1 行业背景

运营商的云计算中心是我国政府信息化建设的关键，随着云计算中心信息化程度的提高，对信息系统的依赖程度亦越来越高。同时，整个云计算中心信息系统所面临的各种安全风险也日渐严重，如何更好地为云计算中心信息系统提供安全保障，确保云计算中心的安全运行和信息化的健康发展，乃重庆市联通云计算中心网络和信息系统建设所面临尤为重要的问题。

目前针对云计算中心的 APT 攻击事件的日益增多，其组织化、潜伏性、持续性、利用 0day 漏洞的攻击特点，导致目前大多数采用的传统信息安全防护体系难以奏效。同时，对于云计算中心管理人员来说，相关系统的信息安全管控能力也受到了前所未有的挑战。

云计算中心迫切需要防止云平台被恶意利用，并且在出现安全隐患时能够准确、有效、及时的实施对恶意行为的定位、取证及追责，从而更好保护正常用户和云计算中心的正当权益，维护云计算中心安全可靠运行。

云计算中心根据自有云平台系统运维经验，提出了信息安全安全要求：

1.1 传统安全设备的合理利用

云计算中心现有网页防火墙 WAF、网络防火墙、IPS 等传统安全设备，在一定程度上对云计算中心现有网络提供了部分安全防护措施，依靠防火墙、路由器 ACL 等对不同安全等级的网络区域进行划分，比如生产、办公、测试、开发、互联网、第三方等，对已经开通的防火墙和 ACL 策略加强管理、及时更新规则库等信息，也及时调整和删除的冗余策略，尽量避免范围过大策略等边界收紧不到位的情况。

1.2 针对新的威胁或可预见性威胁时，及时做出应对策略

由于云计算中心网络客观上总是存在外部接入内部的网络渠道，而且随着互联网的发展，内外部互联互通信息的需求越来越多，攻击者总能找到入侵内部的一条可以用的通道，可能是邮件、貌似正常的 Web 网页数据上传、第三方数据传输通道、各分支机构管理不善开了例外的终端等等，另外由于传统安全设备无法有效的应对恶意代码变形、加壳等隐蔽手段；APT 攻击通常利用看似合法的

输入和非明显恶意特征，但非常针对性的程序代码。对于突破边界后在内网埋伏、感染、操控内部服务器及数据的恶意行为识别和监测缺乏有效手段。在这样新的攻击模式下采用新的技术应对已是必要的手段和措施。

2 痛点及需求

由于传统的防御体系侧重于互联网、第三方等边界的网络安全防护，对于突破边界后在内网埋伏、感染、操控内部服务器及数据的恶意行为，识别和监测缺乏有效手段。面对现在攻击的专业性高，组织性强的黑客团伙，仅靠传统安全设备自身进行防护显得力不从心。如何快速提前获取 0day 攻击恶意代码特征与文件路径、黑客远程控制服务器 IP 地址、钓鱼邮件地址、假冒网站异常威胁情报，并及时与内部防护系统联动，成为云计算中心安全防护的重要保障关键能力之一。同时就现在专业的攻击，单独看每一个步骤可能无法准确判断单个行为是否是恶意攻击，但是如果将整个路径上的行为串起来看是很有可能发现异常行为的。例如：建立一种基于外部连接的异常分析模型，这一方面需要大量的信息安全日志数据作为支撑，包括内外网边界及关键路径上的网络流量情况、服务器设备的异常行为检测情况、恶意远程通讯 IP 地址等外部威胁情报等；另一方面需要有实时快速处理海量数据和建模关联分析的能力，以及可视化展现能力，毕竟可疑事件最终还是需要人工准确判断。以上关键环节的薄弱点正是我们目前静态的、被动式防御体系的薄弱点，传统的安全防护体系已经逐渐不能满足外部攻击防护的需要。

综上所述云计算中心迫切需要建设云平台服务器安全监测工程，对云平台的安全防护体系扩展完善，满足云计算中心的业务发展需要。

3 解决方案

围绕下一代安全防御目标，加强对网络入侵方面的检测，可部署**天蝎 Web 威胁监测与溯源系统**，整体提升了运营商云计算中心的安全监测、威胁检测及应急响应能力，针对来自于 Web 的攻击和破坏行为进行重点监测。同时在操作系统层面，采用安全可控的 Windows10 神州网信政府版桌面操作系统，解决操作系统层面安全问题。

主要体现以下几个方面：

- 建设网站攻击监测统一平台；
- 基于威胁情报的黑客画像；
- 监测与溯源分析一体化平台；
- 通过大数据技术发现更多的攻击和破坏行为（建设集中统一的数据中心存储和管理全部业务数据，便捷的攻击行为与破坏行为线索挖掘检索能力，各种攻击破坏事件数据的关联分析能力）。

4 客户认可的价值

天蝎 Web 威胁监测与溯源系统部署完成以后，信息安全防护体系正朝着如下的四个方向进行转变：

- 由被动监控向主动预防转变。
- 由边界安全向全网安全转变。
- 由静态特征识别向动态异常分析转变。
- 由系统安全向业务驱动安全转变。

最终，信息安全的所有问题本质上将转变为大数据分析问题。传统的应急式安全响应中心将转变为持续安全响应中心。

同时**天蝎 Web 威胁监测与溯源系统**主要能解决用户以下安全需求：

- 通过对实时流量的分析对 Web 攻击的实时监测，识别针对于 Web 的各类尝试攻击攻击，识别各类网页后门及变种。
- 对 Web 攻击的分析，实现了黑客指纹提取和归类，对攻击者进行溯源。建立了攻击事件分析，提供攻击数据的全包分析。实现了攻击武器的识别和黑客画像，并完成攻击者组织实体模型分析。
- 关联和聚合危险性极高的 Web 风险，针对于危险性极高的拖库，网页篡改，水坑攻击的攻击方式进行关联和聚合。
- 对攻击态势特别是对攻击强度和烈度的可视化展示。
- 多服务器协议的安全检测，包括邮件 FTP，Telnet，文件管理等。