



操作系统安全增强系统

RS-CDPS

产品介绍

北京优炫软件股份有限公司

版权所有 侵权必究

目 录

1	产品概述	1
2	产品优势	2
3	产品特点	3
3.1	技术特点	3
3.2	功能特点	4
4	典型应用	6

1 产品概述

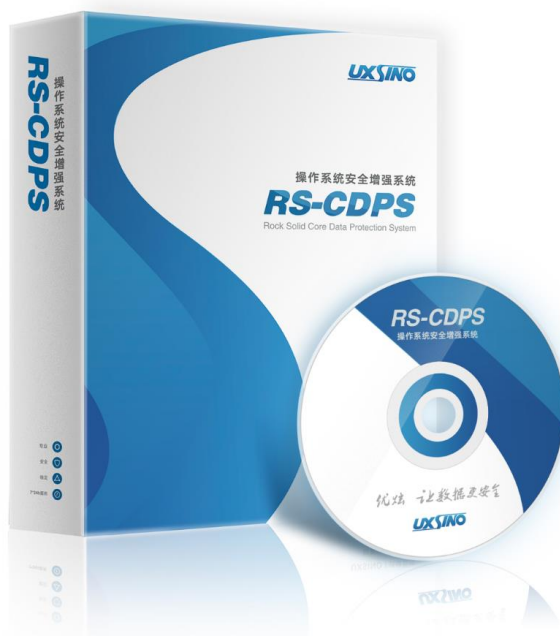


图 1 优炫操作系统安全增强系统 RS-CDPS

优炫操作系统安全增强系统（Rock Solid Core Data Protection System，简称 RS-CDPS）通过安装在服务器的安全内核保护服务器数据，通过截取系统调用实现对文件系统的访问控制，以加强操作系统安全性。它具有完整的用户认证，访问控制及审计功能，不用更改操作系统就可以安装，提供信息系统主动防护功能，操作方便、易于系统管理和安全管理。可对 UNIX 类、Linux 类、WINDOWS 类各种操作系统进行统一管理，为管理人员提供方便，可以保障客户的服务器安全、持续、长效运行。

2 产品优势



- ◆ 可提升操作系统安全等级至 **B1 级**，同时该级别的评价标准符合我国信息安全等级保护（三级）、分级保护（秘密级）的相关标准要求。
- ◆ 支持各类操作系统（如 Windows, Linux, Solaris, HP-UX, Tru64, UnixWare, AIX 等）的安全加固。
- ◆ 不用更改操作系统就可以安装，操作方便；充分考虑最佳的系统性能，系统资源的占用很小，对运行环境“零影响”。
- ◆ 拥有最全面、权威性的资质和报告，具备业界领先的实力。



版权局软件著作权



公安部销售许可证



国家保密局涉密产品
检测证书



解放军认证中心军用
产品认证证书



电力科学研究院信息
安全检测报告



信息安全服务资质



微软WHQL认证
(网页截图)

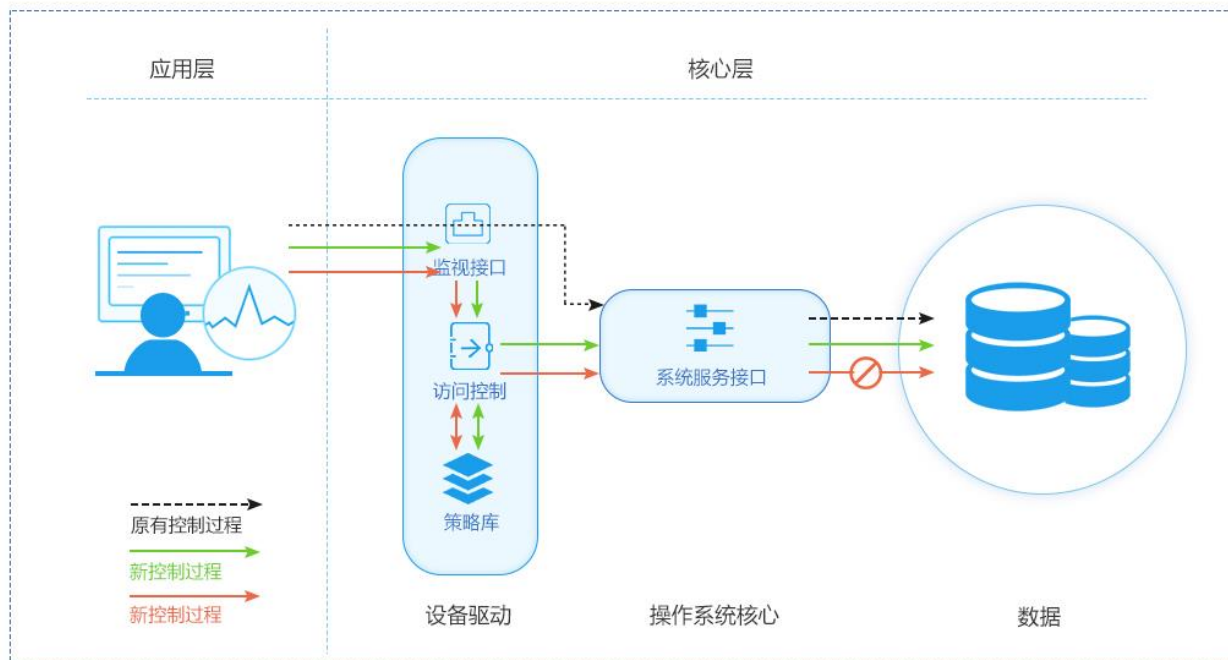


软件产品证书

3 产品特点

3.1 技术特点

- 构建可信操作系统（遵循 CCC 标准，达到相关行业的等级保护要求）。
- 强制安全实现，权限分离，最小特权，细粒度的访问控制，操作系统安全级别从 C2 级提升到 B1 级。
- 核心数据主动防护。
- 防 BOF 攻击，密码与登录策略管理，文件/进程/权限/网络访问。
- 保护核心数据不受泄漏，篡改和被破坏的威胁。
- 分布部署，集中化管理。
- 细粒度、高可靠的审计。
- 多平台支持 Windows, Linux, Solaris, HP-UX, Tru64, UnixWare, AIX。



产品原理图

3.2 功能特点

独一无二的用户认证机制

在操作系统内核层用数字签名方式对用户进行认证，用户使用数字证书通过正常认证以后才能访问系统。

灵活全面的访问控制

可根据用户的需求，依据用户、组、文件、任务、权限等制定安全策略，实行细粒度的访问控制。它可管理 23 个以上的系统调用，对文件、系统、进程进行保护，并可防止由攻击造成的数据篡改，阻止非授权用户中断进程和系统服务，保障服务器的稳定运行。

主动的入侵防护及审计跟踪

可在内核层防止 BOF（缓冲区溢出）攻击，阻止获得 ROOTSHELL。当发生安全问题时，它会强制结束恶意进程及自动阻断相应 IP，并通过管理控制台、短信息、Email 等方式实时报警。

权限分离及最小特权实现

操作系统访问控制的最佳策略是权限分离和最小特权原则。通过严格分开系统管理员和安全管理员的权限，以控制超级用户的权限，可有效防止内部人员的越权访问和外部的攻击。

多系统，多平台统一管理

Agent 模块可部署在 Sun Solaris, IBM AIX, HP-UX, Tru64, Unixware, Linux, Windows 多种服务器平台上，产品管理控制台可以让用户通过一个统一的图形界面，对网络中多个不同平台的服务器进行集中安全监控和策略配置。

全面的服务器资源管理

用户可以使用图形界面进行用户账号管理，通过系统查看文件、进程等信息以及服务器的系统状态信息，包括服务器的 CPU、内存、交换区状态信息，服务器的网络信息，服务器的磁盘使用信息，服务器的进程/守护进程状态、服务器性能的实时运行状况信息等。

先进的程序自我保护

系统使用了全球领先的内核密封技术管理内核模块的加载/卸载，可阻断对内核的恶意攻击。系统还具有内核隐藏功能，它隐藏了安全内核，并自动保护自身系统程序目录和文件，可防止安全内核程序被删除，最大限度地降低了安全风险。

运行环境“零影响”

系统是在充分考虑最佳的系统性能后进行设计的，它对系统资源的占用很小。管理员可以根据应用环境选择相关的系统调用函数，以降低运行时对系统资源的占用。

灵活的网络访问控制

系统提供了主机防火墙功能，系统管理员可以根据需要设计安全策略来控制基于网络的访问，可通过设置拒绝、允许的 IP、服务管理系统的外部的访问,也可对存在漏洞的连接进行控制，阻断外部非法访问，避免被入侵者利用。

4 典型应用

优炫 RS-CDPS 在网络上的应用

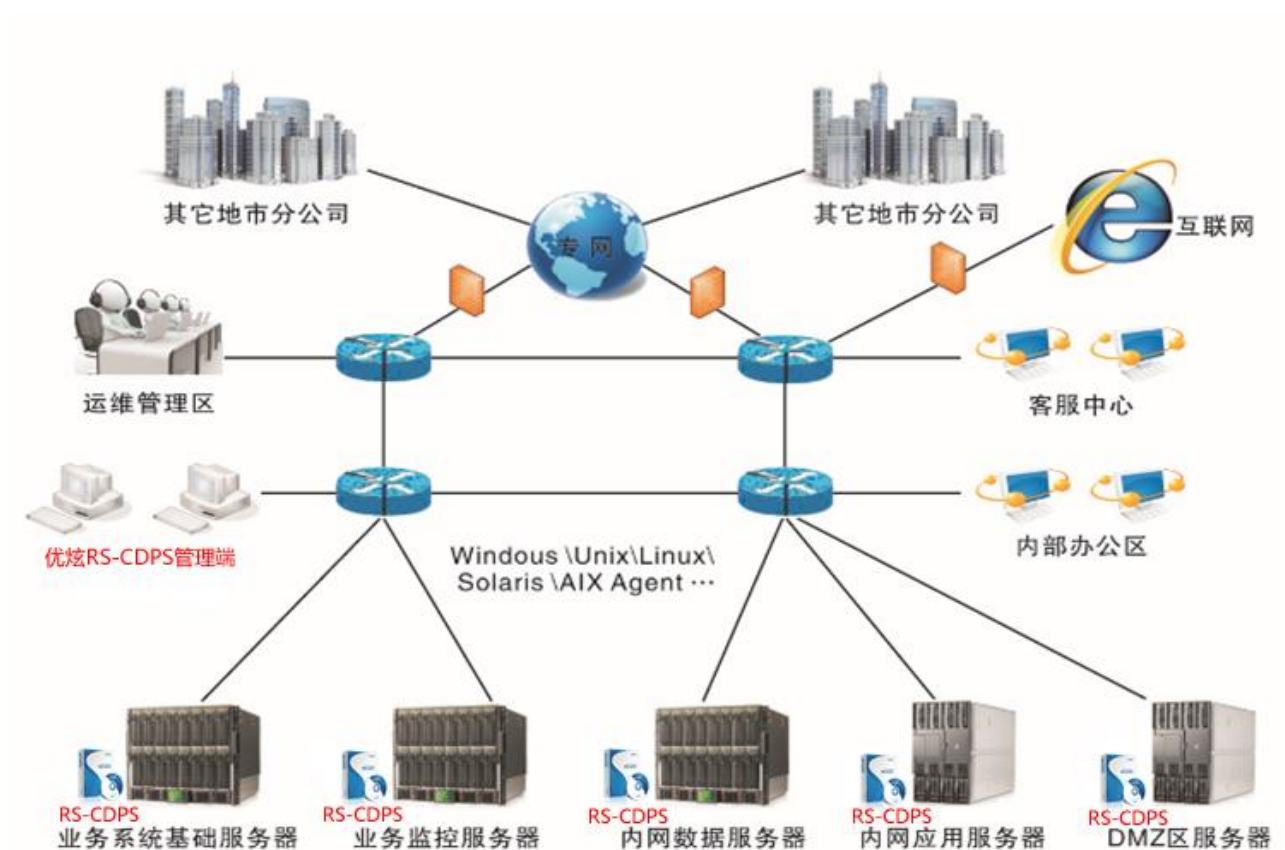


图2 RS-CDPS 在网络上的应用

应用特点：

优炫 RS-CDPS 通过安装在服务器的安全内核保护服务器数据。它在操作系统的安全功能之上提供了一个安全保护层，通过截取系统调用实现对文件系统的访问控制，以加强操作系统安全性。它不用更改操作系统就可以安装，操作方便，宜于系统管理和安全管理。适用于各种应用服务器、KMS 服务器、数据库服务器、群件服务器、文件服务器等，以及其他需要安全保护的系统。