

勒索病毒最新趋势和应对措施常见问题解答

序号	问题	答案
1	能否总结一下防范勒索病毒的宗旨?	总结来说两点: 1. 数据集中, 把所有数据集中到最安全的存储上; 2. 对于存储进行全面的保护并且确保恢复措施; 通过黑白名单设置、主动学习行为监控, 结合联想凌拓存储确保存放于NAS上的重要资料安全, 免受勒索病毒侵犯, 同时进行必要的备份, 防止关键数据丢失。
2	杀毒软件对勒索病毒有用吗?	作用相对有限, 杀毒软件实现原理是根据病毒特征码进行匹配和监控, 以确保终端安全, 需要及时更新病毒库定义并开启监控, 这些操作会消耗系统资源降低服务性能。最关键的是杀毒软件是被动的防御, 只能抵挡外来的已定义病毒, 而无法阻挡病毒的传播, 当新的病毒特征出现时, 没有及时更新病毒库的终端就成了潜在的传播者, 当这些传播者进入生产网络, 后果将不堪设想。
3	联想是否提供相关的培训?	不知道您需要什么内容的具体培训, 建议您联系我们的400热线电话: 400-116-0099, 告知详情, 我们的售前工作人员会向您提供专业的建议。
4	相关PPT能分享下么?	会后我们会将会议PPT资料和其他详细资料, 通过电子邮件的形式发送给您, 请注意查收您的邮箱。同时, 我们也会将会议资料更新到联想凌拓官网: lenovonetapp.com 首页下方的在线研讨会专栏中, 敬请查看。
5	请将凌拓的设备白皮书发给我。	您好, 感谢您对联想凌拓的关注。您可以登录如下地址, 直接下载联想凌拓防勒索病毒白皮书: https://lenovonetapp.com/pdf/ransomware.pdf 。
6	具体如何预防勒索病毒?	人防层面: 制订严格的信息访问及安全制度, 确保生产环境内外网物理分离, 通过培训使员工能基本辨别并避免打开钓鱼网站、邮件, 对于中毒后隐瞒不报或恶意传播病毒者, 依据《中华人民共和国信息安全法》追求其责任。 技防层面: 对于关键数据关键应用使用联想凌拓防勒索存储解决方案, 主动防御, 及时备份。具体可参考问题4、5。
7	备份磁带用什么读取?	备份软件提供读取接口。
8	希望能为我们提供更多专业知识信息。	感谢您的建议和反馈。联想凌拓后续会继续为您准备更多精彩内容和技术干货的分享, 欢迎您持续关注联想凌拓官网: lenovonetapp.com, 如果有任何技术问题, 也欢迎咨询我们的400热线电话, 400-116-0099。
9	解决方案在哪里下载?	您好, 请登陆联想凌拓官网产品页面, 了解方案详情: https://lenovonetapp.com/products/lenovo/datamanagement/DPA.html 。或者您也可以致电400热线电话: 400-116-0099, 告诉我们您的具体需求。
10	和杀毒软件等安全产品如何配合使用?	杀毒软件确保终端不受病毒感染, 避免做传播者; 硬件防火墙切断无关外链端口, 防止敏感信息泄露; 防勒索方案监控读写存取操作, 确保关键数据不被非授权用户访问, 同时屏蔽风险用户的风险操作; 备份解决方案是最后的支撑, 万一数据不幸丢失, 做到有备无患。
11	中勒索病毒, 有没有人承担责任?	主体不明晰, 虚拟货币不具备实名制, 无法追溯, 很难追责。
12	对于近两天爆发的incaseformat预防方案。	这是个蠕虫病毒。对于终端用户, 即时更新杀毒软件定义, 避免中招或者做潜在的传播者; 对于企业关键数据, 使用联想凌拓的防勒索解决方案中的主动学习模式, 监控并拦截异常的读写操作并及时阻断风险用户的风险操作, 同时及时备份, 确保数据安全。
13	如何防御勒索病毒, 如何做好数据安全, 特别是数据的有效备份及恢复?	合并问题18, 参考问题8。使用联想凌拓防勒索数据安全解决方案, 根据不同部门制订相应的黑、白名单访问策略, 对于高风险文件夹结合使用主动行为学习策略以阻挡风险用户及操作; 管理员及时关注操作日志, 及时发现风险用户来源及其访问轨迹; 结合联想凌拓存储的备份策略及时备份, 万一有数据被加密, 可快速恢复到最近一次修改前的状态。