KEMYOND

CDKY-OSM2000

堡垒机（运维审计系统）

解决问题

•接入认证授权：终端数据安全：

识别和确认终端用户的身份信息，完成对终端用户的身份鉴别，确保只有合法的终端用户才能使用终端计算机。

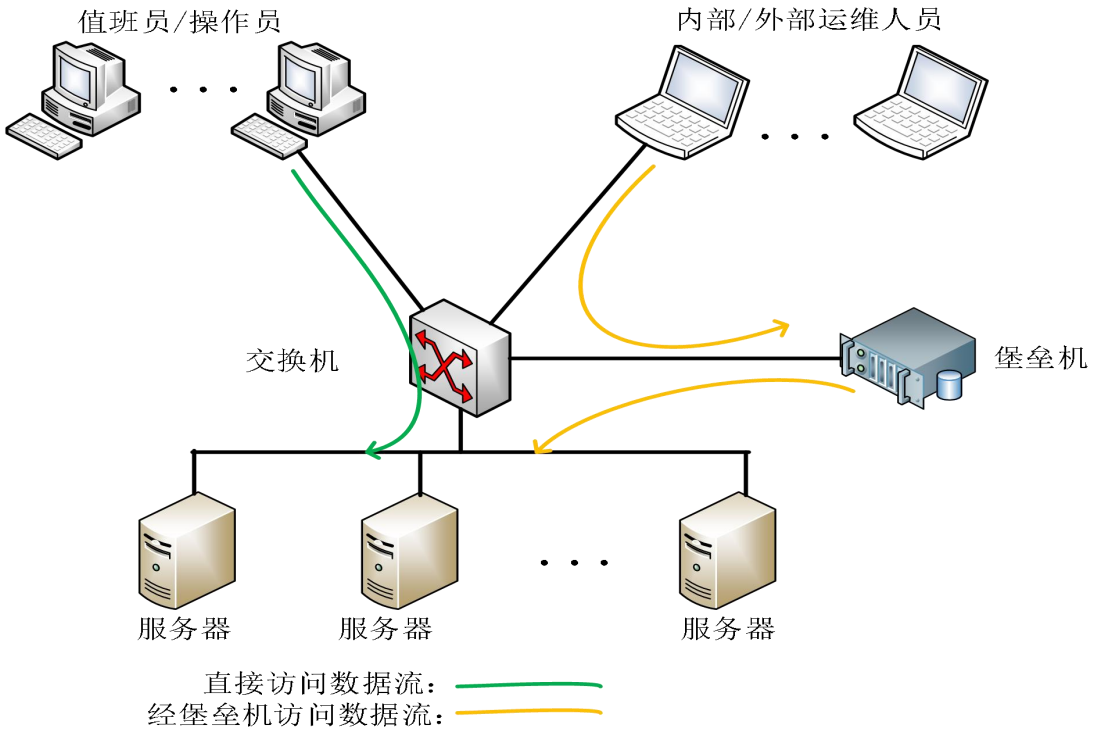
•终端数据安全：

按照相应的授权级别和终端安全管理策略完成对终端授权用户的操作行为控制和文件加密管理。

介绍

CDKY-OSM2000 系列是为满足用户对加强内部运维安全审计日益迫切的需要，而研发的新一代软硬件一体化运维安全专用审计系统——运维安全管理系统。该系统支持对企业内部人员的维护行为进行全面的管理、审计，消除了传统审计系统中的盲点，使企业对运维人员的操作过程，能做到事前防范、事中控制、事后审计的能力，是企业 ICT 内控最有效的运维管理平台

产品部署



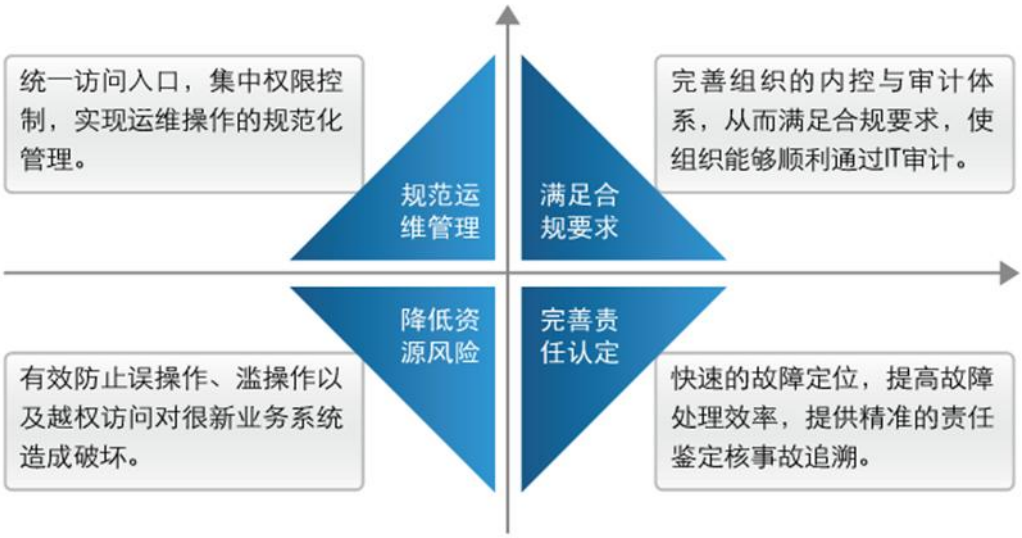
主要功能

功能指标		指标参数
主要功能	管理方式	管理方式：采用 https 的 B/S 方式，不需要在运维终端安装客户端； 设备部署：提供旁路接入模式，设备部署不影响原有网络结构；
	操作设备类型	系统支持对 AIX，HP-Unix，Solaris， SCO-Unix， Linux，Windows 等主机服务器操作系统及各类网络、安全设备的运维管理
	运维协议	图形会话操作：RDP、VNC、X-Window 字符会话操作：Telnet、SSH 文件传输：FTP、SFTP 应用发布: HTTP、HTTPS、Pcanywhere、Radmin、 Oracle、SQL Server、DB2、Sybase、Mysql 以及其它任意客户端协议工业协议：OPC、Modbus、S7 等。

	认证管理	认证模式：系统需要支持静态口令认证（支持中文用户名）、动态口令认证（支持中文用户名）、LDAP 认证、 AD 域认证、RADIUS 认证等多种认证方式； 支持与第三方认证机制的整合：如：安盟、RSA 动态口令系统及 CA 系统等。 动态口令：系统需要内置动态口令系统，内置的动态口令系统需要与主帐号使用共同的用户名和密码，内置的动态口令系统也需要支持英文名和中文名二种方式； AAA 服务器:系统需要内置网络设备的 AAA 认证服务,网络设备可以通过 Radius 协议到运维审计上进行统一认证管理； 认证日志：认证过程需要有详细的日志，为了故障排 除，在前台界面至少需要显示出成功登录和认证错误，认证错误至少可以分为：密码错误、Licenses 错误、权限错误、用户名格式错误、来源地址禁止、有效时间禁止、时间列表错误等明细的选项；
	权限管理	支持按照主账号、系统帐号、系统帐号组等组合方式进行授权； 支持限制运维人员只能从指定的 ip 地址段访问运维系统； 支持登录服务器以来源 IP、时间进行授权； 支持按照助帐号组、系统帐号组进行访问授权； 支持审批模式：运维用户访问特定的服务器设备必须经过管理员的临时审批授权才能进行，否则无法登录；支持限制用户通过 web 登录运维系统的并发数； 支持设定会话连接单位时间内空闲无操作，连接自动断开； 支持运维用户多次登录失败自动锁定账号功能；支持设定帐号锁定失效时间，帐号可以自动解锁；
	资源管理	支持添加、删除、修改运维用户；支持用户、资源的批量导入功能；支持运维用户锁定、解锁管理； 支持运维用户使用有生效时间和过期时间的管理； 支持运维用户密码策略（密码长度、密码强度）管理；支持运维用户组管理，可方便添加、删除、修改； 支持添加、删除、修改资源主机内容；资源主机内容至少包括主机名、IP 地址、访问协议、访问账号、扩展信息、设备组等内容； 支持设备组管理功能，可方便添加、删除、修改组信息及组成员； 系统类型管理：内置常见系统类型，可自定义添加目标设备的系统类型及内容； 支持资源设备帐户同步功能；
	访问控制	支持根据源 IP 地址、时间、用户名、操作指令、目标服务器主机等内容设定告警策略； 支持指令的黑、白名单控制，可根据黑白名单指令集限制用户的操作权限； 支持对违规事件进行告警及自动阻断； 支持针对系统的黑白名单控制方式可分为三类：命令告警（允许执行但记录）；命令阻断（不允许执行记录）；断开连接（直接断开连接）；

	实时监控	实时监控：实时会话监控列表：显示已经连接的会话，运维用户、服务器 IP、服务器用户名等，实时监控支持会话断开，可以切断任意会话；
	审计记录	登录审计：系统需要可以记录主帐号登录 Web 界面的成功、失败事件，可以记录登录 FTP/SFTP/SSH/TELNET/RDP/VNC 的登录成功失败事件，并且可以记录失败原因； 文件传输协议：FTP,SFTP 要求可以保存上传下载文件，同时为了防止存贮占用过大，可以根据上传下载文件大小进行定制选择记录，比如只记录 3M 以下的文件； 字符协议协议：可以不依靠系统提示符进行命令识别记录，可以记录输入命令及回显，并且可以记录操作的整个过程； 系统支持组管理员能够对所属组内资源运维操作进行审计； 系统支持运维人员可以审计自己的操作过程；
	会话回放	Telnet/SSH 协议支持对菜单命令 top、vi、smit 等回放，保证对菜单命令回放时不会出现乱码； RDP/VNC 协议支持键盘录入、鼠标动作及整个操作的过程录像； 应用协议支持应用启动停止时间、登录主帐号及从帐号、键盘录入、鼠标动作及整个操作的过程录像； 录像回放支持快进、慢放、暂停等操作，文本协议支持指定从哪条命令进行回放；

客户收益



选型表

名称	型号	CPU/内存/磁盘	接口	尺寸
固定式堡垒机	CDKY-OSM2000-GT6	主频 3.0 以上 16G 2T	6*千兆电口 2*USB 1*Console	1U
固定式堡垒机	CDKY-OSM2000--QF2-GT6	主频 3.0 以上 16G 1T	6*千兆电口+2*万兆光口 2*USB 1*Console	2U

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