黑龙江亿林网络股份有限公司
政府门户网站等级保护解决方案

政府门户网站是“政务公开”和“服务型政府”两大主导思想，在落实过程中所必须凭借的重要平台，在未来的电子政务规划中，政府门户网站必将占有非常重要的地位。国家正在逐步推进信息安全等级保护工作，这一国家层面的信息安全标准,已成为未来在电子政务安全建设中的重要保障。

亿林数据特别推出的“政府门户网站等级保护解决方案”以业界最为出色的技术底蕴和对等级保护的深刻理解，为政府客户最需要保障之处，提供了最可靠的信心保证。

一、政府门户网站的信息安全需求

政府门户网站的地位非常重要，但其安全形势却不容乐观。据统计，2018 年，有 3000 余个政府门户网站发生过网页被篡改的事件，严重影响了政府的对外形象。随着电子政务建设的逐步推进，政府门户网站所承载业务的数量在逐步增加，网站被入侵或篡改所带来的危害将不仅仅限于“政府形象”的损害，甚至能会造成巨大的经济损失，或者严重的社会问题。

对于政府网站所面临的主要风险，总结如下：

1、页面被篡改

政府门户网站作为“政府形象”的标志之一，常常是一些不法分子的重点攻击对象。政府门户网站一旦被篡改(加入一些敏感的显性内容)，常常会引发较大的影响,严重时甚至会造成政治事件,特别是在建国 70 周年国庆日马上到来的阶段，政府门户网站的安全状况更加需要得到重视。

另外一种篡改方式是网页挂马：网页内容表面上没有任何异常，却可

能被偷偷的挂上了木马程序。网页挂马虽然未必会给网站带来直接损害，但却会给浏览网站的用户带来损失。更重要的是，政府网站一旦被挂马，其权威性和公信力将会受到打击，最终给电子政务的普及带来重大影响。

2、在线业务被攻击

对企业、公众提供在线服务，已经成为政府门户网站的重要功能。这些服务一旦受到拒绝服务攻击而瘫痪、终止，对业务的正常运转必然造成极大的影响，可能会造成经济损失，严重时甚至会影响社会稳定。

3、数据被窃取

在线业务系统中，总是需要保存一些企业、公众的相关资料，这些资料往往涉及到企业秘密和个人隐私，一旦泄露，会造成企业或个人的利益受损，可能会给网站带来严重的法律纠纷。

4、内网被侵入

政府门户网站虽然和政府的办公网络之间有逻辑隔离设备，但仍有可能被手段高明的黑客入侵，从而盗取一些敏感材料，或对电子政务应用系统造成破坏。

以上的总结仅仅是对政府门户网站主要安全需求的简单总结，事实上，政府门户网站要达到真正的安全，需要建立一个完善细致的安全防护体系，不仅要在技术上建立事前、事中和事后的纵深防御系统，还需要建立良好的信息安全管理制度。下文将结合信息安全等级保护政策，提出整体建议方案。

二、亿林数据政府门户网站等级保护解决方案

出于对信息安全的重视，国家出台了信息安全等级保护的一系列文件

和标准，用以促进和指导信息安全的建设。

2007 年 6 月 22 日，公安部与国家保密局、密码管理局、国务院信息办联合会签并印发了《信息安全等级保护管理办法》(公通字[2007]43 号)，确定了信息安全等级保护制度的基本内容及各项工作要求。

2007 年 7 月 16 日，四部委联合会签并下发了《关于开展全国重要信息系统安全等级保护定级工作的通知》(公信安[2007]861 号)，就定级范围、定级工作主要内容、定级工作要求等事项进行了通知。

2017 年 6 月 1 日,《网络安全法》正式实施，明确国家实行网络安全等级保护制度，明确了政府网站等级保护责任归属等问题。

2017 年 6 月 8 号国务院办公厅印发《政府网站发展指引》（以下简称《指引》），对全国政府网站的建设发展作出明确规范，同时对于政府网站的安全提出了更高的要求。

《指引》明确政府网站定义，明确了政府网站的的主管单位、安全管理单位、协同监管单位和职责。指出政府网站开始原则，同时要推进网站集约化，通过统一标准体系、统一技术平台、统一安全防护、统一运维监管、集中管理信息数据，集中提供内容服务，实现网站资源优化融合、平台整合安全、数据互认共享、管理统筹规范、服务便捷高效。

《指引》强调，要根据网络安全法等要求，落实网络安全等级保护制度，建立安全监测预警和应急响应机制，对攻击、侵入和破坏政府网站的行为以及影响政府网站正常运行的意外事故进行防范，确保网站稳定、可靠、安全运行。

1、《指引》对政府网站明确提出了以下几项安全要求：

1）根据网络安全法等要求，落实网络安全等级保护制度

2）网站时效性，政府网站不得随意关停。

安全因素导致政府网站不可用因素包括：

●拒绝服务攻击导致链路瘫痪。

●利用网站漏洞发起攻击耗尽系统资源导致宕机。

3）防范攻击、侵入和破坏政府网站。

●网站被篡改

●网站敏感信息泄露

●网站被挂马

4）发现处理钓鱼/仿冒网站。

2、《指引》明确指明政府网站采取以下技术手段进行监测预警、安全防护和应急响应：

1）政府网站安全持续监测需求

网站篡改持续监测、多链路的网站可用监测、钓鱼/仿冒网站发现、未知资产发现、零日（0day）漏洞感知；

2）政府网站自身安全需求

代码审计安全需求、漏洞发现和管理需求、网站高级威胁（APT）发现需求；

3）网站攻击防护需求

保障网站传输链路可用、防止网站漏洞利用、防止网站敏感数据泄密、防止网站被劫持；

4）政府网站跨区域集中监管需求

5）政府网站跨区域集中防护需求

6）应急响应服务需求

7）网站安全考核评价需求

8）安全人才培养需求

针对政府门户网站的安全需求，以及信息安全等级保护相关文件和标准，亿林数据以安全服务为主线，提出了符合等级保护要求的政府门户网站整体安全解决方案。

根据《信息系统安全等级保护实施指南》中所给出的等级保护的建设过程(如图 1 所示)，可以看到等级保护并不是一个“一劳永逸”的孤立项目，而是一个连续不断，周而复始的“过程”。

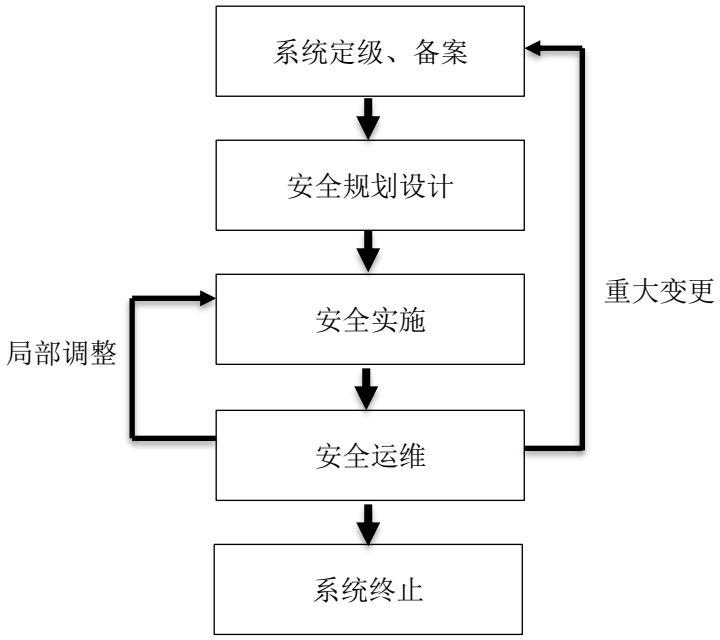


图 1 信息系统安全等级保护实施的基本过程

要实现这样一个过程，就必须要以安全服务为主线，从门户网站的安全评估、差距评估等咨询性服务开始，到整体安全规划、解决方案设计等设计性服务，最终以运维支持、应急响应等持续的技术性服务为政府门户

网站提供一个符合等级保护精神的安全保障体系。

3、等级保护过程中及各阶段安全服务

亿林数据在等级保护过程的各阶段中所提供的系列安全服务如下图所示：

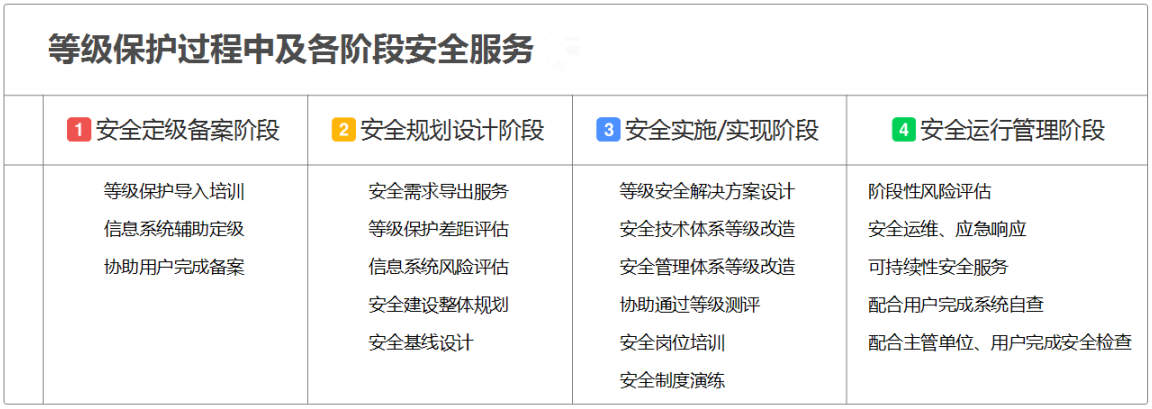
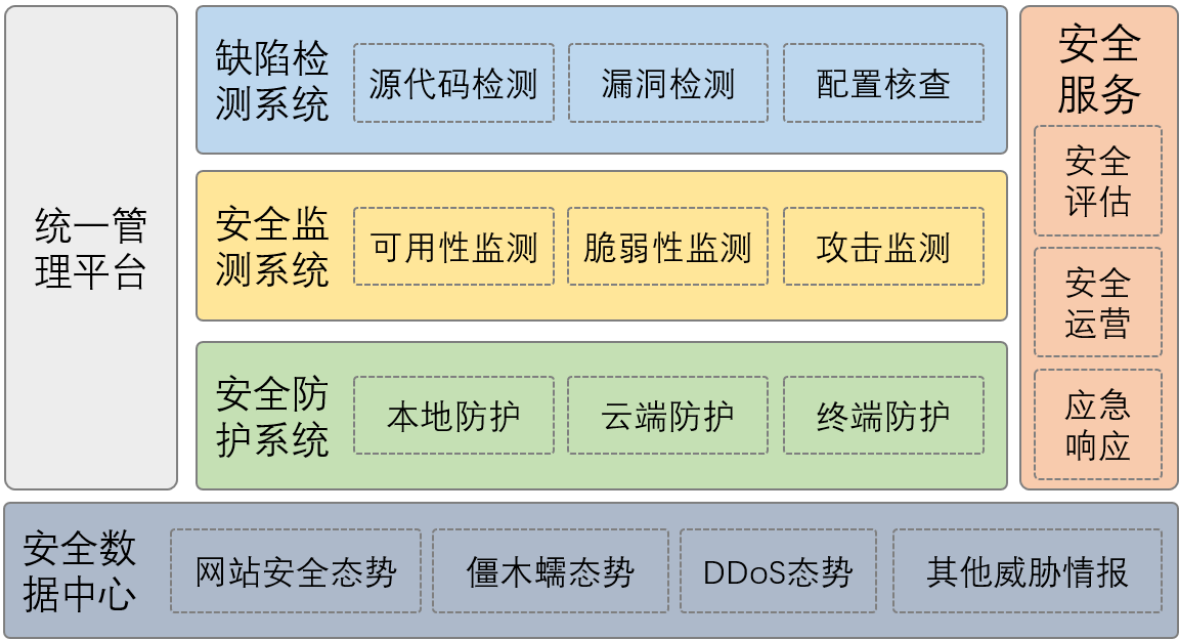


图 2 等级保护过程及各阶段安全服务

上图所示的各阶段都分别对应多个安全服务，限于篇幅，不能一一尽述，下面就各阶段中的主要部分做简要介绍。

亿林数据结合安全滑动标尺中逐渐增强的威胁情报需求，依托亿林数据安全大数据、威胁情报中心，为客户提供传统解决方案前所未有价值。方案架构以网站安全的事前检查预警、事中监督防护、事后规范考核处理流程结合安全服务应急响应、等保咨询进行设计：



1）事前检查预警

首先进行源码级的安全检测，同时采用漏扫工具、配置核查工具以及组织社会白帽子资源发现政府网站安全隐患，进行预警防控。

通过先进的源代码审计商业化产品亿林数据代码检测从源代码上发现安全问题，规避安全风险，解决源代码安全问题。

通过亿林数据全省领先的被动扫描工具云漏扫，采用不占用网站资源、更全面的流量抓取模式被动获取 URL 方式，发现管理漏洞，解决漏洞的全生命周期管理。

通过全省最大的漏洞共享平台组织提供众测服务，发现政府网站其他安全隐患。

2）事中监督防护

持续监测网站可用、篡改、敏感词、钓鱼/仿冒等安全指标，发现问题及时通报处理。采用能够抵御利用漏洞攻击和大流量 DDoS 攻击公有云 + 私有云的方式防护模式进行安全防护。

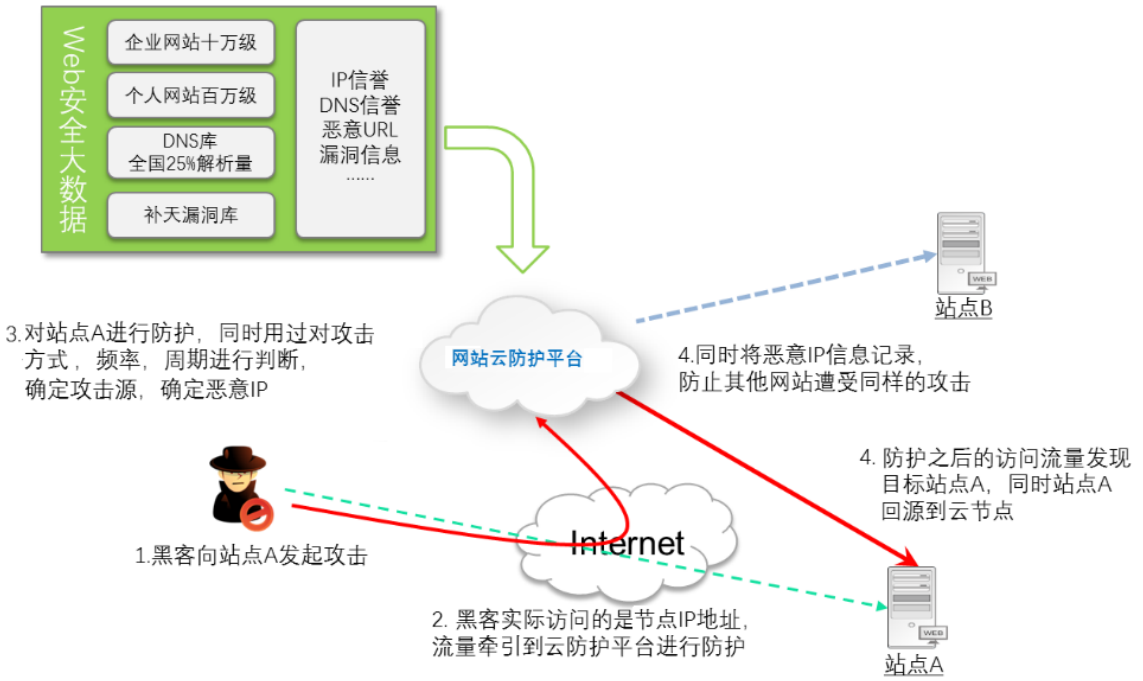
通过基于安全大数据和威胁情报的亿林数据网站云监测产品，在云端对政府网站进行可用性监控、挂马发现、钓鱼/仿冒网站发现、网页篡改发现、暗链发现、漏洞发现、敏感信息等进行持续监测，解决监管需求。通过威胁情报推送国家各个层面发布的漏洞、病毒、网络攻击等预警和通报信息，满足《指引》要求。

为政府网站安全防护提供以下三种方案：

通过亿林数据云端 Web 应用防护系统对政府网站进行云端防护，以抵御 Web 漏洞利用攻击、DNS 攻击、大流量 DDos 攻击、应用层 CC 攻击等网站威胁。亿林数据采用 CDN（内容分发网络）等技术进行缓存加速，提升访问请求响应速度，同时提供 CND 防护、CND 加速，契合《指引》的建议要求

基于混合云部署的网站防护，将亿林数据云端防护系统落地为私有云节点，与公有云防护系统进行联动。常态化的网站防护由私有云防护节点完成，大流量 DDoS 攻击或者私有云节点故障时自动切换到公有云防护。

亿林数据应用云、端联动防护，即通过云端+本地防篡改软进行 WEB 攻击防护，保障网站文件不被非授权人员篡改同时提供 RASP 防护，可以基于主机行为有效防护内部非法人员对政府网站攻击。



通过亿林数据云端防护及部署数据库审计、运维审计系统对数据库的操作行为进行实时监测，发现问题及时处理。从技术手段解决网站数据泄密的需求。

发生安全事件时，依托亿林数据强大的安服应急团队，依照应急处置流程通过远程或现场的方式，对出现的安全事件快速响应，快速处理。解决应急响应需求。在现场进行信息收集，进行 WEB 攻击画像，给出防御体系修复建议。

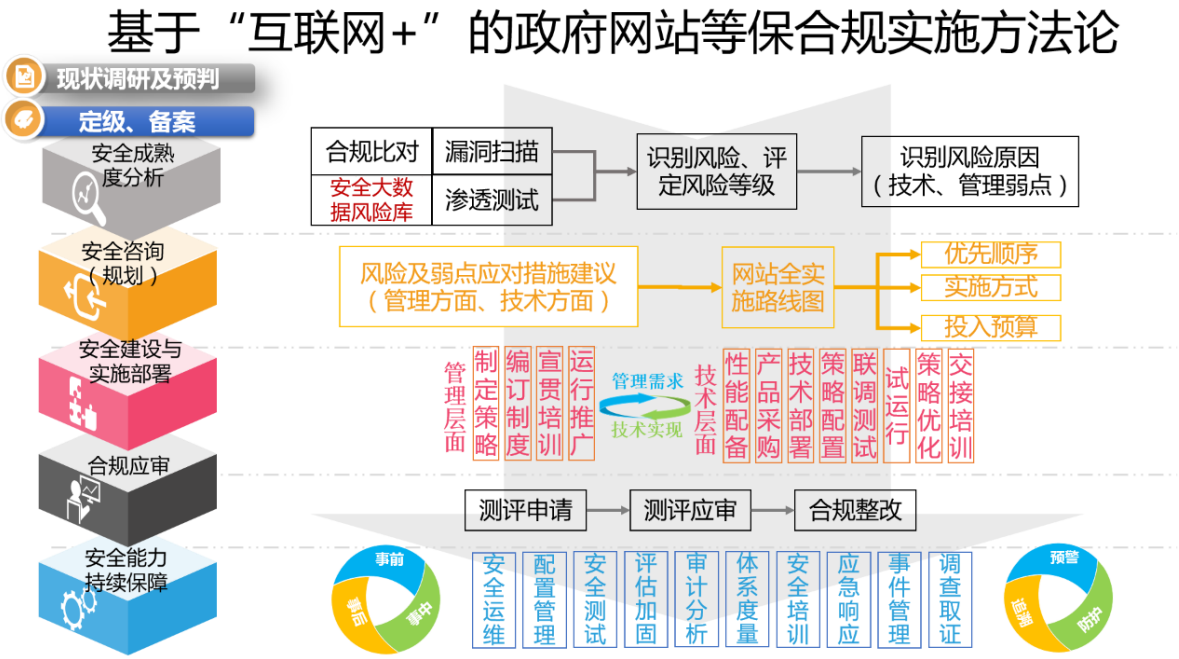
3）事后规范考核

依托亿林数据首创的网站威胁态势感知系统，提供网站安全生命周期的网站安全运营，通过可视化的界面实时展现网站安全事件，周期性网站安全状况，为下一步动作提供决策能力。解决统一监管需求，同时为政府网站主管单位提供考核依据。

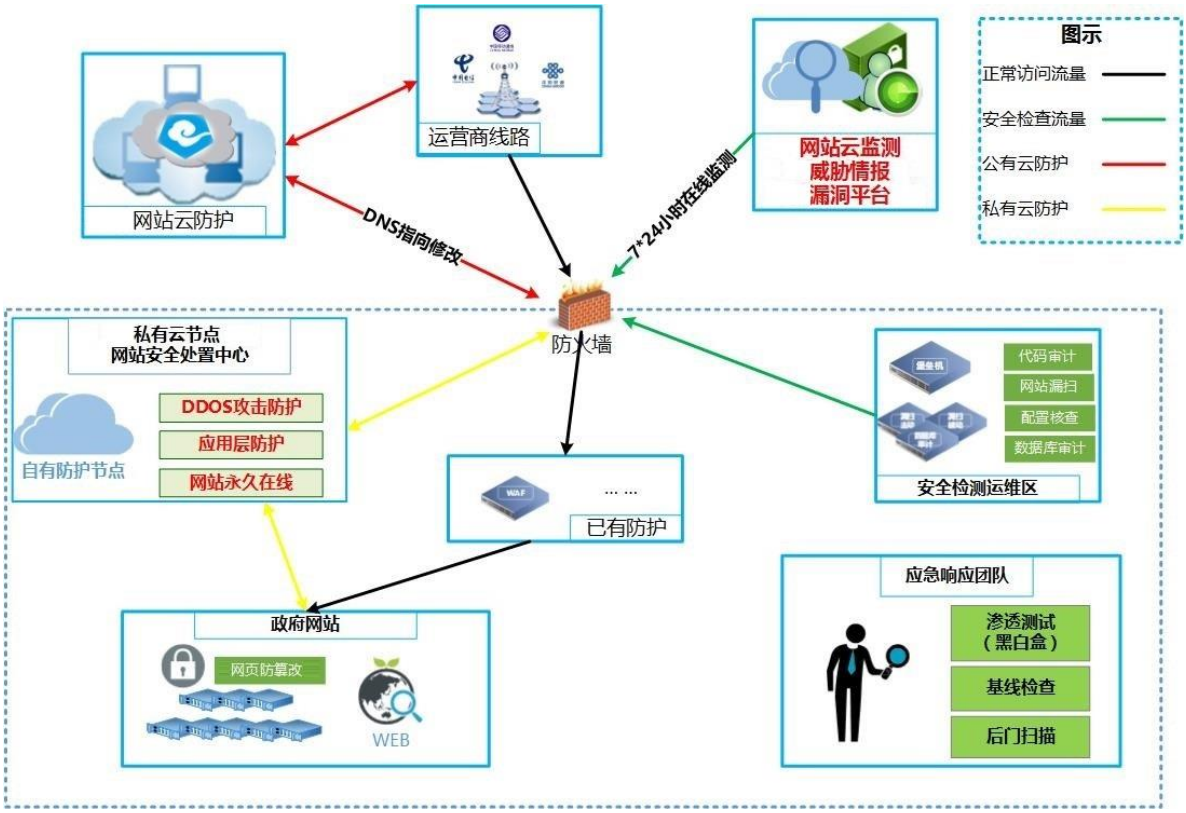
采用亿林数据网络安全实训系统，构建人才培训、考核评估、科研测试于一体培养模式，持续培养网络安全人才。满足安全人才培养与人才考核需求。

4）安全服务

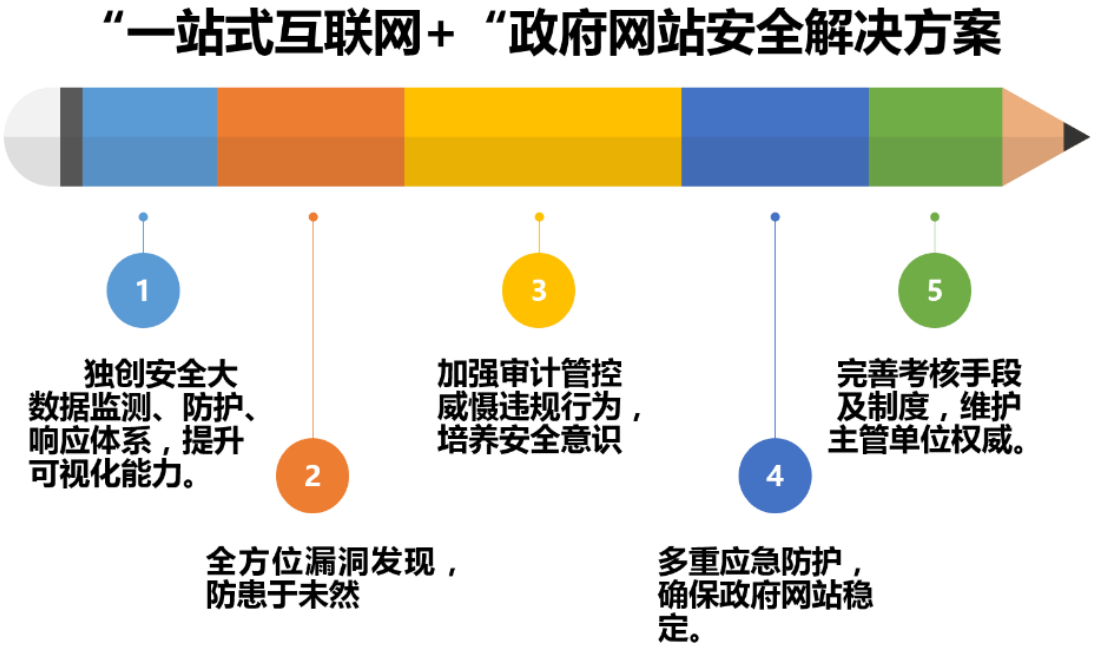
亿林数据不仅提供安全咨询、渗透测试、加固整改等安全服务，同时提供全生命周期的等保咨询服务，亿林数据结合多年互联网安全技术经验及等保标准要求，推出“互联网+”的网站安全等保合规实施方法论，将整个政府网站等保合规实施过程分为三大阶段，核心实施过程分为五大步骤，并将亿林数据威胁情报态势感知技术相融合，增强政府网站防护的预先感知及防护能力。满足政府根据网络安全法等要求，落实网络安全等级保护制度需求。



4、 政府网站整体安全解决方案部署示意图



5、 政府网站整体安全解决方案优势



更多方案详细介绍请咨询亿林数据产品与解决方案中心。

www.xinnetlabs.cn