上海诺未网络科技有限公司

NOVATECH

Shanghai Nova Technology Co Ltd

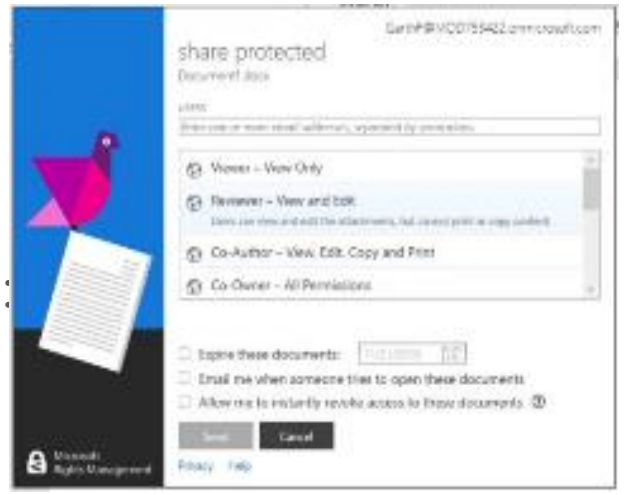
Azure信息保护

文件安全防护方案

什么是 Azure Information Protection

Azure信息保护（Azure Information Protection）是与Office软件及Exchange高度集成的一种安全方案，旨在保护经由Office软件编辑和经由Exchange邮件传递的所有文档。

- 使用分类、标记和保护来保护数据：
  - 根据机密性归类数据
  - 设置规则与策略
- 在内部和外部共享敏感数据：
  - 使用Office中的“共享保护项”
  - 发送加密过的文档
- 跟踪共享数据使用情况并对数据滥用做出响应：
  - 可以追踪谁打开了文档或试图打开文档
  - 可以撤销对共享文档的访问



注： Information Protection的功能需与Office 365 Enterprise E3以上计划搭配实现。

微软企业移动性与安全性组件之一

身份与访问管理	移动设备管理	信息保护	威胁防护
Azure Active Directory 基于多租户云的目录和标识管理服务，提供单一登录 （SSO） 功能来访问数千种云 SaaS 应用程序。	**Microsoft Intune** 从云端管理员工用于访问公司数据的PC、移动设备以及应用，确保设备和应用符合公司安全要求。	**Azure Information Protection** 控制并帮助保护公司防火墙外共享的电子邮件、文档和敏感数据，无论数据存储在何位置以及与谁共享。	**Advanced Threat Analytics** 通过用户行为分析与网络通信分析，来保护企业免受多种类型的高级针对性网络攻击和内部人员威胁。

Azure信息保护功能概述

- 针对单个文件的加密解决方案，尤其适用于Office文档
- 加密作用于文件本身，不受存储位置或其他环境变化的影响
- 可对于不同用户分别设定不同级别的权限
- 通过Azure AD来验证用户身份，以及应用权限
- 用户端操作通过Office软件与AIP客户端来执行
- 加密与访问均需要Internet环境
- 已发出的加密文件仍可追溯

加密方（文档拥有者）所需条件

Azure Information Protection 订阅

包含在EMS（Enterprise Mobility + Security）套件中

Microsoft Office 环境

Office 365 Enterprise E3 以上订阅

Azure Information Protection 客户端

Windows PC 客户端

接收方（文档访问者）所需条件

微软云账号（工作或学校账户）

有Office 365、Azure或其他微软在线服务订阅

无订阅用户可通过企业邮箱申请个人RMS

Microsoft Office 环境

PC或移动端Office软件

建议Office 2016或2013版

Azure Information Protection 查看器

此查看器用来打开加密的非Office文档

（PDF、图片、文本文件等）

加密形式

限定用户访问

指定到单个用户
或用户组

多级别权限

读写打印等权限

文件有效期

文件过期后自动
失效无法打开

水印标记

Office文档加入
页眉/页脚/水印

两种操作方式

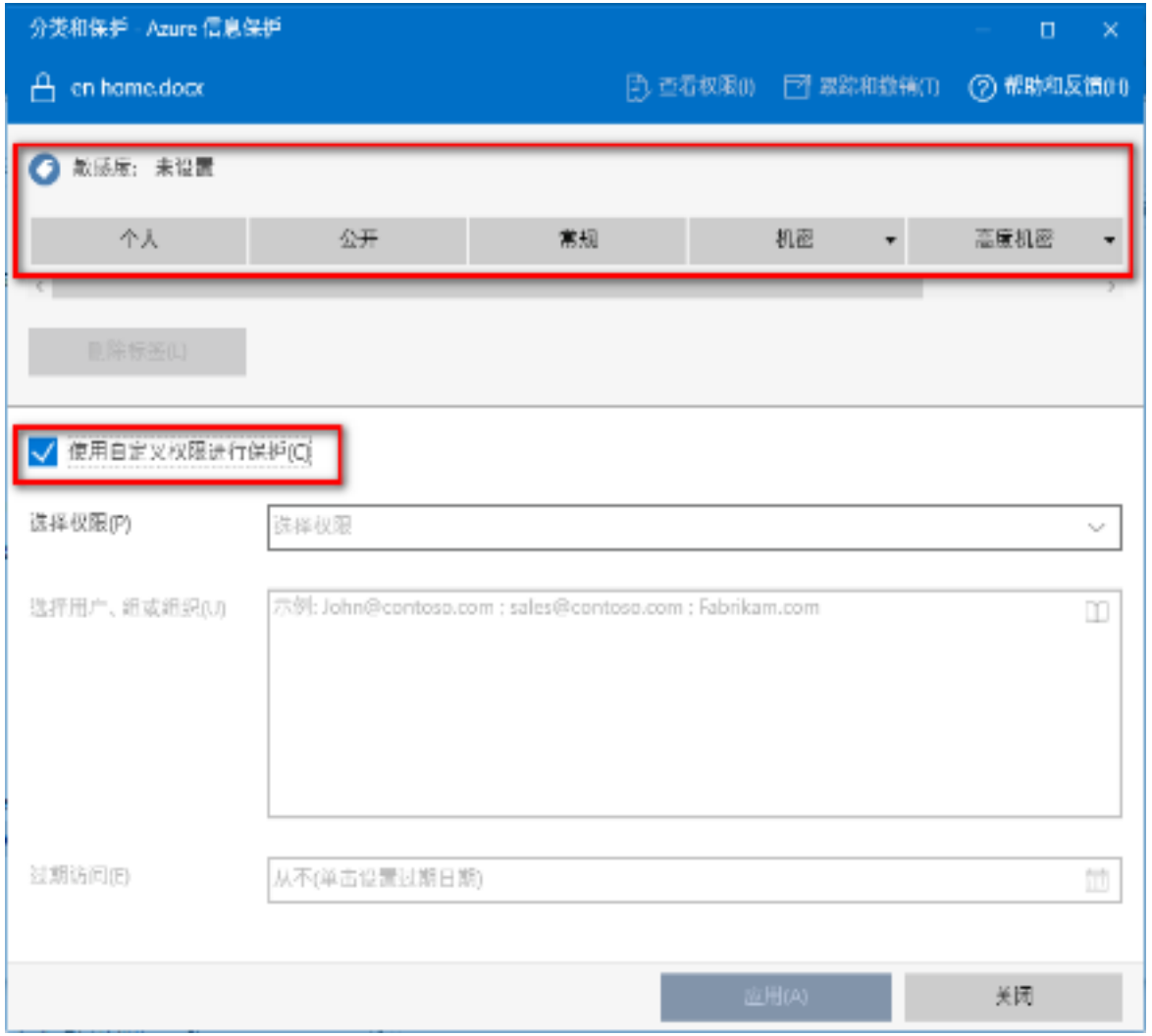
标签+后台策略

后台预定义标签与策略
标签可自动应用，或由用户自行选择
策略自动应用，用户无法选择

自定义权限

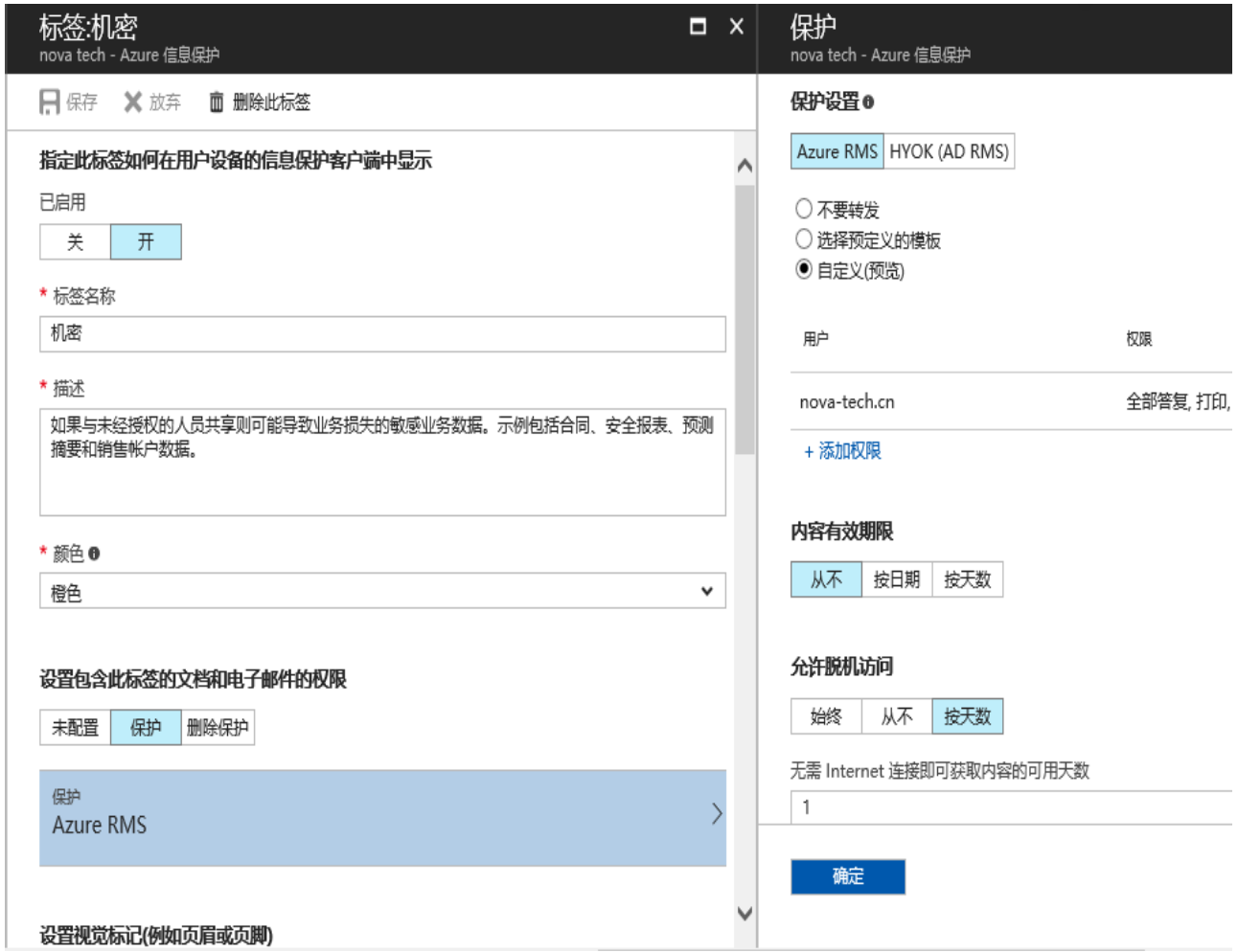
由用户自行设定权限

*** 自定义权限将替换后台策略**



标签的详细配置

- 设置启用或删除保护
- 设置具体的保护措施
  - 访问者
  - 权限级别
  - 有效期
  - 脱机访问
- 设置视觉标记（页眉、页脚、水印）
- 根据关键字给文件打标签
  - 自动给文件打上标签
  - 跳出建议，提示用户打标签



为文件开启信息保护

Word、Excel、PowerPoint

使用“保护”按钮和快捷工具条

为文件开启信息保护

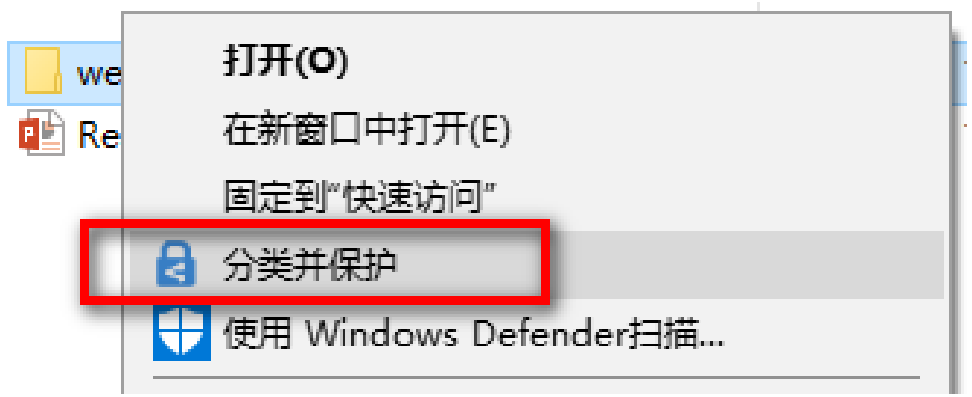
所有Office文档

使用“限制访问”菜单

为文件开启信息保护

Office文档、PDF、图片、文本以及其他各种格式

使用右键菜单“分类并保护”



- 可以对文件夹操作，将文件夹内所有文档批量保护。
- 除Office文档外，其他文件会变成加密的pfile格式，只能通过Azure信息保护查看器打开。

管理已加密的文件

- 加密文件的制作者拥有完全的控制权限
- 加密后的文件可通过任意形式发送和拷贝
- 只需保留原始的加密文件即可追溯管理所有外发副本

- 若要删除加密者的O365/Azure账号（如员工离职），请确保已加密文件拥有解密版本，或其他用户拥有“共有者”权限

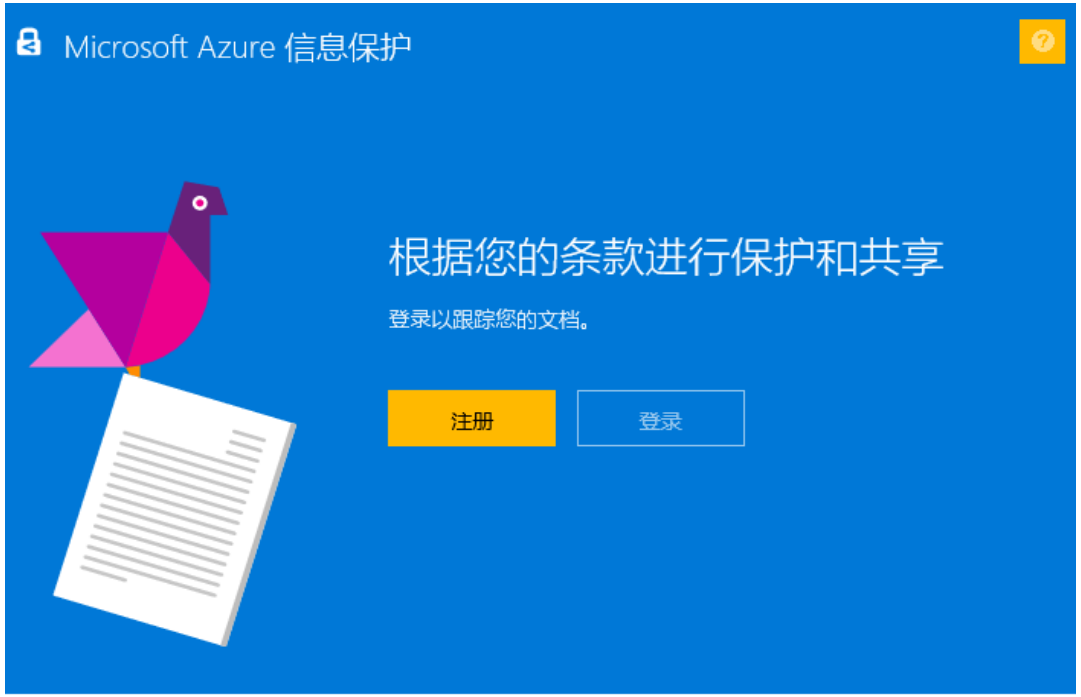
追溯发出的加密文件（加密者）

追溯文档的途径：

- 已加密文件的右键菜单“分类与保护”
  然后点击“跟踪和撤销”按钮
- 直接使用O365或Azure账户登录
  https://track.azurerms.com/

可进行的操作：

- 查看访问记录（包括已拒绝的尝试）
- 撤销权限（文件将无法打开）



访问已加密文件

打开已加密的Office文档：

- 使用PC/Mac上的正版Office软件（建议使用最新版本）
- 使用Office 365订阅中的移动端Office app（iOS/Android版）

打开已加密的PDF、文本、图片等其他格式文件：

- 使用Azure信息保护查看器

PC/移动端下载链接：

https://portal.azurerms.com/#/download

使用微软云账户

打开已加密文件时需有Internet连接，
并使用以下微软云账户登录以验证身份：

- Office 365全球版订阅账户
- Azure全球版订阅账户
- 其他微软在线服务账户

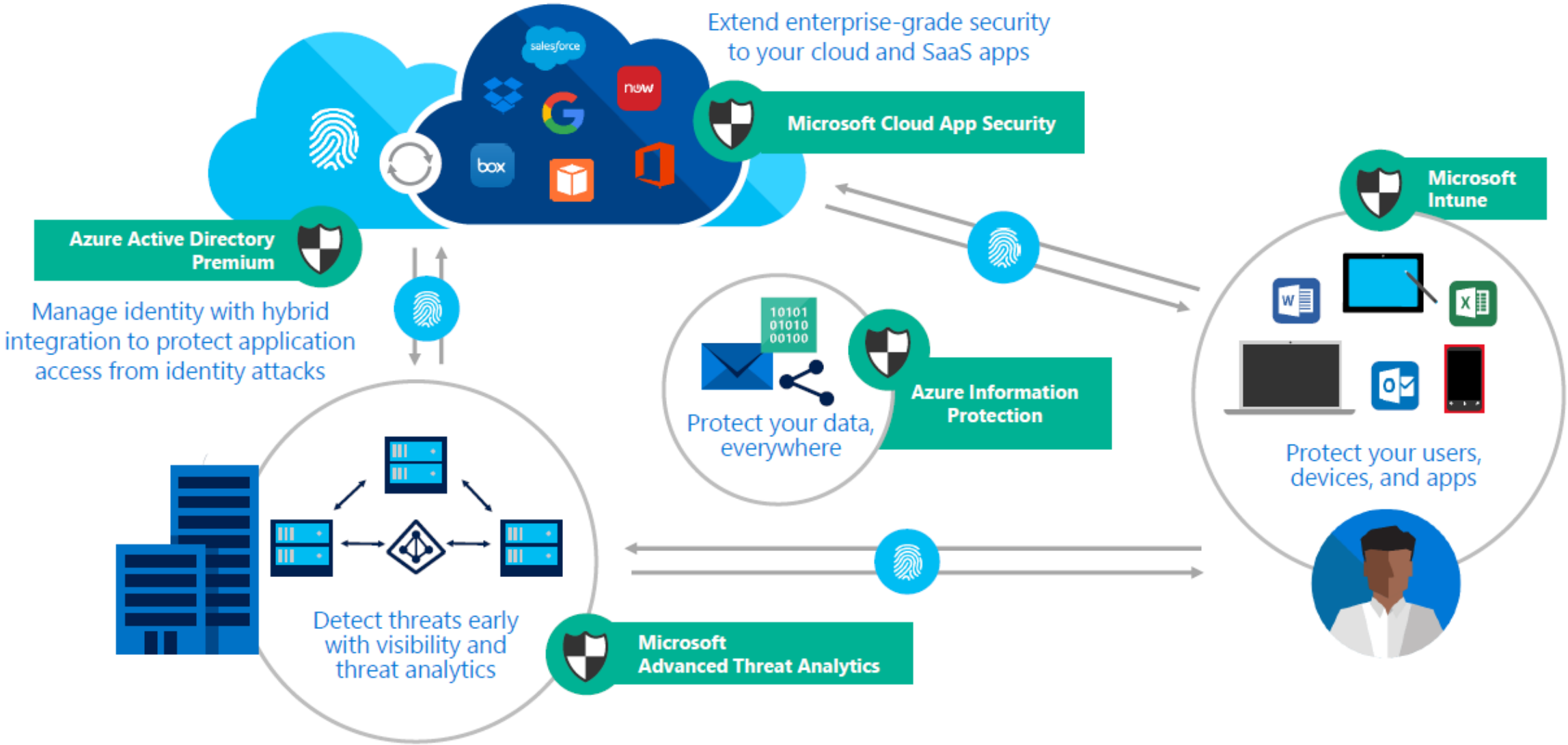
对于没有这些账户的用户，可以通过下面的Microsoft Azure 信息保护页申请个人RMS：

https://signup.microsoft.com/signup?sku=rms

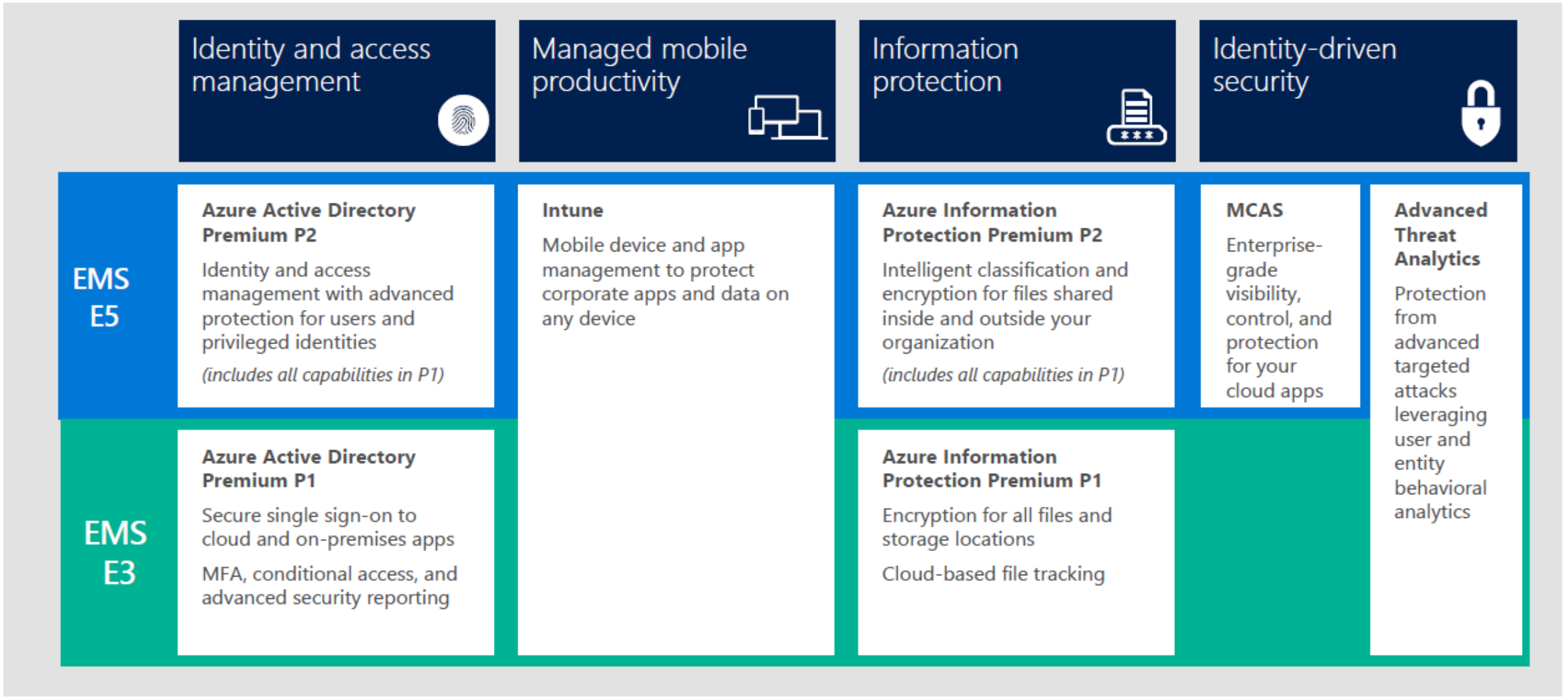
Azure Information Protection 订购选项

- 包含在微软企业移动性与安全性 Enterprise Mobility + Security（EMS套件）中
- EMS套件可叠加在全球版Office 365（海外订阅）之上

Enterprise Mobility + Security 组件



Enterprise Mobility + Security 订阅计划



MOBILE-FIRST + CLOUD-FIRST

Microsoft

联系我们，了解更多产品与服务

上海

+86 021-22065380

上海市浦东新区浦三路21
弄银亿滨江55号1402室

北京

+86 010-53605669

北京市朝阳区广渠路36号
院首城国际5号楼c座938室

香港

+852 94019304

香港九龙尖沙咀广东道17
号海港城环球金融中心南座
13A楼06室

NOVATECH