全球数据保护指数

网络弹性之多云版

了解网络威胁、多云、生成式 AI、运营复杂性等因素带来的影响

导致运营中断的数据保护难题日益增多，其中公有云和网络攻击成为被重点关注的领域。不断推进数据保护现代化的组织在寻求数字化转型的过程中，能够尽可能降低风险并提升信心。

组织普遍对现有数据保护措施表示担忧，并且对其缺乏信心，这使得组织处于弱势地位

60%
的受访者对其组织能够实现备份与恢复服务级别目标不是很有信心

79%
的受访者担心他们将在未来 12 个月内经历中断性事件

2.17TB
过去 12 个月内，**平均丢失**了 2.17 TB 的数据，平均**损失达 261 万美元**

74%
的受访者担心，即使采用了不可变的健全的备份和恢复措施，他们的**备份数据也仍旧可能受到感染或损坏**

网络攻击构成了持续存在且日益严重的威胁

55%
的受访者表示，他们的组织在过去 12 个月内经历过网络攻击或网络相关事件。**组织平均损失达 192 万美元**

75%
的受访者担心，其组织现有的数据保护措施可能不足以应对恶意软件和勒索软件威胁

69%
的受访者对于在发生重大破坏性网络攻击时，恢复所有业务关键数据的能力不是很有信心

尽管如此，59%
的组织在网络预防方面的投资仍然多于网络恢复

人工智能在提高组织的网络弹性方面颇具潜力，但是组织对数据保护存在担忧

42% 的受访者表示，他们的组织正在投资 AI 技术，以期能够更好地抵御攻击

52% 的受访者认为，**生成式 AI** 起初可以为抵御网络犯罪的**组织带来优势**

88%
的受访者一致认为，**生成式 AI** 将**产生大量新数据**，需要采取保护措施来确保其安全无虞

在使用公有多云环境时，安全性是组织的一大顾虑

79%
在更新或部署应用程序时使用**混合云或公有云**的组织中，有 79% 的受访者对其**组织能够保护各公有云中的所有数据**表示**信心不足**

40% 的受访者表示，在公有多云环境中**维护数据**时面临着**数据安全**方面的挑战

大多数受访者认为，实现混合云和多云运营的最重要能力包括：

58% **保护多工作负载环境**

56% **确保网络安全**

组织需要外部支持来保护其工作负载并确保拥有备份能力

在聘请云服务提供商来保护其工作负载的组织中，**95%** 的组织表示他们会为此**专门签订一份单独的合同**

60% 的受访者表示，他们的组织在某种程度上使用其云服务提供商提供的**备份和恢复工具**

50% 的组织引入了外部支持，包括网络恢复服务，以提高网络弹性

Dell Technologies 致力于提供网络恢复、备份、灾难恢复、长期保留等功能，旨在帮助您保护所有数据和应用程序。

详细了解戴尔现代、简单且富有弹性的多云数据保护：

DELL Technologies

Vanson Bourne 在 2022 年 9 月和 10 月期间进行了这项调查。受访者是来自拥有超过 250 名员工的私营和公共组织的 IT 及 IT 安全决策者。总计 1,500 名受访者，来自四个地区 – 300 人来自美洲地区（美国、墨西哥和巴西）、675 人来自欧洲、中东和非洲地区（英国、法国、德国、意大利、南非和阿联酋）、375 人来自亚太及日本地区（澳大利亚、印度、日本、新加坡和韩国）、150 人来自中国大陆地区。

受 Dell Technologies 委托

来源：Dell Technologies Innovation Index。2023 年 10 月。