西数科技
WEST DATA TECHNOLOGY
科 技 创 造 无 限 可 能

西数科技公众号

亡羊补牢 为时不晚

勒索病毒给我带来大量的损失，惨重的代价！

如何抵御勒索病毒？我们根据多年的应对病毒的网络安全实践经验，推荐：

推荐 1:重要的服务器一定要部署防护软件。

如何选择防护软件，目前来看多数客户安装的是 360，安全狗之类免费软件，实际情况看来，这些软件无法防范大部分新版的勒索病毒。有的客户居然没有安装防毒软件。

市场上支持安装服务器的 SERVER 版本都是要收费的，我们推荐卡巴斯基和 EAM 杀毒软件。

杀毒软件对比	支持服务器系统版本	价格（1 年升级）	优势	缺点
卡巴斯基 中小企业版	Windows Server 2008 2011 2012R2 不支持 2014 和 2016	2100 元	抵御未知恶意威胁，确保业务可以稳定运行	占服务器硬件资源。对操作系统版本有要求
EAM 专杀勒索病毒	WindowsServer2008 R2/2012/2012 R2, 2016	880 元/服务器 99 元 /PC	可以防勒索病毒，对服务器实时监控，检测到威胁自动隔离查杀。实时保护服务器数据	过滤机制过于严格，需要人工协助支持。
360	Windows、	9000 元	虚拟化方便管理	不能有效防范勒索病毒
瑞星	WindowsServer2008 R2/2012/2012 R2,	3160 元	可以满足企业整体反病毒需求	不能有效防范勒索病毒
安全狗	Windows all	免费		不能有效防范勒索病毒

公司地址：江苏省南京市玄武珠江路 435 号华海大厦 606 电话：025-83608636 传真：025-86883952

诺顿	WindowsServer2008 R2/2012/2012 R2,	6190 元	适合小型企业	只适用于网络规模简单的网络环境

EAM 的 Anti-Ransomware 防勒索杀毒软件介绍

EAM 的 Anti-Ransomware 保护层是为勒索软件定制的，用于检测勒索软件攻击的行为模式，并在您的文件被加密之前阻止它们。任何勒索加密程序的执行和下载将被拦截，其他反勒索软件解决方案依赖于重复加密的检测，因此您的最有价值的文件

特色功能：

1、反勒索病毒
定制构建的行为监控可以在加密宝贵的业务数据之前停止勒索软件。
2、实时文件保护
此实时保护层使用超快速“EAM”双引擎扫描程序检查所有下载和修改的文件。
3、行为拦截器
为了阻止尚未被签名知晓的全新威胁，“EAM”会持续监控所有活动程序的行为，并在发生可疑事件时立即发出警报。
4、冲浪保护
如果您无意中尝试查看传播特洛伊木马，间谍软件或任何其他类型的恶意软件的网站，“EAM”将阻止您连接并感染病毒。
5：数据安全技术支持,
6：修复漏洞补丁,提供病毒防护设置等技术支持和顾问，协助做好数据安全和防护。

获奖列表：

- 年度最受欢迎的 3 款产品 - AV-Comparatives，AT
- 17 x VB100 奖 - 英国 VirusBulletin
- AV-Test 认证，DE
- 3 x 46 中的第一名 - COMSS，RU
- 8 x 最佳测试 - 英国 MRG-Effitas
- 13 x“高级+”（最好） - AV-Comparatives，AT
- 年度防病毒 - 多个出版物

更多功能：

预防感染

File-Guard 扫描所有加载到工作站上或正在执行的文件。它使用了数百万已知威胁的签名，并且已经被主要的反病毒测试组织授予许多次。

阻止访问恶意和欺诈性网站

Surf Protection 可防止访问钓鱼网站，并在您要从危险网站下载恶意软件时显示警报。Surf Protection 适用于所有程序中的所有浏览器。

阻止使用行为拦截器进行工业间谍活动

针对个人攻击设计的自定义特洛伊木马经常被用来攻击企业，并且它们通常不会被传统的防病毒软件检测到。EAM 的行为阻止技术是针对此类威胁的有效措施。

勒索软件保护

自定义行为监控可以在加密任何文件之前停止勒索软件。勒索软件解密很少可能，因此防止感染是关键。

网上银行保护

包含的行为拦截器专门检测典型的网上银行木马的行为，如宙斯。

扫描并清理感染

双引擎扫描程序可查找并删除各种恶意程序。这是一个完整的防病毒软件包+针对特别高级变体的专门恶意软件清理例程。

找到定制的 rootkit

直接磁盘访问模式可检测隐藏在引导扇区中的 rootkit，为攻击者提供秘密访问。

删除可能不需要的程序（PUP）

许多免费软件程序会安装不需要的软件，例如修改搜索引擎和主页的浏览器工具栏。其他人在冲浪时添加不需要的广告。EAM 反恶意软件专门用于安全和有效地查找和删除这些 PUP。

通过命令行扫描

被称为是围绕最先进，最灵活的命令行界面之一，提供频繁扫描顶级性能。

管理用户权限

使用高级 Active Directory 连接权限系统限制非管理员用户对保护设置的访问。全局管理员密码也可以设置。

发送电子邮件通知

每当检测到恶意文件时即刻收到电子邮件通知，以便进行即时响应和进一步调查。

监视连接的存储设备

任何连接到工作站的新设备都会被实时保护自动覆盖 - 无需采取任何措施。

自动更新

EAM 反恶意软件每天至少提供 24 次新的检测签名，确保实现最佳保护。

保存您的硬件资源

您的工作站的能力属于您的业务，而不属于您的防病毒软件。EAM 反恶意软件资源非常少。

易于理解的配置

你不需要成为 EAM 的专家 - 但这并不意味着你不会找到很多惊人的专家功能。

认证的保护

EAM 反恶意软件已获得多项 VB100 奖项，多项 AV-Test 认证，并在所有正在进行的 AV-Comparatives 真实世界保护和检测测试的上半部分持续显示。

推荐 2：重要的服务器一定要部署异地备份。

防勒索病毒备份方案----------数据备份三原则：

如何构建中小企业廉价有效的防勒索病毒异地备份方案？

一般的企业备份方案和防勒索病毒备份方案有何不同？

1：防勒索病毒方案的备份机一定是 linux 系统，因为目前的勒索病毒攻击目标 95%以上都是 windows 系统。
2：备份方案一定是隔离的网络，而不是在同一个局域网，因为勒索病毒有很强的局域网攻击能力，他可以轻松渗透传播到局域网的其他主机。
3：快照功能的应用，由于病毒攻击了服务器，若没有及时发现，通常的备份方案也会将感染的文件备份到备份机，通过还原的数据还是被加密的状态，所以需要备份机具备快照回滚的功能，可以回滚的之前的任意时间点。
4：价位：一般的企业级备份方案都在 5 万 10 万以上，我们推出的防勒索异地备份方案在千元价位，具备大容量 8TB 和更高容量 RAID 磁盘阵列功能。

公司地址：江苏省南京市玄武珠江路 435 号华海大厦 606 电话：025-83608636 传真：025-86883952

防勒索病毒数据备份简易方案	**方案一**：防病毒数据异地备份设备方案 （包含备份主机硬件和软件） 1：2TB 存储空间（可自己加硬盘升级容量），2 盘位。2：2 核 CPU，Linux 智能系统。3：自动同步备份软件	1 台	2888	硬件一次投资永久使用
	方案二：防病毒数据异地备份设备方案 （包含备份主机硬件和软件） 1：8TB 存储空间（可自己加硬盘升级容量），4 盘位。2：4 核 CPU，Linux 智能系统。3：自动同步备份软件 。 4：支持系统快照功能，多版本快照。	1 台	8888	硬件一次投资永久使用

更多备份方案详情 请联系西数科技的工程师。**关注公众号获取最新病毒防范方案**

西数科技 WEST DATA TECHNOLOGY
科 技 创 造 无 限 可 能

南京西数科技有限公司：

本公司为中国数据恢复协会会长单位,中国最大的数据恢复安全产品和服务企业，擅长领域：数据恢复、数据备份、电子取证、司法鉴定、涉密恢复、数据安全等，提供产品和解决方案。

电话：025-86883952
网站：www.wdsos.com
邮箱：wd@wdsos.com
病毒防护数据备份业务联系 手机：18913825606 陈总