Исследование Forrester на основе методологии Forrester Total Economic Impact™

По заказу компании Cisco

Директор проекта:
Мишель С. Бишоп
(Michelle S. Bishop)

Сентябрь 2016 г.

Общий экономический эффект использования Cisco TrustSec, рассчитанный на основе методологии Total Economic Impact™

Упрощение проектирования систем безопасности и снижение операционных расходов с помощью технологий Cisco

FORRESTER®

Содержание

О КОМПАНИИ FORRESTER CONSULTING

Forrester Consulting предоставляет услуги независимого и объективного консультирования на основе исследований с целью помочь руководителям добиться успеха своих организаций. Forrester Consulting предоставляет различные виды услуг: от коротких семинаров по выработке стратегии до подготовки индивидуальных проектов. В каждом случае вы напрямую сотрудничаете с экспертами-аналитиками, опыт и знания которых позволяют решать самые сложные бизнес-задачи. Для получения подробной информации посетите страницу forrester.com/consulting.

FORRESTER®

Краткий обзор

Cisco поручила компании Forrester Consulting провести исследование на основе методологии Total Economic Impact™ (TEI) и оценить возможную рентабельность инвестиций (ROI) предприятий от внедрения программно-определяемого сегментирования Cisco TrustSec. Целью этого исследования является предоставление читателям концепции оценки возможной финансовой выгоды от внедрения технологий Cisco на своих предприятиях.

«TrustSec упрощает модель защищенного доступа и позволяет существенно снизить объем обслуживания».

— **Корпоративный архитектор, учебное заведение**

Для более глубокого изучения выгод, затрат и рисков, связанных с TrustSec, Forrester опросила представителей четырех заказчиков, использующих TrustSec. Решение TrustSec на основе программно-определяемого сегментирования упрощает выделение ресурсов и управление защищенным доступом к сетевым сервисам и приложениям. В отличие от механизмов контроля доступа, основанных на топологии сети, в политиках TrustSec используется логическое группирование. Поддерживается постоянно высокий уровень безопасности доступа даже при перемещении ресурсов в мобильных и виртуальных сетях. Более подробное описание доступно в обзоре Cisco TrustSec в настоящем документе.

Опрошенные клиенты ставили перед собой ряд целей по внедрению TrustSec, среди которых назывались снижение рисков и обеспечение соответствия требованиям, а также повышение эффективности ИТ-операций. Эти клиенты стремились защитить приложения во всех своих представительствах, а также обеспечить контроль и управление доступом к утвержденным активам. Среди сценариев использования TrustSec назывались управление мобильным доступом для планшетов и телефонов, управление сегментированием сети в организации, ограничение доступа к критически важным приложениям в центре обработки данных, а также переход к модели доступа на основе идентификационной информации для всех ресурсов.

TRUSTSEC СНИЖАЕТ ОПЕРАЦИОННЫЕ РАСХОДЫ, УПРОЩАЕТ ПРОЕКТИРОВАНИЕ СИСТЕМ БЕЗОПАСНОСТИ И ПОВЫШАЕТ ГИБКОСТЬ

Мы встретились с четырьмя имеющимися клиентами и затем проанализировали полученную в ходе встреч информацию. Результаты финансового анализа показали, что для универсальной организации, аналогичной компаниям, представителей которых мы опрашивали, характерны приведенные на рис. 1 показатели окупаемости инвестиций, выгод и издержек с поправкой на риски.[1]

Анализ универсальной организации указывает на выгоды в размере 3 989 498 долл. США и затраты на внедрение в размере 1 663 914 долл. США; таким образом, чистая приведенная стоимость (NPV) составляет 2 325 584 долл. США. Как отметили представители опрошенных организаций, внедрение TrustSec помогло снизить операционные расходы, избежав издержек на альтернативные традиционные решения для обеспечения безопасности по периметру, сократить численность дополнительного персонала для поддержки ИТ-операций и повысить устойчивость сети, тем самым снизив вероятность простоев.

Среди других преимуществ, названных опрошенными организациями, были ускорение вывода проектов на рынок, согласованное и эффективное сегментирование сети, упрощение проектирования систем безопасности за счет упрощения политики безопасности, повышение качества автоматизированного управления правилами межсетевых экранов, повышение уровня гибкости, возможность масштабирования политики безопасности, повышение уровня защищенности сети и более эффективное соответствие нормативным требованиям.

РИС. 1

Финансовая сводка результатов за три года с поправкой на риски

Источник: корпорация Forrester Research

› **Выгоды.** Универсальная организация получила следующие выгоды на основе приведенной стоимости с поправкой на риски, которые отражают выгоды, полученные опрошенными компаниями:

- **Экономия за счет исключения затрат на альтернативные традиционные решения.** Благодаря использованию TrustSec вместо альтернативного традиционного решения для сегментирования, например VLAN и межсетевых экранов, универсальная компания за рассматриваемый трехлетний период смогла сэкономить 2,7 млн долл. США.
- **Снижение операционных расходов на ИТ.** TrustSec сокращает административные расходы на управление доступом, особенно с учетом объема задач по администрированию, необходимого для более традиционных решений, таких как VLAN и межсетевые экраны. Опрошенные организации отметили сокращение операционных расходов на 25–80 %. Без внедрения TrustSec универсальной компании потребовалось бы нанять еще четверых сетевых инженеров; таким образом, она смогла сэкономить 945 402 долл. США.
- **Повышение устойчивости сети и снижение риска простоев.** TrustSec также повышает устойчивость сети организации, что уменьшает риски простоев. При сокращении времени простоев на 1 час в год для 4000 пользователей экономия для универсальной компании составила 319 716 долл. США.
- Другие выгоды, отмеченные опрошенными организациями:
    - **ускорение вывода проектов на рынок;**
    - **упрощение и автоматизация управления правилами межсетевых экранов и снижение соответствующих операционных расходов;**
    - **улучшение соответствия нормативным требованиям;**
    - **согласованное и эффективное сегментирование сети;**
    - **упрощение проектирования систем безопасности за счет упрощения политики безопасности;**
    - **повышение уровня гибкости и возможность масштабирования политики безопасности;**
    - **повышение уровня защищенности сети.**

› **Затраты.** Внедрение традиционного сегментирования или программно-определяемого сегментирования TrustSec предполагает дополнительные расходы. Расходы на традиционное сегментирование представлены в таблице 1. Универсальная компания понесла следующие затраты на основе приведенной стоимости с поправкой на риски, связанные с программно-определяемым сегментированием TrustSec:

- **Затраты на инфраструктуру TrustSec.** Универсальная компания потратила на инфраструктуру TrustSec 346 500 долл. США. Эта сумма включает стоимость Cisco Identity Services Engine (ISE) и необходимых лицензий. В ней не учитываются расходы на модернизацию сети, поскольку универсальная компания внедряла решение TrustSec одновременно с плановой заменой устаревшей сетевой инфраструктуры.
- **Затраты на расширенные услуги Cisco.** Универсальная компания использовала расширенные услуги Cisco для низкоуровневого и высокоуровневого проектирования на сумму231 000 долл. США. Не все опрошенные клиенты обращались к расширенным услугам Cisco при планировании внедрения TrustSec.
- **Оплата профессиональных услуг.** Универсальная компания также потратила 404 250 долл. США на профессиональные услуги по внедрению TrustSec. Не все опрошенные клиенты обращались к профессиональным услугам при внедрении TrustSec.
- **Внутренние работы по внедрению и тестированию.** За шесть месяцев, в течение которых осуществлялось внедрение TrustSec, универсальная компания потратила на эти работы 130 680 долл. США.
- **Затраты на администрирование и поддержку.** В универсальной компании работали два инженера, осуществлявшие текущее администрирование и тестирование регулярных обновлений сетевого ПО; за рассматриваемый трехлетний период соответствующие затраты составили 551 484 долл. США.

Пояснения

При ознакомлении с данным документом следует учитывать следующее:

› Данное исследование проведено компанией Forrester Consulting по заказу компании Cisco. Его не следует рассматривать в качестве конкурентного анализа.

› Компания Forrester не делает каких-либо оценок, связанных с возможной окупаемостью инвестиций в той или иной компании. Компания Forrester настоятельно рекомендует читателям придерживаться собственных оценок, используя концепцию, приведенную в отчете, чтобы определить приемлемость инвестиций в решение TrustSec.

› Компания Cisco ознакомилась с содержанием исследования и предоставила свой отзыв компании Forrester, однако компания Forrester сохраняет за собой право редакционного контроля над исследованием и его результатами и не вносит в исследование изменений, противоречащих полученным компанией Forrester результатам либо затрудняющих восприятие сути исследования.

› Cisco предоставила названия организаций клиентов для проведения интервью, но сама в интервью не участвовала.

Концепция и методология TEI

ВВЕДЕНИЕ

Основываясь на предоставленной в ходе опросов информации, компания Forrester разработала методологию Total Economic Impact (TEI) для организаций, которые рассматривают возможность внедрения решения Cisco TrustSec. Данная концепция призвана определить затраты, выгоды, уровень гибкости и риски, влияющие на принятие инвестиционного решения, и помочь организациям использовать конкретные преимущества, сократить расходы, а также улучшить показатели привлечения, обслуживания и удержания клиентов.

ПОДХОД И МЕТОДОЛОГИЯ

Компания Forrester использовала многоэтапный подход для оценки воздействия решения Cisco на организацию (см. рис. 2). В частности, были предприняты следующие действия:

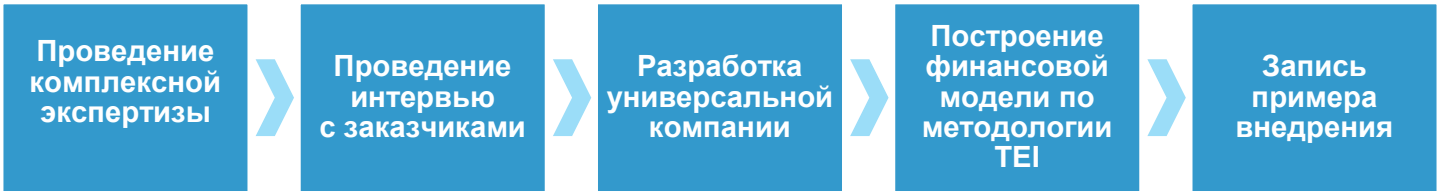
- Проведен опрос сотрудников Cisco из сфер маркетинга, продаж и консалтинговых услуг, а также аналитиков Forrester, что позволило собрать данные о решении TrustSec и рынке решений для сетевой безопасности в целом.
- Проведены опросы представителей четырех организаций, использующих в настоящее время решение TrustSec, что позволило получить данные об издержках, выгодах и рисках.
- На основе характеристик опрошенных компаний (см. Приложение А) создана универсальная компания.
- По методологии TEI и на основании результатов интервью построена финансовая модель. Эта финансовая модель заполнена данными о затратах и выгодах, полученными в ходе интервью (и переработанными с учетом применения к универсальной компании).
- Выполнена корректировка финансовой модели на риски с учетом проблем и затруднений, отмеченных опрошенными организациями.Поправка на риски является одной из основных составляющих методологии TEI. Хотя опрошенные организации предоставили собственные оценки затрат и выгод, по некоторым категориям вопросов наблюдалась широкая вариативность ответов или были отмечены внешние факторы, которые могли повлиять на результаты. По этой причине для некоторых суммарных показателей затрат и выгод, подробно рассмотренных в соответствующих разделах, была выполнена поправка на риски.

При моделировании решения TrustSec компания Forrester задействовала четыре фундаментальных элемента TEI: выгоды, затраты, гибкость и риски.

С учетом того что предприятия подходят к анализу окупаемости инвестиций в ИТ со все большей тщательностью, методология TEI компании Forrester позволяет получить полную картину совокупного экономического эффекта принимаемых решений о приобретении. Дополнительные сведения о методологии TEI приведены в Приложении Б.

РИС. 2

Подход TEI



Источник: корпорация Forrester Research

Анализ

УНИВЕРСАЛЬНАЯ КОМПАНИЯ

Для данного исследования Forrester провела интервью с представителями следующих четырех компаний из числа клиентов Cisco:

- Корпоративная розничная сеть, включающая 1350 магазинов. Компания имеет 20 офисов и два крупных центра обработки данных.
- Образовательное и исследовательское учреждение, имеющее 80 000 проводных портов в 74 зданиях.
- Один из ведущих коммерческих банков с 20 филиалами, который вместе с дочерними банками обслуживает более 30 миллионов клиентов.
- Розничный коммерческий банк, имеющий 2700 отделений и свыше 75 000 сотрудников.

На основе проведенных интервью компания Forrester построила модель TEI и универсальную компанию, а также выполнила соответствующий анализ окупаемости инвестиций, иллюстрирующий области деятельности организации, затрагиваемые с точки зрения финансов. Универсальная компания, которую сформировала компания Forrester на основании полученных результатов, имеет следующие характеристики:

- Это финансовая организация, штат которой составляет около 4000 сотрудников.
- Она использует 30 000 LAN-портов с 250 коммутаторами и 50 маршрутизаторами.
- Целью сегментирования сети для нее является создание уровней глобального трафика с различными рабочими группами для пользователей, приложений и баз данных. Компании требуется разграничить трафик между этими группами, например разрешить для определенных пользователей доступ к конкретным службам приложений, но не к службам баз данных.

ОСНОВНЫЕ МОМЕНТЫ ИНТЕРВЬЮ

Ситуация

Основными причинами, по которым опрошенные организации приняли решение о внедрении TrustSec, являлись снижение рисков и повышение эффективности операций, связанных с безопасностью. Также в ходе интервью были получены следующие важные данные:

- Представитель одной из опрошенных компаний отметил, что внедрение TrustSec являлось частью программы по общему снижению рисков, связанных с сетевой безопасностью. С учетом размера и географического охвата этой сети главными целями компании были: 1) ограничение доступа к некоторым критически важным приложениям в центре обработки данных; 2) повышение ситуационной осведомленности о состоянии сети. С помощью TrustSec эта организация стремилась обеспечить безопасность приложений в ЦОД, головном офисе и филиалах путем контроля и ограничения доступа к утвержденным активам и предоставления доступа к ресурсам и приложениям только пользователям, имеющим соответствующие полномочия.

> *«В случае развертывания TrustSec пропускная способность, в отличие от использования межсетевых экранов, не ограничивается. Таким образом, это решение несет в себе меньше инвестиционных рисков. При этом TrustSec обеспечивает довольно низкий уровень операционных расходов».*
>
> ~ Глава отдела сетевых сервисов одной из опрошенных организаций

- Опрошенные организации также отмечали потребность в повышении эффективности операций, связанных с безопасностью, для поддержки дальнейшего развития и масштабирования этих процессов. Представитель одной из них сообщил, что решение TrustSec было внедрено для повышения качества контроля политики доступа к ресурсам. Эта компания хотела перейти от модели на основе «разрешенных компьютеров» к модели на основе «разрешенных пользователей» и внедрить систему доступа к сети с использованием идентификационной информации. Представитель другой компании отметил, что до внедрения TrustSec организация осуществляла микросегментирование, распределяя похожих пользователей по соответствующим VLAN, что являлось причиной высоких затрат на управление большим количеством сетей.

- Для одной из опрошенных компаний причиной выбора TrustSec стали вопросы регулирования: она использовала решение Cisco для сегментирования и предоставления сетевого доступа только пользователям с соответствующими полномочиями. Эта финансовая организация использовала сегментирование не только централизованно, но и на уровне точек доступа. Ее целью было прохождение аудита сетевой безопасности, предписанного отраслевыми регуляторами.

- Розничная компания, принявшая участие в исследовании, внедрила решение TrustSec в рамках проекта по предоставлению сотрудникам мобильного доступа к сети с планшетных компьютеров и телефонов. Ее целью являлось создание в розничных магазинах различных групп пользователей с разными уровнями доступа к мобильным устройствам на базе Active Directory. Поскольку межсетевые экраны Cisco Adaptive Security Appliance (ASA) и ISE уже были развернуты, в распоряжении компании были необходимые компоненты для реализации этого подхода. Присвоение меток безопасности различным типам пользователей в этом случае было простой задачей. Решение TrustSec являлось эффективным инструментом для дифференциации пользователей мобильных устройств.

> *«Мы рассматривали и другие варианты решений для сетевой безопасности на основе идентификаторов, например программно-определяемые подходы. Но для такой масштабной и традиционной сети, как наша, с типичными наборами компонентов и мейнфреймами оптимально подходило решение TrustSec. Другие инструменты не позволяли охватить 80 % нашей сети».*
>
> ~ Ведущий архитектор сетей, отдел сетевой безопасности, финансовая организация

- Представитель одной из компаний, участвовавших в исследовании, отметил, что выбор TrustSec для обеспечения сетевой безопасности на основе идентификаторов был обусловлен особенностями сети. Организация использовала обширную традиционную сеть с более чем 380 000 активных устройств, и другие подходы на основе идентификаторов не позволяли охватить 80 % этой сети.

Решение

Универсальная компания оценила различные альтернативные варианты сегментирования сети с прицелом на снижение рисков и создание эффективной модели ИТ-операций, которая бы обеспечивала масштабирование одновременно с ростом бизнеса, а также помогала выполнять требования регуляторов. Проект по внедрению сегментирования охватывал ЦОД, а также филиалы банка. Для выполнения требований регулятора универсальная компания провела оценку эффективности межсетевых экранов и программно-определяемого сегментирования TrustSec. Сегментирование на основе VLAN не позволяло обеспечить нормативное соответствие. После анализа масштабных и продолжительных инвестиций в межсетевые экраны и с учетом того, что в распоряжении банка уже была совместимая с TrustSec сетевая инфраструктура, универсальная компания приняла решение в пользу TrustSec.

Опрошенные клиенты рассматривали сети VLAN как дополнение к межсетевым экранам в качестве решений для сегментирования, служащих альтернативой программно-определяемому сегментированию TrustSec. Тем не менее существуют другие сценарии использования TrustSec, которые позволяют еще больше увеличить ценность этого решения. Эти сценарии включают:

- быструю локализацию угроз для изоляции атак и уязвимых устройств;
- ограничение горизонтального распространения угроз с помощью микросегментирования;
- снижение объема нормативных требований, например PCI;
- сегментирование IoT-устройств;
- упрощение управления доступом к экстранету для деловых партнеров и поставщиков;
- распространение корпоративных политик безопасности на гибридные облака и многооблачные среды.

В процессе оценки возможных инвестиций в решение TrustSec читателям рекомендуется проанализировать собственный сценарий использования этого решения и конкретные альтернативные варианты.

Результаты

В ходе интервью клиенты, использующие TrustSec, отметили следующие преимущества:

› **Экономия за счет исключения затрат на альтернативные традиционные решения для обеспечения сетевой безопасности.** Несколько опрошенных организаций отметили, что благодаря TrustSec они смогли избежать расходов на внедрение и управление VLAN и межсетевыми экранами, которые представляют собой более традиционную модель сетевой безопасности по периметру. Один ведущий архитектор сетей отметил: «Управление сетевой безопасностью с использованием межсетевых экранов — довольно дорогостоящий подход. Эта модель обеспечивает надежную внешнюю защиту, но уязвима изнутри, и потому не допускает компромиссов. Используя TrustSec, мы создаем нужный уровень контроля, а не полагаемся на элементы безопасности по периметру. Привлекательность TrustSec заключается в том, что в теории это решение можно развернуть в существующей сетевой инфраструктуре путем конфигурирования. При этом внедрять дорогостоящие межсетевые экраны не потребуется. Речь идет не просто о затратах на оборудование — необходимо учитывать расходы на осуществление проекта, уточнения и тестирование».Другой участник опроса также отметил, что при принятии решения о сегментировании сети «анализировались ожидаемые операционные расходы, устойчивость сети, ограничения пропускной способности и пропускная способность межсетевого экрана, которая может оказаться уязвимым местом. При использовании TrustSec пропускная способность не ограничивается. Таким образом, это решение несет в себе меньше инвестиционных рисков в сравнении с межсетевым экраном. Оно также требует меньших временных затрат. При этом TrustSec обеспечивает довольно низкий уровень операционных расходов».

› **Повышенная эффективность эксплуатации, исключающая необходимость найма дополнительных ИТ-специалистов.** Все опрошенные организации отмечали, что результатом внедрения решения TrustSec стало повышение эффективности ИТ-операций. Без TrustSec некоторые из них были бы вынуждены привлечь дополнительных ИТ-специалистов в области сетевых операций, чтобы обеспечить аналогичный уровень функциональности управления доступом в традиционной системе.

«Без TrustSec мы использовали бы ISE, а вместо меток безопасности — VLAN, сеть и различные политики. Их было бы от шести до восьми вместо одной, как сейчас. Таким образом, TrustSec значительно упрощает для нас обслуживание и администрирование сети. Мы сократили операционные расходы и на четверть снизили затраты на персонал».
— Разработчик сетевых архитектур ИТ, розничная сеть

«Если бы вместо TrustSec нам пришлось использовать межсетевые экраны, я думаю, что нам понадобилось бы еще 10 штатных сотрудников».

~ Ведущий архитектор сетей, отдел сетей передачи речевой информации и доменных сетей, финансовая организация

› **Повышение устойчивости сети и снижение риска простоев.** Используя TrustSec вместо более традиционного подхода на основе периметра, организации также смогли снизить риски и уровень сложности и сократить время простоев.

«Если бы мы не использовали TrustSec, я бы сравнивал это решение со следующей лучше всего подходящей под наши требования альтернативой. При работе с межсетевыми экранами в случае возникновения проблем мне потребовалось бы координировать две группы инженеров: сетевых инженеров и инженеров по безопасности. Сегментирование межсетевых экранов лишь повышает уровень сложности. С помощью TrustSec мы смогли улучшить общую устойчивость сети».
— Глава отдела сетевых сервисов одной из опрошенных организаций

› **Сокращение времени вывода проектов на рынок на 98 % по сравнению с решениями по сегментированию на основе VLAN.** Опрошенные компании также указывали на повышение гибкости, связанное с развертыванием TrustSec. Они обнаружили, что могут быстрее выводить на рынок проекты, например по использованию собственных устройств (BYOD). Участники исследования также отметили, что политика безопасности и другие изменения в сетевом доступе теперь реализуются быстрее. Как отметил представитель одной из финансовых организаций, «при использовании межсетевых экранов реализация изменений в инфраструктуре может быть достаточно затруднительной с точки зрения безопасности». Поскольку компании этой отрасли стремятся минимизировать риски, обычное изменение в традиционной среде межсетевого экрана потребовало бы от 4 до 6 недель, а срочное заняло бы несколько дней.

Розничная компания, использующая TrustSec для управления мобильным доступом с планшетных компьютеров и телефонов для более чем 5500 точек доступа, обнаружила, что время внедрения изменений сократилось на 98 %. Внести изменения в политику, позволяющую пользователям мобильных устройств в сети головного офиса использовать сеть магазинов (другую беспроводную сеть), удалось в течение 30 минут. По оценкам компании, без использования TrustSec эта процедура заняла бы 1–2 дня.

«С помощью TrustSec мы можем намного быстрее и проще вносить изменения без масштабной переработки».
— Разработчик сетевых архитектур ИТ, розничная сеть

› **Упрощение и автоматизация управления правилами межсетевых экранов и снижение соответствующих операционных расходов.** Благодаря TrustSec опрошенные компании автоматизировали управление правилами межсетевых экранов и повысили его эффективность. Автоматизация этих правил и администрирования списков управления доступом (ACL) также привела к сокращению расходов.

› **Соответствие нормативным требованиям.** Для некоторых опрошенных компаний соответствие нормативным требованиям было одним из главных преимуществ внедрения TrustSec. Как отметил один из банков, регуляторы были «полностью удовлетворены новыми решениями». Они одобрили подход банка к управлению правами пользователей, поскольку он связывал сетевую безопасность с ролью пользователя и приложения с помощью TrustSec.

«TrustSec позволяет нам создавать модели пользователей для каждого типа приложений и бизнес-процессов, а затем назначать права в соответствии с этой моделью. С помощью роли пользователя определяются роли в сетевых коммуникациях. Для этого требуется всего несколько секунд. При изменении роли доступ мгновенно меняется. Аудиторы были полностью удовлетворены этим подходом, который не ограничивался средой приложений (в противном случае утверждение требовало бы прохождения двух уровней согласования)».
— Глава отдела сетевых сервисов одной из опрошенных организаций

«Программа защиты от киберугроз, частью которой является TrustSec, призвана снизить риски параллельно с оптимизацией затрат. Мы стремимся минимизировать финансовые и репутационные риски. Одним из таких рисков может быть непрохождение проверки регулятора, результаты которой раскрываются публично. Это своего рода гонка вооружений, и мы должны предугадывать проблемы, опираясь на развивающиеся тенденции».
— Ведущий архитектор сетей, отдел сетевой безопасности, финансовая организация

› **Согласованное и эффективное сегментирование сети.** Все опрошенные организации отмечали возможность получения преимуществ за счет согласованного и эффективного сегментирования с помощью TrustSec. Они отметили, что решение TrustSec оказалось экономичным, поскольку позволило им управлять доступом на основе заданных ролей пользователей и Active Directory. Автоматизированное управление доступом предполагало, что выполнять сегментирование сети вручную не требуется.

› **Упрощение проектирования систем безопасности за счет упрощения политики безопасности.** Участники опроса неоднократно говорили об упрощении проектирования систем безопасности за счет упрощения политики безопасности как непосредственного преимущества внедрения TrustSec. Ключевым фактором такого упрощения является возможность задавать политику безопасности на основе идентификационных данных, а не IP-адреса.

«Политики безопасности стали более понятными, краткими и доступными для чтения. С помощью решения TrustSec мы повысили уровень безопасности».
— Разработчик сетевых архитектур ИТ, розничная сеть

«Мы дали регуляторам обязательства снизить риски с помощью надлежащих и доступных для демонстрации средств контроля. Решение TrustSec оказалось самым экономичным способом выполнить эти обязательства, поскольку использование межсетевых экранов лишь усложнило бы нашу задачу».

~ Ведущий архитектор сетей, отдел сетевой безопасности, финансовая организация

› **Повышение уровня гибкости и возможность масштабирования политики безопасности.** Используя TrustSec, опрошенные компании также смогли повысить гибкость и оптимизировать масштабирование политики безопасности в сравнении с более традиционным подходом на основе межсетевых экранов. Представитель одной из них отметил, что изменения межсетевого экрана становятся серьезной проблемой при запуске новых проектов. С решением TrustSec новые изменения можно внедрить быстрее. Это упрощает требования к будущим проектам. По словам другого респондента, TrustSec позволяет масштабировать политику безопасности и быстрее реализовывать новые проекты. «Мы более гибко выполняем зонирование [сегментирование], — подчеркнул руководитель отдела сетевых сервисов. — Нам не приходится оценивать, справится ли межсетевой экран с дополнительной нагрузкой». Это также позволило более эффективно планировать проекты и несколько сократить время их осуществления.

› **Повышение уровня защищенности сети.** Опрошенные компании отмечали повышение уровня безопасности в связи с внедрением решения TrustSec. Они наблюдают большую защищенность сети, повышение прозрачности, а в некоторых случаях — оптимизацию защиты от киберугроз и улучшенную безопасность ЦОД.

«Правила доступа в зависимости от типа пользователя, а не IP-адреса позволяют получать больше данных о действиях пользователей. Мы можем сопоставить их с несанкционированными действиями под определенной учетной записью. TrustSec обеспечивает для нас прозрачность. Это решение дает возможность выявить нарушителя, а не только место нарушения».
— Разработчик сетевых архитектур ИТ, розничная сеть

ВЫГОДЫ

Универсальная компания в данном примере внедрения получила ряд преимуществ, которые могут быть выражены количественно:

- экономия за счет исключения затрат на альтернативные решения на основе периметра;
- снижение затрат на ИТ-операции;
- повышение устойчивости сети и снижение риска простоев.

Исключение затрат на альтернативные традиционные решения на основе периметра

По мнению респондентов, стоимость решения TrustSec была ниже в сравнении с альтернативными решениями. Без TrustSec розничной компании потребовалось бы внедрить решение VDI (инфраструктуру виртуального рабочего стола) для создания дифференцированных уровней доступа для мобильных пользователей в магазинах и понести дополнительные затраты. Решение TrustSec позволяет использовать единый пул пользователей, привязанный к одному ресурсу. Один из разработчиков сетевых архитектур ИТ отметил: «Нам пришлось бы использовать разные пулы для разных пользователей и неэффективно эксплуатировать оборудование. Понадобилось бы дополнительное пространство: пять различных пулов для VDI и область управления пулами».

Компании, которые проводили оценку более традиционных решений на основе периметра, например межсетевых экранов, также указывают на высокую стоимость этой альтернативы. По свидетельству одной организации, внедрение конфигурации межсетевого экрана с учетом высоких требований к пропускной способности и устойчивости сети стоило бы ей 330 000 долл. США. Чтобы реализовать функции, аналогичные решению TrustSec, понадобилось бы 400 дополнительных межсетевых экранов, что делало эту альтернативу абсолютно нерентабельной. Другая компания отметила, что хотя ее первоначальные инвестиции в TrustSec и были значительными, затраты на ежегодное обслуживание отсутствуют (в отличие от альтернативных решений). Помимо ежегодной экономии, инвестиционные риски ниже, чем при внедрении межсетевого экрана. Один из респондентов рассказал: «По мере роста объема данных, проходящих через межсетевой экран, возникает необходимость в новых инвестициях в оборудование. С TrustSec такой проблемы не возникает».

Благодаря использованию TrustSec вместо альтернативного традиционного решения на основе периметра, универсальной компании удалось сэкономить 1,65 млн долл. США на первоначальных инвестициях в инфраструктуру и 550 000 долл. США на ежегодном обслуживании традиционного решения. Общая экономия за три года составила 3,3 млн долл. США.

Опрошенные компании прибегали к различным сценариям внедрения TrustSec. Сумма экономии различалась в зависимости от организации, и для выравнивания этих расхождений данная выгода была скорректирована с учетом рисков и снижена на 5 %. Итоговая выгода от исключения затрат на традиционные решения на основе периметра с поправкой на риски составила 3 135 000 долл. США. Подробный расчет представлен ниже в таблице 1. Дополнительную информацию см. в разделе «Риски».

ТАБЛИЦА 1

Исключение затрат на альтернативные решения

Обозн.	Показатель	Расчет	Год 1	Год 2	Год 3	Всего	Приведенное значение
A1	Первоначальные инвестиции в инфраструктуру		1 650 000 долл. США				
A2	Текущее обслуживание		550 000 долл. США	550 000 долл. США	550 000 долл. США		
At	Исключение затрат на альтернативные традиционные решения для обеспечения безопасности по периметру	A1 + A2	2 200 000 долл. США	550 000 долл. США	550 000 долл. США	3 300 000 долл. США	2 867 769 долл. США
	Поправка на риски	↓5 %					
Atr	**Исключение затрат на альтернативные традиционные решения для обеспечения безопасности по периметру (с поправкой на риски)**		**2 090 000 долл. США**	**522 500 долл. США**	**522 500 долл. США**	**3 135 000 долл. США**	**2 724 380 долл. США**

Источник: корпорация Forrester Research

Снижение операционных затрат

Опрошенные компании также отмечали снижение операционных затрат как преимущество от внедрения решения TrustSec. Эта экономия обеспечивалась «простотой управления» TrustSec по сравнению с другими решениями. По оценкам одного из респондентов, внедрение TrustSec на 80 % сократило количество времени, которое сетевые инженеры и инженеры по безопасности тратят на управление доступом. Эта цифра включает время, потраченное на внесение изменений в роли и процесс утверждения. Представитель другой компании отметил: «Нам потребовалось бы больше сотрудников, но не для решения повседневных задач, а для реализации изменений, внедрения новых ролей или предоставления доступа новым пользователям». По словам респондентов, без TrustSec им потребовалось быть привлечь дополнительный персонал для ИТ-операций. Экономия от исключения затрат на наем этого персонала составила от 1 до 10 полных ставок. Операционные расходы на ИТ в опрошенных компаниях сократились на 25–80 %.

Без внедрения TrustSec универсальной компании потребовалось бы нанять еще четверых сетевых инженеров. При среднем размере годовой заработной платы инженера на полной ставке в 105 600 долл. США это подразумевает сокращение операционных затрат на ИТ на 422 400 долл. США в год.

Компания Forrester скорректировала этот показатель с учетом рисков и вариативности, снизив его на 10 %; таким образом, в расчете учтена ежегодная выгода в размере 380 160 долл. США. Общая экономия от снижения операционных расходов универсальной компании за три года составила 1,14 млн долл. США. Подробный расчет представлен ниже в таблице 2. Дополнительную информацию см. в разделе «Риски».

ТАБЛИЦА 2
Снижение операционных затрат

Обозн.	Показатель	Расчет	Год 1	Год 2	Год 3	Всего	Приведенное значение
B1	Количество дополнительных сетевых инженеров (не нанятых)		4	4	4		
B2	Ежегодные расходы на человека		105 600 долл. США	105 600 долл. США	105 600 долл. США		
Bt	Сокращение операционных затрат — дополнительная ставка	B1 * B2	422 400 долл. США	422 400 долл. США	422 400 долл. США	1 267 200 долл. США	1 050 446 долл. США
	Поправка на риски	↓10 %					
Btr	**Сокращение операционных затрат — дополнительная ставка (с поправкой на риски)**		**380 160 долл. США**	**380 160 долл. США**	**380 160 долл. США**	**1 140 480 долл. США**	**945 402 долл. США**

Источник: корпорация Forrester Research

Повышение устойчивости сети — снижение риска простоев

В числе преимуществ внедрения TrustSec упоминалось повышение устойчивости сети. Более традиционное сетевое решение, например межсетевой экран, повысило бы уровень сложности и потребовало бы более тщательной координации между различными отделами в процессе устранения проблем.

Глава отдела сетевых сервисов также отметил, что убытки финансовой организации в результате простоя могут исчисляться миллионами долларов, особенно если сбой повлиял на торговую площадку.

За счет внедрения TrustSec универсальной компании удалось сократить время устранения проблем и повысить устойчивость сети. Риск простоя снизился на 1 час для крупного сбоя. При частоте сбоев один раз в год решение TrustSec позволило компании избежать потери дохода в результате простоя и рабочего времени сотрудников. Следуя консервативному принципу оценки, при анализе компания Forrester использует снижение рисков простоев, выраженное в сэкономленном рабочем времени. Стоимость простоев на пользователя в час рассчитывается как функция средней почасовой заработной платы сотрудника. Читатели также могут самостоятельно рассчитать влияние простоев на бизнес своего предприятия.

Для 4000 пользователей и стоимости 1 часа простоя 37,81 долл. США на пользователя общая экономия за счет повышения устойчивости сети и снижения риска простоев составила 151 250 долл. США в год. С учетом широкой вариативности стоимости простоя для разных компаний данная выгода была скорректирована с учетом рисков и снижена на 15 %. Скорректированная совокупная выгода от снижения риска простоев составила 128 563 долл. США в год. За три года она позволила компании сэкономить 385 688 долл. США. Подробный расчет представлен ниже в таблице 3. Дополнительную информацию см. в разделе «Риски».

ТАБЛИЦА 3

Повышение устойчивости сети и снижение риска простоев

Обозн.	Показатель	Расчет	Год 1	Год 2	Год 3	Всего	Приведенное значение
C1	Число пользователей		4000	4000	4000		
C2	Количество инцидентов в год		1	1	1		
C3	Стоимость простоя на пользователя		37,81 долл. США	37,81 долл. США	37,81 долл. США		
Ct	Повышение устойчивости сети и снижение риска простоев	C1 * C2 * C3	151 250 долл. США	151 250 долл. США	151 250 долл. США	453 750 долл. США	376 136 долл. США
	Поправка на риски	↓15 %					
Ctr	**Повышение устойчивости сети и снижение риска простоев (с поправкой на риски)**		**128 563 долл. США**	**128 563 долл. США**	**128 563 долл. США**	**385 688 долл. США**	**319 716 долл. США**

Источник: корпорация Forrester Research

Совокупные выгоды

В таблице 4 показана общая сумма вышеописанных выгод, а также их приведенная стоимость, сниженная на 10 % в целях корректировки. Универсальная компания прогнозирует, что через три года совокупные выгоды с поправкой на риски будут равны приведенной стоимости, которая составляет около 4 млн долл. США.

ТАБЛИЦА 4

Совокупные выгоды (с поправкой на риски)

Обозн.	Категория выгоды	Год 1	Год 2	Год 3	Всего	Приведенное значение
Atr	Исключение затрат на альтернативные традиционные решения для обеспечения безопасности по периметру	2 090 000 долл. США	522 500 долл. США	522 500 долл. США	3 135 000 долл. США	2 724 380 долл. США
Btr	Снижение операционных затрат	380 160 долл. США	380 160 долл. США	380 160 долл. США	1 140 480 долл. США	945 402 долл. США
Ctr	Повышение устойчивости сети и снижение риска простоев	128 563 долл. США	128 563 долл. США	128 563 долл. США	385 688 долл. США	319 716 долл. США
	Совокупные выгоды (с поправкой на риски)	**2 598 723 долл. США**	**1 031 223 долл. США**	**1 031 223 долл. США**	**4 661 169 долл. США**	**3 989 498 долл. США**

Источник: корпорация Forrester Research

ЗАТРАТЫ

Универсальная компания понесла ряд затрат, связанных с внедрением TrustSec:

- затраты на инфраструктуру TrustSec;
- расширенные услуги Cisco — затраты на проектирование TrustSec;
- оплата профессиональных услуг;
- внутренние работы по внедрению и тестированию;
- затраты на администрирование и поддержку.

Эти затраты, понесенные универсальной компанией в связи с первоначальным планированием, внедрением и текущим обслуживанием решения, являются как внутренними, так и внешними.

Затраты на инфраструктуру TrustSec

Опрошенные организации подчеркивали важность планирования и обеспечения совместимости сетевой инфраструктуры с TrustSec. Один участник опроса отметил, что некоторые категории устройств не поддерживают TrustSec, однако компания смогла избежать дополнительных затрат на сетевую инфраструктуру, поскольку ранее уже приобрела высококлассное оборудование Cisco серий 3800 и 4000. Также следует обратить внимание, что решение TrustSec может работать на смешанных устройствах (в сетях, совместимых и несовместимых с TrustSec). Компания Forrester рекомендует проконсультироваться со специалистами Cisco относительно требований к сетевой инфраструктуре для TrustSec в конкретном сценарии использования.

Универсальная компания внедряла решение TrustSec после плановой замены устаревшей сетевой инфраструктуры. В результате компания не понесла дополнительных затрат на инфраструктуру для TrustSec. Она инвестировала 330 000 долл. США в Cisco ISE и необходимые лицензии. В приведенном расчете с учетом вариативности оценок была выполнена корректировка этой суммы с учетом рисков в размере 5 %; таким образом, за три года общая сумма затрат составила 346 500 долл. США.

Поскольку расходы зависят от конкретной организации, а именно сценария использования решения TrustSec, затраты на инфраструктуру для внедрения TrustSec могут значительно различаться, особенно если решение внедряется отдельно от стандартного обновления сетевой инфраструктуры. Компания Forrester настоятельно рекомендует учесть реальные обстоятельства и сценарий использования TrustSec и обратиться к специалистам Cisco для оценки затрат на инфраструктуру.

Расширенные услуги Cisco — затраты на проектирование TrustSec

Универсальная компания выплатила Cisco 220 000 долл. США за услуги низкоуровневого и высокоуровневого проектирования в рамках внедрения решения TrustSec. Расходы на расширенные услуги Cisco составили 220 000 долл. США. После корректировки с учетом рисков на 5 % общая сумма затрат составила 231 000 долл. США.

Оплата профессиональных услуг

Универсальная компания также потратила 385 000 долл. США на профессиональные услуги по внедрению TrustSec. Использование профессиональных услуг по внедрению TrustSec обычно зависит от желания компании обращаться к внешним консультантам в рамках ИТ-проектов. Половина опрошенных компаний пользовалась профессиональными услугами. В приведенном расчете выполнена корректировка затрат с учетом рисков в размере 5 %; таким образом, за три года общая сумма составила 404 250 долл. США.

Внутренние работы по внедрению и тестированию

Несколько респондентов рассказали о затратах на большой объем внутренних работ по тестированию в сравнении с обычной эксплуатацией решения TrustSec. «Средства, потраченные на тестирование коммутаторов, значительно превысили наши прежние расходы», — отметил один из руководителей отделов сетевых сервисов. В универсальной компании два старших специалиста по ИТ-операциям, работающие на полную ставку, в течение шести месяцев занимались внедрением TrustSec. При среднегодовой заработной плате в размере 118 800 долл. США внутренняя стоимость работ по внедрению TrustSec составила 118 800 долл. США. Учитывая вариативность проектов по внедрению, эти затраты были скорректированы с учетом рисков на 10 % — до 130 680 долл. США.

Необходимо учесть, что сценарий использования TrustSec в значительной степени влияет на продолжительность внедрения. Один из опрошенных клиентов имел детальные требования к системе доступа, изначально не реализуемые в бинарной архитектуре TrustSec. В результате сроки внедрения увеличились, поскольку Cisco потребовалось время на добавление необходимой технической функции.

ТАБЛИЦА 5

Внутренние работы: внедрение и тестирование

Обозн.	Показатель	Расчет	Исходное значение	Год 2	Год 3	Всего	Приведенное значение
G1	Количество инженеров, необходимое для первоначального внедрения		2				
G2	Продолжительность внедрения (месяцы)		6				
G3	Ежегодные расходы на человека		118 800 долл. США				
Gt	Внутренние работы: внедрение и тестирование	(G1 * G2) + G3	118 800 долл. США			118 800 долл. США	118 800 долл. США
	Поправка на риски	↑10 %					
Gtr	**Внутренние работы: внедрение и тестирование (с поправкой на риски)**		**130 680 долл. США**			**130 680 долл. США**	**130 680 долл. США**

Источник: корпорация Forrester Research

Затраты на администрирование и поддержку

Хотя тестирование новых версий TrustSec и является более трудоемкой задачей, одна из опрошенных организаций отметила, что эти затраты по мере расширения сети не возрастают, в отличие от более традиционных решений. «Это постоянная величина. Она не растет по мере расширения сети. Объем работы одинаков, будь то 1000 или 50 коммутаторов. Однако если вы добавите 50 новых межсетевых экранов, потребуется привлечь еще 10 сотрудников».

В универсальной компании было выделено два инженера по ИТ-операциям, осуществляющих текущее тестирование регулярных обновлений сетевого ПО и администрирование решения. Такое администрирование также включает в себя устранение неполадок, оценку функций и другие задачи, касающиеся TrustSec, но не связанные с операциями. При полной занятости инженера по ИТ-операциям его заработная плата составляет 105 600 долл. США в год. Таким образом, расходы на администрирование и тестирование в универсальной компании будут равны 211 200 долл. США в год. С учетом вариативности ресурсов, необходимых для администрирования и тестирования TrustSec, эта сумма была скорректирована с учетом рисков и возросла на 5 %. Итоговые совокупные затраты составили 221 760 долл. США в год.

ТАБЛИЦА 6
Затраты на администрирование и тестирование

Обозн.	Показатель	Расчет	Год 1	Год 2	Год 3	Всего	Приведенное значение
H1	Число сотрудников		2	2	2		
H2	Ежегодные расходы на человека		105 600 долл. США	105 600 долл. США	105 600 долл. США		
Ht	Затраты на администрирование и тестирование	H1 * H2	211 200 долл. США	211 200 долл. США	211 200 долл. США	633 600 долл. США	525 223 долл. США
	Поправка на риски	↑5 %					
Htr	**Затраты на администрирование и тестирование (с поправкой на риски)**		**221 760 долл. США**	**221 760 долл. США**	**221 760 долл. США**	**665 280 долл. США**	**551 484 долл. США**

Источник: корпорация Forrester Research

Общие затраты

В таблице 7 показана общая сумма затрат, а также соответствующая приведенная стоимость, сниженная на 10 %. Через три года совокупные затраты будут равны общей чистой приведенной стоимости, которая составляет около 1,66 млн долл. США.

ТАБЛИЦА 7

Совокупные затраты (с поправкой на риски)

Обозн.	Ценовая категория	Исходное значение	Год 1	Год 2	Год 3	Всего	Приведенное значение
Dtr	Затраты на инфраструктуру TrustSec	346 500 долл. США	0 долл. США	0 долл. США	0 долл. США	346 500 долл. США	346 500 долл. США
Etr	Расширенные услуги Cisco — затраты на проектирование TrustSec	231 000 долл. США	0 долл. США	0 долл. США	0 долл. США	231 000 долл. США	231 000 долл. США
Ftr	Профессиональные услуги — внедрение	404 250 долл. США	0 долл. США	0 долл. США	0 долл. США	404 250 долл. США	404 250 долл. США
Gtr	Внутренние работы: внедрение и обучение	130 680 долл. США	0 долл. США	0 долл. США	0 долл. США	130 680 долл. США	130 680 долл. США
Htr	Затраты на администрирование и тестирование	0 долл. США	221 760 долл. США	221 760 долл. США	221 760 долл. США	665 280 долл. США	551 484 долл. США
	Совокупные затраты (с поправкой на риски)	**1 112 430 долл. США**	**221 760 долл. США**	**221 760 долл. США**	**221 760 долл. США**	**1 777 710 долл. США**	**1 663 914 долл. США**

Источник: корпорация Forrester Research

ГИБКОСТЬ

В методологии TEI под гибкостью понимается инвестиция в дополнительные мощности или возможности, которые можно будет превратить в бизнес-преимущество при условии некоторых дополнительных инвестиций в будущем. Это дает организации так называемый реальный опцион — право, но не обязанность предпринять какие-либо инициативы в будущем. Существует ряд сценариев, в соответствии с которыми клиенты могут выбрать внедрение TrustSec с последующим расширением использования и реализацией новых бизнес-возможностей. Гибкость также может быть измерена количественно при оценке в рамках определенного проекта (более подробно см. в приложении A).

«Вместе с Cisco мы проделали большой объем работы по разработке концепции безопасной среды, чтобы сторонние поставщики могли взаимодействовать с TrustSec. С помощью этого решения мы создали масштабную сеть партнеров».

— Ведущий архитектор сетей, отдел сетевой безопасности, финансовая организация

В процессе реализации новых проектов, требующих сегментирования сетей, организации могут открывать для себя дополнительные преимущества. Так, один из респондентов рассказал о внедрении новой среды eBusiness на основе TrustSec; по его оценке, использование межсетевого экрана увеличило бы сроки реализации проектов на несколько недель и привело бы к дополнительным затратам на оборудование. Экономия затрат и времени на реализацию проектов — именно те преимущества, которые компании могут получить при осуществлении каждого последующего проекта в сети. Расширение сети, например слияние или поглощение, также может стать источником дополнительных преимуществ. Несколько компаний отметили, что по мере развития и добавления новых функций они смогут получить от TrustSec еще больше преимуществ. Теперь эти организации могут более эффективно использовать имеющееся ПО и продукты других поставщиков с помощью решения Cisco Platform Exchange Grid (pxGrid). По мере добавления новых возможностей контроля и аналитики в продукты TrustSec организации также могут получить дополнительные преимущества с точки зрения принятия решений, связанных с безопасностью.

Ценность гибкости индивидуальна для каждой организации, и стремление давать ей количественную оценку у разных компаний различается.

РИСКИ

Компания Forrester определяет два типа рисков, связанных с данным анализом: риск внедрения и риск воздействия. Риск внедрения — это риск изменения суммы предполагаемых инвестиций в TrustSec, что может вызвать рост издержек. Риск воздействия предполагает, что бизнес- или технологические потребности организации могут быть не удовлетворены результатами инвестиций в решение TrustSec, что приведет к более низким совокупным выгодам. Чем больше неопределенность, тем шире потенциальный диапазон возможных результатов оценки затрат и выгод.

ТАБЛИЦА 8
Корректировка выгод и затрат с учетом рисков

Выгоды	Корректировка
Исключение затрат на альтернативные традиционные решения для обеспечения безопасности по периметру	↓ 5 %
Снижение операционных затрат	↓ 10 %
Повышение устойчивости сети и снижение риска простоев	↓ 15 %

Затраты	Корректировка
Внутренние работы: внедрение и обучение	↑ 10 %
Все остальные затраты TrustSec	↑ 5 %

Источник: корпорация Forrester Research

Количественное выражение риска внедрения и риска воздействия путем прямой коррекции финансовых оценок позволяет получать более точные и содержательные результаты и более выверенный прогноз окупаемости инвестиций. В общем случае влияние рисков на затраты выражается в увеличении исходных оценок, а на выгоды — в уменьшении исходных оценок. Скорректированные с учетом рисков цифры следует рассматривать как «реалистичные» ожидания, поскольку они представляют собой ожидаемые значения с учетом риска.

В ходе данного анализа были выявлены следующие риски воздействия, которые влияют на выгоды:

- Выгоды для заказчиков могут меняться в зависимости от среды, количества пользователей и определенных сценариев использования TrustSec.
- Стоимость простоев зависит от заказчика и оценки выгоды от повышения устойчивости сети.

В рамках этого анализа определяются следующие риски внедрения, влияющие на издержки и выгоды:

- Затраты на внедрение TrustSec могут значительно различаться в зависимости от текущей среды сети заказчика и объема внедрения. Затраты возрастают, если заказчику также требуется обновить свое сетевое оборудование за счет устройств, совместимых с TrustSec, отдельно от регулярного процесса обновления сетевой инфраструктуры.
- Потребности компаний во внедрении решения TrustSec зависят от текущей структуры их сетевых операций и кадрового состава специалистов по безопасности.

В таблице 8 приведены значения, используемые для корректировки оценок затрат и выгод с учетом рисков и неопределенностей для универсальной компании. Читателям настоятельно рекомендуется применять собственные диапазоны рисков в зависимости от степени уверенности в оценках затрат и выгод.

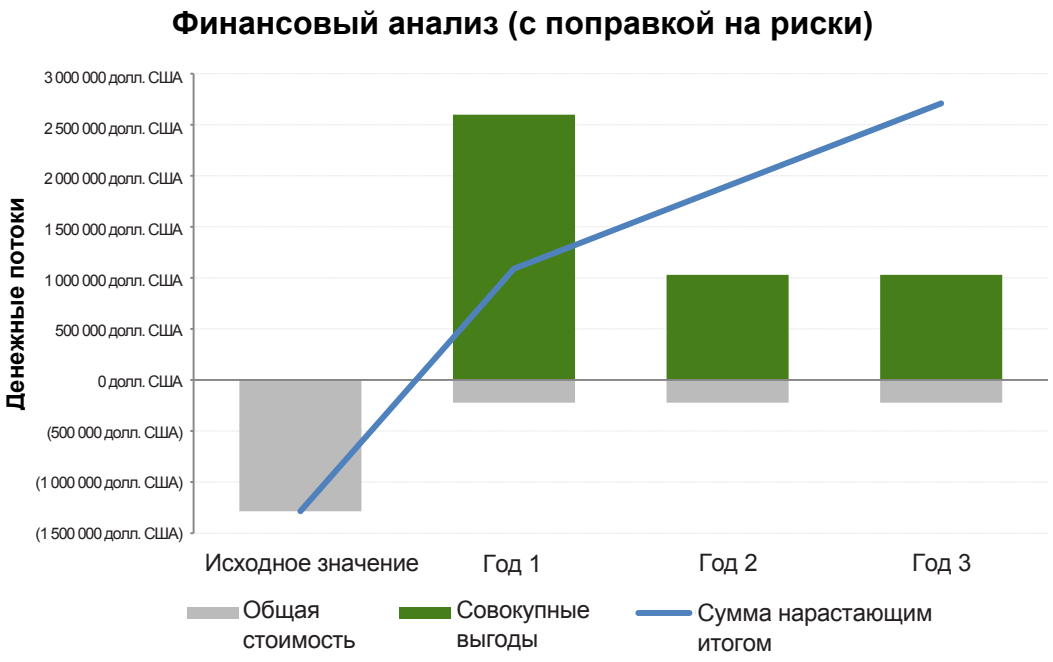
Финансовая сводка

Финансовые результаты, рассчитанные в разделах «Выгоды» и «Затраты», могут использоваться для определения окупаемости инвестиций, чистой приведенной стоимости и срока окупаемости применительно к инвестициям универсальной компании в TrustSec.

В таблице 9 приведены скорректированные с учетом рисков окупаемость инвестиций (ROI), чистая текущая стоимость (NPV) и срок окупаемости. Эти значения определяются путем корректировки предварительных результатов из соответствующих разделов «Затраты» и «Выгоды» с учетом рисков, приведенных в таблице 8 из раздела «Риски».

РИС. 3

График денежных потоков (с поправкой на риски)



Источник: корпорация Forrester Research

ТАБЛИЦА 9

Денежный поток (с поправкой на риски)

	Исходное значение	Год 1	Год 2	Год 3	Всего	Приведенное значение
Затраты	(1 112 430 долл. США)	(221 760 долл. США)	(221 760 долл. США)	(221 760 долл. США)	(1 777 710 долл. США)	(1 663 914 долл. США)
Выгоды	0 долл. США	2 598 723 долл. США	1 031 223 долл. США	1 031 223 долл. США	4 661 169 долл. США	3 989 498 долл. США
Чистые выгоды	**(1 112 430 долл. США)**	**2 376 963 долл. США**	**809 463 долл. США**	**809 463 долл. США**	**2 883 459 долл. США**	**2 325 584 долл. США**
Окупаемость инвестиций						**140 %**
Срок окупаемости						**5,6 месяца**

Источник: корпорация Forrester Research

Cisco TrustSec: обзор решения

Следующая информация предоставлена компанией Cisco. Компания Forrester не проверяла и не подтверждает данные заявления или предложения Cisco.

Cisco TrustSec — это масштабируемая и гибкая программно-определяемая технология сегментирования (или микросегментирования), реализованная в программном и аппаратном виде на платформах Cisco и защищающая ресурсы, например данные, приложения и мобильные устройства, от несанкционированного доступа. В отличие от традиционных механизмов контроля доступа, основанных на топологии сети, элементы управления TrustSec определяются с использованием логического группирования политик, что обеспечивает постоянную поддержку сегментирования ресурсов и безопасного доступа даже при перемещении ресурсов в мобильных и виртуальных сетях. В TrustSec реализована технология идентификации на основе аппаратных средств, которая позволяет распознавать пользовательский трафик в сети без снижения производительности.

TrustSec использует Identity Services Engine (ISE) в качестве контроллера для идентификации и политику для всех средств контроля доступа и выхода. Эта политика легкодоступна и управляется из матрицы политик TrustSec Policy Matrix в ISE.

TrustSec Matrix in ISE: Egress Policy Example

В настоящее время решение TrustSec встроено более чем в 40 различных семейств продуктов Cisco и продуктов других поставщиков и применяется заказчиками в следующих целях:

- быстрая локализация угроз и изоляция атак;
- ограничение горизонтального распространения угроз с помощью сегментирования (микросегментирования);
- сегментирование сетей в комплексах зданий, филиалах и ЦОД;
- предоставление масштабируемых средств контроля доступа для BYOD и мобильности;
- снижение объема нормативных требований, например PCI;
- контроль доступа к внутренним приложениям в организациях из финансовой сферы и отрасли здравоохранения;
- сегментирование IoT-устройств;

- упрощение управления доступом к экстранету для деловых партнеров и поставщиков;
- последовательное распространение корпоративных политик безопасности на гибридные облака и многооблачные среды;
- упрощение управления политиками для снижения требований к ИТ-специалистам;
  предоставление информации о ролях в конечных точках для межсетевых экранов и средств мониторинга трафика.

Основные преимущества Cisco TrustSec:

- **Снижение уровня сложности** — устранение сложностей, связанных со списками контроля доступа на основе топологии благодаря понятным политикам.
- **Упрощение операций, связанных с безопасностью** — ускорение запуска серверов, а также переносов, дополнений и изменений. Возможность централизованного управления микросегментированием на уровне филиалов и комплексов зданий с помощью ISE.
- **Автоматизация** — автоматизация правил межсетевых экранов и администрирования ACL.
- **Безопасная мобильность** — активация мобильных политик в сетях филиалов, комплексов зданий и ЦОД.
- **Соответствие нормативным требованиям** — автоматическая поддержка соблюдения политик, когда пользователи получают доступ к данным из сети.

TrustSec является открытой технологией, поскольку компания Cisco передала форматы SXP и поточной маркировки Инженерному совету Интернета (IETF) для их использования сторонними производителями. ПО SXP с открытым исходным кодом теперь доступно для других поставщиков и заказчиков, которые могут напрямую интегрировать групповые политики TrustSec в собственные продукты. Кроме того, контроллер SDN с открытым исходным кодом OpenDaylight поддерживает SXP в версии Lithium.

Приложение A. Обзор методологии Total Economic Impact™

Total Economic Impact (TEI, совокупный экономический эффект) — это методология, разработанная Forrester Research для облегчения принятия компаниями решений об инвестировании в новые технологии, а также для помощи поставщикам в донесении до заказчиков ценностного предложения в отношении своих продуктов и услуг. Методология TEI позволяет компаниям продемонстрировать, обосновать и оценить практическую ценность ИТ-инициатив как с точки зрения высшего руководства, так и с точки зрения других ключевых заинтересованных лиц. TEI помогает поставщикам технологий привлекать, обслуживать и удерживать клиентов.

Методология TEI предполагает использование для оценки ценности инвестиций следующих четырех компонентов: выгоды, затраты, гибкость и риски.

ВЫГОДЫ

Выгоды представляют собой ценность, полученную компанией-пользователем — ИТ-отделом и (или) бизнес-подразделением — от внедрения предлагаемого продукта или проекта. Зачастую при обосновании продукта или проекта внимание уделяется исключительно ИТ-затратам и их сокращению, а не анализу влияния технологий на компанию в целом. В методологии TEI и получаемой в результате ее применения финансовой модели одинаковое место отводится определению выгод и измерению затрат, что дает возможность полностью изучить влияние внедрения технологий на всю компанию. Вычисление оценок выгод предполагает четкий диалог с компанией-пользователем для понимания конкретной получаемой ценности. Кроме того, компания Forrester требует наличия четкой прослеживаемости между измерением и обоснованием оценок выгод по завершении реализации проекта. Это обеспечивает непосредственную привязку выгод к итоговым результатам бизнес-деятельности.

ЗАТРАТЫ

Затраты представляют собой инвестиции, необходимые для извлечения ценности или выгод из предложенного проекта. ИТ-отдел или бизнес-подразделения могут нести затраты в виде трудозатрат (с учетом начислений на оплату труда), оплаты услуг субподрядчиков или стоимости материалов. В затратах учитываются все инвестиции и расходы, необходимые для получения предлагаемой ценности. Кроме того, категория затрат в методологии TEI отражает все дополнительные (дифференциальные) затраты по сравнению с существующими расходами, связанными с предлагаемым решением. Все затраты должны связываться с создаваемыми выгодами.

ГИБКОСТЬ

В методологии TEI прямые выгоды представляют собой только часть ценности инвестиций. Хотя прямые выгоды обычно являются главным фактором обоснования проекта, компания Forrester полагает, что компании должны иметь возможность измерить стратегическую ценность инвестиций. Под гибкостью понимается ценность, которую можно будет получить при условии некоторых будущих инвестиций в дополнение к уже сделанному первоначальному вложению. Например, инвестиции в модернизацию программного обеспечения для офисной работы в рамках всей организации могут повысить уровень стандартизации (тем самым повышая эффективность) и снизить затраты на лицензирование. Однако встроенные функции для совместной работы могут повысить производительность труда каждого сотрудника в случае их использования. Функции совместной работы могут быть использованы только при условии вложения дополнительных средств в обучение персонала в некоторый момент времени в будущем. Однако возможность получения этой будущей выгоды имеет приведенную ценность, которая может быть выражена количественно. Компонент «гибкость» в TEI отражает именно эту ценность.

РИСКИ

Риски представляют собой меру неопределенности, связанной с оценками выгод и затрат применительно к данным инвестициям. Неопределенность измеряется двумя способами: 1) как вероятность того, что оценки затрат и выгод будут соответствовать первоначальным прогнозам; 2) как вероятность того, что оценки будут измеряться и отслеживаться с течением времени. В методологии TEI факторы риска основаны на функции плотности вероятности, известной как треугольное распределение. Для оценки фактора риска для каждого показателя затрат и выгод вычисляются как минимум три значения.

Приложение Б. Глоссарий

Ставка дисконтирования (учетная ставка): процентная ставка, используемая в анализе денежных потоков для учета изменения стоимости денег с течением времени. Компании определяют собственные ставки дисконтирования на основе бизнес-среды и инвестиционной ситуации. В данном анализе компания Forrester предполагает, что ставка дисконтирования составляет 10 %. Как правило, компании используют ставки дисконтирования в пределах от 8 до 16 % в зависимости от текущей ситуации. Читателям настоятельно рекомендуется проконсультироваться со специалистами на предмет определения наиболее подходящей ставки дисконтирования для использования в расчетах для их компании.

Чистая приведенная стоимость (net present value, NPV): текущая стоимость (дисконтированных) будущих чистых денежных потоков при заданной процентной ставке (ставке дисконтирования). Положительная NPV проекта обычно говорит о том, что вкладывать в него средства целесообразно, кроме случаев, когда NPV альтернативных проектов выше.

Приведенная стоимость (present value, PV): текущая стоимость (дисконтированных) оценок затрат и выгод при заданной процентной ставке (ставке дисконтирования). Текущая стоимость затрат и выгод используется в расчете чистой приведенной стоимости денежных потоков.

Срок окупаемости: точка безубыточности капиталовложения. Момент времени, когда чистые выгоды (выгоды минус затраты) становятся равны первоначальным инвестициям или затратам.

Окупаемость инвестиций (return on investment, ROI): мера ожидаемой окупаемости проекта в процентном выражении. Окупаемость инвестиций вычисляется путем деления чистых выгод (выгод за вычетом затрат) на затраты.

ПРИМЕЧАНИЕ К ТАБЛИЦАМ ДЕНЕЖНЫХ ПОТОКОВ

Следующее примечание относится к таблицам денежных потоков, используемым в данном исследовании (см. таблицу-пример ниже). Столбец исходных инвестиций содержит затраты, понесенные на момент времени 0 или на начало года 1. Эти затраты не дисконтируются. Все остальные денежные потоки с первого по третий год дисконтируются по ставке дисконтирования, приведенной в разделе «Допущения модели», в конце года. Приведенная стоимость (PV) вычисляется для каждой оценки совокупных затрат и выгод. Чистая приведенная стоимость (NPV) не рассчитывается вплоть до составления сводных таблиц и представляет собой сумму исходных инвестиций и дисконтированных денежных потоков в каждом году.

Суммы и расчеты приведенной стоимости в таблицах «Совокупные выгоды», «Совокупные затраты» и «Денежный поток» не могут быть просто сложены из-за возможных округлений.

ТАБЛИЦА [ПРИМЕР]
Пример таблицы

Обозн.	Показатель	Расчет	Год 1	Год 2	Год 3

Источник: корпорация Forrester Research

ДОПУЩЕНИЯ МОДЕЛИ

Коэффициент скидки, используемый в расчетах приведенной стоимости и чистой приведенной стоимости, равен 10 %, а период времени, охватываемый финансовым моделированием, равен трем годам. Как правило, компании используют ставки дисконтирования в пределах от 8 до 16 % в зависимости от текущей ситуации. Читателям настоятельно рекомендуется проконсультироваться с финансовым отделом своей компании на предмет определения наиболее подходящей ставки дисконтирования для использования в своих расчетах.

Приложение B. Сноски

[1] Специалисты Forrester корректируют сводные финансовые показатели с учетом риска для учета возможного уровня неопределенности при оценке издержек и выгод. Дополнительную информацию см. в разделе «Риски».