Microsoft

Microsoft Online Tech Forum

微软在线技术峰会

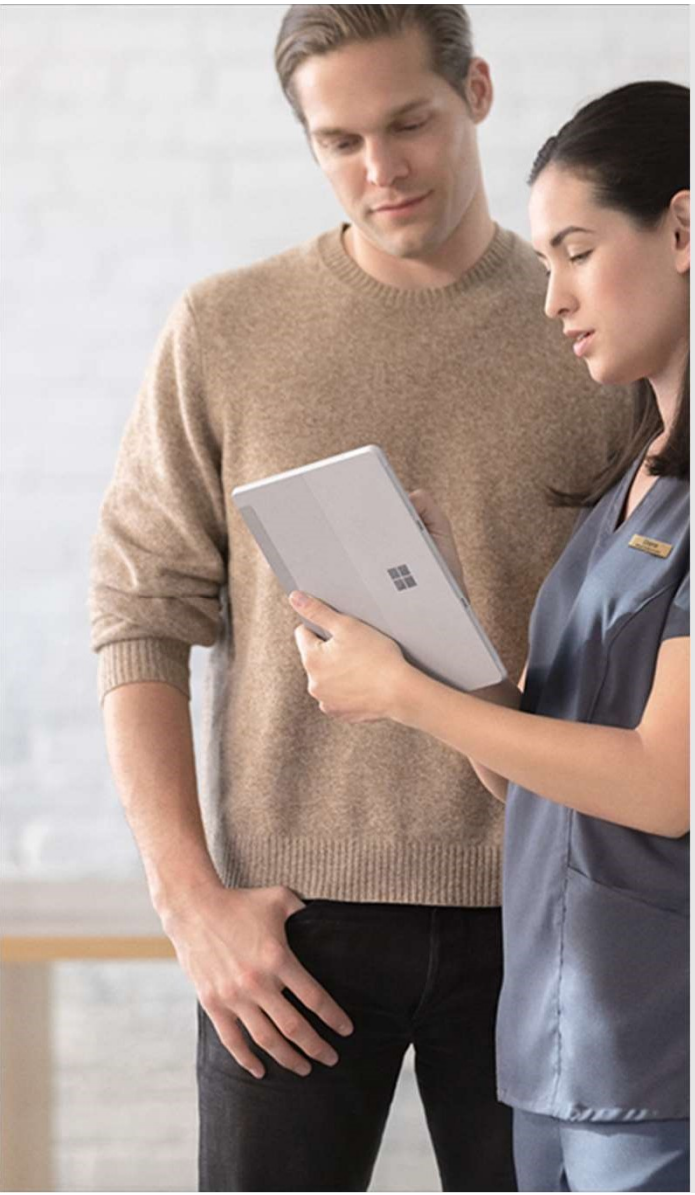
Microsoft

数据防泄露，基于 Microsoft 信息保护和威胁防护全流程实战

李辉

微软特约资深讲师 微软技术社区 Regional Director

Microsoft Online Tech Forum
微软在线技术峰会



58%

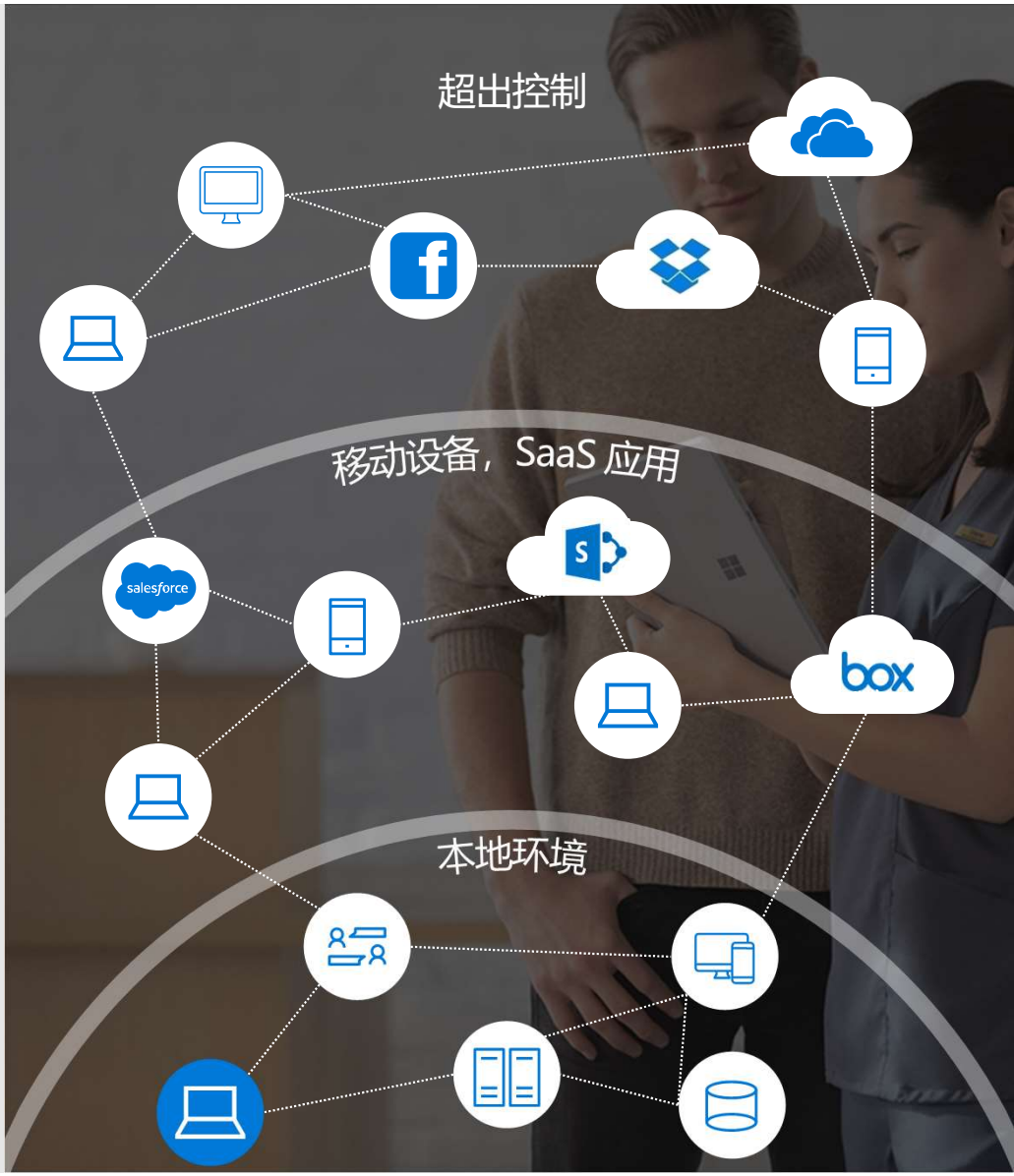
工作人员曾经无意地将敏感数据分享给错误的人

Stroz Friedberg

企业安全边界正在发生变化

企业安全边界正在发生变化

您对数据有多少控制权?

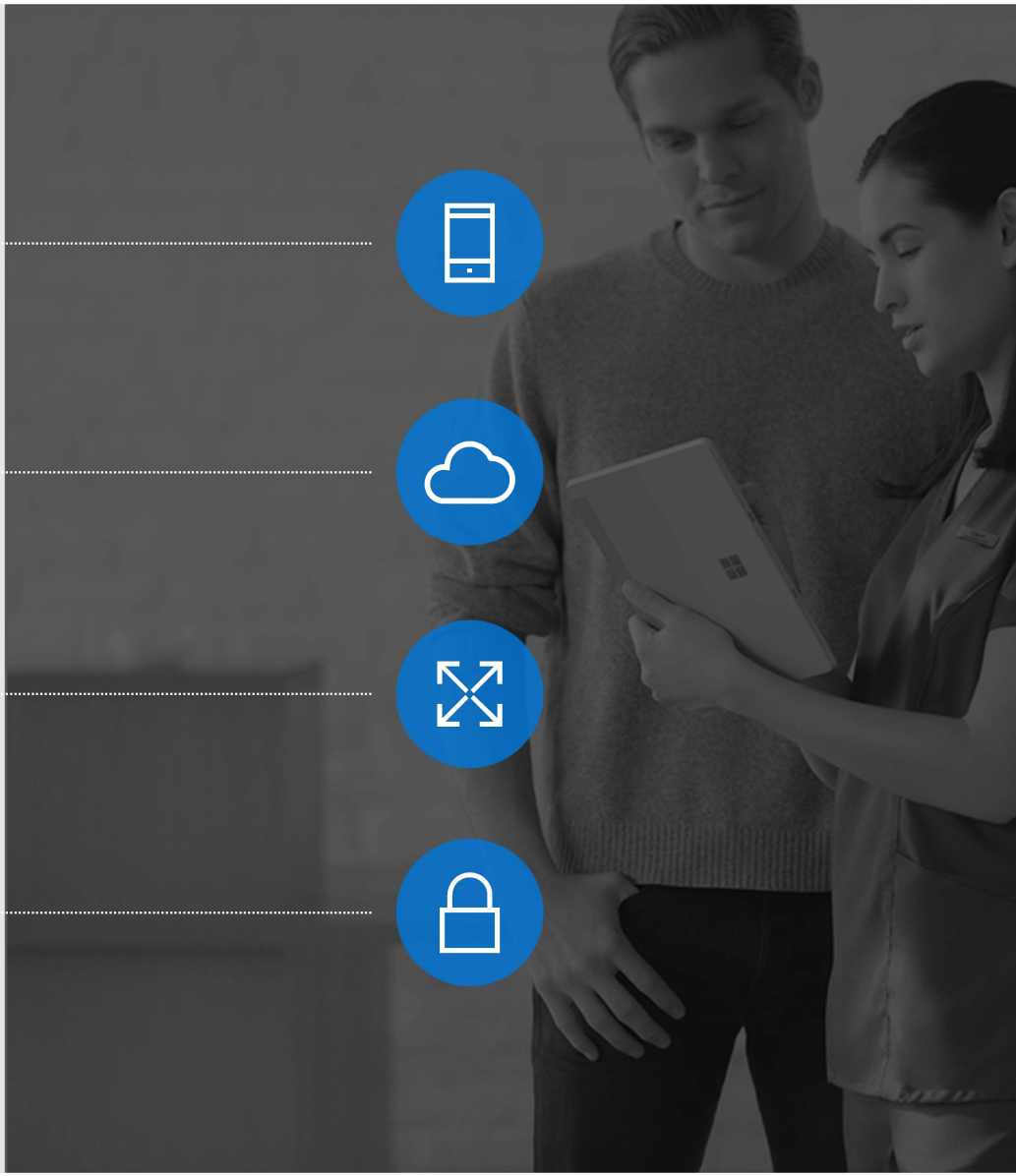


如何在移动设备中
保护企业数据和文件?

如何发现,
并保护在 SaaS 应用中的数据?

如何保护分享到企业外部的数据?

如何保护本地环境和
云服务中的敏感数据?



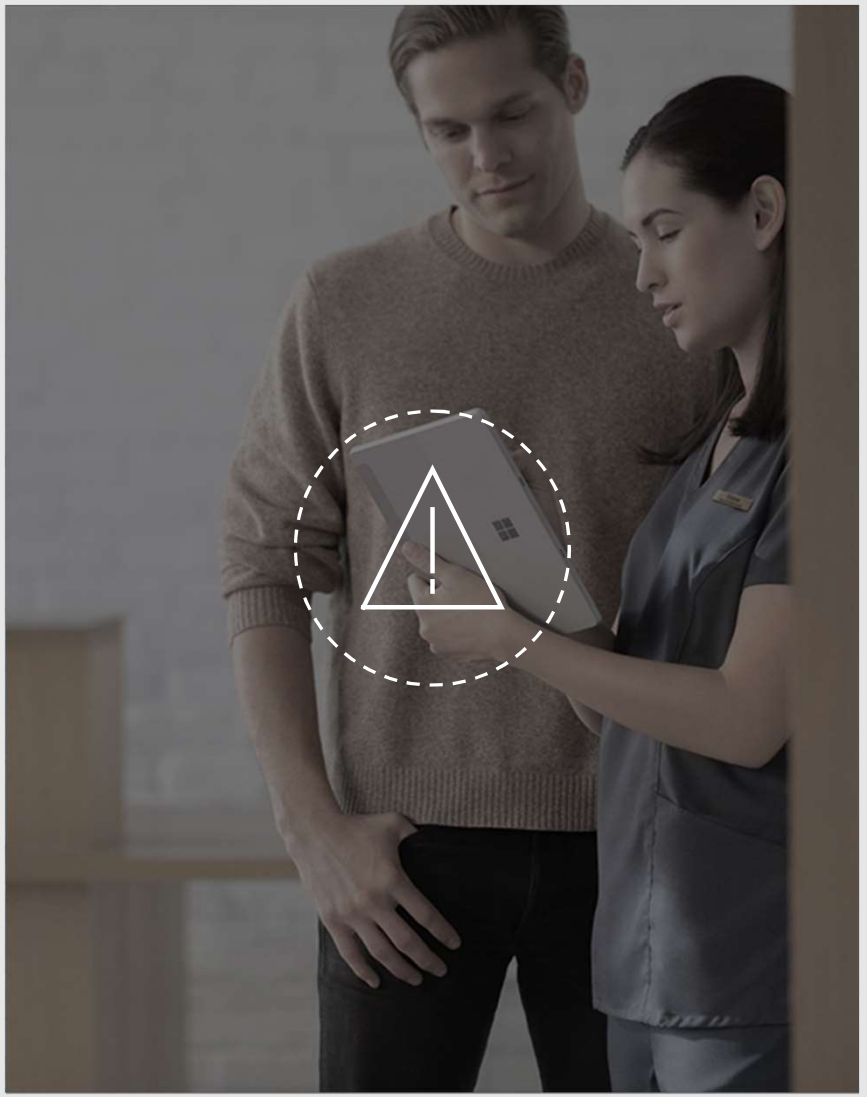
信息保护

保护任何位置的数据

零碎的信息 ..... → 统一分类

分散的知识 ..... → 丰富的仪表板

用户执行不力 ..... → 直观体验



Microsoft 信息保护

跨设备、应用程序和云服务，全面保护敏感数据的整个生命周期

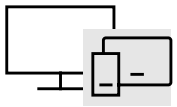
敏感信息检测和分类

基于策略保护应用

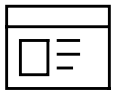
监控和补救

加速合规性

覆盖



设备



应用程序

云服务

本地环境

全面保护您的信息安全

AZURE ADVANCED THREAT PROTECTION
识别高级数据攻击和内部威胁

MICROSOFT CLOUD APP SECURITY
监控15k+ 云应用中的数据访问、使用，防范数据非法访问

OFFICE 365 DATA LOSS PREVENTION
防范Exchange Online/SharePoint Online/OneDrive for Business 中的数据泄露

OFFICE 365 MESSAGE ENCRYPTION
在Office 365中向公司内外的任何人发送加密电子邮件

WINDOWS INFORMATION PROTECTION
在Windows 10设备上分离个人和工作数据，防止工作数据移动到非工作位置

OFFICE 365 ADVANCED DATA GOVERNANCE
对Office 365 中的敏感和重要数据应用保留和删除策略

MICROSOFT INFORMATION PROTECTION

检测 | 分类 | 保护 | 监控

CONDITIONAL ACCESS
基于策略控制对文件的访问，如身份认证、计算机配置、地理位置

OFFICE APPS
在Excel/Word/PowerPoint/Outlook 中保护工作中的敏感信息

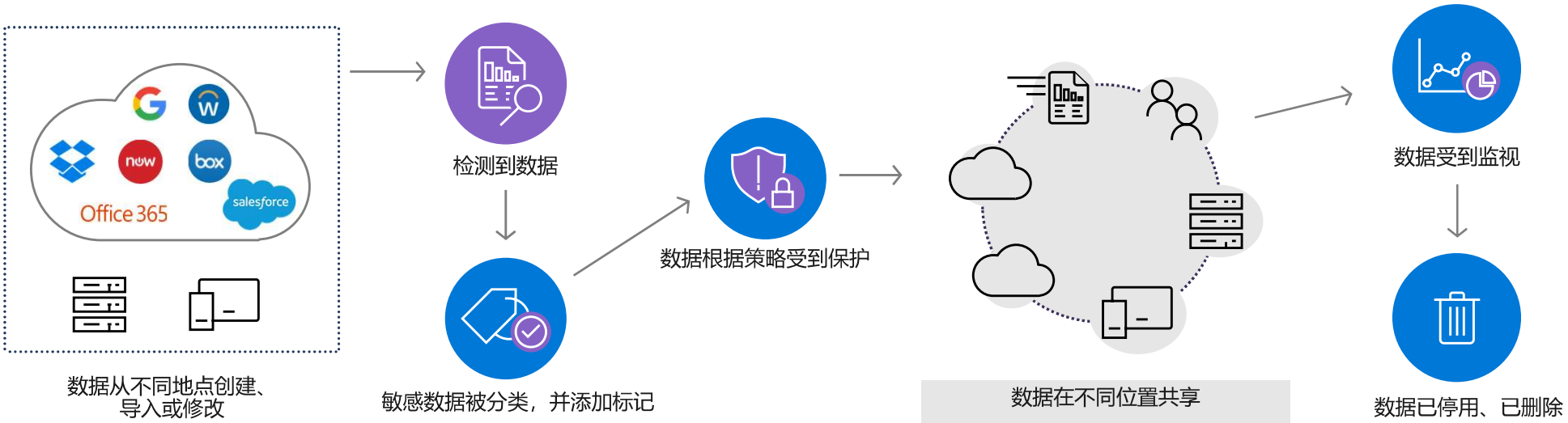
SHAREPOINT & GROUPS
保护文档库和列表中的文件

AZURE SECURITY CENTER INFORMATION PROTECTION
在Azure SQL、SQL Server 和其他Azure 存储库中分类和标记敏感的结构化数据

SDK FOR PARTNER ECOSYSTEM & ISVs
在ISV 中使用标签、应用保护

ADOBE PDFs
在Adobe Acrobat Reader上查看本地标记和受保护的PDF

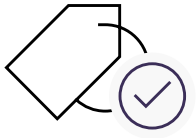
在整个生命周期中跟踪数据



Microsoft 信息保护解决方案

检测

基于策略对敏感数据
进行扫描与检测



分类

基于敏感度
对数据进行分类与标注

保护

应用保护操作，
包括加密、访问限制

监控

查看报告并评估分类、
标记和受保护的数据

Demo

安全与合规中心的统一标签

应用与文档内容一致的敏感度标签

标签 是可定制的，
明确显示的，
持续保护的。

标签将是应用和实施数据保护策略的基础

在文件和电子邮件中，标签作为文档元数据持久保存

在SharePoint Online中，标签作为容器元数据持久保存

Demo

在跨平台的 Office 应用中使用标签

Demo

在 Microsoft Cloud App Security 自动标签

Demo

监控受标签保护的数据

安全的设备，并在应用级别保护数据

数据控制 / 隔离

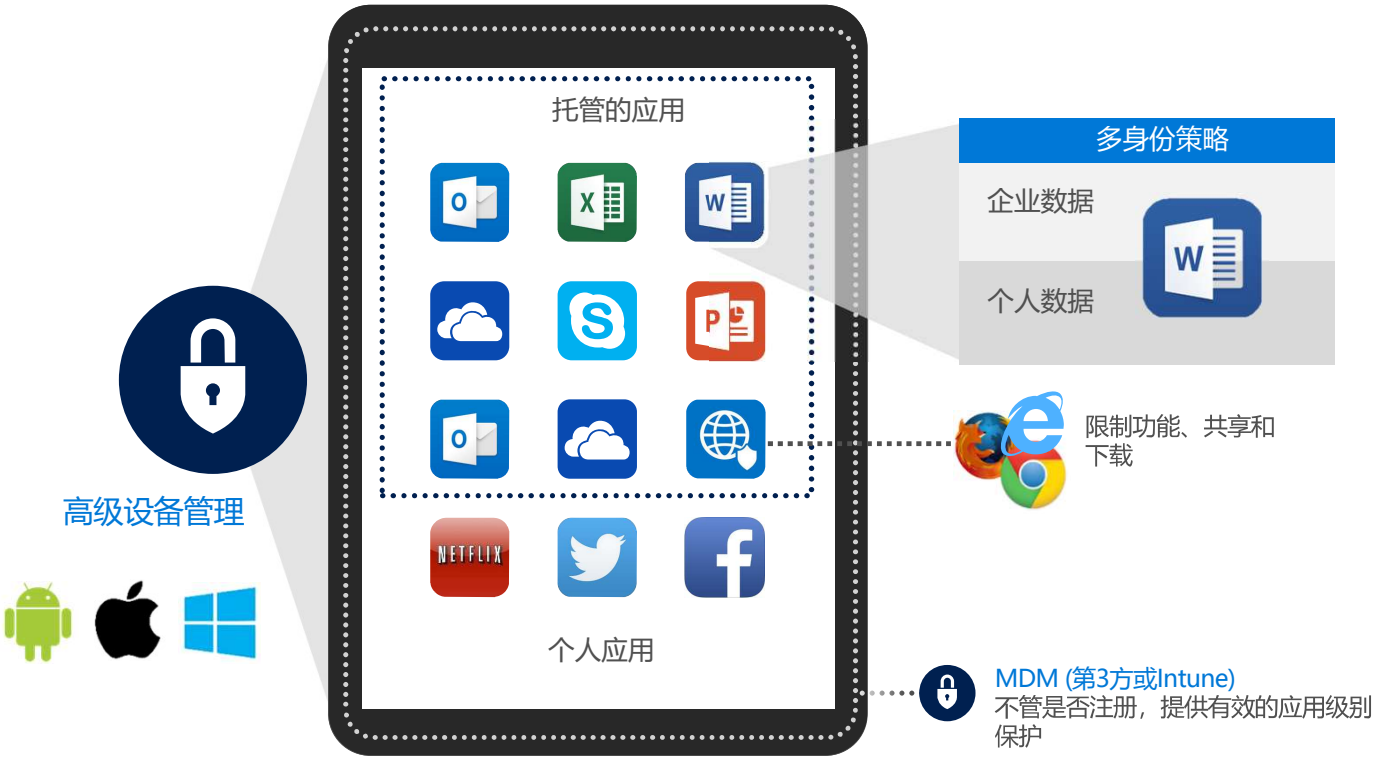
在访问后控制企业数据，并将其与个人数据分开

设备安全配置

强制设备加密、密码 / PIN 要求、越狱检测 / 根检测等

限制应用程序和URLs

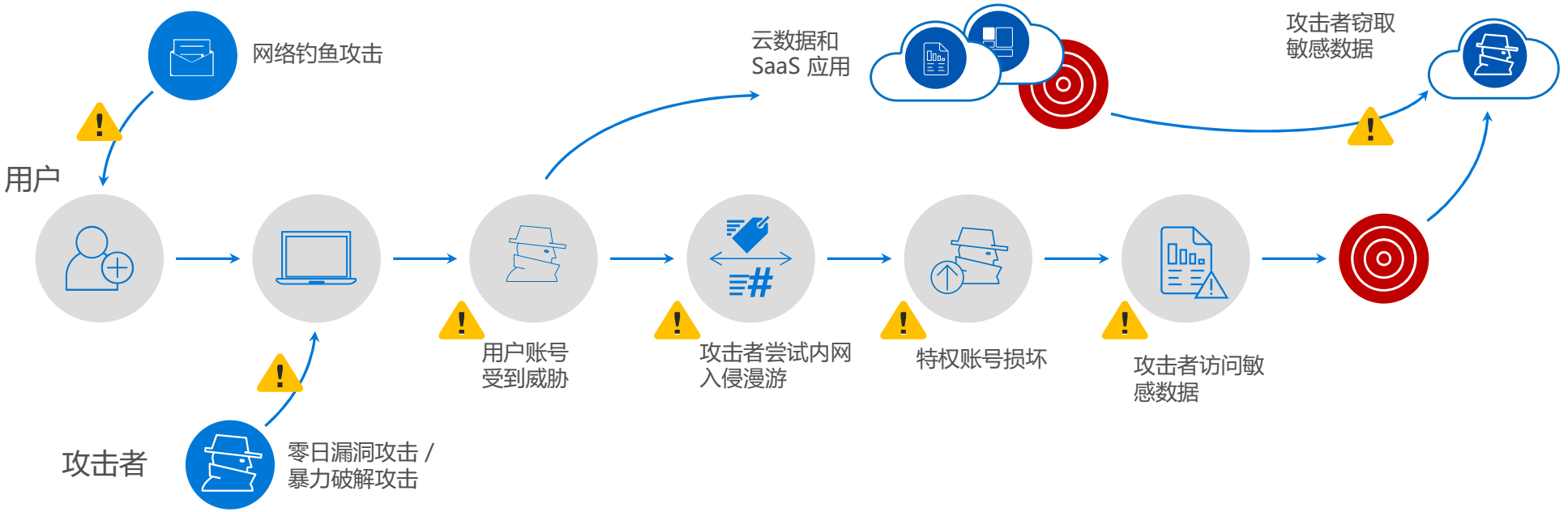
限制在移动设备和PC上对特定的应用程序或URL地址访问



91%

网络攻击和数据破坏
始于仿冒的电子邮件

加快攻击检测



匿名用户行为

不熟悉的登录位置

匿名用户行为

入侵漫游攻击

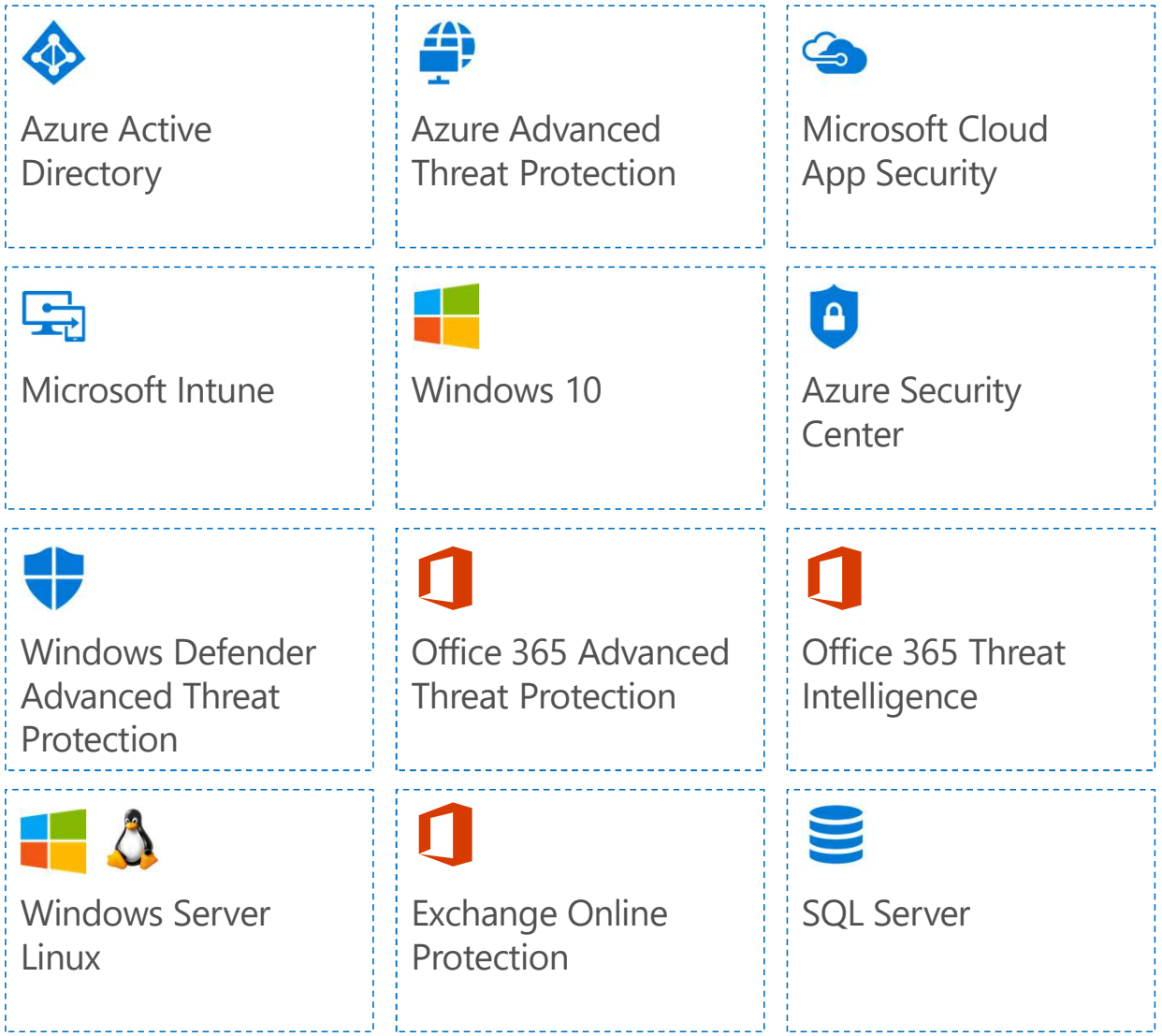
特权升级

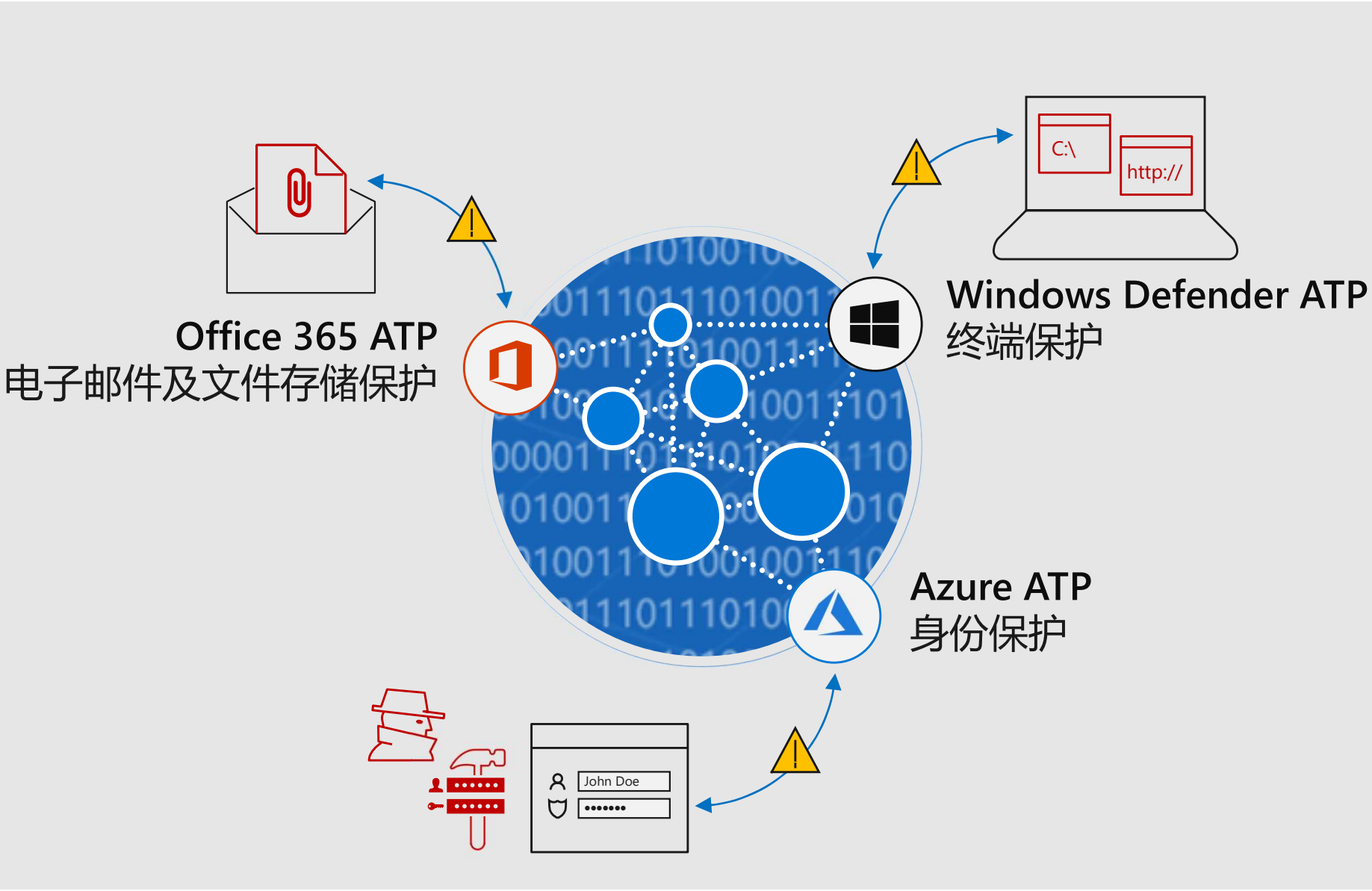
账户模拟

数据泄露

Microsoft 威胁防护

1. **身份：** 验证和保护用户和管理员帐户
2. **终端：** 保护来自传感器或用户设备的信号
3. **用户数据：** 评估电子邮件和文档中是否包含恶意内容
4. **云应用：** 保护 SaaS 应用程序及其相关数据存储
5. **基础设施：** 保护云和本地位置的服务器、虚拟机、数据库和网络




C:\
http://
Office 365 ATP
电子邮件及文件存储保护
Windows Defender ATP
终端保护
Azure ATP
身份保护
John Doe

Demo

自动检测信息威胁，实现智能防护

使用统一标签对信息进行分类

启用 DLP 和 AIP 策略

了解并开始使用 Cloud Apps Security

Office 365 ATP、Windows Defender ATP 和 Azure ATP

Microsoft

扫码下载讲师PPT

更多精彩尽在【微软市场活动】