产品简介

CipherTrust Transparent Encryption Ransomware Protection

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

勒索软件事件自2020年以来一直呈上升趋势。在所有数据泄露事件中，勒索软件占比达到了25%。[1]在遭受勒索软件攻击时，关键数据访问会被阻断，支付赎金才能恢复，这会使企业经营活动陷入停顿。预计到2031年，每两秒钟就会发生一起勒索软件攻击企业及个人的事件。[2]

使用下一代防火墙、安全电子邮件/网络入口等外围控制以及只专注关闭漏洞差距的基本安全措施并不足以防止勒索软件攻击事件。财富500强公司所面临的主要挑战是，保护关键业务数据不被终端和服务器上未经授权的进程和用户加密。

解决方案: CipherTrust Transparent Encryption Ransomware Protection

CipherTrust Transparent Encryption Ransomware Protection（CTE-RWP）提供了一种非侵入性的保护方式，它可以保护文件/文件夹免受勒索软件攻击。CTE-RWP会针对每个进程，监视存储关键业务数据的文件上的异常I/O活动。它允许管理员在勒索软件控制您的终端/服务器之前，针对可疑活动发出警告或阻止可疑活动。

关键优势

- **数据防护透明。**CTE-RWP会持续地以很低的资源消耗，针对每个卷设置强制性的勒索软件防护机制，无需修改终端/服务器上的任何应用程序。它会持续监控由勒索软件感染的进程所引起的异常文件活动，并在检测到此类活动时发出警报或阻止此类活动。
- **易于部署。**借助CTE-RWP，管理员只需启用勒索软件防护，无需针对每个文件/文件夹设置限制性访问控制和加密策略，这一功能在CTE许可证中可实现。
- **强大的勒索软件检测功能。**CTE-RWP会使用基于进程的机器学习模型来动态检测可疑的文件I/O活动。它会识别终端/服务器上的勒索软件，并发出警告或阻止勒索软件。用户还可以将已批准进程添加到受信列表中，以绕过监视。

授权

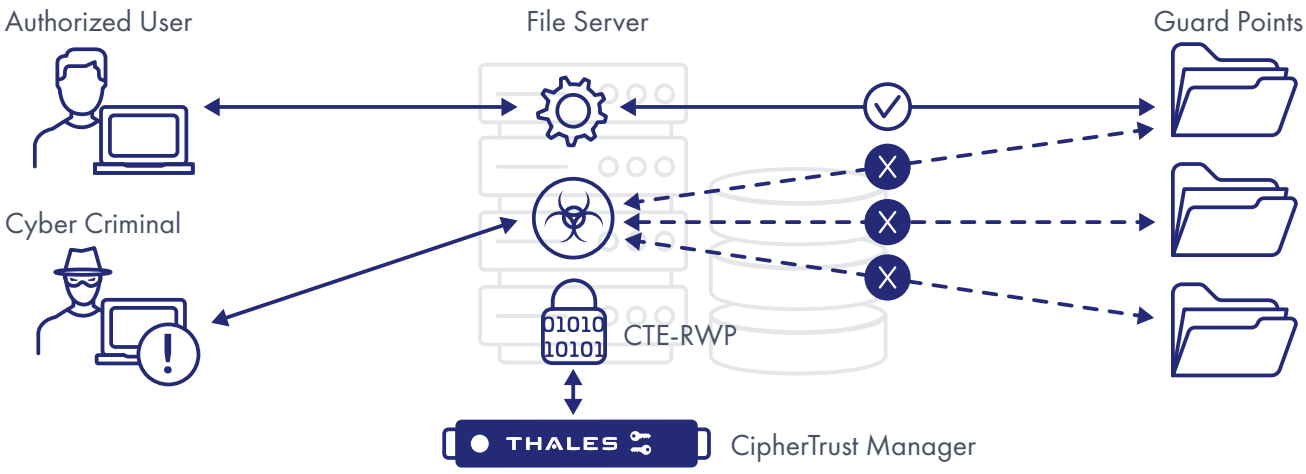
CTE-RWP会单独授权。它的勒索软件检测功能具有充分的细分级别，用户无需在每个终端/服务器上配置文件/文件夹级别的详细访问控制策略。结合CTE许可证，管理员还可以应用细粒度访问控制和加密策略。CTE-RWP可以单独授权，也可以结合CTE授权。

其他采用CipherTrust Transparent Encryption的勒索软件数据防护

客户可以通过添加CipherTrust透明加密(CTE)许可证，最大化其终端/服务器上的勒索软件防护，从而获得CTE-RWP并未提供的以下额外好处。

细粒度访问控制

- 定义有权加密/解密/读/写或列出关键业务数据所在目录的(用户/组)
- 针对备份进程设置严格的访问控制策略，包括对备份进行加密，防止数据泄露
- 保护文件的点级别的可信列表(二进制文件)，这些文件已被批准可访问并加密/解密受保护的文件夹，包括对受信任应用程序的签名进行检查，以确保其完整性。



CipherTrust Transparent Encryption - Ransomware Protection (CTE-RWP)

静态数据加密

- 对本地或云存储中的关键业务数据进行加密
- 使入侵者无法通过威胁发布将加密数据变现从而使关键数据对入侵者丧失价值
- 保护文件的点级别的可信列表(二进制文件)，这些文件已被批准可访问并加密/解密受保护的文件夹，包括对受信任应用程序的签名进行检查，以确保其完整性

针对CipherTrust Encryption使用MFA

客户可以为CipherTrust Encryption(CTE)添加多因素身份验证(MFA)，以获得额外的文件夹/文件级别的防护层。在系统管理员和特权用户试图访问保护点后的敏感数据时，CTE的MFA会提示系统管理员和特权用户，除密码外，出示另外的验证方式。

用于CTE的MFA可用于Windows平台。它支持与包括泰雷兹的SafeNet Trusted Access、Okta和Keycloak在内的多因素身份验证提供商集成。

关于 Thales

你所依赖的保护你隐私的人，他们依赖泰雷兹来保护他们的数据。当涉及到数据安全时，企业面临着越来越多的决定性时刻。无论这个时刻是建立一个加密策略，转移到云端，还是满足合规性要求，你都可以依靠泰雷兹来保障你的数字化转型。

为决定性的时刻提供决定性的技术。