Безопасность Интернета вещей и медицинских устройств в организациях сферы здравоохранения

С каждым годом компьютерные сети организаций здравоохранения и используемые в них медицинские устройства становятся значительно более сложными, что представляет собой всё более заметную проблему для ИТ-сотрудников, осуществляющих их поддержку. Если ранее такие организации мыслили исключительно в терминах количества установленных устройств и пропускной способности сети, то сегодня им предстоит пересмотреть свой подход к обеспечению поддержки медицинских устройств и переосмыслить свою стратегию по внедрению инструментов бизнес-аналитики в своей сети.

В некоторых случаях ИТ-подразделениям ещё не доводилось сталкиваться с поддержкой медицинских устройств. Ранее медицинские устройства было принято размещать в единой VLAN сети, которая была защищена межсетевым экраном. Однако сегодня такой подход является устаревшим по целому ряду причин, в числе которых:

- отсутствие возможностей для ограничения и контроля внутреннего доступа сотрудников, подрядчиков и специалистов технической поддержки производителя устройств;
- риск того, что некорректная конфигурация одного типа устройств будет негативным образом сказываться на работе других устройств.

Поскольку производители медицинских устройств стали всё чаще использовать в своей продукции Wi-Fi, в беспроводных локальных сетях многих лечебных учреждений теперь можно встретить инфузионные насосы, анализаторы газов крови, системы телеизмерений, портативные рентген-аппараты, УЗИ-установки, устройства для гемодиализа и измерители глюкозы. По мере добавления в сеть новых медицинских устройств прежняя стратегия, использовавшая, скажем, пять лет назад, при изначальном развёртывании сети, уже себя изжила. Например, один из распространённых подходов заключался в том, чтобы поместить все медицинские устройства в одну выделенную физическую или виртуальную сеть. Предполагалось, что таким образом эти устройства будут защищены от внешних рисков безопасности и от факторов, приводящих к снижению их производительности.

Но как выяснилось, такой подход не всегда себя оправдывал. Спустя годы, медицинские учреждения начали испытывать сложности с поддержкой беспроводного медицинского оборудования от различных поставщиков определённого вида медицинских устройств в своих виртуальных сетях, что обусловлено помимо прочего:

- отсутствием поддержки современных технологий аутентификации и шифрования в устаревших беспроводных медицинских устройствах;
- необходимостью уникальных сетевых конфигураций для подключения устройств, например, параметров качества обслуживания в сети или настроек безопасности;
- необходимостью соблюдения нормативных требований, предъявляемых к медицинским устройствам, и требований Управления США по контролю за качеством продуктов и медикаментов (FDA);
- по мере добавления новых медицинских устройств, становится неприемлемым перемещение всех медицинских устройств в выделенную сеть без предварительного уведомления пользователей;
- необходимостью ограничения доступа к единому паролю от беспроводной сети.

Заметив, что учреждения отрасли здравоохранения сталкиваются с необходимостью подключения всё большего числа медицинских устройств к одой и той же сети, FDA недавно опубликовало информационный бюллетень, в котором указаны современные риски использования медицинских устройств в больничных сетях, а также приведены следующие рекомендации для больниц:

- необходимо ограничивать неавторизованный доступ к сетям и к медицинским устройствам и отслеживать сетевую активность;
- обновлять антивирусные программы, настройки межсетевых экранов и своевременно устанавливать обновления для системы безопасности;
- разрабатывать и анализировать стратегии для сохранения функциональности сети в случае неблагоприятного развития событий.

Основные технологические задачи при использовании IoT и медицинских устройств в больничном окружении

НЕДОСТАТОЧНОЕ ПОКРЫТИЕ WI-FI ДЛЯ РАБОТЫ МЕДИЦИНСКИХ УСТРОЙСТВ

По мере того, как всё больше производителей медицинских устройств переходят с применявшихся ранее диапазонов Wireless Medical Telemetry Service (WMTS) на Wi-Fi, учреждениям отрасли здравоохранения приходиться планировать далеко не только модель покрытия Wi-Fi сети. Идёт ли речь о передвижных рабочих станциях, сканерах штрих-кодов, аппаратах для внутривенного вливания или обычных телефонах, сети должны поддерживать работу любых устройств, оснащенных Wi-Fi, которые больницы или медицинские учреждения сегодня используют для оказания медицинской помощи. Для обеспечения гладкой работы в сети не должно быть узких мест – ни в точках доступа в Wi-Fi, ни в обслуживающей эти точки проводной инфраструктуре, ни в широкополосном подключении к Интернету, ни в центрах обработки данных. Для обеспечения бесперебойной работы больницы все эти соединения должны отличаться высокой доступностью и отказоустойчивостью.

ОТСУТСТВИЕ ДОЛЖНЫХ МЕХАНИЗМОВ КОНТРОЛЯ ЗА МЕДИЦИНСКИМИ УСТРОЙСТВАМИ

Активное распространение медицинских устройств означает рост автоматизации процессов межмашинного взаимодействия (Machine-to-Machine, M2M) и взаимодействия машины и человека (Machine-to-People, M2P). С учётом развития этих процессов в условиях больниц, ИТ-подразделениям необходимо сосредоточиться не столько на обеспечении надёжных сетевых соединений, сколько на проактивном мониторинге и управлении такими системами как системы вызова медсестры, аппараты внутривенного вливания или системы телеметрии, где требуется постоянное взаимодействие с базовыми приложениями и персоналом медицинского учреждения. Для каждого нового медицинского устройства, появляющегося в сети, существует отдельный поток прикладных данных между этим устройством и более крупной системой.

Прозрачность информационного обмена медицинских устройств, их местоположения, производительности и характера их использования играют важную роль в оптимизации медицинской помощи. Кроме того, обеспечение прозрачности необходимо для оптимизации инфраструктуры и повышения эффективности краткосрочного и долгосрочного планирования при осуществлении автоматизации медицинских устройств и их поддержке.

- Инструменты Network analytics обеспечивают ИТ-подразделениям более полное представление о том, насколько хорошо настроены или адаптированы их новые системы или устройства, предоставляют базовые показатели производительности по каждому приложению, не важно, размещено ли это приложение в собственной инфраструктуре, или в облаке, и даже предоставляют информацию о периодах наименьшей нагрузки по подразделению для планирования окон управления изменениями (change control windows). Сетевая аналитика обеспечивает полученное на основе Больших данных полноценное понимание состояния и уровня использования больничной инфраструктуры.

НЕИЗВЕСТНЫЕ РИСКИ БЕЗОПАСНОСТИ И РИСКИ НЕСОБЛЮДЕНИЯ НОРМАТИВНЫХ ТРЕБОВАНИЙ

Это риски для всей сети, которые в конечном итоге сводятся к неавторизованным приложениям и устройствам, которые могут появляться в сети и обеспечивать неавторизованный доступ или осуществлять несанкционированное взаимодействие с другими устройствами. Поэтому ИТ-подразделениям необходимо постоянно следить за всеми устройствами и приложениями, которые работают в сети. Порой случается, что вследствие некорректно сконфигурированной DHCP службы в больнице перестаёт работать целая VLAN сеть. Инструменты для контроля сетевого доступа Network Access Control (NAC) позволяют автоматизировать конфигурирование сетевых настроек новых устройств и применение политик на основе правил в масштабах всей проводной и беспроводной инфраструктуры.

ЭКСПЛУАТАЦИОННАЯ ПОДДЕРЖКА В РЕЖИМЕ 24/7

Больницы работают круглосуточно – в таком же режиме и собственный глобальный центр технической поддержки Extreme Networks Global Technical Access Center (GTAC.). Круглосуточная 24/7 поддержка гарантирует оперативное решение любых вопросов, что позволяет обеспечивать непрерывную работу сети.

Extreme является единственной компанией во всей отрасли, которая использует архитектурный подход при выводе своей продукции на рынок – с начала научных исследований и разработок до выпуска продукта. В результате, все наши сетевые продукты – начиная с беспроводного оборудования и заканчивая проводными устройствами – управляются с помощью единого экрана, что упрощает процесс администрирования для ограниченных определёнными рамками ИТ-подразделений в учреждениях здравоохранения.

С более подробной информацией о решениях Extreme Networks для отрасли здравоохранения можно ознакомиться на сайте:
http://www.extremenetworks.com/healthcare

РЕШАЕМАЯ ЗАДАЧА	РЕКОМЕНДУЕМОЕ РЕШЕНИЕ	ПРЕДЛАГАЕМЫЕ НАМИ ПРЕИМУЩЕСТВА
Обеспечение стабильной работы существующей проводной и беспроводной инфраструктуры в условиях увеличения числа медицинских устройств	• ExtremeSwitching • Extreme Management Center	• Единая панель управления обеспечивает централизованное представление о работе всей унифицированной сети, а также инструменты для комплексного детализованного управления сетью.
Сквозное Wi-Fi подключение и магистральные каналы для обеспечения клинической деятельности и внутрибольничных коммуникаций	• ExtremeWireless • ExtremeSwitching	• Гибридные архитектуры внедрения (с мостовым соединением на уровне точек доступа или контроллера), единая учётная запись для упрощения процессов управления. Механизмы управления политиками на уровне приложений и устройств. Технология встроенных датчиков потока на основе специализированных микросхем на каждый порт, с поддержкой обработки до 3 млн. потоков в секунду.
Автоматизация процессов инициализации устройств с поддержкой средств аудита	• Extreme Access Control	• Автоматизированная и безопасная инициализация и управление медицинскими устройствами в проводных/беспроводных сетях.
Мониторинг критически важных устройств и приложений без агентов	• ExtremeAnalytics	• Мониторинг производительности и защищенности сетевых функций медицинских устройств без использования специальных агентов.
Поддержка сотрудников и консалтинг для обеспечения лучших в своём классе ИТ-сервисов	• Профессиональные сервисы • Обучение заказчика	• Сервисы Extreme, включая консультирование заказчиков на месте, услуги проектирования и внедрения, а также комплексная программа обучения пользователей.
Эксплуатационная поддержка в режиме 24/7	• Техническое обслуживание	• Глобальный центр поддержки (GTAC) обеспечивает техническую поддержку 24 часа в день, 365 дней в году. • Extreme Networks SupportNet позволяет вам выбирать тот уровень сервиса, который наилучшим образом отвечает требованиям вашей организации.

Extreme®
Connect Beyond the Network

http://www.extremenetworks.com/contact / Тел. +1-408-579-2800