阿里云
阿里政务云

重保应急方案

文档版本：20190730

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 确定。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *`[-all|-t]`*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *`{stand | slave}`*

目录

1 重保应急原则

政府重大事件期间，阿里云提供重点保护云环境业务的服务，可调用全阿里集团的力量，进行统一的封网流程和时间的规划和实施，为重大政务活动保驾护航。

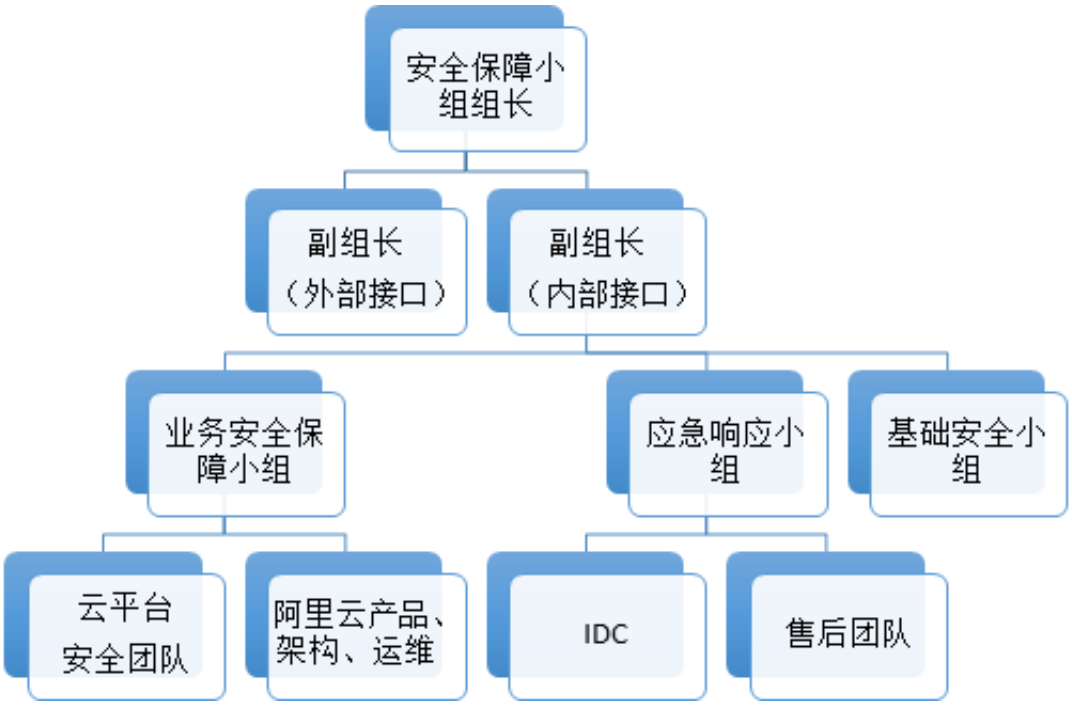
重保封网期间对政务云平台的变更有严格要求：紧急度较高的线上故障处理一般遵循服务团队的用户通知流程；常规紧急变更需提前申请，待评估审批后才能实施变更，保障政务云平台及云产品的稳定性。

此外，政务云提供重保服务时，会组建重保团队，根据情况定制重保封网期的应急预案，为各类安全隐患定制安全防护解决方案。

组建重保团队

重保团队至少包括：

- 组长：就应急保障工作进行整体管理与协调。
- 副组长（外部接口）：就来自各部委相关应急工作进行应急响应及外部协调工作。
- 副组长（内部接口）：就实地应急进行保障与落地。



应急响应与保障，根据情况可设置业务安全保障小组、应急响应小组、基础安全小组等角色。

应急联络规划

为确保政府重大事件云环境相关业务保障期间阿里云能对各类紧急事件及时响应，在成立重保团队之外，也会规划重保期间的应急联络规划：

- 开通应急保障专线电话及各种网络应急专号。
- 专线电话由应急保障小组成员7*24小时负责接听，采取5分钟响应机制，协调处理各类与阿里云相关的安全事件。

应急预案

应急预案计划在落地前需与商务、法务等团队确认重保范围和职责，再与安全GOC以及合规团队确认落地方案。方案具有一定的统一性，但均会根据重保场景定制个案方案。以下为您介绍常见的对政务云平台的被攻击风险，以及通用的应急预案方案。

常见的被攻击风险包括：

攻击类型	攻击原理	风险说明
DDoS攻击	DDoS全名是Distributed Denial of service （分布式拒绝服务攻击），是指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动拒绝服务攻击，从而导致目标无法正常访问。	可能导致重点保护目标在政府重大事件云环境相关业务保障期间不可访问／不可提供服务，造成负面社会影响。
Web攻击	web攻击是指针对web应用发起的攻击，比如SQL注入、XSS、文件上传等攻击。	可能导致重点保护目标网站在政府重大事件云环境相关业务保障期间被篡改／不可提供服务，造成不可接受的负面影响。
暴力破解攻击	暴力破解攻击是指攻击者通过系统地组合穷举所有可能性（例如登录时用到的账户名、密码），尝试所有的可能性破解目标的账户名、密码等敏感信息。	暴力破解攻击旨在获取重点保护目标服务器权限后造成进一步的破坏 （依赖重点保护目标是否在互联网上开放22/3389等远程管理端口以及3306/1433/1521等数据库端口）。
注马攻击	云内主机被注马属于云上用户应用端带来的风险，目前不在阿里云基础设施管理范畴，需要用户允许在其应用内提前部署必要的安全产品与策略才可达到预防效果，阿里云正在紧急通知各重保单位开始共同采取预防方案，并同时制定应急响应策略，确保政府重大事件云环境相关业务保障期间的安保工作。	

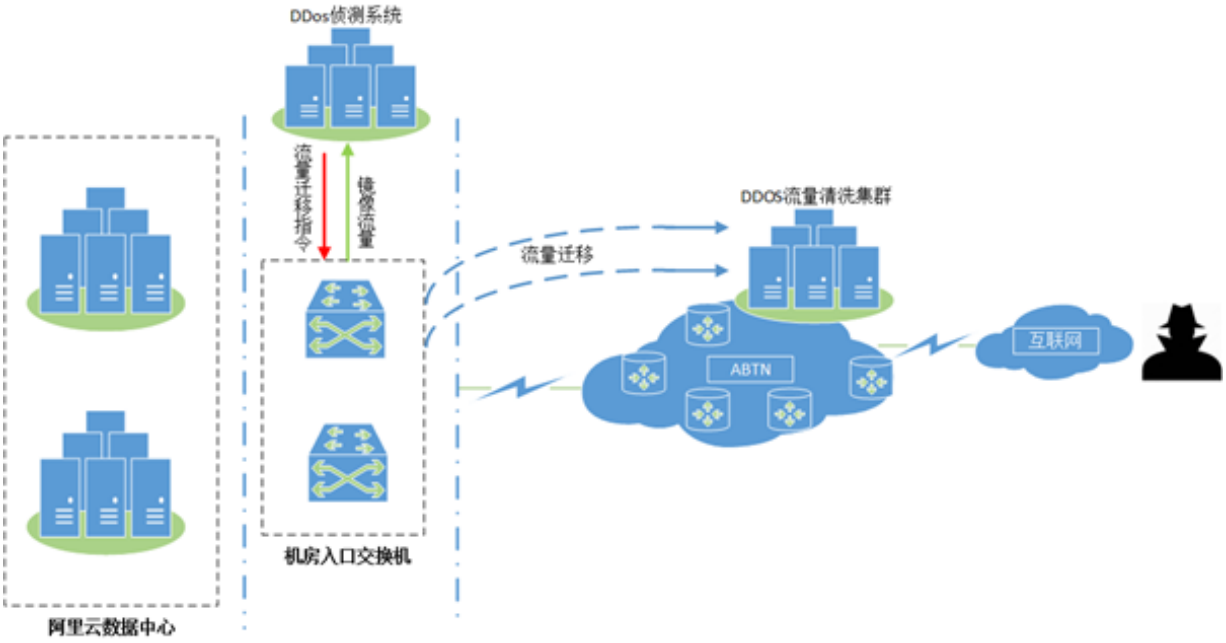
针对以上常见的攻击及带来的风险，阿里政务云分别制定了对应的预防方案，详细方案需根据实际防护需求和场景定制，通用方案制定原则和说明可参考DDoS防御方案、Web攻击防御方案、暴力破解攻击防御方案和注马攻击防御方案章节。

2 重保防御解决方案

2.1 DDoS防御方案

针对DDoS攻击，政务云在公网入口部署了DDoS识别系统，可以自动检测到攻击行为，并且针对被DDoS攻击的流量直接牵引后进行流量清洗回注进行防御。

分布式拒绝服务攻击（DDoS攻击）是一种针对目标系统的恶意网络攻击行为，DDoS攻击经常会导致被攻击者的业务无法正常访问，也就是所谓的拒绝服务。对于此类攻击来说，用户除了自己架构做好全面的防护以外，仍需做好业务监控和应急响应，特别是对于风险的预估和预判，通过这些信息可以提前采购适合的商业安全方案。



方案说明

在本方案中，虽然阿里政务云已经提供了安全防护措施，但用户仍旧需要选择多款阿里云产品及其自带的功能来构建安全体系：

- 配置安全组：尽量避免将非业务必须的服务端口暴露在公网上，从而避免与业务无关的请求和访问。通过配置安全组可以有效防止系统被扫描或者意外暴露。
- 使用专有网络（VPC，Virtual Private Cloud）：通过专有网络VPC实现网络内部逻辑隔离，防止来自内网肉鸡的攻击。
- 优化DNS解析：通过智能解析的方式优化DNS解析，可以有效避免DNS流量攻击产生的风险。

采用安骑士，WAF等安全产品再结合服务器安全加固，提升服务器自身的连接数等性能。对服务器上的操作系统、软件服务进行安全加固，减少可被攻击的点，增大攻击方的攻击成本。

方案优势

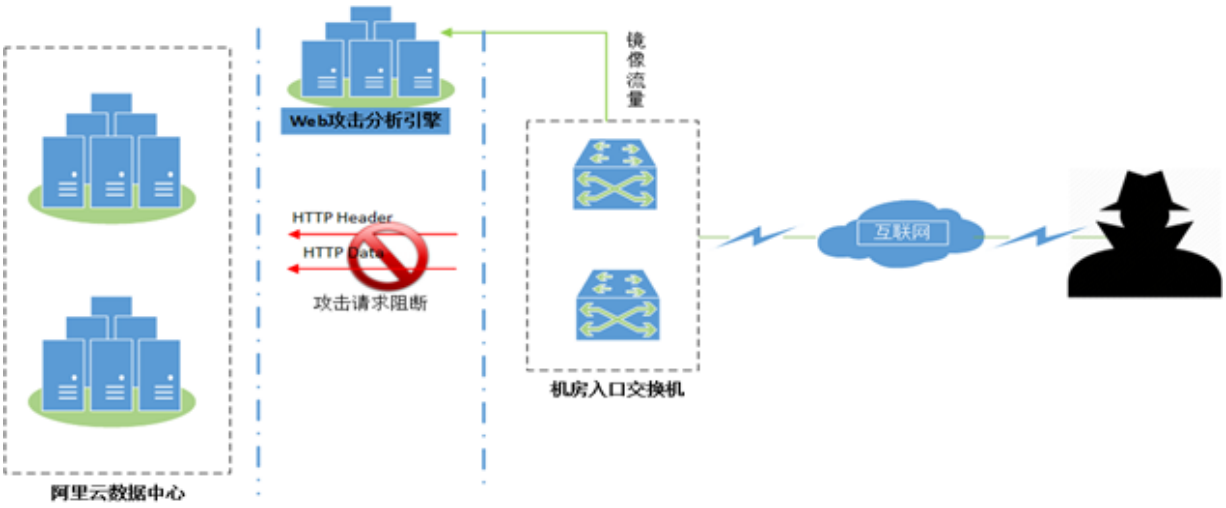
- 高性价比：无需采购全套安全产品便可以防护住大部分的DDoS攻击，且给后续情况恶化时的进一步弹性升级预留了充足的空间。
- 体系完善：不仅从云平台的角度，更考虑到了客户业务的多变性和个性化，从而不用“一棒子打死”的粗糙手法确保了安全却影响了业务。这种细分颗粒度的安全管控和以白名单、黑名单以及专有网络隔离、账号隔离的方式来进行管理维护。
- 运维轻松：运维人员无需时刻关注集群情况，而是可以通过云监控等报警信息来保持高效运维，并且可以通设定预案来面对紧急情况，例如资源的弹性扩容，DDoS防护的弹性增加等等。
- 使用安心：阿里云的机房资源可以帮助任意客户在海量DDoS到来时进行防御，无需担心阿里云本身无法承受。

针对阿里云政务云机房的客户，阿里云协调资源，可以为客户最大抵抗300G的攻击流量。

2.2 Web攻击防御方案

针对云上主机的Web攻击（包括但不限于sql注入，远程代码执行，文件包含等），部署在云机房外围的旁路WAF系统会通过其上的规则／模型实时识别web攻击并对识别到的web攻击进行阻断（类GFW，双向reset），以保护云内主机的安全。

web攻击是最常见的一种攻击类型，在此场景中，我们推荐使用阿里云的：web应用防火墙来抵御web攻击。



方案说明

一般情况下，只需要使用最低配的web应用防火墙即可防御大部分的低级攻击，但如果是政府部门则有可能会成为黑客的重点目标，所以在采用web应用防火墙时，我们需要注意利用这个产品的几个特性和优势：

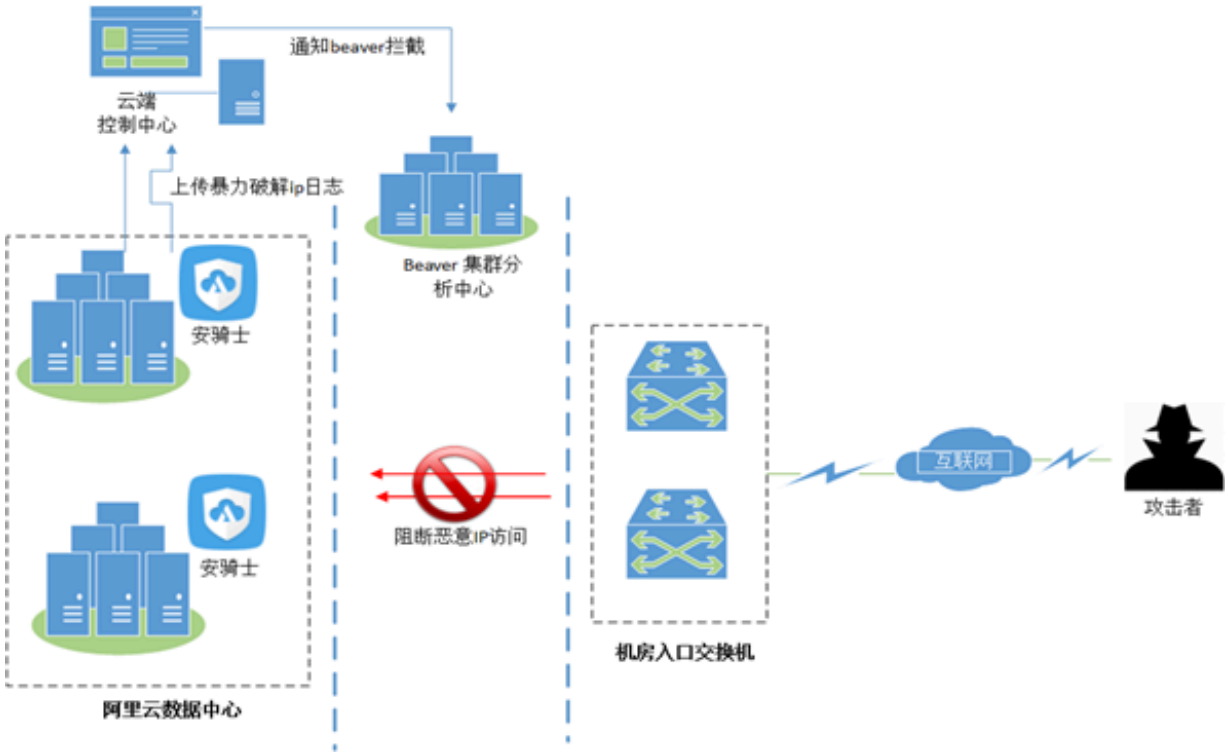
- 防数据泄密，避免因黑客的注入入侵攻击，导致网站核心数据被拖库泄露。数据库的泄露会导致大量内部数据被窃取，造成恶劣影响，这是阿里云安全主要防范并且提供众多安全产品的主战场之一。
- 防恶意CC，通过阻断海量的恶意请求，保障网站可用性。通过使用CC攻击可以使得政务网站宕机，从而影响民众的使用，而防恶意CC攻击的功能则可以解决这个问题。
- 阻止木马上传网页篡改，保障网站的公信力。政府网站被攻击挂马已经不是罕见的事情，政府公信力会遭受影响，所以使用web应用防火墙来阻止木马上传是非常具有性价比的功能。
- 提供虚拟补丁，针对网站被曝光的最新漏洞，最大可能地提供快速修复规则。安全防护不仅仅看的是短期的事情，更是长期防御，而长期防御就不能是死守等候，而是要随着时代，科技的发展不断更新其安全防御措施，才能够不被入侵。阿里云的虚拟补丁提供数量以及速度都属于全球领先，所以不用担心会被时代淘汰。

此方案的优势在于可以充分利用阿里云安全在全球的高水准，无需自身运维人员达到这个水平即可轻松使用，并且阿里云安全更会提供诸如：精准访问控制，友好访问观察等等动态调整的功能来使得安全体系不仅完善，更具备柔性。

2.3 暴力破解攻击防御方案

当前暴力破解暂无系统免费防御方案，仅有商业安全解决方案。云内大部分主机部署安骑士，针对识别到的暴力破解源加入旁路WAF的阻断名单进行实时阻断（TCP层，双向reset），阻止其后续的暴力破解行为。

为了避免暴力破解，政务用户可以云盾爬虫风险管理（Anti-Bot Service，简称Anti-Bot）是一款网络应用安全防护产品，可有效检测高级爬虫，降低爬虫、自动化工具对网站业务的影响。云盾爬虫风险管理提供从Web、APP、到API接口一整套全面的恶意Bot防护解决方案，避免由于业务中某一环节的防护薄弱而导致的安全短板。



方案说明

购买开通Anti-Bot产品后，您只需要将您的网站域名解析到Anti-Bot产品提供的CNAME地址，并在爬虫风险管理控制台中配置源站服务器IP，即可启用防护。将网站域名接入Anti-Bot产品后，您网站所有的公网流量都将先经过Anti-Bot实例，所有恶意爬虫流量都将在云端被检测、过滤，最终将正常的流量返回给源站服务器，从而确保源站业务免受恶意爬虫流量引发的数据泄露、业务欺诈等安全问题的影响。

暴力破解兜底方案：在政府重大事件云环境相关业务保障期间，一旦发现严重违规行为，一键执行切断云上对重点保护目标的访问权限（通过旁路reset）。安装阿里云安全产品后，上述所有风险由系统识别后实时通知用户处置，使用者在系统上一键操作后即时生效。

方案优势

- 充分利用阿里云在安全领域里的情报汇聚能力：

  通过跨多行业的爬虫行为分析，利用关系网络实现恶意爬虫的扩充发现。爬虫在行业性业务目的方面非常明确，利用生态体系达成行业内协同防御。沉淀网络黑灰产业中已知常用的针对性恶意爬虫的IP/User Agent数据。共享亿级由阿里巴巴集团业务经验沉淀的风险情报。

- 多场景多维度的安全防护

  提供最合适Web、H5、APP、API业务的恶意Bot防护方案。提供多维度的防护策略，更精准地刻画恶意Bot特征。针对不同风险等级的恶意Bot，提供不同的处置手段。

2.4 注马攻击防御方案

云内主机遭受木马注入攻击（简称注马攻击）属于云上用户应用端存在的安全风险，目前不属于阿里云基础设施管理范畴，需要用户允许在其应用内提前部署必要的安全产品与策略才可达到预防效果。

阿里政务云建议各个政府单位提前准备预防方案，并制定应急响应策略，确保政府重大事件云环境相关业务保障期间的安保工作。

被注马的虚拟机对非阿里云业务发起攻击处理

针对重保网站，阿里政务云采取对所有虚拟机（特别是承载web应用和网页）进行封闭端口通信模式以阻止攻击，仅保留80端口以保障重保网站可以通过80端口与阿里云上的资源间的互联网交互，该方案基本保障重保业务不受影响。

方案风险：如果有重保网站与阿里云上资源间有非80端口间的通信会在政府重大事件云环境相关业务保障期间受到影响。

被注马的虚拟机对阿里政务云内用户发起攻击处理

针对重保网站（特指部署在阿里政务云内），阿里政务云将安排专人与相关客户沟通并协助客户在主机内部安装特定商用的安全防护产品并调整安全组要求，以确保该用户不会遭受到来自云内其他被注马用户主机发起的攻击，从而保障重要用户的政府重大事件云环境相关业务保障安全。

方案特别需求：由于需要在客户端进行安装，并依据客户情况进行安全组建，故此，需要重保客户接受相应的安全服务。

阿里政务云建议政务用户可以分别采用以下产品如范此类攻击：

- 先知：

  在业务代码上线前，进行代码安全测试、白盒代码审计等。杜绝代码级别可能存在的重大风险和漏洞。
- 自动更新：

  政务用户需要开启云盾以及虚拟机上的自动补丁功能，在业务允许的情况下通过日常运维，定期检测并修补网站本身以及网站所在服务端环境的各类漏洞，及时更新操作系统、应用服务软件补丁、软件补丁等。
- Web应用防火墙：

  一般情况下，只需要使用最低配的web应用防火墙即可防御大部分的低级攻击，但如果是政府部门则有可能会成为黑客的重点目标可参考方案说明章节。

网页防篡改

由于网页防篡改与网站建设及网站应用漏洞有直接关联，属于用户安全责任范畴，阿里云无法直接进行处置，故此，建议政府重大事件云环境相关业务保障重保用户选择阿里云平台上的安全合作伙伴的商业服务，如安恒公司提供的防篡改服务，以达到防篡改的效果。