Безопасность в облаке Microsoft

Федяев Павел

Руководитель направления решений Microsoft

Pavel.Fedyaev@softline.com

На чем сейчас акцент?

700К
Кибератак в неделю

75%
Взломов с помощью скомпрометированных учетных записей

$3.5M
Средняя стоимость последней утечки данных

$500B
Потенциальные издержки мировой экономики

80 Млрд.

Входящих сообщений для **O365** в месяц – только 31% является бизнес письмами

55 Млрд.

Спам и вал писем, которые переполняют почтовые ящики пользователей

↑ 600%
Вредоносные Программы

За последний год в 6 раз увеличилось кол-во вредоносного ПО

Microsoft 365 Enterprise

Office 365 Enterprise	Windows 10 Enterprise	Enterprise Mobility + Security Enterprise

Комплексное интеллектуальное решение для творческой и совместной работы в безопасной среде

Microsoft 365
Сценарии безопасности

Управление доступом

Единый портал доступа к корпоративным ресурсам

Сценарии многофакторной аутентификации

Сценарии сквозной аутентификации

Самостоятельный сброс пароля.

Защита от киберугроз

Защита почты от спама

Защита почты от вирусов и фишинга

Защита ПК от вирусов

Мониторинг и аналитика поведения пользователей

Выявления подозрительных действий и таргетированных атак

Управление устройствами

Управление ПК и мобильными устройствами

Управление приложениями

Выявление подозрительной активности

Защита учётных данных пользователя

Защита информации

Классификация и маркировка документов на основе контента

Шифрование

Управление Правами и политиками доступа

Отслеживание документов и отзыв прав

Контроль облачных сервисов

Аналитика использования облачных сервисов

Выявление потенциальных угроз

Обнаружение фактов публикации корпоративных документов

Борьба с «теневым IT»

Microsoft 365 Enterprise

MICROSOFT 365 E3

Office 365 корпоративный E3

Рабочее пространство на основе чата
Microsoft Teams

Электронная почта и календарь
Exchange, Outlook

Голосовая связь, видео и собрания
Skype для бизнеса

Совместное создание содержимого
Office профессиональный плюс

Управление сайтами и содержимым
SharePoint и OneDrive

Аналитика
Delve

Безопасность и соответствие требованиям

Enterprise Mobility + Security E3

Управление удостоверениями и доступом
Azure Active Directory Premium P1

Управление мобильной работой
Microsoft Intune

Защита информации
Azure Information Protection Premium P1

Безопасность на основе удостоверений
Microsoft Advanced Threat Analytics

Windows 10 Корпоративная E3

Расширенная безопасность конечных точек
Credential Guard, Device Guard

Создано для современных ИТ
Присоединение к Azure AD, динамическое управление

Еще большая продуктивность
Windows Ink

Мощные современные устройства
Инновационный дизайн, новые классы устройств

Microsoft 365 Enterprise

MICROSOFT 365 E5

Office 365 корпоративный E5

Голосовая связь
Конференц-связь по ТСОП, облачная УАТС

Аналитика
Power BI Pro, Delve Analytics

Безопасность и соответствие требованиям
ATP, TASM, Advanced eDiscovery и другое

Enterprise Mobility + Security E5

Управление удостоверениями и доступом
Azure Active Directory Premium P2

Защита информации
Azure Information Protection Premium P2

Безопасность на основе удостоверений
Microsoft Cloud App Security

Windows 10 Корпоративная E5

Расширенная безопасность конечных точек
Advanced Threat Protection в Защитнике Windows

MICROSOFT 365 E3

Office 365 корпоративный E3

Enterprise Mobility + Security Suite E3

Windows 10 Корпоративная E3

Возможности Office 365 E3/E5

Office 365

Приложения	Клиентский доступ и сервисы	Безопасность	Аналитика	Коммуникации в облаке
Office 365 Pro Plus: Office на 5 ПК или Mac **Office для мобильных устройств:** Приложения для планшетов и смартфонов	**Exchange Std + Ent CAL + Exchange online + EOP:** Электронная почта и календарь бизнес-класса **One Drive for Business:** Облачное хранилище и обмен файлами **SharePoint Std + Ent CAL:** Внутренние порталы и сайты **SfB Std + Ent CAL + SfB online:** Встречи, IM, Видеоконференции **Yammer:** Частная социальная сеть **Teams:** Взаимодействие команд в чате **StaffHub:** Управление сменными рабочими	**Advanced Threat Protection:** Расширенная защита почты: от неизвестных угроз (угроз «нулевого дня») и фишинговых атак **Advanced Security Management:** Панель для сбора аналитики и контроля за действиями пользователей **Customer Lockbox:** Тотальный контроль и защита данных в облаке **Advanced eDiscovery:** Сервис для поиска данных, проведения электронного аудита и расследования действия пользователей	**Power BI Pro:** Корпоративная аналитика по всем источникам данных в реальном времени **MyAnalytics:** Трекер персональной продуктивности работы сотрудников (количество и качество встреч, аналитика общения с коллегами и руководителем и т.д.)	**Cloud PBX + SfB Plus CAL:** Подключение облака O365 к корпоративной телефонии, выделение номеров пользователям **PSTN Conferencing:** Присоединение к онлайн-собраниям по звонку из любой точки мира, выделение номера для конференции

Office 365 **E3**

Office 365 **E5**

Возможности Windows 10 Enterprise

Windows 10 Enterprise **E5**

Windows 10 Enterprise **E3**

Доверенная платформа

Enterprise Data Protection
Защита от утечек данных за счет отделения корпоративной информации от личной.

Windows Hello for Business
Доступ к системе на основе биометрии

Credential Guard
Защита учетных записей с помощью аппаратных средств изоляции

AppLocker
Запуск нежелательных и подозрительных приложений в изолированной среде.

Device Guard
Запрет на запуск недоверенных приложений на устройстве.

Advanced Threat Protection
Анализ угроз за счет обнаружения подозрительного поведения, сопоставления с базой данных известных атак.

Повышение продуктивности

Azure Active Directory Join
Включение устройства в облачную или гибридную инфраструктуру организацию.

MDM enablement
Управление устройством средствами MDM-решений

Windows Store for Business, Private Catalog
Каталог приложений, предоставляемых сотрудникам организацией.

Application Virtualization (App-V)
Упрощение развертывания и управления приложениями

Персонализация

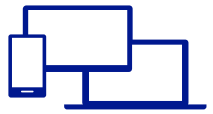
User Experience Virtualization (UX-V)
Синхронизация пользовательских настроек между устройствами и виртуальными средами Windows

Granular UX Control
Управление интерфейсом через централизованные политики

Широкий спектр устройств

Windows 10 for Industry Devices
Использование недорогих, массовых устройств в качестве терминалов, киосков и др.

Возможности Enterprise Mobility + Security E3/E5



Управление учетными записями и доступом	Безопасность учетных записей	Управление устройствами, в т.ч. мобильными	Защита информации
WS RMS CAL + WS CAL + Azure Active Directory Premium P1 Единая учетная запись для локальных и облачных приложений Многофакторная аутентификация, контроль доступа с разных устройств, отчетность и аналитика	**Microsoft Advanced Threat Analytics** Анализ трафика и событий безопасности в локальном AD заказчика, предупреждения и проактивные действия. Локальный сервис (не облако).	**SC Config Manager + + Microsoft Intune** Управление мобильными устройствами и приложениями (политики пароля, пин-кода, шифрования для устройства, разделение приложений и учетных записей в них на личные и рабочие)	**SC Endpoint Protection + Azure Information Protection Premium P1** Защита файлов через шифрование с помощью RMS (Azure и локального) Отслеживание доступа к файлам (только через Azure RMS) Ручная классификация документов
Azure Active Directory Premium P2 Расширенная аналитика и действия по событиям, связанным с учетными записями (на базе машинного обучения) Дополнительная защита (временное предоставление доступа) для привилегированных учетных записей	**Microsoft Cloud App Security** Обнаружение фактов использования облачных сервисов (через анализ сетевых журналов) Управление облачными сервисами (Microsoft и др.)		**Azure Information Protection Premium P2** Автоматическая классификация и наложение политик защиты на файлы Одновременное использование локального RMS и Azure RMS

EMS E3

EMS E5

Преимущества EMS для заказчиков с O365

	Управление учетными записями и доступом	Управление мобильными устройствами	Защита информации	Безопасность учетных записей
Enterprise Mobility + Security	**Azure AD для O365+** • Расширенная отчетность • Единый вход для всех приложений • **Расширенные возм-ти МФА** • Самостоятельное управление группами и сброс пароля • Динамические группы, назначение лицензий на группы	**MDM для O365+** • Управление ПК • **Управление мобильными приложениями (запрет передачи данных между корп. и личной средой)** • Безопасный просмотра контента • Установка сертификатов • Интеграция с SysCenter	**Azure Information Protection (RMS) для O365+** • Отслеживания и уведомления об открытии для защищенных документов • Защита для информации на локальных файловых хранилищах Windows Server • **Классификация и метки для документов**	**Cloud App Security** • Обнаружение и управление облачными приложениями **Advanced Threat Analytics** • Обнаружение угроз в локальной среде заказчика **Azure AD Premium P2** • Условный доступ с учетом расширенного спектра рисков
Office 365	**Базовое управление учетками через Azure AD для O365:** • Единая учетная запись для сервисов O365 + локальной среды • Базовая многофакторная аутентификация при доступе к O365	**Базовое управление устройствами через MDM для O365** • Управление настройками мобильных устройств • Выборочное удаление данных • Встроено в центр администрирования O365	**RMS-защита через RMS для O365** • Защита для документов Office (локальных или в O365) • Доступ к RMS SDK • Импорт собственного ключа в Azure RMS	**Advanced Security Management** • Обнаружение подозрительной активности в рамках сервисов Office 365

Безопасная электронная почта

Обзор Exchange Online
Advanced Threat Protection (ATP)

Расширенная защита от угроз для Exchange Online

Защита от неизвестного вредоносного ПО и вирусов

- Анализ поведения при помощи машинного обучения
- Оповещения администраторов

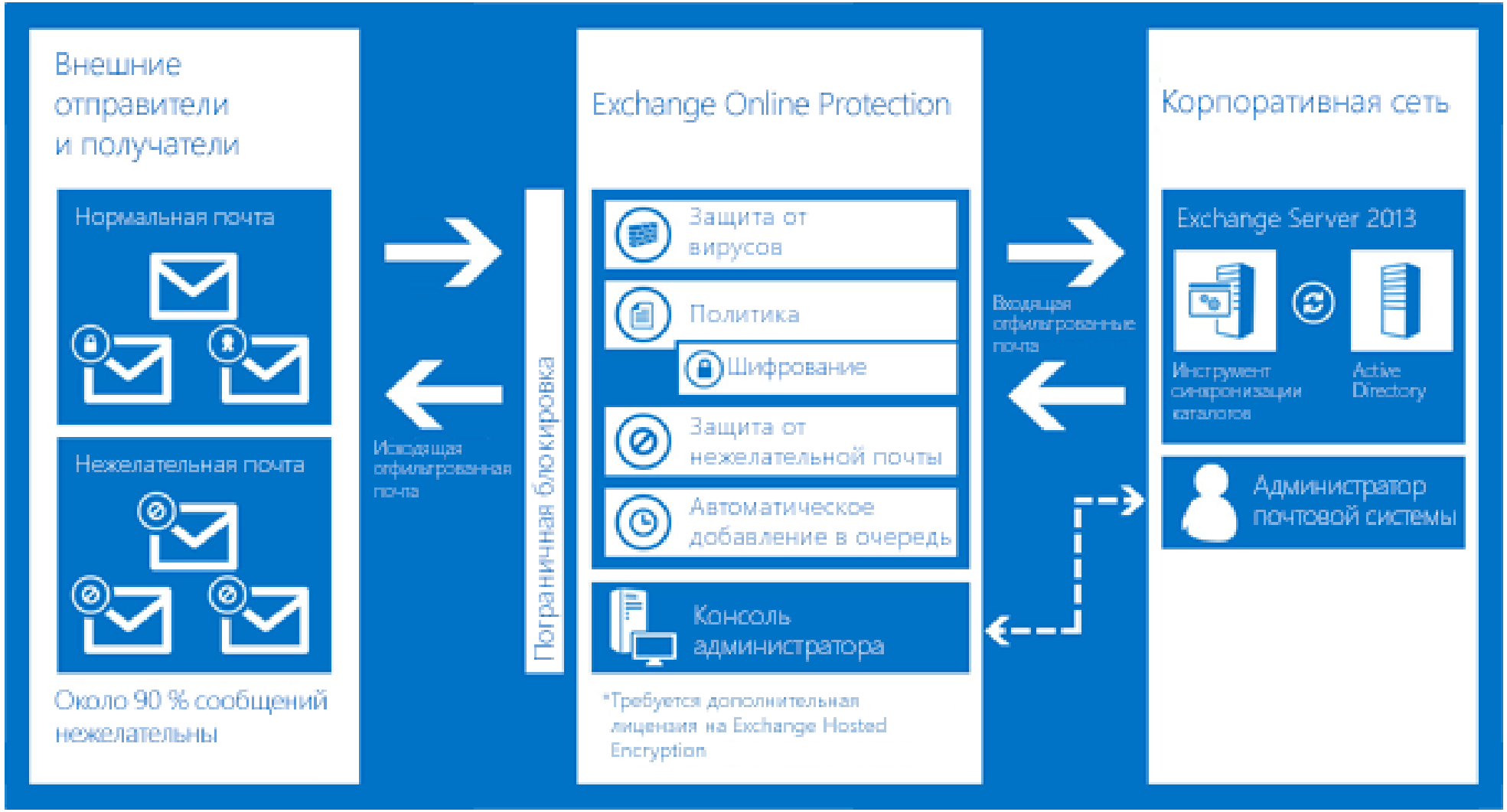
Защита во время попытки перехода по ссылкам

- Защита от вредоносных URL-адресов в режиме реального времени
- Растущая база URL-адресов

Широкие возможности создания отчетов и трассировки

- Встроенные средства трассировки URL-адресов
- Отчеты о сложных угрозах

Exchange Online Protection



Exchange Online Protection

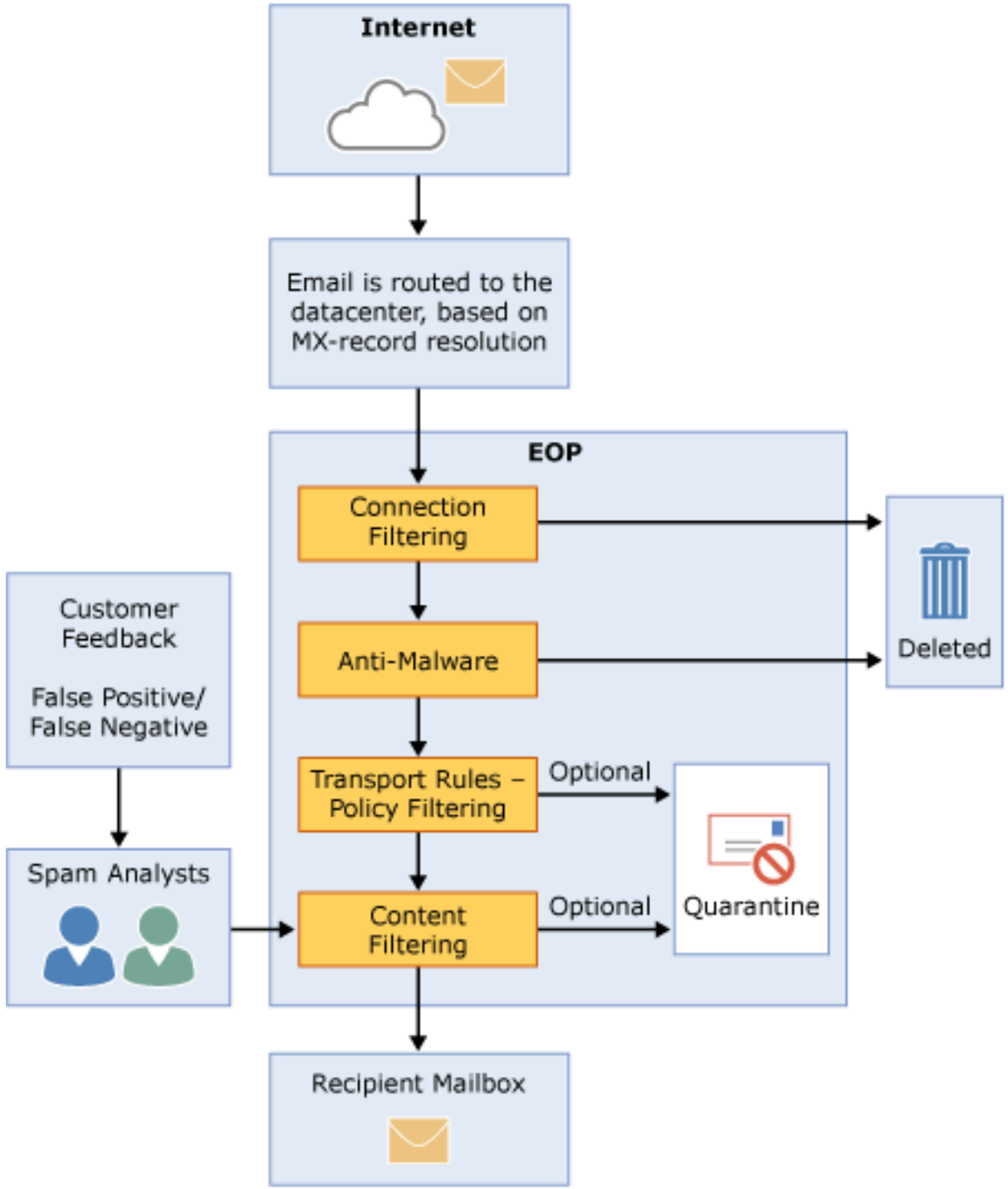
1. проходит через фильтрацию подключений, которое проверяет репутацию отправителя и проверяет сообщение на наличие вредоносных программ;

2. Прохождение фильтрации политик - сообщения оцениваются по настраиваемым правилам для обработки почты;

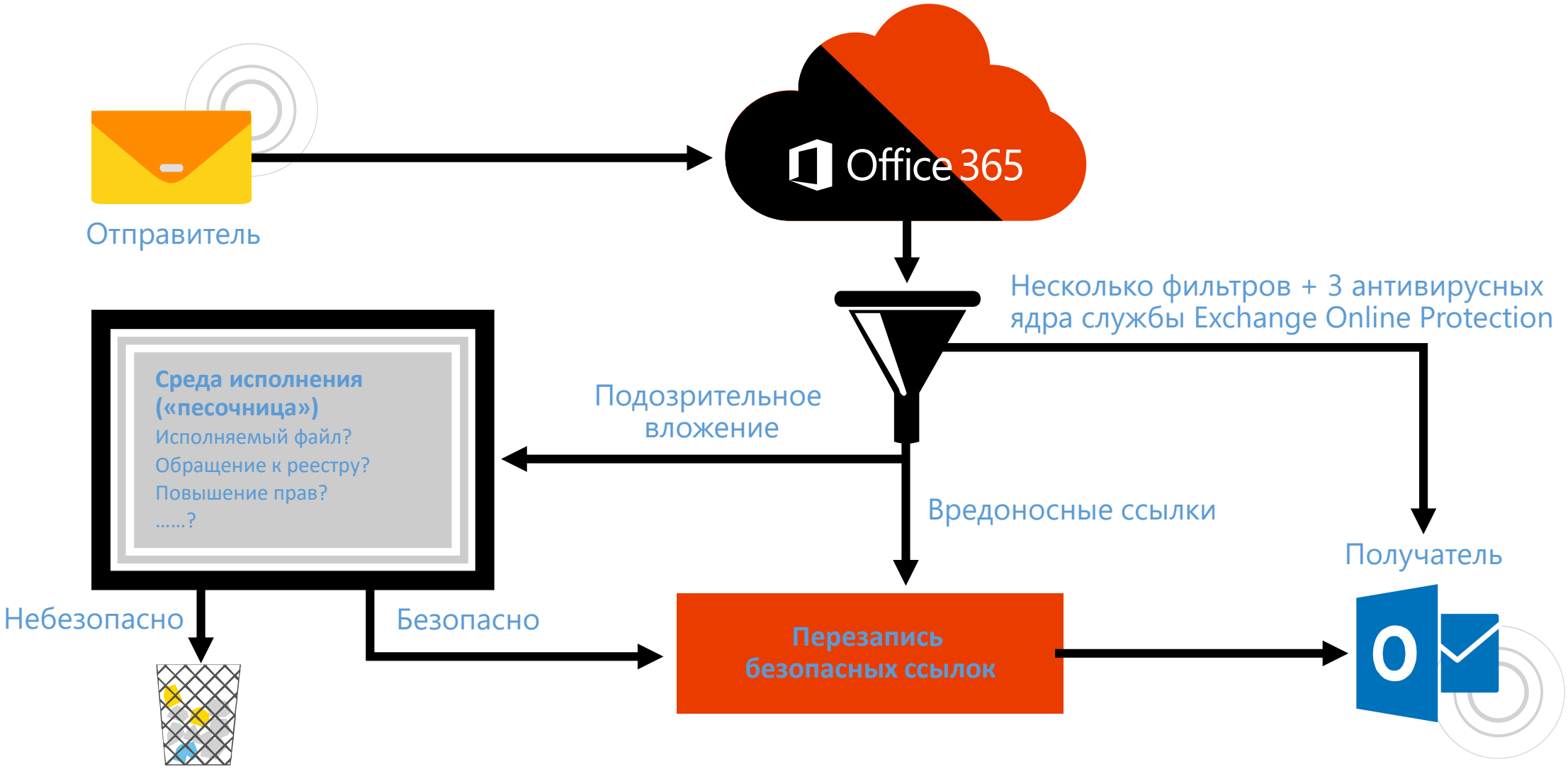
3. фильтрация содержимого - содержимое проверяется на наличие терминологии или свойств, общих для нежелательной почты;

4. Доставка отфильтрванных писем в папку Нежелательной почты или в карантин.

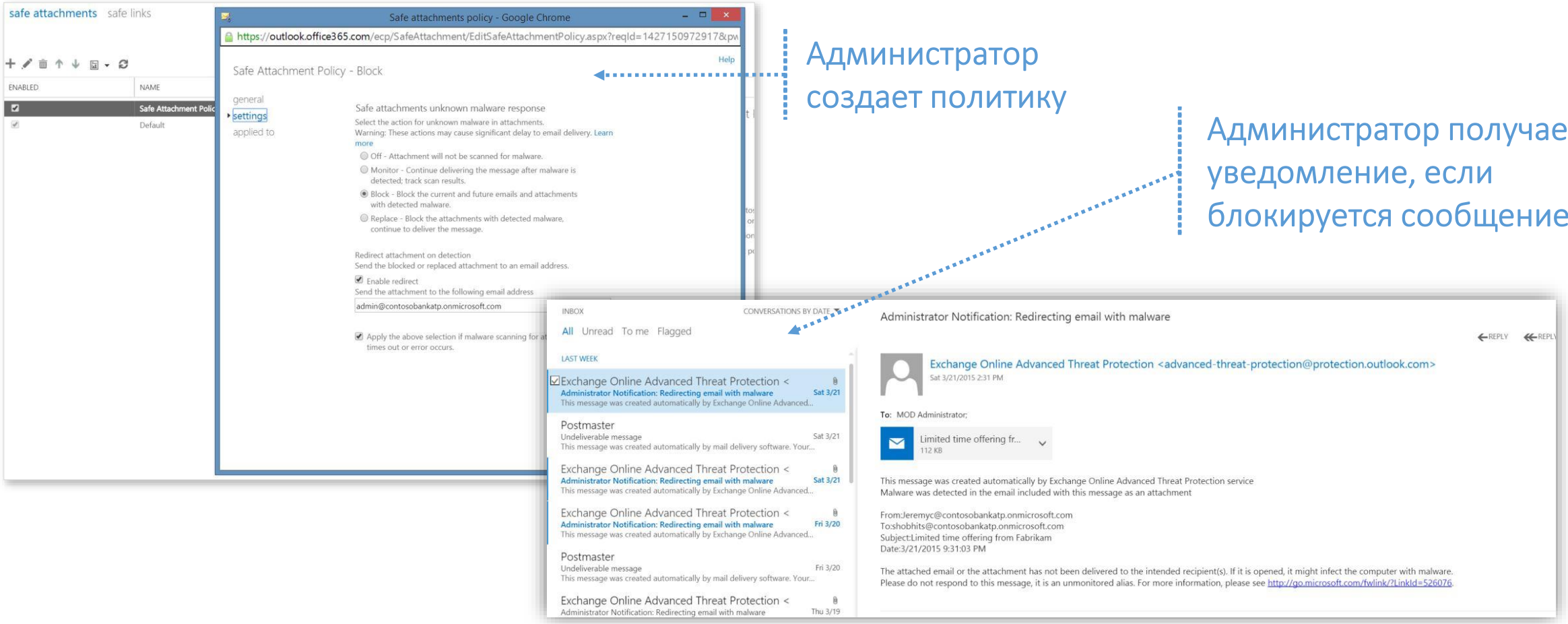
5. Доставка письма получателю.



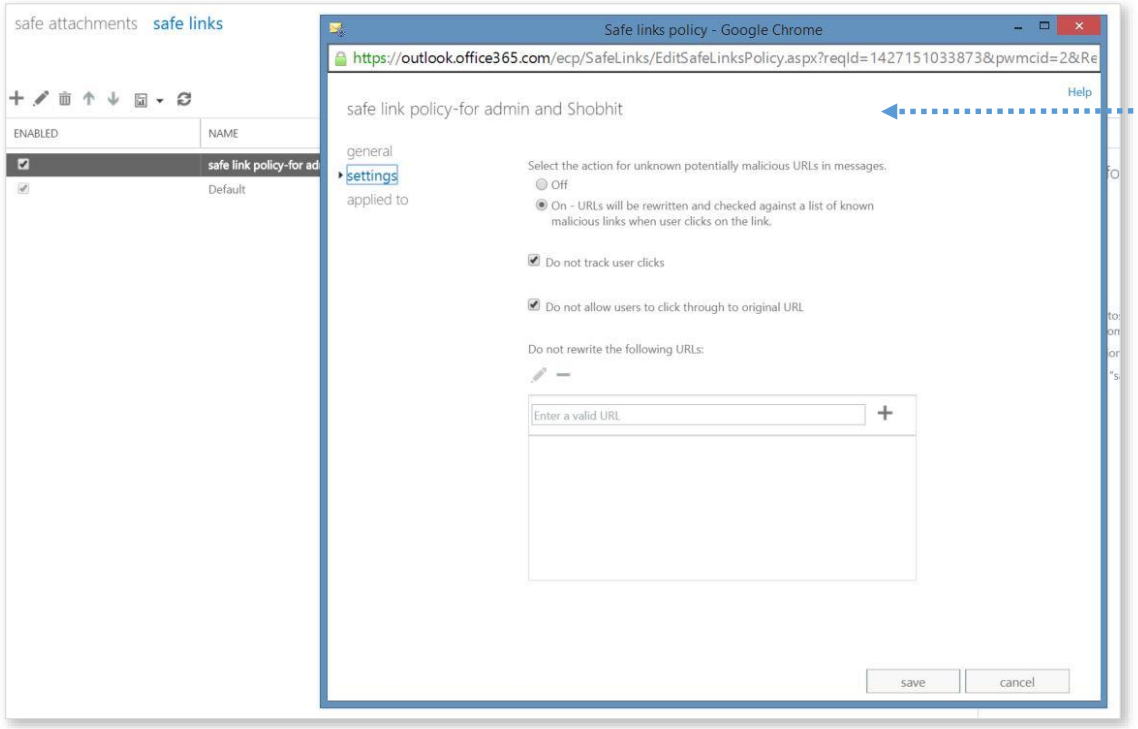
Архитектура службы Exchange Online Protection



Safe Attachments (Безопасные вложения) — использование

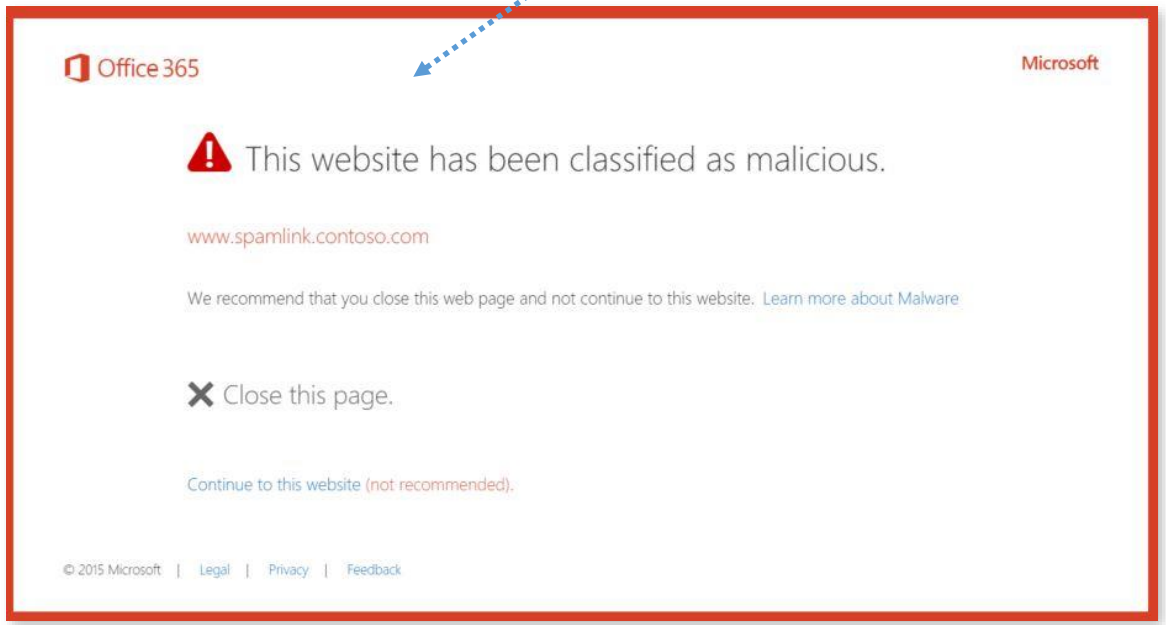


Safe Links (Безопасные ссылки) – использование

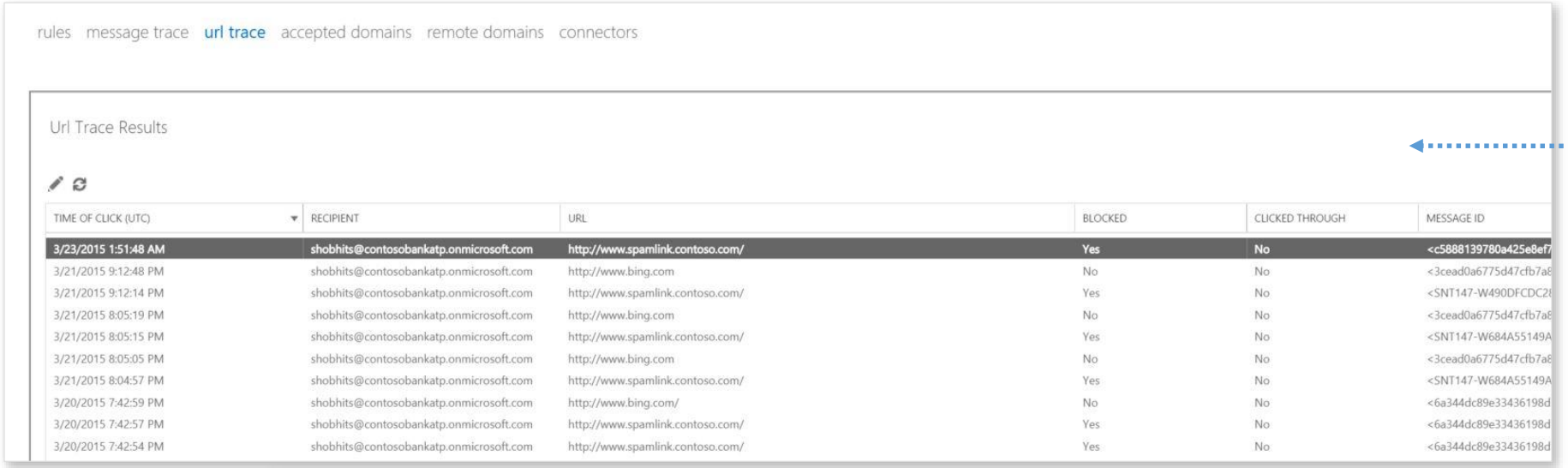


Администратор создает политику

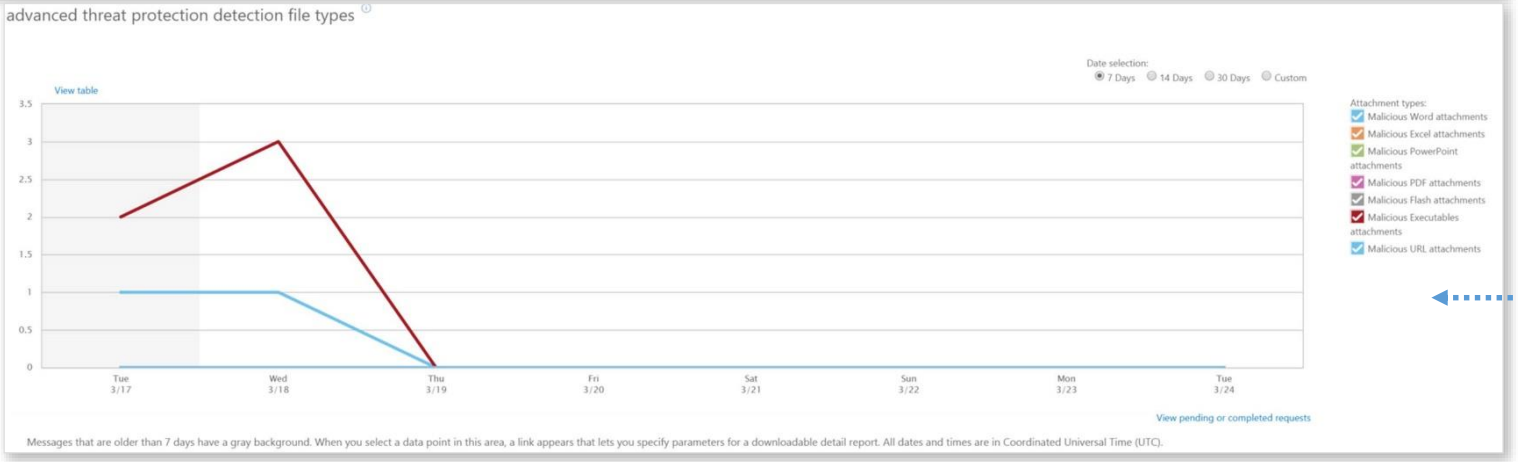
Пользователи получают уведомление, если в электронном сообщении была нажата вредоносная ссылка



Широкие возможности создания отчетов и отслеживания нажатий

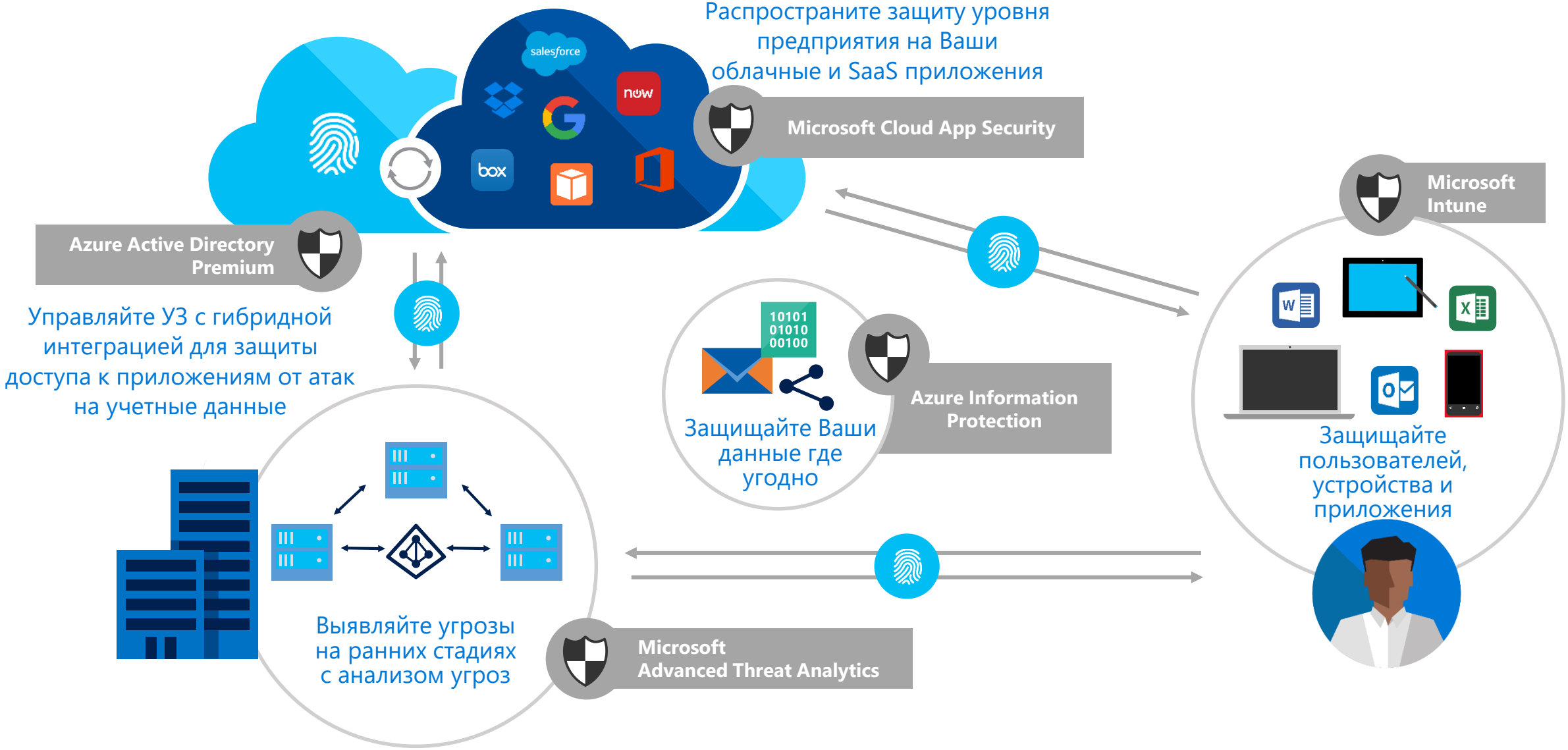


Администраторы получают всю информацию о том, кто перешел по той или иной ссылке



Отчеты по типу и поведению файлов

Комплексный подход к защите



Контролируйте доступ из любого места

“Мне необходимо контролировать доступ к ресурсам на основании ряда условий”

АТРИБУТЫ ПОЛЬЗОВАТЕЛЕЙ

Учетная запись

Членство в группах

Надежность аутентификации (MFA)

УСТРОЙСТВА

Является ли членом домена

Соответствие требованиям

Тип платформы (Windows, iOS, Android)

ПРИЛОЖЕНИЕ

Политики на основе приложений

Тип клиента

Критичность для бизнеса

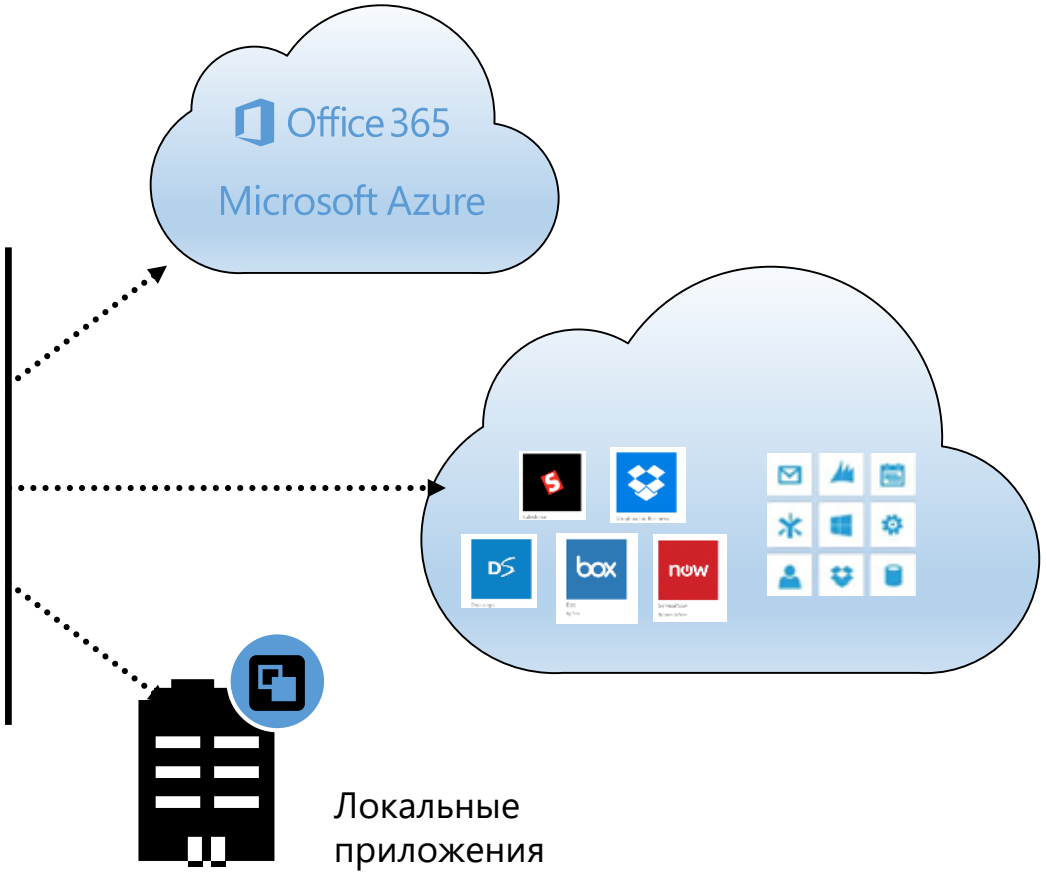
ИНОЕ

Из какой сети

Профилирование риска

Azure AD – единая точка контроля

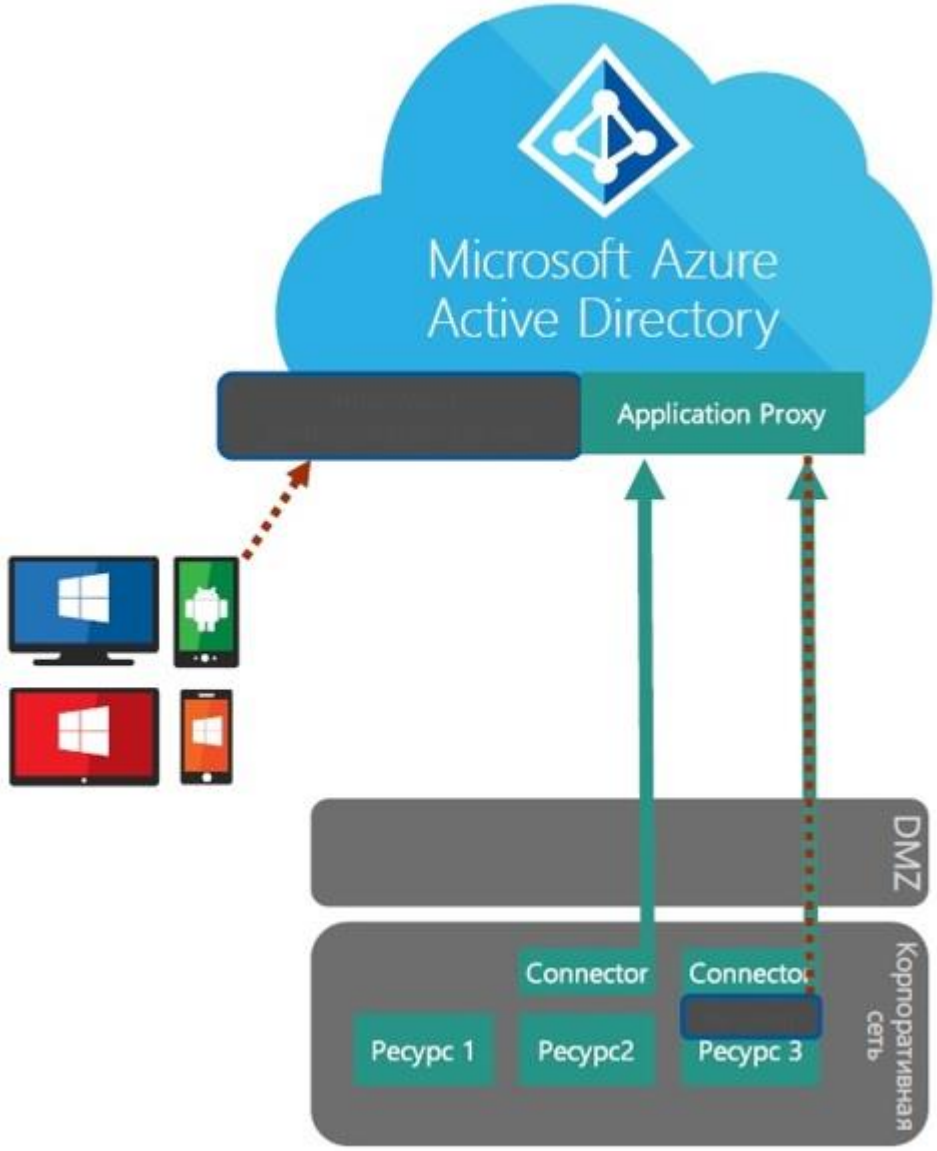
- Разрешить
- Потребовать MFA
- Блокировать



Локальные приложения

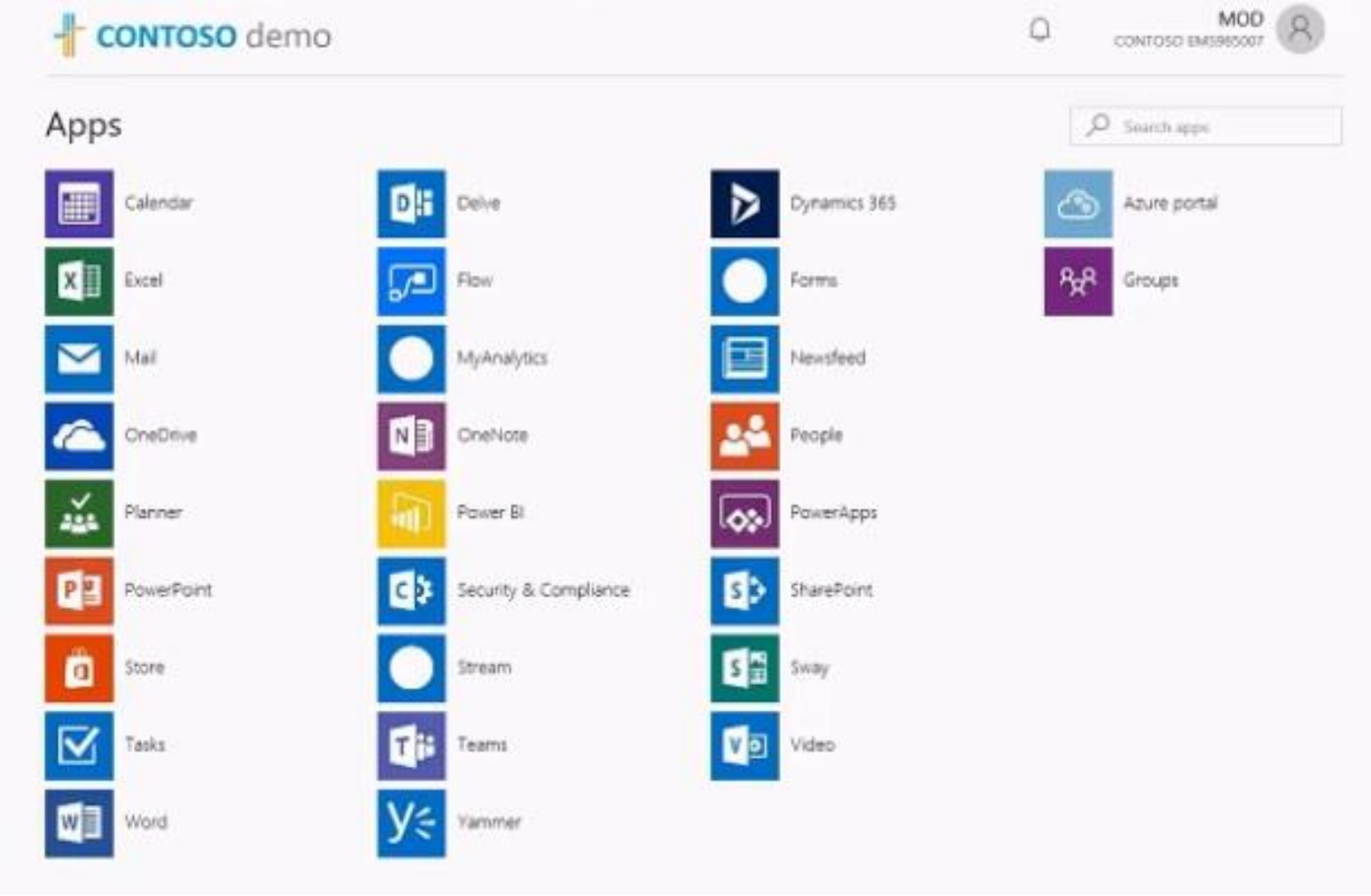
Azure Active Directory

- Многофакторная аутентификация
- Самостоятельный сброс пароля
- Защита от DOS – атак
- Возможность установки множества коннекторов, автоматически подключаемых к сервису, для обеспечения масштабируемости.



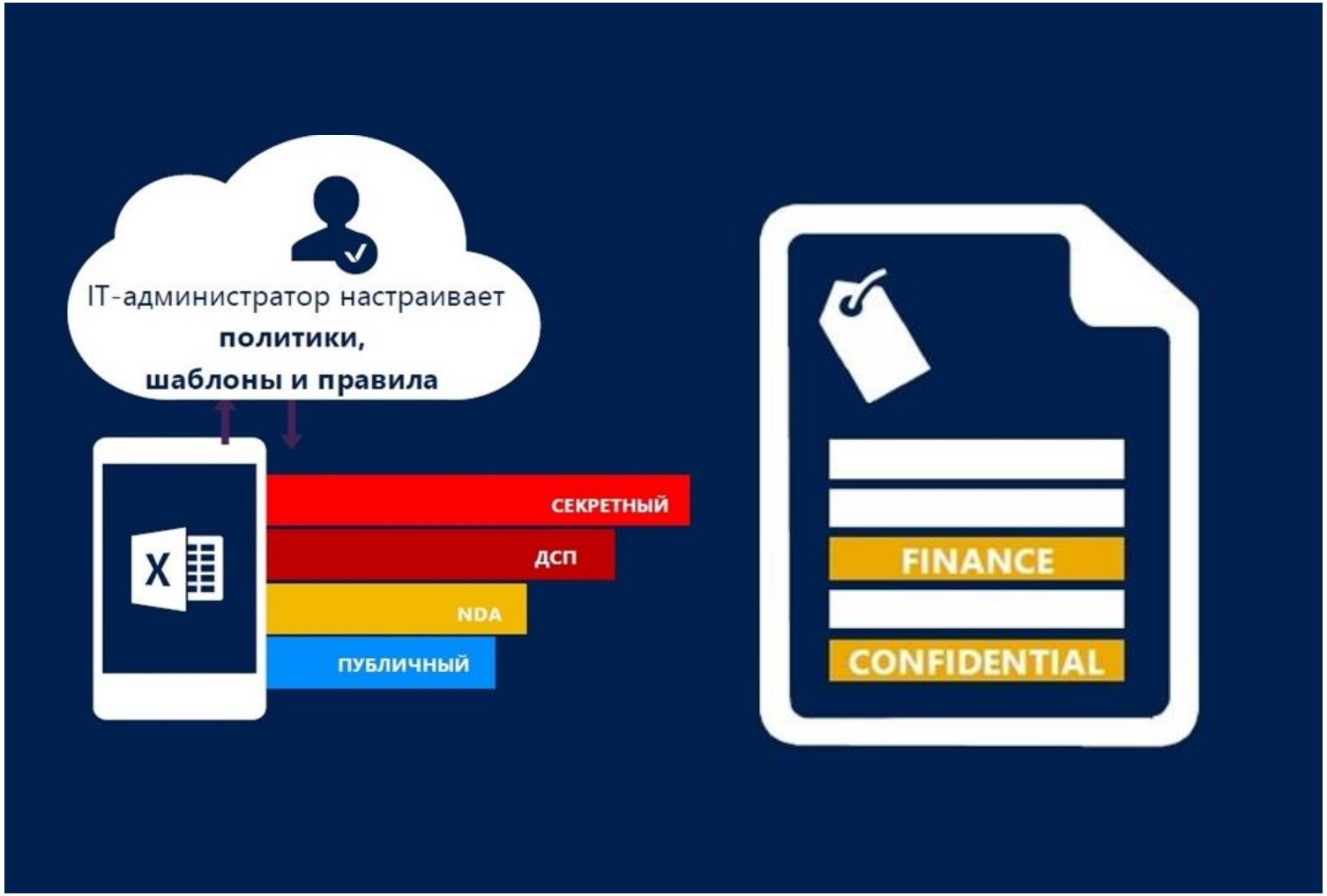
Портал Azure Active Directory

- Единая рабочая область
- Объединение под один логин/пароль различных учётных записей
- Единый пакет инструментов под разные роли сотрудников
- Возможность брендирования портала



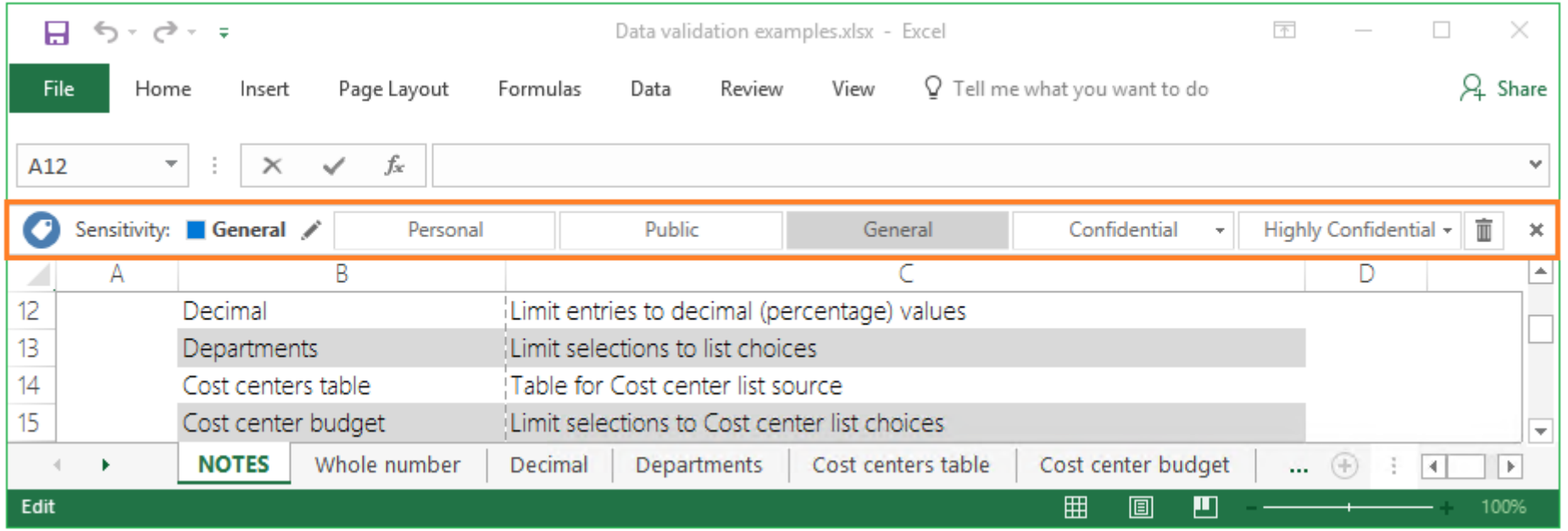
Azure Information Protection

- Классификация и шифрование файлов
- Отзыв прав
- Ограничение времени жизни файла
- Отслеживание успешного и безуспешного использования файла
- Возможность видимости в привязке к карте



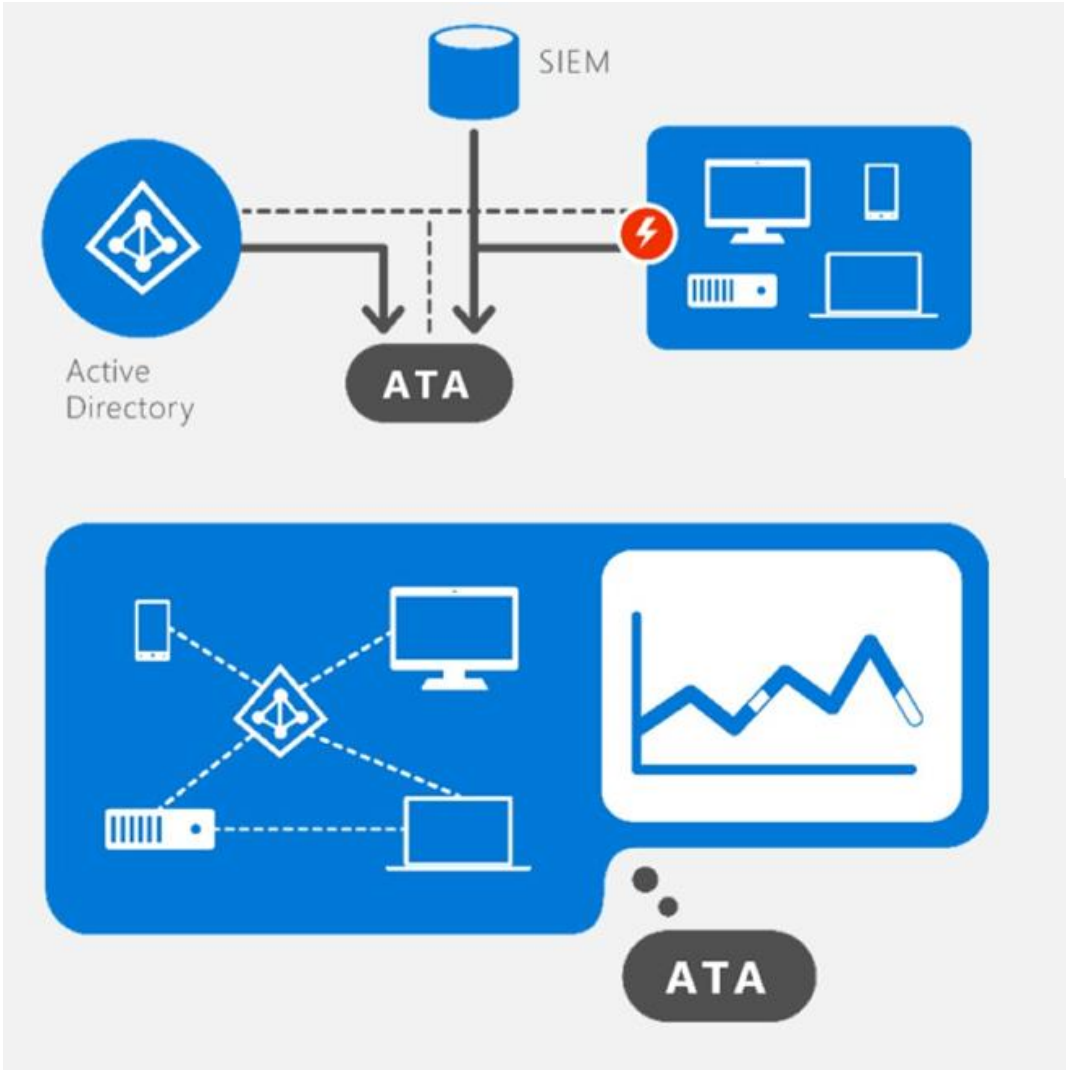
Azure Information Protection

- Формирование наборов меток под каждую роль
- Принудительная или выборочная классификация по содержанию
- Защита путешествует с файлом через облако



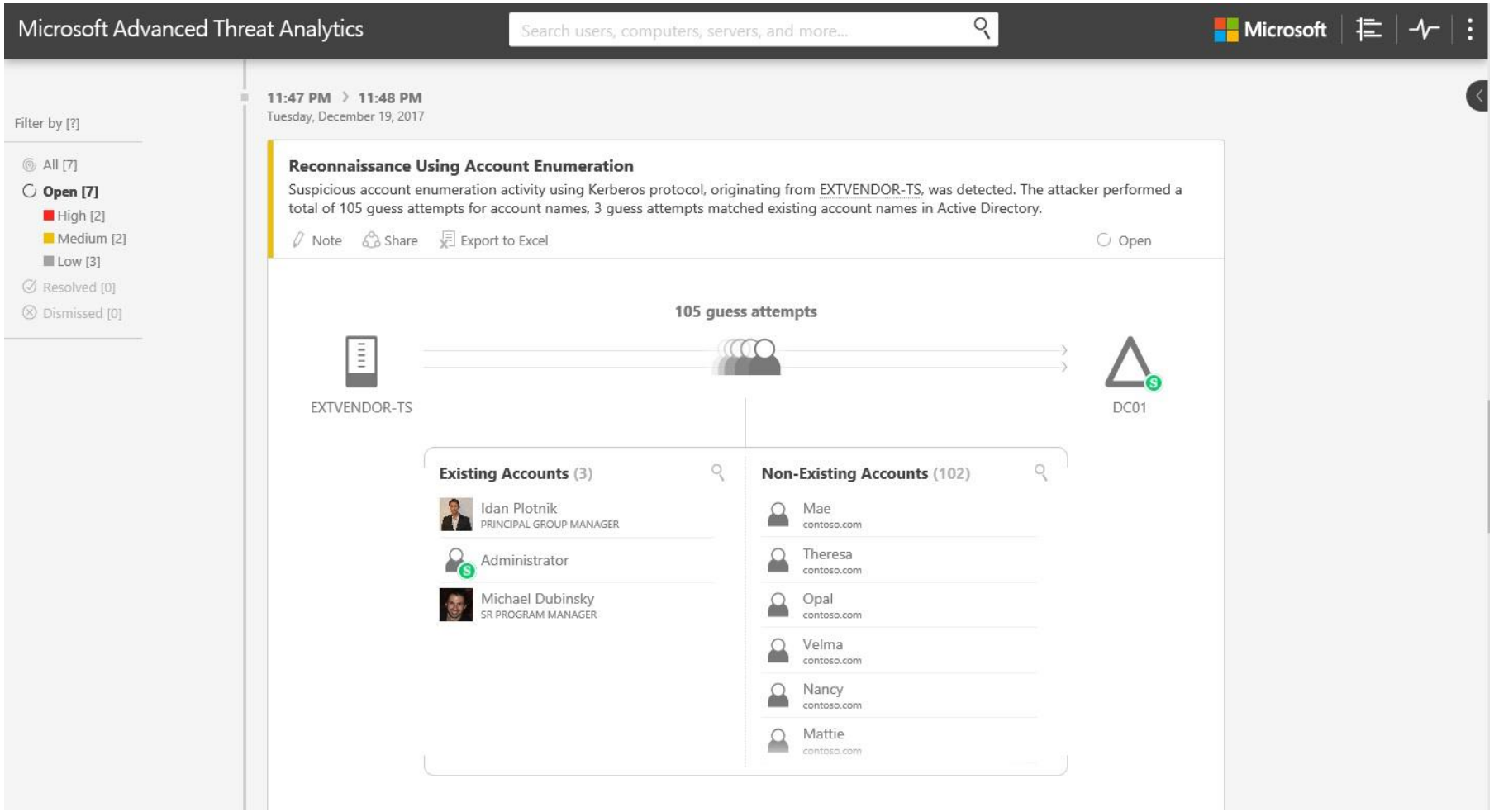
Advanced Threat Analytics (ATA) – превентивная идентификация атак

- Поведенческая аналитика
- Обнаружение известных атак
- Рекомендации для каждой угрозы
- Бесшовное развертывание (Port-Mirroring)
- Быстрое обучение и адаптация



ATP - Как это работает

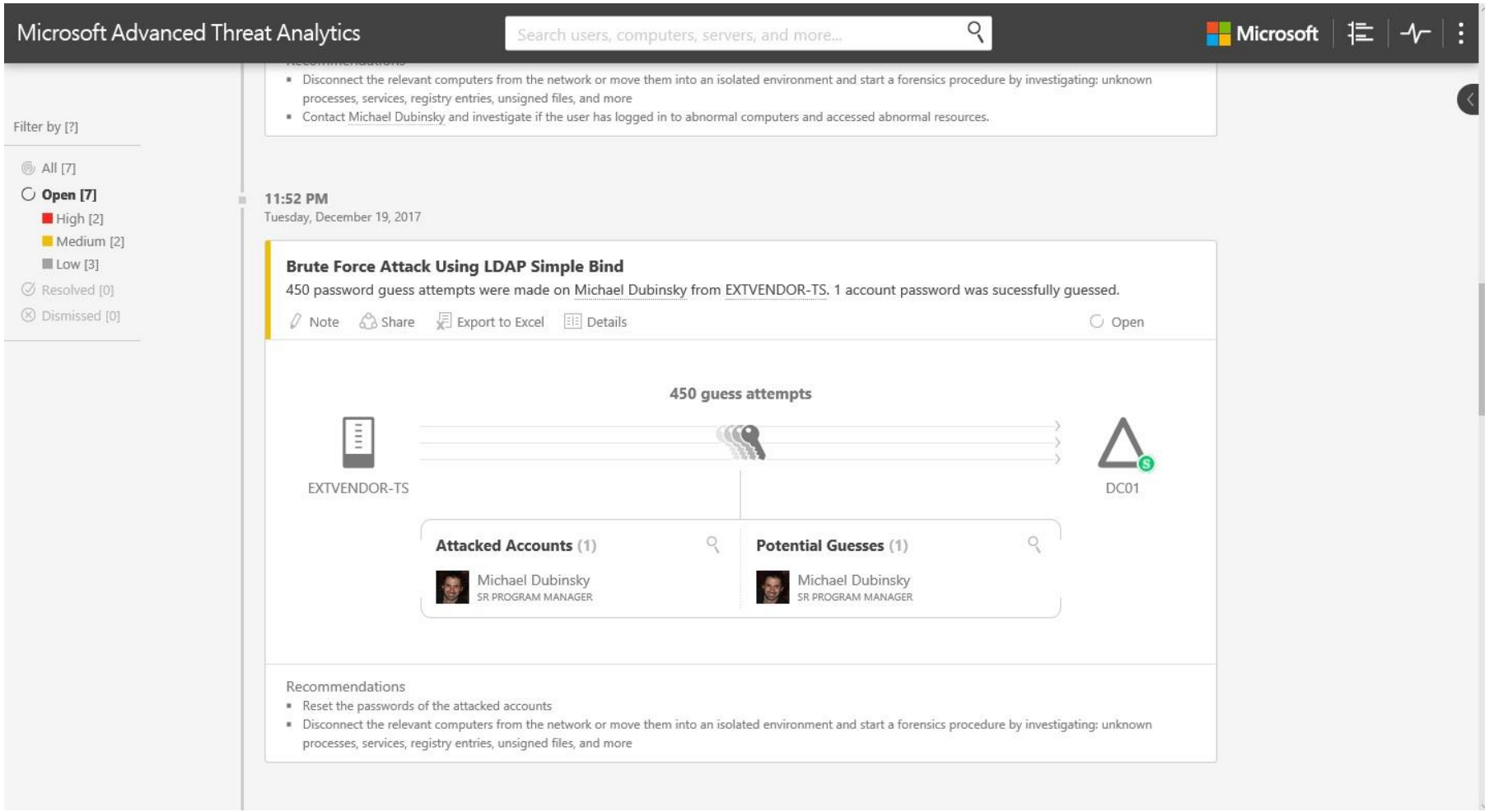
Перебор учеток



ATP - Как это работает

Перебор учеток

Взлом учетки

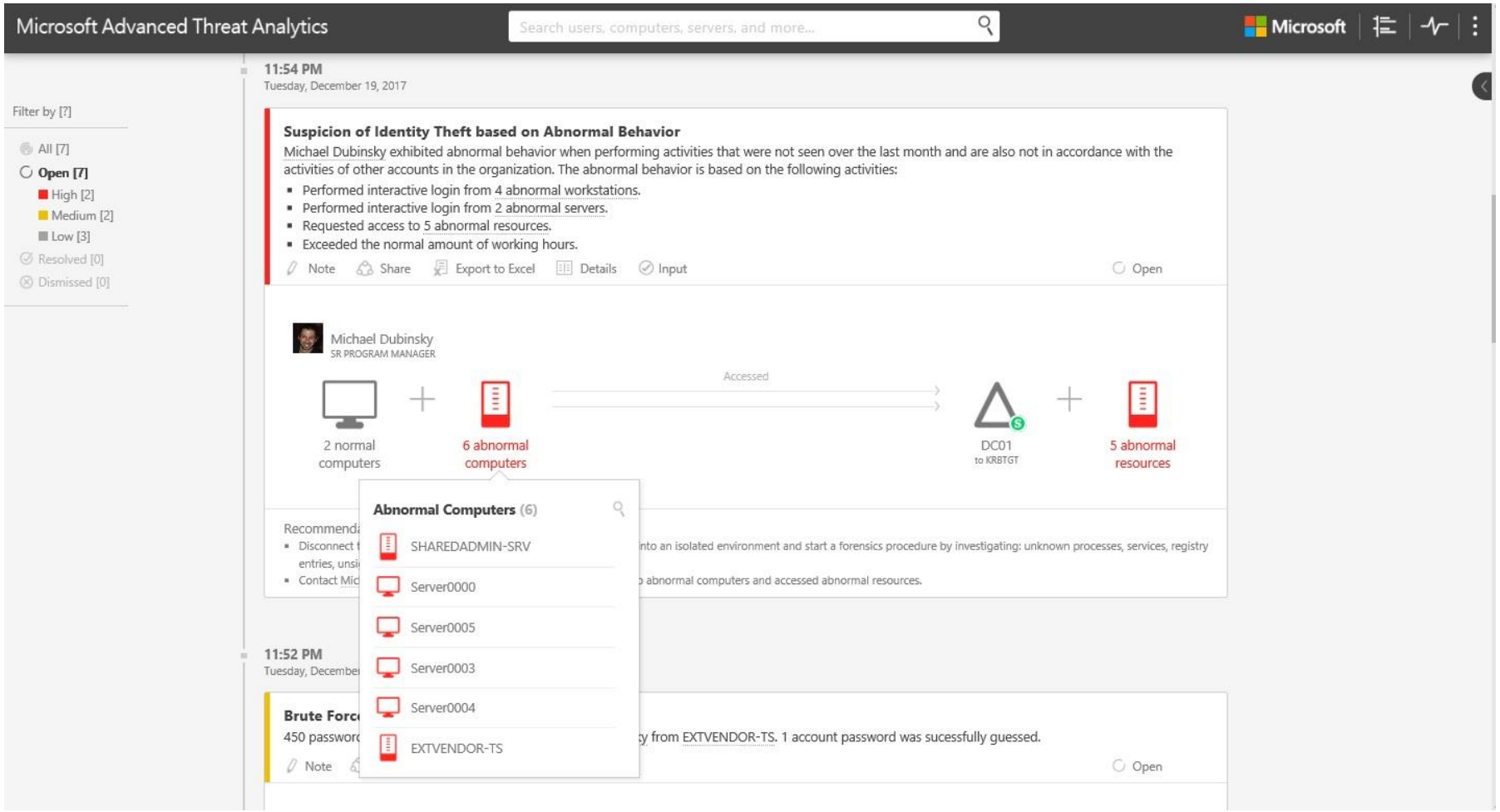


ATP - Как это работает

Перебор учеток

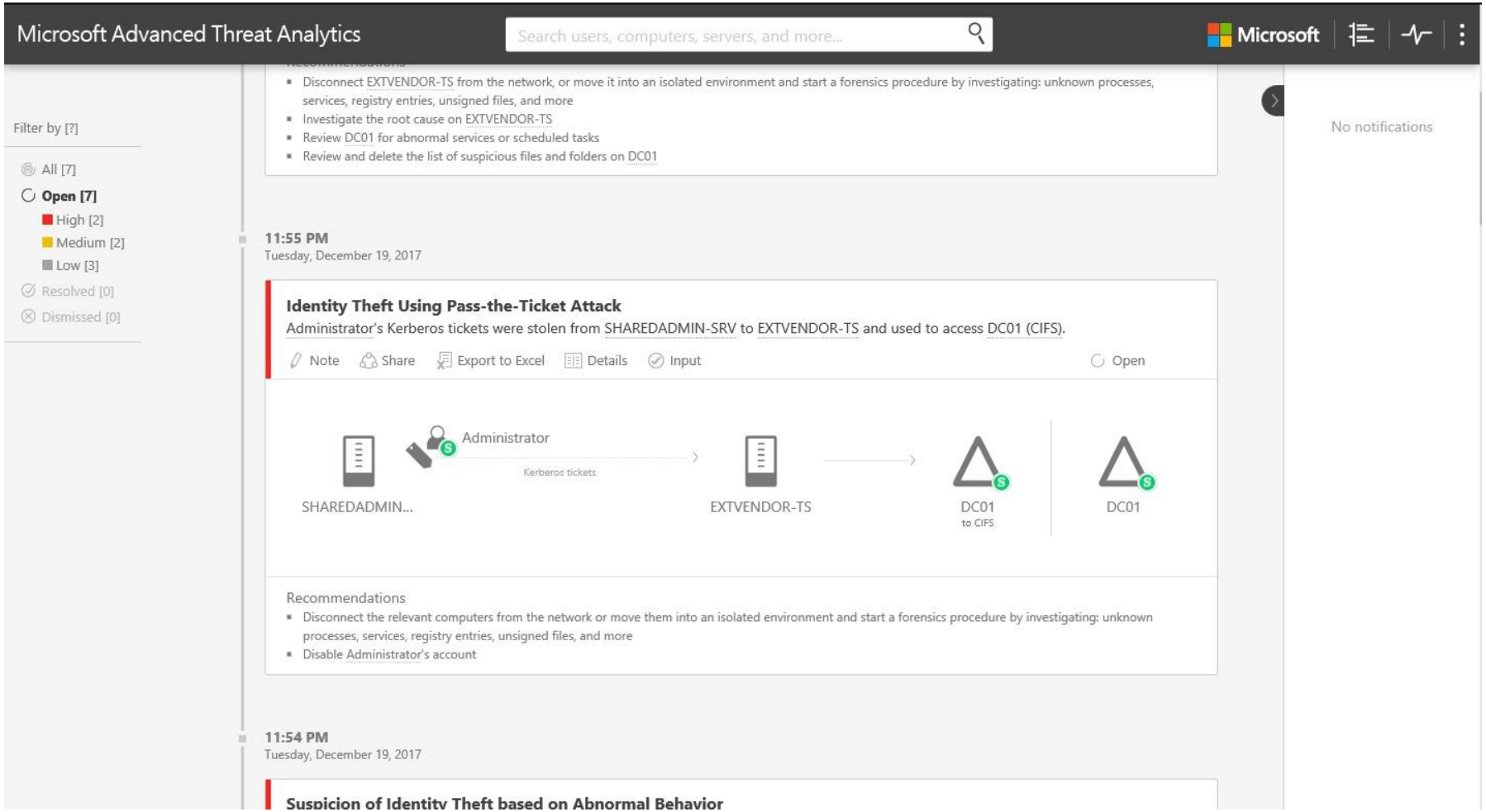
Взлом учетки

Масштабирование



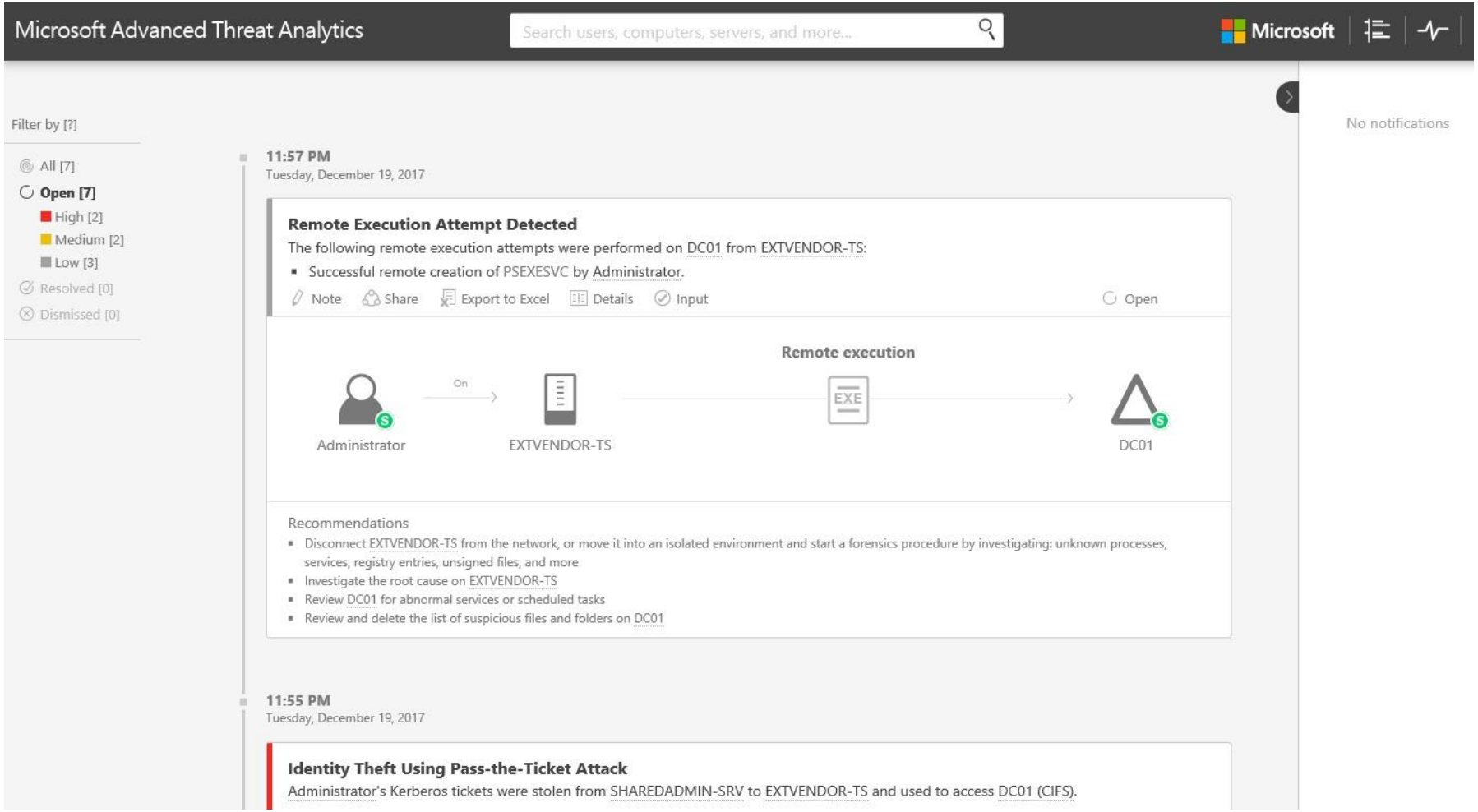
ATP - Как это работает

- Перебор учеток
- Взлом учетки
- Масштабирование
- **Попытка увеличения прав**



ATP - Как это работает

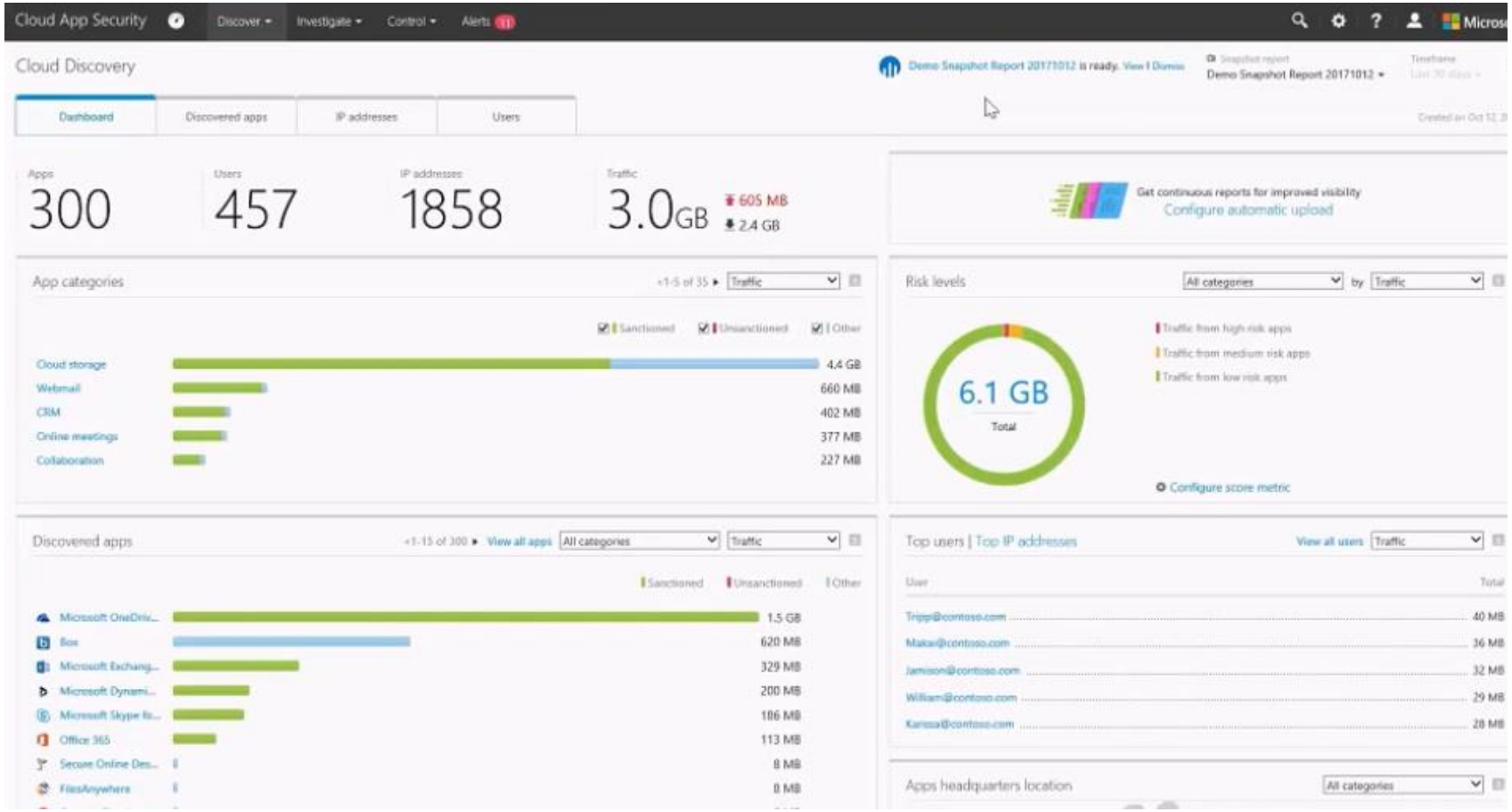
- **Перебор учеток**
- Взлом учетки
- Масштабирование
- Попытка увеличения прав
- Попытка запуска исполняемого файла



Microsoft Intune. Новый подход

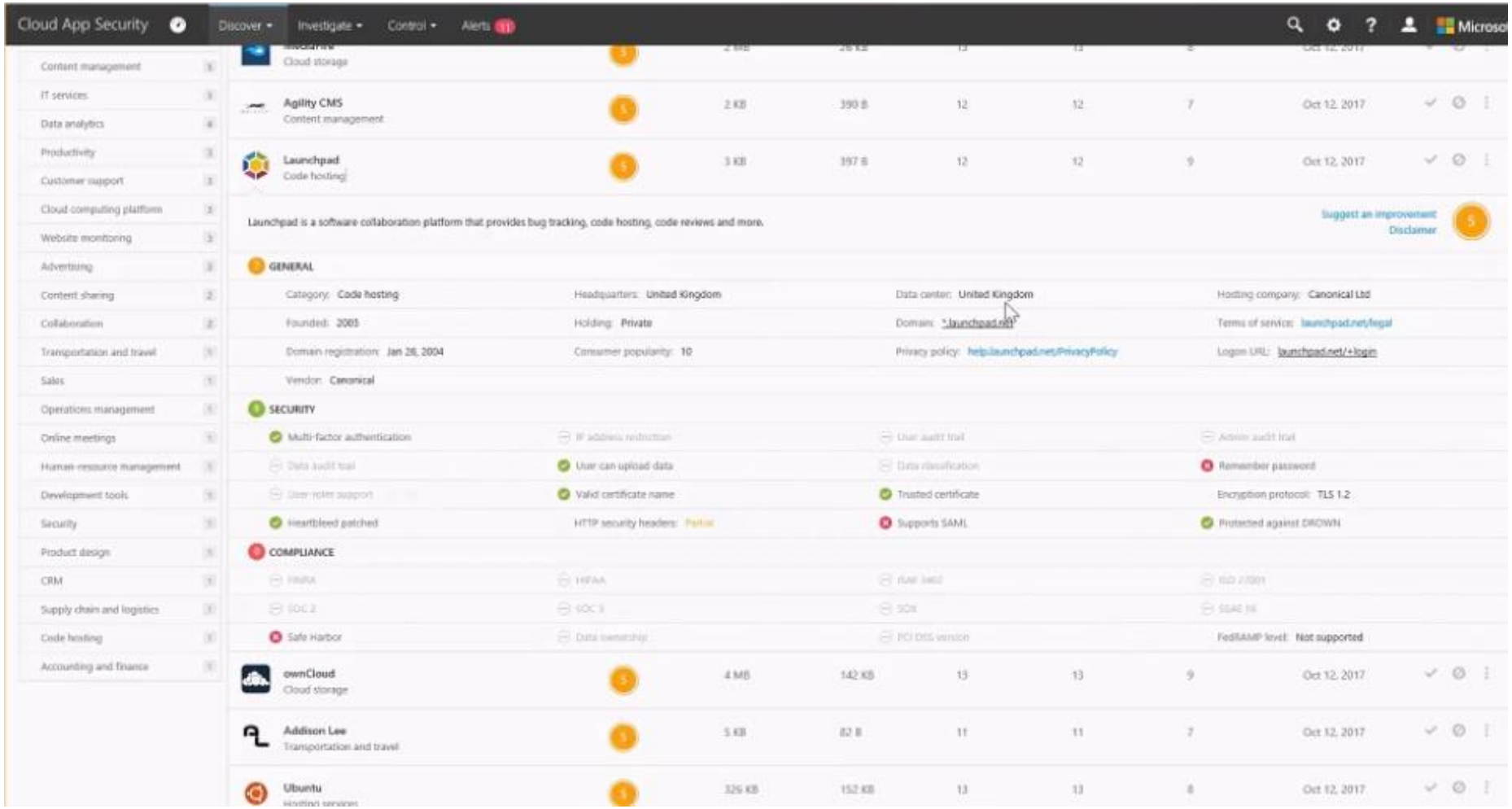
Cloud App Security

- Мониторинг трафика
- Отслеживание работы с файлами и их миграции.
- Отзыв файлов со сторонних сервисов
- Анализ контента в документе



Cloud App Security (CAS).
Контроль используемых облачных сервисов

- Рейтинг безопасности сервисов
- Возможность интеграции с рядом сервисов



Вопросы