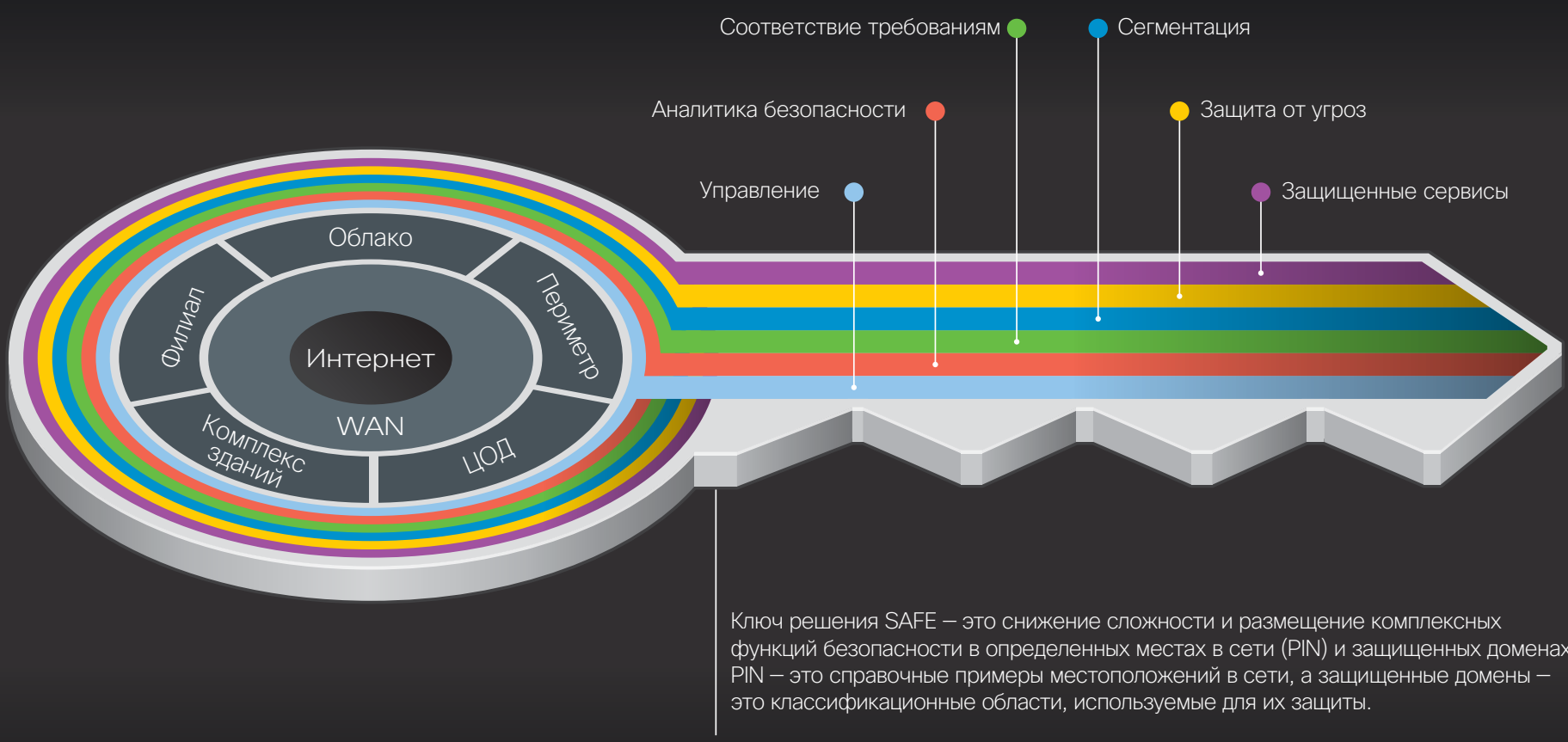
SAFE

УПРОЩАЕТ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

Август 2015

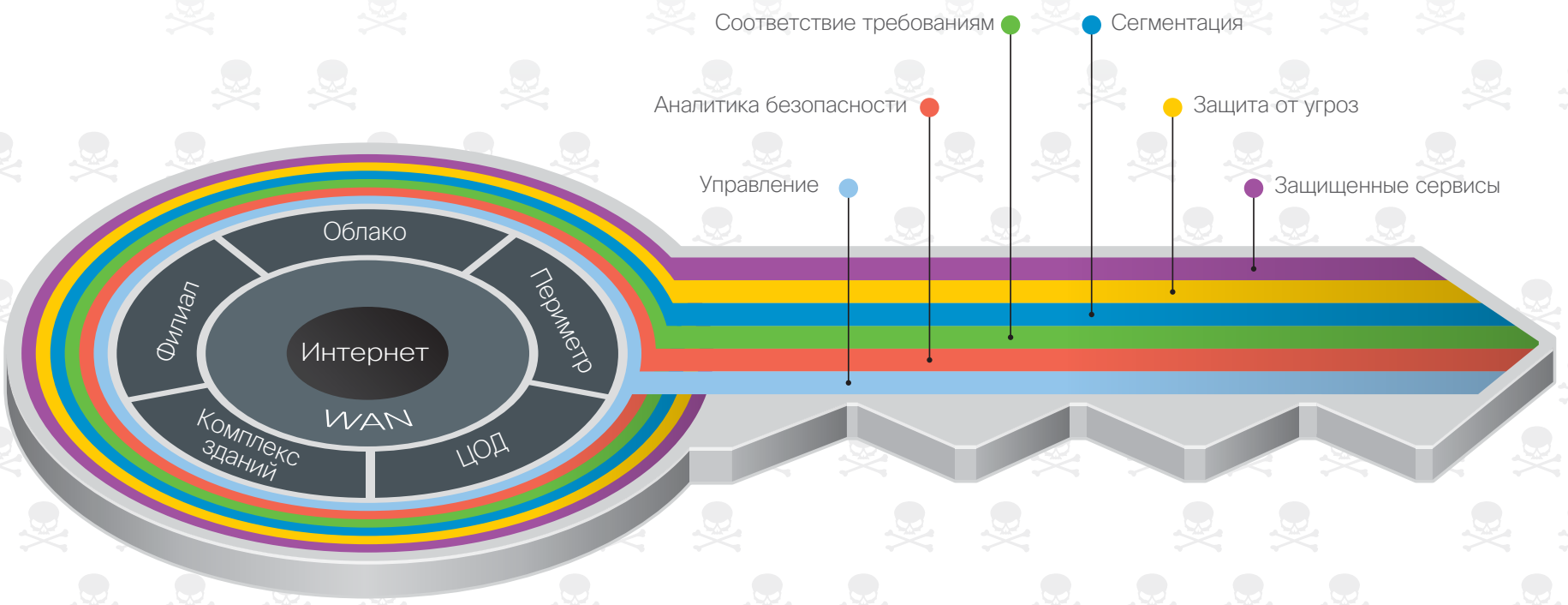


Ключ решения SAFE – это снижение сложности и размещение комплексных функций безопасности в определенных местах в сети (PIN) и защищенных доменах. PIN – это справочные примеры местоположений в сети, а защищенные домены – это классификационные области, используемые для их защиты.

Введение

SAFE – это пример архитектуры безопасности для сетей предприятий. SAFE снижает сложность благодаря использованию модели, ориентированной на области, которые компания должна защищать. Каждая область определяется с учетом комплексного анализа современных угроз и возможностей, необходимых для защиты этих областей. Компания Cisco выполнила развертывание, тестирование и подтверждение критически важных функций. Эти решения включают в себя инструкции и шаги по конфигурации, что позволяет обеспечить их эффективное и надежное развертывание у наших заказчиков.

Для получения более подробной информации посетите сайт cisco.com/go/safe



Защищенные домены

Защищенные сервисы

Включает такие технологии, как управление доступом, виртуальные частные сети (VPN) и шифрование. Также обеспечивает защиту небезопасных сервисов, например приложений, инструментов совместной работы и беспроводного доступа.

Защита от угроз

Обеспечивает мониторинг наиболее трудно выявляемых и опасных кибератак. Для этого используются такие возможности, как информация о телеметрии и репутации сетевого трафика и учет контекста. Обеспечивает возможности оценки характера и потенциального риска подозрительной деятельности в сети с целью принятия соответствующих мер для предотвращения кибератаки.

Сегментация

Устанавливает границы для данных и пользователей. В традиционной ручной сегментации для применения политик используется сочетание сетевой адресации, сетей VLAN и возможностей межсетевого экрана. В основе усовершенствованной сегментации лежит инфраструктура на основе идентификации для применения политик автоматически и с возможностью масштабирования, что значительно снижает трудности при эксплуатации.

Соответствие требованиям

Регулирует как внутренние, так и внешние политики. Показывает, как несколько средств управления можно реализовать в одном решении. Примеры соответствия внешним требованиям – PCI, HIPAA и закон Сарбейнса-Оксли(SOX).

Аналитика безопасности

Обеспечивает глобальное определение и агрегацию появляющегося вредоносного ПО и угроз. Предоставляет инфраструктуру для динамического применения политик, так как репутация согласуется с учетом контекста новых угроз. Таким образом, обеспечивается комплексная и своевременная защита.

Управление

Управление устройствами и системами с использованием централизованных сервисов абсолютно необходимо для согласованного развертывания политик, управления изменениями рабочих процессов и возможности регулярного обновления систем. Управление обеспечивает координацию политик, объектов и предупреждений.

Обзор практических рекомендаций и схем по внедрению функций безопасности

5 |Защищенный филиал

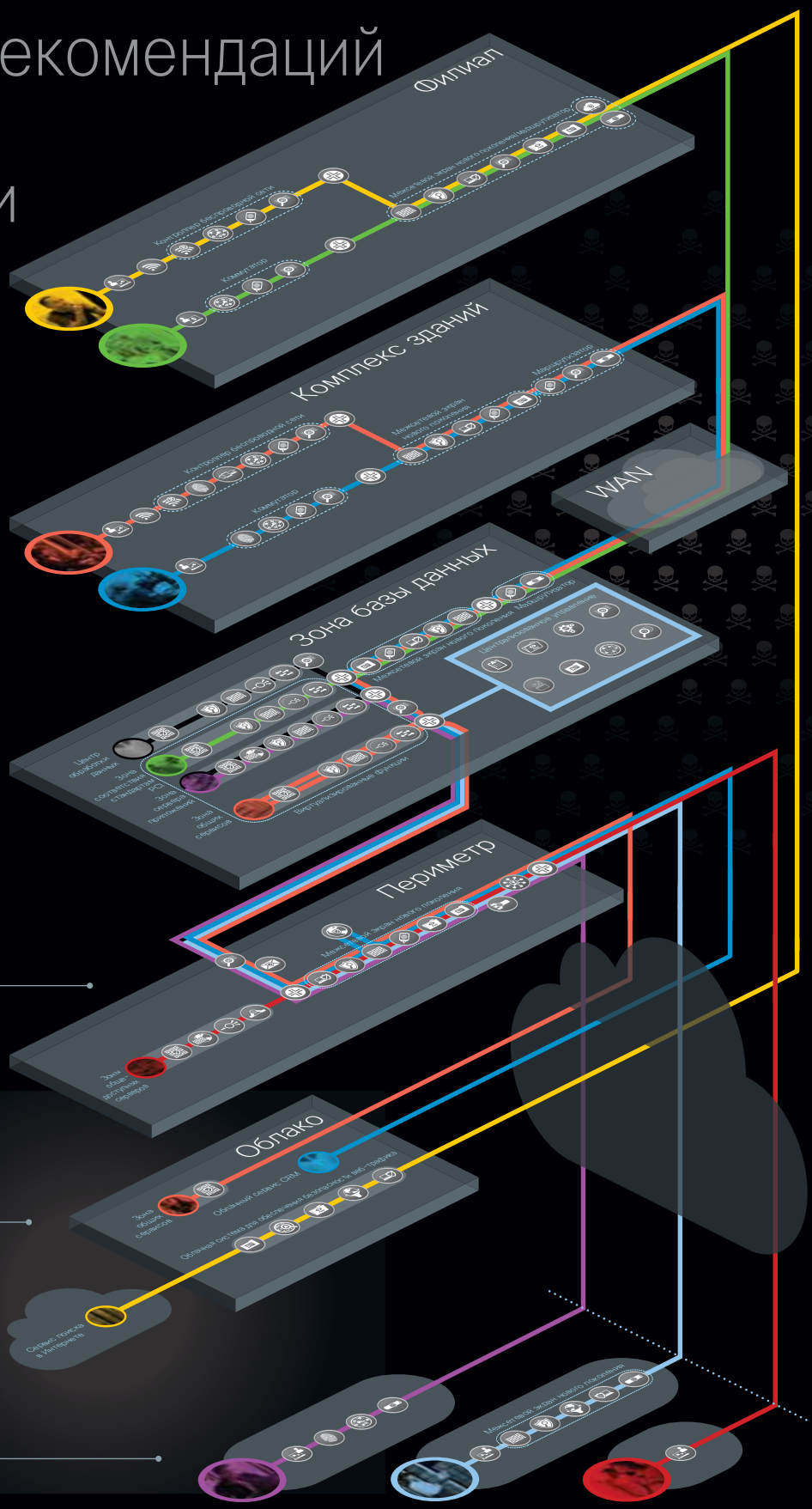
6 |Защищенный комплекс зданий

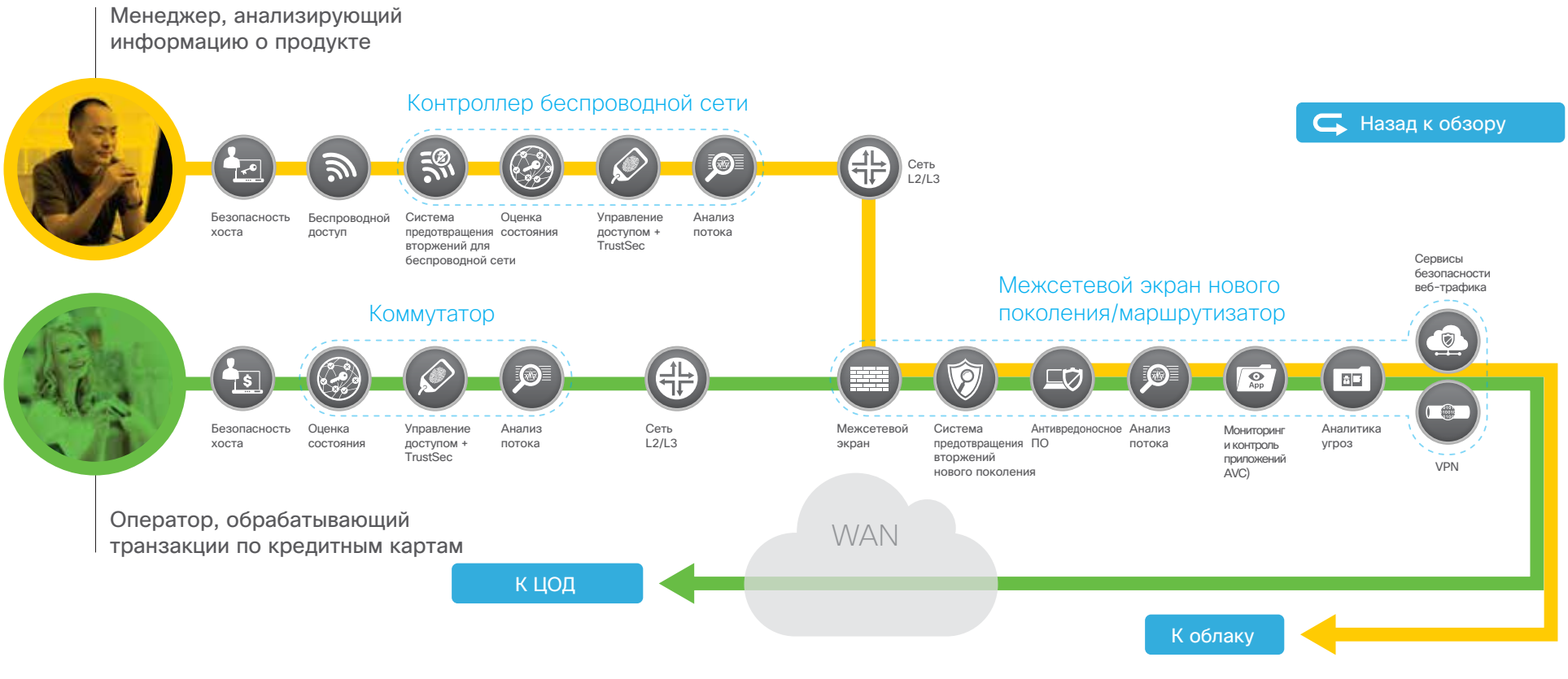
7 |Защищенный ЦОД

8 |Защищенный периметр

9 |Защищенное облако

10 |Внешние зоны





Защищенный филиал

Основные проблемы обеспечения безопасности

Сети филиалов обычно защищены меньше, чем сети комплексов зданий и центров обработки данных. Зачастую считается, что дублировать все функции обеспечения безопасности, которые используются в крупных сетях, для сотен небольших филиалов экономически нецелесообразно. Однако таким образом филиалы становятся привлекательной целью для проведения атаки и более уязвимы для проникновения. Поэтому при проектировании сети филиала важно включать в нее функции безопасности, не забывая при этом об обеспечении экономической эффективности филиала.

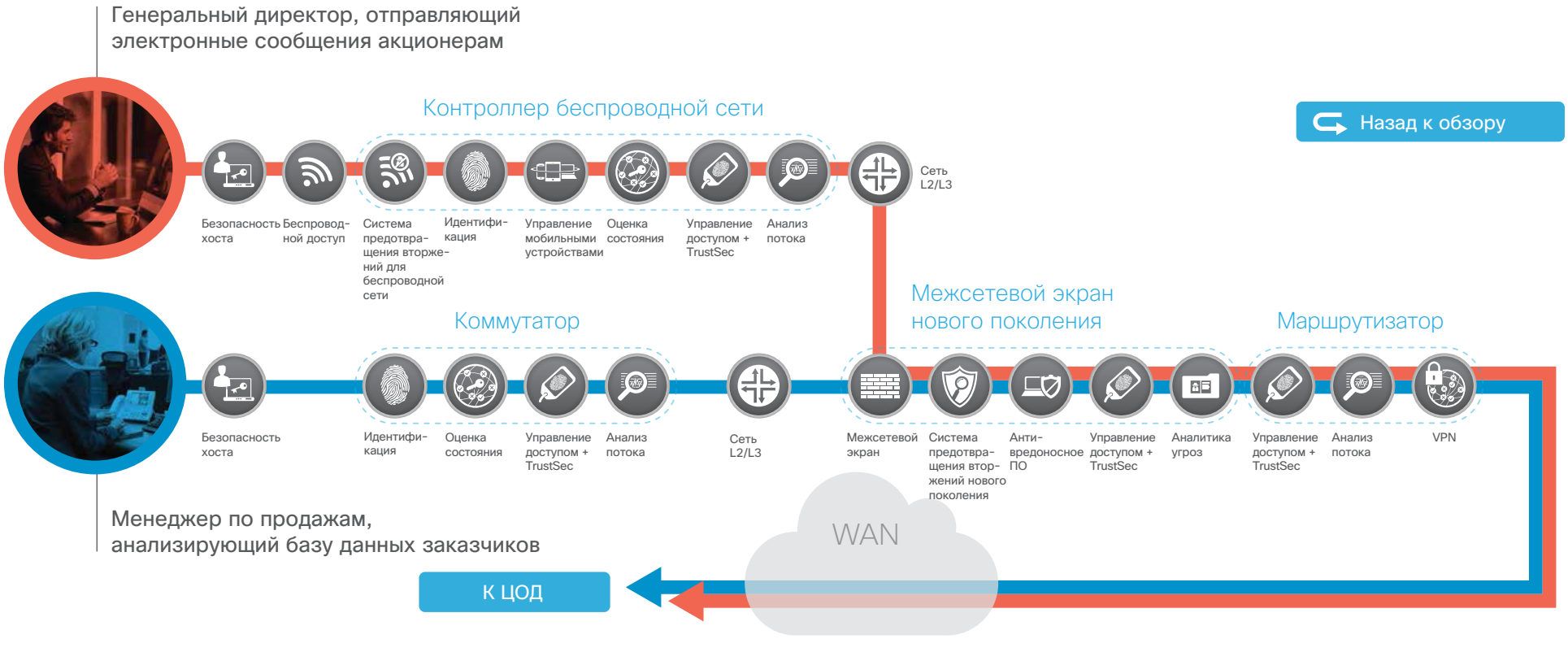
Основные предотвращаемые угрозы

- Вредоносное ПО для оконечных устройств (например, вредоносное ПО для платежных терминалов)
- Несанкционированные/вредоносные действия клиента
- Эксплойты для беспроводной инфраструктуры (например, вредоносные точки доступа, MitM)
- Эксплуатация доверия

Функция	Продукт
	Облачная система для обеспечения безопасности веб-трафика, Meraki MX, FirePOWER URL
	Многофункциональное устройство обеспечения безопасности (ASA), маршрутизатор с интегрированными сервисами (ISR), Meraki MX
	Cisco Collective Security Intelligence, Cisco Talos Security Intelligence
	Маршрутизатор с интегрированными сервисами (ISR), многофункциональное устройство обеспечения безопасности (ASA), беспроводная локальная сеть

Функция	Продукт
	Cisco Advanced Malware Protection (AMP) для сетей
	Контроллер беспроводного доступа/коммутатор Catalyst, централизованная платформа Cisco Identity Services Engine (ISE)
	Сервисы Cisco FirePOWER на многофункциональном устройстве обеспечения безопасности, UCS-E или устройстве FirePOWER
	Многофункциональное устройство обеспечения безопасности (ASA), маршрутизатор с интегрированными сервисами (ISR), Meraki MX

Функция	Продукт
	Агент AnyConnect, централизованная платформа Cisco Identity Services Engine (ISE)
	Cisco Advanced Malware Protection (AMP) для оконечных устройств, AnyConnect, антивирусное ПО (партнера)
	Централизованная платформа Cisco Mobility Services Engine (MSE), контроллер беспроводной локальной сети с централизованным управлением, Meraki
	Модуль или устройство с сервисами FirePOWER, Meraki MX



Защищенный комплекс зданий

Основные проблемы обеспечения безопасности

В комплексе зданий обычно много пользователей с самыми разными типами устройств, а средств обеспечения внутренней безопасности, наоборот, не хватает. В связи с большим числом зон безопасности (подсети и сети VLAN) обеспечить их надежную сегментацию очень сложно. Недостаточное количество средств обеспечения безопасности, ограниченные возможности мониторинга и гостевой доступ (или доступ партнеров) – все это делает комплекс зданий привлекательной целью для атаки.

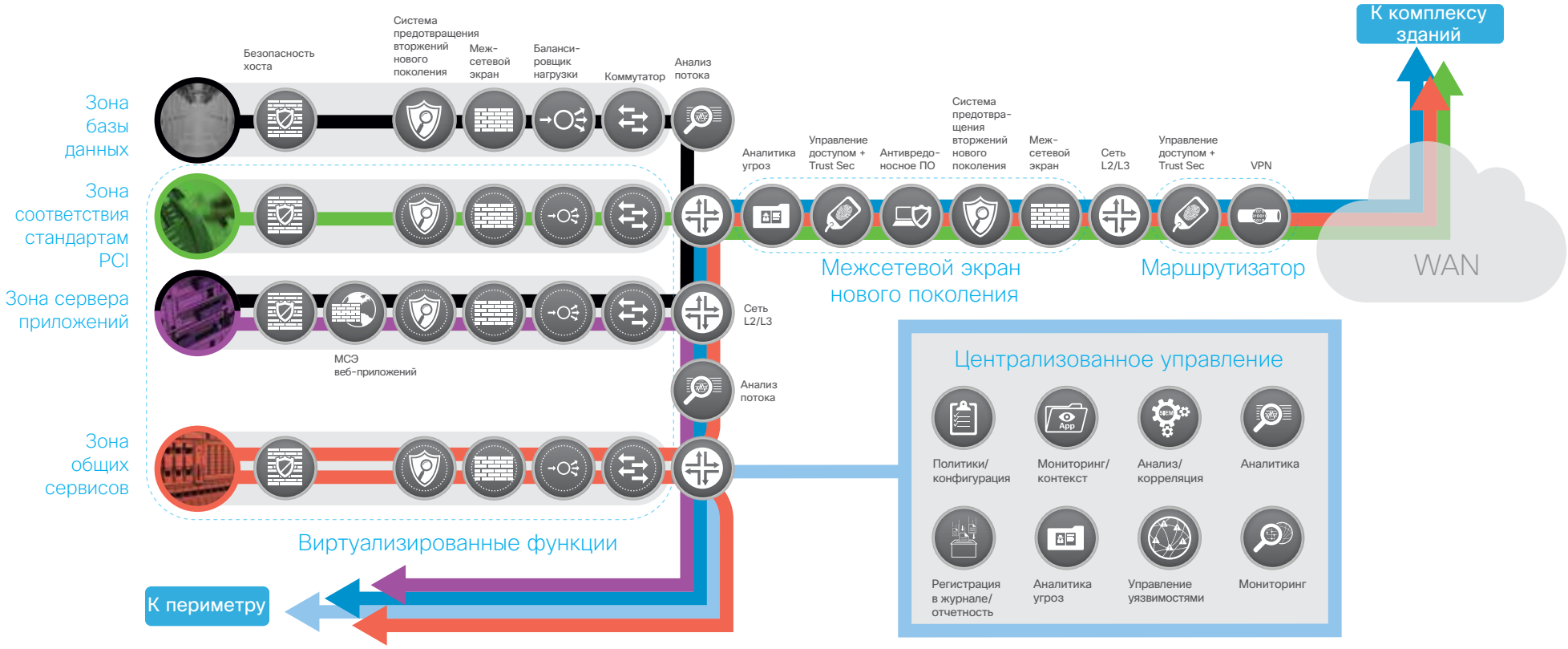
Основные предотвращаемые угрозы

- Фишинг
- Эксплойты для веб-продуктов
- Несанкционированный сетевой доступ
- Распространение вредоносного ПО
- BYOD – большая поверхность атаки/увеличение риска потери данных
- Заражение ботами

Функция	Продукт
	Облачная система для обеспечения безопасности веб-трафика, устройство защиты веб-трафика с централизованным управлением
	Многофункциональное устройство обеспечения безопасности (ASA), маршрутизатор с интегрированными сервисами (ISR), Meraki MX
	Cisco Collective Security Intelligence, Cisco Talos Security Intelligence
	Маршрутизатор с интегрированными сервисами (ISR), контроллер беспроводной локальной сети, коммутатор Catalyst

Функция	Продукт
	Cisco Advanced MalwareProtection (AMP) для сетей
	Контроллер беспроводного доступа/ коммутатор Catalyst, платформа Cisco Identity Services Engine (ISE)
	Сервисы Cisco FirePOWER на многофункциональном устройстве обеспечения безопасности, UCS-E или устройстве FirePOWER
	Многофункциональное устройство обеспечения безопасности (ASA), маршрутизатор с агрегированными сервисами (ASR), Meraki MX

Функция	Продукт
	Агент AnyConnect, платформа Cisco Identity Services Engine (ISE)
	Cisco Advanced Malware Protection AMP) для оконечных устройств, AnyConnect, антивирусное ПО (партнера)
	Платформа Mobility Services Engine (MSE), контроллер беспроводной локальной сети
	Платформа Cisco Identity Services Engine (ISE), управление мобильными устройствами Meraki



Назад к обзору

Защищенный ЦОД

Основные проблемы обеспечения безопасности

В центрах обработки данных находятся основные информационные ресурсы и интеллектуальная собственность. Центры обработки данных являются главной целью для всех целенаправленных атак и поэтому требуют самого высокого уровня обеспечения безопасности. Центры обработки данных содержат сотни и тысячи физических и виртуальных серверов, сегментированных по типам приложений, зонам классификации данных и т. д. Создание надлежащих правил для контроля за доступом к ресурсам как на входе/выходе из ЦОД («север/юг»), так и внутри ЦОД («восток/запад») и управление этими правилами может быть чрезвычайно сложной задачей.

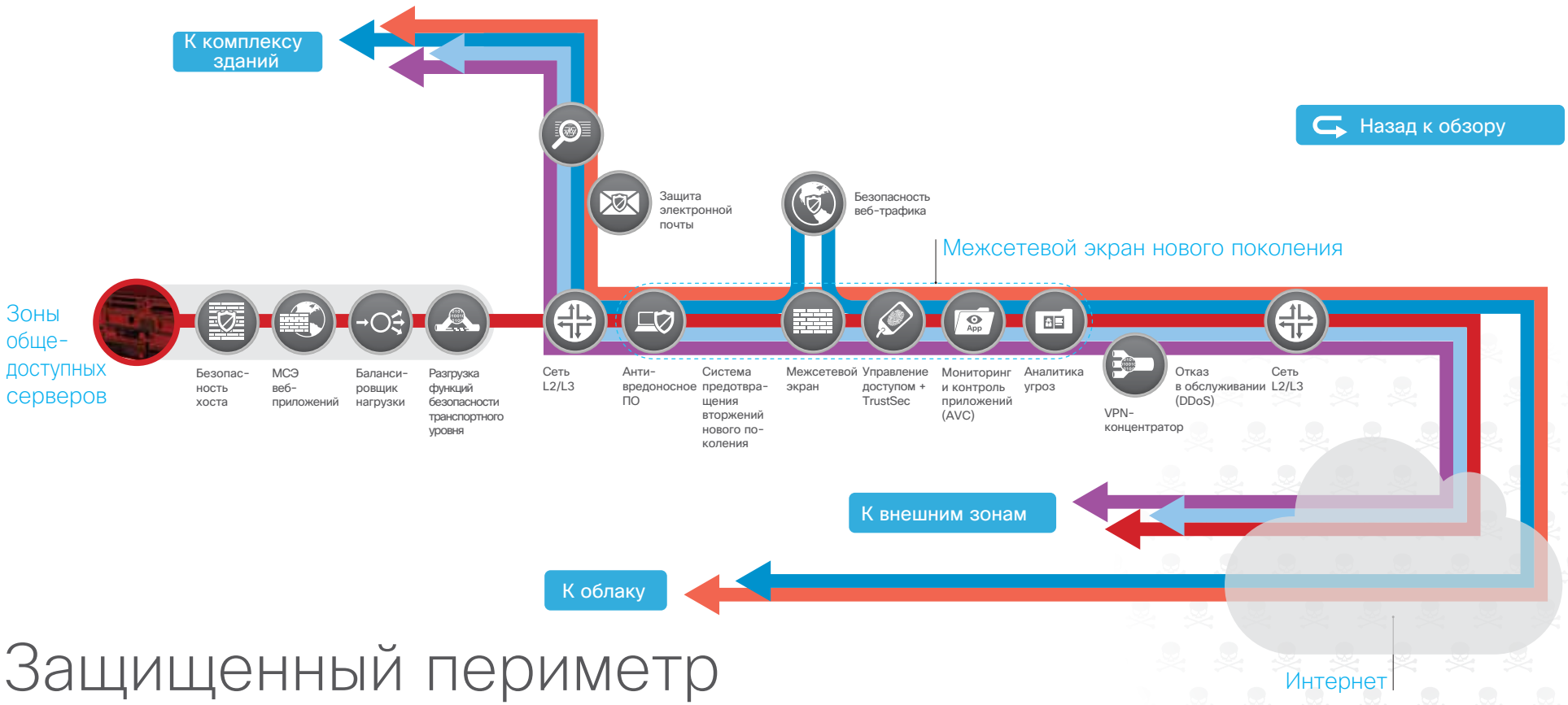
Основные предотвращаемые угрозы

- Утечка (потеря) данных
- Распространение вредоносного ПО
- Несанкционированный сетевой доступ (например, компрометация приложений, потеря данных, эскалация привилегий, разведка)
- Заражение ботами (например, кража ресурсов (скрампинг))

Функция	Продукт
	Многофункциональное устройство обеспечения безопасности (ASA), виртуальный шлюз безопасности, устройство Firepower 9300
	Модуль, физическое или виртуальное устройство с сервисами FirePOWER, устройство Firepower 9300
	Cisco Collective Security Intelligence, Cisco Talos Security Intelligence
	Cisco Netflow Generation Appliance (NGA), Lancope FlowSensor, многофункциональное устройство обеспечения безопасности (ASA)

Функция	Продукт
	Многофункциональное устройство обеспечения безопасности (ASA), маршрутизатор с агрегированными сервисами (ASR)
	Многофункциональное устройство обеспечения безопасности (ASA), маршрутизатор с агрегированными сервисами (ASR), устройство Firepower
	Cisco Advanced Malware Protection (AMP) для сетей
	Коммутатор Nexus/Catalyst

Функция	Продукт
	МСЭ веб-приложений (партнер по технологиям)
	Балансировщик нагрузки (партнер по технологиям)
	Cisco Advanced Malware Protection AMP) для оконечных устройств, AnyConnect, антивирусное ПО (партнера)



Защищенный периметр

Основные проблемы обеспечения безопасности

Интернет-периметр наиболее всего подвержен риску атак, так как является основной точкой входа публичного трафика и основной точкой выхода в Интернет. Кроме того, это критически важный ресурс, который так необходим предприятиям в условиях современной экономики, тесно связанной с Интернетом.

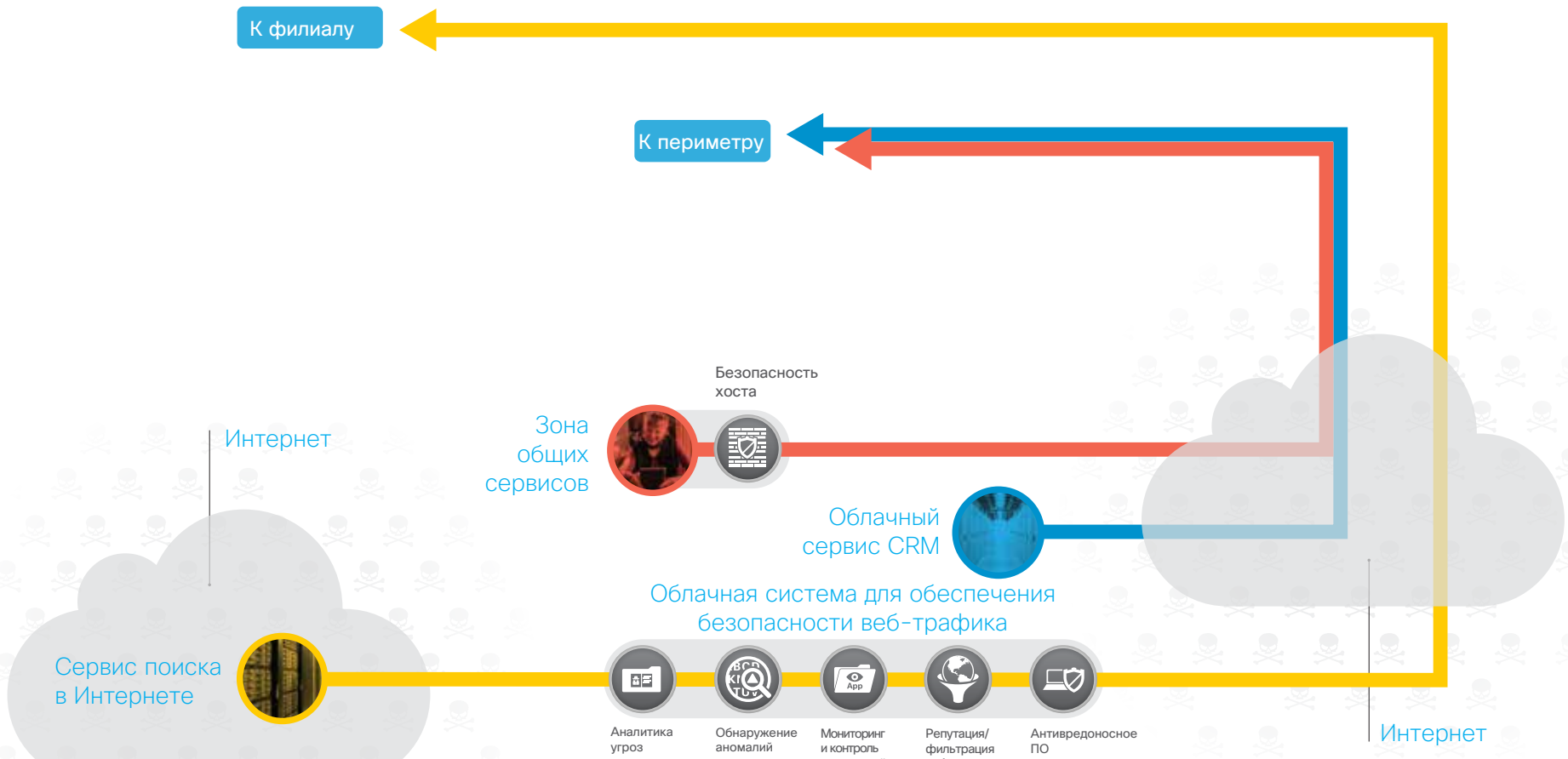
Основные предотвращаемые угрозы

- Уязвимости веб-сервера
- DDoS
- Потеря данных
- Атака «человек посередине» (MITM)

Функция	Продукт
	Многофункциональное устройство обеспечения безопасности (ASA), маршрутизатор с агрегированными сервисами (ASR)
	Cisco Collective Security Intelligence, Cisco Talos Security Intelligence
	Многофункциональное устройство обеспечения безопасности (ASA), маршрутизатор с агрегированными сервисами (ASR), коммутатор Catalyst
	Многофункциональное устройство обеспечения безопасности (ASA), устройство Firepower 9300, Meraki MX
	Модуль или устройство с сервисами FirePOWER

Функция	Продукт
	Cisco Advanced Malware Protection (AMP) для сетей
	Облачная система для обеспечения безопасности веб-трафика, устройство защиты веб-трафика
	Облачная система для обеспечения безопасности веб-трафика, устройство защиты электронной почты
	Разгрузка функций безопасности на транспортном уровне (партнер по технологиям)
	Отказ в обслуживании (DDoS) (партнер по технологиям)

Функция	Продукт
	МСЭ веб-приложений (партнер по технологиям)
	Cisco Advanced Malware Protection (AMP) для оконечных устройств, AnyConnect, антивирусное ПО (партнера)
	Модуль или устройство с сервисами FirePOWER, Meraki MX



Назад к обзору

Защищенное облако

Основные проблемы обеспечения безопасности

Основные риски для безопасности облака связаны со слабым контролем, недостатком доверия, общим доступом и «теневыми» ИТ-ресурсами. Для предприятий основным средством регулирования функций безопасности, выбранных ими в предложенных облачных сервисах, являются соглашения об уровне обслуживания (SLA). Для повышения доверия необходимо использовать независимые аудиторские оценки риска и сертификаты.

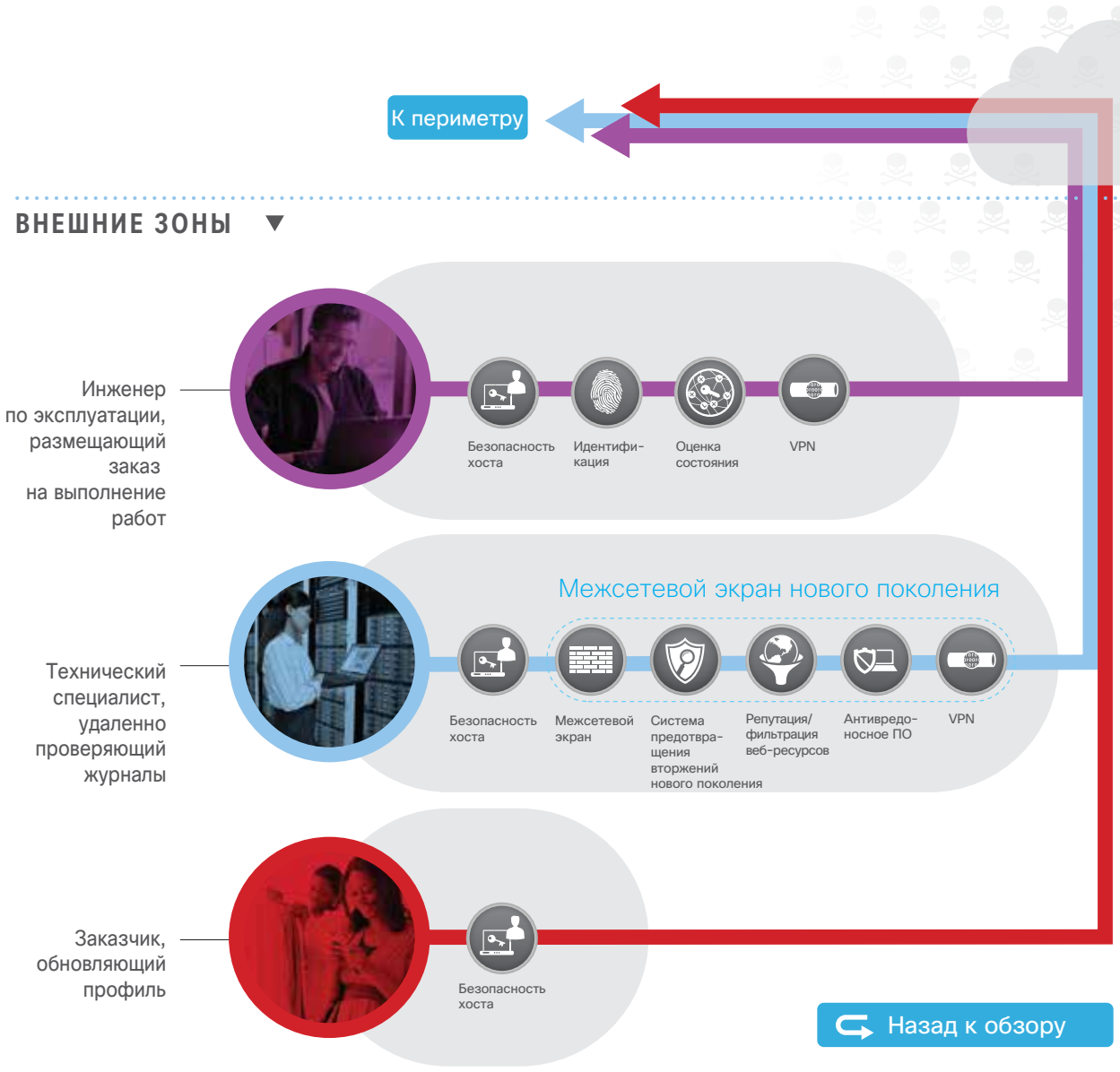
Основные предотвращаемые угрозы

- Уязвимости веб-сервера
- Вирусы и вредоносное ПО
- Потеря доступа
- Атака «человек посередине» (MITM)

Функция	Продукт
	Многофункциональное устройство обеспечения безопасности (ASA), маршрутизатор с интегрированными сервисами (ISR), AnyConnect, Meraki MX
	Многофункциональное устройство обеспечения безопасности (ASA), маршрутизатор с интегрированными сервисами (ISR), Meraki MX

Функция	Продукт
	Сервисы Cisco FirePOWER на ASA и UCS-E
	Защита от усовершенствованного вредоносного ПО (AMP)

Функция	Продукт
	Облачная система для обеспечения безопасности веб-трафика, устройство обеспечения безопасности веб-трафика, Meraki MX, OpenDNS партнера
	Cisco Advanced Malware Protection (AMP) для оконечных устройств, AnyConnect, антивирусное ПО (партнера)



Заказчики

Основные проблемы обеспечения безопасности

Обеспечение надежного и безопасного подключения к предоставляемым услугам – это основная цель при установлении коммуникаций с заказчиками, находящимися за пределами корпоративного офиса. Утечка или потеря данных немедленно становятся причиной полной утраты доверия, что в результате приводит к падению объемов продаж.

Удаленные сотрудники

Основные проблемы обеспечения безопасности

Обеспечение безопасного удаленного доступа для сотрудников, подключающихся к корпоративному офису с недоверенных узлов (например, из кафе и отелей), очень важно для безопасности данных. Такие возможности, как управление доступом на основе идентификации, оценка состояния и шифрование, обеспечивают реализацию согласованного набора политик прежде, чем разрешить доступ.

Сторонние поставщики и партнеры

Основные проблемы обеспечения безопасности

Небезопасный доступ партнеров и поставщиков может быстро привести к негативным последствиям для функционирования вашего предприятия. Для блокировки несанкционированного доступа и эксплуатации доверия необходимо применение средств тщательного контроля доступа, обнаружения аномалий и соглашений об уровне обслуживания (SLA).

Внешние зоны

Предприятия подвержены риску

Последние уязвимости в системах безопасности подчеркивают необходимость рассматривать всю экосистему ваших партнеров, заказчиков, поставщиков и сотрудников в комплексе. Традиционные средства защиты периметра уже не достаточны для защиты от современных векторов атак. Для обеспечения доверия и надежной защиты необходимо также внедрять такие возможности, как идентификация, применение политик и анализ аномалий.

Основные предотвращаемые угрозы

- Вредоносное ПО для оконечных устройств
- Несанкционированные/вредоносные действия клиента
- Эксплуатация доверия
- Атака «человек посередине» (MITM)

Функция	Продукт
	Многофункциональное устройство обеспечения безопасности (ASA), маршрутизатор с интегрированными сервисами (ISR), AnyConnect, Meraki MX
	Многофункциональное устройство обеспечения безопасности (ASA), маршрутизатор с интегрированными сервисами (ISR), Meraki MX

Функция	Продукт
	Сервисы Cisco FirePOWER на ASA и UCS-E
	Защита от усовершенствованного вредоносного ПО (AMP)

Функция	Продукт
	Облачная система для обеспечения безопасности веб-трафика, устройство обеспечения безопасности веб-трафика, Meraki MX, OpenDNS партнера
	Cisco Advanced Malware Protection (AMP) для оконечных устройств, AnyConnect, антивирусное ПО (партнера)