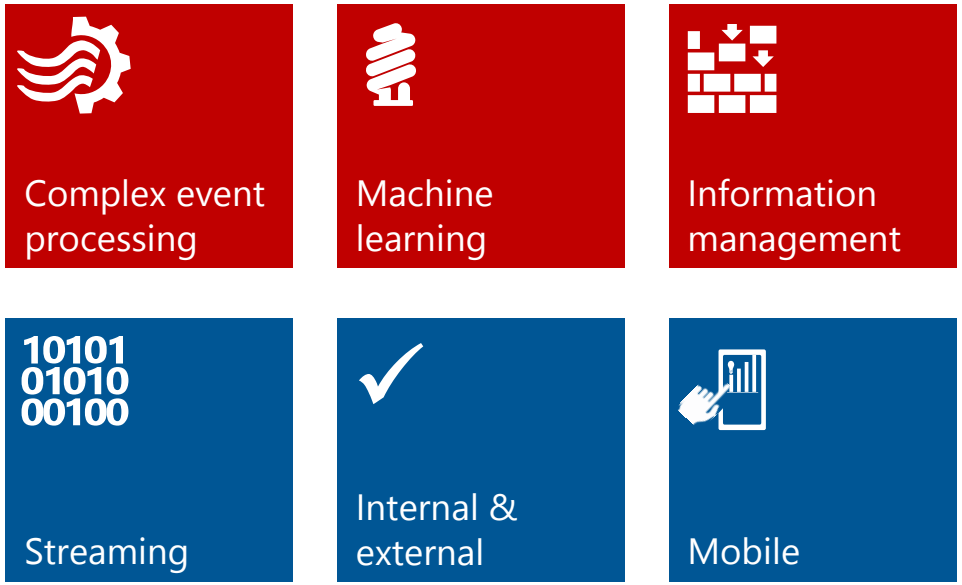
Microsoft

Средства обеспечения защиты информации для сценариев мобильной работы и облачных сервисов.

Валентин Елисеев
Руководитель направления Cloud & Enterprise
Майкрософт Украина

"Top Ten Strategic Technology Trends for 2016." by Gartner

1. **The device mesh**
2. **Ambient user experience**
3. **3D printing**
4. **Information of everything**
5. **Deep neural nets**
6. **Autonomous agents**
7. **Adaptive security architecture**
8. **Advanced system architecture**
9. **Mesh app and service architecture**
10. **Internet of Things platforms**

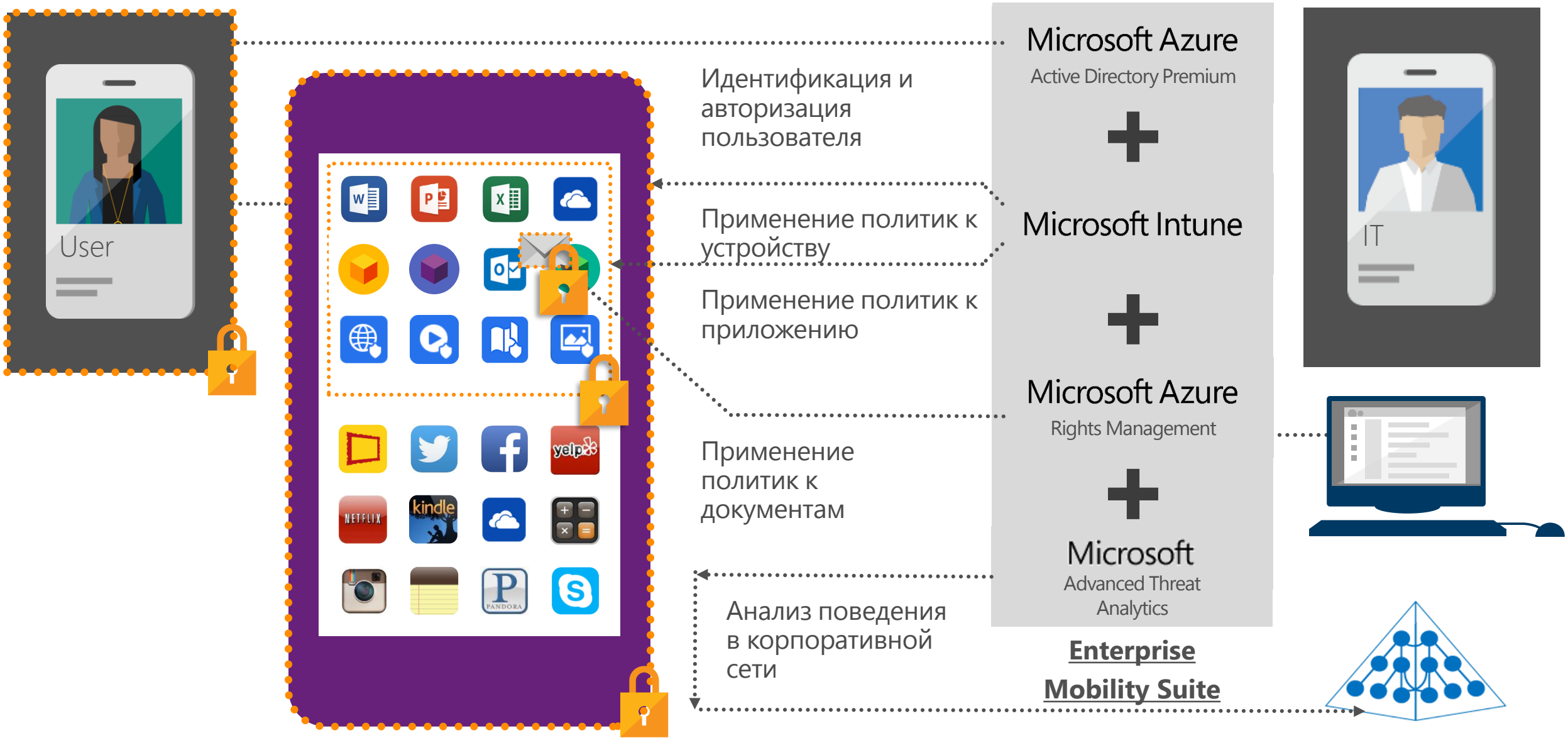


Cloud First
Mobile First

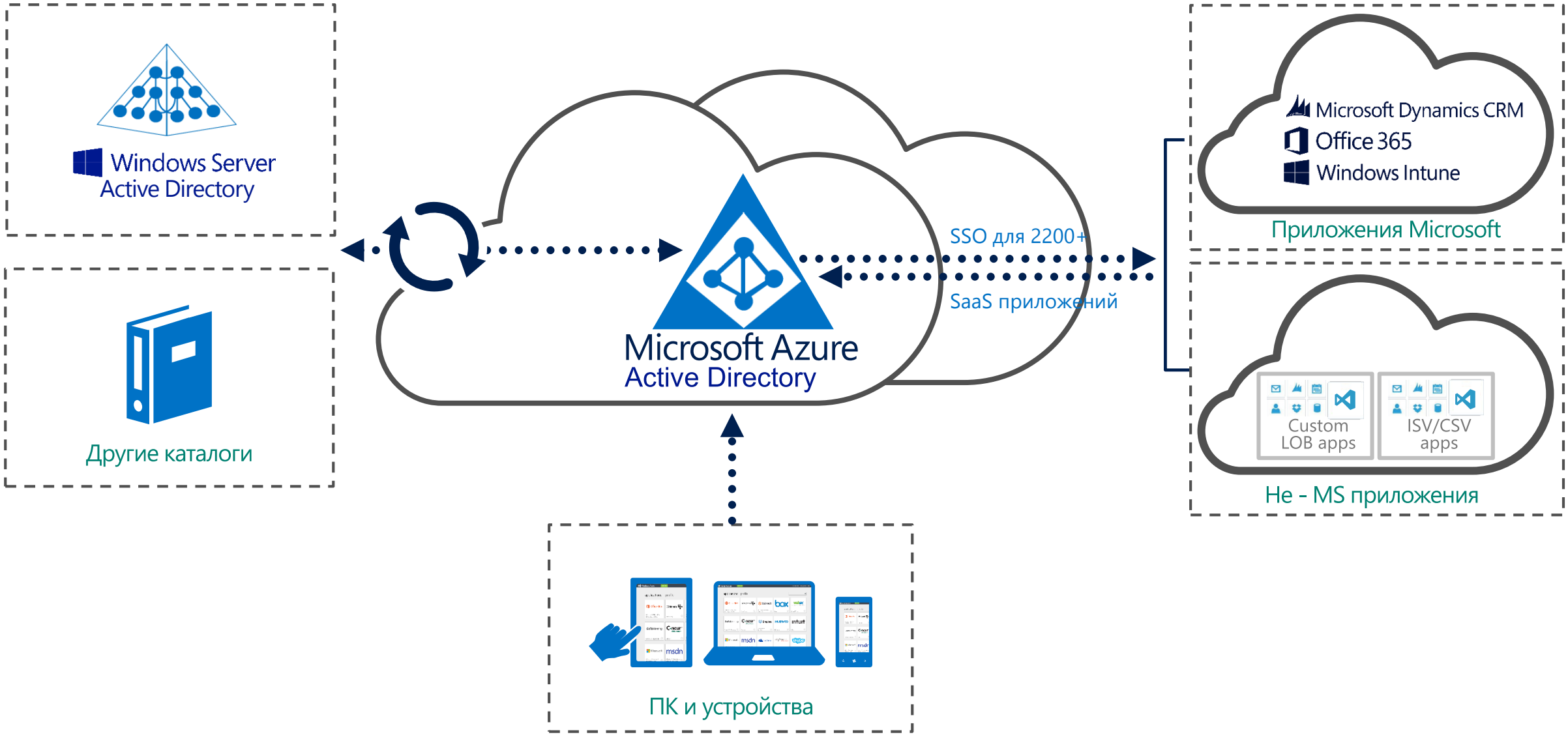
Новые сценарии – новые решения

- Доступ к корпоративным системам через интернет
- Доступ к корпоративным системам для подрядчиков, партнеров, поставщиков и т.д.
- Доступ и работа с данными и документами с мобильных устройств
- Защита данных и документов

Уровни защиты данных

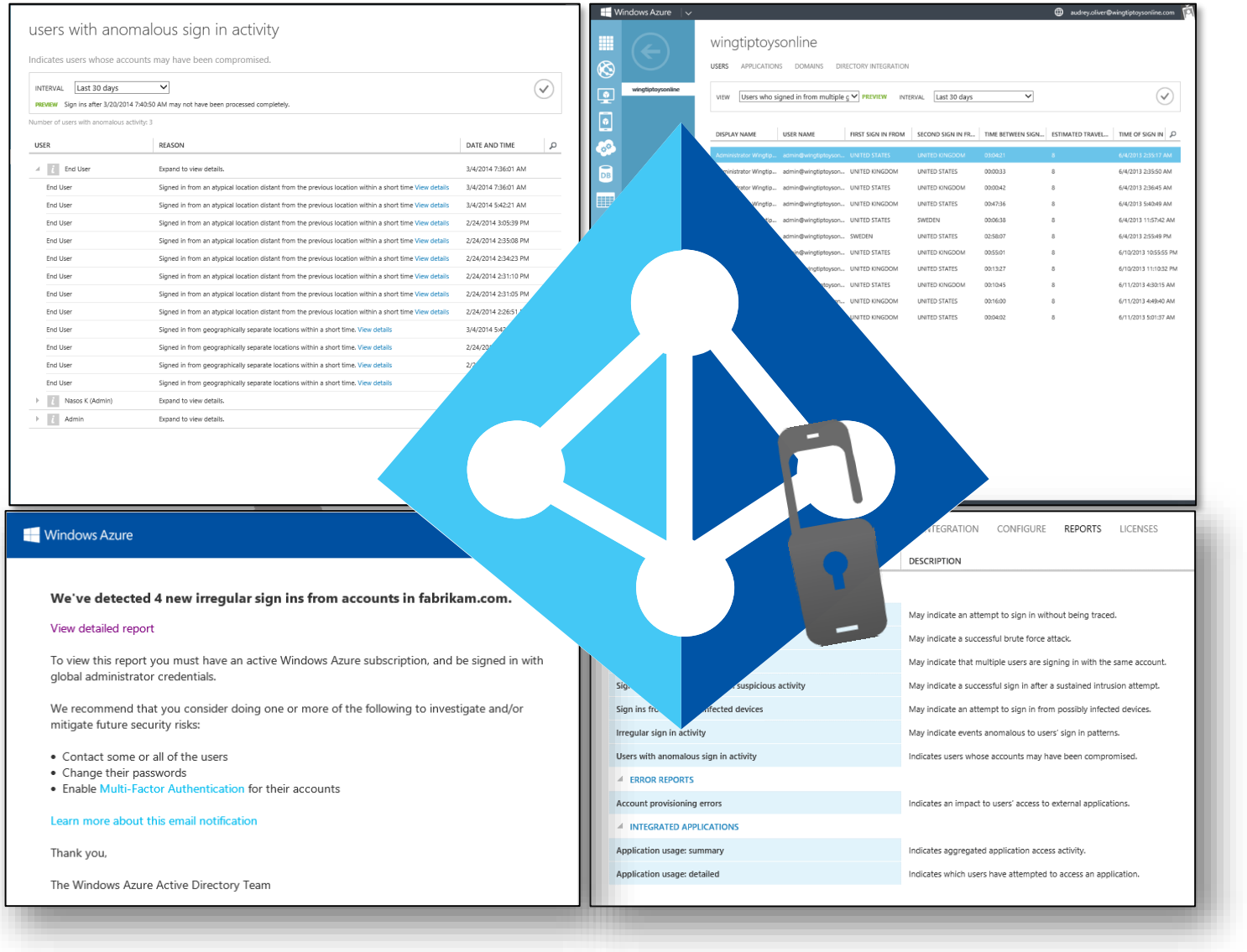


Облачный каталог пользователей

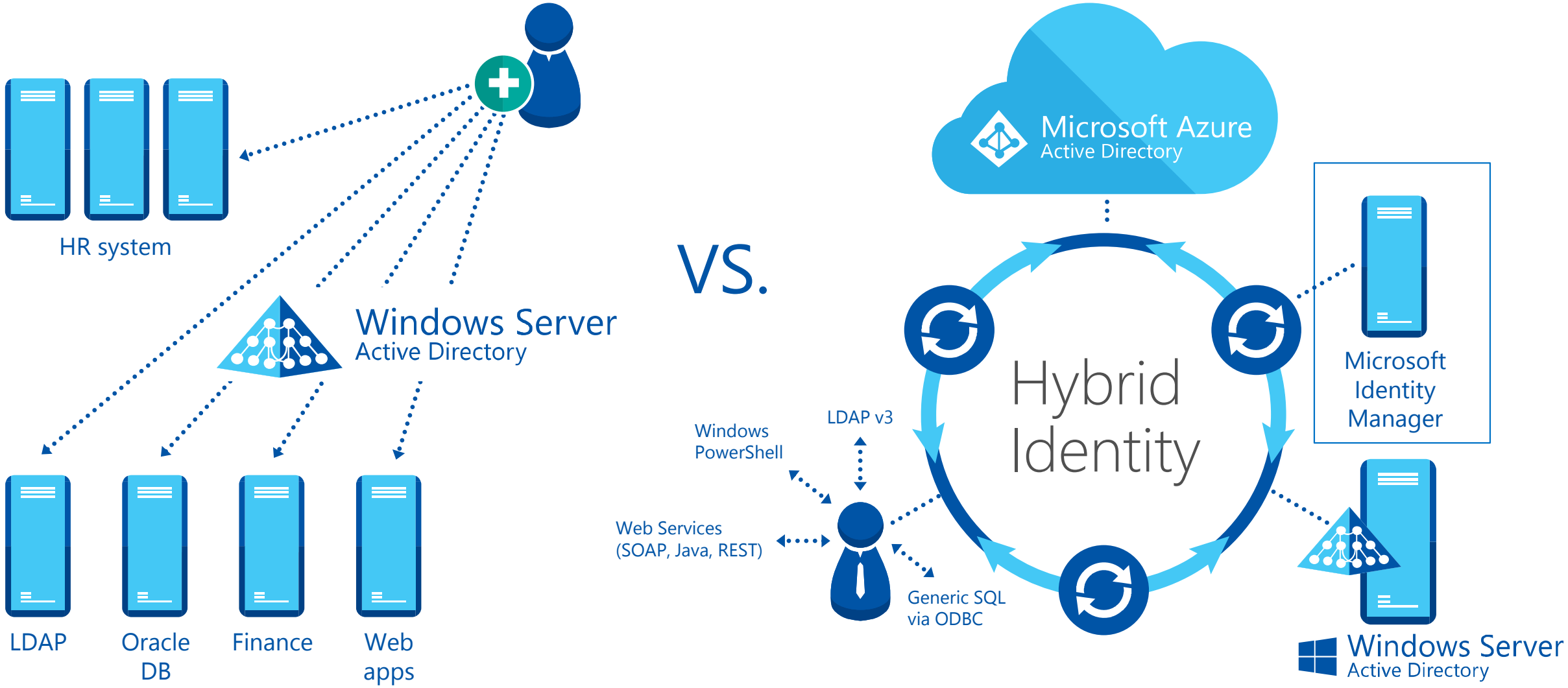


Мониторинг и защита доступа к корпоративным приложениям

Отчеты безопасности, отслеживание подозрительных действий, аналитика и оповещения.



Управление идентификационными данными



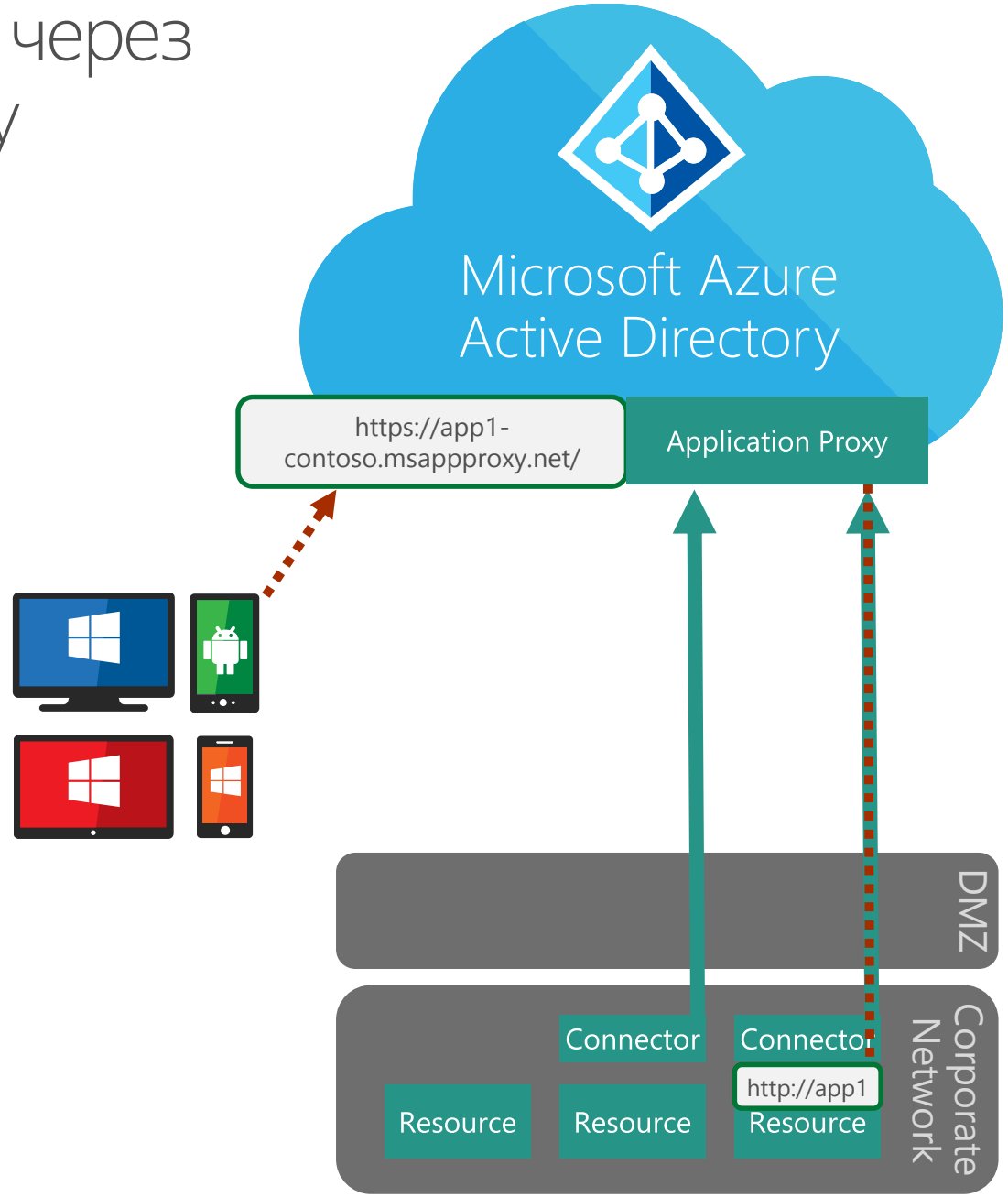
Публикация приложений через Azure AD Application Proxy

Коннектор к облачному сервису

Несколько коннекторов могут быть установлены для отказоустойчивости.

Коннекторы устанавливаются внутри корпоративной сети.

Пользователи подключаются к облачному сервису, которые перенаправляет траффик к приложению

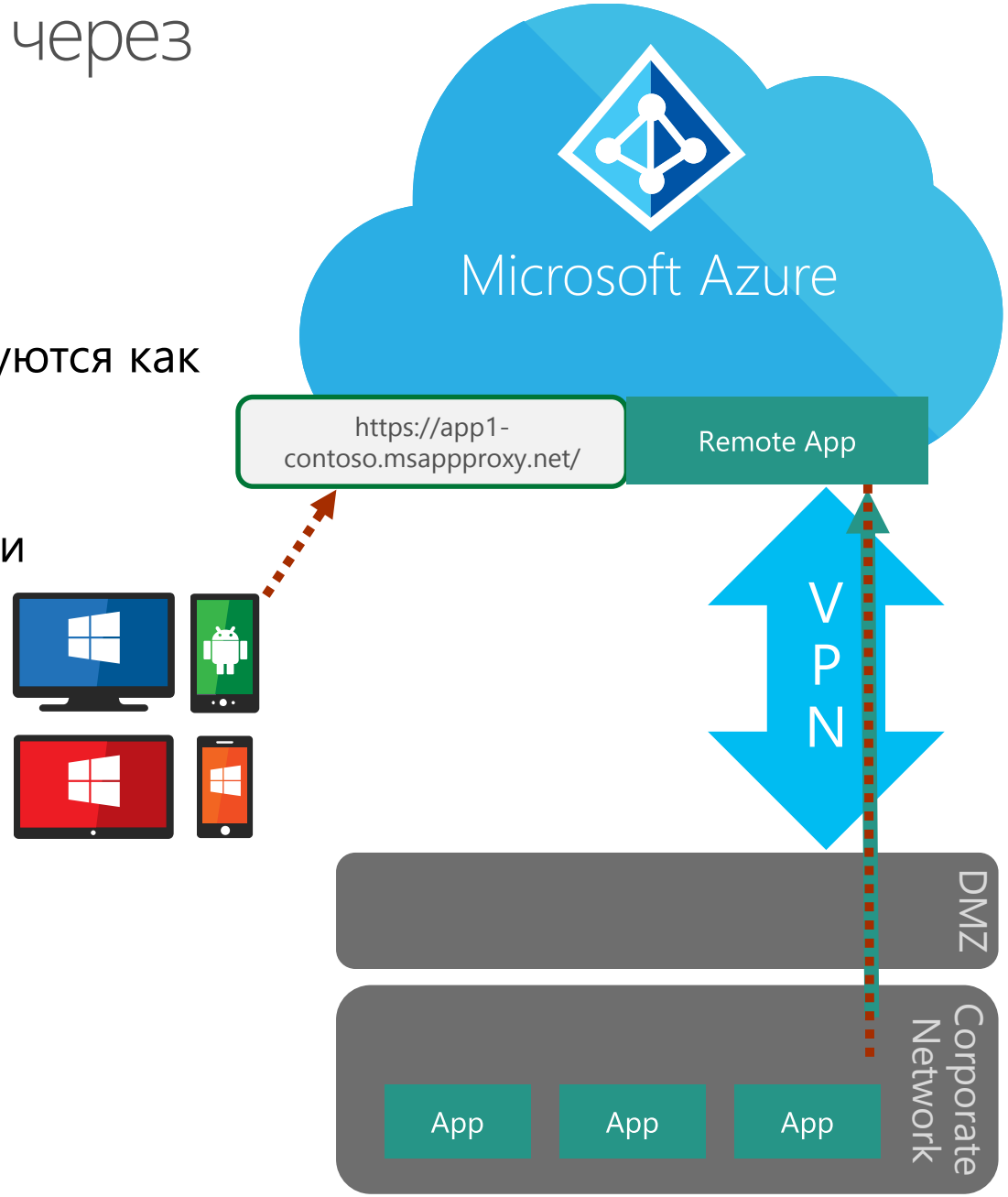


Публикация приложений через Azure Remote App

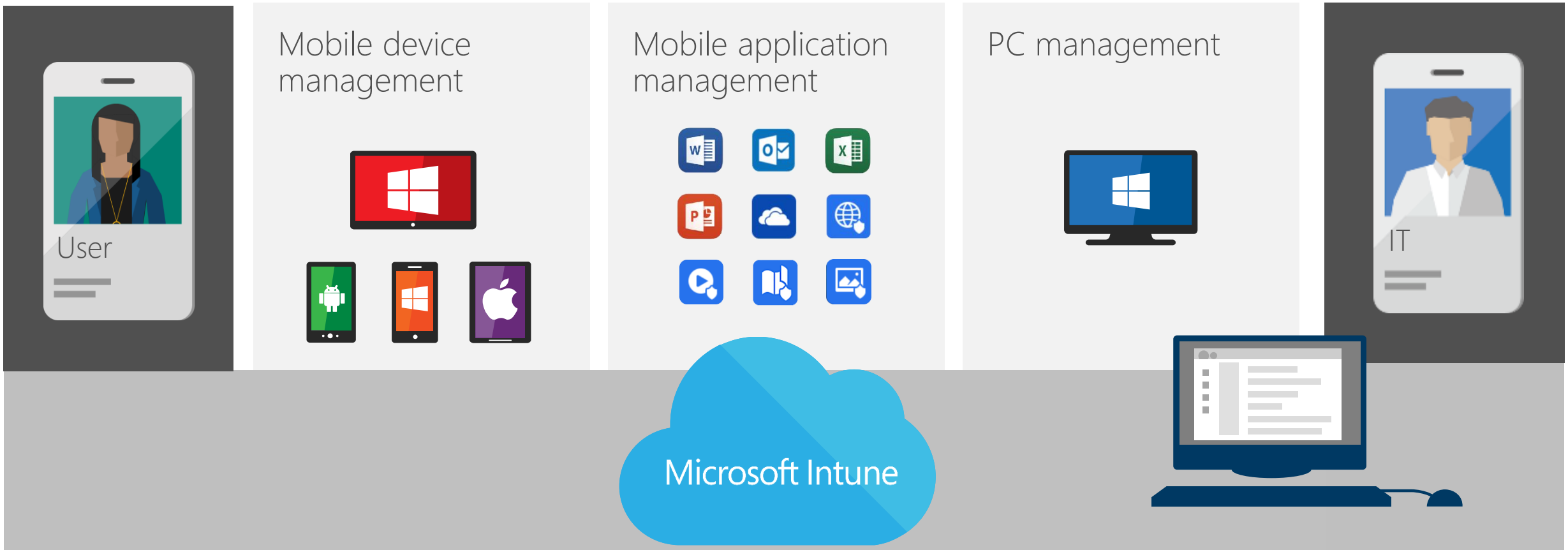
Толстый клиент и сопутствующие драйвера публикуются как Remote App приложение.

Пользователь использует RDP протокол для старта и работы с приложением.

Толстый клиент или приложение подключается к корпоративной сети через VPN.

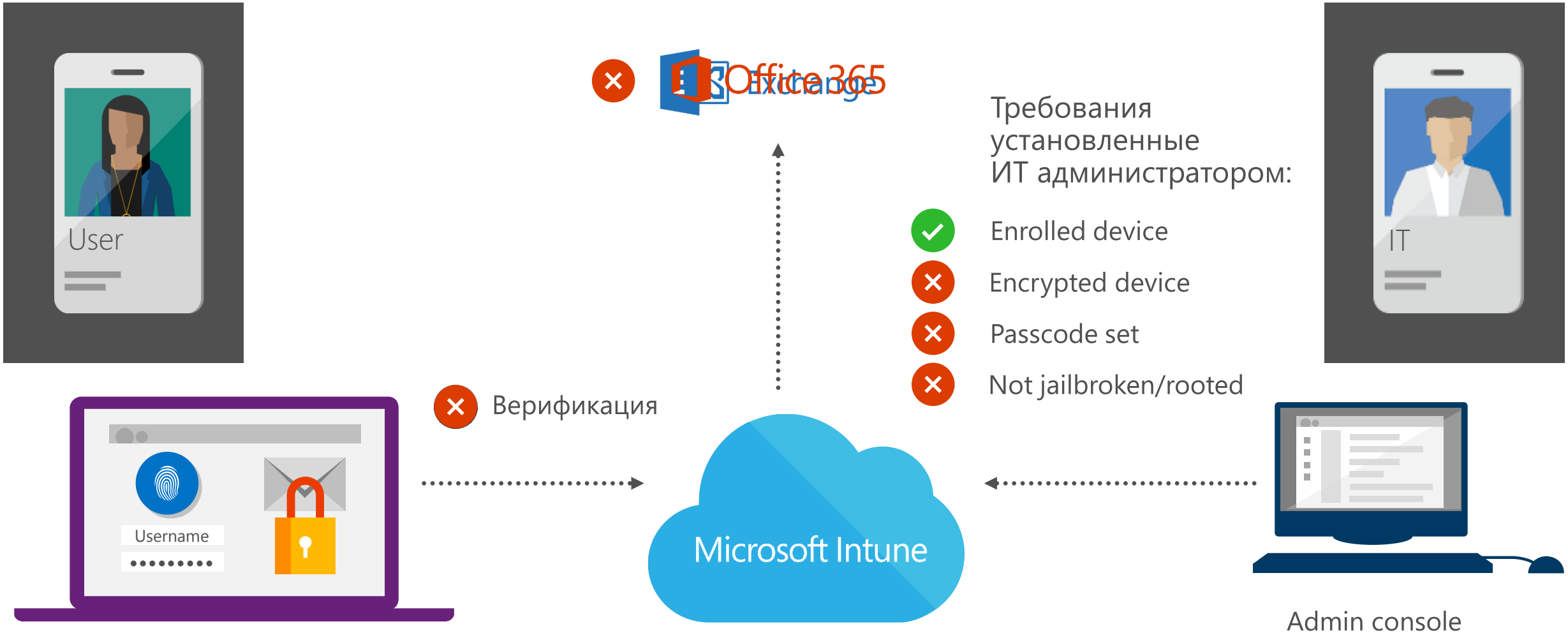


Enterprise mobility management with Intune

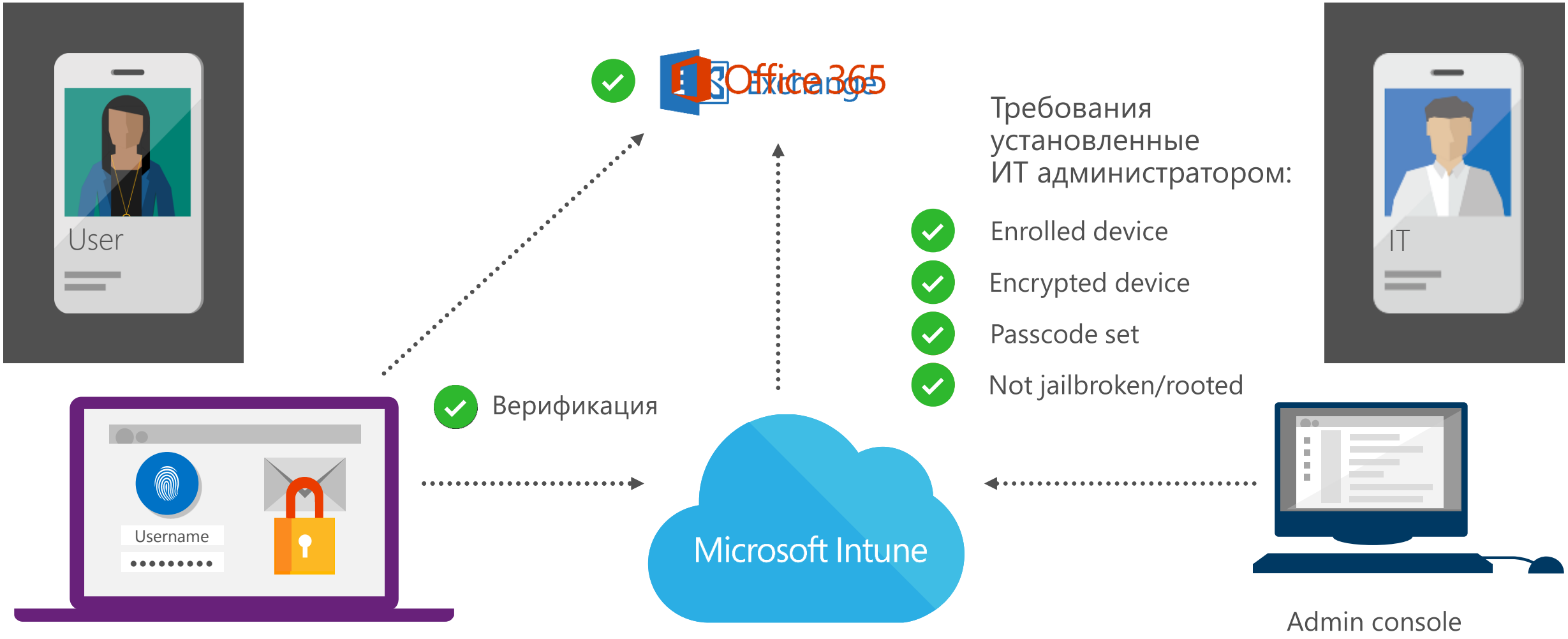


Intune помогает организациям обеспечить сотрудников доступом к корпоративным сервисам, приложениям и данным через сеть Интернет, и при этом обеспечить информационную безопасность

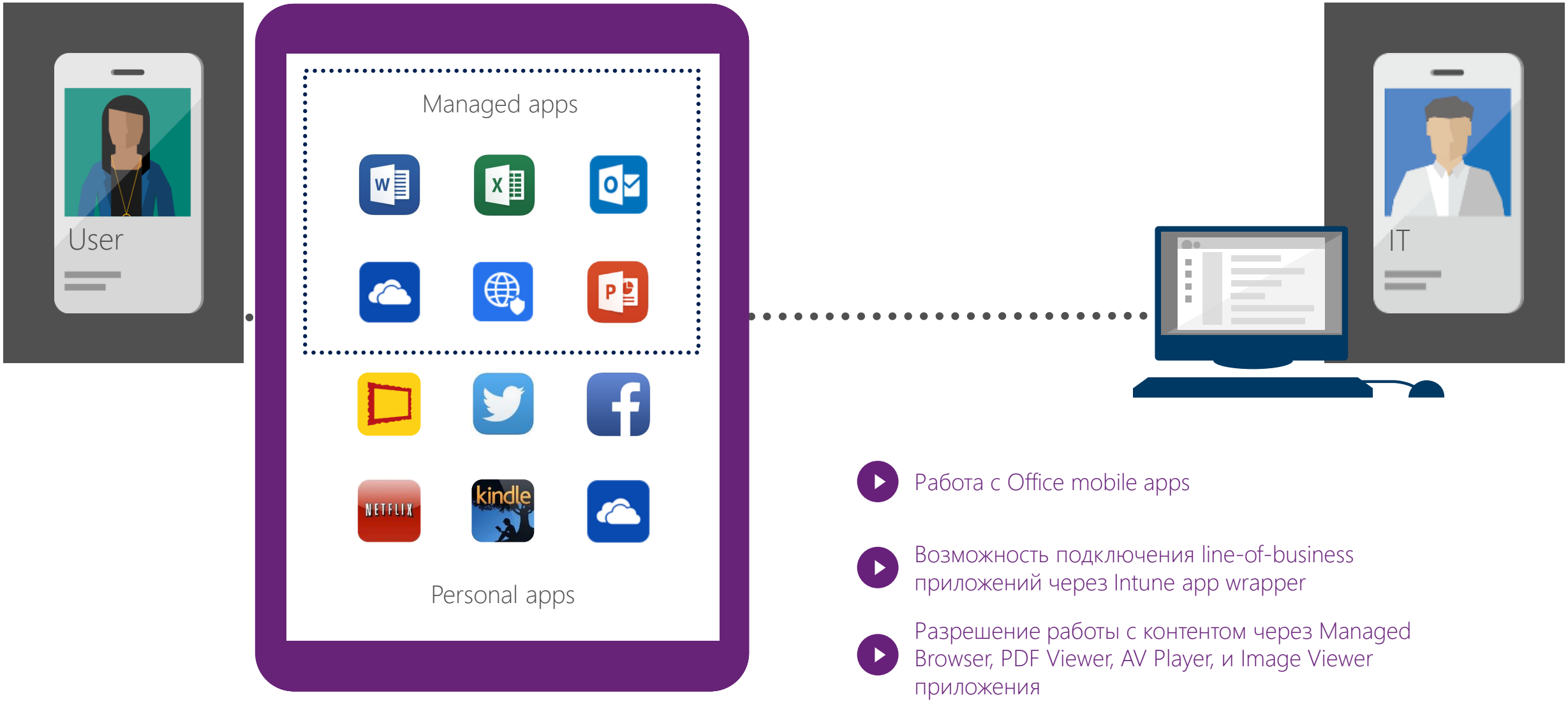
Условный доступ к почте



Условный доступ к почте

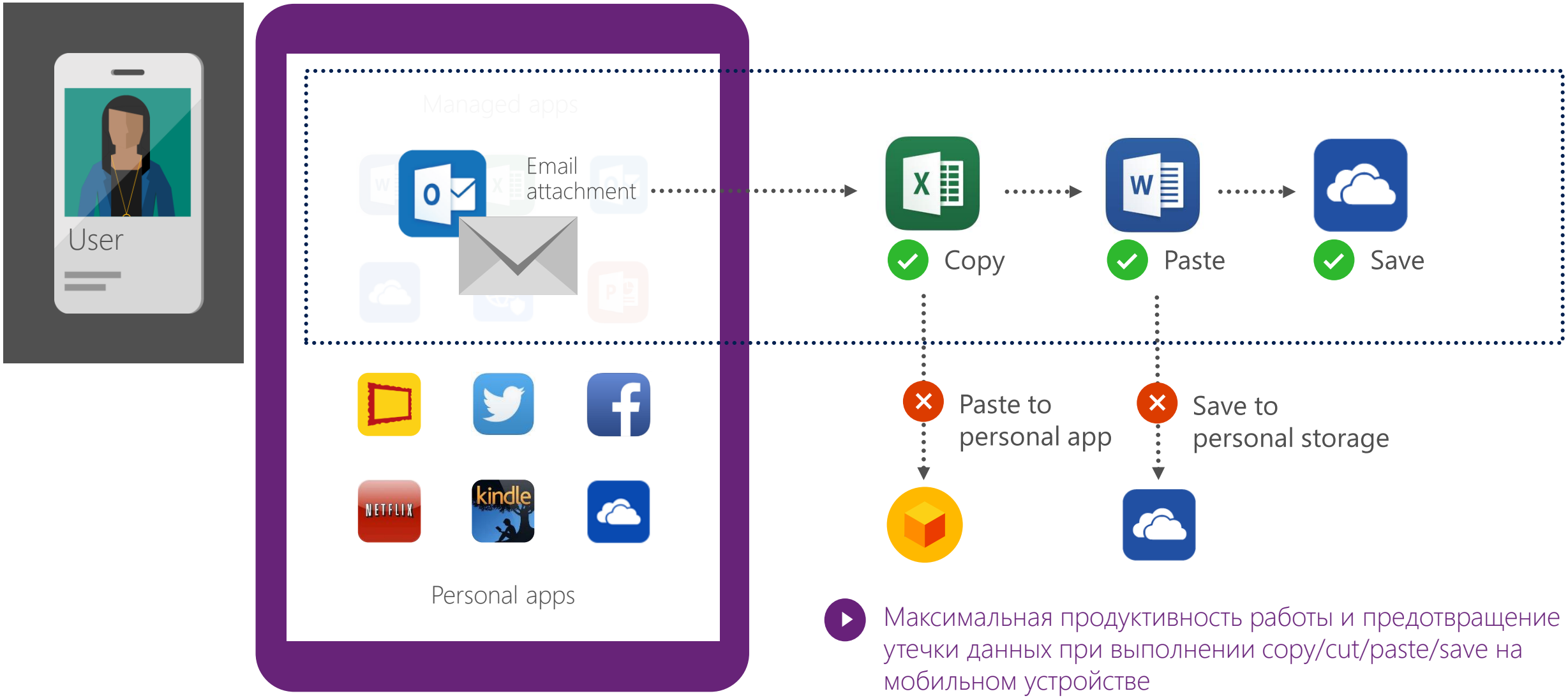


Mobile application management



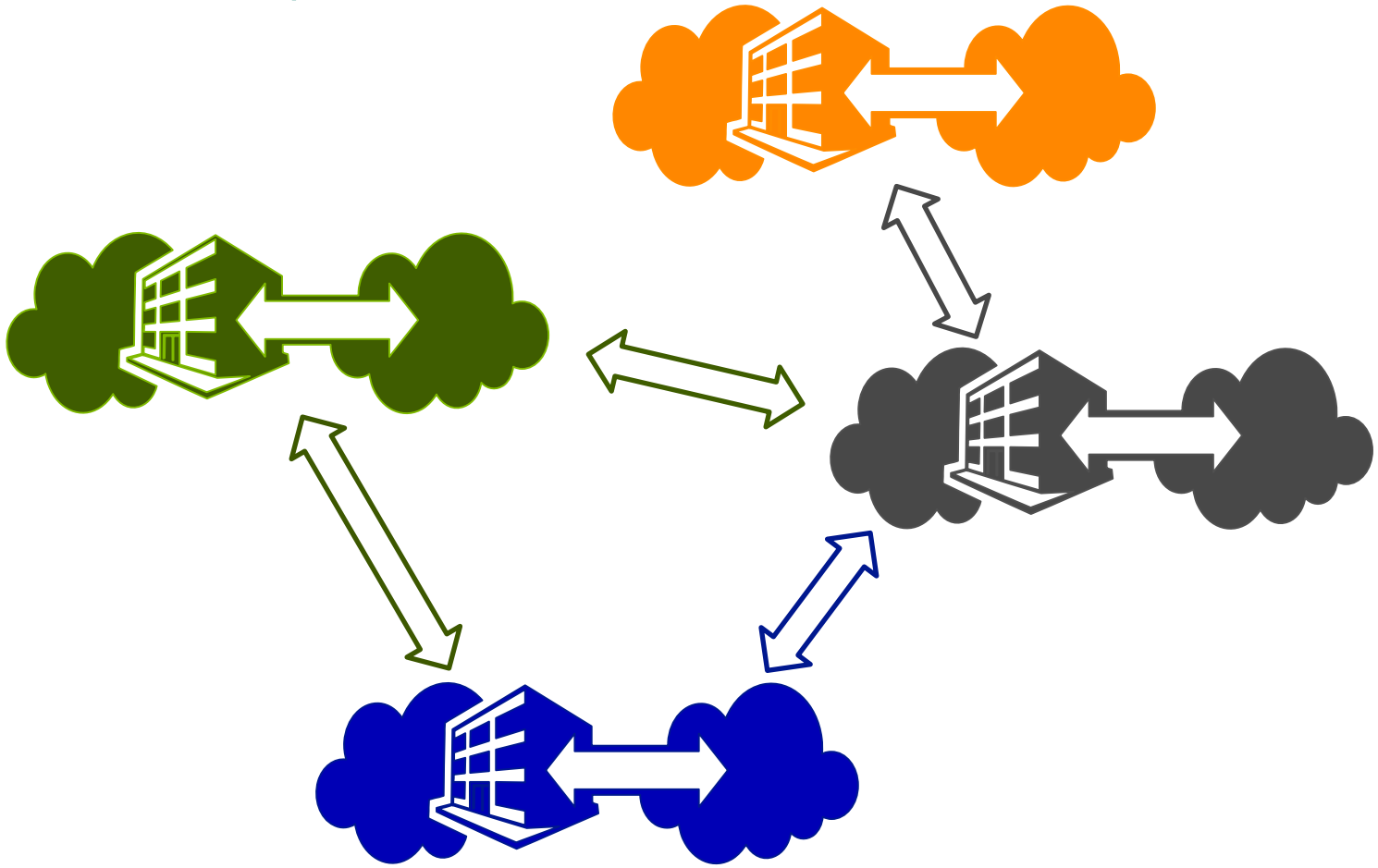
- Работа с Office mobile apps
- Возможность подключения line-of-business приложений через Intune app wrapper
- Разрешение работы с контентом через Managed Browser, PDF Viewer, AV Player, и Image Viewer приложения

Mobile application management



- Максимальная продуктивность работы и предотвращение утечки данных при выполнении copy/cut/paste/save на мобильном устройстве

Azure RMS - Передача защищенных документов между организациями



Обмен данными

Безопасный обмен документами любого типа

Между организациями

Аутентификация пользователей из других организаций (без федерации)

Контроль доступа

Приложения, умеющие работать с шифрованными документами (Office или PDF readers) обеспечивают выполнение прав доступа.

Грустная статистика

243

Среднее количество дней, которые атакующие находятся внутри сети до обнаружения

76%

всех сетевых вторжений происходят посредством взломанных учетных данных пользователей

$500B

Полный потенциальный ущерб киберпреступности в общемировом масштабе

$3.5M

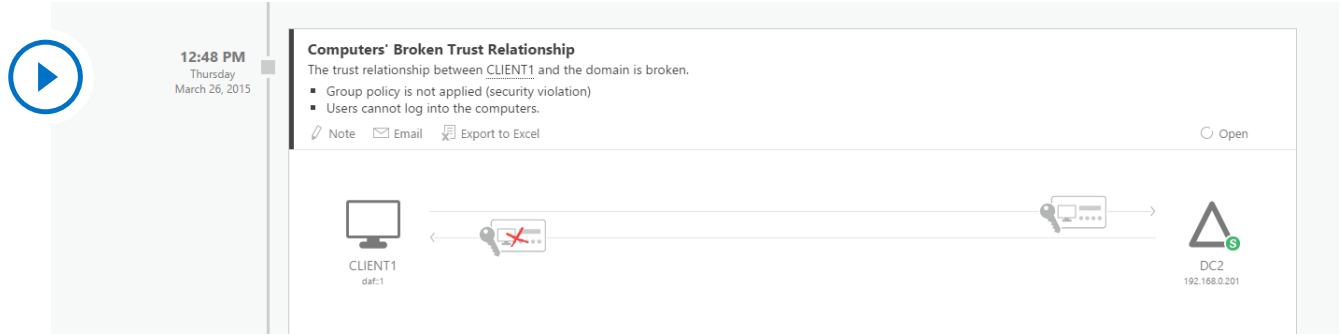
Средний ущерб от взлома для компании

Частота и продуманность атак возрастают постоянно.

Microsoft Advanced Threat Analytics

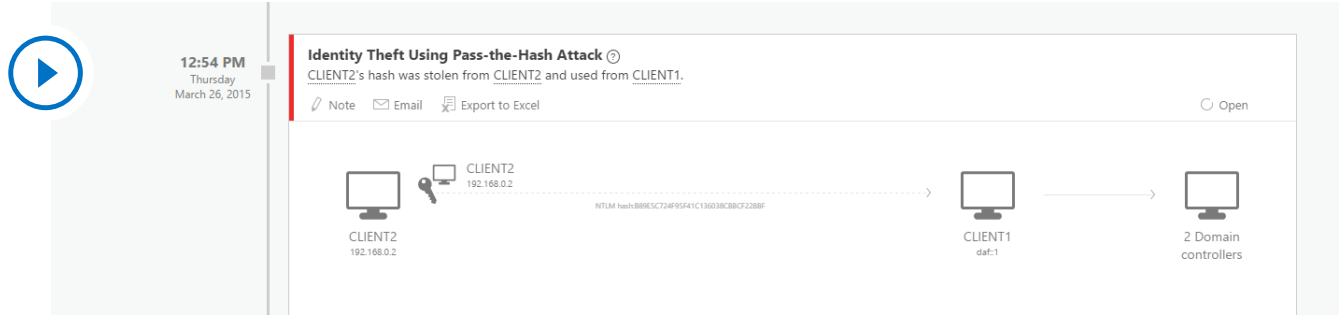
Проблемы и риски безопасности

- Разрушенные трасты
- Слабые протоколы
- Известные уязвимости протоколов



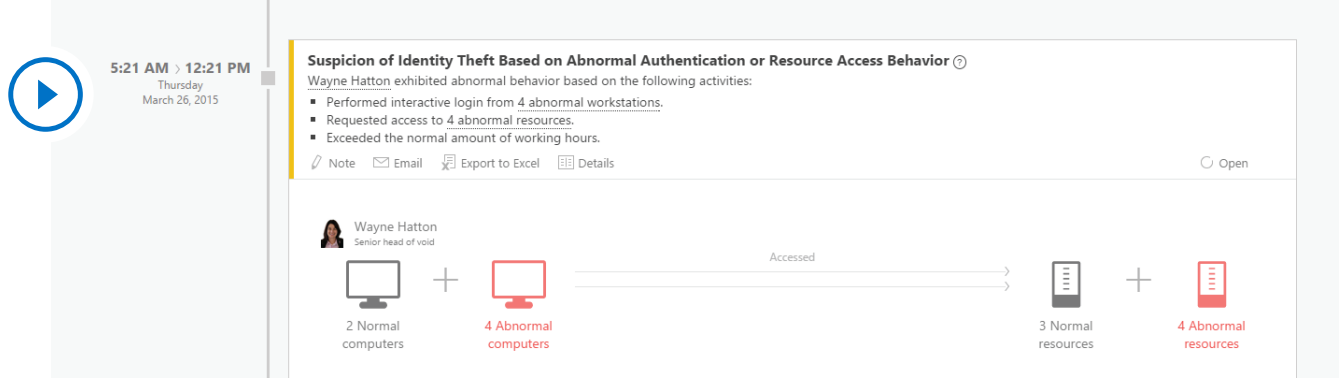
Злонамеренные атаки

- Pass-the-Ticket (PtT)
- Pass-the-Hash (PtH)
- Overpass-the-Hash
- Forged PAC (MS14-068)
- Golden Ticket
- Skeleton key malware
- Reconnaissance
- BruteForce



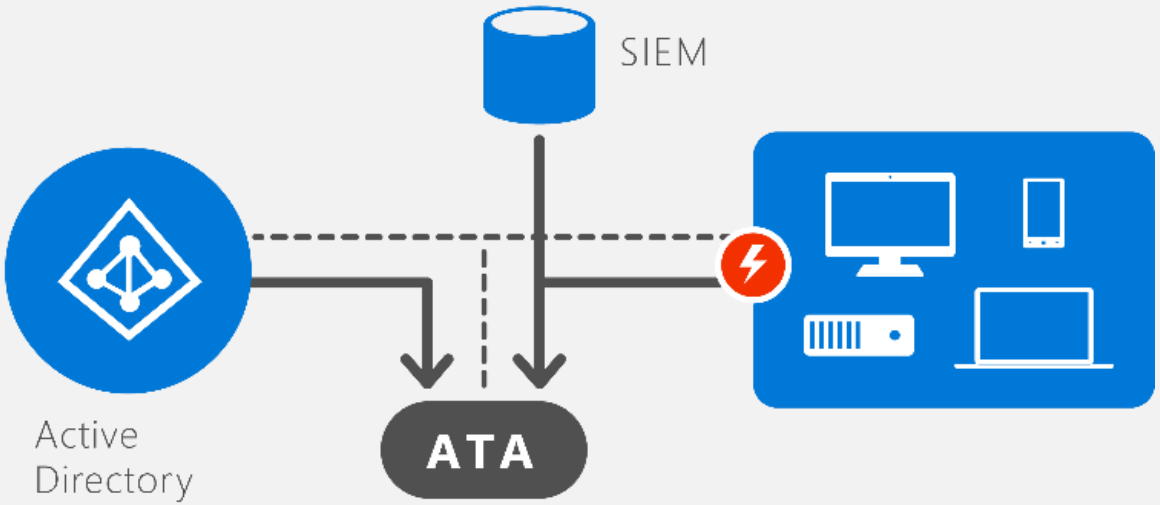
Нестандартное поведение

- Anomalous logins
- Remote execution
- Suspicious activity
- Unknown threats
- Password sharing
- Lateral movement



Как работает Microsoft Advanced Threat Analytics

1 Анализ

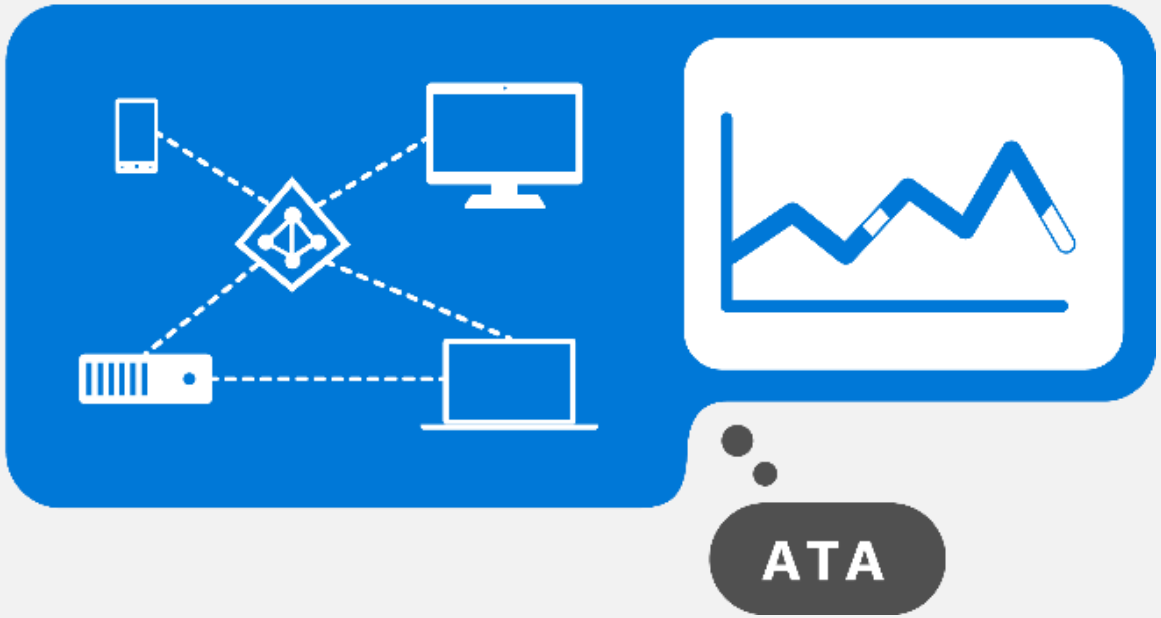


После инсталляции:

- Получение копии данных трафика AD посредством port mirroring
- Остается невидимым для злоумышленников
- Анализирует весь трафик Active Directory
- Собирает сообщения SIEM и других источников

Как работает Microsoft Advanced Threat Analytics

2 Изучение



ATA:

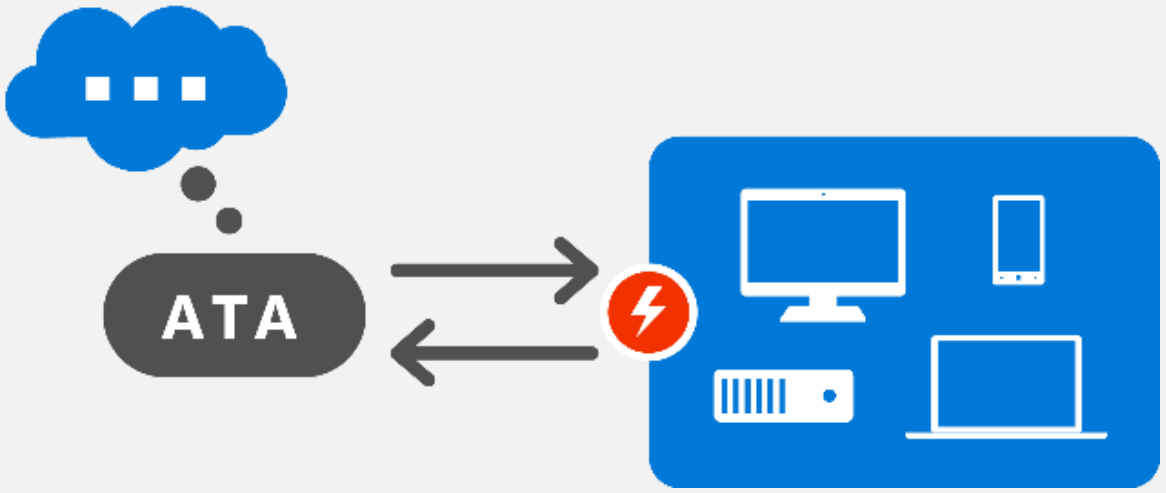
- Автоматически начинает изучать и профилировать поведение пользователей
- Идентифицирует нормальное поведение
- Постоянно обучается для обновления шаблонов поведения пользователей и устройств

What is entity?

Entity represents users, devices, or resources

Как работает Microsoft Advanced Threat Analytics

3 Обнаружение



Microsoft Advanced Threat Analytics:

- Отслеживает нестандартные и подозрительные запросы и действия
- Выдает оповещение если действия выпадают из шаблона поведения данного пользователя или ресурса
- Использует наработки информационной безопасности для обнаружения атак и проблем в защите

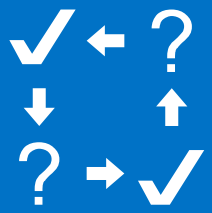
ATA не только сравнивает поведение ресурса с самим собой, но и с другими, принадлежащими к этой группе.

Как работает Microsoft Advanced Threat Analytics

4 Оповещение

ATA рапортует о всех подозрительных активностях в виде новостной ленты

ATA определяет
- Кто?
- Что?
- Когда?
- Как?



Для каждого случая, ATA предлагает рекомендации для проведения расследования и исправления.

Microsoft Advanced Threat Analytics Preview

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

Microsoft

Filter by [?]

- All [16]
- Open [15]
  - High [4]
  - Medium [7]
  - Low [4]
- Resolved [1]
- Dismissed [0]

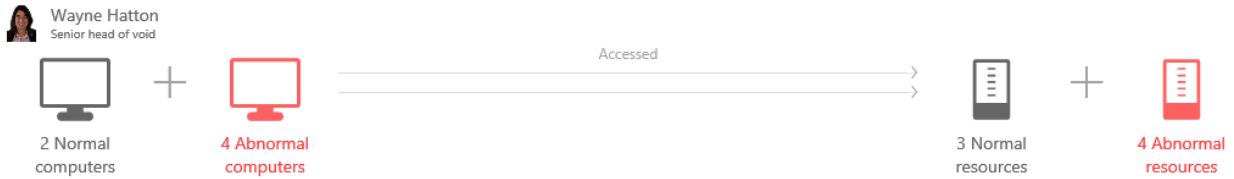
5:21 AM › 12:21 PM
Thursday
March 26, 2015

Suspicion of Identity Theft Based on Abnormal Authentication or Resource Access Behavior

Wayne Hatton exhibited abnormal behavior based on the following activities:

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

Note | Email | Export to Excel | Details | Open



Recommendations

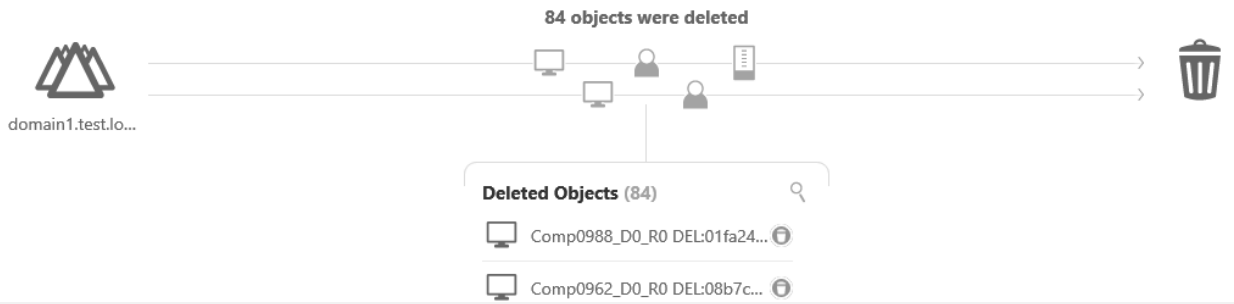
- Disconnect the relevant computers from the network or move them into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more
- Contact Wayne Hatton and investigate if the user has logged in to abnormal computers and accessed abnormal resources.

11:22 AM
Thursday
March 26, 2015

Massive Object Deletion

84 objects (5.36% of total AD objects) were deleted over a period of a few seconds from domain domain1.test.local.

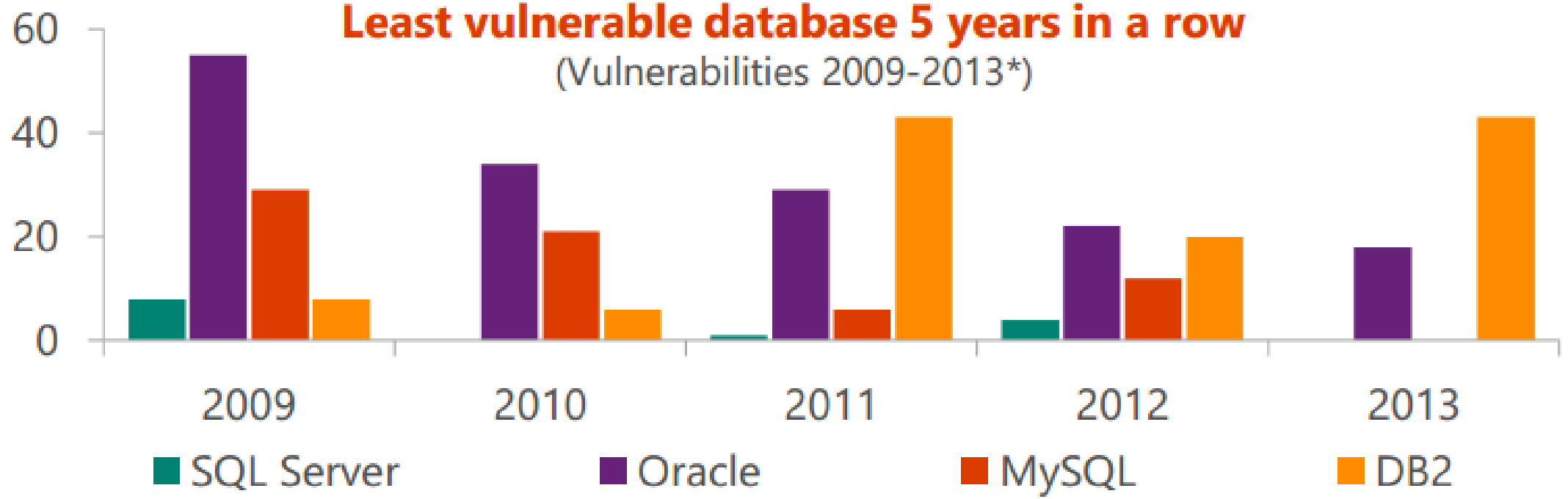
Note | Email | Export to Excel | Open



- Suspicion of Identity Theft Based on Abnormal Authentication or Resource Access Behavior — 7 days ago
- Services Exposing Account Credentials — 7 days ago
- Identity Theft Using Pass-the-Ticket Attack — 7 days ago
- Identity Theft Using Pass-the-Hash Attack — 7 days ago
- Identity Theft Using Pass-the-Hash Attack — 7 days ago
- Sensitive Account Credentials Exposed — 7 days ago
- Honeytoken Activity — 7 days ago
- Reconnaissance Using DNS — 7 days ago
- Reconnaissance Using DNS — 7 days ago
- Computers' Broken Trust Relationship — 7 days ago
- Brute Force Attack Using LDAP Simple Bind — 7 days ago

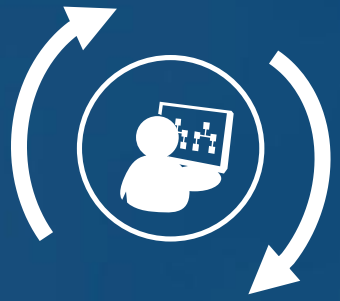
SQL Server Security

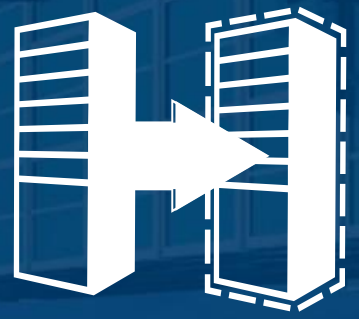
Enhanced Security & Scalability
Least vulnerable 5 years in a row



*National Institute of Standards and Technology Comprehensive Vulnerability Database 4/17/2013

Operation Management Suite – управление облачным и наземным датацентром





Лог аналитика	Автоматизация	Доступность	Безопасность
Анализ и отчет по состоянию систем в облаке и на земле	Автоматизация сложных повторяющихся операций	Решения класса Disaster Recovery	Состояние защищенности серверов и рабочих станций

Microsoft

Дополнительная информация

- Microsoft Enterprise Mobility http://www.microsoft.com/en-us/server-cloud/enterprise-mobility/products.aspx
- Больше информации о Microsoft Advanced Threat Analytics:
  - www.microsoft.com/ata
- Триальная версия ATA:
  - www.microsoft.com/en-us/evalcenter/evaluate-microsoft-advanced-threat-analytics
- Microsoft Operations Management Suite:
  - http://www.microsoft.com/en-us/server-cloud/operations-management-suite/overview.aspx
- Если Вас заинтересовали решения по безопасности или есть вопросы, напишите на адрес itssua@microsoft.com

itssua@microsoft.com

Microsoft Cloud Compliance Certifications and Attestations – as of 1/15/15

Regulatory and Compliance Domain	Office 365	Microsoft Dynamics CRM	Microsoft Azure	Microsoft Intune	Yammer
CJIS	Yes	No	Yes	No	No
EU Model Clauses	Yes	Yes	Yes	Yes	No
EU Safe Harbor	Yes	Yes	Yes	Yes	Yes
FedRAMP (Moderate)	Yes	No	Yes	No	No
FERPA	Yes	Yes	Yes	N/A	Yes
HIPAA BAA	Yes	Yes	Yes	Yes	No
US Government Cloud	Yes	Yes	Yes	No	No
UK G-Cloud (OFFICIAL)	Yes	Yes	Yes	No	No
ISO 27001:2013 (w/ISO 27018:2014	Yes	Yes	Yes	Yes	Yes ISO 27001:2005
PCI DSS Level 1	N/A	N/A	Yes	N/A	N/A
SOC 1 Type 2 (SSAE 16 / ISAE 3402)	Yes	Yes	Yes	Yes	No
SOC 2 Type 2 (AT Section 101)	Yes	No	Yes	Yes	No