC-решений, когда по каким-то причинам было заблокировало критичное легитимное устройство. Как правило, после нескольких повторов такой ситуации NAC переводится в режим мониторинга и становится всего лишь «еще одним» инструментом e-discovery.
Хорошая новость – это все не о Portnox! Более 80% наших клиентов используют активные меры защиты, которые предлагает Portnox, в автоматическом режиме.

Portnox напрямую подключается к корпоративным ПК без использования какого-либо агента для проведения всех необходимых проверок, включая уровень патчинга ОС, наличие и статус AV, активные сетевые интерфейсы, привилегии локального пользователя, наличие съемного хранилища, авторизованные (или неавторизованные) программы, сервисы и многое другое. И даже если у Вас уже есть другое решение для проверки уровня соответствия конечных устройств, то Portnox может использовать его статус как один из параметров для своих собственных проверок.
То, что по-настоящему отличает Portnox от других решений, – это **гибкость**, которую Portnox предлагает в настройке и выборе действий, которые должны выполняться в зависимости от устройства, пользователя, статуса аутентификации, местоположения и уровня соответствия корпоративным стандартам. Такая гибкость является критичной для достижения и соблюдения баланса между безопасностью и продуктивностью. Вы должны принять одни действия, если компьютер подключается без установленного антивируса, другие – если антивирус установлен, но не обновлен и т.п. Хотите более строгие меры безопасности для бухгалтерии или АСУТП-сегмента сети – без проблем!
Любое устройство, которое подключается из конференц-зала, должно иметь доступ только к гостевому VLAN? Пожалуйста!
И эта гибкость Portnox характерна для всех стадий и операций, включая фазу подключения устройства к сети. Portnox поддерживает различные модели проверок, включая pre-connect, postconnect и partial pre-connect. Вы можете выбирать различные модели для различных сегментов сети или групп устройств.
Наконец, гибкость Portnox распространяется и на процесс внедрения решения, позволяя осуществить плавный, комфортный переход от режима обнаружения и мониторинга – к активным мерам защиты для выбранных портов, коммутаторов, сегментов сети, локаций и, наконец, всего предприятия.

## МЕРЫ ЗАЩИТЫ

- Гибкие меры защиты на основе устройства, пользователя, расположения, аутентификации, степени соответствия
- Детальные проверки и валидация уровня соответствия конечных точек
- Возможность поэтапного, гранулярного ужесточения политик доступа
- Оптимальный баланс безопасности и продуктивности




## НЕДОСТАТКИ 802.1X

- Сложное, ресурсоемкое внедрение и эксплуатация
- Поиск причин сбоев затруднен
- Требует ведения списков разрешённых MAC адресов для IoT и других неподдерживаемых устройств
- Обновления, модификации любого компонента могут вызвать сбои в работе
- Отсутствие продвинутых механизмов проверки соответствия принятым стандартам

## Особенности 802.1X

Большинство вендоров NAC и многие поставщики сетевых решений требуют наличия 802.1x как основного инструмента обеспечения аутентификации устройств и контроля доступа, по крайней мере, теоретически. Мы говорим теоретически, потому что для многих организаций уровень усилий, времени и опыта, необходимый для эффективного развертывания 802.1x в масштабе всего предприятия, во всех сетях - проводных и беспроводных, часто является недостижимым.

Если рассматривать 802.1x только в проводной сети, то мы сразу же сталкиваемся с проблемой просто сложности 802.1x by design. Вам нужно продумать и настроить три основных компонента, часто от разных поставщиков: клиентские устройства, коммутаторы и RADIUS. При этом не забудьте о растущем количестве IoT-устройств, IP-камер, для которых не существует 802.1ъ-саппликантов. Поэтому будьте готовы выделить ресурсы на создание и управление растущим списком MAC-адресов (и будьте готовы к успешным MAC spoofing атакам). Чем сложнее система, тем больше вероятность, что что то пойдет не так во время развертывания и эксплуатации. В случае с 802.1x эта вероятность близка к 100%.

Поэтому при планировании внедрения 802.1x заранее заложите определенное количество человеко-часов на анализ логов и поиск причин некорректной работы. Если Ваши сетевые инженеры еще не очень глубоко разбираются в PEAP, EAP-TTLS и PKI - не расстраивайтесь. К концу внедрения 802.1x они станут настоящими экспертами.

Следующая головоломка – клиентские устройства. Основная проблема – далеко не все устройства, которые подключаются к сети, имеют поддержку 802.1x. Но это не единственная проблема. Даже если все Ваши устройства поддерживают 802.1x, все равно остается масса интересных вопросов. Например - Как организовать настройку и управление сапплikантами на всех устройствах? Что делать с обновлениями? Все ли будет работать, если у Вас разные сетевые вендоры, разные производители ПК и ноутбуков? Даже если все наконец построено и работает, расслабляться и выдыхать рано – даже регулярные обновления могут нарушать работу 802.1x сапплikантов. При использовании 802.1X диагностирование и поиск причин ошибок является не тривиальной задачей. Вы должны быть уверены, что Ваша служба поддержки с ней справится.

Кстати, о службе поддержки. Заранее выделите несколько человек, которые будут заниматься исключительно ручным подключением в сеть устройств, которые ошибочно были заблокированы, так как 802.1x не содержит средств автоматической повторной аутентификации устройств!

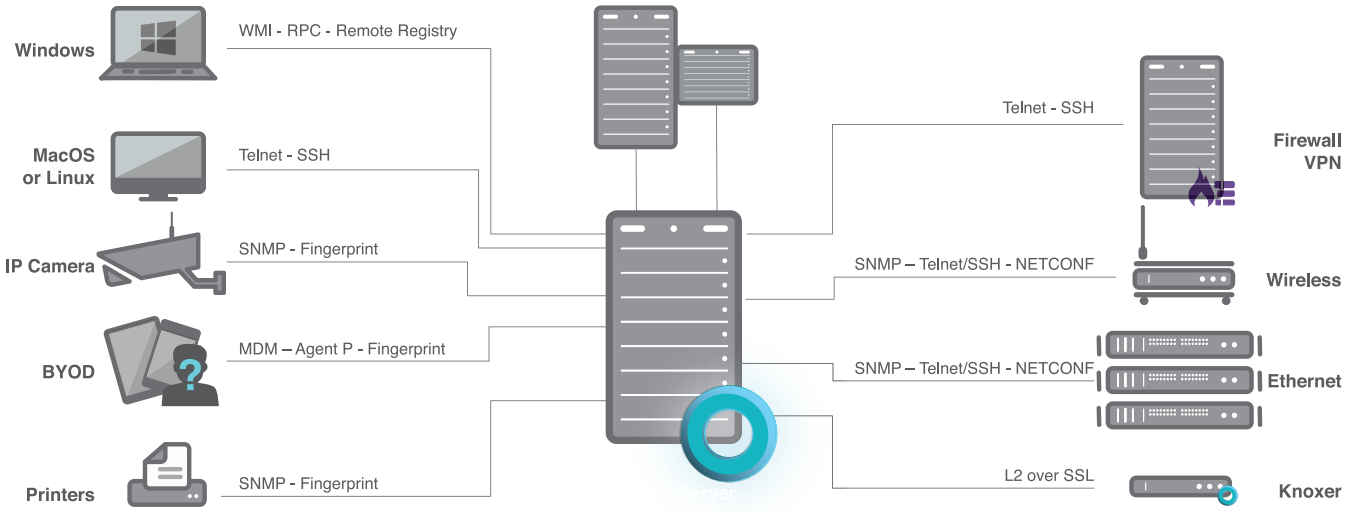
**Перед тем как вы опуститесь к пути 802.1X, рассмотрите Portnox POC – бок о бок с выбранным вами решением 802.1X – и увидите непосредственное различие!**

# Отличия Portnox

Организации всех размеров должны иметь четкую видимость и контроль в реальном времени всех устройств, подключающихся к их сети. Вопрос только в том, как лучше всего выполнить эту задачу.

В Portnox мы концентрируемся только на одном: предоставить такое решение по управлению доступом к сети, которое обеспечивает обнаружение 100% устройств независимо от типа подключения (проводное, беспроводное, VPN, виртуальное). Мы уделяем особое внимание простоте использования, простоте развертывания и гибкости. Мы также стремимся сделать наше решение доступным для организаций любого размера и легко масштабируемым по мере роста бизнеса наших Клиентов.

Мы можем много писать о нашем решении - «бумага все стерпит». Поэтому мы предпочитаем, чтобы Вы сами увидели Portnox в действии и получили личный опыт использования. Просто напишите нам по электронной почте - мы сможем установить демонстрацию или пилотный проект.




Контакты
Softprom by ERC – Value Added Distributor
info@softprom.com | https://softprom.com/vendor/portnox