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

防勒索病毒-数据安全方案

南京西数科技有限公司

2019 年 09 月 28 日

公司地址：江苏省南京市玄武珠江路 435 号华海大厦 601 电话: 4006184118 网址:http://www.wdsos.com

目录

一、 项目背景

以 Internet 为代表的全球性信息化浪潮迅猛发展，信息网络技术的应用正日益普及和广泛，应用层次正在深入，应用领域也从传统的、小型业务系统逐渐向大型、关键业务系统扩展，典型的如行政部门业务系统、金融业务系统、企业商务系统等。伴随网络的普及，越来越多的企业、个人通过互联网进行重要数据的传输、商务活动的实现。因此网络安全问题也更加关键和重要。因为在开放的 Internet 上有形形色色的人，他们的意图也是多种多样的。如何使网络信息系统不受黑客和工业间谍的入侵，已成为企事业单位信息化健康发展所必需考虑和解决的重要问题。

最新统计数据显示，100 多个国家和地区超过 10 万台电脑遭到了勒索病毒攻击、感染。[2] 勒索病毒是自熊猫烧香以来影响力最大的病毒之一。WannaCry 勒索病毒全球大爆发，至少 150 个国家、30 万名用户中招，造成损失达 80 亿美元，已经影响到金融，能源，医疗等众多行业，造成严重的危机管理问题。中国部分 Windows 操作系统用户遭受感染，校园网用户首当其冲，受害严重，大量实验室数据和毕业设计被锁定加密。部分大型企业的应用系统和数据库文件被加密后，无法正常工作，影响巨大。

2017 年 5 月 12 日晚，中国大陆部分高校学生反映电脑被病毒攻击，文档被加密。病毒疑似通过校园网传播。随后，山东大学、南昌大学、广西师范大学、东北财经大学等十几家高校发布通知，提醒师生注意防范。除了教育网、校园网以外，新浪微博上不少用户反馈，北京、上海、江苏、天津等多地的出入境、派出所等公安网也疑似遭遇了病毒袭击。[9]　　中石油所属部分加油站运行受到波及。5 月 13 日，包括北京、上海、杭州、重庆、成都和南京等多地中石油旗下加油站在当天凌晨突然断网，因断网无法刷银行卡及使用网络支付，只能使用现金，加油站加油业务正常运行。[10]

截至 14 日 10 时 30 分，国家互联网应急中心已监测到约 242.3 万个 IP 地址遭受勒索病毒漏洞攻击；被该勒索软件感染的 IP 地址数量近 3.5 万个，其中中国境内 IP 约 1.8 万个。　　2017 年 5 月 15 日，珠海市公积金中心下发了《关于 5 月 15 日暂停办理住房公积金业务的紧急通知》，为有效应对 Windows 操作系统敲诈者病毒在互联网和政企专网大面积蔓延，对住房公积金业务数据和服务终端资料可能造成的安全威胁，珠海市住房公积金管理中心决定加固升级内外网络，暂停办理所有住房公积金业务。

陕西部分地市的交通管理网络也受到了勒索病毒爆发的影响，暂停了业务办理[12] 。此外，部分地区因“系统维护”发布相关通知，暂停办理交管、出入境等业务. 俄罗斯：内政部称约 1000 台 Windows 计算机

遭到攻击，但表示这些计算机已经从该部门计算机网络上被隔离。 英国：2017 年 5 月 13 日，全球多地爆发“”勒索病毒，受影响的包括英国 16 家医院。 朝鲜：在这大范围的攻击下逃过一劫，守住了一方净土。 日本：日本警察厅当天表示在该国国内确认了 2 起，分别为某综合医院和个人电脑感染病毒，并未造成财产损失。尚不清楚日本的案例是否包含在这 150 个国家中。 西班牙：国家情报中心证实，西班牙多家公司遭受了“大规模”的网络黑客攻击。该国电信业巨头西班牙电信总部的多台电脑陷入瘫痪。

本建议书的目标是在不影响客户网络架构当前业务的前提下，实现对数据病毒攻击，数据缺失等方面进行预防，确保数据安全。

针对对客户的网络状况和实际应用情况，我们建议在“统一规划”的前提下，进行**“一防护+二备份+三恢复”**方案。

一是可以先对网络客户端做一个比较全防病毒软件安装，将病毒攻击有针对性杜绝在局域网之外；

二是根据网络和数据应用的实际应用状况，建立一个基础的备份体系，保证基本的数据的完整性；

三是随着今后应用的种类和复杂程度的增加，由于客观环境，包括病毒攻击文件的变异、网络新环境的兴起等外部环境和企业内部硬件设施老化、或者误操作等内部环境的变化导致数据意外丢失。所以在出现数据安全事故的情况下我们用数据恢复来补救数据。

依照循序渐进的原则来实施和部署！

二、 产品配置及介绍

2.1 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

AT17 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 PU

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。

2.2 重要的服务器一定要部署异地备份。

西数科技防勒索病毒备份方案---数据备份三原则：

2.2.1：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，根据我们的统计，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 8 万 10 万以上，我们推出的防勒索异地备份方案价位相对会物美价廉，具备大容量 8TB 和更高容量 RAID 磁盘阵列功能。

2.2.2：我们研发的数据备份一体机系列， LINUX 系统,友好的图形管理界面,专为中小型企业和 IT 爱好者而设计。配备强大的内置 AES-NI 硬件加密引擎，可提供出众的加密文件传输。还能够同时转码多达两个通道的 H.265/H.264 4K 视频，是用于共享和存储超高清媒体内容的理想之选。

cpu	四核 1.4GHz，至高可超频到 2.3GHz
网络	双 1GbE LAN 端口
内存容量	2GB DDR3L，可扩展到 4GB
性能	加密连续读取速度每秒 225 MB 以上，加密连续写入速度每秒 221 MB 以上,支持快照备份,多版本备份,数据库备份,文件备份.

（1）**满足您对性能和容量**的需求支持多达两个 M.2 NVMe 2280 SSD，无需占用内部硬盘插槽即可快速创建系统缓存。可通过扩充设备 扩展到多达 9 个硬盘，满足了对灵活存储容量的需求

（2）**Btrfs 文件系统**保护你的企业资料新一代文件系统确保数据完整性和高效率快照。当面对庞大的数据储存时，企业应当有一套预防数据毁损的解决方案，同时提供弹性的数据备份工具。新一代 Btrfs 文件系统提供 西数科技备份服务器这些实用的工具，让企业组织能有效率地储存数据并减少维护成本支出。Btrfs 文件系统采用了更先进的存储技术，可满足大型现代企业的管理需求：
a、元数据镜像，提升数据可用性：
在任何储存系统确保元数据的完整性非常重要，因为其中包含重要的信息，如档案架构、名称、登入权限以及档案位置。 Btrfs 文件系统将两份元数据储存于一个储存空间，让档案即便在硬盘损坏或坏轨的状况下，亦能进行数据还原。
b、Btrfs 文件自我修复： 传统储存系统可能遇到错误但完全被忽略掉，导致将损坏的数据提供给应用程序，而且不会有任何警告或错误消息。为了避免这类错误，Btrfs 会提供数据和元数据的校验和，生成两份元数据，然后在每个读取过程中验证校验和。一旦发现不匹配（静默数据损坏），Btrfs 文件系统就能通过镜像元数据自动检测到损毁的文件（静默数据损坏），并使用支持的 RAID 存储卷来还原受损的数据，包括 RAID0、 1。
C、快照与数据保护：

Btrfs 文件系统提供出色的快照功能，让你在任意时间点复制整个共享文件夹。因此，若因人为疏失导致数据库毁损，你可以在短时间内利用快照还原资料。

(3)**数字资产保护**

提供支持，能提供先进的安全措施，预防突发性数据丢失，防范潜在安全漏洞。

（4）**安全顾问**

可用于分析系统设置、密码强度和网络偏好，删除可疑恶意软件。

（5）AppArmor

这是一种内核级增强功能，能阻止恶意程序访问未经授权的系统资源。

(6)AES 256 位加密

可对共享文件夹和网络数据传输进行加密，防止数据遭到未经授权的访问。

（7）**两步验证功能**

此功能通过在您的移动设备上生成一次性密码 (OTP) 来防止他人登录您的 DSM。

（8）**信任等级**

可在套件中心自定义信任等级，避免安装来自不信任来源的套件，从而保护您的 NAS 免遭未知或篡改套件文件的侵害。

（9）**定期备份你的重要数据：** 内建的磁盘阵列可提供相当程度的数据防护，但定期将重要数据备份至其他储存媒介也是相当重要的课题,的外接装置备份功能除了支持双向传输外，也同时支持增量备份，并可设定排程 自动定时进行备份作业。你可以透过外接装置备份功能来进行以下任务：将 数据传送或备份至外接储存装置中。

（10）**理想的异地备份方案：**使用本机备份，可充分利用 SATA 接口的 1Gbps 高传输带宽快速将数据备份到 MyArchive 硬盘。无论是机密数据保存，或是历史录像归档，都可设定排程转移到 MyArchive 硬盘里，再定期送到安全的地点集中收藏。同时达到无限容量扩充和异地数据备份的目的。

2.3 数据容灾服务：

南京西数科技有限公司成立于 2007 年，自成立之日起一直专注于企、事业单位、军队和政府等涉密单位数据安全容灾服务工作，目前已经累计了超过 100000 例客户数据丢失恢复还原成功的经验。客户范围覆盖包括港、澳、台全国地区、阿拉伯地区及非洲国家。 针对东达铝业数据中心我们提供两类数据容灾恢复方案：

1、针对黑客攻击导致数据删除破坏和病毒勒索导致数据加密勒索原因：我们根据病数据破坏的程度进行测试，按照破坏情况来具体做出修复恢复方案和服务价格。

2、针对内部客观环境原因， 比如由于人为误操作导致数据丢失、机器硬件故障导致数据丢失，考虑到长期合作，客户第一的原则，我们将会提供一个统一优惠标准和价格。

3、溯源分析,针对病毒入侵,找到内部网络漏洞,分析病毒入侵的原因,提供防护措施和安全建议.

4、巡检服务,这是西数科技的特色服务.数据安全最重要的是制度保障,任何一个企业和个人都很难做到 10 年如一日的坚持看管病毒活动,因为好了伤疤忘了疼,时间一长很多人难于坚持专注,疏于防范,所以我们推出的安全巡检服务,每月帮助客户巡逻检查数据备份设备,检查备份是否有效,新的漏洞是否出现,病毒库是否升级到最新,等安全问题,一年 12 次巡检.

5、数据恢复服务,我们从事数据恢复 20 年,有丰富的数据数据恢复经验,针对紧急情况下的数据丢失,病毒破坏,硬件损毁,我们都有紧急预案和解决方案,最大限度地挽救你的数据.

三、 建议产品清单

数据防护和备份清单							
	名称	型号	描述	数量	单价	总价	品牌
1	杀毒软件	EAM-PC 版（1 年专杀勒索病毒）	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 1:1 年 12 次服务器巡检，每月一次。 2:远程检查西数备份机备份文件完整	1	190.00	190.00	EAM

		EAM-服务器版（1 年专杀勒索病毒）	性。 3:服务器内杀毒病毒检测。 4:黑客入侵检测。 5:系统漏洞修复。 6:系统补丁修补。 7:弱密码检查，系统安全设置检查。 8:病毒库升级检查，更新		680.00	680.00	
溯源分析:针对病毒入侵,找到内部网络漏洞,分析病毒入侵的原因,提供防护软件措施和安全建议.价格面议.							
2	网络自动**静态文件备份** NAS	**双硬碟网络文件存储服务器**	中央处理器: 4 核心 Intel Celeron 1.6GHz。 *内存大小:2*4 GB SO-DIMM DDR3L。 *内置硬盘：2 盘位，支持 SATA2/SATA3/SSD /3.5or2.5 硬盘热插拔，可扩充最大支持 196T。 存储：每秒超过 223.64 MB 的读取速度及每秒 219.99 MB 的写入速度。 *加密：锁定企业档案加密需求，内建 AES-NI 硬件加密引擎，提供每秒读取超过 222.97 MB；写入超过 117.88 MB 的资料加密传输速度。 配备 S/PDIF 光纤音源输出、HDMI 1.4b 连接埠 节能：运转 16.6W,硬盘休眠 9,5W,系统休眠 0.96W. 相容:VMware、Citrix 及 Hyper-V 的存储环境，透过支援的 iSCSI 与 NFS，可让您无缝接轨既有的 IT 环境，提供实务的存储解决方案。 虚拟运用： VirtualBox 安装各式各样的作业系统到 NAS 中，进入该虚拟机器后， 支援 Windows / Mac 的/ Unix 类等跨平台档案分享，支持桌机，笔记本或 iOS 版/ Android 的平板手机多人多工同时存取。 外接接口： USB 3.0 x 3/ USB2.0 x 2/eSATA x 2 /Gigabit Ethernet x 2 认证机构: FCC, CE, VCCI, BSMI, C-TICK 企业级硬盘 4TB 7200 转\256M SATA3 *2 质保：3 年原厂有限质保	1	4500.00	4500.00	原厂 3 年质保和软件升级

3	网络自动**动态文件备份**NAS	**双硬碟网络 NAS 存储**	中央处理器: 4 核心 Intel Celeron 1.6GHz。 *内存大小:2*4 GB SO-DIMM DDR3L。 *内置硬盘：2 盘位，支持 SATA2/SATA3/SSD /3.5or2.5 硬盘热插拔，可扩充最大支持 196T。 存储：每秒超过 223.64 MB 的读取速度及每秒 219.99 MB 的写入速度。 *加密：锁定企业档案加密需求，内建 AES-NI 硬件加密引擎，提供每秒读取超过 222.97 MB；写入超过 117.88 MB 的资料加密传输速度。 配备 S/PDIF 光纤音源输出、HDMI 1.4b 连接埠 节能：运转 16.6W,硬盘休眠 9,5W,系统休眠 0.96W. 相容:VMware、Citrix 及 Hyper-V 的存储环境，透过支援的 iSCSI 与 NFS，可让您无缝接轨既有的 IT 环境，提供实务的存储解决方案。 虚拟运用： VirtualBox 安装各式各样的作业系统到 NAS 中，进入该虚拟机器后， 支援 Windows / Mac 的/ Unix 类等跨平台档案分享，支持桌机，笔记本或 iOS 版/ Android 的平板手机多人多工同时存取。 外接接口： USB 3.0 x 3/ USB2.0 x 2/eSATA x 2 /Gigabit Ethernet x 2 认证机构: FCC, CE, VCCI, BSMI, C-TICK 企业级硬盘 4TB 7200 转\256M SATA3 *2 质保：3 年原厂有限质保。 **数据库存储备份：2TB 存储空间/CDP 动态增量备份/虚拟带库功能秒级还原/数据备份软件支持 SQL Server、Oracle、IBM DB2、MySQL、DBMaker、Sybase、Informi/支持 Vmware、Hyper-V/支持客户端 Windows 、AIX、Solaris 、HP-UX 、FreeBSD 、SCO Unix、Linux 、Mac OS/ 支持管理端平台 Windows XP 、Win 7 、Win8 、Windows Server 2003、2008、2012/**	1	9600.00	9600.00	原厂 3 年质保和软件升级

4	网络自动**动态文件备份** NAS	**四硬碟网络 NAS 存储**	中央处理器: Intel Celeron 1.6GHz 内存大小: 8GB SO-DIMM DDR3L 硬盘插槽总数: 4 支持硬盘热插拔 外接硬盘接口: USB 3.0 x 4 网络: Gigabit Ethernet x 4 系统风扇: 40mm x 2 单电源供应器 / 变压器: 250W 输入电压: 100V to 240V AC 认证机构: FCC, CE, VCCI, BSMI, C-TICK 企业级硬盘 4*4TB 7200 转\256M SATA3 整机 3 年质保	1	19950.00	19950.00	原厂 3 年质保和软件升级
			ADM3.2NextVault 数据备份软件：4TB 存储空间/CDP 动态增量备份/虚拟带库功能秒级还原/数据备份软件支持 SQL Server、Oracle、IBM DB2、MySQL、DBMaker 、 Sybase 、 Informi/ 支持 Vmware 、 Hyper-V/ 支持 客户端 Windows 、AIX、Solaris 、HP-UX 、FreeBSD 、 SCO Unix、Linux 、Mac OS/ 支持管理端平台 Windows XP 、 Win 7 、 Win8 、 Windows Server 2003、2008、2012/	1			
备注：本次报价 15 天内有效							

更多企业网络安全方案

详情咨询业务经理 :18913825606 陈兵兵 lwf@wdsos.com