**五种Linux EDR产品比较**

在线文档：http://www.trustcomputing.com.cn/help/linux\_edr\_compare.docx

导论：安全狗偏重于WEB应用安全防护，云锁偏重于网络主机管理及WEB应用安全防护，青藤万相偏重于网络主机管理及通用应用安全防护，中神通大地云控服务器安全防护及NAT、防火墙、IPv6、SSL证书、代理、VPN等基础网络防护相对较强，安恒明御除基础网络防护外其它比较全面。中神通大地云控、安全狗、云锁都提供免费下载使用的软件包，但安全狗、云锁已经停止更新软件包。

具体对比详见下“表1 Linux EDR产品特点比较表”以及“表2 Linux EDR产品综合比较表”。

**一、产品比较表**

**1、Linux EDR产品特点比较表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **项目** | **中神通大地云控** | **安全狗** | **云锁** | **青藤** | **安恒** |
| 基础OS | 服务器 | 服务器 | 网络主机 | 网络主机 | 网络主机 |
| WEB应用防护 | 强 | 强 | 强 | 弱 | 强 |
| 通用应用防护 | 强 | 弱 | 弱 | 强 | 强 |
| 基础网络防护 | 强 | 无 | 无 | 无 | 无 |

**表1 Linux EDR产品特点比较表**

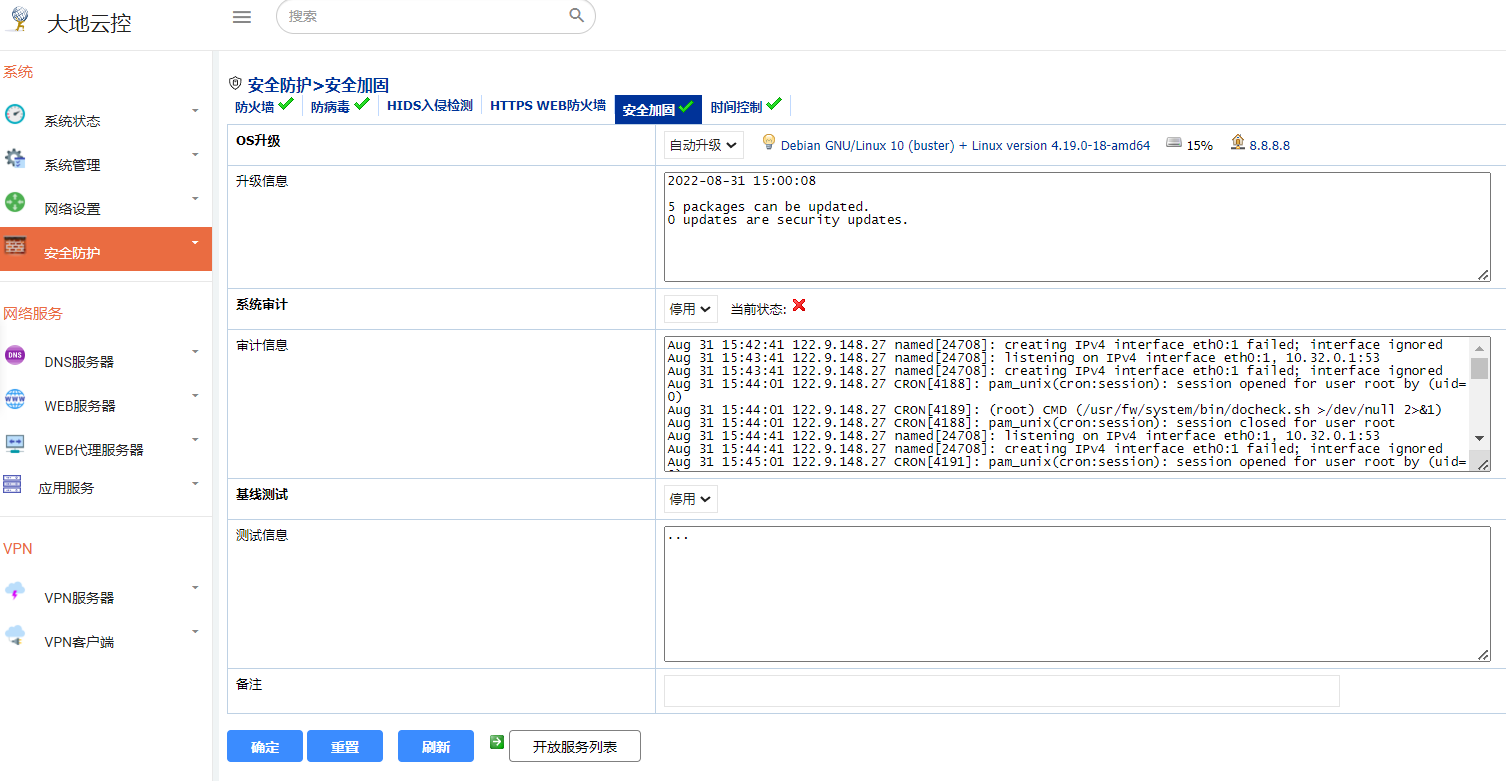
**2、Linux EDR产品综合比较表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **项目** | **中神通大地云控** | **安全狗** | **云锁** | **青藤** | **安恒** |
| 1.适用对象 | 个人、团体、单位、MSP、IDC | 个人、 IDC 运营商、虚拟主机服务商、企业主机、服务器管理者 | 个人、单位 | 单位 | 单位 |
| 2.产品功能 | EDR/XDR/EFF终端网络安全防护、网络服务器、网络客户端、网络路由器服务、日志留存及WEB管理面板 | 服务器防护、Apache 防护和 Nginx 防护 | 操作系统加固和 Web 访问技术控制 | 资产清点、风险发现、入侵检测、合规基线、病毒查杀 | 资产管理、高级威胁、系统防护、网络防护、WEB应用防护、风险评估、运维管理 |
| 3.基础OS | CentOS、 Redhat、 Ubuntu、 Debian、  Fedora、  WSL、  Oracle、  Aliyun、  Kali、  OpenEuler、  Rocky、  SUSE、  统信UOS/Deepin  麒麟等 | Ubuntu 、Centos 、Fedora 和 RHEL 等发行版的较新版本 | CentOS、Ubuntu、Redhat、SUSE、中标麒麟等超过 60 个 Linux 发行版本（包括小版本） | centos6/7、rhel6/7 、ubuntu12/14/16 | Linux |
| 4.虚拟化平台 | KVM、 OpenVZ、 VMWare、 Xen、  LXC、  WSL、  HyperV、  VirtualBox、  Proxmox、  QEMU、  Docker、  裸金属等 | / | OpenStack 等云操作平台，Xen、Hyper-V、Vmware 等虚拟化架构，以及大部分云厂商自主开 发的云主机虚拟化架构 | / | / |
| 5.安装软件包 | 64位，可以裁剪服务、定制界面，可以OEM、ODM，可以与其它软件共处一机，节省机位、电力，统一管理，可以使用优惠云服务器，可以私有化部署；另外提供raw、vmdk、docker格式的服务器OS镜像方便裸金属、虚拟平台、容器平台的私有化部署 | 32位以及64位 | 有 | 无（需要申请试用或购买） | 无（需要申请试用或购买） |
| 6.上架的云市场、应用商店 | 阿里云、  腾讯云、  华为云、  金山云、  百度云、  天翼云、  浪潮云、  青云、  AWS国际云、  统信、  深度、  银河麒麟 | 阿里云、  腾讯云、  华为云等；  麒麟、中科红旗、普华、凝思、统信 | 阿里云、  腾讯云、  华为云等 | 阿里云、  腾讯云、  华为云等；  统信 | 阿里云、  腾讯云、  华为云、青云等；  统信、麒麟 |
| 7.部署位置 | 可作为服务器及或客户端部署在：  云端、边界、内网、虚拟机、硬件设备 | Linux终端 | Linux终端、Windows终端 | Linux终端、Windows终端 | Linux终端、Windows终端 |
| 8.防火墙 | **Iptables主机防火墙****；**  **SNAT及DNAT端口映射,用于中转服务，带流量统计与控制功能；**  **IPv6总体开关以及基于规则的防DDoS、CC攻击等功能；**  **可以在标准安全策略模板文件的基础上做修改，达到适配实际安全需求的目的；**  **生成“开放服务列表”，一个页面显示系统配置、应用服务资产清点、全部功能及相关参数** | WEB服务的IP黑白名单 | WEB服务的IP黑白名单；  自定义CDN IP；  端口防护；  应用防护，应用列表 | 无 | 微隔离；  违规外联防护（黑白名单）；  资产管理 |
| 9.防暴力破解 | 对WebAdmin、WEB服务器、WEB代理服务器、SSH服务器等进行防暴力破解防护 | FTP、SSH | 主要对远程登录、SSH 登录、FTP、SMTP 等应用进行防护 | vsftpd 或者 sshd | SSH |
| 10.防病毒 | 提供本地文件实时防护以及网络防病毒服务；为WEB服务、网络存储服务以及OS自身提供安全无毒的环境，防止勒索病毒、挖矿病毒、后门木马蠕虫等运行 | 文件实时防护，使用云查杀引擎 | 无 | 小红伞、ClamAV、青藤 Hash 库、青藤 Yara 库 | 有。病毒查杀，自研病毒引擎，第三方病毒引擎 |
| 11.HIDS入侵检测 | **本地文件异常检测、文件变化检测（不基于特征值，探测加密WEBSHELL、拖库、rootkit等异常文件，可用于网页防篡改、数据防泄露），系统日志监控，rootkit检测，软件漏洞检测等** | 异常文件检测；  帐户监控和设置；  远程登录监控；  日志监控； | “一键巡检”功能针对服务器和网站的目录及文件进行全面巡检扫描，对服务器和网站 存在的安全隐患进行检查并修复；“服务器安全”主要针对计划任务、账户及云锁 V3 各功能开启状态进行检查和修复 | 入侵检测：  异常登录；  反弹 Shell监控；  本地提权监控；  可疑操作监控；  Web 命令执行监控 | 高级威胁：  单机扩展；隧道搭建；远控持久化；内网探测；痕迹清除  系统防护：系统登录防护 |
| 12.主机安全加固 | **设置自动OS升级，每小时检查一次官方提供的可升级软件包并自动升级（保留老版本），可以消除大部分已知安全漏洞，防患于未然；**  **系统审计可用于记录并追溯****SSH远程登录等系统安全事件；**  **基线测试，包括检查WEBSHELL网马、rootkit木马、挖矿等后门程序以及弱口令、异常权限文件等不安全因素** | 对 Linux 系统权限、目录权限、应用程序权限、密码强度、网站目录权限、网站应用程序权限、数据库权限进行安全加固；  对云服务器进行全方位安全体检，检测各种可能出现的服务器安全漏洞，并提供相应的修复功能 | 禁止修改 passwd 及 shadow 文件；  禁止添加系统自 启动项；  禁止在系统目录下创建及修改可执行文件；  禁止临时目录执行脚本及二进制文件；  登录防护；  强制访问控制；  服务器漏洞修复（Windows） | 资产清点；  合规基线；  安全补丁；  弱密码检测； | 系统防护：漏洞管理；进程防护；文件访问控制 |
| 13.HTTPS WEB防火墙 | **具有WAF功能的HTTPS反代服务器，可以为任意WEB服务器提供WAF防护，除了本机的WEB服务器，还可以为VPN、GRE客户端的WEB服务器（内网穿透）提供HTTPS连接****、SSL证书及WAF防护** | 无 | 应用防护，WEB应用代理 | 无 | 无（WEB应用防护） |
| 14.安全的WEB服务器 | **系统内置apache WEB服务器，具备PHP、Python、CGI、SQL等扩展接口；**  **默认安全的文件权限设置，文档根目录、子目录、文件均为只读，防止普通用户创建、替换文件，防网页篡改、防数据泄露；**  **默认没有SQL服务器，防止SQL注入；或者通过数据库防火墙连接数据库；**  **中性化服务特征，防止0day风险牵连；**  **安全的SSL等服务器配置，通过了绿盟、Nessus等扫描器的安全评估；**  **内置WAF（WEB应用防火墙）、外置HTTPS WAF；**  **提供http和https、IPv4和IPv6 、标准端口和非标准端口WEB服务，并内置多种WEB应用** | 集成Nginx、PHP、MYSQL；  Apache 防护、Nginx 防护 | 支持 IIS、Apache、Nginx、Tomcat 及 Weblogic 等主流 Web 中间件 | 无 | 无（WEB应用防护） |
| 15.WAF功能 | **集成Modsecurity模块，可以防止以下攻击：**  **SQL Injection (SQLi)：SQL注入；**  **Cross Site Scripting (XSS)：跨站脚本攻击；**  **Local File Inclusion (LFI)：利用本地文件包含漏洞进行攻击；**  **Remote File Inclusione(RFI)：利用远程文件包含漏洞进行攻击；**  **Remote Code Execution (RCE)：利用远程命令执行漏洞进行攻击；**  **HTTP Protocol Violations：违反HTTP协议的恶意访问；**  **HTTPoxy：阻止利用远程代理感染漏洞进行攻击；**  **Shellshock：阻止利用Shellshock漏洞进行攻击；**  **Session Fixation：阻止利用Session会话ID不变的漏洞进行攻击；**  **Scanner Detection：阻止黑客扫描网站；**  **Metadata/Error Leakages：阻止源代码/错误信息泄露；**  **GeoIP Country Blocking：根据判断IP地址归属地来进行IP阻断** | 防 SQL 注入；  防XSS攻击；  防盗链/黑链，畸形文件清理；  文件下载保护；  文件上传保护；  危险组件防护；  禁止执行程序；  响应内容保护；  IP黑白名单；  网页防篡改 | 防 SQL 注入；  防XSS攻击；  漏洞利用攻击防护；  溢出攻击防护；  防盗链/黑链/畸形文件；  敏感词过滤；  防非法请求；  防多线程下载；  文件解析漏洞；  HTTP请求防护；  禁止下载特定类型文件；  网页浏览实时防护；  网站后台防护；  登录防护；  高级防护功能：文 件上传漏洞防护、Struts2 漏洞防护、反序列化漏洞防护、任意文件读写漏洞防护和命令执行漏洞 | 无 | WEB应用防护，网站漏洞防护：SQL 注入攻击、XSS 跨站、Web 容器及应用漏洞 |
| 16.WEBSHELL网马/rootkit木马查杀 | **有。至少有三种不同的方法查杀：防病毒、HIDS入侵检测、基线测试** | 有网马/木马查杀 | 有。已知 WebShell 自动隔离、未知 WebShell 实时防护；  网页浏览实时防护 | 检测 Booitkit、Rootkit、应用后门、病毒木马、Web 后门 | 网站后门查杀；网马查杀；防御勒索、挖矿病毒 |
| 17.防网页篡改、防数据泄露 | **有。默认安全的文件权限设置，文档根目录、子目录、文件均为只读，防止普通用户创建、替换文件，防网页篡改、防数据泄露；**  **HIDS入侵检测对文件变化做监控及报警** | 有。网页防篡改（结合安全狗服云使用） | 有。当选择受保护的网站目录后， 其目录下的所有文件及子目录所有文件将禁止被篡改。对于允许修改文件的进程可以添加到 例外进程中（Windows） | 无 | WEB应用防护：网站访问控制 |
| 18.防端口扫描 | 有。只开放启用的服务对应的端口，除非允许，否则拒绝 | 扫描防护 | 有。通过限制单位时间内扫描端口数量， 并对扫描 IP 进行锁定来防护，并在发现端口被扫描时生成时间告警 | 无 | 有 |
| 19.DDOS 攻击检测和防御系统（防CC 攻击） | 基于规则的防DDoS、CC攻击 | DDOS 攻击检测和防御系统能够有效防御 CC 攻击 | CC 防护策略通过三个级别对服务器进行保护 | 无 | CC攻击防护 |
| 20.TCP转换 | TCP转换为WS/SSL，进而利用CloudFlare CDN实现TCP应用接入，达到网络应用加速、防DDoS攻击、隐藏服务器信息、防屏蔽中转、过WEB代理过滤、IPv4/IPv6接入等目的 | 无 | 无 | 无 | 无 |
| 21.数据库防火墙 | **连接真实SQL数据库，并过滤非法指令，保障数据库安全** | 无 | 应用防护，数据库应用 | 无 | 无 |
| 22.蜜罐Honeypot | **开启DNS、SSH、WEB服务器、WEB代理、KMS、防暴力破解等真实服务（仿真度更高），并查看相关日志（包括/var/log下的日志），将有恶意企图的不良IP加到“防火墙”的IP黑名单中** | 无 | 无 | 微蜜罐 | 无 |
| 23.弱点扫描 | **主动扫描本机或网络中其它主机，先于黑客发现OS及WEB等开放服务存在的漏洞，以利及时修补** | 无 | 无 | 资产清点 | 无（风险评估） |
| 24.时间控制 | **支持，几十种服务有不同的时间控制，一个时间定义包含多个时间段** | 无 | 登录防护，时间范围设置 | 无 | 无（定期巡检） |
| 25.流量控制 | **支持，针对WEB代理、VPN及NAT服务，每个用户按天、月、年等统计控制，可将VPN接入的应用转变为可计费、可运营的网络服务；针对每个来源IP不限协议进行总流量统计与控制，防止网络资源被滥用、防DdoS攻击、拖库等非法操作** | 网络流量监控 | 流量统计 | 无 | 流量画像 |
| 26.系统优化 | 对Linux 操作系统网络、系统配置等进行全面优化；  尽量启用使用kernel内核模块，提高系统性能及稳定性，包括ppp、l2tp、tun、ip\_tunnel、wg、se网桥、aes、 bbr等 | 对Linux 操作系统网络、系统配置等进行全面优化 | 智能分析服务器，扫描分析可以一键修改提升您服务器的安全性（Windows） | 无 | 无（资产管理） |
| 27.环境配置 | 对WEB、 PHP、SSL 环境配置进行加固，通过了绿盟、Nessus扫描器的弱点评估；  中性化服务器特征，防止被SODAN、FOFA等网络扫描标记，避免被零日攻击 | 对 PHP 环境配置、Nginx 环境配置进行加固，禁用相关风险配置 | 应用防护 | 风险发现 | 无（资产管理） |
| 28.集成软件 | **权威智能DNS服务器、大规模DNS域名库、DDNS服务器、WEB服务器、WEB代理服务器、VPN/SS/SSH服务器、VPN/SS/SSH/IPv6客户端、Stunnel/TLSProxy/KMS/BT客户端/NFS/CIFS/V2/Nginx服务，NAT/路由/流量统计等；**  **通过DNAT、VPN服务器、VPN客户端构筑Intranet安全网络，用于应用发布、资源共享** | 集成开源的 Nginx、PHP、MYSQL，轻松部署数据库及建立网站 | / | 无 | 无（资产管理） |
| 29.高可用性状态监控 | 定期检查系统负载；  定期检查进程健康；  NTP客户端、服务器，确保时间正确；  集成第三方集中管理Agent；  服务器状态监控，集中实时查看页面，阈值报警；  SNMP服务，远程状态查询，可自定义查询内容；  Netflow探针，留存流量的五元素信息；  实时显示IPv4、IPv6 TCP、UDP、ICMP及其它流量的会话统计及具体内容，快速了解系统网络流量的分布，方便采取进一步的措施，例如，将异常流量的IP添加到防火墙黑名单中等。配合最新、历史日志内容、日志统计，能快速全面地定位异常流量。 | CPU、内存、网络IO监控；  系统运行状态展示 | CPU、内存、网络IO监控；  系统运行状态展示 | 主机硬件配置：查看所有主机 CPU、磁盘、内存等相关信息 | 性能监控，对 CPU、内存、网络、磁盘的使用率进行监控 |
| 30.日志审计 | 18种日志，统计、查询、下载，无需第三方存储服务，留存本机N天，配合DNS、WEB、SSH等服务构成真实的Honeypot蜜罐 | 有 | 有 | 有agent日志 | 日志检索中记录了网站防护、登录防护、异常文件、性能监控、系统防护的日志 |
| 31.TOTP认证 | **IKEv2/IPSec、**  **OCSERV/AnyConnect、**  **PPTP、**  **L2TP、**  **OpenVPN/SSLVPN、**  **WireGuard、**  **SSH** | 无 | 无 | 无 | 无 |
| 32.自签名CA证书 | **支持，用于IKEv2、SSTP、STUNNEL、TJ、HTTPS代理等，第一次启动时自动生成，每台不一样** | 无 | 无 | 无 | 无 |
| 33.真实域名SSL证书 | **支持，用于IKEv2、SSTP、STUNNEL、TJ、HTTPS代理等，用户免安装CA证书；免费申请、自动持续更新证书** | 通过输入服云帐号用户名和密码，自动下载服务器证书 | 无 | 无 | 无 |
| 34.用户自服务WEB门户 | **支持，显示信息、资源、服务，修改口令，激活TOTP码，下载客户端配置文件、查看二维码；无需破坏安全的ActiveX插件，与VPN客户端功能分离，安全性更好** | 无 | 无 | 无 | 无 |
| 35.测试工具 | **WEB界面ping、traceroute、nslookup、端口扫描、带宽测试等** | 无 | 无 | 无 | 无 |
| 36.国际化 | **中日英等多语种界面，上架AWS国际云市场** | / | / | / | / |
| 37.管理接口 | **单机使用即可，不需要第三方注册管理（非SaaS模式），也无需安装agent客户端软件（存在软件供应链安全风险）；**  **通过命令行的方式调用WEBAdmin管理界面的功能，实现部署自动化；**  **管理员原子化；**  **通用文件堡垒机** | 云端、命令行 | 服务器端 Agent+远程控制台；  采用了 CS 架构的方式进行管理。需要安装服务器端 和 PC 端，通过 PC 端进行管理 | Agent+控制中心 | Agent+控制中心 |
| 38.隐私防护 | **防止VPN隧道建立后的DNS泄露及WEBRTC泄露真实IP；**  **无需注册，无需连接厂家服务器** | 无 | 无 | 无 | 无 |
| 39.设置复杂程度 | 一键安装、一页开局；设置十分简单，零基础设置；提供客户端配置文件及二维码 | 系统参数快速设置 | 一键巡检 | / | / |
| 40.自身安全 | **C语言前后台程序，非PHP、Java等解释型语言，没有源码泄露的隐患，内存少，运行快；**  **安全的SSL协议设置；**  **中性化服务器特征，防止被SODAN、ZoomEye、FOFA等网络扫描标记，避免被零日攻击；**  **有所在OS的安全补丁提示；**  **通过了绿盟、Nessus等扫描器的网络安全评估** | 系统体检 | 一键巡检；  服务器安全 | / | / |
| 41.IPv6支持 | **除个别服务外，全部几十种服务均支持IPv6，还提供IPv6隧道接入服务** | / | / | / | / |
| 42.在线帮助、视频演示、DEMO网站 | **完整的管理员、用户手册，以及在线帮助、视频演示、DEMO网站** | 有文档 | 有文档 | 有文档 | 无（需要先购买产品） |
| 43.免费版本 | **有，公众版12用户按季度更新免费使用，无需注册登记** | 需要用户注册，软件包已经不再更新 | 需要用户注册，软件包已经不再更新 | 无 | 无 |
| 44.交付方式 | **无需人工，即买即用，镜像商品** | 人工服务类商品 | 人工服务类商品 | 人工服务类商品 | 人工服务类商品 |
| 45.产品使用及许可证验证 | **和厂家服务器、云API无关，IP保密，内网、专网可用** | SaaS方式必须连接厂家服务器才能使用 | SaaS方式必须连接厂家服务器才能使用 | SaaS方式必须连接厂家服务器才能使用 | SaaS方式必须连接厂家服务器才能使用 |
| 46.付费周期 | **按需（1小时起）、**  **包年包月** | 包年 | 包年 | 包年 | 包年包月 |
| 47.正式版价格 | 适中 | 高 | 高 | 极高 | 极高 |

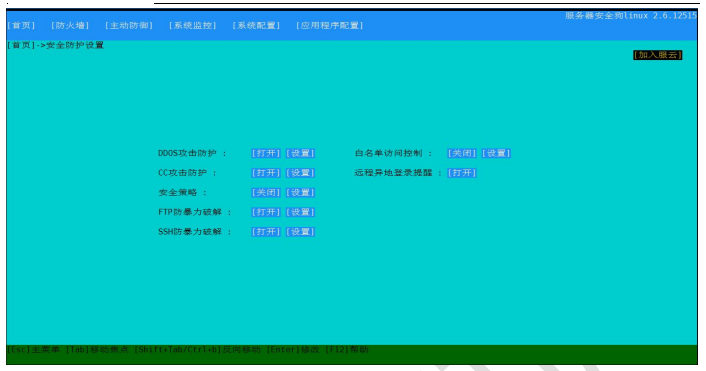
**表2 Linux EDR产品综合比较表**

**二、WEB管理界面示意图**

以下截图是上述几家产品的WEB管理界面示意图。



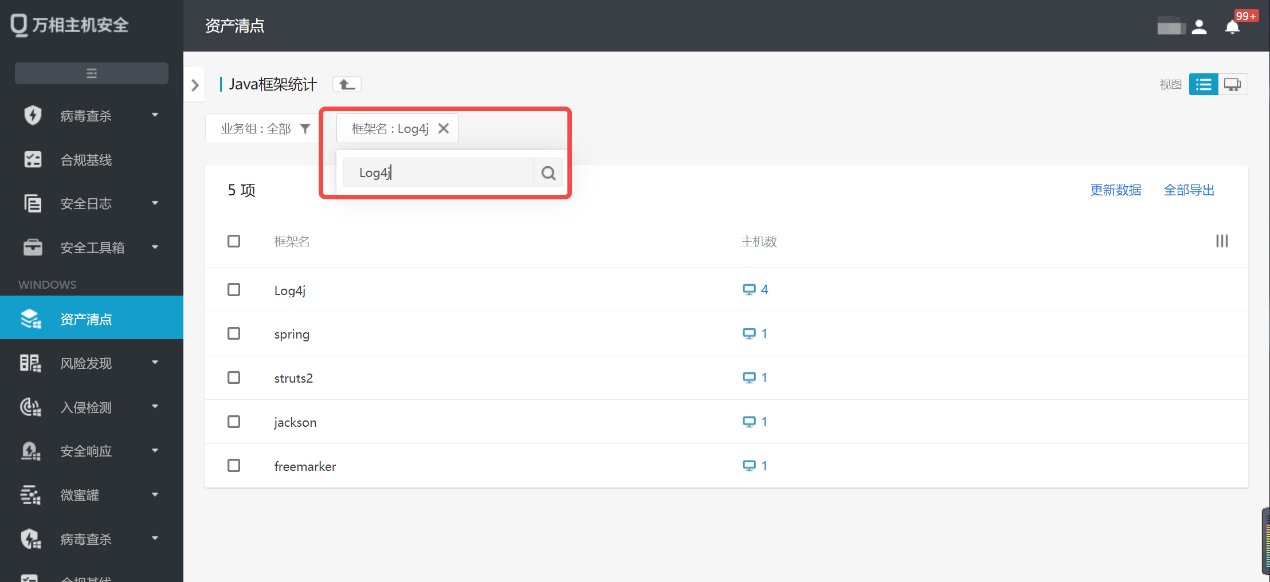
**图1 中神通大地云控WEB管理界面示意图**



**图2 安全狗管理界面示意图**



**图3 云锁WEB管理界面示意图**



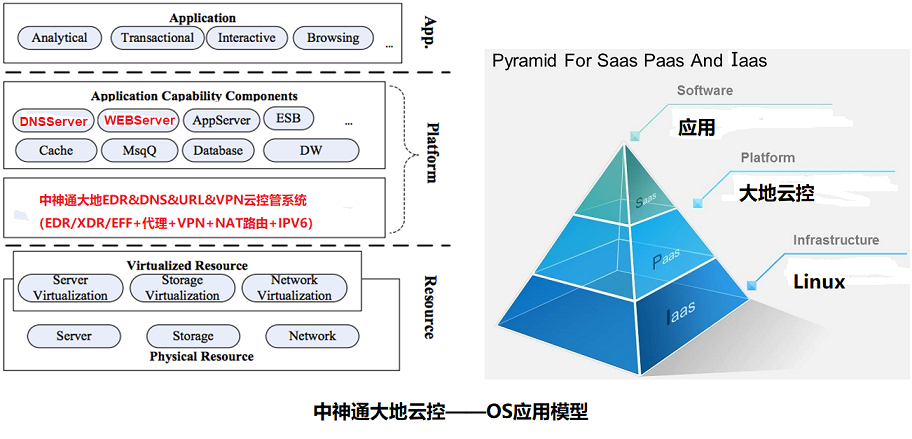
**图4 青藤万相WEB管理界面示意图**

****

**图5 安恒明御终端安全及防病毒系统(EDR)**

**三、中神通大地云控简介**

中神通大地EDR&DNS&URL&VPN云控管系统（简称大地云控/TrustGate）是一套专业的终端网络安全防护及互联互通网络应用增值软件，可将硬件、虚拟化平台打造为IPv4/IPv6双栈分布式云路由器/云原生安全接入网关（DNS/WEB/VPC/NAT/VPN/WAF/EDR/负载均衡/CASG/SASE/SD-WAN），为线上线下OS应用软件/SaaS/PaaS提供**全面防护、互联互通的数字化安全网络底座**。



借助于云计算模型的IaaS、PaaS、SaaS分类，把Linux Stack也做同样的分类，中神通大地云控处在SPaaS层（Security Platform as a Service），包括终端网络安全防护，网络服务器、客户端、路由器，以及安全的DNS、WEB、数据库应用服务器，具体如上图所示。

​中神通大地云控EDR/XDR/EPP全家桶能全方位保护主机及应用安全，包括防火墙、防病毒（文件系统实时防护）、HIDS入侵检测、即插即用安全WEB服务器、WAF防火墙、数据库防火墙、主机安全加固（自动升级系统，修补安全漏洞、安全审计、基线测试、漏洞检测、rootkit检测、WEBSHELL检测、弱口令检测）、蜜罐、时间控制等功能。

**参考资料**

中神通大地EDR&DNS&URL&VPN云控管系统（大地云控）

http://www.trustcomputing.com.cn/cn/index.php/product/dns-url

https://market.aliyun.com/products/56812015/cmjj034510.html

https://marketplace.huaweicloud.com/contents/7bb75ddd-5f06-4a58-bc01-b5eec1ed7800

https://market.cloud.tencent.com/products/30287

服务器安全狗Linux版V2.8使用手册

http://down.safedog.cn/download/software/safedogfwq\_linux\_Help.pdf

安全狗·云安全系统Ubuntu 14.04 64 位镜像使用说明手册

https://oss.aliyuncs.com/netmarket/product/ca5cbfbd-df7c-4ae5-9666-8732b4400b2d.pdf

云锁网站安全防御系统 V3使用手册

https://market-cdn.yonyoucloud.com/ffe81ea5-d272-4d7f-b96f-efaf9d40d3ea\_%E4%BA%91%E9%94%81V3%E4%BD%BF%E7%94%A8%E6%89%8B%E5%86%8C\_1.0.pdf

青藤云安全\_4合1产品使用手册v3.3.0.3

https://portal-data-cn.obs.cn-north-4.myhuaweicloud.com/marketplace/public/app/attachment/20220407/49b06e74-c9ba-4d2f-b198-cea781454ec9/2204070259145689.pdf

安恒明御®终端安全及防病毒系统（EDR）

https://www.dbappsecurity.com.cn/product/cloud158.html

https://www.yun88.com/product/2749.html

明御®主机安全及管理系统操作手册

https://pek3b.qingstor.com/cloudmarket/public/ca-wivqxznn