

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 **0365** 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 TCOП, 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



Приложения

Office 365 Pro Plus:
Office на 5 ПК или Mac

Office для мобильных устройств:
Приложения для планшетов и смартфонов

Клиентский доступ и сервисы

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

Безопасность

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

Аналитика

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.)

Коммуникации в облаке

Cloud PBX + SfB Plus CAL:
Подключение облака Office 365 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



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.

Windows 10 Enterprise E5
Windows 10 Enterprise E3

Возможности Enterprise Mobility + Security E3/E5

	 Управление учетными записями и доступом	 Безопасность учетных записей	 Управление устройствами, в т.ч. мобильными	 Защита информации
EMS E5 	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 				

Преимущества EMS для заказчиков с O365

Enterprise
Mobility
+ Security



Office 365

Управление учетными записями и доступом



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

Базовое управление учетками через Azure AD для O365:

- Единая учетная запись для сервисов O365 + локальной среды
- Базовая многофакторная аутентификация при доступе к O365

Управление мобильными устройствами



MDM для O365+

- Управление ПК
- **Управление мобильными приложениями (запрет передачи данных между корп. и личной средой)**
- Безопасный просмотра контента
- Установка сертификатов
- Интеграция с SysCenter

Базовое управление устройствами через MDM для O365

- Управление настройками мобильных устройств
- Выборочное удаление данных
- Встроено в центр администрирования O365

Защита информации



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**

RMS-защита через RMS для O365

- Защита для документов Office (локальных или в O365)
- Доступ к RMS SDK
- Импорт собственного ключа в Azure RMS

Безопасность учетных записей



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

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

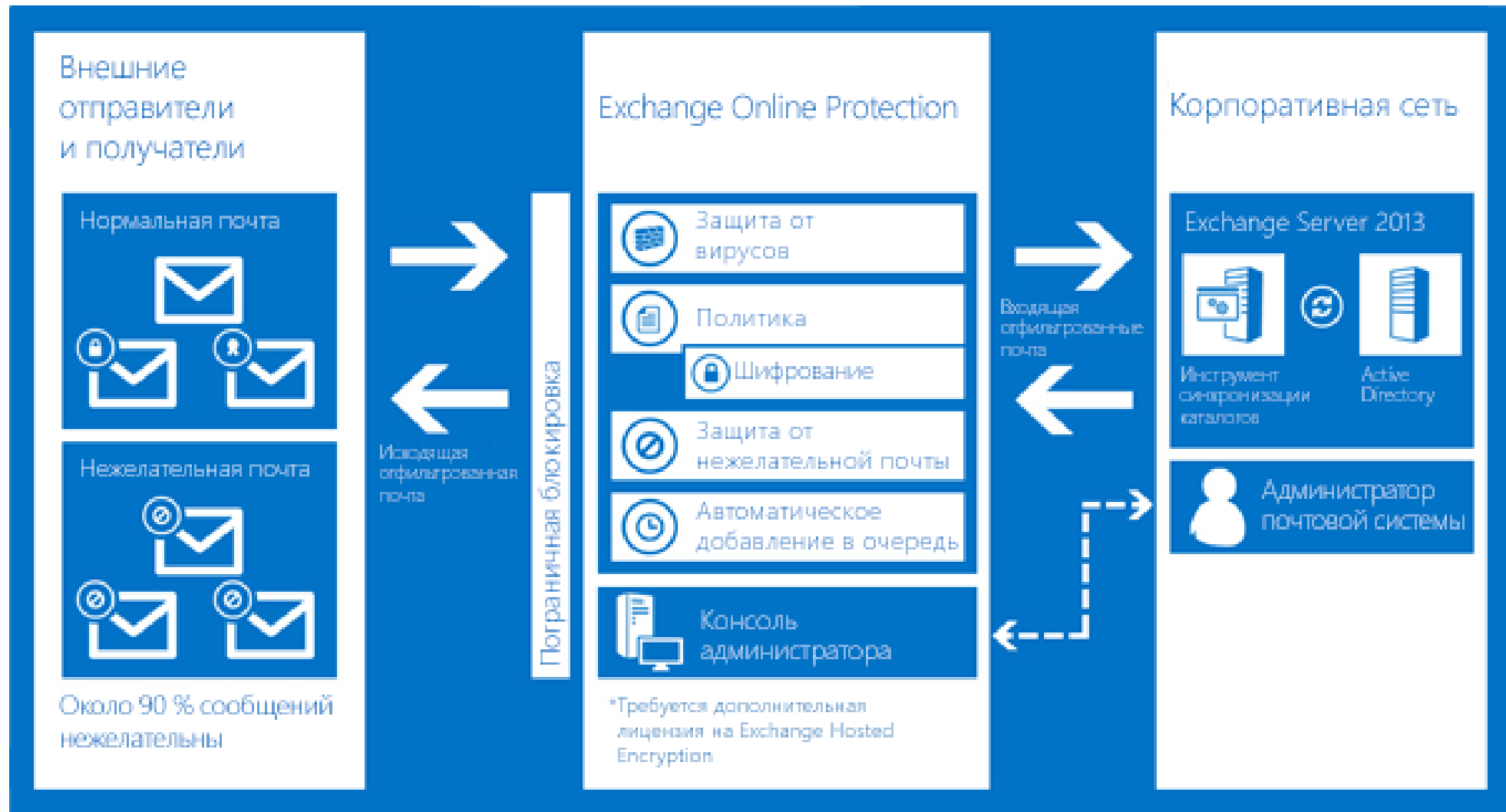
- Защита от вредоносных URL-адресов в режиме реального времени
- Растущая база URL-адресов



Широкие возможности создания отчетов и трассировки

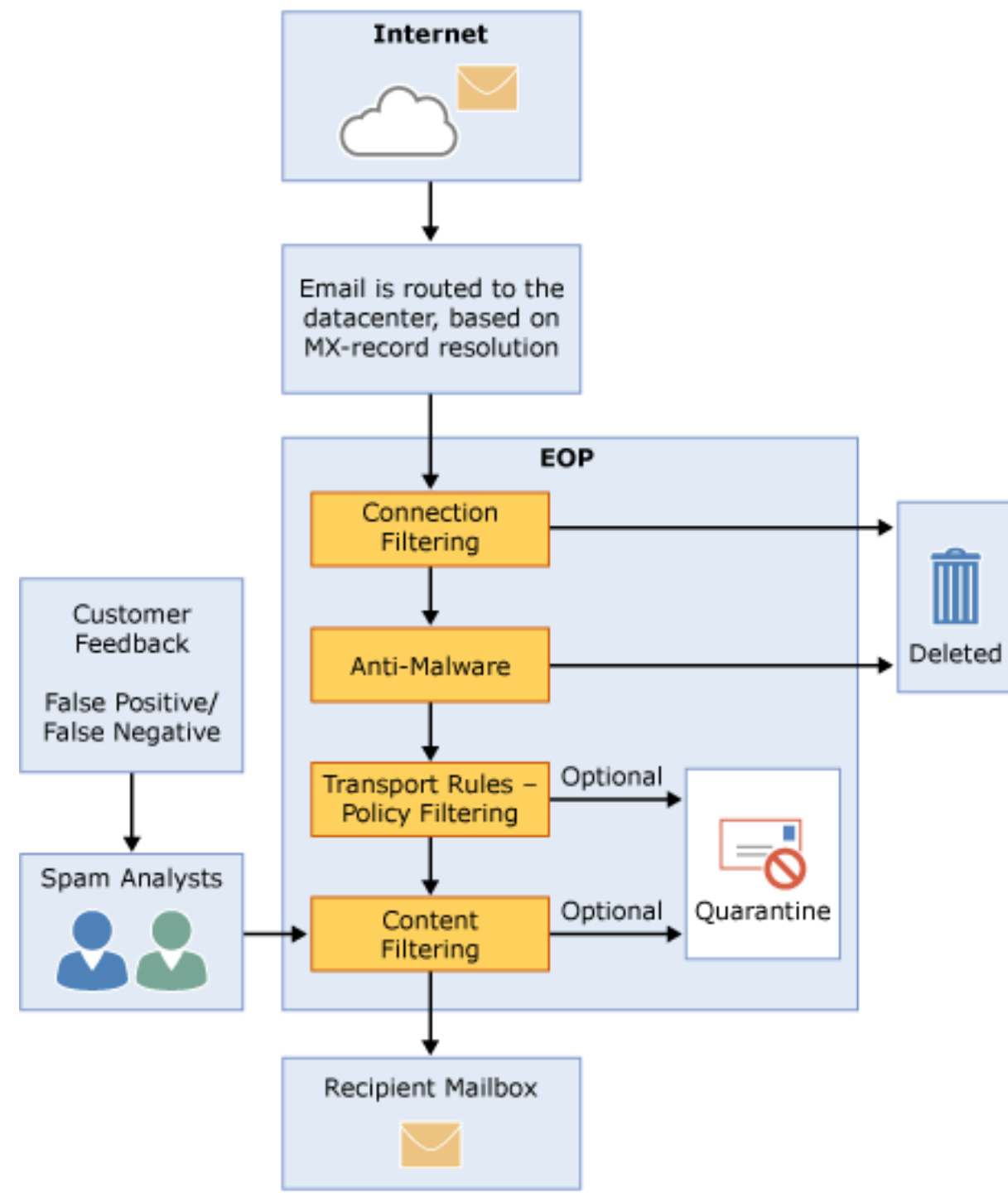
- Встроенные средства трассировки URL-адресов
- Отчеты о сложных угрозах

Exchange Online Protection

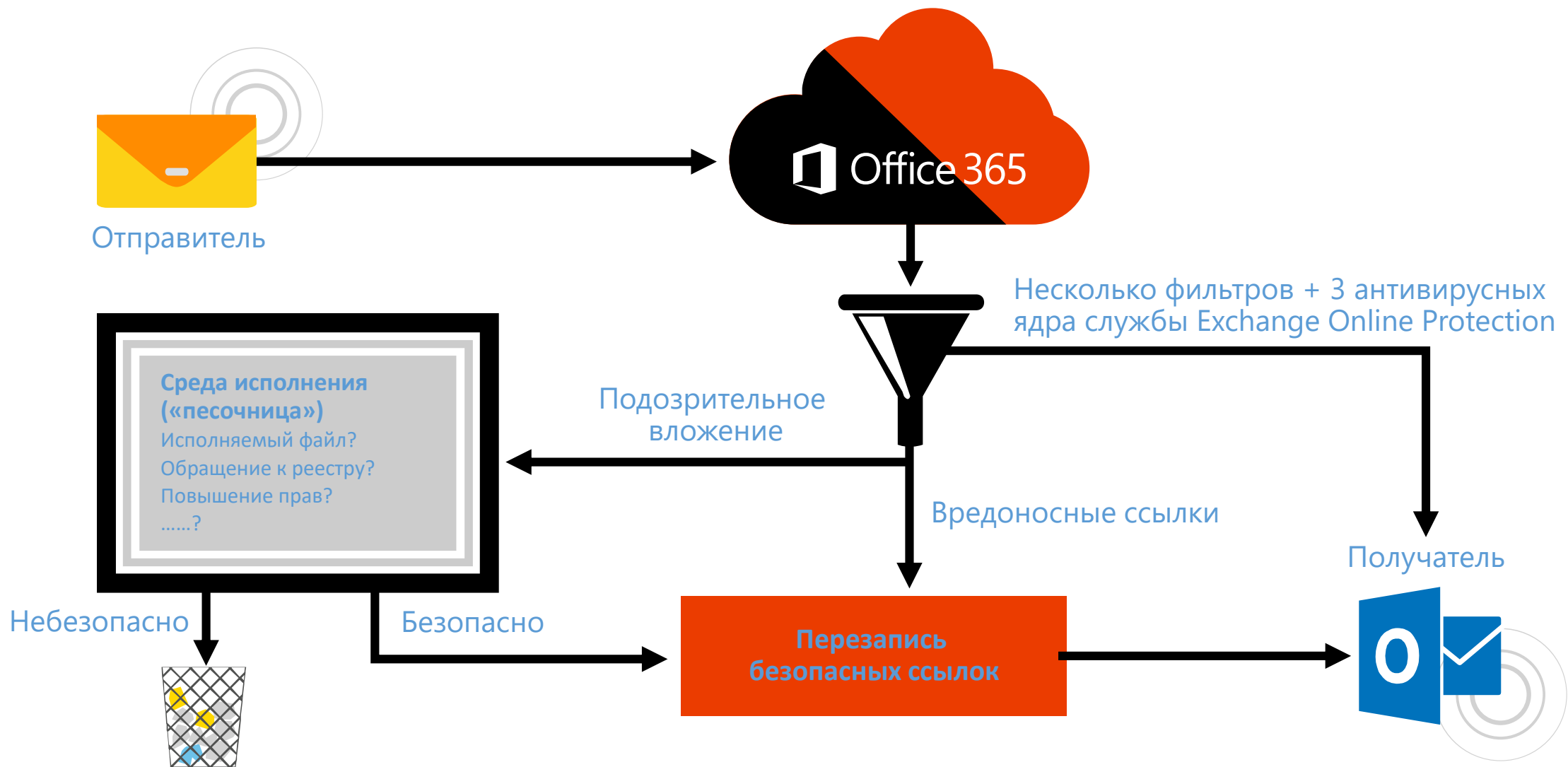


Exchange Online Protection

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 отфильтрованных писем в папку Нежелательной почты или в карантин.
5. Доставка письма получателю.



Архитектура службы Exchange Online Protection



Safe Attachments (Безопасные вложения) — ИСПОЛЬЗОВАНИЕ

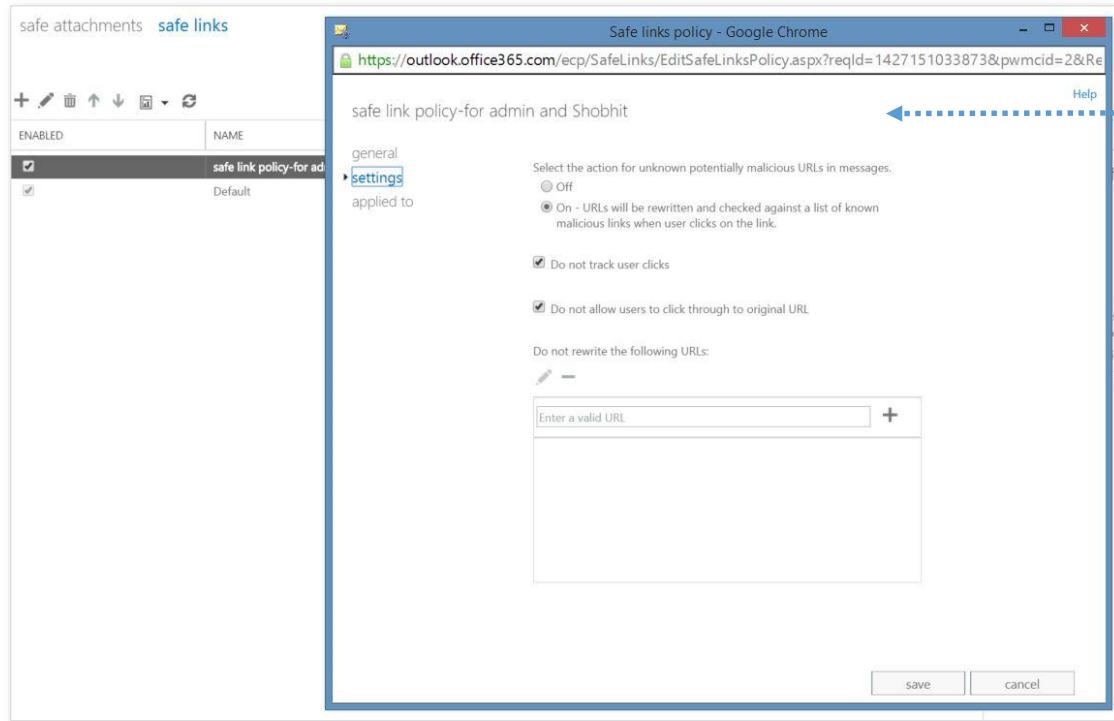
The image displays the configuration of a Safe Attachment Policy in the Exchange Admin Center. The policy is named "Safe Attachment Policy - Block" and is set to "Block" for unknown malware. The "Block" action is selected, which prevents the current and future emails and attachments with detected malware from being delivered. The "Enable redirect" option is checked, and the attachment is redirected to the email address "admin@contosobankatp.onmicrosoft.com".

Administrative actions are indicated by blue dashed arrows:

- An arrow points from the "Block" radio button to the text: "Администратор создает политику" (Administrator creates policy).
- An arrow points from the "Enable redirect" checkbox to the text: "Администратор получает уведомление, если блокируется сообщение" (Administrator receives notification if message is blocked).

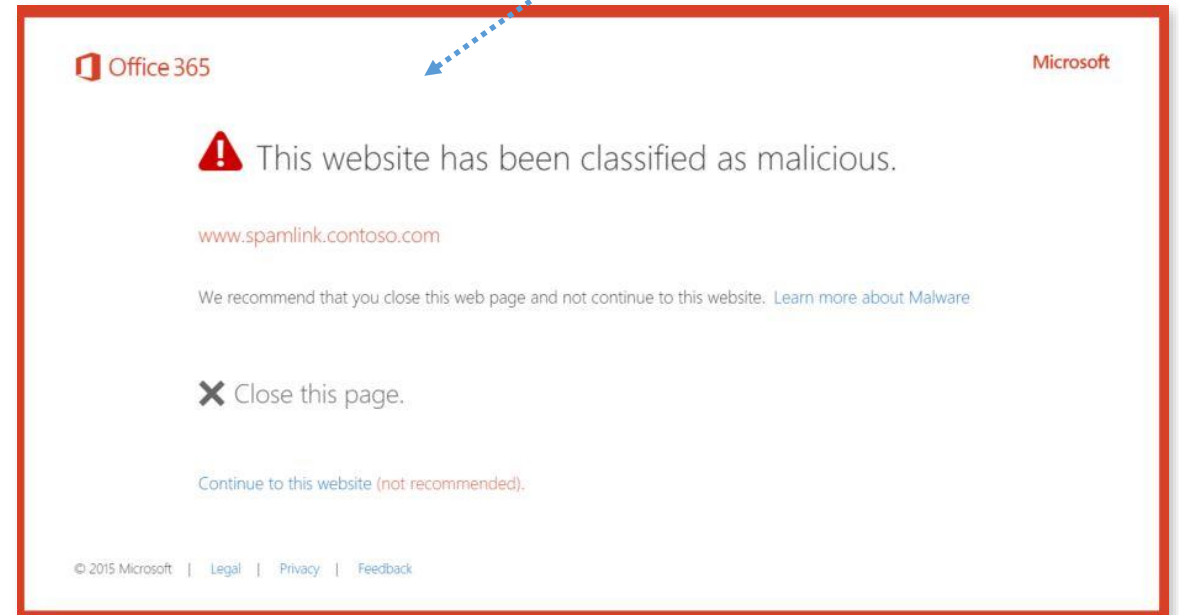
The bottom part of the image shows an email notification from "Exchange Online Advanced Threat Protection" with the subject "Administrator Notification: Redirecting email with malware". The notification states: "This message was created automatically by Exchange Online Advanced Threat Protection service. Malware was detected in the email included with this message as an attachment." It also includes the sender's name "Jeremyc@contosobankatp.onmicrosoft.com" and a warning: "The attached email or the attachment has not been delivered to the intended recipient(s). If it is opened, it might infect the computer with malware. Please do not respond to this message, it is an unmonitored alias. For more information, please see <http://go.microsoft.com/fwlink/?linkid=526076>."

Safe Links (Безопасные ссылки) – использование



Администратор создает политику

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



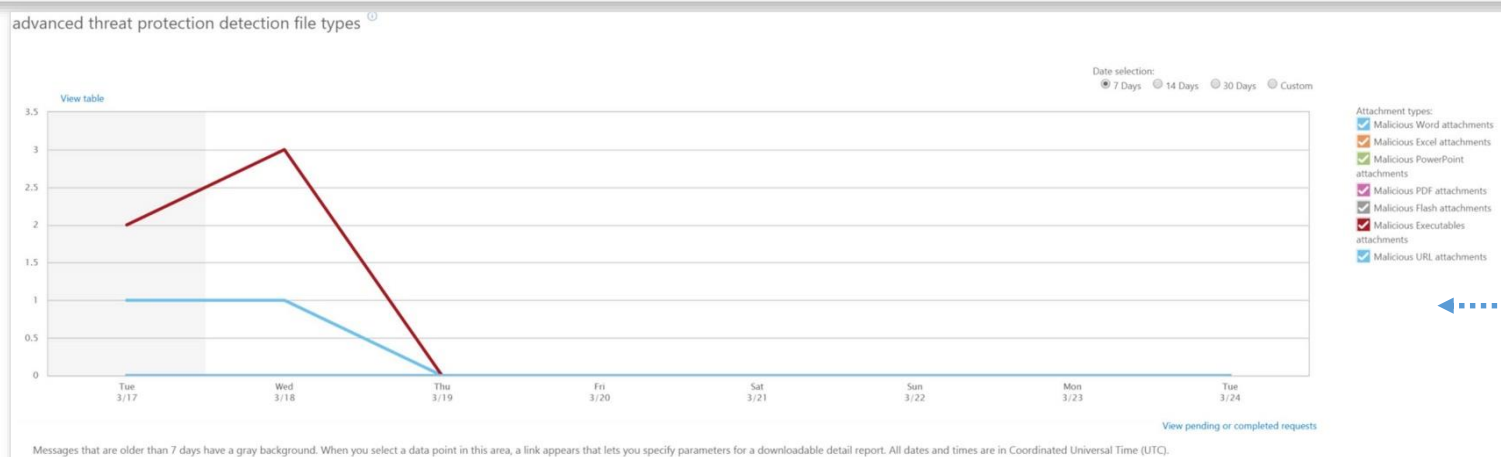
Широкие возможности создания отчетов и отслеживания нажатий

rules message trace url trace accepted domains remote domains connectors

Url Trace Results

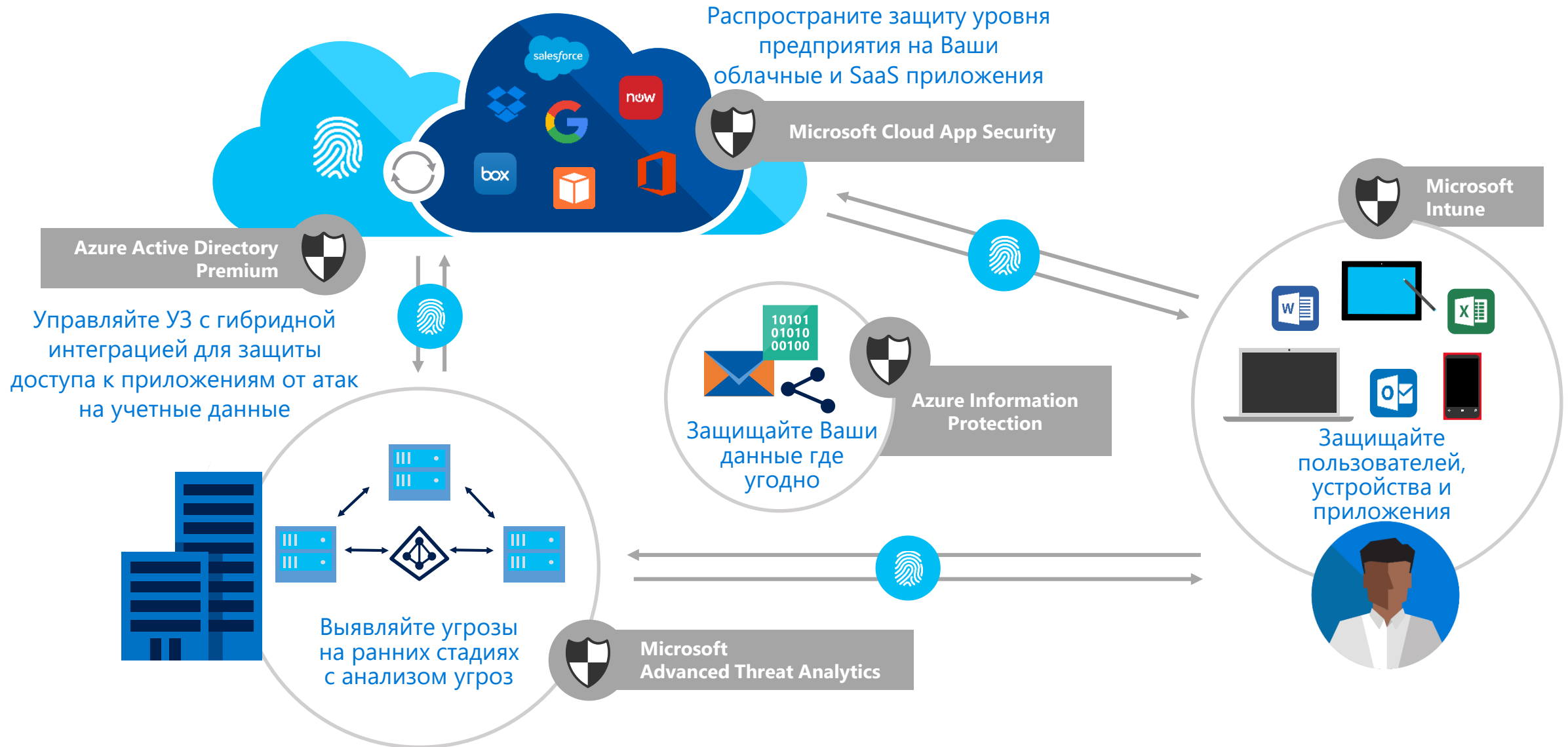
TIME OF CLICK (UTC)	RECIPIENT	URL	BLOCKED	CLICKED THROUGH	MESSAGE ID
3/23/2015 1:51:48 AM	shobhits@contosobankatp.onmicrosoft.com	http://www.spamlink.contoso.com/	Yes	No	<c5888139780a425e8e7f
3/21/2015 9:12:48 PM	shobhits@contosobankatp.onmicrosoft.com	http://www.bing.com	No	No	<3cead0a6775d47cfb7a8
3/21/2015 9:12:14 PM	shobhits@contosobankatp.onmicrosoft.com	http://www.spamlink.contoso.com/	Yes	No	<SNT147-W490DFDC2l
3/21/2015 8:05:19 PM	shobhits@contosobankatp.onmicrosoft.com	http://www.bing.com	No	No	<3cead0a6775d47cfb7a8
3/21/2015 8:05:15 PM	shobhits@contosobankatp.onmicrosoft.com	http://www.spamlink.contoso.com/	Yes	No	<SNT147-W684A55149A
3/21/2015 8:05:05 PM	shobhits@contosobankatp.onmicrosoft.com	http://www.bing.com	No	No	<3cead0a6775d47cfb7a8
3/21/2015 8:04:57 PM	shobhits@contosobankatp.onmicrosoft.com	http://www.spamlink.contoso.com/	Yes	No	<SNT147-W684A55149A
3/20/2015 7:42:59 PM	shobhits@contosobankatp.onmicrosoft.com	http://www.bing.com/	No	No	<6a344dc89e33436198d
3/20/2015 7:42:57 PM	shobhits@contosobankatp.onmicrosoft.com	http://www.spamlink.contoso.com/	Yes	No	<6a344dc89e33436198d
3/20/2015 7:42:54 PM	shobhits@contosobankatp.onmicrosoft.com	http://www.spamlink.contoso.com/	Yes	No	<6a344dc89e33436198d

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



Отчеты по типу и поведению файлов

Комплексный подход к защите



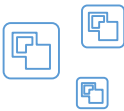
Контролируйте доступ из любого места

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



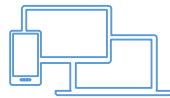
АТРИБУТЫ ПОЛЬЗОВАТЕЛЕЙ

Учетная запись
Членство в группах
Надежность аутентификации (MFA)



ПРИЛОЖЕНИЕ

Политики на основе приложений
Тип клиента
Критичность для бизнеса



УСТРОЙСТВА

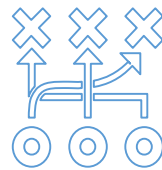
Является ли членом домена
Соответствие требованиям
Тип платформы (Windows, iOS, Android)



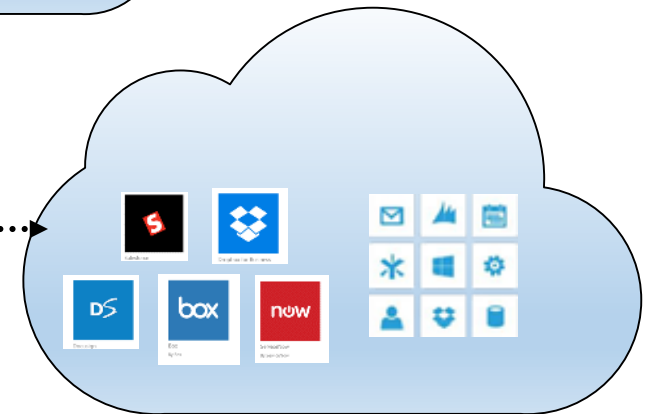
ИНОЕ

Из какой сети
Профилирование риска

Azure AD – единая точка контроля



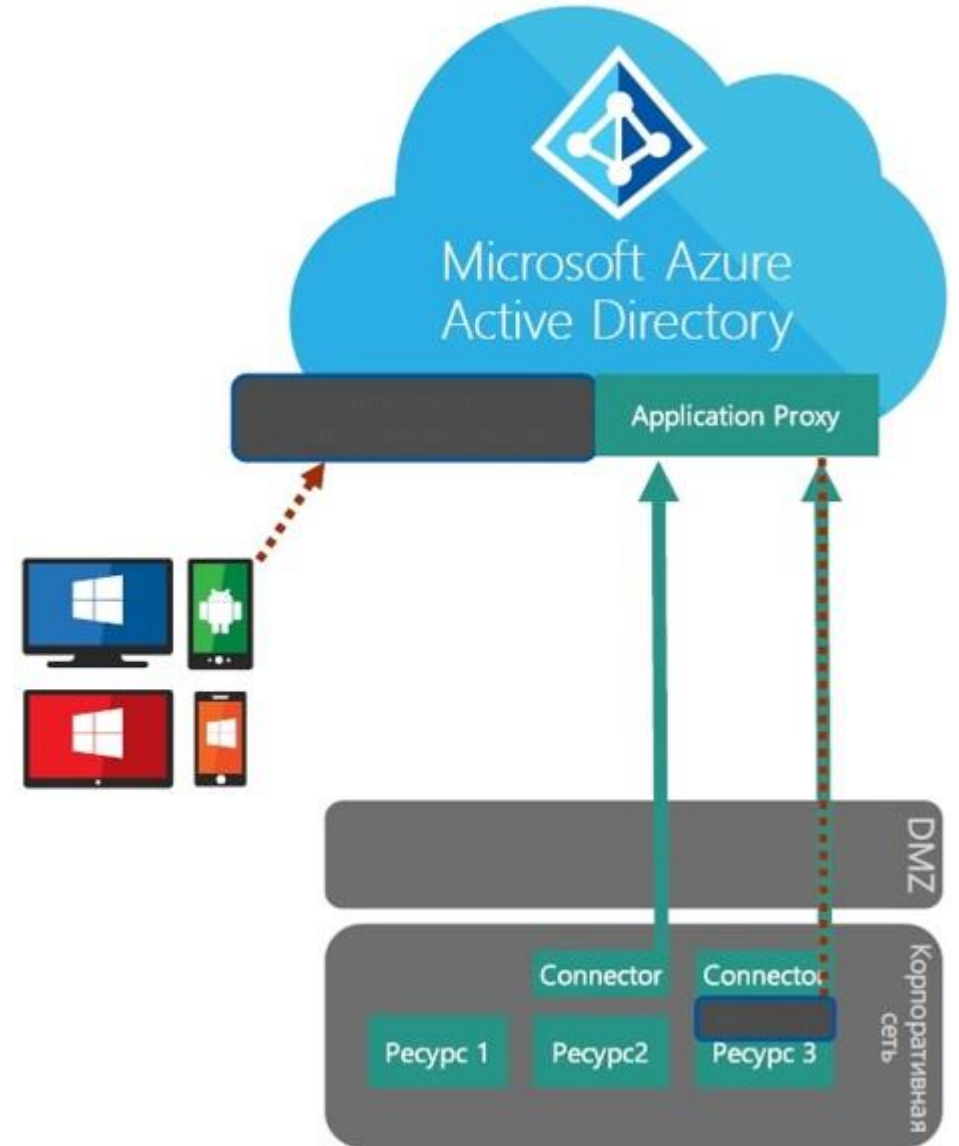
- Разрешить
- Потребовать MFA
- Блокировать



Локальные приложения

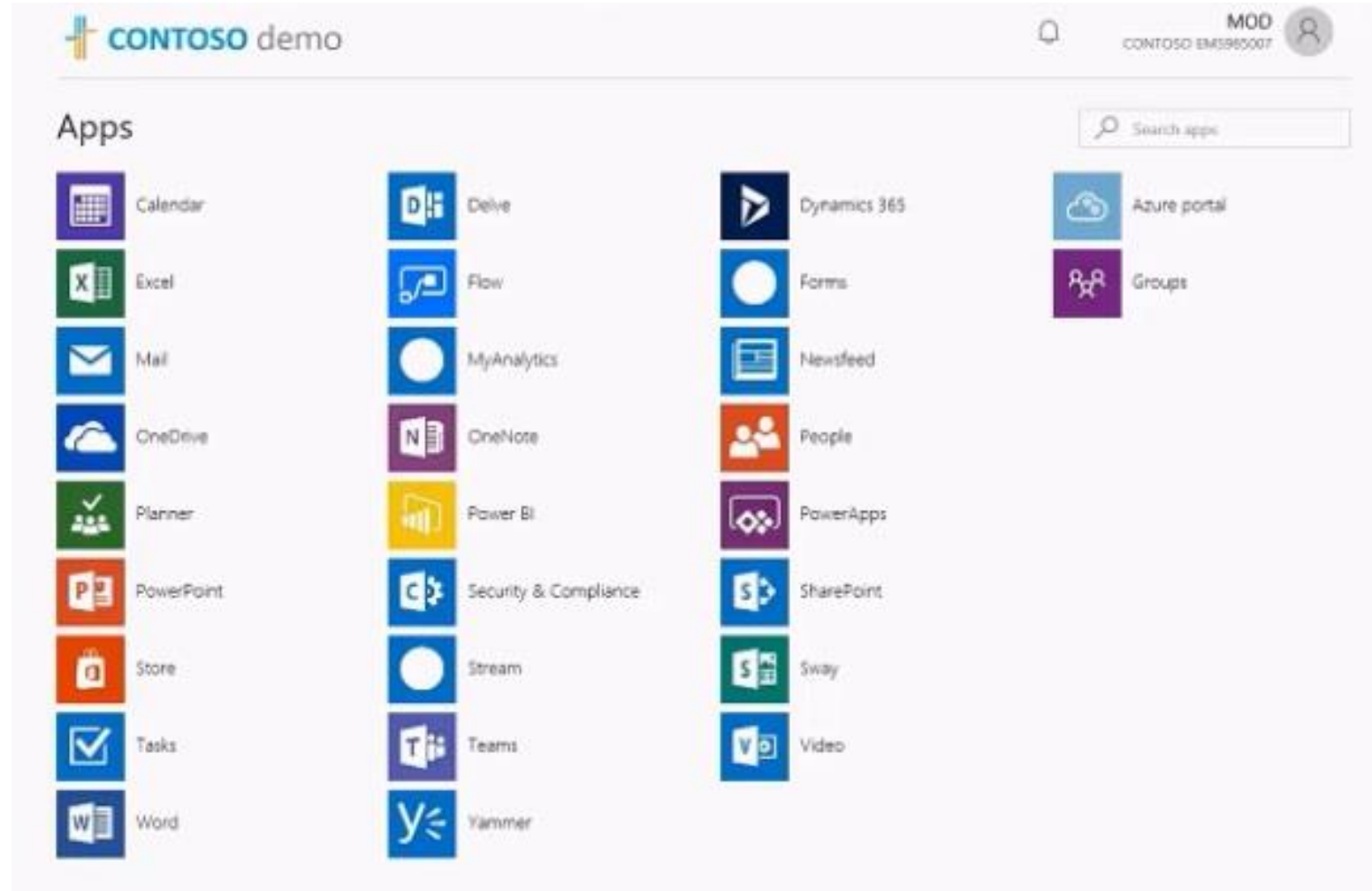
Azure Active Directory

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



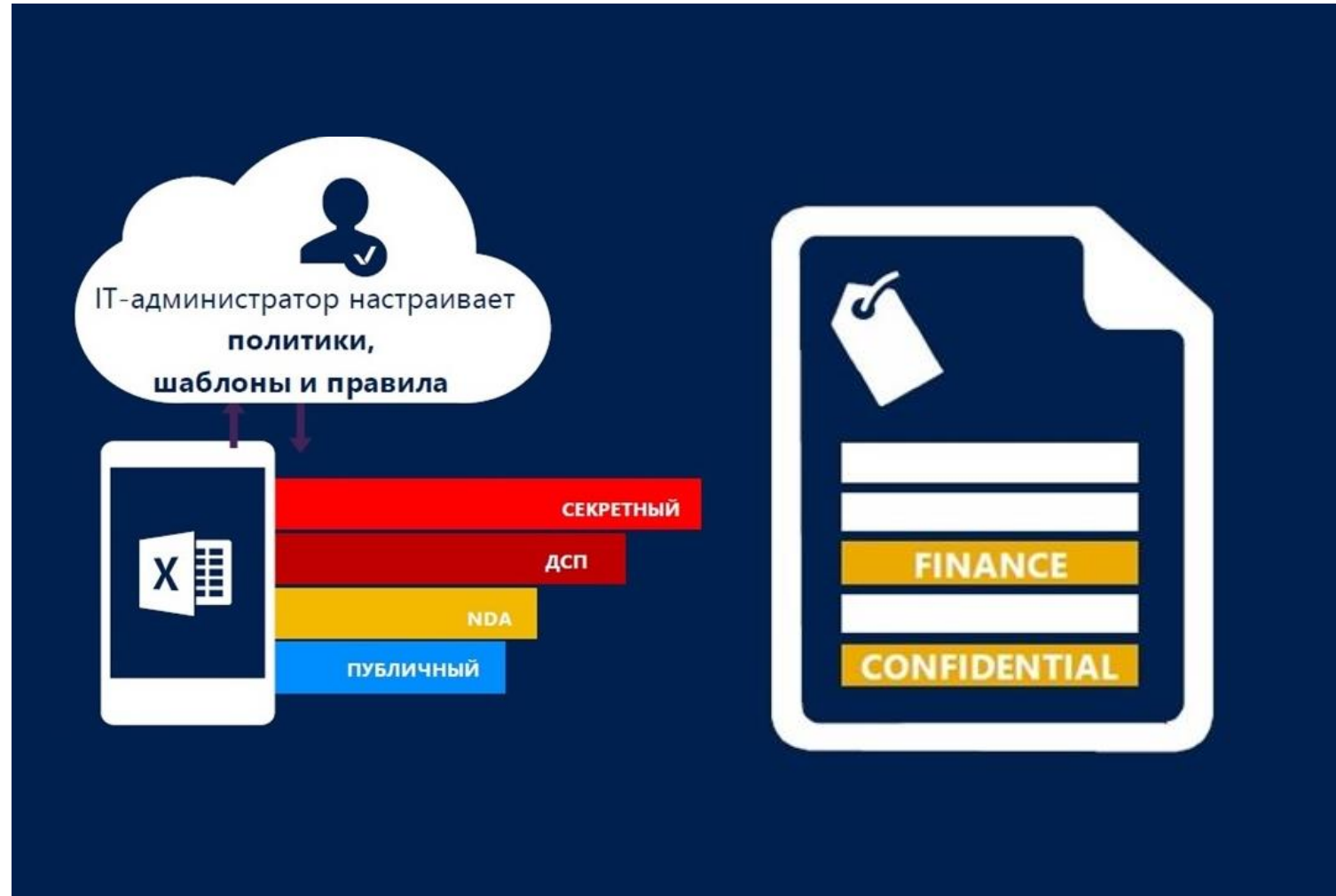
Портал Azure Active Directory

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



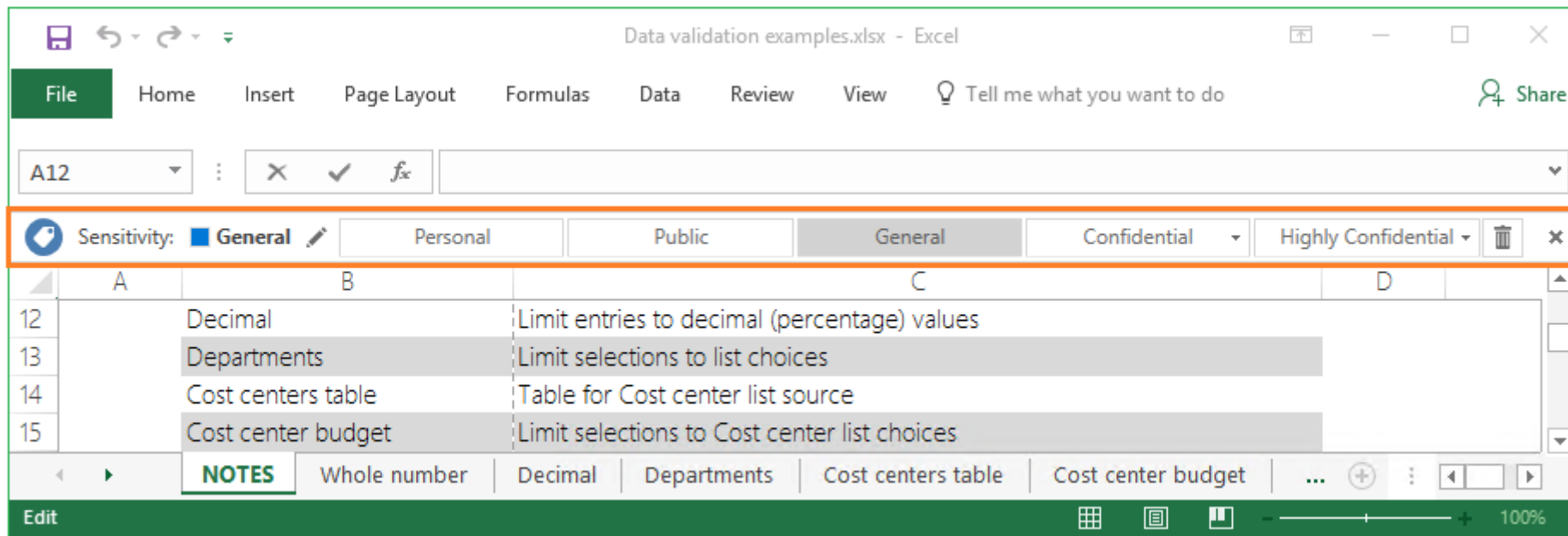
Azure Information Protection

- 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

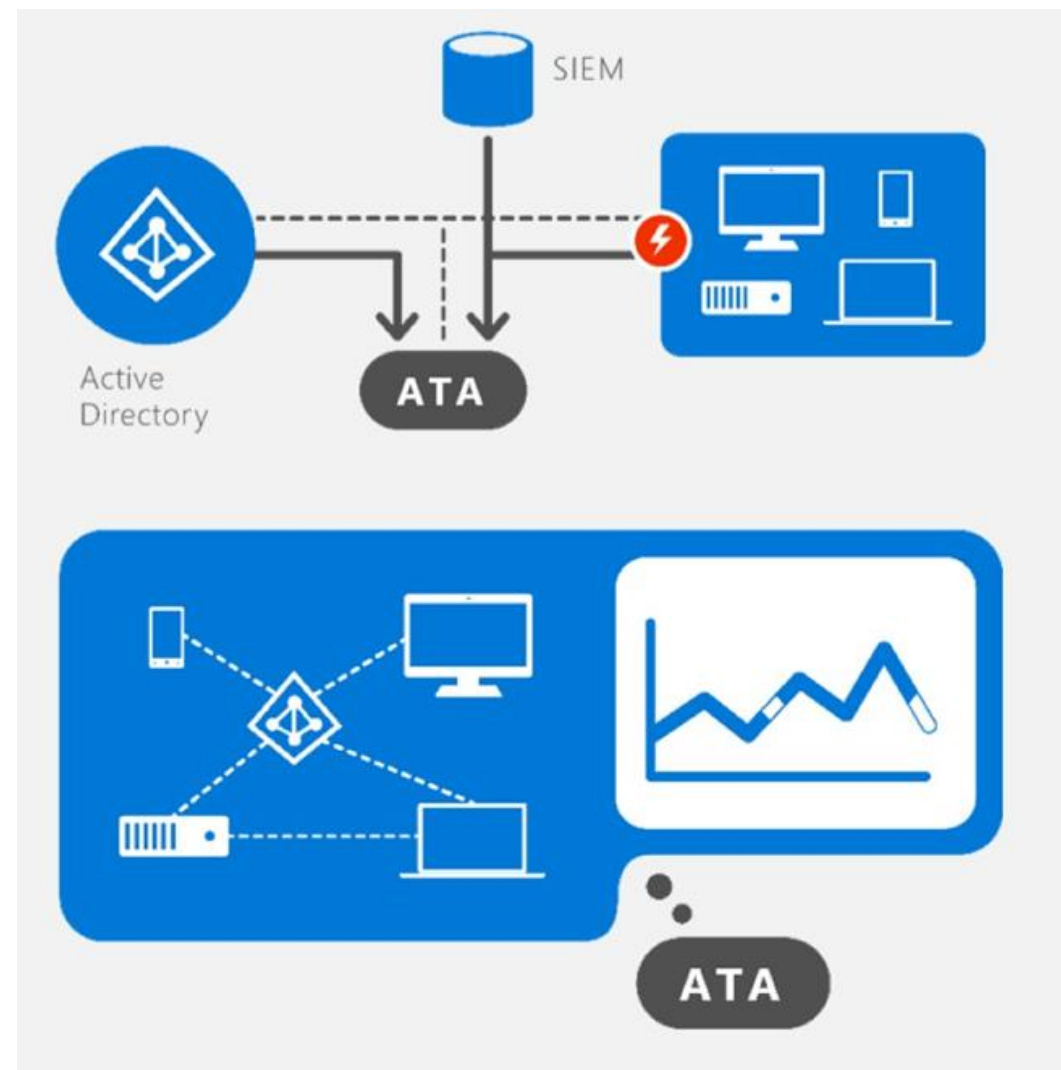
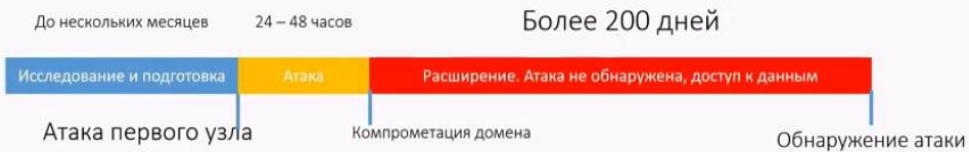
- Формирование наборов меток под каждую роль
- Принудительная или выборочная классификация по содержанию
- Защита путешествует с файлом через облако



Advanced Threat Analytics (ATA) – превентивная идентификация атак

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

Хронология атаки



АТР - Как это работает

Перебор учеток

Microsoft Advanced Threat Analytics

Search users, computers, servers, and more...

Microsoft

11:47 PM > 11:48 PM
Tuesday, December 19, 2017

Filter by [?]

- All [7]
- Open [7]
 - High [2]
 - Medium [2]
 - Low [3]
- Resolved [0]
- Dismissed [0]










Reconnaissance Using Account Enumeration

Suspicious account enumeration activity using Kerberos protocol, originating from EXTVENDOR-TS, was detected. The attacker performed a total of 105 guess attempts for account names, 3 guess attempts matched existing account names in Active Directory.

Note Share Export to Excel Open

105 guess attempts

EXTVENDOR-TS → DC01

Existing Accounts (3)	Non-Existing Accounts (102)
 Idan Plotnik PRINCIPAL GROUP MANAGER	 Mae contoso.com
 Administrator	 Theresa contoso.com
 Michael Dubinsky SR PROGRAM MANAGER	 Opal contoso.com
	 Velma contoso.com
	 Nancy contoso.com
	 Mattie contoso.com

АТР - Как это работает

Перебор учеток

Взлом учетки

Microsoft Advanced Threat Analytics

Search users, computers, servers, and more...

Microsoft

Filter by [?]

- All [7]
- Open [7]
 - High [2]
 - Medium [2]
 - Low [3]
- Resolved [0]
- Dismissed [0]

11:52 PM
Tuesday, December 19, 2017

Brute Force Attack Using LDAP Simple Bind
450 password guess attempts were made on Michael Dubinsky from EXTVENDOR-TS. 1 account password was successfully guessed.

Note Share Export to Excel Details Open

450 guess attempts

EXTVENDOR-TS → DC01

Attacked Accounts (1)

- Michael Dubinsky
SR PROGRAM MANAGER

Potential Guesses (1)

- Michael Dubinsky
SR PROGRAM MANAGER

Recommendations

- Reset the passwords of the attacked accounts
- Disconnect the relevant computers from the network or move them into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more

АТР - Как это работает

Перебор учеток

Взлом учетки

Масштабирование

The screenshot displays the Microsoft Advanced Threat Analytics (ATA) dashboard. At the top, there is a search bar and the Microsoft logo. The main content area shows a security alert titled "Suspicion of Identity Theft based on Abnormal Behavior" for user Michael Dubinsky, dated Tuesday, December 19, 2017, at 11:54 PM. The alert text states: "Michael Dubinsky exhibited abnormal behavior when performing activities that were not seen over the last month and are also not in accordance with the activities of other accounts in the organization. The abnormal behavior is based on the following activities:"

- Performed interactive login from 4 abnormal workstations.
- Performed interactive login from 2 abnormal servers.
- Requested access to 5 abnormal resources.
- Exceeded the normal amount of working hours.

Below the text, a diagram illustrates the user's activity. It shows "2 normal computers" and "6 abnormal computers" on the left, connected by an arrow labeled "Accessed" to "DC01 to KRBTGT" and "5 abnormal resources" on the right. A pop-up window titled "Abnormal Computers (6)" lists the following servers:

- SHAREDADMIN-SRV
- Server0000
- Server0005
- Server0003
- Server0004
- EXTVENDOR-TS

At the bottom of the screenshot, another alert titled "Brute Force" is partially visible, dated Tuesday, December 19, 2017, at 11:52 PM. It mentions "450 password" and "EXTVENDOR-TS. 1 account password was successfully guessed."

АТР - Как это работает

Перебор учеток

Взлом учетки

Масштабирование

Попытка
увеличения прав

Microsoft Advanced Threat Analytics

Search users, computers, servers, and more...

Microsoft

Filter by [?]

- All [7]
- Open [7]
 - High [2]
 - Medium [2]
 - Low [3]
- Resolved [0]
- Dismissed [0]

Recommendations

- Disconnect EXTENDOR-TS from the network, or move it into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more
- Investigate the root cause on EXTENDOR-TS
- Review DC01 for abnormal services or scheduled tasks
- Review and delete the list of suspicious files and folders on DC01

11:55 PM
Tuesday, December 19, 2017

Identity Theft Using Pass-the-Ticket Attack
Administrator's Kerberos tickets were stolen from SHAREDADMIN-SRV to EXTENDOR-TS and used to access DC01 (CIFS).

Note Share Export to Excel Details Input Open

```
graph LR; SHAREDADMIN[SHAREDADMIN-SRV] -- Kerberos tickets --> EXTENDOR[EXTENDOR-TS]; EXTENDOR --> DC01_CIFS[DC01 to CIFS]; EXTENDOR --> DC01[DC01]
```

Recommendations

- Disconnect the relevant computers from the network or move them into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more
- Disable Administrator's account

11:54 PM
Tuesday, December 19, 2017

Suspicion of Identity Theft based on Abnormal Behavior

No notifications

АТР - Как это работает

Перебор учеток

Взлом учетки

Масштабирование

Попытка
увеличения прав

Попытка запуска
исполняемого
файла

Microsoft Advanced Threat Analytics

Search users, computers, servers, and more...

Microsoft

Filter by [?]

- All [7]
- Open [7]
 - High [2]
 - Medium [2]
 - Low [3]
- Resolved [0]
- Dismissed [0]

11:57 PM
Tuesday, December 19, 2017

Remote Execution Attempt Detected

The following remote execution attempts were performed on DC01 from EXTVENDOR-TS:

- Successful remote creation of PSEXESVC by Administrator.

Note Share Export to Excel Details Input Open

Remote execution

Administrator → On → EXTVENDOR-TS → EXE → DC01

Recommendations

- Disconnect EXTVENDOR-TS from the network, or move it into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more
- Investigate the root cause on EXTVENDOR-TS
- Review DC01 for abnormal services or scheduled tasks
- Review and delete the list of suspicious files and folders on DC01

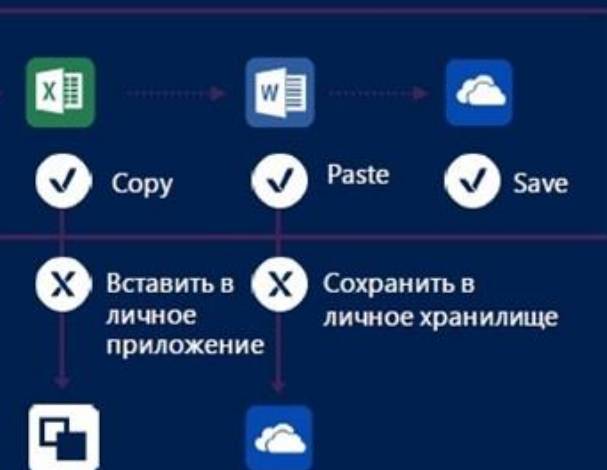
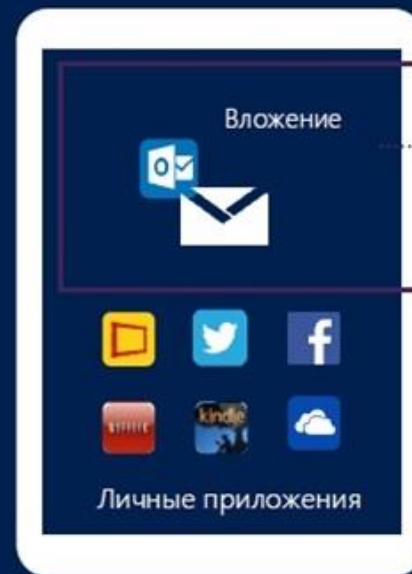
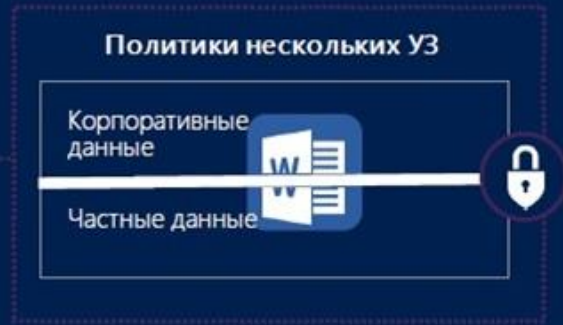
11:55 PM
Tuesday, December 19, 2017

Identity Theft Using Pass-the-Ticket Attack

Administrator's Kerberos tickets were stolen from SHAREDADMIN-SRV to EXTVENDOR-TS and used to access DC01 (CIFS).

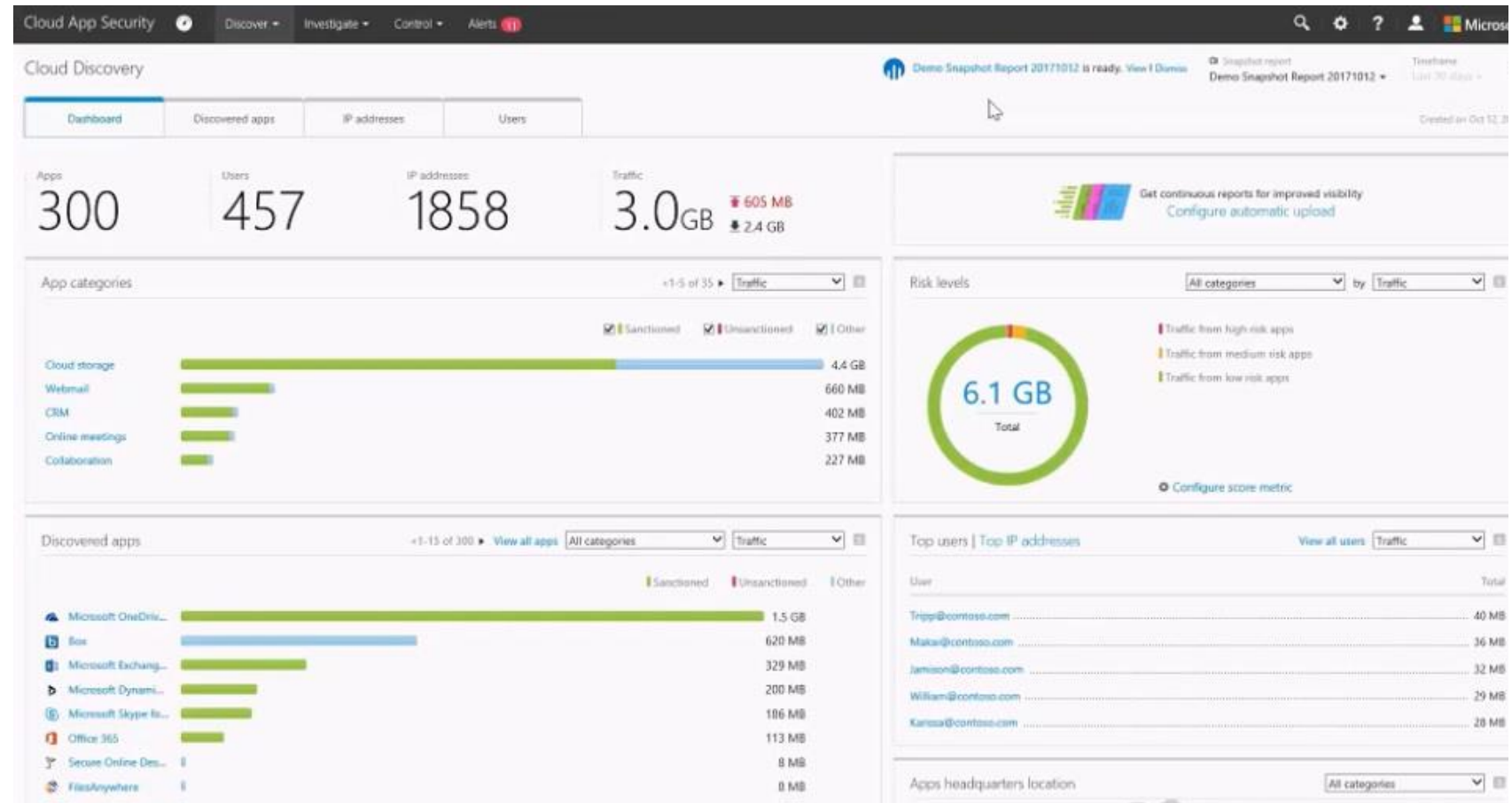
Microsoft Intune. Новый подход

Intune



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

The screenshot displays the Microsoft Cloud App Security (CAS) dashboard. The top navigation bar includes 'Discover', 'Investigate', 'Control', and 'Alerts'. The left sidebar lists various service categories such as Content management, IT services, Data analytics, Productivity, Customer support, Cloud computing platform, Website monitoring, Advertising, Content sharing, Collaboration, Transportation and travel, Sales, Operations management, Online meetings, Human resource management, Development tools, Security, Product design, CRM, Supply chain and logistics, Code hosting, and Accounting and finance.

The main content area shows a list of cloud services with columns for service name, icon, and various metrics. The services listed include:

- Cloud storage (2 MB, 26 KB, 13, 13, 8, Oct 12, 2017)
- Agility CMS (2 KB, 390 B, 12, 12, 7, Oct 12, 2017)
- Launchpad (3 KB, 397 B, 12, 12, 9, Oct 12, 2017)

Below the list, there is a detailed report for Launchpad, which is a software collaboration platform. The report is organized into sections:

- GENERAL**
 - Category: Code hosting
 - Headquarters: United Kingdom
 - Data center: United Kingdom
 - Hosting company: Canonical Ltd
 - Founded: 2003
 - Holding: Private
 - Domain: launchpad.net
 - Terms of service: launchpad.net/legal
 - Domain registration: Jan 26, 2004
 - Consumer popularity: 10
 - Privacy policy: help.launchpad.net/PrivacyPolicy
 - Login URL: launchpad.net/+login
 - Vendor: Canonical
- SECURITY**
 - Multi-factor authentication:
 - IP address restriction:
 - User audit trail:
 - Admin audit trail:
 - Data audit trail:
 - User can upload data:
 - Data classification:
 - Remember password:
 - User roles support:
 - Valid certificate name:
 - Trusted certificate:
 - Encryption protocol: TLS 1.2
 - Heartbleed patched:
 - HTTP security headers: **Partial**
 - Supports SAML:
 - Protected against DROWN:
- COMPLIANCE**
 - GDPR:
 - HIPAA:
 - ISO 27001:
 - SOX:
 - SOX:
 - SOX:
 - SOX:
 - SOX:
 - Safe Harbor:
 - Data ownership:
 - PCI DSS version:
 - FedRAMP level: Not supported

At the bottom of the screenshot, other services are visible in the list, including ownCloud (4 MB, 142 KB, 13, 13, 9, Oct 12, 2017), Addison Lee (5 KB, 87 B, 11, 11, 7, Oct 12, 2017), and Ubuntu (325 KB, 152 KB, 13, 13, 8, Oct 12, 2017).

Вопросы

