KEMYOND

CDKY-OSH8000

工业主机卫士（主机加固）

特性及优势

- **合规**

符合等级保护三级安全操作系统标准；
强大的日志采集分析；
拥有完全自主知识产权；

- **实用**

增强操作系统对抗恶意代码和黑客攻击的能力；
有效抵御已知/未知安全威胁；
兼容 windows、linux、aix、hp-ux、solaris 等多种操作系统；
兼容实体机、虚拟化环境；
高可用性，在实现安全加固的基础上，不影响用户原有的运行；

介绍

CDKY-OSH8000 是宽域自主研发的支持跨平台的系统保护产品，它在操作系统的安全功能之上提供了一个安全保护层，通过从内核层截取文件访问控制方式，加强操作系统安全性。支持多种操作系统加固，包括 IBM AIX、HP-UX、Solaris、Compaq Tru64 以及 RedHat Linux 和 Windows 等多种系统。从而即使一个未经授权的入侵者获得系统管理员权限，他也不能对系统及数据进行窃取或篡改，从而在根本上防止由于操作系统自身缺陷所造成的入侵。

部署应用范围

- ◇ 需要受保护的服务器组（数据库服务器\网站服务器\邮件服务器\应用服务器\文件服务器等）。
- ◇ 工作站 PC。

产品功能

身份鉴别：采用 UKEY 和密码双重身份认证的方式，只有插入 UKEY 输入正确的口令才能登录，否则无法登陆。

访问和系统资源控制：强制访问控制，通过符合等级保护要求的“自主访问控制”规则，控制被访问的客体范围包括文件、进程、服务、共享资源、磁盘、端口、注册表等；主体包括用户、进程和 IP，同时支持用户与进程的绑定，可以控制到指定用户的指定进程。从而将主机资源各个层面紧密结合，可根据实际需要对资源进行合理控制，实现权限最小原则。

访问控制：强制使用三权分立，采用了三个管理角色：系统管理员、安全管理员和审计管理员，不同管理员之间相互独立、相互监督、相互制约，每个角色各司其职，共同保障服务器操作系统的安全，从而实现三权分立。

恶意代码防范：通过设置可视化虚拟安全域，将资源实现权限最小原则。恶意代码无法对安全域内的资源进行访问，根本无法获得执行所需的资源。从而从根本上杜绝了恶意代码，解决了使用传统恶意代码防范软件需要更新恶意代码库的滞后性问题，可以有效抵御已知、未知安全威胁。

入侵防范：对重要的系统的错误操作、入侵行为、服务器的状态问题等引发的报警机制，通过邮件、短信方式发送到报警工作站。

安全审计：违规日志记录所有与访问控制策略不匹配的动作和越权访问行为，记录事件的主体、客体、发生的时间和违规动作等信息。检测日志包含文件、用户、服务、注册表（仅 windows）完整性检测的日志信息，其中包括检测的时间、检测的目标文件、检测的结果等，以及对恢复等操作进行日志记录。并将记录系统内所有操作包括成功、失败、违规等，并统一发送到审计中心，审计员可通过访问审计中心对所有操作进行审计。

备份与保护：可实现自定义的需要保护的数据的数据自动备份功能，以及扩展实现双机冗余服务。

订购信息

型号	提供方式	支持系统
CDKY-OSH8000	纯软件	windows\linux

上海宽域工业网络设备有限公司

上海市宝山区园丰路69号3幢5层

189-1779-7159 (技术支持)　021-56561181 (座机)

189-1819-0263 (销售咨询)　zhouaixia@kemyond.com (邮箱)

成都研发中心

成都市高新区天府大道北段1480号孵化园6号楼105号

028-86263902 (座机)

官方网站

www.kemyond.com

宽域公众号

Copyright © 2023 上海宽域工业网络设备有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除上海宽域工业网络设备有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。 本文档中的信息可能变动，恕不另行通知。