Microsoft

infosolution

Microsoft Security

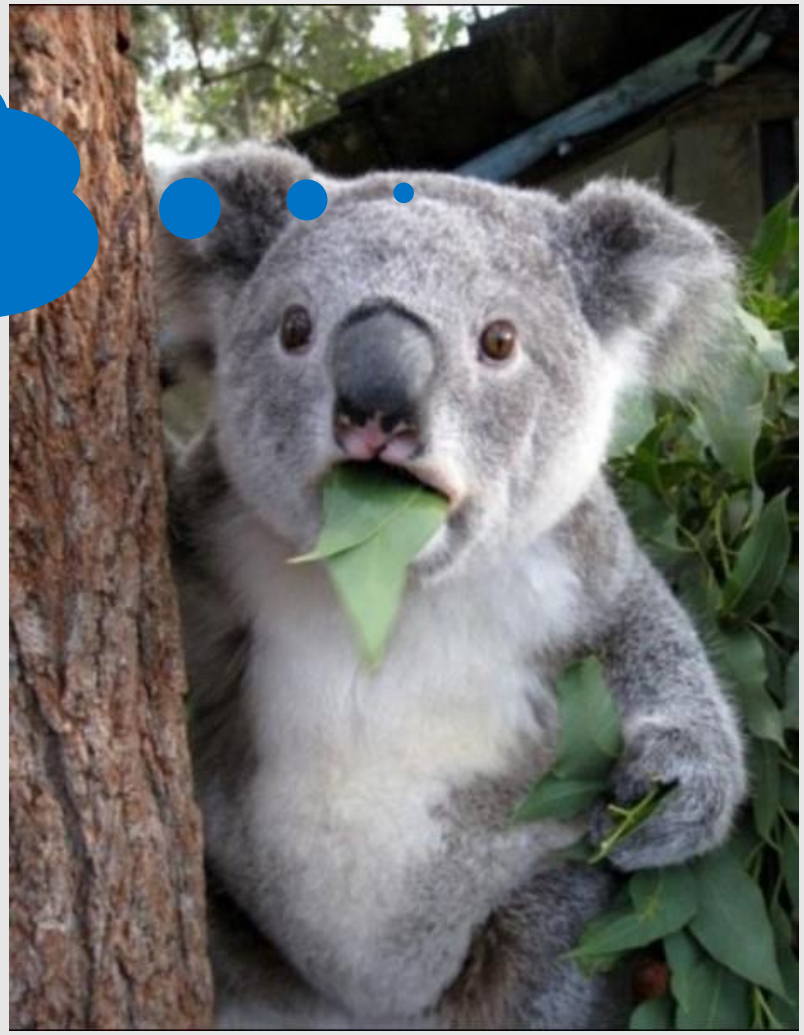
INFOSOLUTION LLC
IT Manager, Zolboo

Товч


5 сая
5 сая ам долларын үнийн дүн бүхий жилийн борлуулалт
Вендортой албан ёсны түнш
35
15,000
Улсын хэмжээнд нийт нийлүүлсэн лиценз хэрэглэгчдийн тоо
Нийт ажилчид
8
6
Монгол дахь албан ёсны Дистрибютор
Олон улсын Дистрибютор компаниудын албан ёсны түншлэл
20

Microsoft

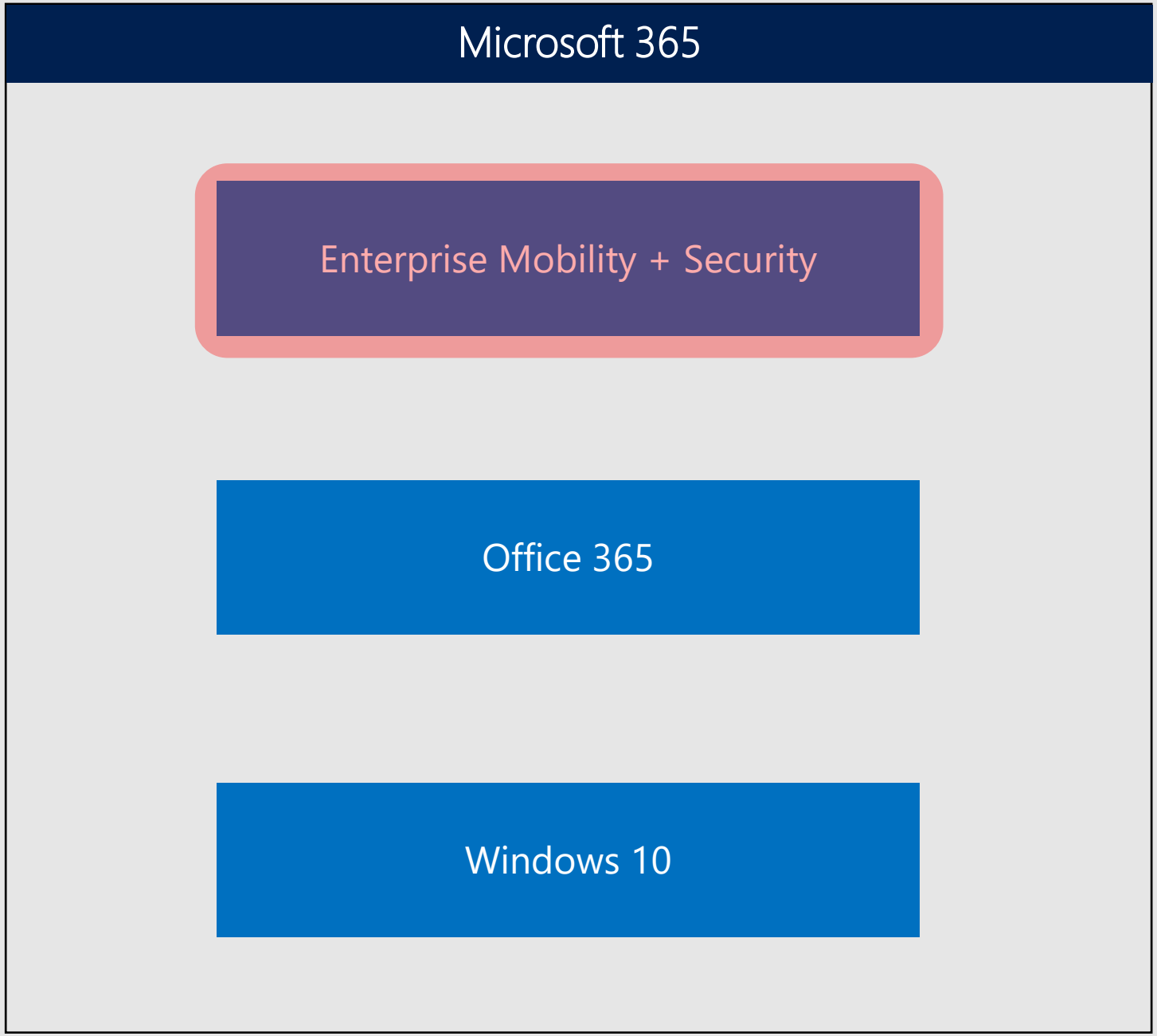
Microsoft Cloud Security Features



infosolution

Microsoft Security ?


Microsoft 365
Enterprise Mobility + Security
Office 365
Windows 10


Microsoft 365
Enterprise Mobility + Security
Office 365
Windows 10

Identity & access management

Protect users' identities & control access to valuable resources based on user risk level

- Azure Active Directory
- Conditional Access
- Windows Hello
- Windows Credential Guard

Threat protection

Protect against advanced threats and recover quickly when attacked

- Advanced Threat Analytics
- Windows Defender Advanced Threat Protection
- Office 365 Advanced Threat Protection
- Office 365 Threat Intelligence

Information protection

Ensure documents and emails are seen only by authorized people

- Azure Information Protection
- Office 365 Data Loss Prevention
- Windows Information Protection
- Microsoft Cloud App Security
- Office 365 Advanced Security Management
- Microsoft Intune

Security management

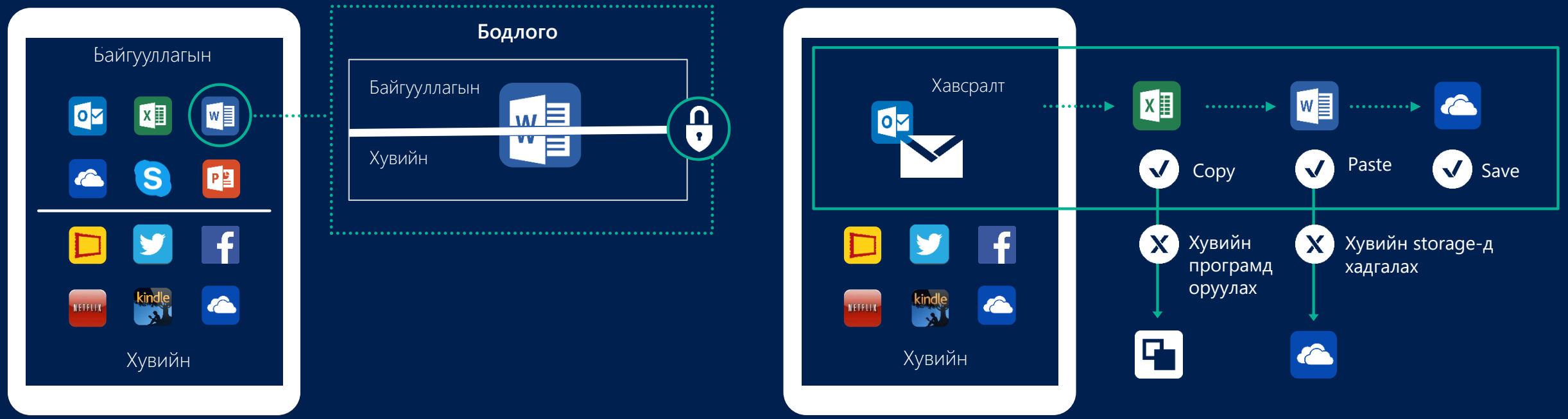
Gain visibility and control over security tools

- Azure Security Center
- Office 365 Security Center
- Windows Defender
- Security Center

Control data on Mobile Devices

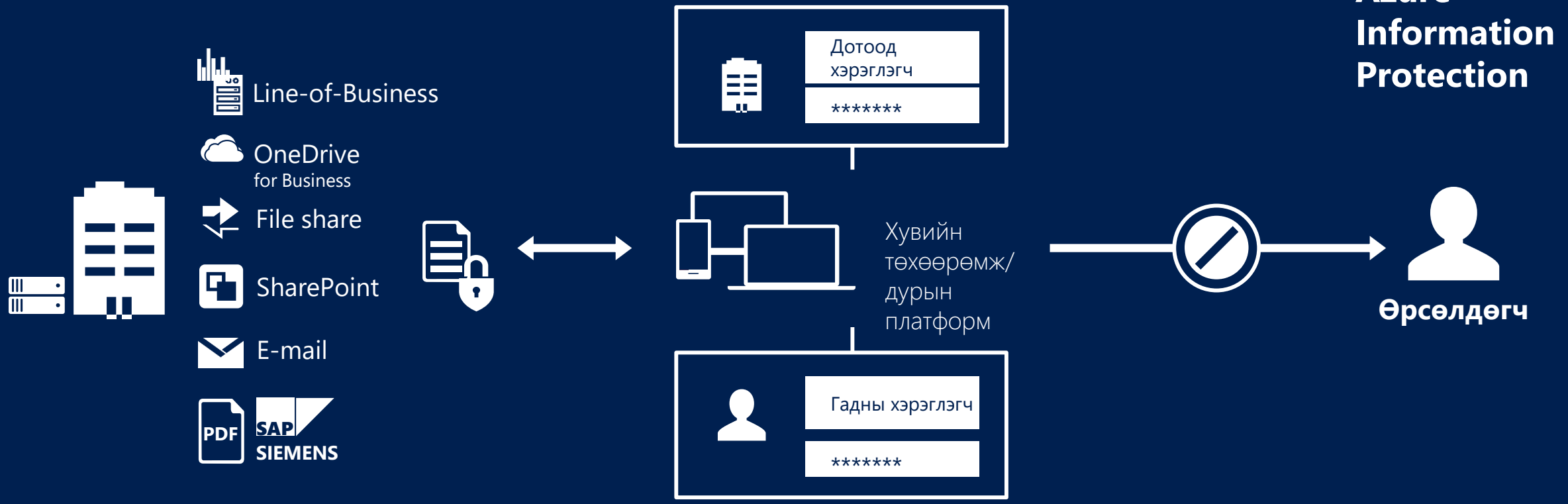
Манай байгууллагын ажилчдын mobile device –ууд дээрх байгууллагын өгөгдлийг хамгаалах шаардлагатай

Intune



Protect and Share Information

Миний эсвэл байгууллагын нууц мэдээлэл өрсөлдөгчдөд маань хүрэхгүй гэдэгт итгэлтэй байх ёстой.



Analyze and Classify Data

Бид байгууллагынхаа ямар өгөгдлийг хамгаалах ёстойгоо тодорхойлох ёстой.

Azure Information Protection

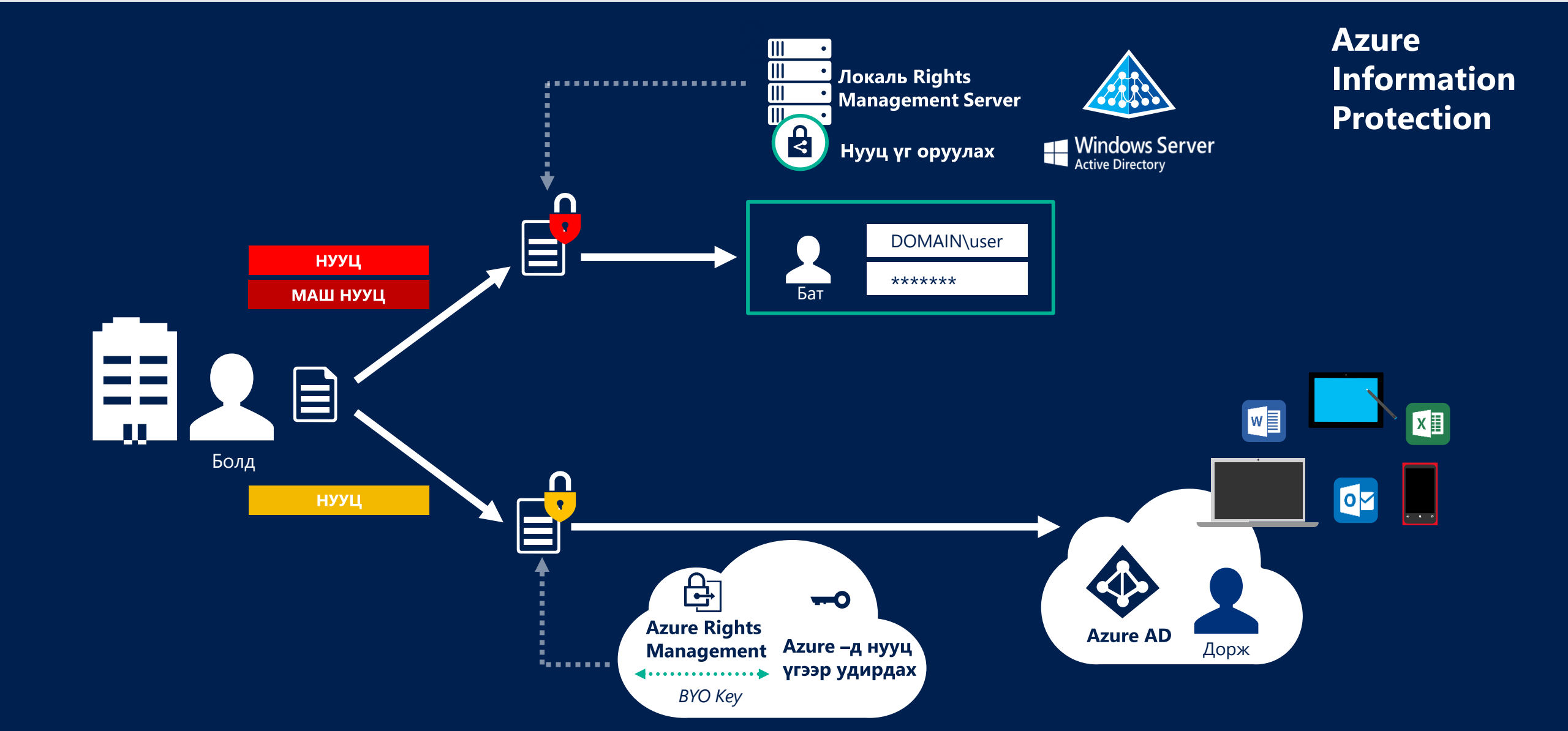
Та өгөгдлийг автоматаар ангилж, хамгаалах дүрмийг үүсгэж болно.

Хэрэглэгчийн ажиллаж буй агуулгаас/контентоос хамааран ангиллын зөвлөмжийг өгч болно.

Хэрэглэгчид мэдээллийн ангиллыг өөрчилж болох бөгөөд өөрчилсөн үндэслэлийг заавал өгөх шаардлагатай.

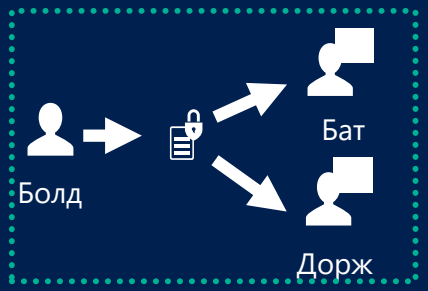
Хэрэглэгчид өөрийн ажиллаж буй имэйл болон файлдаа 1 даралт/click –аар нууцын зэрэглэлийг тодорхойлох боломжтой.

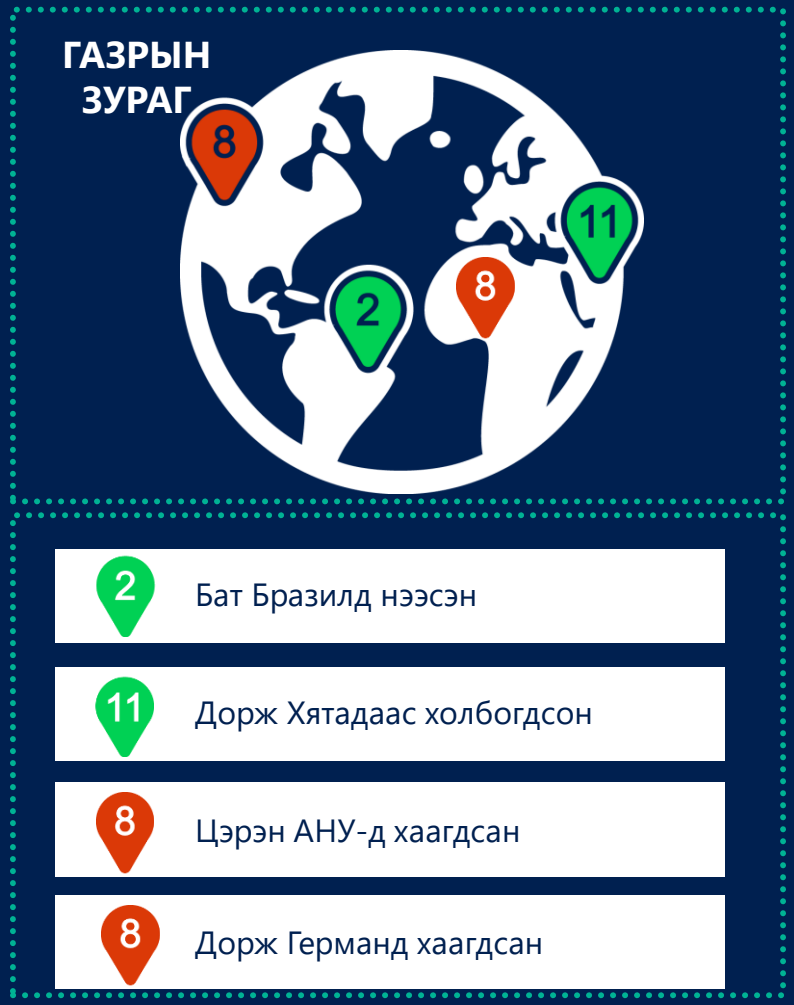
Document Protection by Category (RMS-Hybrid)



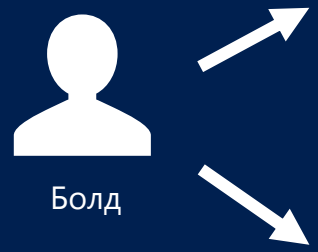
Monitoring and Action

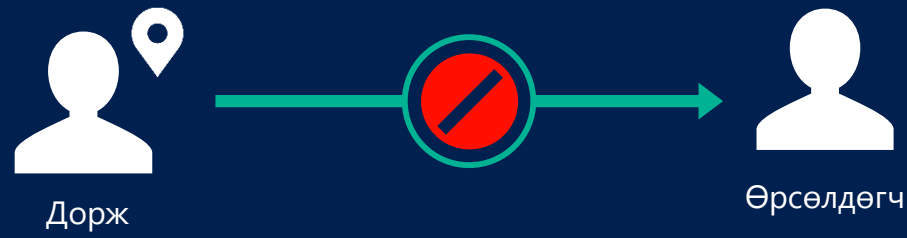
Хэрэглээг хянах, удирдах, хаах боломж





Azure Information Protection





Доржын эрхийг хаасан

Identify and Control Shadow IT

Хэрэглэгчдийн ашигладаг Cloud хэрэглээний талаар надад тодорхой байдал, хяналт хэрэгтэй байна

Cloud App Security

DETECTION

Agent суулгалгүйгээр хэрэглэгчлийн хэрэглээний талаар маш тодорхой мэдээллийг авна.

DATA CONTROL

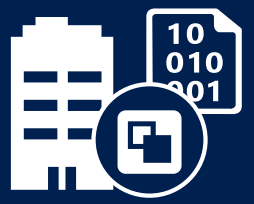
Хандах эрх, мэдээлэл солилцох болон DLP хяналт бүхий өөрийн Cloud орчинг үүсгэх

PROTECTION

Өндөр эрсдэлтэй хэрэглээ ба аюулгүй байдлын тохиолдлыг тодорхойлох, хэвийн бус хэрэглэгчийн зан авирыг тодорхойлох, аюул заналхийллээс урьдчилан сэргийлэх

Identify Attack

On-Premise Detection



Microsoft Advanced Threat Analytics (ATA)

- Behavioral analysis
- Identify known malicious attacks
- Identify unknown security incidents

Cloud Detection

Azure Advanced Threat Protection + Cloud App Security + Azure AD Premium

- Behavioral analysis
- Anomaly Detection
- Security reporting and monitoring

User OS Protection

Windows Defender Advanced Threat Protection

Агент Windows 10 суулгагдсан
Нэмэлт суурилуулалт эсвэл дэд бүтцийн өөрчлөлт шаардагддаггүй.

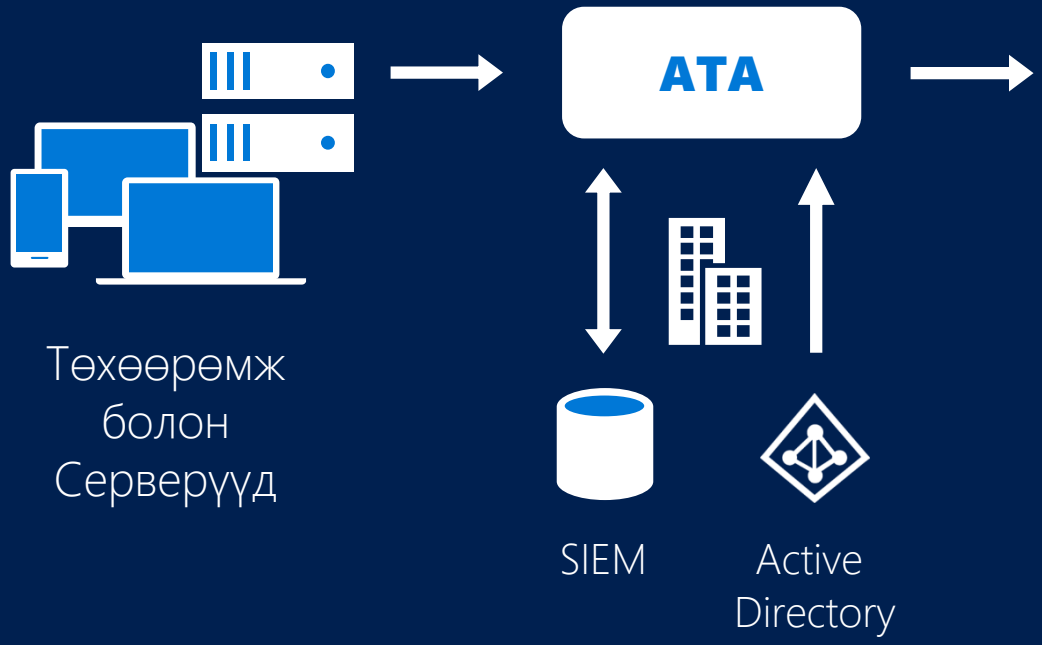
Cloud –д суурилсан эмзэг байдлын дүн шинжилгээ
Төрөл бүрийн хүчин зүйлүүдтэй уялдаатай мэдэгдэж буй болон үл мэдэгдэх аюулын тухай анхааруулга. Үйл ажиллагааны болон түүхэн мэдээлэл.

Урт хугацаанд шинжилсэн
Эмзэг байдлын цар хүрээг дүрслэн харуулах. Төрөл бүрийн төгсгөлийн өгөгдлийн хураангуй. Файл болон URL-уудын нарийвчилсан дүн шинжилгээ.

Халдлагын талаар Unique болон ухаалаг мэдлэгийн баазтай
Халдагчдын талаар мэдээлэл авахын тулд аюул заналхийллийг хянах.
Microsoft –ийн болон third-party програмын аюулын анализ.

Server Infrastructure Protection

Advanced Threat Analytics



Behavior analysis

(Хэвийн бус байдлыг мэдээлэх)

Analysis of known attacks and problems

(Жишээ: LDAP Simple Bind, DNS Reconnaissance)

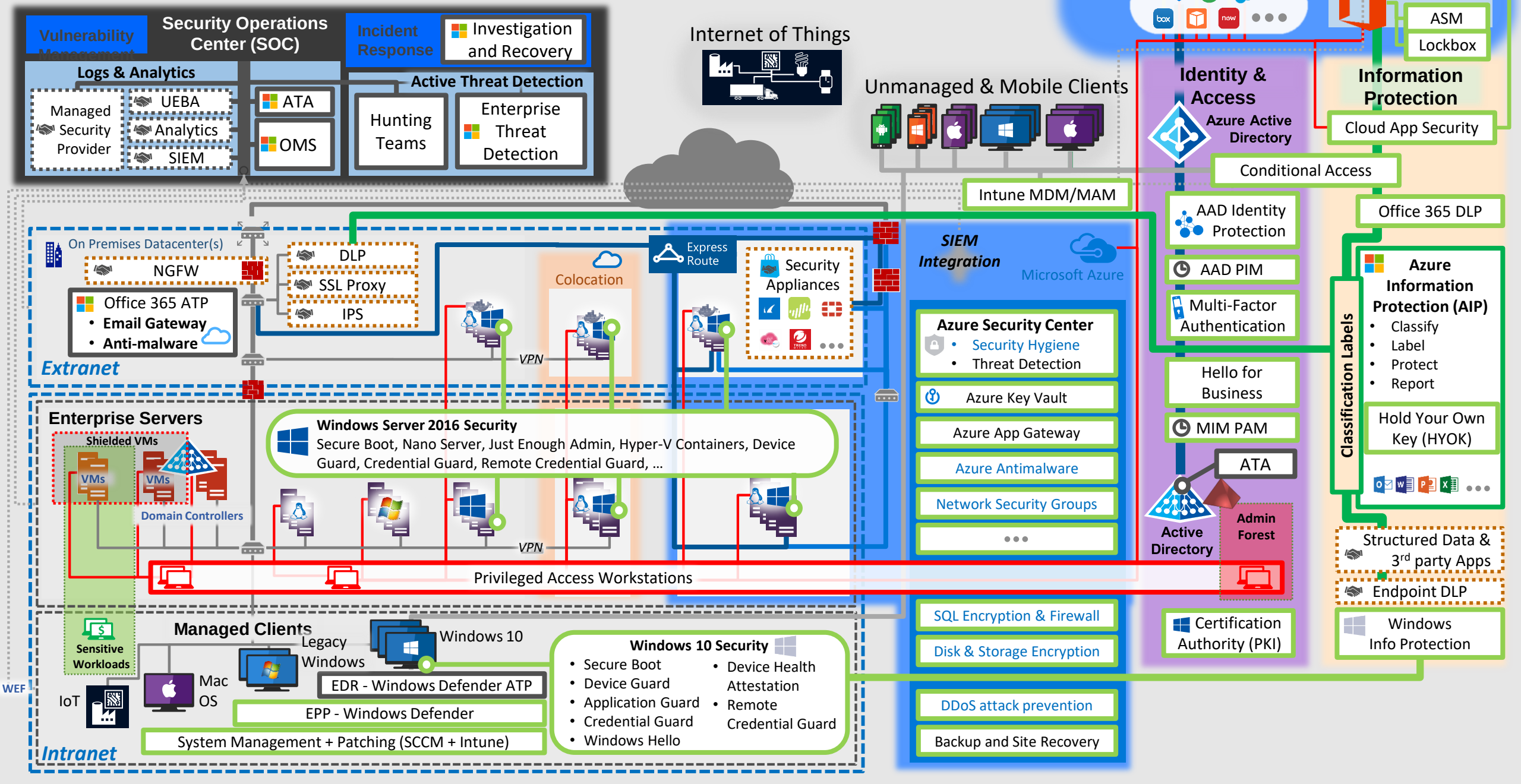
Advanced Threat Analytics

Аюулгүй байдлын талаар баялаг мэдлэгийн сан

Figure 1. Magic Quadrant for Endpoint Protection Platforms

Reference Architecture - Cybersecurity

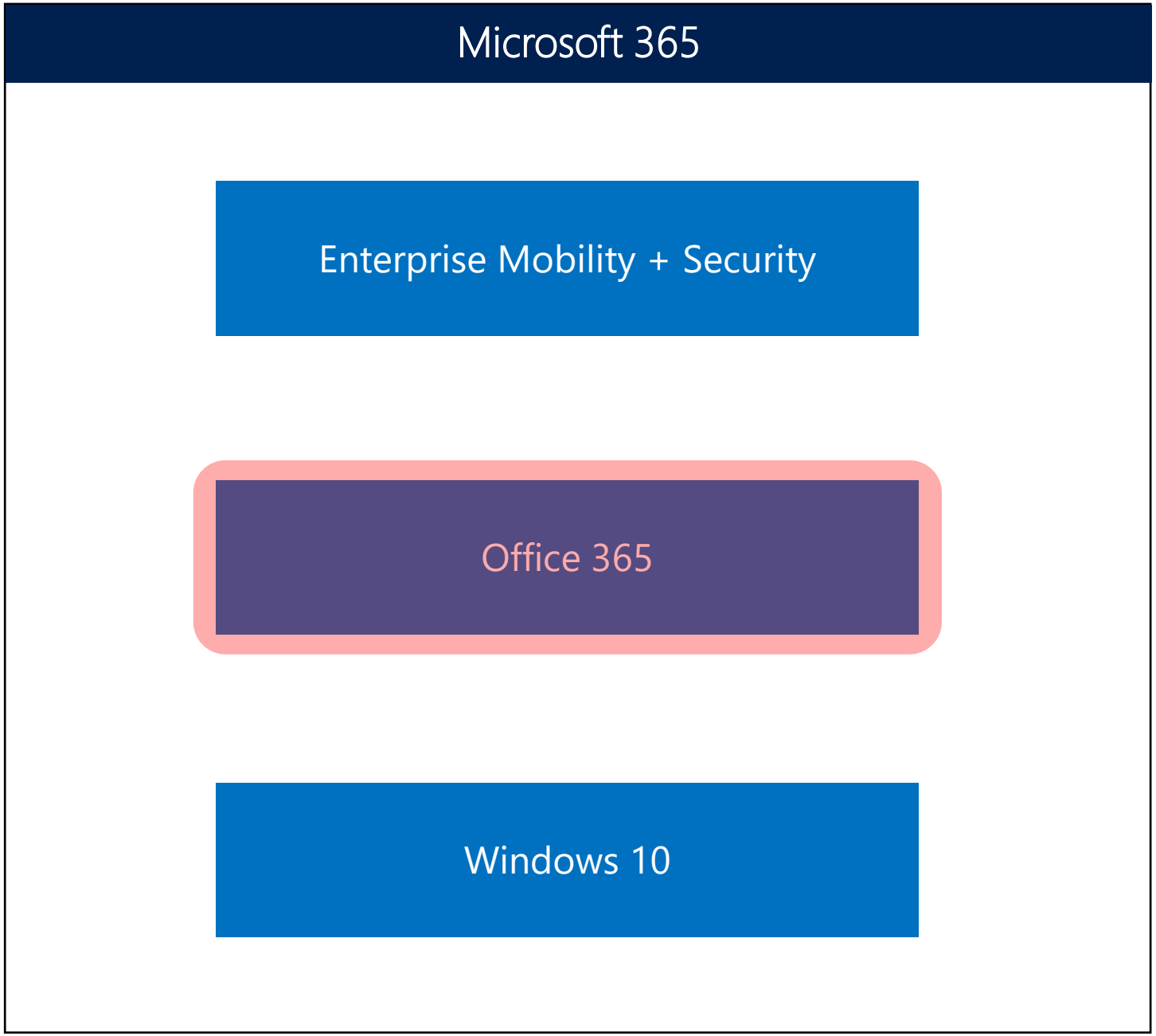
Microsoft



Microsoft

infosolution

БАЯРЛАЛАА...


Microsoft 365
Enterprise Mobility + Security
Office 365
Windows 10

Azure Active Directory

	Office 365	Azure AD Premium
Directory as a service (no object limit)	• for Office 365 user accounts only	• No limit
User and group management	•	•
Single sign-on for pre-integrated SaaS and custom applications	• 10 apps per user**	• No limit
Security/usage reports	• Basic	• Advanced
Self-service password reset for cloud users	•	•
Company branding (logon pages/access panel customization)	•	•
Application proxy	•	•
SLA 99.9%	•	•
Self-Service Group and app Management/Self-Service application additions/ Dynamic Groups	•	•
Self-service password reset/change/unlock with write-back to on-premises directories	•	•
Multi-Factor Authentication (cloud and on-premises (MFA server))	• Limited cloud-only for Office 365 Apps	•
MDM auto-enrollment, Self-service BitLocker recovery, additional local administrators to Windows 10 devices via Azure AD Join, Enterprise State Roaming	•	•
Group-based access management/provisioning		•
MIM CAL + MIM Server***		•
Cloud app discovery		•
Connect Health		•
Conditional Access based on group/location/device state		•
Identity Protection		•
Privileged Identity Management		•
Join a Windows 10 device to Azure AD, Desktop SSO, Microsoft Passport for Azure AD, Administrator BitLocker recovery		•

*Default usage quota is 150,000 objects. An object is an entry in the directory service, represented by its unique distinguished name. An example of an object is a user entry used for authentication purposes. If you need to exceed this default quota, please contact . The 500K object limit does not apply for Office 365, Microsoft Intune, or any other Microsoft paid online service that relies on Azure Active Directory for directory services. **With Azure AD Free and Azure AD Basic, end-users are entitled to get single sign-on access for up to 10 applications. ***Microsoft Identity Manager Server software rights are granted with Windows Server licenses (any edition). Since Microsoft Identity Manager runs on Windows Server OS, as long as the server is running a valid, licensed copy of Windows Server, then Microsoft Identity Manager can be installed and used on that server. No other separate license is required for Microsoft Identity Manager Server.

Azure Information Protection

	Azure Information Protection для O365*	Azure Information Protection (EMS)
Protection for Microsoft Exchange Online, Microsoft SharePoint Online, and Microsoft OneDrive for Business content	●	●
Bring Your Own Key (BYOK) for customer-managed key provisioning life cycle[2]	●	●
Custom templates, including departmental templates	●	●
Protection for on-premises Exchange and SharePoint content	●	●
RMS software developer kit for all platforms: Windows, Windows Mobile, iOS, Mac OSX, and Android	●	●
Protection for non-Microsoft Office file formats, including PTXT, PJPG, and PFILE (generic protection)	●**	●
RMS content consumption by using work or school accounts from RMS policy-aware apps and services	●	●
RMS content creation by using work or school accounts	●***	●
Manual document classification and consumption of classified documents		●
Automated data classification and administrative support for automated rule sets		●
Hold Your Own Key (HYOK) that spans Azure RMS and Active Directory RMS for highly regulated scenarios		●
RMS connector with on-premises Windows Server file shares by using the File Classification Infrastructure (FCI) connector		●
Document tracking and revocation		●

*Some Office 365 subscriptions also include data protection using Microsoft Azure RMS. For information on those Office 365 subscriptions and the data protection capabilities they include, refer to Azure Information Protection licensing datasheet. **Azure subscription required to use configured key for Bring Your Own Key (BYOK).
***Currently, you can also use this free subscription to help protect documents and create new email messages with enhanced protection. However, the ability to author new protected content is intended for trial use only and might be removed in the future.

Управление приложениями и устройствами

	Device management feature comparison – REVISED	Exchange ActiveSync	Office 365 MDM	Intune (EMS)
	Cloud-based management for iOS, Android, and Windows Phone.	●	●	●
Device configuration	Inventory mobile devices that access corporate applications	●	●	●
	Remote factory reset (full device wipe)	●	●	●
	Mobile device configuration settings (PIN length, PIN required, lock time, etc.)	●	●	●
	Self-service password reset (Office 365 cloud only users)	●	●	●
Office 365	Provides reporting on devices that do not meet IT policy		●	●
	Group-based policies and reporting (ability to use groups for targeted device configuration)		●	●
	Root cert and jailbreak detection		●	●
	Remove Office 365 app data from mobile devices while leaving personal data and apps intact (Selective wipe)		●	●
	Prevent access to corporate email and documents based upon device enrollment and compliance policies		●	●
Premium mobile device & app management	Self-service Company Portal for users to enroll their own devices and install corporate apps			●
	Deploy certificates, VPN profiles (including app-specific profiles), and Wi-Fi profiles			●
	Prevent cut/copy/paste/save as of data from corporate apps to personal apps (Mobile application management)			●
	Secure content viewing via Managed browser, PDF viewer, Imager viewer, and AV player apps for Intune			●
	Remote device lock via self-service Company Portal and via admin console			●
	Enroll and manage collections of corporate-owned devices, simplifying policy and app deployment.			●
	Deploy your internal line-of-business apps and apps in stores to users.			●
	Enable more secure web browsing using the Intune Managed Browser app			●
PC management	Cloud-based management for Mac OS X and Windows PCs.			●
	PC management (e.g. inventory, antimalware, patch, policies, etc.)			●
	OS deployment (via System Center ConfigMgr)			●
	PC software management			●
	Single management console for PCs and mobile devices (through integration with System Center ConfigMgr)			●

Cloud App Security vs. O365 Advanced Security Management

	Cross-SaaS security	Office 365 security
	Cloud App Security	**Office 365 Cloud App Security** (ранее Advanced Security Management)
App discovery	• Discovers 13,000 apps and provides an automated risk score • Provides ongoing risk assessment for discovered services (usage patterns, upload/download traffic anomalies) • Anomaly detection for discovered apps • Manual or automatic log upload	• Discovers apps that have similar functionality to Office 365 • Manual log upload
Data control	• Policy setting and enforcement • DLP and data sharing controls all sanctioned apps (cross-SaaS) • Identify and control apps connected to supported cloud services with the ability to revoke access • Use Azure AD Premium for user and session access control, SAML proxy for non-Azure AD customers for any app	• Use existing Office DLP (available in E3 and above) • Use Azure AD Premium for user and session access control • Identify and control apps connected to Office 365 with the ability to revoke access
Threat prevention	• Alerts dashboard includes all policy violations, threat detection, and anomaly detection across SaaS apps • Manual or automatic alert remediation	• Anomaly detection and security alerts for Office 365 • Manual and automatic alert remediation

App discovery – сравнение функционала

	Azure AD **Cloud App Discovery**	**Office 365 Cloud App Security** App Discovery	Microsoft **Cloud App Security** App Discovery
Promise	Uncover shadow IT and onboard selected apps to Azure AD.	Gain visibility over your organization adoption and utilization of Office 365 cloud apps.	Uncover shadow IT and onboard selected apps to Azure AD. Block unwanted apps. Sanction and protect apps with anomaly detection.
Deployment	Automatic update via endpoint agents	Manual log upload	Manual or automatic log upload
Coverage	Only Windows 7 or newer devices, on and off-premises	All organization network traffic, any devices	All organization network traffic, any devices
Cloud App Catalog	~2,100+ business cloud apps that can be managed through Azure AD Cloud App Discovery; can discovery every web app employees are using.	~1,000 apps Limited to apps that have similar functionality to Office 365	>13,000 apps
Cloud trust index (Trust score/app)	No	No	Assessed by specialists inspecting more than 50 attributes including compliance industry standards, security features and posture, terms of service, and more.
Cloud usage analytics	Usage per user and per app	Discovery dashboard providing an overview	Dive into specific service, business unit, geographic area, user, or IP address
SIEM integration	No. All the information can be exported to Azure Storage and presented through Power BI.	No	Yes. Simply with SIEM agents.
App alerts	New app discovery weekly email and alerts on Azure AD Identity Protection console.	No	New app discovery Risky app alerts Custom-built alerts based on the Cloud Trust Index
Anomaly detection for cloud apps	No	Yes. Office 365 focus only.	Yes. For example: large amounts of uploaded data compared to other users, large user transactions compared to user history.

Расширение возможностей Office 365

	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** • 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	**Office 365 Cloud App Security** Обнаружение подозрительной активности в рамках сервисов Office 365

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 O365 к корпоративной телефонии, выделение номеров пользователям

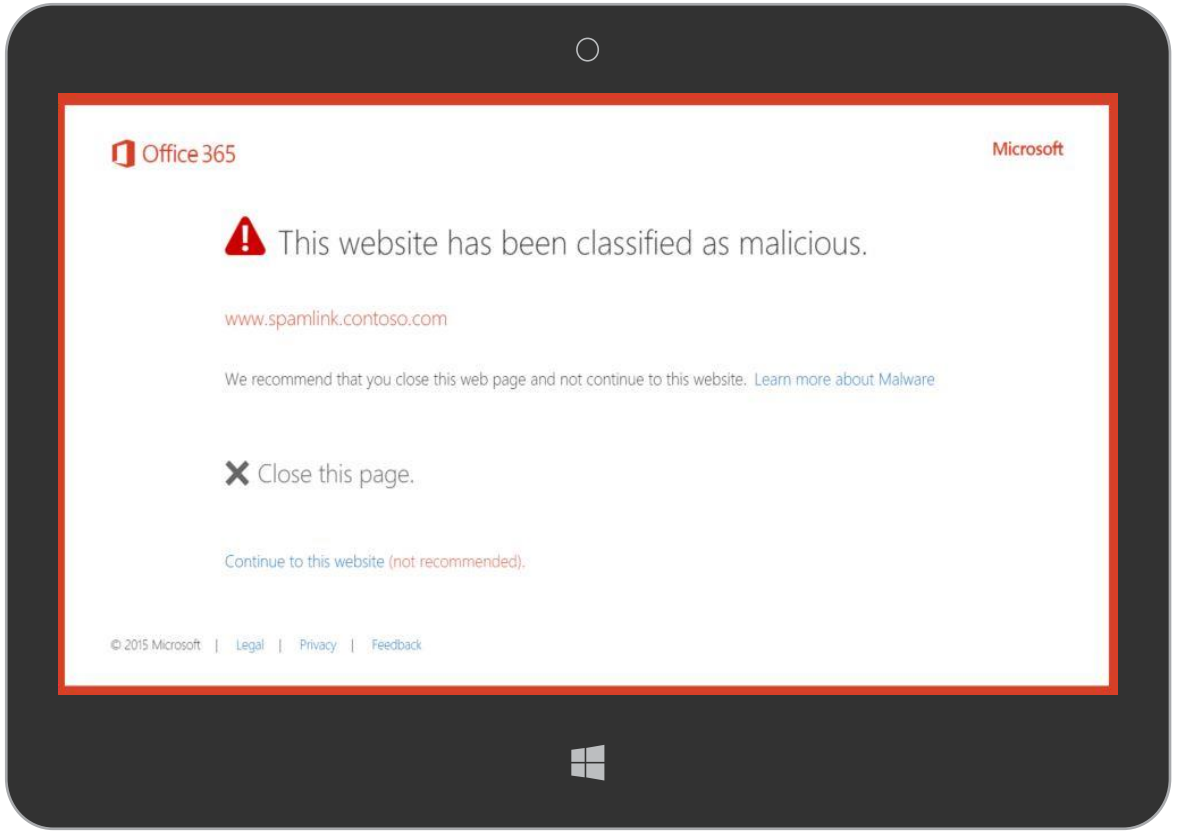
PSTN Conferencing:

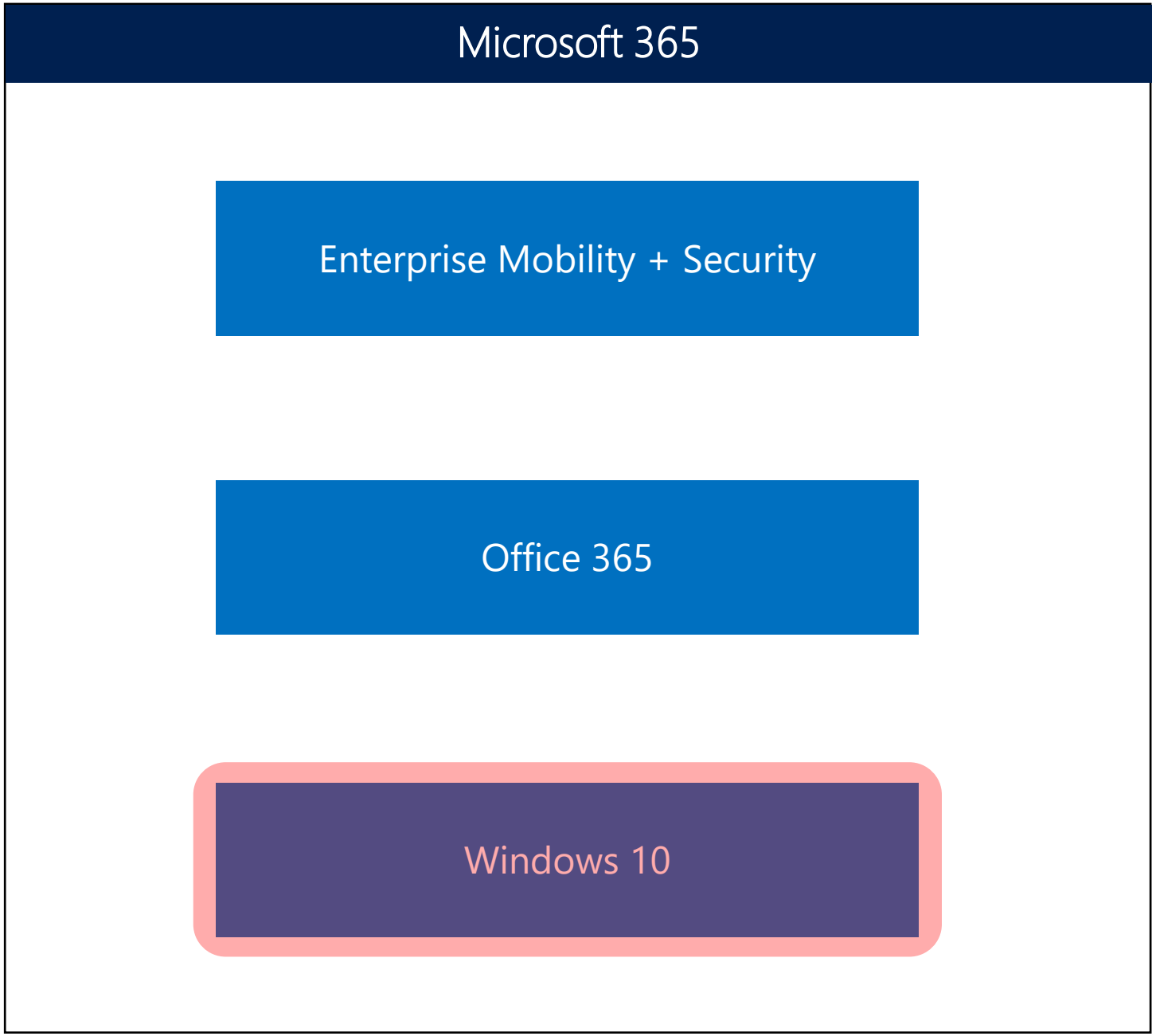
Присоединение к онлайн-собраниям
по звонку из любой точки мира, выделение номера для конференции

Office 365 Advanced Threat Protection

Защита от вредоносных URL-адресов в момент перехода по ссылке
Проверка репутации URL-адресов с блокированием загрузки подозрительных вложений.

Защита от угроз «нулевого дня», исходящих от вредоносных вложений
Вложения с неизвестными вирусными сигнатурами направляются в особую безопасную среду, где выполняется анализ их поведения.




Microsoft 365
Enterprise Mobility + Security
Office 365
Windows 10

Возможности Windows 10

Доверенная платформа	Повышение продуктивности	Персонализация	Широкий спектр устройств
Windows Information Protection Защита от утечек данных за счет отделения корпоративной информации от личной.	**Azure Active Directory Join** Включение устройства в облачную или гибридную инфраструктуру организацию.	**User Experience Virtualization** (UX-V) Синхронизация пользовательских настроек между устройствами и виртуальными средами Windows	**Windows 10 for Industry Devices** Использование недорогих, массовых устройств в качестве терминалов, киосков и др.
Windows Hello for Business Доступ к системе на основе биометрии	**MDM enablement** Управление устройством средствами MDM-решений	**Granular UX Control** Управление интерфейсом через централизованные политики	
Credential Guard Защита учетных записей с помощью аппаратных средств изоляции	**Windows Store for Business, Private Catalog** Каталог приложений, предоставляемых сотрудникам организацией.		
AppLocker Запуск нежелательных и подозрительных приложений в изолированной среде.	**Application Virtualization** (App-V) Упрощение развертывания и управления приложениями		
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.			

Windows 10 **E3**

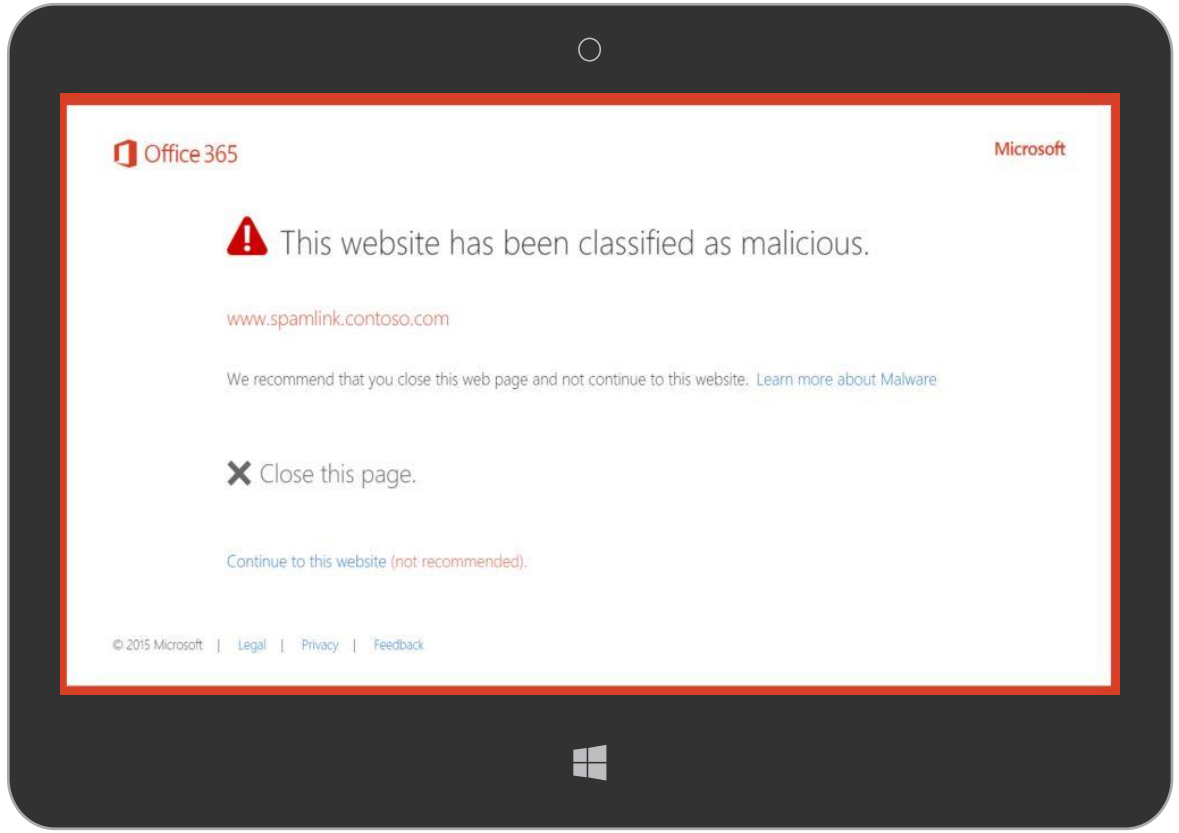
Windows 10 **E5**

Сервисы Microsoft Advanced Threat

Защита почты
Office 365 Advanced Threat Protection

Защита от вредоносных URL-адресов в момент перехода по ссылке
Проверка репутации URL-адресов с блокированием загрузки подозрительных вложений.

Защита от угроз «нулевого дня», исходящих от вредоносных вложений
Вложения с неизвестными вирусными сигнатурами направляются в особую безопасную среду, где выполняется анализ их поведения.



Enterprise Mobility + Security

	Управление учетными записями и доступом	Управление мобильными устройствами	Защита информации	Безопасность учетных записей
EMS E5	**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 *(включает возможности P1)*		**Azure Information Protection Premium P2** Классификация и наложение политик защиты на файлы (автоматическая и ручная) Одновременное использование локального RMS и Azure RMS) *(включает возможности P1)*	**Microsoft Cloud App Security** Обнаружение фактов использования облачных сервисов (через анализ сетевых журналов) Управление облачными сервисами (Microsoft и др.)
EMS E3	**Azure Active Directory Premium P1** Единая учетная запись для локальных и облачных приложений Многофакторная аутентификация, контроль доступа с разных устройств, отчетность и аналитика	**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)	**Azure Information Protection Premium P1** Защита файлов через шифрование с помощью RMS (Azure и локального) Отслеживание доступа к файлам (только через Azure RMS)	**Microsoft Advanced Threat Analytics** Анализ трафика и событий безопасности в локальном AD заказчика, предупреждения и проактивные действия. Локальный сервис (не облако).