SQL Blackmail Defense

安全管理系统

5.1

技术白皮书

版权声明

用户隐私及数据安全声明

1、SQL Blackmail Defense 尊重用户的隐私权、数据所有权，不会上传用户的任何文件、数据等。

2、SQL Blackmail Defense 仅在联网升级、在线注册等情况下，上传用户许可相关信息（License），用于验证正版授权。

公　　司：远数科技责任有限公司
部　　门：安全技术部
技术支持：086-15555588445
网　　址：http://www.nmgyuanshu.com

目 录

1 概述

欢迎阅读《“SQL Blackmail Defense 5.1 安全管理系统”技术白皮书》。为了能够更好的服务于用户，特别编写本文件。本文件详细的介绍了 “SQL Blackmail Defense 安全管理系统”的理念策略、核心技术、产品功能等内容，可让用户对本产品有更深入的了解。

Tips:

➢ 如果您想了解“SQL Blackmail Defense 5.1 安全管理系统”的安装需知和部署流程，请参阅《“SQL Blackmail Defense 5.1 安全管理系统”安装部署手册》。

➢如果您是初次体验“SQL Blackmail Defense 5.1”，想要快速了解使用方法及操作流程， 请参阅《“SQL Blackmail Defense 5.1 安全管理系统”使用手册》。

➢如果您想了解“SQL Blackmail Defense 5.1 安全管理系统”产品的详细介绍，请参阅《“SQL Blackmail Defense 5.1 安全管理系统”产品说明书》。

2 产品

2.1 产品介绍

“SQL Blackmail Defense 5.1 安全管理系统”是秉承“服务至上、将数据安全放置第一位”新理念。

SQL Blackmail Defense 5.1 安全管理系统是专门针对企业服务器安全开发一款勒索病毒防御软件。

可以充分满足企事业单位 SQL Server 用户在目前严峻的互联网威胁环境下的服务器防护需求。

2.2 产品特点

2.2.1 自主知识产权

◆ 自主知识产权，完全避免产品后门和用户敏感信息外泄等隐患。

◆ 自主核心技术，能够更好地开发产品。对系统资源占用低，主动、被动相互结合的防御手段确保服务器安全，数据安全。

◆ 自主研发团队，能够及时响应本地安全问题，专门针对挂接 Microsoft SQL Server 数据库的服务器安全而研发。

◆ 对国内安全问题的特殊性有深刻认知，除了反病毒、反黑客，更能有效防范商业软件侵权和国内病毒产业链。

2.2.2 成熟的系统，强悍轻巧干净

◆ SQL Blackmail Defense 5.1 安全管理系统产品稳定成熟，运营和服务经验丰富。

◆ 多层次主动防御系统，反勒索病毒、主被动防御、深度整合，并且可主动、被动、本地、异地备份数据。即使本地突破重重防御任可保证数据库、备份等不被破坏、加密。

◆ 基于新技术、新理念运营体系，SQL Blackmail Defense 5.1 安全管理

系统安装体积不超过 2MB，几乎不占用系统资源。

◆ 秉承安全厂商的基本操守，SQL Blackmail Defense 5.1 安全管理系统没有任何捆绑、弹窗、侵占资源等行为，并强

力狙杀各种流氓软件、商业软件的侵权行为，确保电脑系统干净清爽，就像每天都在使 用新电脑。

2.2.3 高效的控制中心，可靠、易用

◆ “SQL Blackmail Defense 5.1 安全管理系统功能以最易操作的形式体现，能轻松掌握。

◆ 基于对用户的深刻理解，“SQL Blackmail Defense 5.1 安全管理系统”的控制中心设计简单合理，拥有友好的界面、人性化的统计报表，安全管理信息和日志一目了然，能极大的提高安全管理效率。 简单快速的完成整个网络反勒索病毒体系的部署。

3 理念和策略

3.1 理念

3.1.1 什么是勒索病毒？

大数据显示自 2010 年以来勒索病毒逐步替代传统木马、病毒成为新型主流黑客病毒。而 Windows 环境下的各服务器因攻击、传播简单、中毒后更容易支付高额赎金而成为黑客攻击、传播的主要目标。经过统计，服务器中毒后黑客以区块链匿名货币为支付方式敲诈勒索数万元，如不支付赎金服务器宕机、数据几乎全部丢失而无法恢复。给企业造成不可估量的损失。

3.1.2 服务至上、数据安全第一的运营体系

◆ “SQL Blackmail Defense 5.1 安全管理系统”是秉承“服务至上、将数据安全放置第一位”的理念对授权使用的客户在进行服务器安全部署（包括服

务器系统安装、系统驱动程序安装、Microsoft SQL Server 2008 等数据库安装部署、SQL Blackmail Defense 5.1 安全管理系统部署、服务器安全加固、配置等）

3.2 策略

一些企业雇佣安全相关技术人员，但优秀合格的安全维护技术人员工资成本高，对企业来说将会付出较高成本。为此我们针对企业安全作出 “安全防御+服务”为一体的产品为企事业单位保驾护航。企业以最低廉的成本获取最优质、专业的服务。从而降低风险节约成本。

4 核心技术

4.1 自主知识产权的新一代反勒索病毒引擎

自主产权的 SQL Blackmail Defense 5.1 安全管理系统、多重防御体系与黑客级恶意程序对抗。

4.2 多层次驱动级主被动防护

SQL Blackmail Defense 5.1 安全系统不依赖白名单、不依赖指纹，采用对恶意程序行为分析的方式识别病毒。有效地防御勒索病毒威胁。同时还能实时感知动态的系统级威胁行为信息，有效地针对服务器操作系统的脆弱点进行防护。

5 运行环境

5.1、运行环境

SQL Blackmail Defense 5.1 安全管理系统适用于以下环境：

系统：

➢ Windows 版本（暂不支持 Linux/Unix/Mac 版本）： ◆ Windows XP

（SP3）、Windows Vista、Windows 7、Windows 8、Windows 8.1、Windows 10 ◆ Windows Server 2003（SP1 及以上） /2008/2012/2016

➢防御勒索程序功能需要 64 位系统，32 位系统只支持备份防御功能，防御强度低于 64 位系统，所以为了您的服务器安全建议使用 64 位系统，其他功能不影响。

内存：

推荐 1024MB 以上即可正常运行

推荐 2048MB 以上

CPU：

推荐 1.6GHZ 以上

5.2、升级服务

程序通过系统升级服务模块升级文件的更新与传递进行升级。

6 主要功能介绍

数据库主动、被动、本地、异地备份功能。

服务器勒索病毒防御功能。

数据库保护功能。

备份保护功能。

其他详见软件相关功能