华为乾坤安全云服务

随着企业业务不断的数字化、云化，网络在企业运营中占据的位置愈发重要。出于破坏及获利目的，网络攻击者通过身份仿冒、网站挂马、恶意软件等多种方式进行网络渗透与攻击，影响企业网络的正常使用，网络安全建设成为刚需。本地部署防火墙、IPS、沙箱、漏洞扫描、态势感知等多种安全产品是当前防护企业网络安全的主要方式，但是受限于专业安全人员不足，不少单位并不能较好的应用这些安全产品从而达到良好的安全防护效果。部分安全产品上线后无人关注安全告警、缺乏及时调整安全防护策略，导致安全防护效果差强人意、安全事故频发。

企业采用传统的安全建设方式，往往存在着投资大、运维难、效果不理想的困扰。针对传统安全方案无法适配广众用户安全诉求的现状，华为全新推出乾坤安全云服务。华为乾坤安全云服务采用云边一体创新架构，华为安全云平台在云端提供多种安全能力和云端专家运维能力；华为天关作为本地防御节点，结合云端智能分析与安全专家能力为用户提供防护、响应一体的云化安全服务。

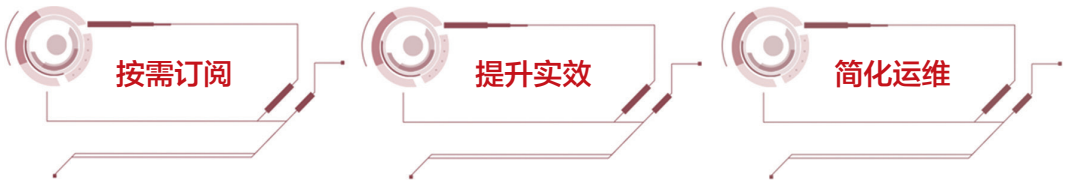
HUAWEI

创新架构

华为乾坤安全云服务采用云边一体创新架构，部署在本地的天关作为安全防御节点将对进出网络的流量进行深度安全检测，提供IPS、反病毒和URL过滤等安全检测/拦截能力。

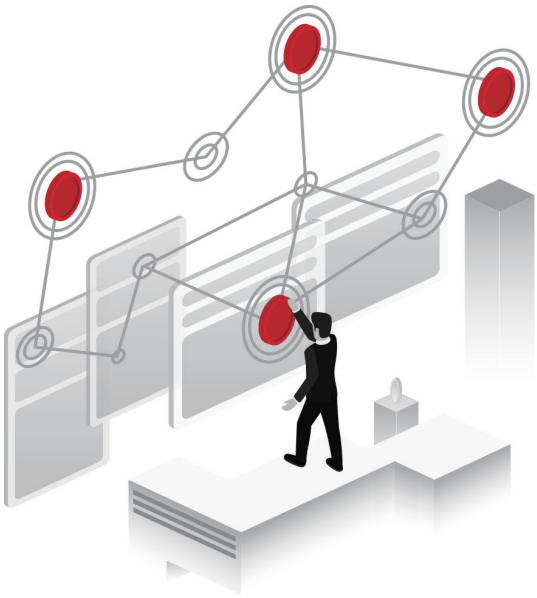
同时，天关会将检测到的安全事件以及取证信息上传至华为安全云平台，在云端华为安全运营专家将借助智能大数据分析技术并结合自身攻防经验为用户进行安全事件的分析与响应。在用户授权情况下，安全运营专家将通过黑白名单策略为用户阻拦高危攻击源的持续攻击行为。用户侧则大幅减少本地运维的投入，直接通过华为乾坤安全云服务提供的紧急告警短信、邮件周报/月报等内容轻松了解网络安全防护状态，直达网络安全防护效果。在遇到本地运维难以处置的安全事件时，用户还可以求助云端MSSP（安全托管服务商）服务专家来提供应急指导或处置服务，第一时间响应、闭环紧急安全事件。

亮点



安全云服务按需订阅

乾坤安全云服务提供多种安全能力按需订阅：威胁信息关联分析、安全日志分析、入侵防御、反病毒、URL远程查询等，并且安全能力持续增加。多种安全能力根据场景需要开通和关闭，只需很少的安全投资，即可完全替代在本地部署多种传统安全产品。



安全云服务提升实效

云端专家深入攻防对抗过程，整合安全能力，全局统筹，快速准确识别复杂攻击，云端自动应对业界最新漏洞与攻击方法，一处发现威胁，全局快速免疫。

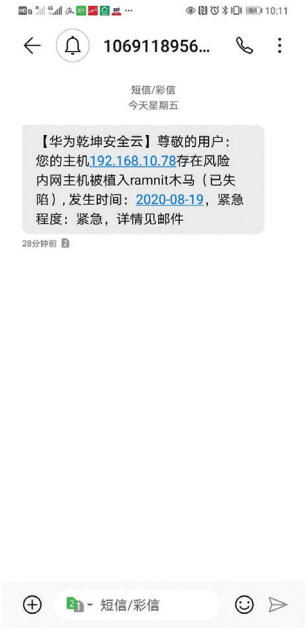
天关作为安全防御节点在实现本地安全检测后，会将安全告警/取证信息上传至云端平台，云端安全运营专家将针对用户处发现的每一条安全告警进行统一分析。凭借云端可信签名、误报检测模型等多项智能分析技术，安全运营专家将准确剔除现网误报，威胁检测准确率高达99%，实现一处检出、全网免疫。通过为用户提供精准的安全告警事件，指导用户对失陷主机、高危攻击事件等进行及时处置。同时，基于安全误报事件，云端还将快速实现检测规则优化，实时更新天关的检测防护能力，不断提升本地防护效果。

自动拦截，分钟级响应效率。在用户授权前提下，华为安全运营专家还将结合全局威胁信息对用户网络产生威胁的攻击源IP进行及时处置，通过黑白名单联动功能下发至天关，阻断攻击源的持续、高级渗透攻击行为，使得攻击响应效率由小时级提升至分钟级。

安全云服务简化运维

网络安全实效的达成离不开专业人员的运维，华为乾坤安全云服务云端专家+智能分析降低本地运维难度，专家解决安全“疑难杂症”。

- 云端安全专家7*24小时在线，解决最新安全网络问题；
- 利用智能分析能力提升自动运维效率，自动拦截攻击，响应效率由小时级提升到分钟级；
- 按周、按月提供安全报告，紧急事件短信通知；
- App随时检查网络安全状态评分，处置安全事件。



部署

华为乾坤安全云服务以云化模式实现简易部署，除本地部署天关作为安全防御节点外，无需在用户现网部署其他产品硬件，可在不改变现有网络拓扑情况下实现服务部署。

整体服务中的天关内置云端专用通信服务模块，用户只需为天关配置一个具有访问外网权限的IP地址，即可自动与华为乾坤安全云服务平台完成可信认证，实现加密连接，支撑华为乾坤安全云服务的秒级上线。

应急响应

华为乾坤安全云服务基于云端共享安全专家资源，通过技术手段将专家能力注入平台，实现专家安全运营服务标准化提供。在出现紧急需要处理的安全威胁事件时，按需提供应急响应服务，做好安全服务“最后一公里”。

安全能力

安全云服务功能项	
定期周报月报	基于安全防护事件，定期生成周报、月报，并通过邮件发送至用户邮箱。
紧急安全通知	基于安全防护事件，提取紧急通知，并同时通过短信、邮件两种方式通知用户。
监测、断网内网问题主机	基于已知流量特征，监测发现内网问题主机并切断问题主机外联行为（如C&C、远控、对外攻击等行为）。
恶意网站访问拦截	基于已知的恶意网站域名库，拦截网络内的恶意网站访问行为。
阻拦已知的钓鱼邮件、恶意软件传输	基于已知的文件特征与检测能力，阻拦钓鱼邮件、恶意软件（如病毒、木马）的传输行为。
不良应用及网站访问行为过滤	可实现基于IP、IP段、应用（类别）、网站（类别）规范网络中应用及网站访问行为。
应用及网站访问可视化	监测内部用户应用及网站访问行为，按周/月提供统计分析报表。
安全事件可视化	针对所有安全事件，按周/月提供统计分析报表。
安全事件分析	利用智能分析技术结合专家人工手段对防护节点检测到的安全事件进行分析确认，保障攻击拦截以及安全告警的准确性，及时优化攻击识别规则，提升现网防护效果。

安全云服务功能项	
入侵防御	准确检测并防御针对操作系统、应用、服务器等各种漏洞的攻击，支持0 day攻击防护。
防病毒	支持流检测和病毒引擎全文检测双检测模式，流模式支持500万种病毒。
攻击源自动阻拦	对基于安全事件分析的结果产生外部高危（持续攻击、复合攻击）攻击源进行黑名单下发，直接阻拦其后续的攻击行为。【需要客户注册云端账号时授权】

配套华为天关硬件规格

型号	天关510（USG6501E-C）	天关520（USG6502E-C）	天关530（USG6503E-C）
固定接口	2*GE WAN+8*GE Combo+2*10GE(SFP+)	16*GE(RJ45)+8*GE Combo+2*10GE(SFP+)	
产品形态	1U		
尺寸 (W×D×H) mm	442×420×43.6		
存储	选配，支持M.2卡，64G/240GB	选配2.5英寸形态硬盘，支持SSD 240/HDD 1TB	
电源	标配单电源，选配双电源		

订购指南

产品	型号	描述
USG6501E-C	USG6501E-C-AC	USG6501E-C交流主机 (2×10GE(SFP+)+8×GE Combo+2×GE WAN，1交流电源，含SSL VPN100用户)
USG6502E-C	USG6502E-C-AC	USG6502E-C交流主机 (16×GE+2×10GE(SFP+)+8×GE Combo+2×GE WAN，1交流电源，含SSL VPN100用户)
USG6503E-C	USG6503E-C-AC	USG6503E-C交流主机 (16×GE+2×10GE(SFP+)+8×GE Combo+2×GE WAN，1交流电源，含SSL VPN100用户)

产品	型号	描述
基本License		
云服务授权	LIC-USG6501E-C-CSS-1Y	云服务12个月 (适用于USG6501E-C，天关510)
	LIC-USG6501E-C-CSS-3Y	云服务36个月 (适用于USG6501E-C，天关510)
	LIC-USG6502E-C-CSS-1Y	云服务12个月 (适用于USG6502E-C，天关520)
	LIC-USG6502E-C-CSS-3Y	云服务36个月 (适用于USG6502E-C，天关520)
	LIC-USG6503E-C-CSS-1Y	云服务12个月 (适用于USG6503E-C，天关530)
	LIC-USG6503E-C-CSS-3Y	云服务36个月 (适用于USG6503E-C，天关530)