
IBM
安世加沙龙第三十一期
数据安全及个保法
2022年1月14日 / 周五下午 / 线上
安世加

零信任助力企业安全管理：场景与实践

IBM大中华区资深安全架构师

袁笑鹏

零信任原则在企业安全管理场景中的应用

IBM

保护客户隐私

简化并保护用户登录
管理用户偏好和同意
执行隐私条例和控制措施

保护混合云环境

管理和控制所有访问
监视云活动和配置
保护云原生工作负载

降低业务中断和勒索风险

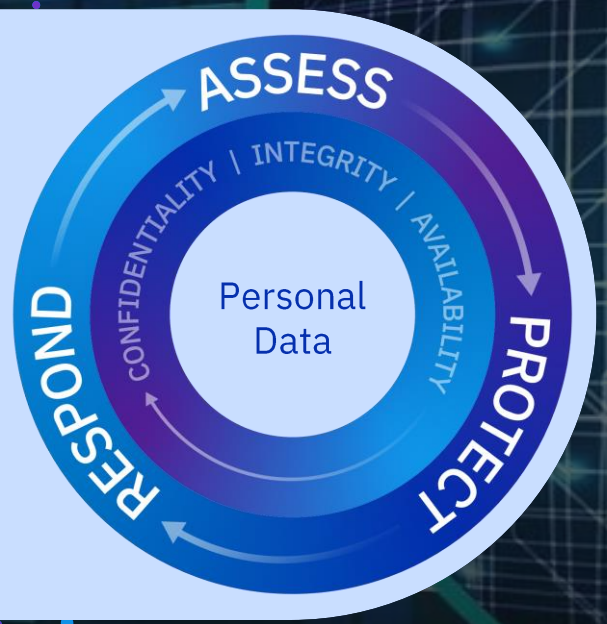
强制最小权限访问
发现有风险的用户行为

确保远程办公安全

保护终端设备
提供无密码体验

安世加

1. 保护客户隐私



- **评估**数据使用情况，并动态调整以限制风险
- **保护**个人数据
- 迅速**响应**，以解决事件、客户请求和法规要求

构建客户隐私数据保护能力

隐私数据保护能力

评估

数据发现和分类 | 数据资产清单 | 数据谱系 | 风险洞察

保护

身份和访问治理 | 活动监测 | 威胁分析 | 加密和数据遮蔽

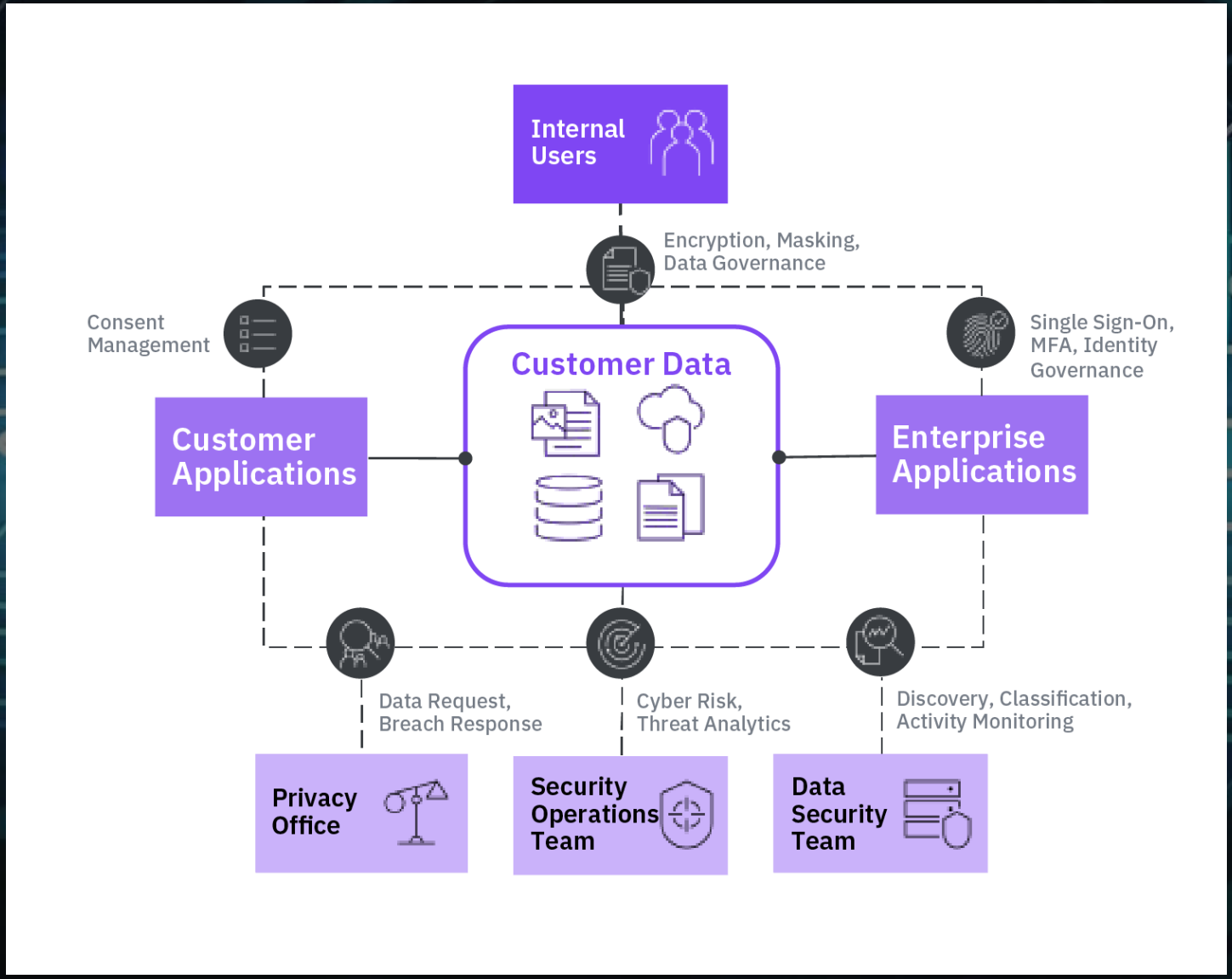
响应

数据泄露响应 | 数据主体权利实现 | 同意管理

开放式混合多云平台

合作伙伴生态

零信任原则保护客户隐私



2. 降低业务中断和勒索风险

泄露的凭据

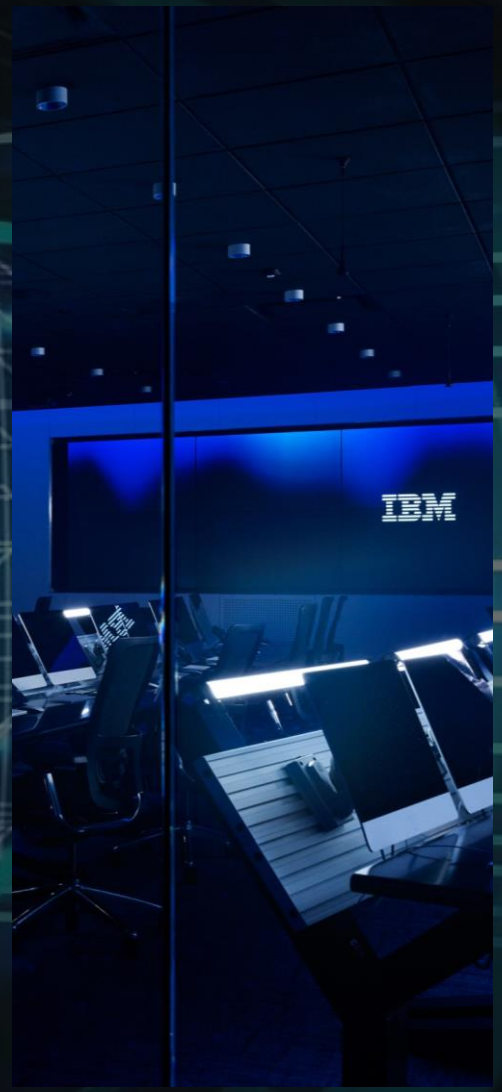
- 特权用户的凭据被承包商窃取，承包商使用这些凭据获取访问权限

勒索病毒

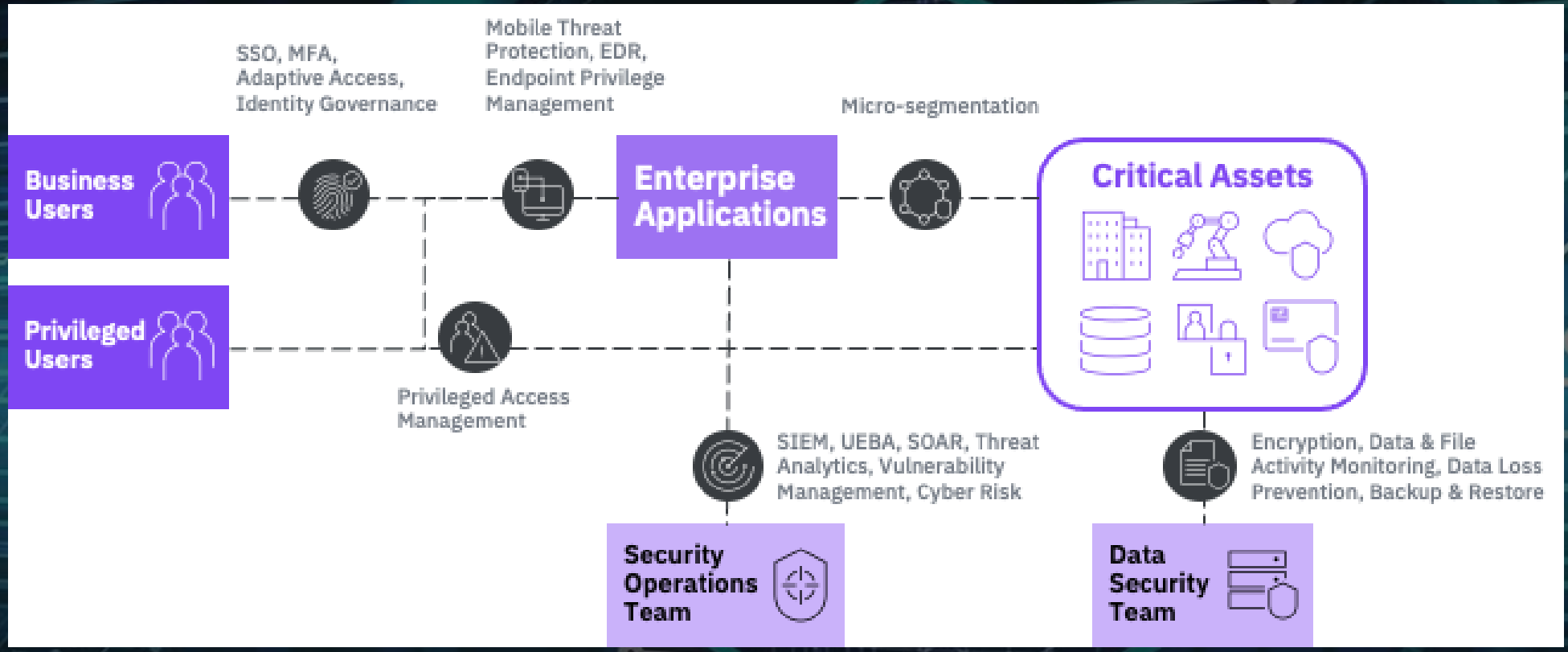
- 通过电子邮件传播，加密用户文件，要求支付赎金

数据外泄

- 内部人员复制机密文件并发送到个人电子邮件或云存储帐户



使用零信任方法降低业务中断的风险



3. 保护企业混合多云环境

IBM

- ✓自适应
- ✓计划性
- ✓零信任为中心

现代化

分析并改进安全性和法规遵从性态势

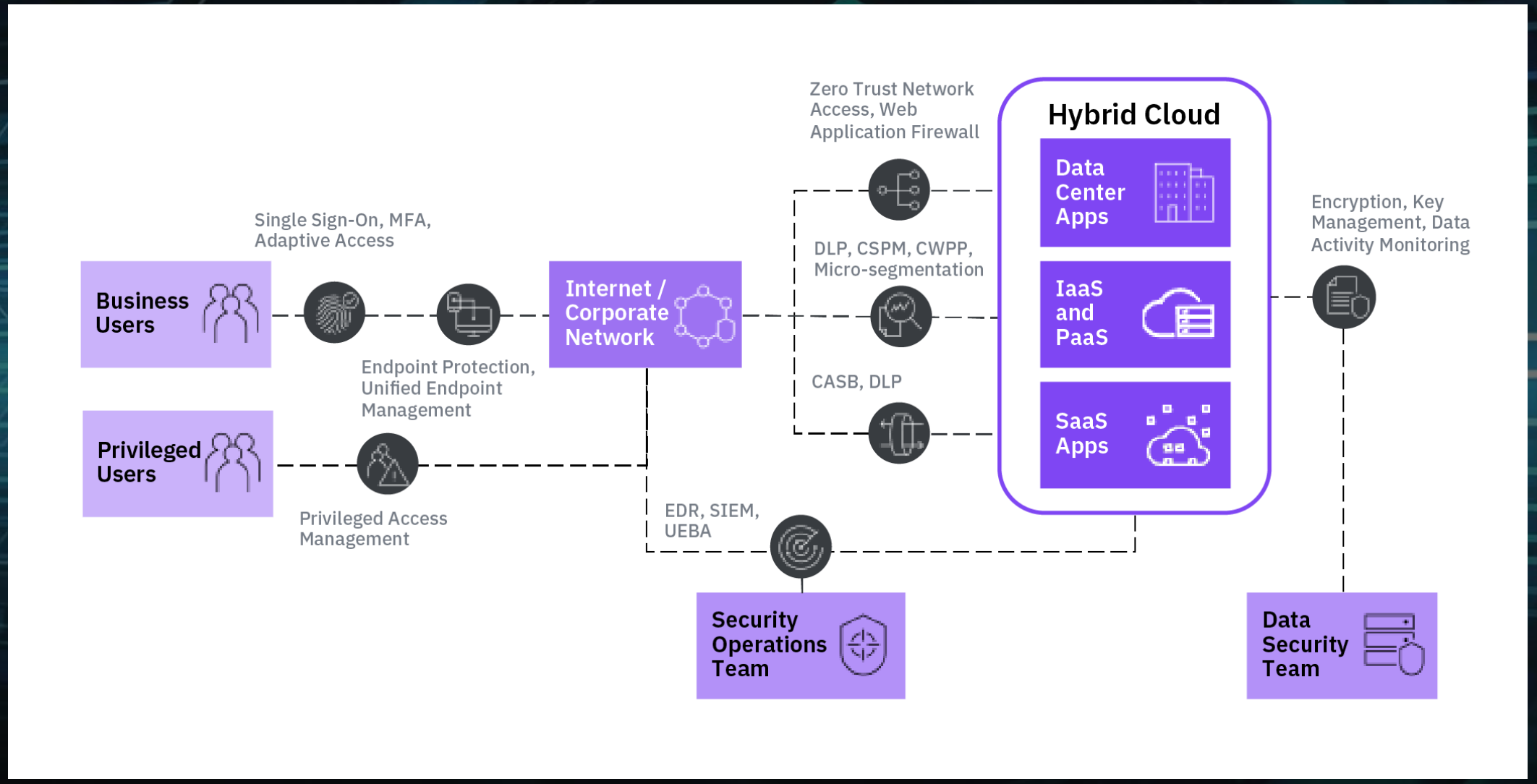
Red Hat IBM Cloud vmware aws Google Cloud Microsoft Azure

Open security ecosystem & strategic alliances with cloud providers

混合云环境中零信任的应用

	应用程序现代化	使用云应用程序	迁移工作负载	数据平台现代化
访问验证 （用户，应用，数据）	- **特权访问管理** - 自适应访问 - 多因子认证 - API安全与安全开发 - 多云密钥管理 - Web应用程序防火墙 - 基于角色的访问/基于标签的访问	- **数据丢失防护** - **云访问安全代理** - **安全访问服务边缘** - 自适应访问 - 多因子认证 - 特权访问管理	- **安全访问服务边缘** - 特权访问管理 - 自适应访问 - 多因子认证 - 数据加密 - 多云密钥管理	- **数据加密** - **多云密钥管理** - 特权访问管理 - 隐私保护(HPDC) - 密钥管理 - 保护诊断
工作负载保护 （服务器，容器，网络）	- **云工作负载保护** - **云安全态势管理** - 安全容器生命周期管理 - 漏洞扫描 - 网络分段 - 防止未经授权的访问	- 保护云中使用的数据 - 保护和隔离工作负载	- **云安全态势管理** - 云工作负载保护 - 漏洞扫描 - 网络分段	- 分区的安全隔离 - 保护使用中的数据（安全执行） - 保护容器
快速检测和响应威胁	- SIEM, UEBA - EDR for Containers - XDR - 网络入侵检测/报告	- SIEM, UEBA - EDR - XDR	- **EDR for VM** - SIEM, UEBA - XDR	- SIEM, UEBA - XDR

零信任原则保护多云环境



4. 保护远程办公的安全

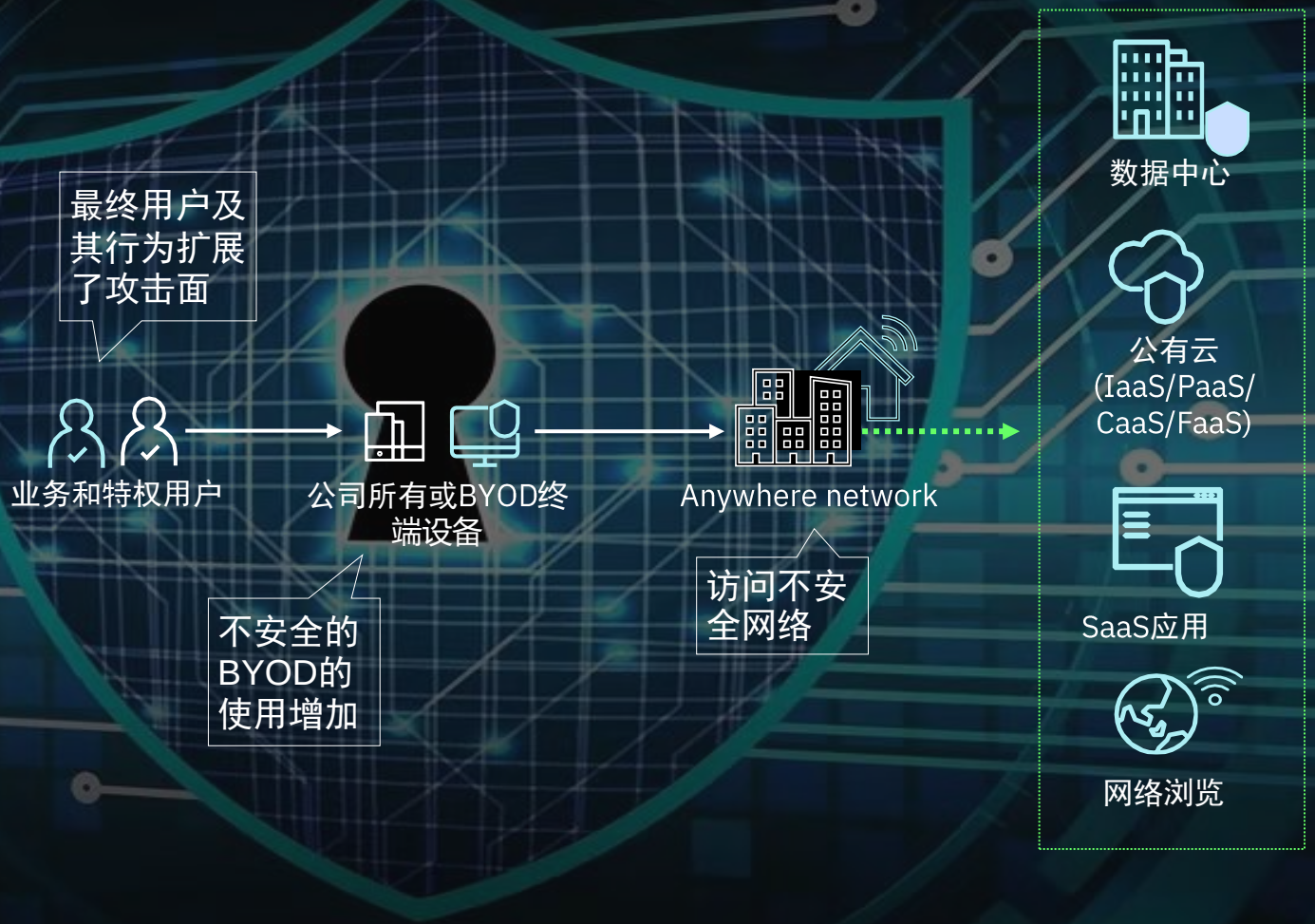
远程办公面临的风险：

1.内部网络暴露在外部攻击之中

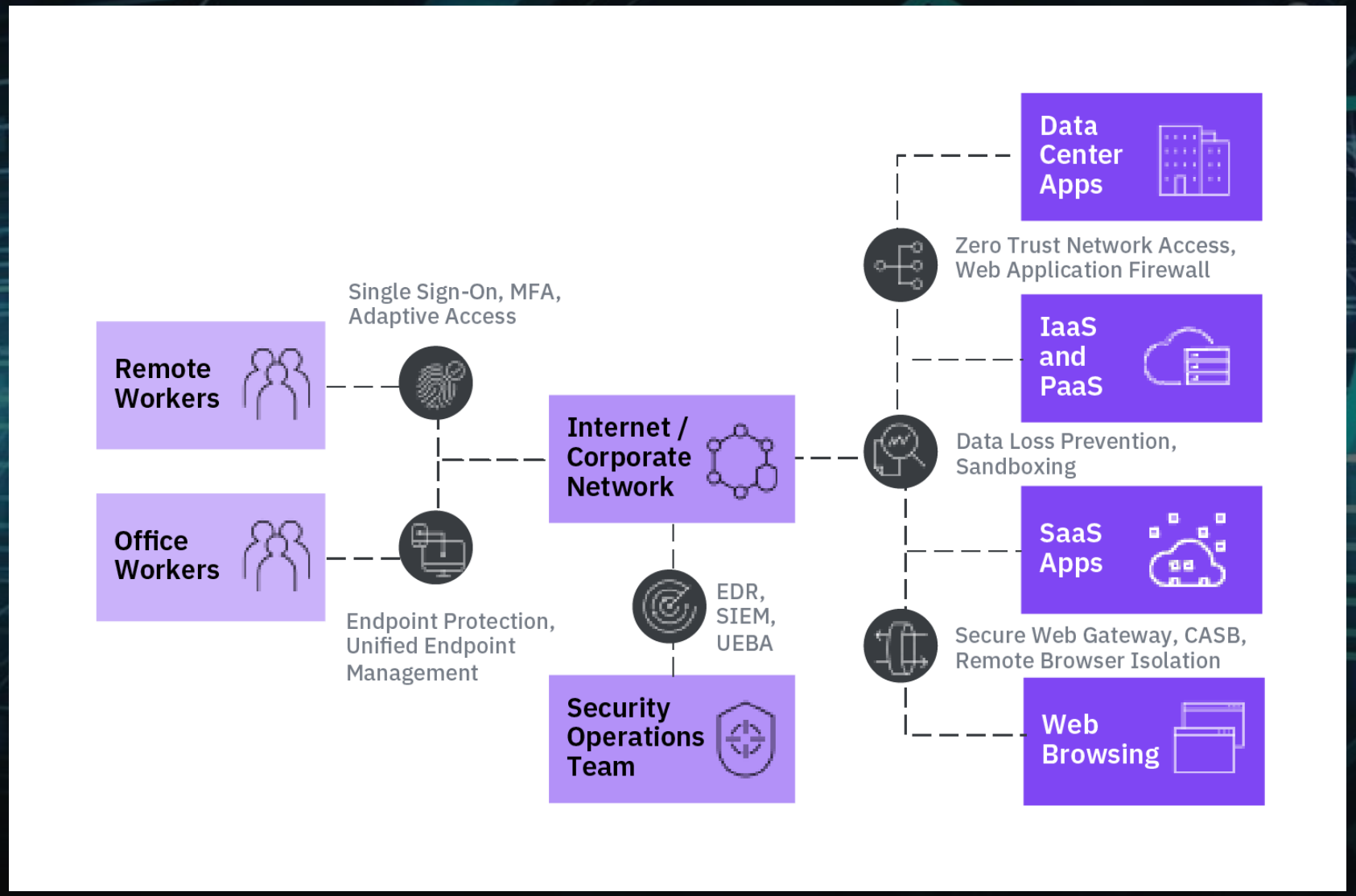
2.恶意软件可以通过VPN传播，感染数据中心的系统

3.为了加强安全性，流量可能会有延迟

4.VPN账号共享



零信任保护远程办公安全



零信任在企业安全管理中的应用案例

保护个人信息，维护数据安全。 IBM 助力某物流行业龙头企业打造企业级数据安全体系

客户现状：

截至2021年，客户在全国拥有3,663个加盟商及32,441个网点及门店，服务网络覆盖全国31个省、自治区和直辖市，网点密集、设备多，平时的包裹量非常大，每天海量订单数据信息，做好每个业务环节的数据安全管控极其重要。

解决方案及业务价值：

客户以IBM Cloud Pak for Security 和 IBM QRadar 为核心，建立起统一的、现代化的、企业级安全体系，实时监控企业各环节数据安全，以标准化流程自动响应海量数据处理需求，大幅提高数据处理的效率，降低了成本，保证了业务的稳定、安全运营。

IBM零信任产品组合

全面、完整的零信任产品和服务组合

数据	数据发现、分类和保护，数据加密，密钥管理 (Guardium，数据安全服务)
网络	微隔离托管，流量分析 (QRadar，网络安全服务)
人员身份	IAM，认证，特权账号管理 (Verify Access，Verify Privilege，Cloud Identity)
设备与工作负载	移动设备管理, 容器安全服务 (MaaS360)
可见性与分析	企业安全洞察力和分析, SIEM (QRadar, X-Force Threat Management)
自动化与编排	安全编排、自动化与响应，安全事件响应 (Cloud Pak for Security，Resilient, X-Force Threat Management)

IBM

关注我们

安世加专注于网络安全行业领域，通过互联网平台、线下沙龙、峰会、人才招聘等多种形式，培养安全人才，提升行业的整体素质，助推安全生态圈的健康发展。

安世加