NETWELL

paloalto NETWORKS

Palo Alto Networks

Справочное руководство

Нажмите для просмотра

STRATA БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

PRISMA БЕЗОПАСНОСТЬ ОБЛАКА

CORTEX БЕЗОПАСНОСТЬ БУДУЩЕГО

Факты и цифры

Болевые точки отдельных отраслей

БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

STRATA

Предотвращение угроз - Межсетевой экран нового поколения

Защита предприятия начинается с межсетевого экрана (МСЭ).

Одно из лучших в отрасли семейств МСЭ нового поколения Palo Alto Networks определяет стандарты сетевой безопасности на протяжении уже 15 лет и продолжает стремиться к новым вершинам. Комплексные средства защиты от эксплойтов, вредоносного ПО и C&C атак помогут компании устранить известные угрозы на каждом этапе атаки. МСЭ Palo Alto Networks остается в лидерах Магического квадранта Gartner уже восемь лет подряд.

Аппаратные устройства

Серия PA

Весь ассортимент аппаратных устройств МСЭ нового поколения Palo Alto Networks можно легко развернуть в сети вашей организации, ведь они были специально разработаны для удобства пользователей, со встроенными возможностями автоматизации и интеграции.

Виртуализированные МСЭ

Серия VM

Виртуализированные МСЭ нового поколения Palo Alto Networks защищают частные и публичные облачные среды с помощью сегментации и предотвращения угроз

МСЭ с поддержкой 5G

Серия K2

МСЭ нового поколения Palo Alto Networks серии K2 с поддержкой 5G разработаны специально для мобильных сетей поставщиков услуг.

УТОЧНЯЮЩИЕ ВОПРОСЫ

STRATA

МСЭ

- Как вы защищаете вашу сеть от известных угроз?
- Есть ли у вас решение для мониторинга внутреннего трафика?
- Основаны ли правила вашего МСЭ на IP-адресах и портах?
- Сложно ли откалибровать ваши бизнес-потребности, используя эти параметры?
- Если бы я мог показать вам, как упорядочить ваши правила с учетом контекста и специфики вашего бизнеса, вам было бы это интересно?
- Устраивает ли вас текущее управление защитой облаков, филиалов и мобильных сотрудников? Происходит ли оно без проблем и с равной поддержкой всех функциональных возможностей?
- Как вы обеспечиваете слаженную и синхронизированную работу всех инструментов безопасности для предотвращения угроз?
- Что происходит, когда вам нужно устранить неполадки по заявке или расследовать угрозу на разных устройствах?
- Сейчас часто можно услышать, что атаки стали более изощренными. Как это отразилось на вашей команде?
- У вас есть проблемы с укомплектованностью или наймом специалистов ИБ? (Совет: посмотрите открытые вакансии на сайте компании)
- Как в ваших инструментах безопасности применяется автоматизация, чтобы сократить рутинную работу и задачи, выполняемые вручную?

УТОЧНЯЮЩИЕ ВОПРОСЫ

STRATA

URL FILTERING

С помощью URL Filtering можно безопасно использовать веб-ресурсы для решения бизнес-задач. Помимо базовой фильтрации веб-контента, можно еще выявлять угрозы с помощью уникального сочетания статического анализа и машинного обучения.

- Какие системы вы внедряете для автоматического выявления и предотвращения веб-угроз?
- Расшифровываете ли вы свой веб-трафик? У вас есть возможность выборочно расшифровывать отдельные веб-сайты?
- Работают ли ваши текущие средства веб-безопасности совместно с МСЭ, чтобы выборочно расшифровывать SSL-трафик или предотвращать кражи учетных данных в режиме реального времени?
- Работают ли они совместно с системой предотвращения вторжений (IPS) для обеспечения усиленной защиты от угроз в динамическом режиме?
- Как затронули вашу организацию фишинговые или целевые фишинговые атаки в прошлом году?
- Как вы защищаете пользователей от этих угроз?
- Сколько продуктов сетевой безопасности вы используете в настоящее время?
- Сколько времени вы тратите на интеграцию этих продуктов?
- На какие задачи вы хотели бы, чтобы у ваших ИБ-специалистов было больше времени?

УТОЧНЯЮЩИЕ ВОПРОСЫ

STRATA

DNS SECURITY

Новую подписку можно добавить в МСЭ нового поколения вместе с TP, WF, GP, URL и т. д. Сервис DNS Security определяет потенциально вредоносные домены, созданные на основе алгоритма генерации доменов, блокирует их, а также с помощью анализа на базе машинного обучения быстро обнаруживает кражу данных через DNS-туннелирование.

- Вы можете заблокировать миллионы вредоносных доменов одновременно в режиме реального времени?
- Вы проверяете DNS на предмет кражи данных? Если бы кто-то начал извлекать данные через DNS, вы бы об этом узнали?
- Какие инструменты вы сейчас используете для защиты DNS-трафика?
- На какие задачи вы хотели бы, чтобы у ваших ИБ-специалистов было больше времени?

УТОЧНЯЮЩИЕ ВОПРОСЫ

STRATA

WILDFIRE

Неизвестные атаки можно обнаруживать и отражать автоматически. Выявляйте новые угрозы с помощью расширенного анализа, машинного обучения и общедоступной аналитики угроз – автоматизированные средства защиты помогут вам быть на шаг впереди злоумышленников.

- Сколько целенаправленных атак на вашу организацию вы обнаруживаете?
- Как выстроен текущий процесс обнаружения и блокировки неизвестных атак?
- Достаточно ли у вас времени и ресурсов для борьбы с этими угрозами?
- Как вы получаете доступ к актуальным данным об угрозах?
- Есть ли у вас команда, чтобы анализировать эти данные об угрозах?
- Насколько вы уверены в том, что фиксируете все направленные на вас угрозы?
- Сколько этапов нужно для блокировки неизвестной угрозы?
- Сколько инструментов вы используете от обнаружения угрозы до ее предотвращения?

УТОЧНЯЮЩИЕ ВОПРОСЫ

GLOBAL PROTECT

Каждый раз когда пользователи выходят из здания со своими ноутбуками или смартфонами, они покидают границы корпоративного МСЭ и соответствующих политик по защите пользователей и сети. Решение GlobalProtect™ поможет устранить проблемы безопасности, связанные с нахождением пользователей вне зоны МСЭ, т.к. распространяет действие тех же политик на основе МСЭ нового поколения, что применяются в пределах физического периметра, на всех пользователей независимо от их местонахождения.

- Как вы защищаете своих сотрудников, когда они работают из дома или вне офиса?
- У вас много мобильных сотрудников?

УТОЧНЯЮЩИЕ ВОПРОСЫ

СИСТЕМА УПРАВЛЕНИЯ PANORAMA

Решение Panorama упрощает структуру сети, упорядочивая устройства в логические и функциональные группы, а также облегчает управление сетью благодаря простому контролю над глобальными политиками и сокращает время нахождения угроз в сети: собранные данные позволяют сразу принять меры, выделить важную информацию и определить приоритет реагирования.

- Как обеспечить согласованность политик МСЭ в корпоративном масштабе?
- Как обеспечить согласованность политик МСЭ, предотвращения угроз, фильтрации веб-контента и файловых политик во всех инструментах сетевой безопасности?
- Вы уверены, что ваши политики МСЭ отражают ваши бизнес-политики?
- Устраивает ли вас текущее управление защитой облаков, филиалов и мобильных сотрудников? Происходит ли оно без проблем и с равной поддержкой всех функциональных возможностей?
- Вы можете получить единую картину происходящего в локальной инфраструктуре и в SaaS-приложениях, к которым обращаются ваши пользователи?

УТОЧНЯЮЩИЕ ВОПРОСЫ

STRATA

SD-WAN

Программно-определяемая глобальная вычислительная сеть (ГВС), или SD-WAN, – это виртуализированный сервис, который соединяет и расширяет корпоративные сети на расстоянии. SD-WAN отслеживает производительность подключений к ГВС и управляет трафиком, чтобы сохранить высокую скорость и оптимизировать подключение. Средства защиты и SD-WAN должны быть единым целым. Когда система безопасности встроена в SD-WAN по умолчанию, вы можете подключать свои филиалы, не создавая при этом угрозы для безопасности.

- Как вы оптимизируете «среднюю и последнюю мили» вашей сети, чтобы обеспечить оптимальные возможности для работы конечных пользователей?
- Планируете ли вы расширение регионального присутствия, открытие новых филиалов или слияния?
- Что изменилось бы, если бы вы смогли открывать филиалы быстрее?
- Насколько важно для вас самостоятельно конфигурировать межсетевое соединение и управлять им?
- Как вы планируете интегрировать защиту SD-WAN с остальной инфраструктурой безопасности?
- Начата ли в вашей организации инициатива по консолидации поставщиков и упрощению инфраструктуры безопасности?

УТОЧНЯЮЩИЕ ВОПРОСЫ

STRATA™

AUTOFOCUS THREAT INTELLIGENCE

Служба анализа угроз AutoFocus™ от Palo Alto Networks меняет подход ИБ-команд к защите организации от уникальных целенаправленных атак. Эта облачная служба безопасности предоставляет информацию, аналитику и контекст, чтобы можно было лучше понять, какие атаки требуют немедленного реагирования, а также сделать индикаторы более полезными с практической точки зрения и предотвратить атаки в будущем.

- Нужно ли вашим ИБ-командам быстро определять приоритеты и реагировать на атаки?
- Ваши текущие методы сложны и требуют ручной работы?
- Нужно ли вашим ИБ-командам быстро определять приоритеты и реагировать на атаки?
- Ваши текущие методы сложны и требуют ручной работы?
- Насколько вашему бизнесу важна информация об угрозах?

УТОЧНЯЮЩИЕ ВОПРОСЫ

STRATA

ИНТЕРНЕТ ВЕЩЕЙ (IOT), СЕРВИС ZINGBOX

Облачный сервис Zingbox использует технологии искусственного интеллекта и машинного обучения, чтобы помочь организациям обнаружить, идентифицировать, защитить и оптимизировать неуправляемые устройства. Усилив свой портфель сервисом Zingbox, компания Palo Alto Networks теперь предлагает защиту IoT-сред, а также лучшую в своем классе визуализацию и автоматизированное устранение угроз в режиме реального времени.

- Трудно ли вам управлять жизненным циклом ваших многочисленных IoT-устройств?
- Можете ли вы решить эту проблему и распространить лучшие ИТ-практики и на IoT-устройства?

УТОЧНЯЮЩИЕ ВОПРОСЫ

PRISMA

Prisma Access

Prisma Access – это пограничный сервис безопасного доступа (SASE), который позволяет мобильным пользователям и филиалам получить безопасный доступ к облаку с помощью масштабируемой архитектуры ИБ, предоставляемой из облака. Это значит, что вам не нужно беспокоиться о масштабировании и развертывании МСЭ в каждом филиале. Удаленный доступ через VPN непредназначен для поддержки облачных приложений с Prisma Access. Решение использует облачную инфраструктуру, чтобы подключить пользователей к облачным приложениям и ЦОД.

- План развития для конечного пользователя? Обеспечиваете ли вы целостную защиту мобильных пользователей и сотрудников филиалов?
- Работаете ли вы с большим количеством удаленных пользователей или филиалов?
- Вы хотели бы, чтобы оборудование занимало меньше места?

Prisma Cloud

Prisma Cloud (ранее Redlock и Evident) – это решение для комплексной защиты от угроз, управления и соблюдения требований регуляторов, которое визуализирует и защищает данные и рабочие нагрузки в облаке Google, AWS и Microsoft Azure, тем самым позволяя отказаться от частного облака/ЦОД.

- Вы знаете, что именно вы храните в облаке и соблюдаете ли вы требования по защите данных (регламент GDPR)?
- Вы используете публичное облако?
- Безопасность контейнеров: могут ли команды SecOps видеть, что происходит у команд DevOps?
- Вы можете обеспечить целостную безопасность и в облаке, и в сети?
- Вы уверены, что соответствуете требованиям регуляторов и применяете согласованные политики безопасности при использовании публичного облака?

УТОЧНЯЮЩИЕ ВОПРОСЫ

PRISMA

Prisma SaaS

Prisma SaaS (ранее Aperture) закрывает потребности вашего брокера безопасного доступа в облако (CASB), предотвращает потерю данных и сбои в работе благодаря подробной визуализации приложений, мониторингу и защите от угроз. Защита на лету и на базе API-интерфейса помогает минимизировать облачные риски, которые могут привести к нарушениям.

- Как вы управляете данными, к которым ваши пользователи получают доступ через SaaS-приложения? Как вы контролируете использование несанкционированных приложений?
- Вы можете контролировать доступ с неуправляемых устройств к таким
- SaaS-приложениям как Office 365, Dropbox и SFDC?

Серия VM

МСЭ нового поколения серии VM позволяют безопасно трансформировать традиционные ЦОД в программно-определяемые благодаря тесной интеграции с партнерами по инфраструктуре ЦОД. МСЭ нового поколения серии VM упрощают рабочие процессы безопасности за счет автоматизации и успешно предотвращают атаки с боковым смещением в ЦОД.

- У вас есть проекты по микросегментации/сегментации сетей?
- У вас есть проекты по созданию программно-определяемых сетей в ЦОД (с VMware NSX, Cisco ACI, Nuage VSP, Juniper Contrail, BigSwitch BIG-IP или OpenStack)?
- Вам нужна визуализация внутреннего трафика в ЦОД и публичном облаке?

УТОЧНЯЮЩИЕ ВОПРОСЫ

CORTEX

Cortex XDR

Избавьтесь от разрозненных решений для обнаружения и реагирования и объедините данные оконечных устройств, облака и сети, чтобы отразить сложные атаки. Решение строит профиль конкретной машины, чтобы изучить и понять особенности ее функционирования.

Защита оконечных устройств не имеет себе равных по широте и глубине охвата:

- Блокировка вредоносного ПО, эксплойтов и программ-вымогателей на основе наблюдений за методами и паттернами атак.
- Машинное обучение и искусственный интеллект помогают автоматически обнаруживать сложные атаки и реагировать на них.
- Включает в себя сервис WildFire® по противодействию вредоносному ПО для более широкого охвата и высокой точности обнаружения.
- Технология Cortex XDR™ по обнаружению и реагированию ускоряет расстановку приоритетов и реагирование на инциденты, автоматически предоставляя полную картину по каждой угрозе и ее первопричине.
- Координация принимаемых мер с работой команд сетевой и облачной безопасности для успешного предотвращения атак.
- Единый нересурсоемкий агент для защиты и реагирования.
- Защита оконечных устройств в режиме онлайн и офлайн, с подключением к сети и без него.

УТОЧНЯЮЩИЕ ВОПРОСЫ

CORTEX

Cortex XDR

- Как ваши ИБ-аналитики расследуют инциденты и ищут их первопричины?
- Как они контролируют наличие всей полноты картины и находят решение?
- Используете ли вы в настоящее время защиту оконечных устройств/антивирус нового поколения?
- Как вы сейчас обнаруживаете угрозы и реагируете на них?
- Чем вы пользуетесь для обнаружения внешнего или внутреннего злоумышленника в вашей сети?
- Какой процент оповещений системы безопасности вы можете сейчас расследовать?
- Сколько времени уходит на расстановку приоритетов и расследование оповещений?
- Сколько оповещений вы получаете в неделю?
- Как выглядит стандартная процедура расследования оповещения?
- Какие у вас главные трудности при обеспечении безопасности?
- У вас достаточно сотрудников для обработки всех оповещений ИБ?
- У вас есть в работе проекты по обнаружению угроз и реагированию на них на оконечных устройствах (EDR) или анализу сетевого трафика?
- Вы проводите упреждающий поиск угроз?
- У вас есть выделенная команда ИБ-специалистов?
- Как вы обрабатываете оповещения и проводите расследования?
- Сколько человек работает в вашей команде ИБ?
- Рекомендация: Cortex XDR – не лучший вариант для организаций, у которых нет выделенной команды для расследования оповещений. Обратитесь к партнеру, который предлагает управляемое обнаружение и реагирование на угрозы.
- Как вы относитесь к защите, доставляемой из облака?

УТОЧНЯЮЩИЕ ВОПРОСЫ CORTEX

Cortex Data Lake

Платформа обеспечивает постоянную защиту на основе ИИ, предназначена для работы в больших масштабах и предлагается как облачный сервис. Решение Cortex Data Lake легко агрегирует все данные и аналитику по глобальным угрозам по всей инфраструктуре безопасности.

Продукты Palo Alto Networks отправляют подробные данные о сети, оконечных устройствах и облаке в Data Lake. Такой способ доступен решениям Palo Alto Networks и сторонним приложениям через Cortex Hub.

Cortex XSOAR

Платформа оркестрации безопасности, автоматизации и реагирования (SOARплатформа) сочетает полное управление инцидентами и умную автоматизацию, которые находятся в распоряжении команды ИБ на протяжении всего жизненного цикла инцидента. Цель платформы – разгрузить сотрудников центра обеспечения безопасности (SOC), взяв на себя обработку части оповещений, и повысить продуктивность аналитиков, тем самым улучшив эффективность защиты.

- Как вы автоматизируете реагирование на инциденты? Ваш центр SOC занят нескончаемым потоком оповещений?

ФАКТЫ И ЦИФРЫ

Palo Alto Networks и Prisma Public Cloud

Palo Alto Networks

- 85 компаний из списка Fortune 100 пользуются нашими продуктами и доверяют нам.
- 8 лет подряд наш МСЭ возглавляет Магический квадрант Gartner.
- 2 года подряд он занимает верхние строчки в рейтингах лучших решений на основе принципа нулевого доверия.
- 65 000 заказчиков в более чем 150 странах.
- 80% утечек данных происходит по вине тех, кого вы сами пустили внутрь.
- 100% попыток обхода защиты пресечено, за что получен наивысший балл за эффективность ИБ.
- Количество устройств, подключенных к интернету, очень быстро растет;по прогнозам компании IDC, к 2025 году их число достигнет 41,6 млрд.
- По мере того, как ваши данные распространяются все дальше, появляется все больше возможностей для атак; старыми системами безопасности становится слишком неудобно управлять.
- Наша архитектура, основанная на превентивных мерах, упрощает структуру системы безопасности вашей организации благодаря интегрированному решению.
- Предполагается, что к 2021 году будет не хватать около 3,5 миллионов ИБ-специалистов.

Prisma Public Cloud

- К 2022 году на 60% серверных рабочих нагрузок будет использоваться контроль приложений вместо антивируса, что на 35% больше по сравнению с 2018 годом.
- К концу 2020 года из-за незрелости уже используемых платформ защиты облачных рабочих нагрузок (CWPP) 70% организаций будут использовать другие платформы CWPP для защиты контейнеров и бессерверных систем, отличные от тех, что они используют для защиты виртуальных машин.

ФАКТЫ И ЦИФРЫ

Расширенная система обнаружения и устранения угроз и Межсетевой экран

Расширенная система обнаружения и устранения угроз

- Обычно организациям требуется 197 дней для выявления и 69 дней для устранения угроз.
- Для обеспечения безопасности своих сетей многие организации используют точечные инструменты: обнаружение и реагирование на угрозы на оконечных устройствах (EDR), анализ сетевого трафика (NTA), аналитика поведения пользователей и объектов (UEBA) и многие другие, причем крупные предприятия часто используют продукты от 50, 60 или даже 70 разных поставщиков. Вместо того, чтобы согласованно отражать атаки, каждый из этих инструментов генерирует тьму оповещений в уникальном формате своего собственного журнала. В действительности, организации получают 174 000 оповещений в неделю, но расследовать успевают только 7% из них.
- Сокращение объема оповещений в 50 раз, ускорение расследований в 8 раз и снижение затрат на 44% (В 50 раз меньше оповещений: инновационный интеллектуальный механизм обработки инцидентов группирует оповещения, связанные с одним и тем же инцидентом, и помогает справиться с этой информационной лавиной.
- Расследование в восемь раз быстрее: быстро подтверждайте наличие угрозы, имея перед глазами полную картину атак и анализ первопричин. Максимальная рентабельность: используйте существующую инфраструктуру для сбора и контроля данных, чтобы снизить затраты на 44%).

ФАКТЫ И ЦИФРЫ

Межсетевой экран и Расширенная система обнаружения и устранения угроз

Межсетевой экран

- Согласно Gartner, к концу 2023 года причиной 99% несанкционированных проникновений через МСЭ будет их ошибочная конфигурация, а не их дефекты.
- 100% попыток обхода защиты пресечено, за что получен наивысший балл за эффективность ИБ.
- Благодаря новым прикладным технологиям релизы ПО теперь выходят несколько раз в день, а не пару раз в год как раньше. В новые приложения могут быть встроены компоненты, работающие одновременно в локальной сети, в облаке и в гибридном облаке.
- Разработанная нами технология помогла компаниям значительно сократить беспорядочное разрастание сети.
- Как правило, мы помогаем заказчикам сэкономить 65% капитальных и 80% операционных затрат.

ФАКТЫ И ЦИФРЫ

XSOAR и SASE

Расширенная платформа оркестрации безопасности, автоматизации и реагирования (XSOAR)

- В среднем ИБ-команды просматривают 12 000 оповещений в неделю, в том числе очень много ложных срабатываний.
- ИБ-аналитиков сложно найти, обучить и удержать. Подготовка новых специалистов занимает 8 месяцев, а 25% из них уходят в течение 2 лет.
- Более чем у 50% опрошенных ИБ-команд либо нет процессов, либо они редко обновляются. В результате возникает больше ошибок, качество разнится и не соблюдаются требования регуляторов.
- Компания Esri использовала сценарии Demisto и сократила объем оповещений на 95%.
- Заказчик, занимающийся разработкой приложений, смог сократить среднее время завершения процесса с 4 часов до 10 минут с помощью сценария Demisto.

ФАКТЫ И ЦИФРЫ

XSOAR и SASE

Пограничный сервис безопасного доступа (SASE)

- К 2023 году 20% предприятий будут использовать защищенный веб-шлюз, брокер безопасного доступа в облако, сетевой доступ по принципу нулевого доверия и МСЭ как услугу в филиалах – и все это от одного поставщика, тогда как в 2019 году таких было меньше 5%.
- К 2024 году у минимум 40% предприятий будет четкая стратегия по внедрению SASE-решений, тогда как в 2018 году таких было меньше 1%.
- К 2025 году как минимум один из ведущих поставщиков IaaS будет предлагать конкурентоспособный набор SASE-возможностей.
- Гибкость: С облачной инфраструктурой можно внедрять и предоставлять такие услуги безопасности, как предотвращение угроз, фильтрация веб-контента, песочница, DNS Security, предотвращение утечки данных и кражи учетных данных, а также политики МСЭ нового поколения.
- Экономичность: Использование единой платформы вместо покупки и управления несколькими точечными продуктами значительно сократит расходы и сэкономит ИТ-ресурсы.
- Упрощение: Можно упростить ИТ-инфраструктуру, сократив до минимума количество ИБ-продуктов, которые ИТ-команда должна использовать, обновлятьи поддерживать, и консолидировав стек ИБ-решений в облачную сервисную модель сетевой безопасности.

БОЛЕВЫЕ ТОЧКИ ОТДЕЛЬНЫХ ОТРАСЛЕЙ

Финансовый сектор

- Поддержка технологических инноваций, например, возможности внесения чеков на счет с помощью мобильного устройства, многоканального обслуживания клиентов, использования социальных сетей, а также более широкого спектра ИТ-трендов, таких как виртуализация ЦОД, облачные вычисления и интернет как глобальная вычислительная сеть (ГВС).
- Обеспечение безопасного доступа к финансовым данным клиентов из бесчисленного количества мест, включая банковские отделения для розничных клиентов, объекты партнеров, компьютеры клиентов и мобильные устройства.
- Соответствие требованиям регуляторов: Службы регулирования отрасли финансовых услуг (FINRA), Комиссии по ценным бумагам и биржам (SEC), Управления валютного контроля (OCC), Европейской службы банковского надзора (EBA), Денежно-кредитного управления Сингапура (MAS), а также другим нормативным актам в отношении финансовых операций и конфиденциальных данных клиентов.
- Директива MiFID II (Директива Евросоюза «О рынках финансовых инструментов») = сегментация клиентских данных – это обычно хороший стимул для компаний использовать публичное облако.
- Традиционным финансовым организациям приходится внедрять инновации и повышать гибкость из-за конкуренции с финтех-компаниями, которые отнимают гораздо большую долю рынка, чем когда-либо раньше.
- Стандарты банковского обслуживания в открытом формате (open banking), установленные Управлением по защите конкуренции и рынкам Великобритании, требуют, чтобы банковские приложения были интегрированы друг с другом.
- Общая тенденция по масштабному агрегированию аналитики на базе клиентских данных для увеличения дополнительных/перекрестных продаж (не только в финансовой отрасли).

БОЛЕВЫЕ ТОЧКИ ОТДЕЛЬНЫХ ОТРАСЛЕЙ

Здравоохранение

- Соблюдение требований регуляторов: Закона об ответственности и переносе данных о страховании здоровья граждан (HIPAA), Стандарта безопасности платежных карт и других нормативных актов в отношении данных пациентов, медицинского оборудования и операций с кредитными картами.
- Обеспечение безопасного доступа к данным пациентов из бесчисленного количества мест, включая больницы, клиники, страховые компании, кабинеты врачей частной практики, филиалы, мобильные устройства и т. д.
- Обнаружение и блокирование угроз; расследование ИБ-инцидентов.
- Защита компьютеров с ОС Windows, на которые сложно установить патчи.

Право

- Защита данных.
- Удаленные сотрудники/большой периметр.Сами клиенты оказывают сильное влияние на технологический стек/безопасность (у них нет возможности использовать облако и т.д.).

Высшее образование

- Фишинговые атаки/социальная инженерия.
- Сотрудники не соблюдают процедуры.
- Использование легитимных учетных записей без ведома университета.
- Программы-вымогатели.
- Потеря контроля над данными в облаке.
- Отсутствие связной картины.

Ритейл

- Стандарт безопасности платежных карт/платежи.
- Единое представление о клиенте – разрозненные данные.
- Омниканальность: единая система коммуникации с клиентом.
- Внедрение Big Data через магазин/сайт/телефон.
- Использование технологий в торговом зале для оптимизации розничных продаж.

БОЛЕВЫЕ ТОЧКИ ОТДЕЛЬНЫХ ОТРАСЛЕЙ

Промышленность

- Индустрия 4.0: цифровизация промышленности, например, высокая степень автоматизации на всех этапах производственного цикла (e2e).
- Роботизированное производство и управление складом.
- Слияние центра SOC с центром SOC по системам оперативного контроля (например, на заводе).
- Физическая изоляция сети завода от остальной сети постепенно сходит на нет из-за того, что машинам нужно подключение к интернету, а ERP-платформам нужен доступ.
- Контролируемое обслуживание: на производстве машины передают телеметрические данные вендорам для контроля, в результате снижается риск простоя, но при этом возникают новые риски.
- Ритейл.
- Стандарт безопасности платежных карт/платежи.
- Единое представление о клиенте – разрозненные данные.
- Омниканальность: единая система коммуникации с клиентом через магазин/сайт/телефон.
- Внедрение Big Data.
- Использование технологий в торговом зале для оптимизации розничных продаж.

КОНТРОЛЬНЫЙ СПИСОК

STRATA

БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

- МСЭ нового поколения
- для предотвращения угроз
- URL Filtering
- DNS Security
- Wildfire
- Global Protect
- Система управления
- Panorama SD-WAN
- Autofocus
- IoT, Zingbox

PRISMA

БЕЗОПАСНОСТЬ ОБЛАКА

- Prisma Access
- Prisma Cloud
- Prisma SaaS
- Серия VM

CORTEX

БЕЗОПАСНОСТЬ БУДУЩЕГО

- Cortex Data Lake
- Cortex XDR
- XSOAR
- Zingbox

НАШИ КОНТАКТЫ

115114, г. Москва, 1-й Дербеневский пер., 5,
БЦ «Derbenevskaya Plaza», подъезд 4, офис 407

info@netwell.ru
+7 (495) 66-239-66

NETWELL | paloalto NETWORKS