

卡巴斯基网络安全解决方案-服务器新增功能

产品名称	卡巴斯基网络安全解决方案-服务器新增功能
公司名称	江苏国骏信息科技有限公司
价格	面议
规格参数	
公司地址	徐州市解放南路矿大科技园软件园A座
联系电话	0516-83887908-608

产品详情

卡巴斯基实验室宣布，最新版本的卡巴斯基网络安全解决方案-linux邮件服务器更新包现已提供广大用户安装使用。该方案在独立测试中表现出众，足以证明新增强组件显著提升了管理功能和总体安全效率。

新增实时保护与通知功能

新版本的卡巴斯基网络安全解决方案-linux邮件服务器整合了卡巴斯基安全网路的全部功能。如此一来，实时威胁信息就可以通过云端，从全球数以百万计的客户端传送给卡巴斯基实验室的专家们，从而确保用户免遭最新威胁的侵扰。此外，更新包还具有垃圾邮件增强检测功能，并新增了钓鱼软件检测功能。标记通过垃圾邮件过滤器的恶意钓鱼链接。通过新增的邮件过滤设置，管理员可以阻止或限制海量邮件成为合法资源，从而节省了网络流量，避免工作人员浪费精力。

值得一提的是，卡巴斯基网络安全解决方案-linux邮件服务器还增加了url分析技术。它能够分析邮件中的链接，判断出该链接是否会将用户指向恶意网站。当遇到合法网站近期被泄密，并通过恶意软件感染访问者的情况时，这一技术显得尤为有用。卡巴斯基实验室的这项新技术会自动扫描疑似有害链接，继而检测出等候在另一端的攻击企图，阻止该链接被发送给用户。

上述新技术现已全部纳入卡巴斯基网络安全解决方案-linux邮件服务器安全工具的豪华阵容之中。这其中也包括卡巴斯基实验室先进的零日漏洞防护技术。该技术能够有效抵御恶意软件的攻击。恶意软件一般利用其它软件存在的漏洞，发起定向攻击。零日漏洞防护技术通过扫描数据流来实现，如对收到的邮件附件进行扫描，以检测附件中是否含有可被用于攻击软件漏洞的特定代码段。零日漏洞防护技术可以搜索出这些独立的代码段，并根据防护目标的特点运用适当的扫描技术。因此，即便恶意软件隐匿在那些看似合法的文件之中，也照样难逃零日漏洞防护技术的法眼。对于新近产生的潜在漏洞，该防护技术能够在它未被发现之前成功拦截。此外，由于该技术重点对较短的代码段进行扫描与检测，这样就可以在短时间内完成海量数据的处理，对企业发送邮件系统的延迟降到最低。

新增邮件管理功能

卡巴斯基网络安全解决方案-linux邮件服务器增强功能的另一亮点是，它极大地方便了网络管理员的管理

工作。为此，卡斯基实验室开创性地将服务器的运行情况呈现在网络管理员眼前。现在，网络管理者只需在网络覆盖之处，通过卡斯基网络安全管理中心就可以清楚地看到卡斯基网络安全解决方案--linux邮件服务器的全部情况。管理控制平台新增了这一功能之后，管理员无须一一打开各自的管理平台，就能够监控到邮件服务器集群的安全情况，管理许可，查看故障通知。卡斯基实验室将继续为喜爱用传统方法管理邮件服务器的用户，提供网页管理界面和命令行控制等高级功能。