inspur 浪潮

浪潮操作系统安全增强系统（SSR）

您关注您的业务，放心把安全交给我们。

产品介绍

V1.0

北京浪潮嘉信计算机信息技术有限公司

SSR浪潮操作系统安全增强系统，是一款基于操作系统内核层开发的安全加固软件，采用ROST技术和三权分立思想，实现了从根本上免疫各类病毒、木马和黑客攻击，与传统的信息安全产品形成良好的互补，完善了当前国内用户整体安全解决方案中最为重要的环节，填补了国内长期在操作系统层面安全产品的空白，并符合国家等级保护、分级保护以及军工、军队、电力等多个行业的信息安全建设要求。目前已经在全国各地的政府、军工、军队、能源、金融和央企等国家重要部门的信息安全防护中获得广泛的应用和认同，成为国家当前信息安全建设中又一不可或缺的产品体系。

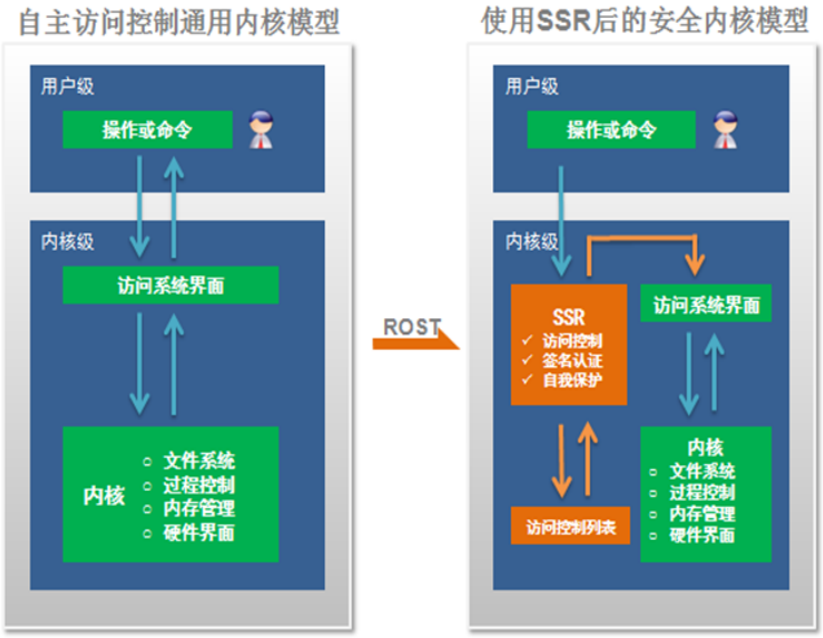


图 SSR安全内核模型图

该图说明SSR的防御核心模块为“安全内核”+“访问控制列表”，用户的操作或者命令需要先通过“安全内核”的校验才能到达系统底层存取数据等，而“安全内核”在接到用户的操作或者命令以后会判断其操作或者命令是否在访问控制列表的“白名单”中，在“白名单”中即认为是合法的、可信的操作，放行，否则拒绝。该模型的优势是即使恶意程序和入侵者获取了系统管理员的权限，也不能破坏被保护的资源。

用户收益

免疫病毒木马，抵御黑客攻击

SSR采用多方位立体防护体系，层层把关，从根本上免疫各种已知未知病毒、木马以及黑客攻击对系统的破坏，确保系统和应用的稳定运行。

分权管理，合理合规

SSR规避了原操作系统管理员“一权独大”的风险，将其权限分散为系统操作员、安全管理员和审计管理员，三个权限各司其职，相互制约，实现最小权限。

强制访问控制，提升安全级别

SSR在操作系统内核层实现强制访问控制机制，与用户系统自身的自主访问控制相融合，为系统和用户重要应用提供更强的约束和更高的安全控制级别，即使原系统管理员也不能破坏被保护的系统和资源。

立体防护，多重效果

变“被动”为“主动”的防御；变“修补”为“免疫”的安全；变“脆弱”为“强壮”的系统；变“分散”为“统一”的管理；变“手工加固”为“永久自动防御”。

统一管理 ，化繁为简

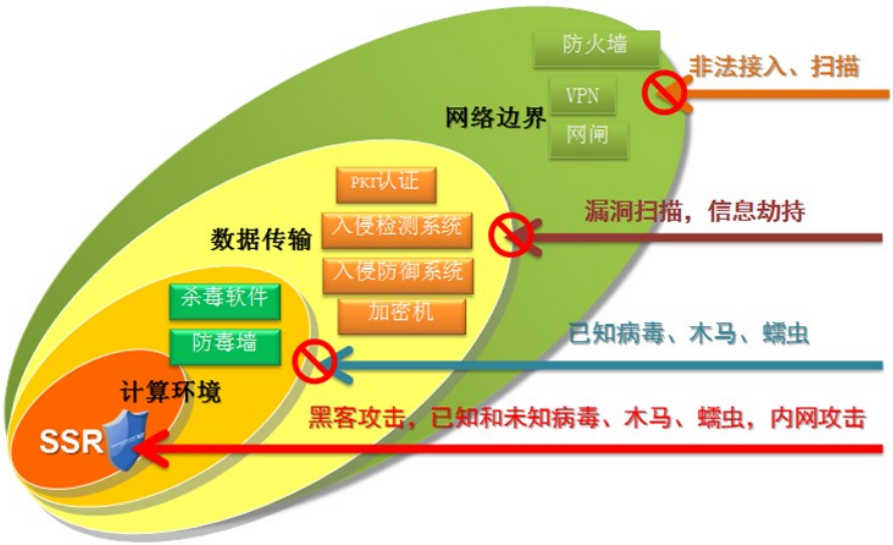
管理员可以从任何地方通过双因子身份认证后，对所有被保护的服务器进行安全策略制定和维护，实现集中管理，减少日常维护工作量 。

通过权威机构检测

SSR 通过微软 Certified for Windows Server 2008 R2认证以及国家权威机构检测，验证了产品和应用系统的兼容性和稳定性。

10年主机安全经验，高品质服务

浪潮自2002年起研究主机安全防护解决方案，2004年发布SSR产品，成为国内首款自主知识产权的服务器安全加固产品。10年时间，浪潮在主机安全领域不仅积累了丰富的防护经验，还培养出一支攻防兼备的技术队伍，为上万家客户提供了高品质服务。



该图说明SSR作用在系统层，在最贴近用户数据和应用的计算环境进行保护，其防御的效果为抵御黑客攻击，免疫已知和未知病毒木马，防范针对系统漏洞攻击。

防护功能

文件强制访问控制

允许制订文件/目录访问规则，任何系统帐户（包括系统管理员）对敏感文件或目录进行创建、删除、修改、读取等操作时，将根据SSR规则进行过滤（允许或拒绝），如保护系统和用户应用（如网站）重要的文件，防止被恶意程序和入侵者破坏。

注册表强制访问控制

允许制订注册表访问规则，任何用户（包括系统管理员）对注册表敏感键值进行创建、删除、修改、读取等操作时，将根据SRR规则进行过滤（允许或拒绝），如保护系统随机启动项避免被恶意程序利用。

进程强制访问控制

允许用户制订进程访问规则，任何用户（包括系统管理员）对敏感进程进行内存操作、非法终止、复制句柄等操作时，将根据SSR规则进行过滤（允许或拒绝），如保护重要的系统进程和用业务进程，防止被恶意程序终止。

服务强制访问控制

该模块可及时发现并阻断对系统服务的更改行为，如新增服务、修改服务属性等，可有效防止rootkit、伪装成服务木马以及恶意程序和入侵者修改服务。

帐户强制访问控制

该模块可及时发现并阻断对帐户的恶意更改行为，如新增帐户、删除帐户、修改帐户密码等，可有效防止恶意程序和入侵者建立隐藏帐户、克隆帐户等，保护系统帐户安全。

防格式化保护机制

该模块可防止病毒和入侵者恶意格式化磁盘，同时降低管理员意外格式化磁盘的风险。

文件完整性检测

需要校验的重要目录及校验信息所存放的文件由用户指定后，检测程序便自动记录目录中所有文件的基本属性及内容校验和。通过定期对该目录进行校验和的有效性检测，可以达到验证重要目录完整性的目的。该模块可用来判断程序安装时生成的文件或者查验文件是否被恶意修改。

服务完整性检测

检测程序自动记录系统所有服务的基本属性及内容校验和并存放到用户指定的信息文件中。通过定期对系统服务进行校验和的有效性检测，可以达到验证服务完整性的目的。该模块可用来判断服务是否被恶意修改。

双因子认证

安全管理员和审计官员的必须具备USB KEY+密码才能登陆管理平台管理SSR，以此确保自然人的可信。

自我保护机制

SSR采用内核密封技术和完整性保护技术来保证SSR的文件不被恶意篡改，进程不被恶意注入。

审计功能

违规日志审计

记录系统内的所有违反强制访问控制策略的事件，并提供日志的查询、删除、备份、导出、日志分析和syslog转发功能。

操作日志审计

记录管理员对SSR的所有操作事件如登陆、功能停用等，并提供日志的查询、删除、备份和导出。

管理功能

统一管理机制

在一个SSR控制台可以同时对多个平台的SSR进行管理和维护，且SSR可开放接口给第三方管理平台集成，实现与不同产品间管理的融合。

灵活多样的策略模板

提供经过验证的分等级的安全策略模板，全面保护系统，方便易用，降低用户的使用难度。

信息收集

提供对系统信息以及SSR运行信息收集打包功能，当SSR在使用过程中出现问题或者用户有疑问时，可将收集的信息包发给SSR技术人员，技术人员可通过这些信息快速定位问题并解决用户疑问。