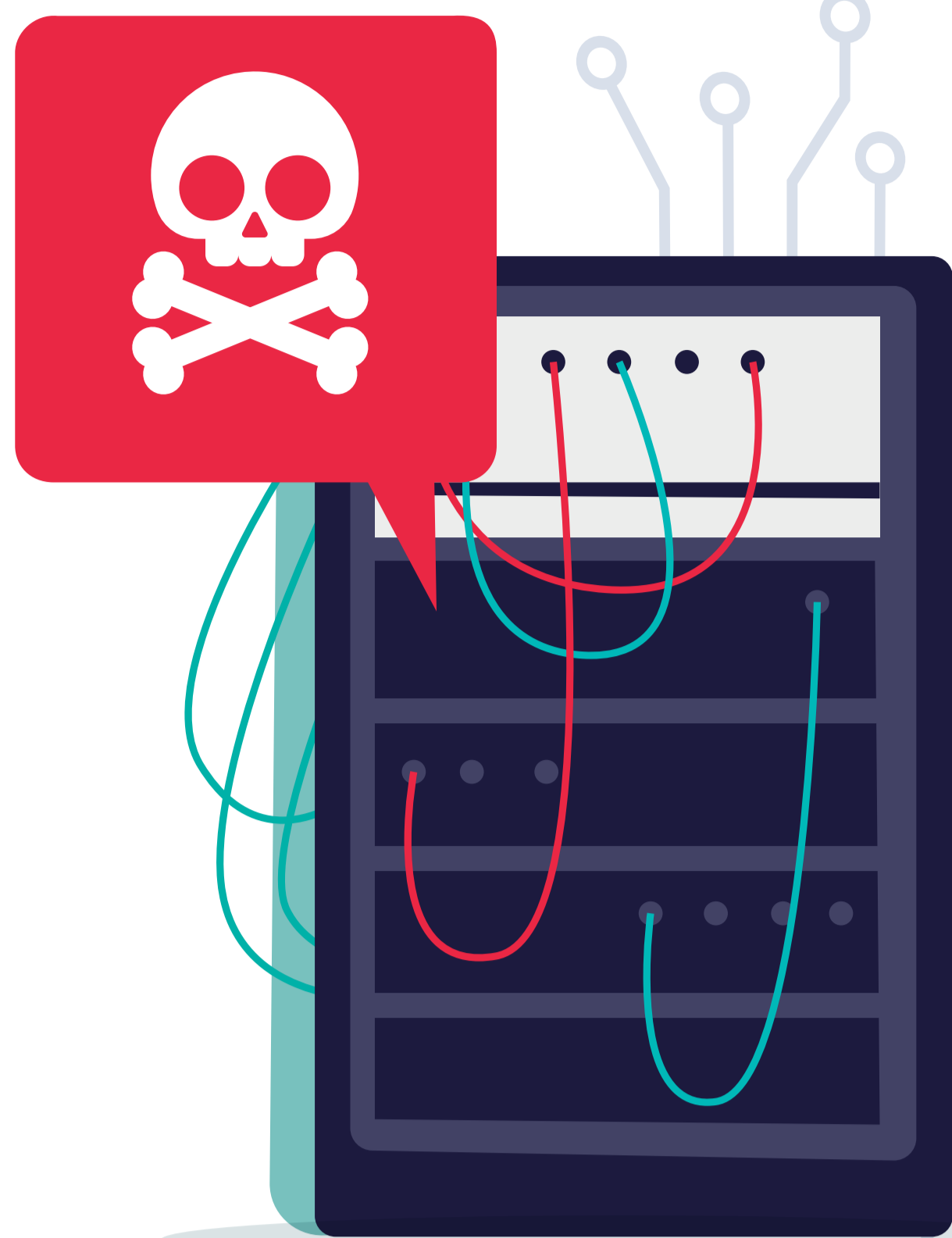


勒索软件抗风险能力

勒索软件攻击是一种重大危险

根据Forrester Research的调查,过去一年针对企业的勒索软件攻击数量增加了500%,对企业造成的损失超过115亿美元。



一切尽在数字之中...

全球超过**72%**的企业受到勒索软件攻击的影响。*

90%遭受攻击的组织都是中型企业,即收入不足10亿美元的企业。**

除赔付外,勒索软件攻击平均造成的损失在2023年上升至**513万美元**。***

勒索软件的勒索严重程度达到历史新高,平均损失金额超过**365,000美元**。****

*2023年Statista报告
**2023年Gartner报告
***2023年Fisher Phillips报告
****2023年Coalition Cyber Claims报告

备份是您的最后一道防线

NetVault Plus可保护您的生产数据和备份,帮助确保快速进行恢复并提高勒索软件抗风险能力

CDP和即时还原

降低数据丢失和业务停机的风险。

不可变的备份

防止在保留期内更改或删除关键备份数据。

异常检测

使用机器学习算法检测备份和恢复期间的任何异常行为并发出相应警报

对象和云锁定

安全备份存储在云中且不可改变。

“隔空”备份

备份到磁带以提供“隔空”保护。

数据加密

对传输中的数据和静态数据进行加密。

未发布的存储协议

数据不会被浏览,也不会公开广播。

备份复制

将备份复制到异地和云中以实现冗余。

多因素身份验证

保护您的备份系统免遭未经授权的访问。

重复数据删除

将本地和云备份存储成本降低高达93%。



[了解详情](#)

其他资源

[阅读我们的勒索软件技术简报](#)

[阅读我们的勒索软件白皮书](#)

[了解NetVault Plus](#)