Решения для защиты от продвинутых email угроз

Email безопасность, ориентированная на угрозы

Павел Родионов
CSE Security, Cisco Systems
29 сентября 2016

Электронная почта – это метод коммуникации #1

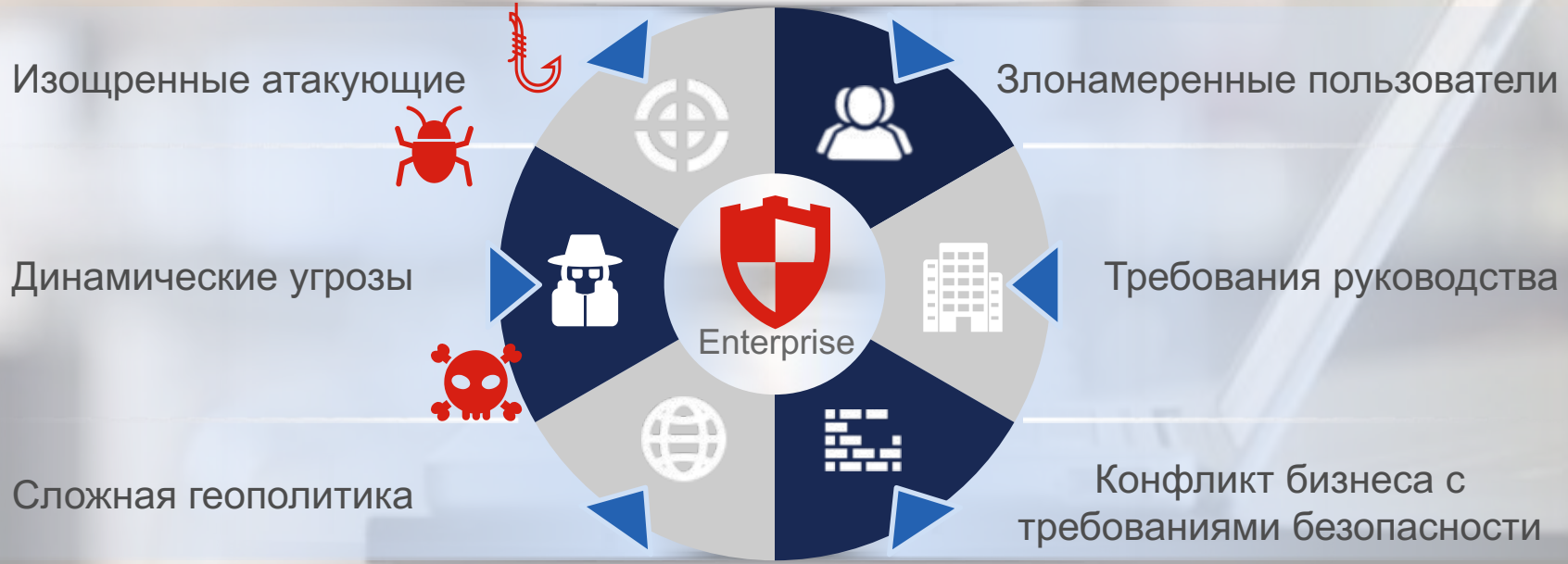
- Пользователей надо защищать от самих себя
- Безопасность всегда должна быть включена
- Сложность Email сообщений постоянно возрастает
- Защита корпоративной репутации и предотвращение утечек данных

© 2015 Cisco and/or its affiliates. All rights reserved.

Email – это вектор угроз №1

© 2015 Cisco and/or its affiliates. All rights reserved.

Проблемы безопасности могут возникнуть внезапно



© 2015 Cisco and/or its affiliates. All rights reserved.

Безопасность email не должна отставать
Точечные методы легко обходятся

- Сигнатурные решение слишком статические
- Сама по себе репутация не помогает от распределенных атак
- Постоянно изменяющиеся атаки на web скрывают угрозы
- Файловые атаки постоянно изменяются, чтобы избежать обнаружения
- Сама по себе видимость email имеет мало пользы без дополнительной информации

Требуется объединить все в одном общем решении

© 2015 Cisco and/or its affiliates. All rights reserved.

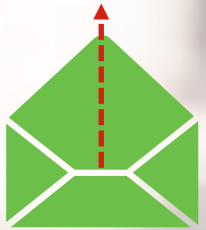
Фишинг держит бизнес «на крючке»

Фишинг

Спуфинг

Ransomware

94%
фишинг-писем имеют вредоносные вложения[1]



30%
фишинг сообщений открываются[1]

$500M

Потерь вызваны фишинг-атаками в США [2]

[1]2016 Cisco Annual Security Report
[2]2016 Verizon Data Breach Report, Kerbs on Security

Сообщения содержат вложения и URL'и

Социально ориентированные сообщения хорошо составлены и направлены

Зацепки учетных записей дают преступникам доступ к системам

Увеличивается количество спуфинг-писем

Фишинг

Спуфинг

Ransomware

$2.3B

Потерь от спуфинга в 2013 - 2015[1]

[1]FBI Warns of Dramatic Increase in Business email scams, 2016

Поддельные адреса обманывают получетелей

Злоумышленники активно изучают цели

Цель – деньги и информация

Ransomware атаки берут компании в заложники

Фишинг

Спуфинг

Ransomware

Ransomware представляет самый большой прыжок в активности криминального ПО[1]

9,515
пользователей в месяц платят выкуп[2]

$60M

Стоимость одной кампании для пользователей и организаций[2]

[1]2016 Verizon Data Breach Report, Kerbs on Security
[2]2016 Cisco Annual Security Report

Malware шифрует критические файлы

Крадет доступ к вашей собственной системе

Для получения доступа надо заплатить

По мере перемещения в облака безопасность email усложняется

Миграция на Office 365 создает новые риски

Gartner оценивает 60% адаптацию облака к 2022[1]

Access control

Data leaks

Infections

Visibility and Audits

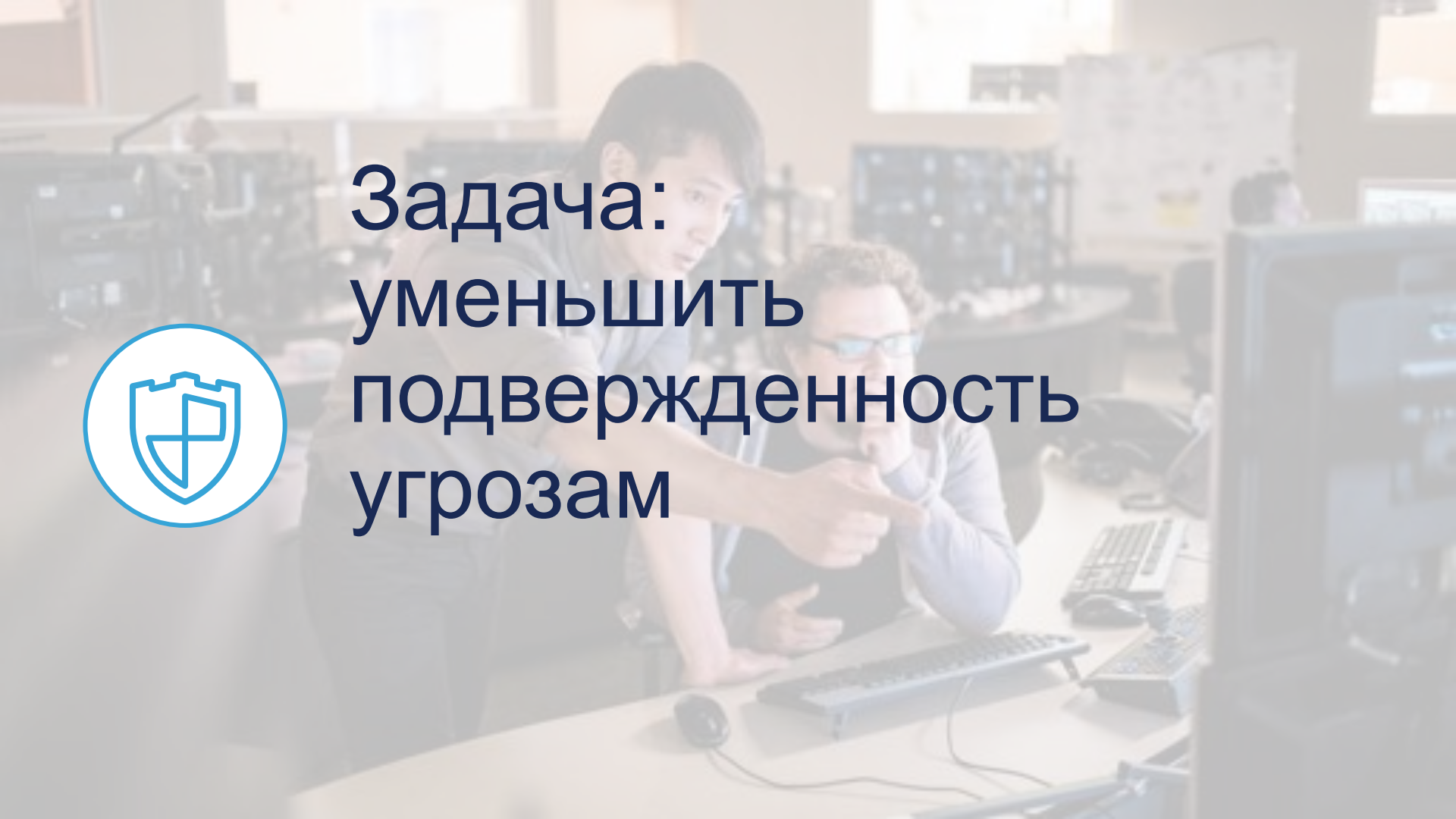
[1]Gartner Report “Office 365, Google Apps for Work and Other Cloud Office Key Initiative Overview” July 2015

Cisco защищает ваш email, облачный или локальный

Снижение количества угроз

Поддержка роста

Достигается гибкость



Задача: уменьшить подверженность угрозам


Software
Vulnerability Information
Reputation Center
Library
TALOS
Support Communities
About
Careers
Blog
Email Traffic Overview
100 TB
Of Data Received Daily
1.5 MILLION
Daily Malware Samples
600 BILLION
Daily Email Messages
16 BILLION
Daily Web Requests
24 • 7 • 365 Operations
250+
Full Time Threat Intel Researchers
MILLIONS
Of Telemetry Agents
4
Global Data Centers
Over 100
Threat Intelligence Partners
Global scanning
CISCO
30 years building the world's networks

Репутационная база Cisco Email

Информация об угрозах

- Более 1.6 миллиона глобальных устройств
- Историческая библиотека нескольких десятков тысяч угроз
- Ежедневная статистика о 35% глобального email трафика
- Ежедневно видим более 13 млрд веб запросов
- Отслеживается более 200 параметров
- Мультивендорный обзор

Преимущества

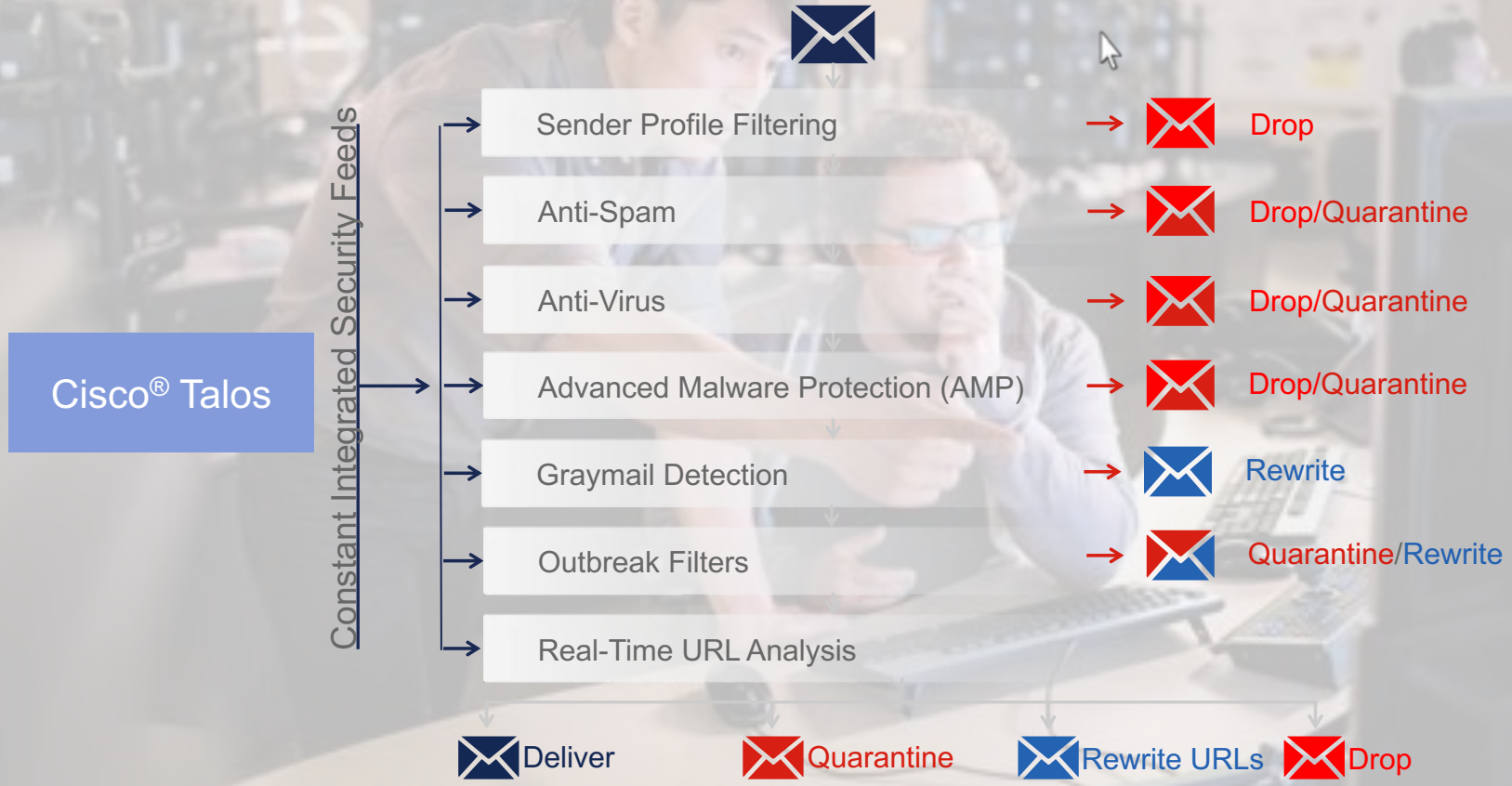
- Постоянный динамический обзор угроз 360 градусов
- Понятие уязвимостей и технологий эксплоитов
- Обзор самых мощных технологий атак
- Последние техники и тренды атак

Spam Traps	Complaint Reports	IP Blacklists and Whitelists
Message Composition Data	Compromised Host Lists	Website Composition Data
Global Volume Data	Domain Blacklist and Safelists	Other Data

© 2015 Cisco and/or its affiliates. All rights reserved.

Защита от угроз Cisco Email Security

Полная безопасность



Построено с наилучшей защитой от спама

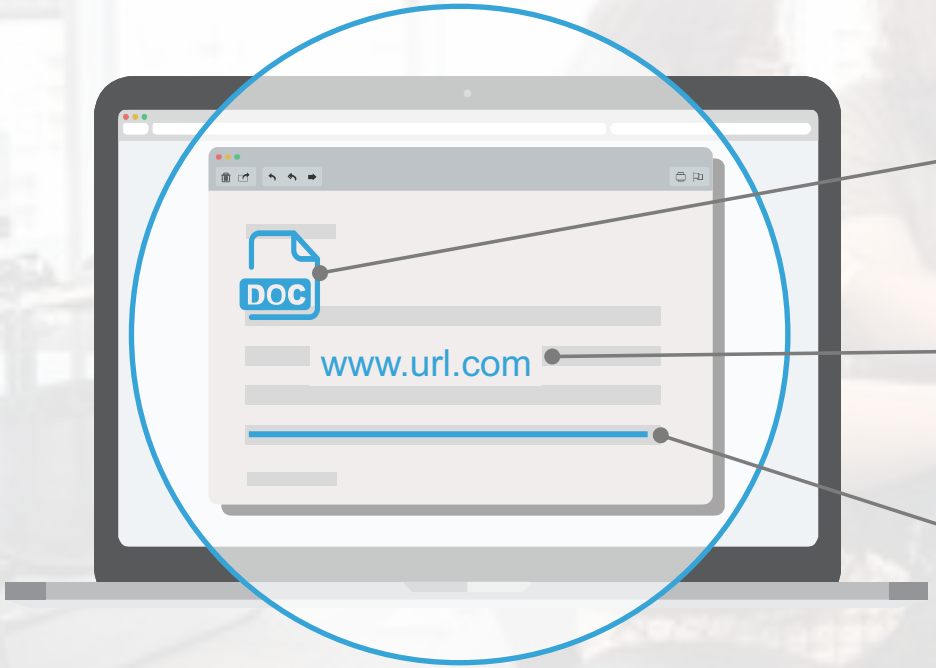
Антиспам / Context Adaptive Scanning Engine (CASE)

Анализ репутации отправителя, репутации URL и содержимое сообщения

Блокирование спама с точностью 99% с количеством ложных срабатываний менее 1 на 1 млн.

Карантин подозрительных сообщений для анализа

Снижает вероятность атаки через три основных компонента email



Вложения

URLи

Содержимое

Вложения

Защита от

Ransomware

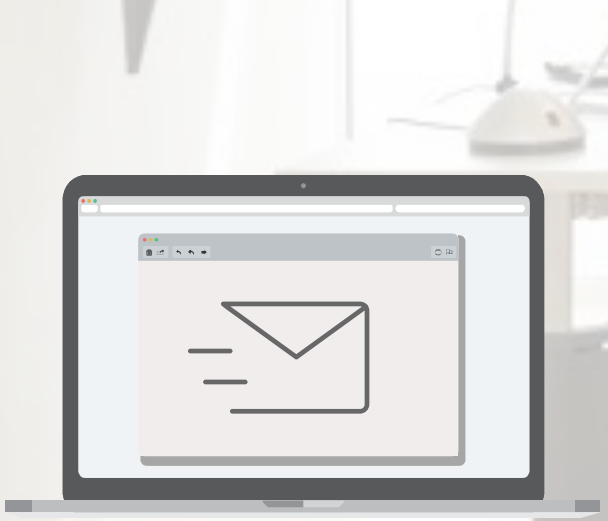
Фишинг

Остановить вредоносные сообщения, которые выглядят легитимными

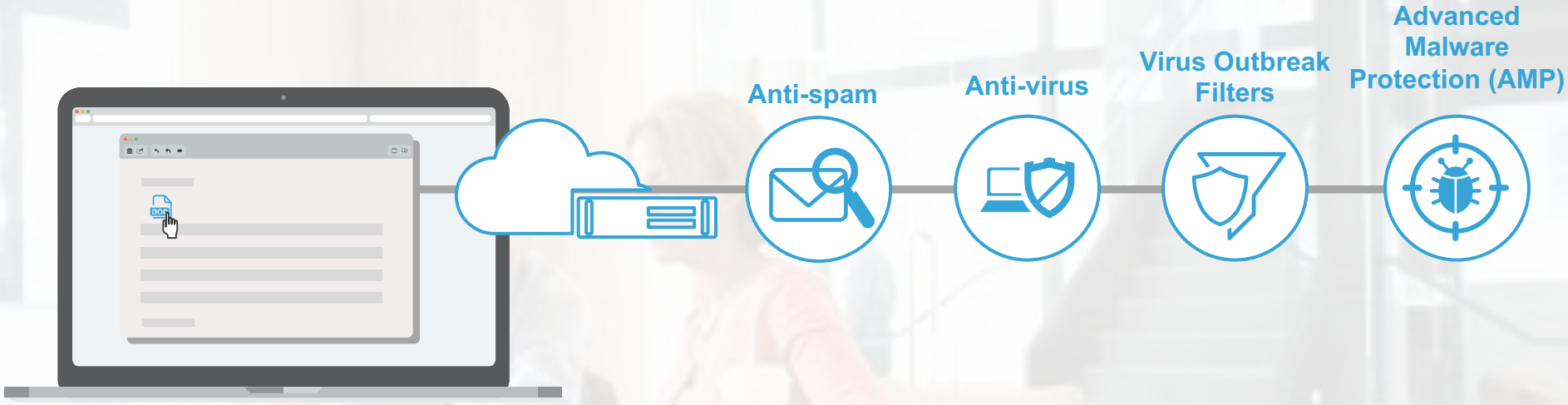
Василий из отдела кадров получает сообщения с вложениями-резюме

Все выглядит нормально, Василий открывает вложение

Исполняемый файл загружает malware без его уведомления

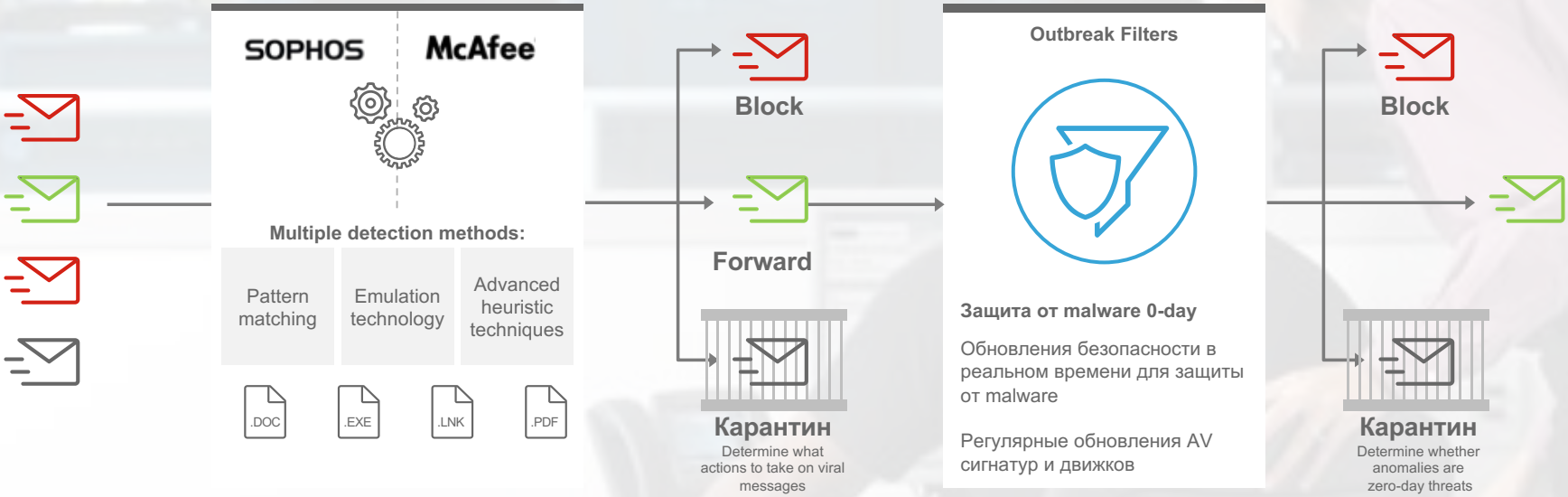


Cisco защищает от угроз, скрытых во вложениях



Блокирование известых и вирусов 0-day

Защита от вирусов



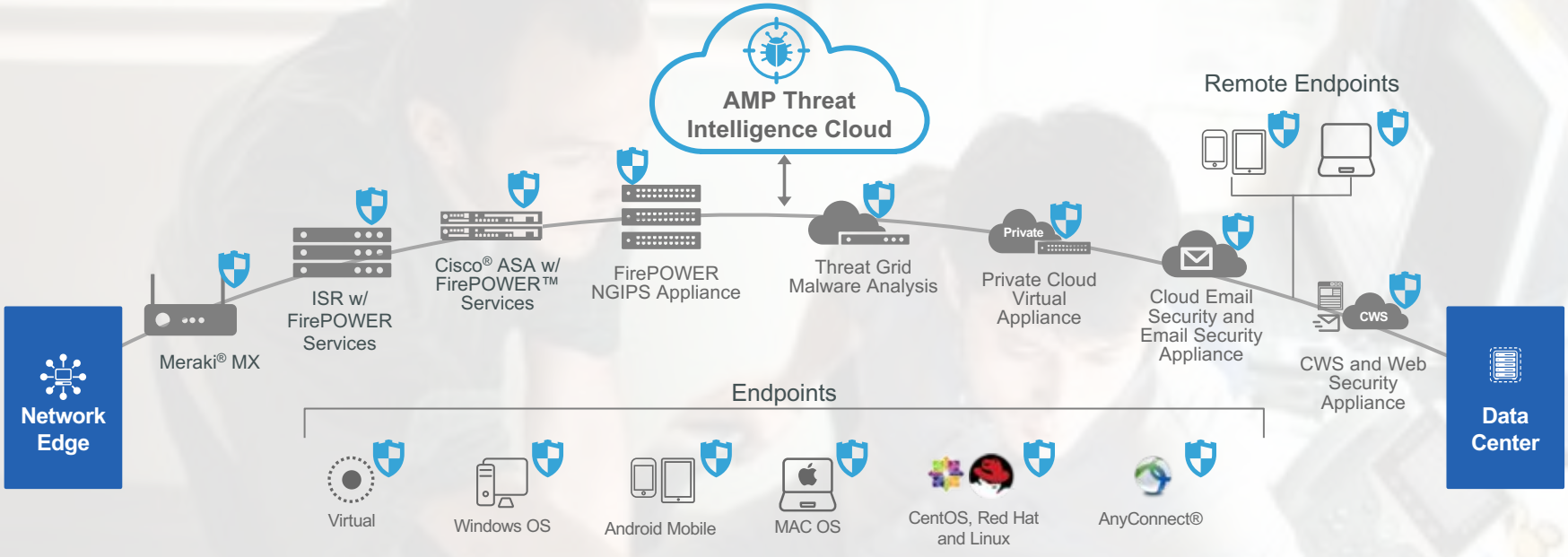
Сканирование вложений на вирусы

Перенаправление чистой почты для дополнительных проверок

Защита от атак 0-day

Обнаружение и блокирование продвинутых угроз

Архитектура Advanced Malware Protection (AMP)



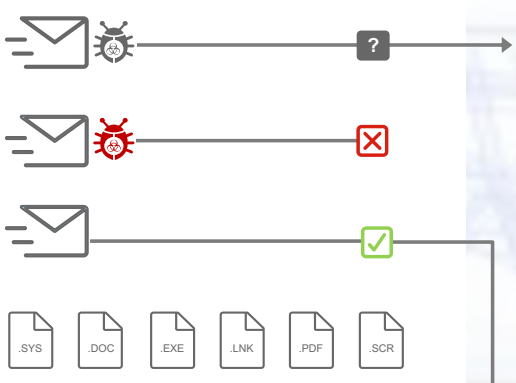
Использование threat intelligence и динамического анализа

Простое развертывание на нескольких платформах

Учитывать все письма, поторым разрешен доступ даже после анализа

Advanced Malware Protection (AMP)

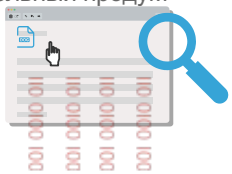
Репутация файлов



Known Signatures | Fuzzy Fingerprinting | Indications of compromise

Песочница

- Расширенная аналитика
- Динамический анализ
- 560+ индикаторов
- Отдельный продукт



Unknown | Clean | Malicious

Ретроспектива

Блокирование известного malware

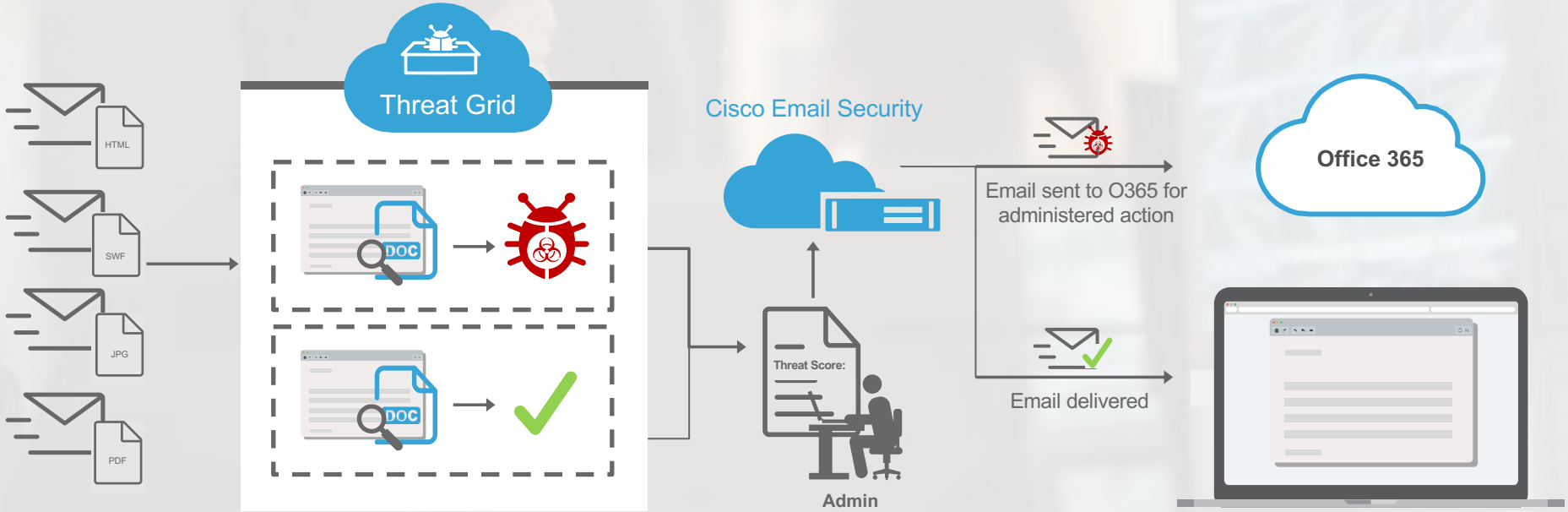
Безопасное исследование файлов

Автоматическая защита в O365

Видимость сообщений, которые пытаются попасть в сеть.

Безопасное исследование нераспознанных вложений

AMP Threat Grid для песочниц



Загрузка неизвестных файлов в ThreatGrid

Проверка файлов с расширенной аналитикой

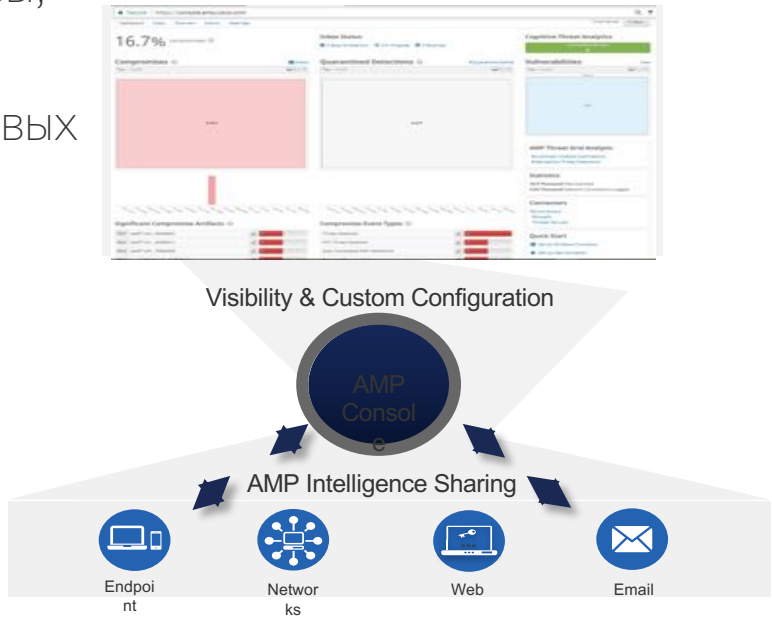
Получение отчета и значений для принятия решение

Автоматическое реагирования для пользователей O365

Новое: интеграция с AMP консолью

Унифицированная консоль для всех устройств с AMP

- Группировка нескольких устройств (Email шлюзы, Хосты, Firepower) и создание общей политики
- Создайте кастомный ‘Whitelist’, ‘Blacklist’ файловых хешей на всех устройствах
- Посмотрите индикаторы компрометации и траектории на всех устройствах



© 2015 Cisco and/or its affiliates. All rights reserved.

URLs

Защита от

Ransomware

Фишинг

Спуфинг

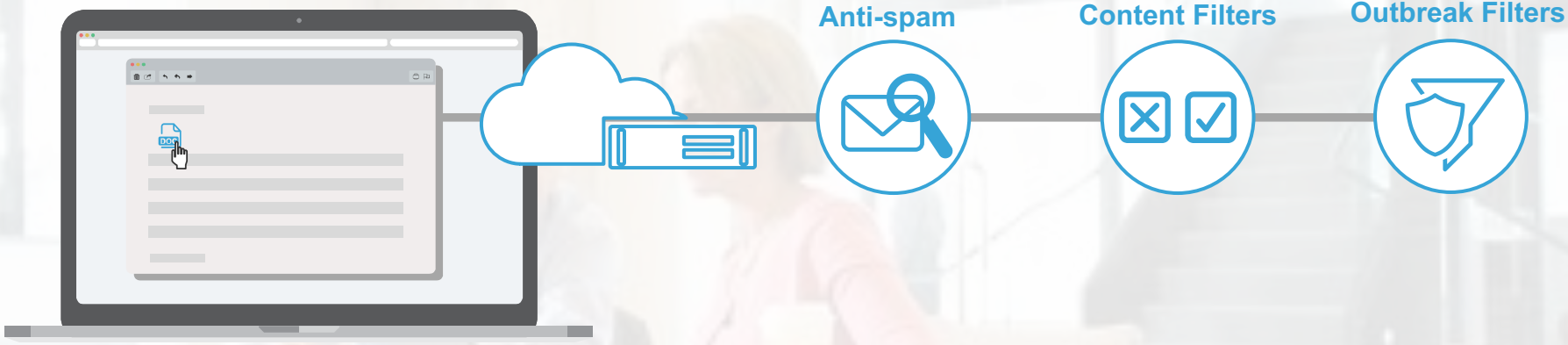
Защититесь от URL угроз, которые скрываются в обычной почте

Наталья получает email от ее банка с предупреждением о необычной активности

В панике Наталья кликает на ссылку и регистрируется

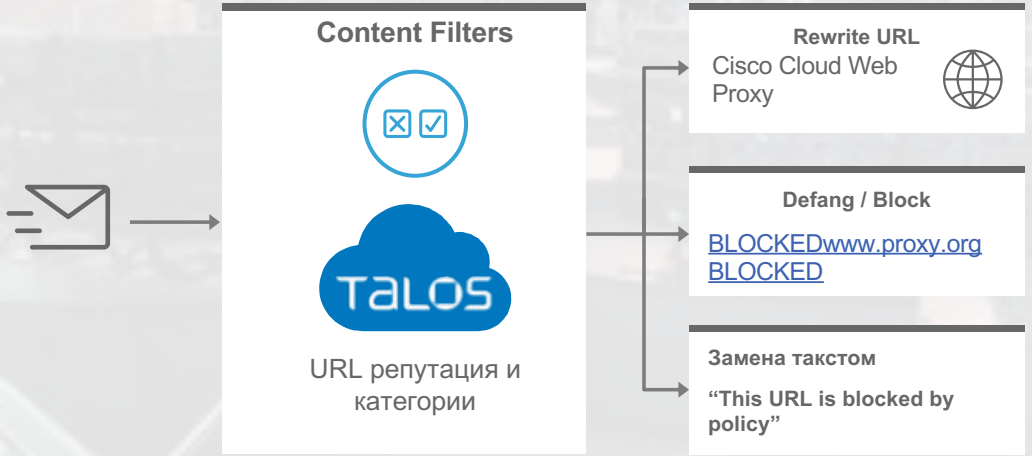
Ссылка вредоносная и учетная запись Натальи теперь скомпрометирована

Cisco защищает от скрытых ссылок



Управление, какие письма проходят в сеть

Content Filters



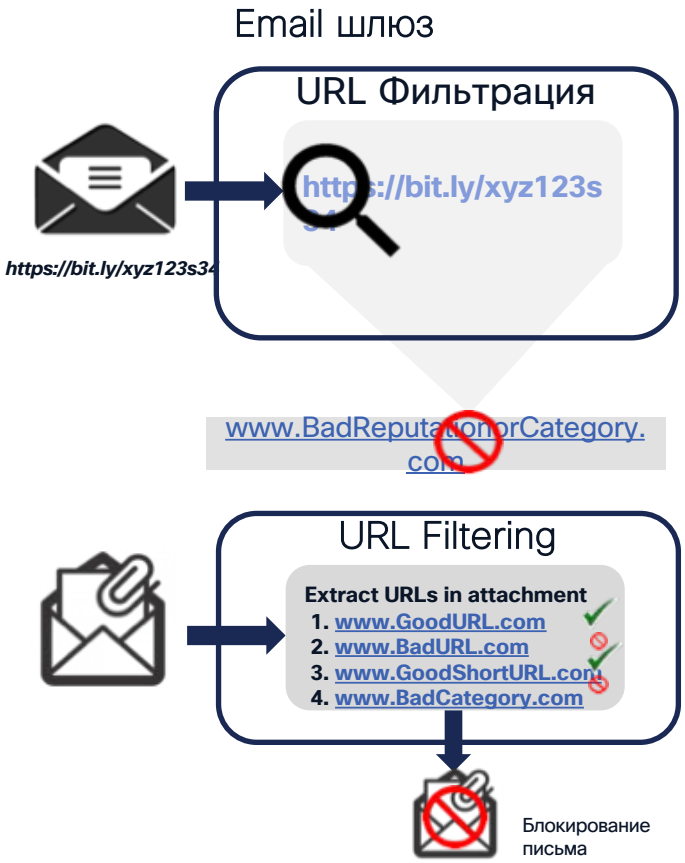
Настройте фильтры несколькими способами для дополнительной безопасности

Простое применение корпоративных политик

Новое: улучшенная фильтрация URL

Обнаружение реальный URL за сокращенными
- Глубина 10 “уровней”
- Content или Message Filter
- Детальное логирование в ***mail_logs***

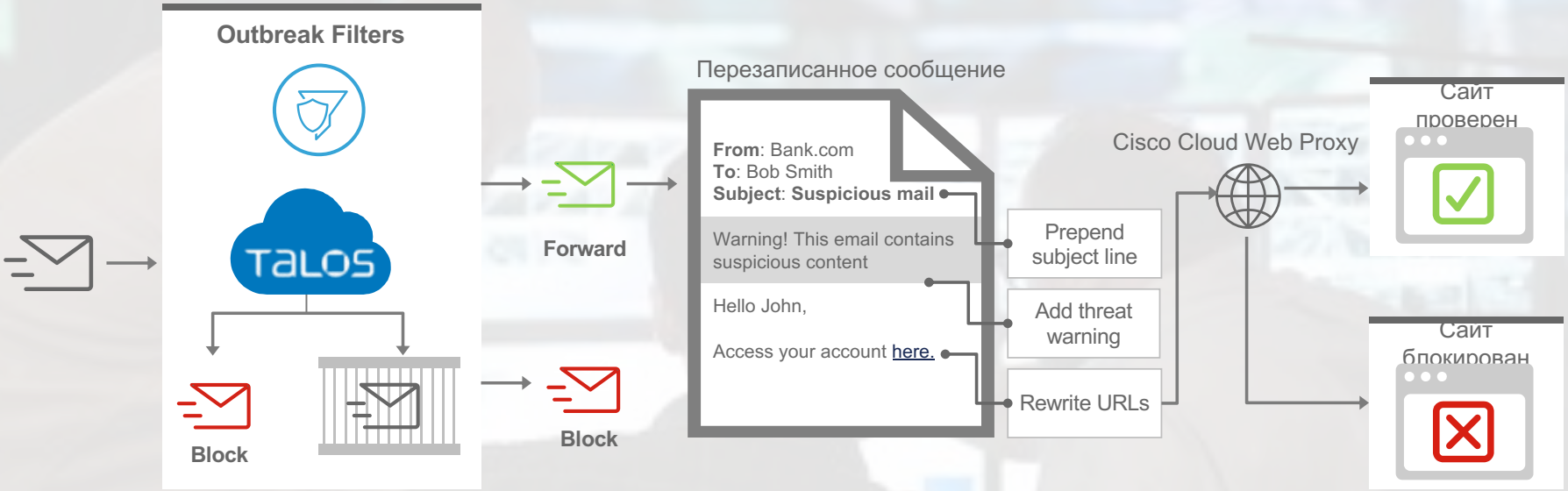
- Детектирование URL в присоединенных файлах
  - Content или Message Filter
  - В теле Email иди Attachment
  - Детальное логирование в ***mail_logs***



© 2015 Cisco and/or its affiliates. All rights reserved.

Автоматическое определение целевых и смешанных атак

Outbreak Filters



Блокирование известных угроз с Talos

Канатин email с подозрительными URL

Модификация писем для защиты конечного пользователя

Перенаправление трафика для защиты от вредоносных линков

Email контент

Защита от

Спуфинг

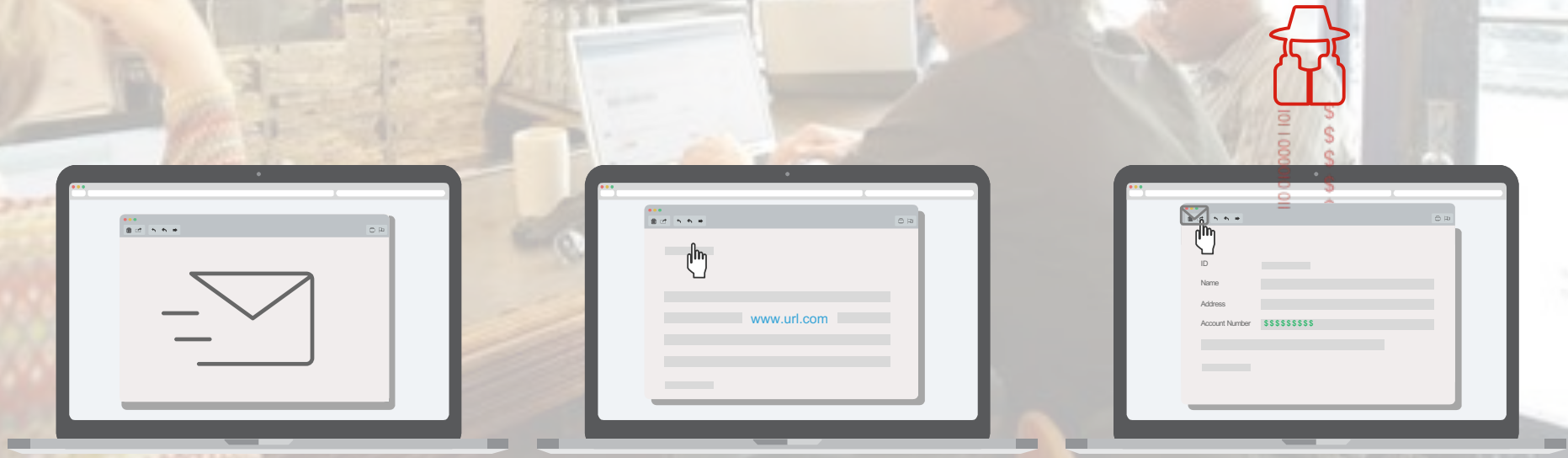
Фишинг

Защитите пользователей от компрометации бизнес-[illegible]

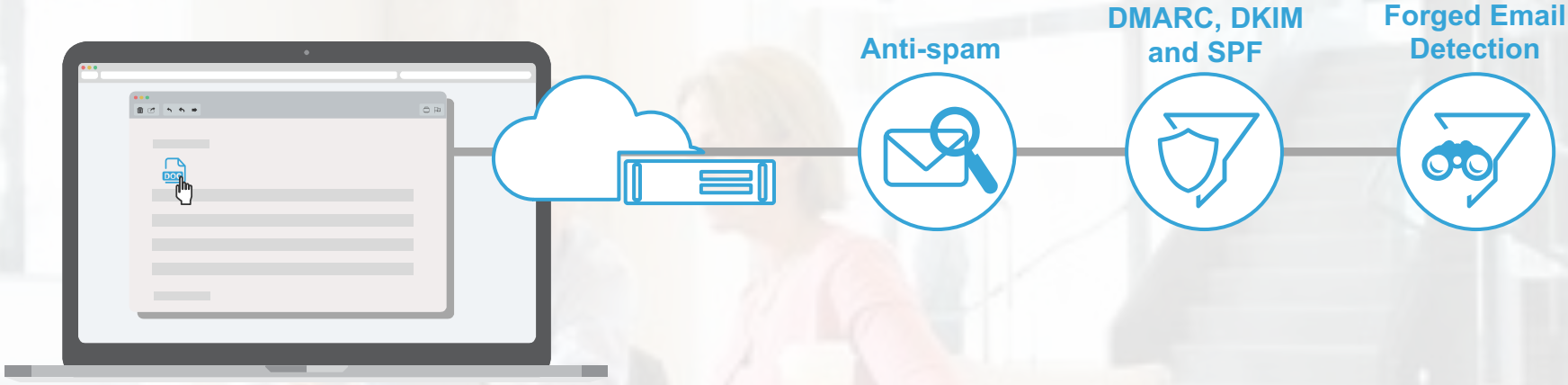
Николай получает письмо от шефа с просьбой срочно отправить финансовый отчет

Для того, чтобы избежать задержек, Николай отправляет отчет немедленно

Николай, сам того не зная, отправил отчет мошеннику

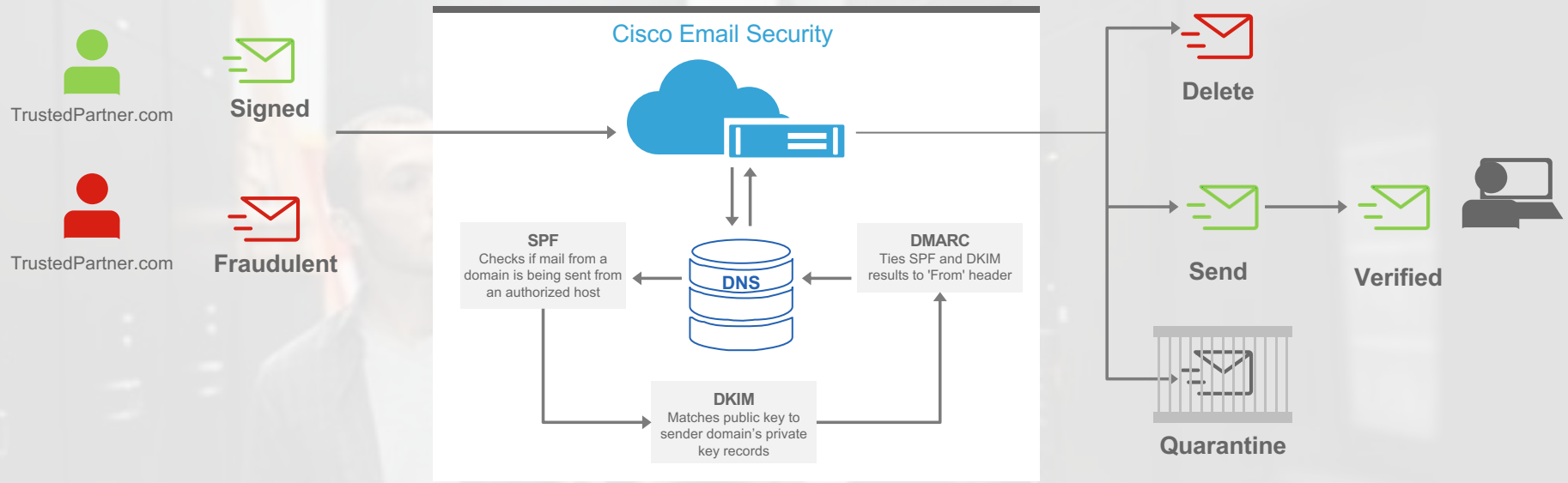


Cisco защищает от человеческой ошибки



Блокирование поддельных отправителей

DMARC, DKIM and SPF



Проверка того, что отправитель «правильный»

Проверка деталей отправителя для входящих сообщений

Блокирование неправильных отправителей и определение следующих шагов

Защита от спуфинг-атак

Forged Email Detection

Пре-обработка

From: Chuck <chuck.robbins@mail.com>

Subject: [URGENT] Need help transferring funds

Inspects the SMTP envelope address:

$ telnet mail-smtp-in.l.mail.com 25

Trying 74.125.206.26...

Connected to mail-smtp-in.l.mail.com.

Escape character is '^]'.

220 mx.mail.com ESMTP i11si22058766wmh.67 - gsmtp

HELO mail.outside.com

250 mx.mail.com at your service

MAIL FROM:<adam@outside.com>

250 2.1.0 OK i11si22058766wmh.67 - gsmtp

RCPT TO:<alan@mail.com>

250 2.1.5 OK i11si22058766wmh.67 – gsmtp

Data

Recipient Domain

Sending Domain

Actual Sender

SMTP Envelope

Проверка каталога компании

- Allison Johnson
- Barry Smith
- **Chuck Robbins**
- Dave Tucker

From: adam@outside.com

Subject: {Possibly Forged} [URGENT] Need help transferring funds

Пост-обработка

Проверка SMTP конверта на предмет адреса отправителя

Проверка соответствия адреса

Отправка модифицированного письма для того, чтобы предупредить пользователей

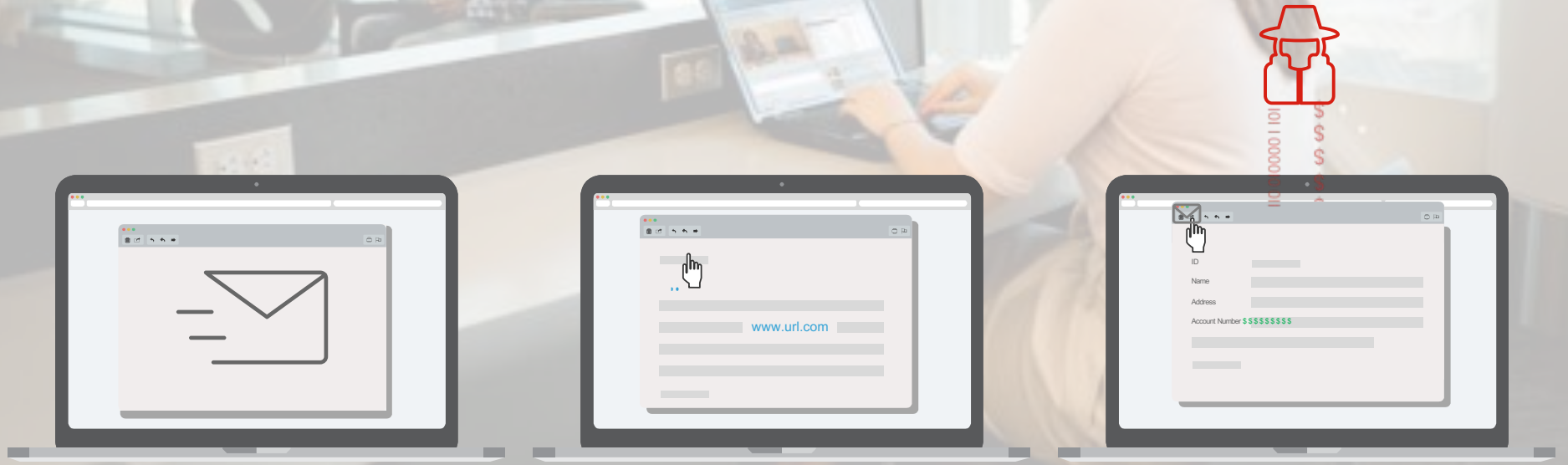
Запись в журнал всех действий

Защита от утечек данных

Валентина должа отправить важный документ о результатах внутренней проверки в HR

При выборе отправителя Валентина выбирает ошибочный email адрес из drop-down списка, у получателя совпадает имя

Валентина отправила важные персональные данные в чужие руки



Cisco обнаруживает важные данные перед тем, как они покинут сеть

Защита важной информации и IP

Data Loss Prevention (DLP)

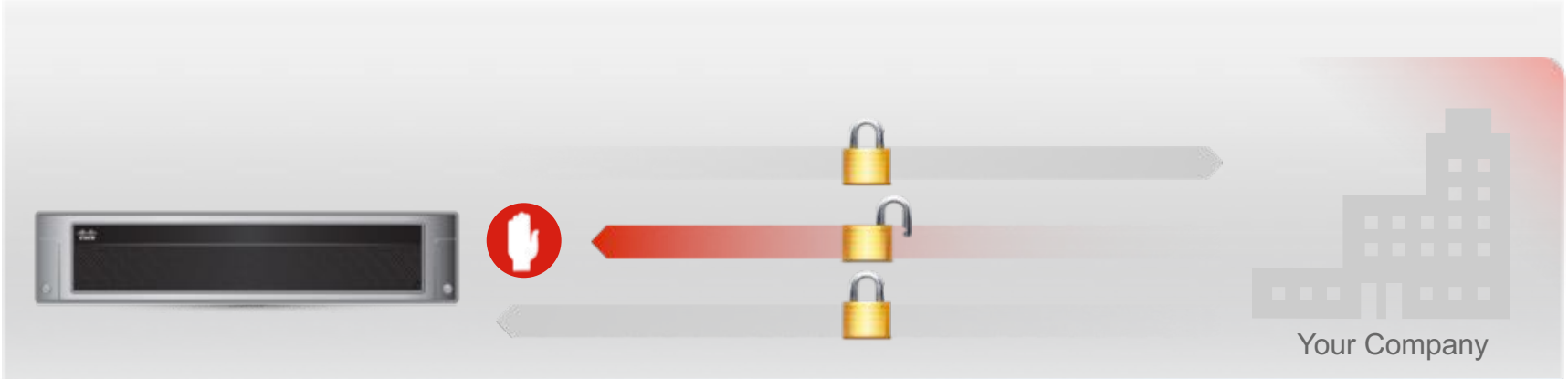
Управление, что покидает сеть и настройка политик

Сканирование контента email для обнаружения чувствительной информации.

Автоматическое предотвращение эксфильтрации

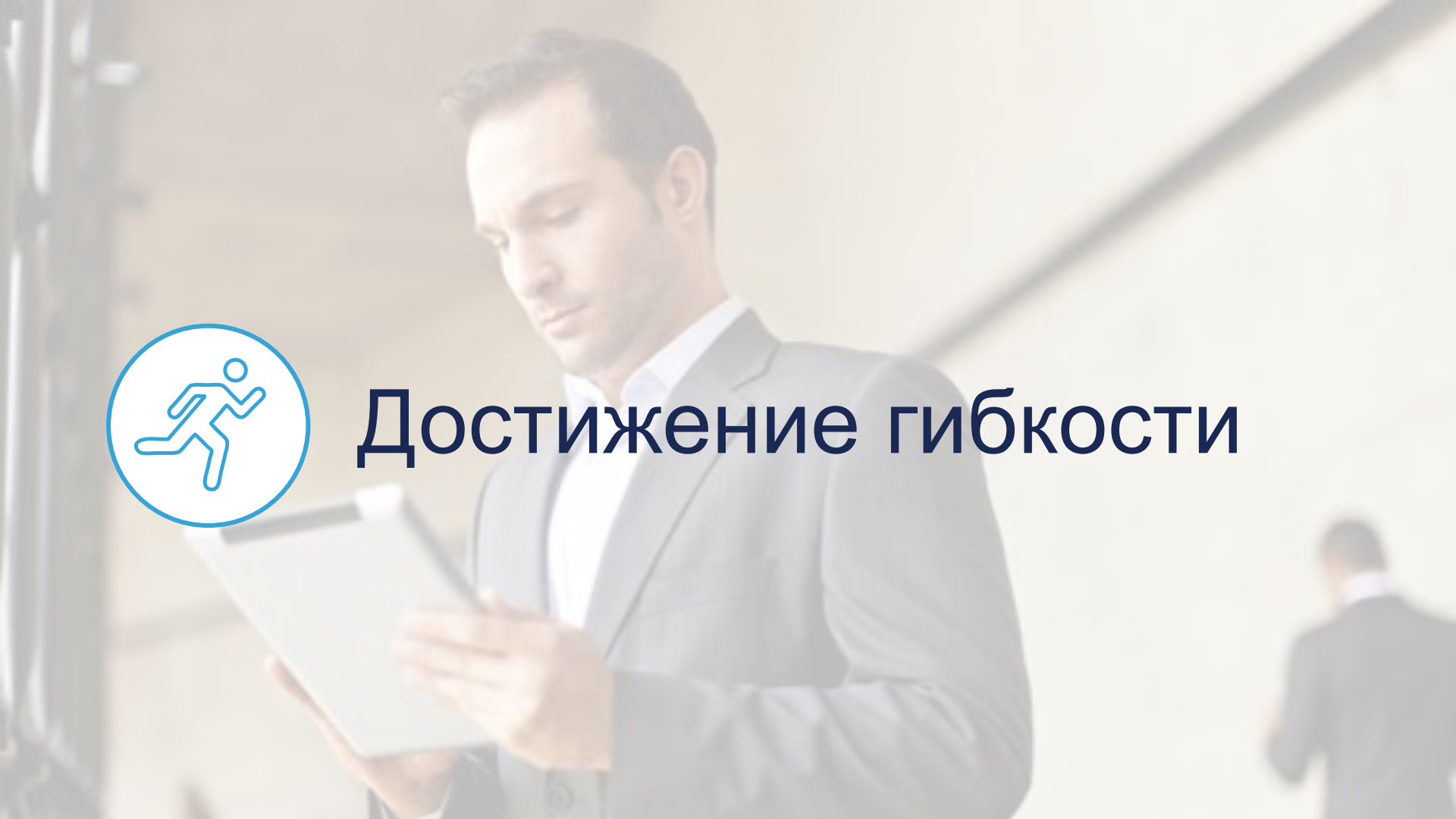
Безопасность внешний коммуникац

TLS настройки на основании Mail From



- Применение контрактных обязательств
- Предотвращение отправки важных данных в открытом виде
- Предотвращение приема чувствительных данных в октрытом виде от неправильно настроенных серверов

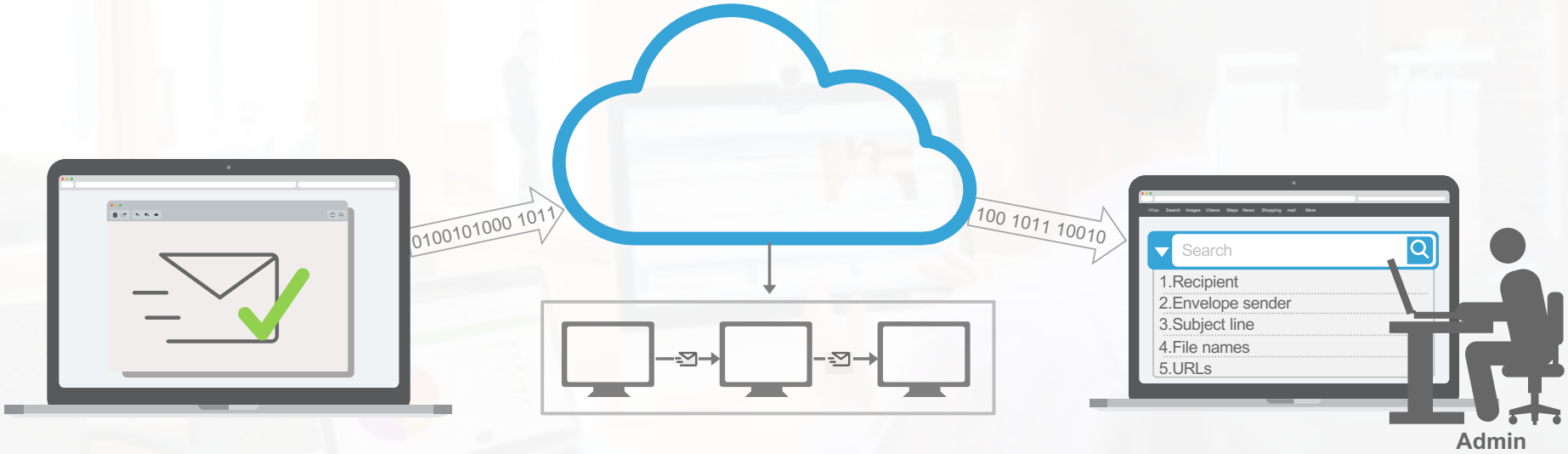
© 2015 Cisco and/or its affiliates. All rights reserved.



Достижение гибкости

Расследование без запуска новых отчетов

Message tracking



Отслеживание сообщений в режиме «почти реального времени»

Поиск одного письма с набором параметров

Поиск общих угроз в письмах

Понять здоровье системы

Унифицированные бизнес-отчеты

Детали:

- Email Threats
- Malicious Attachments
- Email Volume
- Spam Counters
- Policy Violations
- Virus Reports
- Outgoing Email Data
- Reputation Service
- System Health View

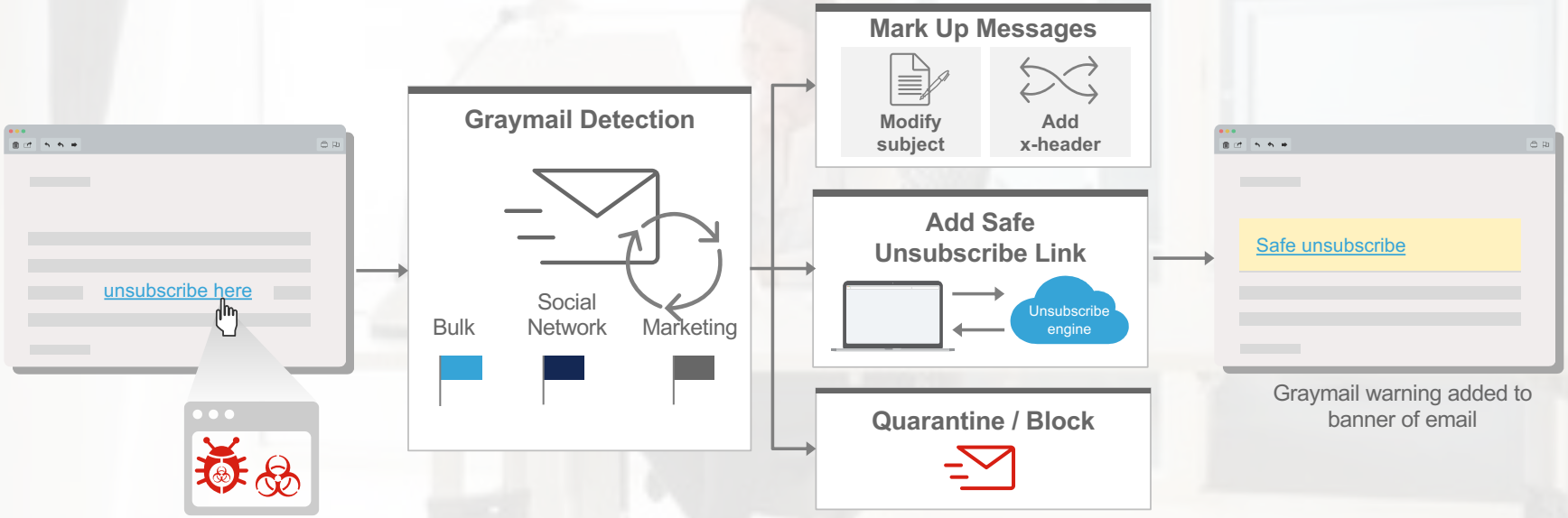
Консолидированные отчеты

Снижение времени реагирования и расследования

Идентифицировать тенденции с немедленными и отчетами по расписанию

Разделить, что важно, а что нет

Graymail обнаружение, safe unsubscribe

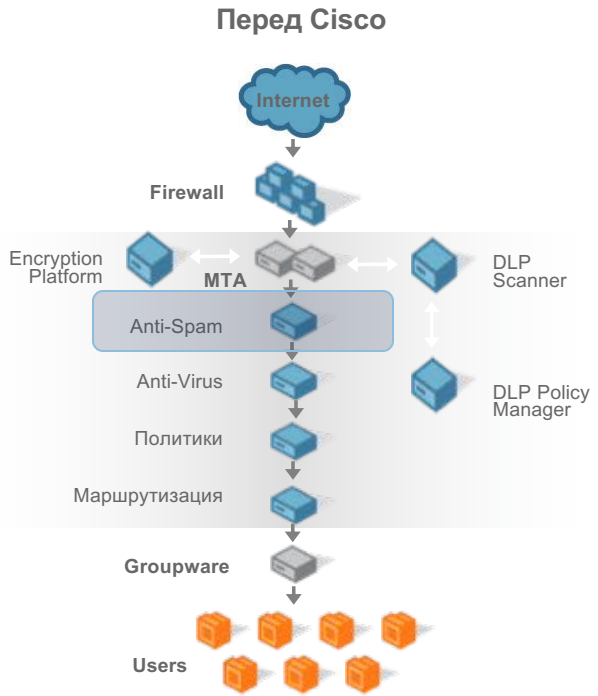


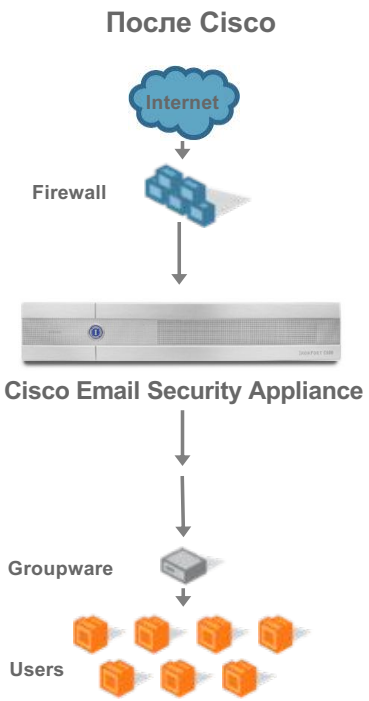
Идентификация сообщений, которые не являются спамом, но похожи

Категоризировать входящие bulk, marketing, и social networking emails

Предоставление пользователям возможность отписаться

Традиционное развертывание





© 2015 Cisco and/or its affiliates. All rights reserved.

Выберите наилучшую опцию развертывания

Облако

Гибрид

Локально

Email Security Appliance – Cisco on Cisco

Emails delivered	Emails / mo	Emails / day	Emails / employee / day	%
Attempted	124 M	5.6 M	73	
Blocked	77 M	3.5 M	46	63%
Delivered	37 M	1.7 M	22	30%
Delivered, marked “Marketing”	9 M	0.4 M	5	7%

ESA Blocked Emails	Emails* / mo	Emails / day	Emails / employee / day	%
By reputation	73 M	3.3 M	43	94%
By spam content	4.3 M	0.2 M	3	5%
By invalid receipts	0.4 M	0.02 M	0.25	1%

Malware Spam

3.5M Emails blocked each day

© 2015 Cisco and/or its affiliates. All rights reserved.

Следующие шаги

Договоритесь о демо или тестировании

Свяжитесь с Cisco

Learn more at
cisco.com/go/emailsecurity
or
cisco.com/go/cloudemail


CISCO