BS2
Penki kontinentai group

Diebold Nixdorf

Комплексное решение для обеспечения безопасности устройств самообслуживания

Vynamic™ Security

25+
лет работы

7
дочерних компаний в Азербайджане, Эстонии, Грузии, Кыргызстане, Казахстане, Узбекистане, Латвии

80
стран мира, где BS/2 ведет свою деятельность

1500+
международных клиентов

90+
партнеров по всему миру

25+
лет партнерских отношений с Diebold Nixdorf

400+
профессионалов работают в компании

Компетентность как основа

Компания BS/2 входит в состав группы Penki kontinentai и предоставляет свои услуги в 80 странах мира, создавая программные решения, которые помогают автоматизировать и оптимизировать ваш бизнес.

Более 25 лет мы создаем специализированное инновационное программное обеспечение и технологические решения для банков, финансовых учреждений и предприятий розничной торговли. Мы предлагаем высококачественные ИТ-продукты для удовлетворения нужд ваших клиентов.

Услуги

- Разработка, продажа, установка программного обеспечения и его обслуживание.
- Мониторинг ИТ-инфраструктуры.
- Техническое обслуживание и ремонт банковского и другого оборудования.
- Консультации и обучение персонала.
- Поставка запасных частей.
- Аутсорсинг ИТ-услуг.
- Продажа оборудования для банков и сектора розничной торговли.

Сертификаты

ISO 27001, ISO 20000, ITIL V3, PCI PA- DSS.

Клиенты

- Банковские и финансовые учреждения.
- Предприятия розничной торговли.
- Автозаправочные станции.
- Почтовые службы.
- Компании сферы игорного бизнеса (казино, ипподромы и др.).

Международное признание

Diebold Nixdorf / Wincor Nixdorf

- Special Achievement Banking 2019.
- Special Achievement Banking 2007, 2013, 2014, 2017.
- Best Banking Solution 2012, 2013, 2016.
- Best Banking Service 2002, 2003, 2012, 2013, 2014.
- Most Innovative Software Solution 2004, 2005.
- Most Innovative Concept 2002, 2003, 2004, 2005.

ATM Industry Association

- Best ATM Security Technology 2002.

Конфедерации промышленников Литвы

- Приз за инновации 2016.
- Продукт года 2001, 2005, 2006, 2007, 2008, 2012, 2017.

Комплексная безопасность для устройств самообслуживания

В последние годы не только растет само количество атак на устройства самообслуживания (банкоматы и др.), но и появляются новые способы мошенничества. Логические атаки (то есть атаки с применением специального программного обеспечения) становятся все более сложными и изощренными, злоумышленники создают новое вредоносное ПО, придумывают устройства, которые способны считывать данные банковских карт, увеличивается и число атак с применением физической силы (взрывы, взлом корпуса, похищение банкоматов).

В контексте проблемы логических атак первостепенной задачей любой финансовой организации становится защита персональных данных клиентов и самой организации. В случае кражи такой информации банки несут не только финансовые, но и репутационные потери.

Основная причина распространенности логических атак – невысокий уровень базовой защиты терминалов. Операционные системы, установленные на банкоматах, имеют множество уязвимостей и требуют обновлений, при этом для некоторых операционных систем (например, для Windows XP)

обновления уже несколько лет не выпускаются. Свои уязвимости, через которые злоумышленники получают доступ к терминальным сетям, могут иметь и внутренние банковские сети. Как правило, они связаны с ошибками конфигурации или вызваны человеческим фактором.

Перед банками стоит важная задача - обеспечить комплексную всестороннюю защиту парка устройств самообслуживания.

Для защиты вашего терминального оборудования компания BS/2 предлагает комплексное решение, объединяющее современные программные продукты компаний BS/2 и Diebold Nixdorf.

Внедрение комплексного решения помогает:

• снизить потенциальную поверхность атаки на инфраструктуру самообслуживания за счет одновременной работы нескольких защитных модулей;

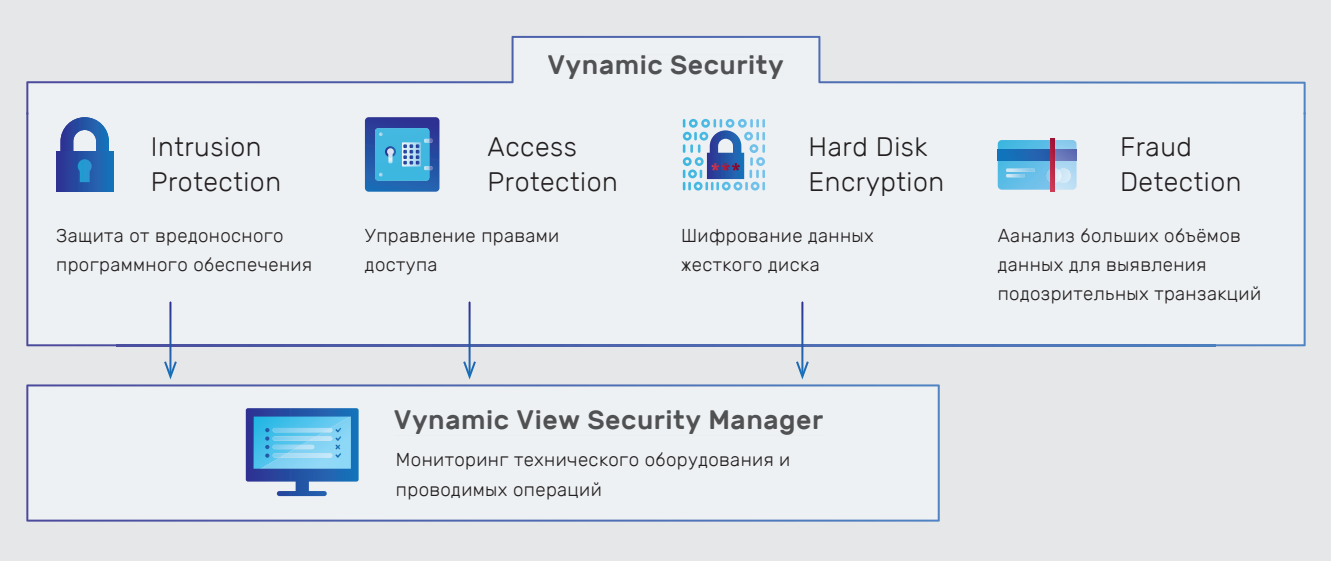
• снизить общую стоимость владения парком устройств за счет оптимизации рабочих процессов, связанных с обеспечением безопасности.

** Подробнее о решении ATMeye.iQ читайте в материалах BS/2 «Решение для видеонаблюдения и предотвращения мошенничества».*

Решение Vynamic Security

Для защиты терминальной сети от логических атак компания Diebold Nixdorf предлагает решение Vynamic Security. Это решение обеспечивает комплексный подход к защите устройств самообслуживания (банкоматов, платежных киосков, электронных кассиров и др.) от любых типов взлома, хакерских атак и других угроз.

Решение Vynamic Security состоит из четырех отдельных модулей.



Такая многоуровневая защита устройств самообслуживания помогает существенно снизить риски, связанные с мошенничеством. В случае взлома одного из уровней, остальные модули продолжают свою работу, что обеспечивает необходимую защиту терминала.

Модуль Intrusion protection

Сегодня для установки на банкомат вредоносного программного обеспечения злоумышленники используют уязвимости операционных систем устройств самообслуживания. Преступники делают это с помощью внешних носителей, которые подключают напрямую к терминалу через USB-порты. Банку сложно отследить и предотвратить такое подключение, однако его последствия наносят огромный ущерб финансам и репутации кредитной организации.

Модуль Intrusion Protection отвечает за защиту терминальной сети от проникновения всех видов вредоносных программ в компьютер банкомата.

Функциональное назначение модуля Intrusion Protection

Защита от вредоносного ПО

Многоуровневая система защиты делает невозможным установку вредоносного программного обеспечения на компьютер банкомата.

Технология белых списков

На терминале запускаются только разрешенные и проверенные процессы, соответствующие установленному набору правил (создание «песочницы»). Модуль отслеживает, чтобы в техническом оборудовании и приложениях банкомата не было несанкционированных изменений.

Контроль USB-портов

При попытках подключения сторонних USB-носителей модуль блокирует соответствующие порты на компьютере терминала, защищая тем самым от несанкционированного доступа.

Контроль целостности системы

Отслеживает любые попытки подмены файлов и несанкционированных изменений в системных настройках (в том числе BIOS) и нейтрализует потенциально опасные действия подозрительных приложений.

Защита сети и передачи данных

Ограничивает создание новых входящих и исходящих подключений на основании списка разрешенных IP-адресов и портов, а также дополнительно установленных правил.

Проактивный мониторинг

Мгновенно уведомляет оператора в случае потенциальной угрозы, создавая электронный журнал данных по инциденту.

Модуль Access Protection

Чтобы защитить компьютер банкомата от воздействия вредоносных программ банки сосредотачивают свои усилия на внешних угрозах, однако этого бывает недостаточно. Финансовые организации также должны защитить свои системы от несанкционированного доступа и утечки конфиденциальных данных.

Модуль Access Protection защищает компьютер АТМ в случае неправомерного использования доступа и контролирует действия пользователей в системе. Решение соответствует международным стандартам, правилам и политикам, что снижает риски ошибочного или преступного проникновения в систему.

Функциональное назначение модуля Access Protection

Ограничение прав доступа

Обеспечивает эффективный контроль доступа при помощи управления правами отдельных учетных записей и групп пользователей, а также возможностью логирования всех действий.

Контроль уязвимостей операционной системы

Отключает и удаляет необязательные для работы терминала компоненты операционной системы, которые могут быть использованы злоумышленниками в качестве точки атаки.

Оптимизация процедуры авторизации

Стандартная процедура авторизации администратора терминальной сети расширяется специальной процедурой шифрования логина и пароля.

Управление работой файрвола

Управляет настройками файрвола для контроля входящих и исходящих данных на основании установленных правил.

Модуль Hard Disk Encryption

Многие финансовые учреждения используют шифрование во время передачи данных, но упускают из виду необходимость шифровать информацию, которая хранится на жестком диске компьютера терминала. Кража незашифрованного жесткого диска позволяет преступникам получить доступ к его данным, заразить его вредоносным ПО и установить на другом устройстве самообслуживания.

Модуль Hard Disk Encryption предотвращает несанкционированный доступ к конфиденциальным данным, хранящимся на жестком диске, даже когда банкомат выключен. Данные хранятся в зашифрованном виде, их нельзя прочитать или скопировать без уникальных ключей. Модуль использует определенные параметры программно-аппаратной среды банкомата – это значит, что процедура дешифрования возможна только на устройстве, использующем заданный жесткий диск.

Функциональное назначение модуля Hard Disk Encryption

Защита данных

Шифрование данных на жестком диске обеспечивает их безопасность даже в случае, когда банкомат выключен (транспортируется или находится на ремонте).

Надежное шифрование

По стандартам, соответствующим требованиям PCI, шифрует все данные, хранящиеся на жестком диске, а также данные, передаваемые с устройства или на него. Для шифрования данных во время передачи использует стандарт AES (256-бит).

Защита доступа

Блокирует доступ к данным на жестком диске, если дешифрование не соответствует заданным параметрам, или предпринимаются попытки внешней модификации операционной системы.

Контроль работоспособности жесткого диска

Работа жесткого диска обеспечивается исключительно в рамках заданной программно-аппаратной среды устройства самообслуживания, что позволяет обеспечить целостность системы.

Модуль Fraud Detection

Киберпреступники постоянно совершенствуют свои методы, придумывают новые виды атак – это требует все более совершенных решений для обеспечения безопасности. Стандартные меры, основанные на заданных правилах и предусмотренных моделях поведения, не всегда могут защитить от новых угроз.

Отдельный антифрод-модуль Fraud Detection позволяет обрабатывать большие массивы транзакционных данных для выявления подозрительных операций на устройствах самообслуживания, а также обеспечивает проактивную защиту технической инфраструктуры кредитного учреждения или другой организации.

Функциональное назначение модуля Fraud Detection

Поиск ранее неизвестных уязвимостей

Находит потенциально уязвимые места в инфраструктуре самообслуживания и системе управления терминальным парком и составляет список превентивных действий.

Отслеживание аномалий в работе устройств

Распознает отклонения в привычной модели поведения банкоматов и изменения в учетных записях, предоставляя сотрудникам банка возможность принять меры для предотвращения атак на терминалы уже при первых признаках аномальной активности.

Борьба с отмыванием денег

Проводит мониторинг финансовых транзакций на устройствах самообслуживания с целью выявить подозрительные операции, потенциальной целью которых может быть отмывание денежных средств или финансирование незаконной деятельности.

Автоматизация оценки рисков

Автоматизированная (чтобы исключить человеческий фактор) обработка поступающей в систему информации с последующим формированием списка необходимых действий для банковского персонала.

Модуль Vynamic View Security Manager

Комплексная стратегия по обеспечению безопасности терминальной сети от различных видов атак (как физических, так и логических) не сможет обойтись без централизации процессов администрирования и мониторинга работы технического оборудования и проводимых транзакций.

Для удобного мониторинга всех событий, связанных с обеспечением безопасности устройств самообслуживания, банковским и другим организациям предлагается отдельный модуль Security Manager, являющийся частью решения Vynamic View.

Функциональное назначение модуля Security Manager

Специализированный мониторинг безопасности

Отслеживает статусы безопасности каждого подключенного устройства самообслуживания и передает проактивные уведомления об угрозах ответственному персоналу для детального разбора и оперативного принятия решений.

Удаленное управление терминалами

Предоставляет возможность удаленного включения, выключения и перезагрузки терминалов, их периферийных устройств и камер видеонаблюдения, а также возможность активации и деактивации сервисного режима для каждого подключенного терминала.

Оптимизация управления терминальной сетью

Группирует устройства самообслуживания и создает необходимые иерархические связи для более удобного мониторинга и управления актуальным состоянием терминалов в аспекте обеспечения безопасности.

Установка и обновление ПО

Обеспечивает возможность централизованной и дистанционной установки, обновления и настройки необходимого ПО для обеспечения более высокого уровня защиты устройств самообслуживания.

Преимущества решения

Многоуровневая защита

Архитектурно решение Vynamic Security содержит несколько уровней защиты. В случае падения одного из уровней, остальные модули продолжают работать, благодаря чему устройство самообслуживания будет надежно защищено.

Работа с терминалами разных производителей

Vynamic Security является мультивендорным решением, которое может быть внедрено для защиты устройств разных производителей. Это позволяет унифицировать процессы обслуживания терминалов и снизить итоговую стоимость владения терминальной сетью.

Комплексный подход

Vynamic Security использует прогрессивные методики защиты ИТ-инфраструктуры, такие как создание списков доверенного программного обеспечения и ограниченной среды для безопасного исполнения каждого из разрешенных процессов. Все это позволяет системно подходить к обеспечению безопасности терминальной сети.

Простота эксплуатации

Развернутое программное обеспечение не требует постоянного обновления антивирусных баз и сканирования системы. Таким образом, решение существенно упрощает процессы администрирования терминальной сети.

Соответствие стандартам безопасности

Решение работает с операционными системами Windows 7, Windows 10, полностью соответствует стандартам безопасности PCI DSS и может быть адаптировано к требованиям различных регулирующих органов. Также решение позволяет продлить срок эксплуатации оборудования со старыми версиями ОС.

Гибкая лицензионная политика и широкие интеграционные возможности

Решение может быть адаптировано под различные потребности банка. Гибкая лицензионная политика позволяет приобрести отдельные модули в необходимом для бизнеса количестве. Программный комплекс Vynamic Security совместим с другими решениями по обеспечению безопасности и легко интегрируется в инфраструктуру финансовой организации.

Связанные продукты

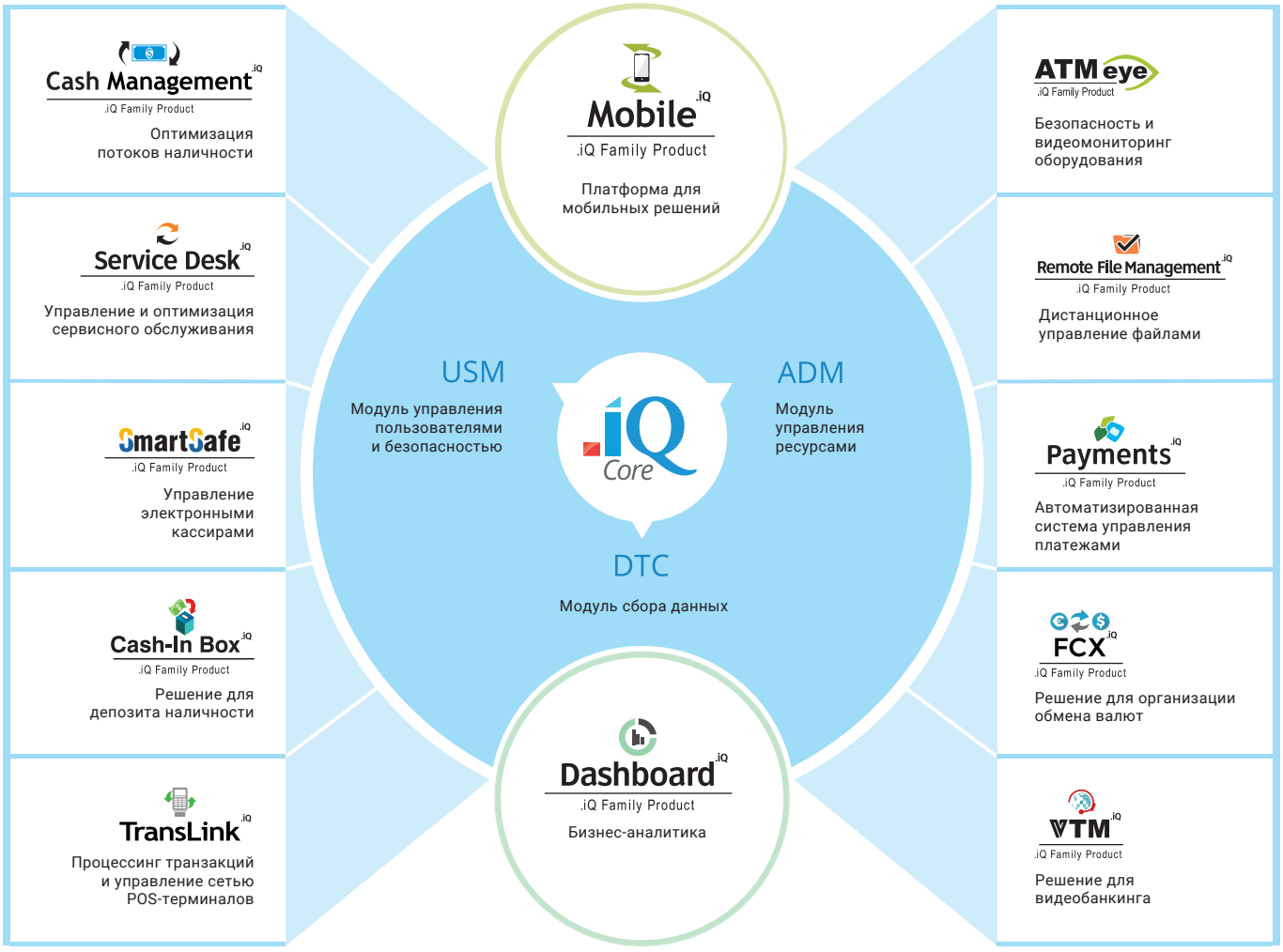
ATMeye.iQ - программно-аппаратное решение нового поколения, предназначенное для мониторинга подозрительных действий у устройств самообслуживания в режиме реального времени и обеспечения своевременной реакции на неправомерные действия.

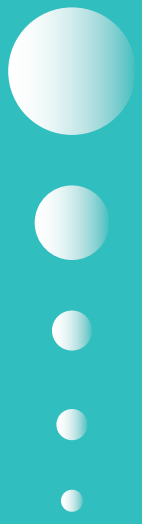
FRN.iQ - система распознавания лица для расширения возможностей по обеспечению безопасности при авторизации пользователей, проведении платежей и других операций.

Remote File Management.iQ — продукт семейства .iQ, представляющий собой систему для безопасной передачи файлов между удаленным устройством самообслуживания и рабочим местом администратора или сервером сбора данных.

Vynamic™ View — программный комплекс, предназначенный для мониторинга и управления сетями банковских устройств самообслуживания. Решение предоставляет функции получения информации с устройств, дистанционного администрирования, диагностики и генерации отчетов.

Семейство продуктов .iQ





ЗАО Penkių kontinentų bankinės technologijos
Ул. Карейвю 2, LT-08248 Вильнюс, Литва
Эл. почта: info@bs2.lt | Тел.: +370 5 266 45 95 | www.bs2.lt