APAC 版

THALES
Building a future we can all trust

2022 Thales 数据威胁报告

在混合办公、勒索软件和加速云转型的时代
领航数据安全

#2022DataThreatReport

safeploy.com

数据蔓延：我的数据到底在哪里？

16%

2022 年，只有 16% 的 APAC 受访者完全知道他们的数据存储在哪里

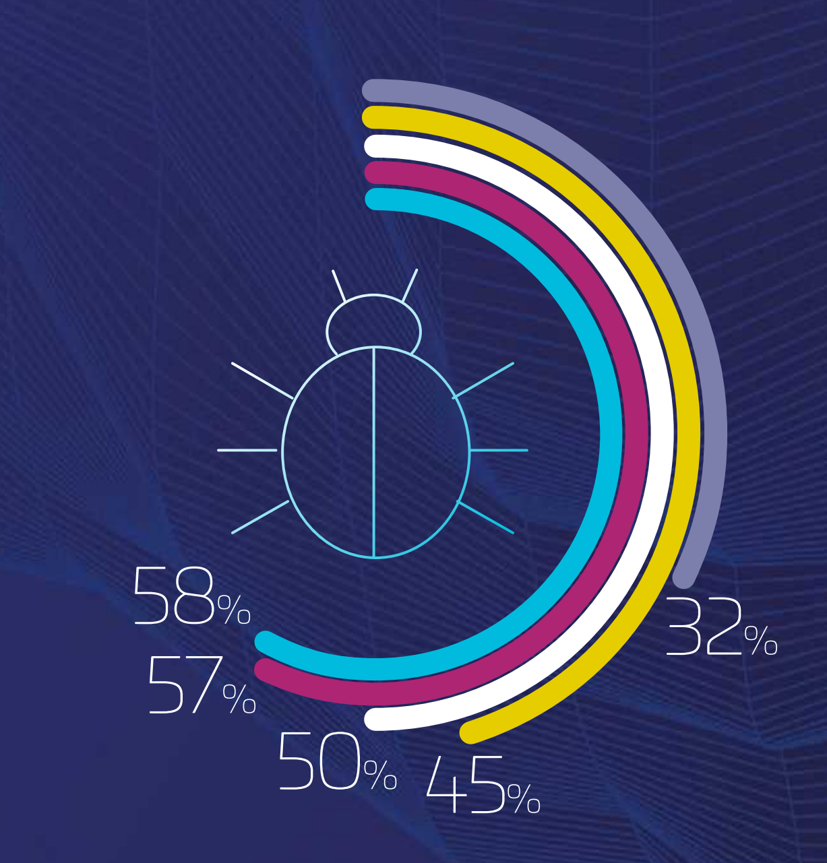
48%

的受访者表示，他们至少加密了 40% 的敏感云数据

21%

的受访者表示，他们至少加密了 60% 的敏感云数据

破坏和安全威胁使其复杂性增加



- ● 勒索软件被列为不断增长的安全攻击的主要来源
- ● 恶意软件被列为不断增长的安全攻击的主要来源
- ● 拒绝服务被列为不断增长的安全攻击的主要来源
- ○ 过去经历过一次安全损失
- ● 在过去 12 个月里经历了一次损失

勒索软件改变破坏经济的方式

24%

的企业称遭遇勒索软件攻击

27%

被勒索软件攻击的企业认为对运营产生了重大影响

只有 47%

的受访者已经或将要实施适当的勒索应对方案

云动量

51%

的受访者表示，他们至少有 40% 的数据位于云中，19% 的受访者表示超过 60% 的数据位于云中

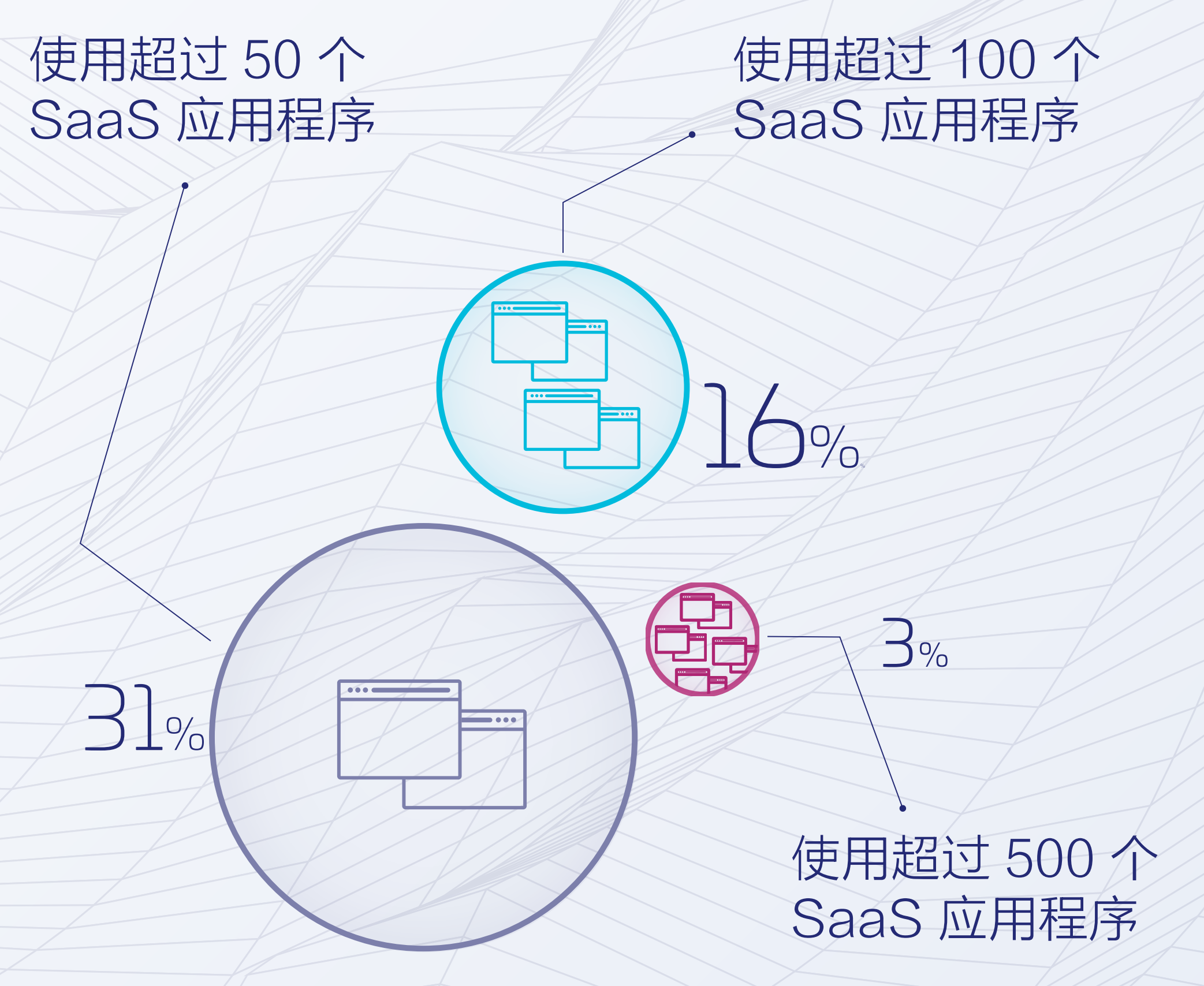
53%

的受访者表示，至少 40% 存储在外部的数据是敏感数据

26%

的人报告他们的云存储数据中超过 60% 是敏感数据

多云环境



零信任策略

30%

零信任在很大程度上塑造了他们的云安全策略

48%

的人依赖零信任安全策略的部分“概念”

量子计算

关于量子计算最常见的三个问题

57%

网络加密风险

54%

今天数据的未来解密

52%

未来加密破坏

持续远程工作时代的安全风险和威胁

安全远程访问解决方案的特点

24%

高度自信

34%

非常自信

26%

略微自信

16%

完全不自信

零信任世界的数据安全

在任何地方发现和分类数据

保护储存、传送和使用中的敏感数据

控制用户对敏感数据的访问和密钥的整个生命周期管理

访问 www.safeploy.com 或公众号下载完整的报告，包括 451 Research 的建议。

451 Research
S&P Global
Market Intelligence

资料来源：来自标普全球市场财智所属 451 Research 的 2022年 Thales 数据威胁定制调查（由 Thales 委托）