全面的数据保护：普遍加密案例

基于 IBM 赞助的 Solitaire 研究的精选数据

数据泄露损害业务发展

- 失去客户：**78%** 的客户在发生数据泄露之后就会一去不返。[1]
- 损失利润：每次数据泄露平均造成 **390** 万美元的损失。[2]

通过加密保护数据

加密是**防范数据泄露最有效的**手段之一。自 2013 年以来发生的 140 多亿起记录中，只有 4% 的数据得到了加密。[3]

加密可将数据泄露的平均**成本降**低近 32 万美元。[2]

理想情况下，**要对每个数**据进行加密。这种做法被称为“全加密”或“普遍加密”。

但全加密实施起来困难重重

Solitaire 发现，**加密会占用大量计算能力**，并且那些运行 x86 架构的企业通常只会选择性地加密最敏感的数据。[2]
但即便是这种加密水平也需要大量技能、资源和预算才能得以实施和维持。它同样也会带来诸多挑战：

如何区分要加密的数据?

找出并分类要加密的数据需要付出大量时间和人力。

在哪里进行加密?

加密应该操作系统内部、在数据库级别、在应用程序里还是在网络上进行? 无论在哪里进行加密，都会影响效率、成本和复杂性 — 并且可能需要更改应用程序。

谁负责进行加密?

数据加密可能会涉及到整个组织。哪个业务职能部门可以获得企业级数据保护和加密策略?

IBM Z® 让普遍加密成为现实

对于大多数 x86 架构而言，普遍加密都难以落实。

基于 IBM 赞助的 Solitaire 研究数据

IBM Z 让您能够：

优化
安全保护，保护能力是同类平台的 8.5 倍以上。[4]

降低加密
成本，与同类平台相比，整体成本降低 93%，投入减少 81%。[4]

加密速度更快，
与其他同类产品相比，加密速度提高 18.4 倍。[4]

减少需要，
应对入侵威胁的需要减少 87.2%，响应时间缩短 85.8%。[4]

降低
复杂性，威胁减少 92%， 易受攻击的拓扑从 2,423 点减少至 196 点

数据是您最重要的资源。IBM Z 普遍加密技术可比同类网络安全解决方案更高效地保护数据。

了解普遍加密如何成为数据加密策略的中流砥柱。

了解更多信息

立即开始使用

IBM

业务代表为您服务：
400 810 1818 转 5139

注册告诉我们您的需求：
https://ibm.biz/Bd2ZcV

敬请访问网站：
https://ibm.biz/BdzZAs

1. 越过数字化山丘 - Solitaire企业数字化报告核心洞察：https://www.ibm.com/account/reg/cn-zh/signup?formid=urx-35233
2. Ponemon Institute - 2017 数据泄露成本调研：https://www.ibm.com/downloads/cas/861MNWN2
3. Breach Level Index: https://www.breachlevelindex.com. Accessed 11 October 2018; written approval to use source received 10 October 2018.
4. Solitaire 分析报告 - 该报告介绍了普遍加密为什么是全新的保护范式：https://www.ibm.com/account/reg/cn-zh/signup?formid=urx-33908