



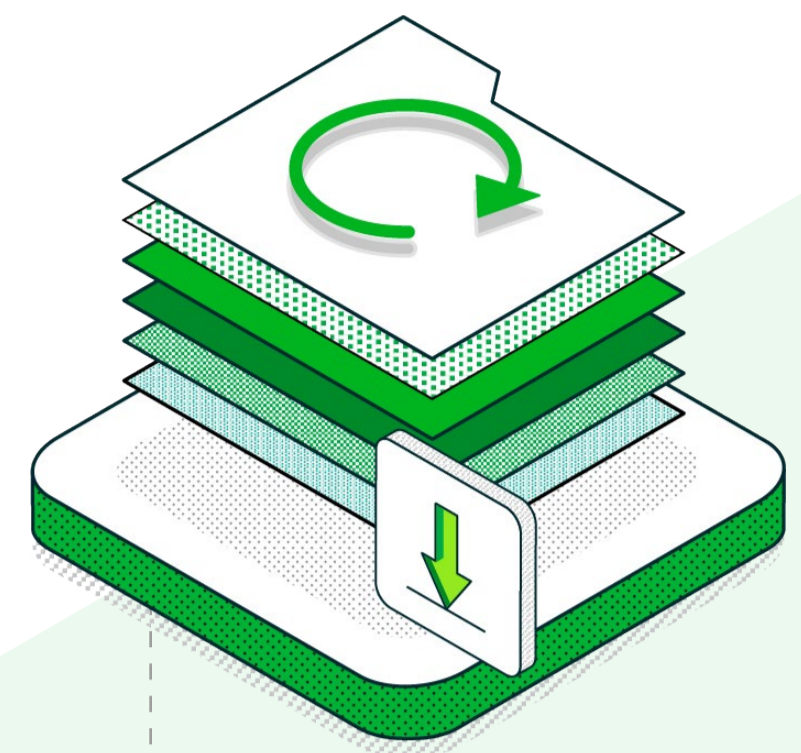
# 2023年数据保护趋势

2022 年底，一家独立研究公司针对数据保护驱动因素、挑战及策略，面向 4,200 名无偏见 IT 领导者和实施者（其中 277 人来自中国）展开了一项调研。以下是受访者反映的影响中国地区数据保护实践的一些关键统计数据。

## 预计 2023 年数据保护方面的增量投资将发生重大转变

预计 2023 年，组织的数据保护预算将增加

# 6.4%

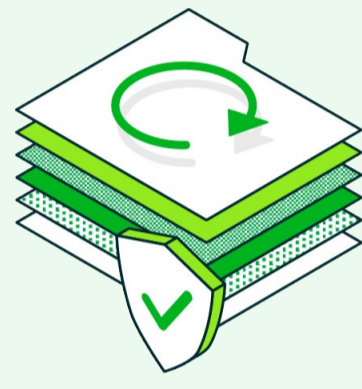


# 53%

的组织预计将于 2023 年更换其备份解决方案

## 更换的主要驱动因素是寻求更高的可靠性和可恢复性，部分原因在于其现有数据保护策略不尽如人意

# 44%



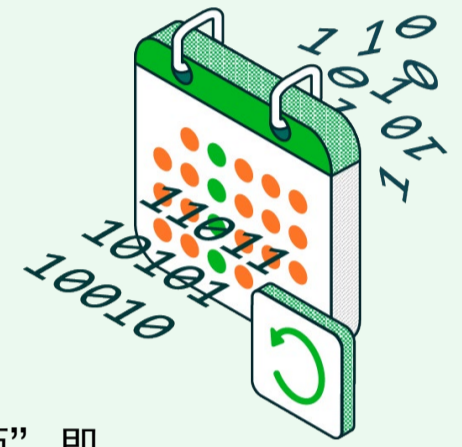
表示他们更换备份解决方案的动机是“提高备份的可靠性/成功率”

# 86%



的组织存在“可用性差距”，即所需的恢复运行时间和IT部门能够实现的时间差

# 87%



的组织存在“保护差距”，即可承受的数据丢失与 IT 部门数据备份频率之间的落差

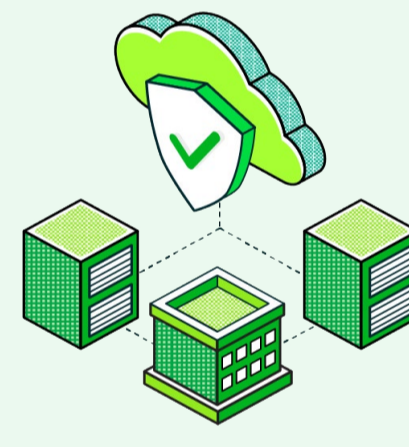
## 勒索软件及其他 BC/DR 事件仍然是组织面对 2023 年最关注的一个问题

# 76%



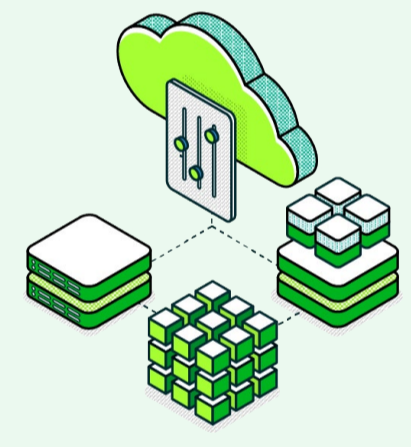
的组织在 2022 年遭遇至少一次勒索软件攻击

# 87%



认为已基本或完全整合了其网络和 BC/DR 策略

# 29%



认为基于云的和/或编排的 DR 是现代数据保护解决方案的最重要能力

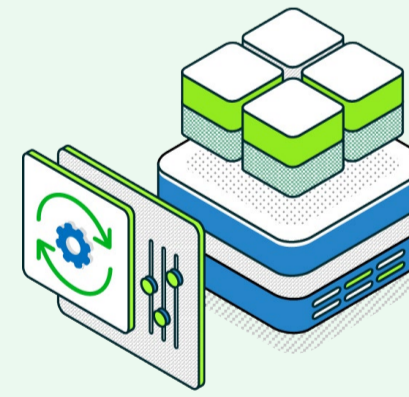
## 也许 2023 年影响数据保护策略的最具挑战性的趋势是不同规模的组织广泛使用混合 IT 环境

# 30%



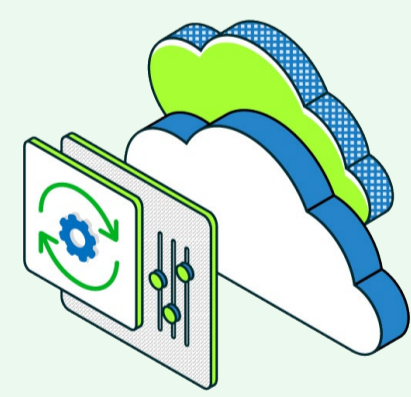
物理服务器

# 24%



虚拟机

# 46%

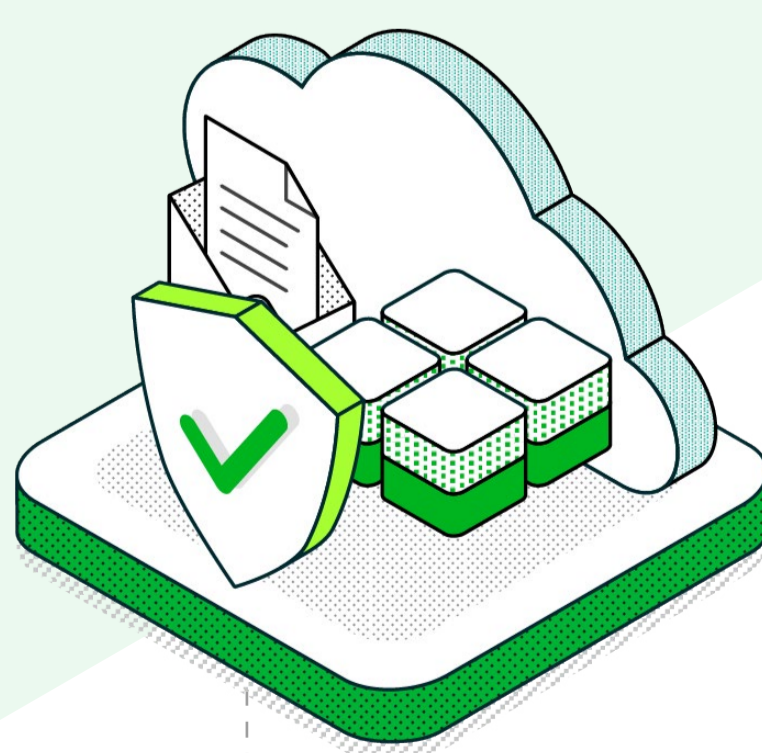


云托管平台

## 在生产和保护方面增加云技术使用也是 2023 年数据保护的主要驱动因素

# 19%

的组织正寻找下一个企业级备份解决方案，以“保护 IaaS 和 SaaS 工作负载”



# 86%

的组织预计将在 2025 年前将云服务作为其数据保护解决方案的一部分

