

IBM Cloud Pak for Security

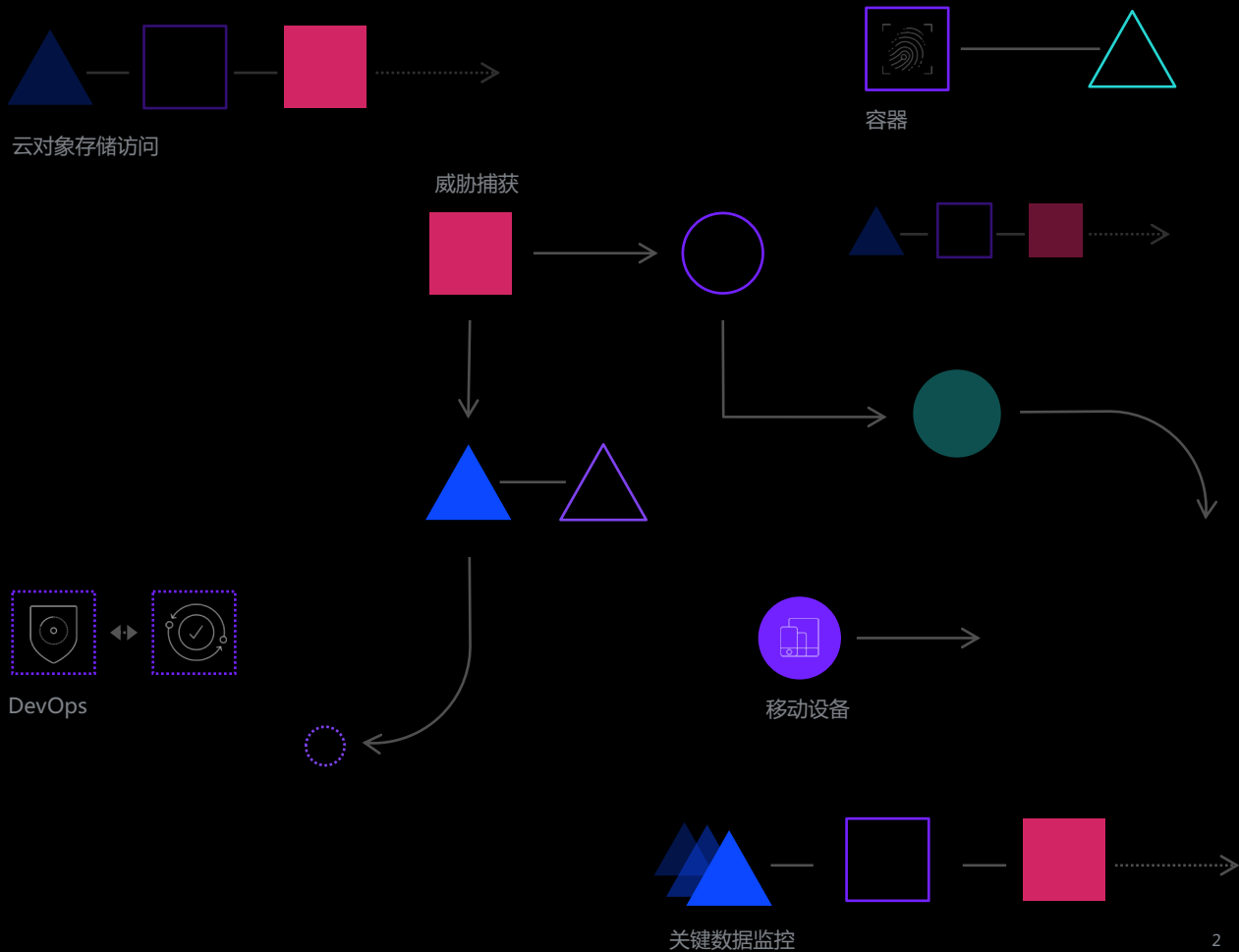
专为混合多云世界而构建的互联安全

IBM Security

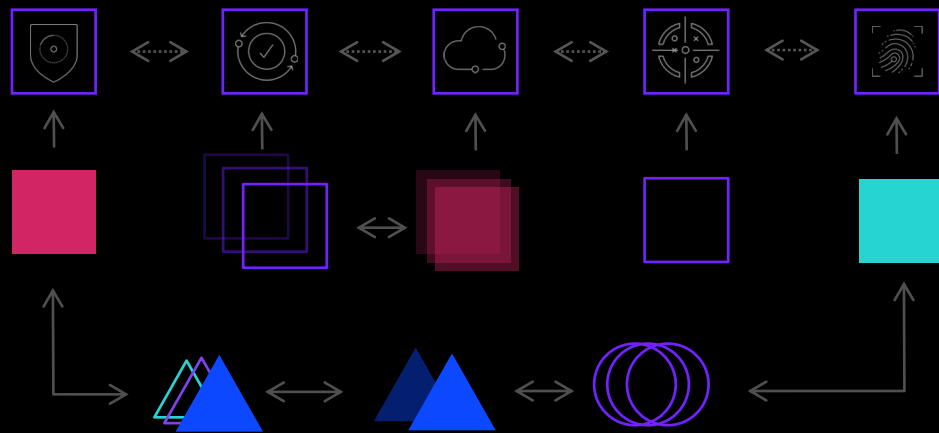
依照 NDA 之规定共享



安全性因多云环境变得分裂、无关联且更趋恶化



如果安全性
变得统一且
相互关联，
情况将会怎样？



随处运行

获取安全洞察力

更快采取行动

开放连接

连接数据

连接 workflow

随处运行

开放连接

- 随处运行
- 根据需要增加并调整投资
- 减少供应商锁定
- 促进可互操作性

获取安全洞察力

连接数据

- 发现潜在威胁
- 作出更明智的基于风险的决策
- 原地存储数据
- 充分发挥投资的价值

更快采取行动

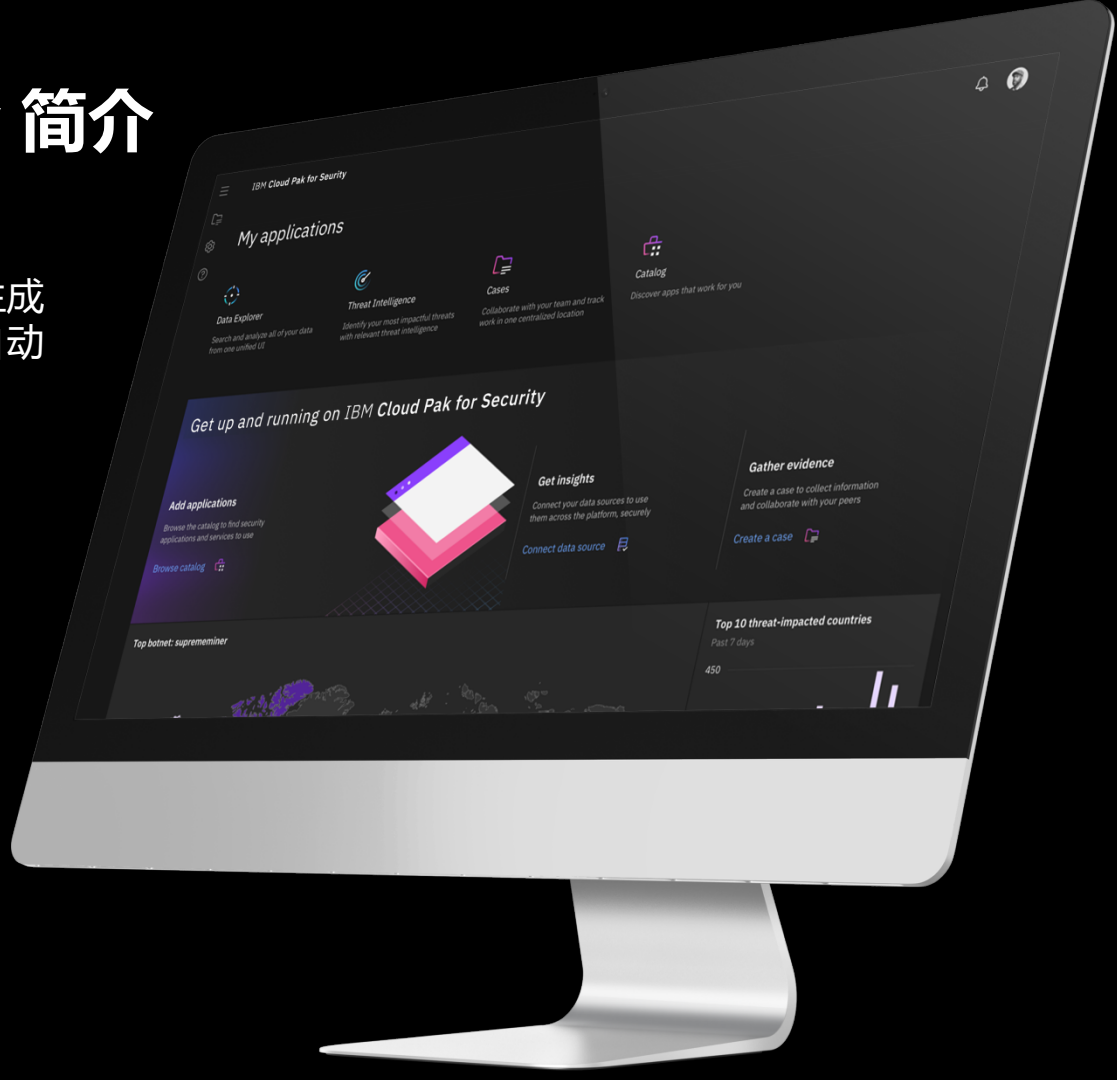
连接 workflow

- 团队和业务部门更快地作出响应
- 编排各种安全用例
- 降低集成成本
- 拓展团队能力

Cloud Pak for Security 简介

一个有助于您更快集成现有安全工具，进而生成更深入威胁洞察力、编排行动并实现响应自动化，同时确保原地数据存储的平台。

- 混合多云架构
- 互联的开放生态系统
- 自动化和编排



Cloud Pak - 面向企业的云软件

将核心业务应用迁移到任何云端的开放、速度更快、更安全的方式
—— 借助面向企业的容器化解决方案

IBM 容器化软件

与开源组件进行打包，预先与通用运营服务相集成并在设计上确保安全



容器平台和运营服务

日志记录、监控、安全、身份访问管理



完整但简单

完全模块化、易于使用

经过 IBM 认证

完全的软件堆栈支持，同时确保持续安全性、合规性和版本兼容性

随处运行

可在内部、私有云、公有云和预集成的系统上运行



Google Cloud



Edge



Private



Systems



统一的数据服务

获得完整洞察力同时确保原地数据存储

开放的合作伙伴生态系统

在现有安全基础架构中安全连接第三方工具



混合多云平台

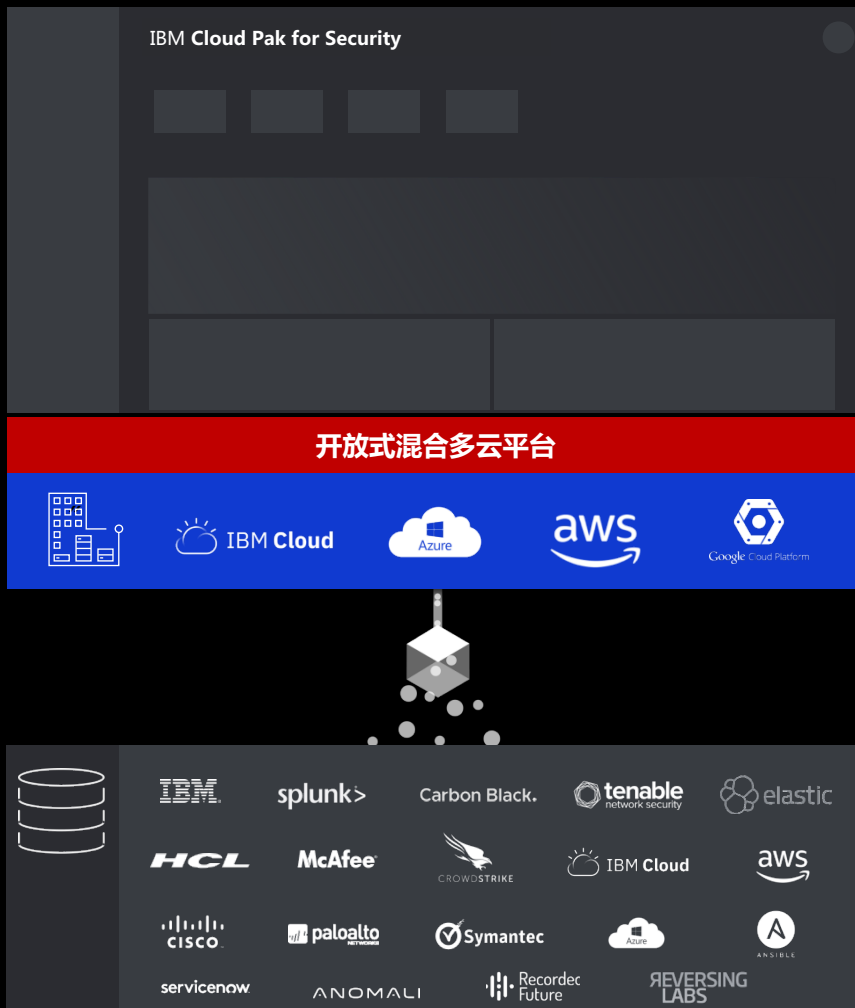
面向公有云、私有云和混合云的、随时可部署、随处可运行的现代化开放架构，

统一的数据服务

获得完整洞察力同时确保原地数据存储

开放的合作伙伴生态系统

在现有安全基础架构中安全连接第三方工具



统一的界面和设计系统

统一的使用体验，降低培训成本，更快地构建应用

成效驱动型解决方案

开箱即用的安全业务流处理能力，并由编排和自动化加以辅助

混合多云平台

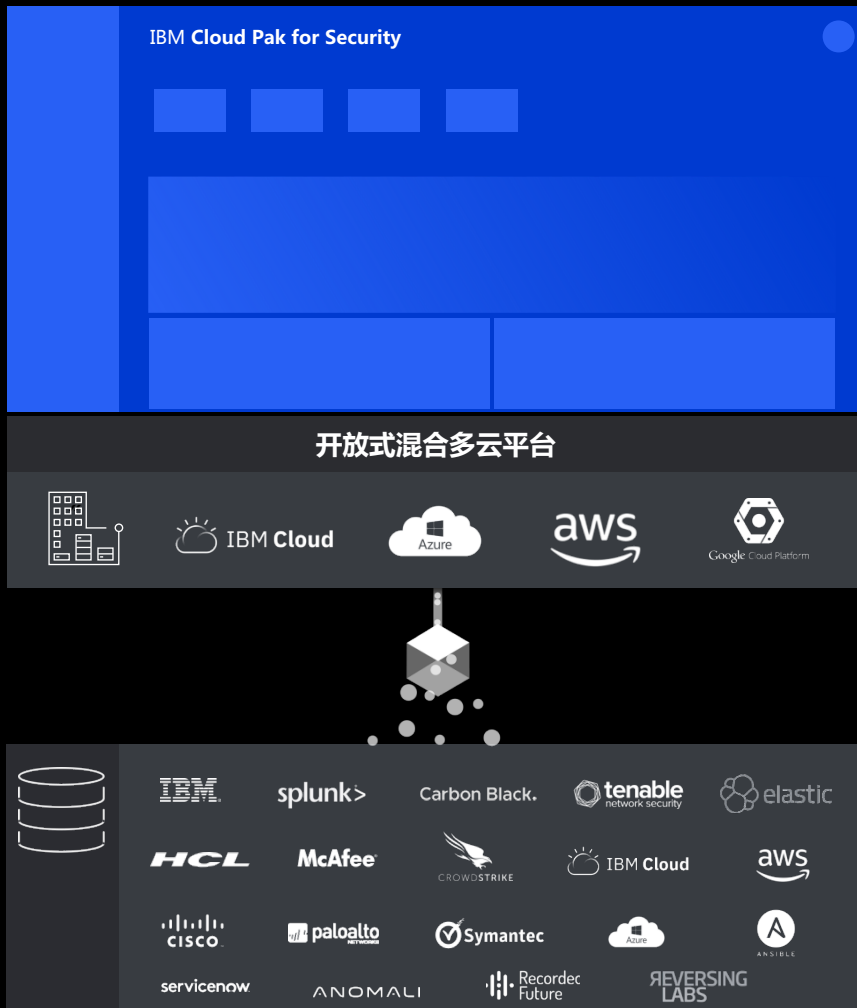
面向公有云、私有云和混合云的、随时可部署、随处可运行的现代化开放架构，

统一的数据服务

获得完整洞察力同时确保原地数据存储

开放的合作伙伴生态系统

在现有安全基础架构中安全连接第三方工具



IBM Cloud Pak for Security - 2019

随处运行

获取安全洞察力

更快采取行动

跨领域安全解决方案

核心平台服务

混合多云架构

与现有安全工具的开放集成

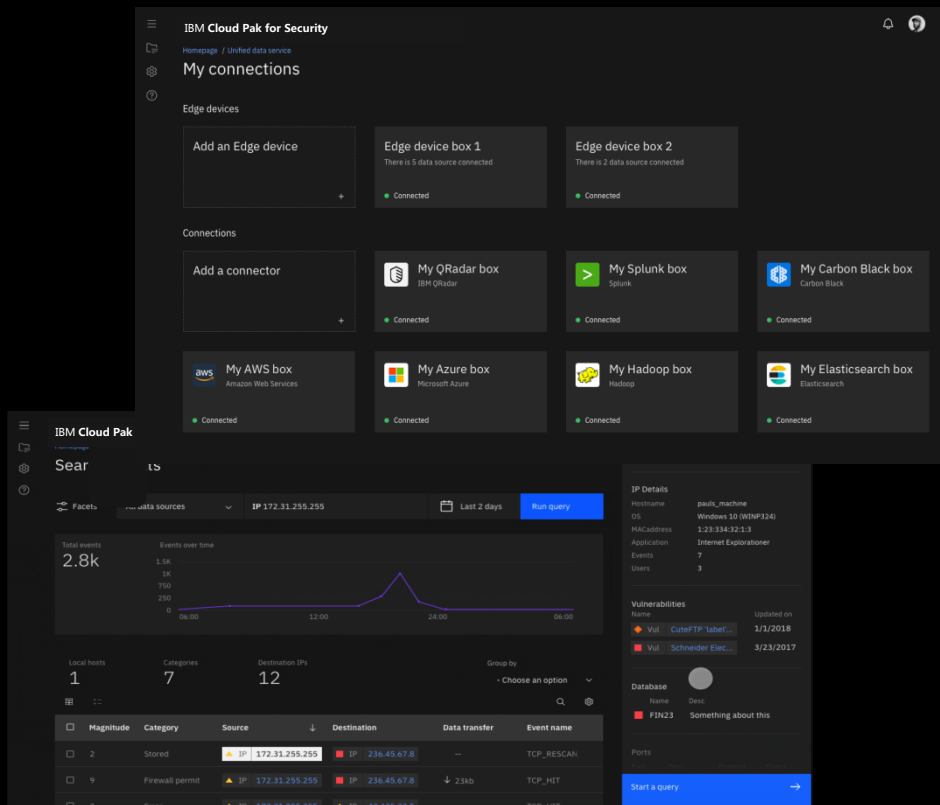
IBM Security / © 2019 IBM Corporation



*在试用启动后可用

联合搜索和调查

- 使用连接器将**关键安全数据**连接到云和安全数据源，同时**无需移动数据**
- 对多个数据源运行查询，同时**无需移动数据**
- 在单个统一的界面中进行调查，以**搜索威胁和 IOC**
- 对所有连接的数据进行强大的搜索，以**发掘洞察力**，同时**确保数据在原位存储**
- 通过案例管理功能**无缝跟踪调查**
- 借助 SDK 或 IBM 服务构建新的连接器，进而**扩展数据源和功能**



事件响应

- 通过 IR 流程自动化**缩短响应时间并补救复杂网络威胁**
- **简化手动的重复性任务**（如 IOC 扩充）并实现其自动化
- 通过强大的案例管理功能和任务，以一致的方式**指导并执行调查与响应活动**
- 通过引导分析师的响应，**让分析师优先处理高价值的调查和响应活动**
- 通过广泛的第三方应用和集成件**推动整个组织范围内的调查**
- 通过可视化工作流编辑器**定制并扩展运行手册**

The screenshot displays the 'Fake AppleID Phishing Email' incident details in the IR console. The interface includes a top navigation bar with tabs for Tasks, Details, Breach, Notes, Members, News Feed, Attachments, Stats, Timeline, Artifacts, and Email. The 'Details' tab is active, showing a description: 'This has fooled a number of employees because it looks so real!'. Below this, there are sections for 'Basic Details' (Name, Description, Incident Type, NEST Attack Vectors, Incident Disposition, Phase, Resolution, Resolution Summary, Owner, Created By) and 'Date and Location' (Date Created, Date Occurred, Date Discovered). On the right side, there is a 'Summary' section with fields for ID, Phase, Severity, and various dates. Below that is a 'People' section listing the creator and owner as 'Muddy Admin'. At the bottom right, there are sections for 'Related Incidents' and 'Attachments'.

The screenshot shows the 'Activity Dashboard' for the 'Fake AppleID Phishing Email' incident. It features a 'News Feed' section with a vertical timeline of actions:

- 2 minutes ago: Muddy Admin wrote a note on the incident Fake AppleID Phishing Email. The note content is: "We have seen so many of these emails within our organization - can we confirm it."
- 4 minutes ago: Muddy Admin modified the incident Fake AppleID Phishing Email.
- 5 minutes ago: Muddy Admin updated the task list on the incident Fake AppleID Phishing Email.
- 5 minutes ago: Muddy Admin created the incident Fake AppleID Phishing Email.

 To the right of the news feed, there are sections for 'Tasks Due Soon' (stating 'You have no tasks due soon.'), 'Need Help?' (with a 'Documentation' link), and 'Resource Library' (with a link to 'Comprehensive resources for breach notification rules and security incident response best practices.'). A 'Show Types' dropdown menu is set to 'All'. The footer indicates '© Copyright IBM Corporation 2019'.

开放性是未来趋势所在

专为开放性而 构建

- 开放生态系统/数据连接器
- 开源计划
- OASIS 开放网络安全联盟

智能化、量身定制

由专家提供 支持

- 连接器开发
- 按需访问相应的专业知识
- 综合性战略咨询

专为混合多云世界而构建的 互联安全解决方案

随处运行 | 获取安全洞察力 | 更快采取行动



Cloud Pak : 针对云计算场景预集成的软件包

目前, IBM 为客户提供了首批的 5 个 Cloud Pak

Cloud Pak for Applications

构建、部署和运行应用

Cloud Pak for Data

收集、组织和分析数据

Cloud Pak for Integration

集成应用、数据、云服务和 API

Cloud Pak for Automation

推动实现业务流程、决策和内容的转型

Cloud Pak for Multicloud Management

多云可视性、治理与自动化的

IBM 容器化软件



开放式混合多云平台



IBM Public Cloud



AWS



Microsoft Azure



Google Cloud



Edge



Private



IBM Z
IBM LinuxOne
IBM Power Systems

Cloud Pak : 针对云计算场景预集成的软件包

Cloud Pak for Security 可帮助企业以现代化、敏捷的方式确保混合多云环境的安全

Cloud Pak for Applications

构建、部署和运行应用

Cloud Pak for Data

收集、组织和分析数据

Cloud Pak for Integration

集成应用、数据、云服务和 API

Cloud Pak for Automation

推动实现业务流程、决策和内容的转型

Cloud Pak for Multicloud Management

多云可视性、治理与自动化

Cloud Pak for Security

实现安全数据、工具和团队的互联

IBM 容器化软件



开放式混合多云平台



IBM Public Cloud



AWS



Microsoft Azure



Google Cloud



Edge



Private



IBM Z
IBM LinuxOne
IBM Power Systems

关注我们

<https://www.ibm.com/cn-zh/security>

<https://www.ibm.com/cn-zh/products/cloud-pak-for-security>

<https://www.ibm.com/cn-zh/security/services/cloud-security-services>

© Copyright IBM Corporation 2019. All rights reserved. 本材料中所含信息仅供参考之用，而且按现状提供，不包含任何明示或默示的保证。本材料中有关 IBM 未来发展方向的声明仅代表 IBM 当前的意图，在未来可能会有变更或撤销，且仅用于说明目标之用。IBM、IBM 徽标及其他 IBM 产品和服务是 International Business Machines Corporation 在美国和/或其他国家/地区的商标。其他公司、产品或服务名称可能是其他公司的商标或服务标记。

良好的安全实践声明：IT 系统安全涉及通过对来自企业内外部的非法访问进行阻止、检测和响应来保护系统和信息。非法访问会导致信息变更、损毁、盗用或滥用，或导致对您的系统的破坏或滥用，包括用于对他人的攻击。没有任何 IT 系统或产品可被视为完全安全，也没有单一产品、服务或安全措施可完全有效地阻止非法使用和访问。IBM 系统、产品和服务设计为合法、全面的安全方法的一部分，该方法必然涉及其他操作程序并可能需要其他系统、产品或服务，以达到最大效力。IBM 不保证任何系统、产品或服务可免受，或使企业免受任何一方的恶意或非行为的影响。

致电IBM安全解决方案顾问免费咨询：400-810-1818转2395 陈梦琳