国家电子政务外网标准

GW0204—2014

国家电子政务外网安全监测体系
技术规范与实施指南

Technical Requirements and Implementation Guide

for Security Monitoring System of National E-Government Network

2014－11－13 发布　　2015－1－1 实施

国家电子政务外网管理中心

目　　次

前　言

根据我国有关法律、法规和技术规范的相关规定，落实国家电子政务外网安全监测体系建设要求，并结合国家电子政务外网安全监测体系建设实际需求和建设经验，编制本标准。各级政务外网建设运维单位可依据本标准有计划、有步骤地建设和完善安全监测体系。

本标准由国家电子政务外网管理中心提出并归口。

本标准起草单位：国家电子政务外网管理中心、北京天融信科技股份有限公司、北京启明星辰信息安全技术有限公司、东软集团股份有限公司、网神信息技术（北京）股份有限公司、深圳华为技术有限公司、湖南蚁坊软件有限公司、深圳市奥联科技有限公司。

本标准主要起草人：吕品、罗海宁、马英、周民、邵国安、张锐卿、刘震、卢珂、范永、苑向兵、丁凌风、李经通、孙燕辉、徐浩、陈亮、范仲辉、倪德东、郑玮、吴昊。

引　　言

本标准包括国家电子政务外网安全监测体系技术框架及实施指南，适用于指导各级政务外网建设运维单位开展安全监测体系规划设计、建设实施等具体工作，也可为接入政务外网的各级政务部门安全监测系统建设提供参考。

国家电子政务外网安全监测体系技术规范与实施指南

1 范围

本标准适用于指导各级政务外网安全监测体系的规划、设计、建设和管理等相关工作。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注明日期的引用文件，其后所有的修改（不包括勘误的内容）或修订版均不适用于本标准。凡是不注明日期的引用文件，其最新版本适用于本标准。

GB/T 5271.8 信息技术 词汇 第8部分：安全

GB/T22239 信息安全技术 信息系统安全等级保护基本要求

GB/T20985 信息技术 安全技术 信息安全事件管理指南

3 术语和定义

GB/T 5271.8-2001确定的以及下列术语和定义适用于本标准。

3.1

安全监测 Security Monitoring

以信息安全事件为核心，通过对网络和安全设备日志、系统运行数据等信息的实时采集，以关联分析等方式，实现对监测对象进行风险识别、威胁发现、安全事件实时报警及可视化展现。

3.2

网络安全态势感知 Network Security Situation Awareness（NSSA）

在大规模网络环境中，对能够引起网络态势发生变化的安全要素进行获取、分析、图形化显示以及预测未来一段时间内的发展趋势。

3.3

网络管理系统 Network Management System（NMS）

提供拓扑管理、设备配置、故障告警、性能监测和报表等网络运维管理功能，实现对网络运行的集中统一监测与配置管理。

3.4

安全策略 Security Policy

为信息系统安全管理制定的行动方针、路线、工作方式、指导原则或程序。

3.5

安全威胁 Security Threat

某个人、物、事件或概念对某一资源的保密性、完整性、可用性、真实性或可控性所造成的危害。

3.6

信息安全事件 Information Security Incident

由单个的或一系列的有害或意外信息安全事态组成,它们具有损害业务运作和威胁信息安全的极大

可能性。

3.7

安全监测体系　Security Monitoring System

综合利用动力环境管理、网络管理、终端管理、日志管理、风险管理、审计等安全管理功能，采取多种技术手段和安全管理规范，对运行环境、网络设备、安全设备、操作系统、应用系统等 IT 资源实现实时安全监测与趋势分析，通过各级政务外网安全监测系统的上下互联，以及与网络管理系统、审计系统等互联，实现体系化部署与监测管理。

3.8

互联网统一出入口

各级政务外网城域网设置互联网接入区为政务部门提供接入到互联网的统一网络通道，互联网统一出入口在本标准中特指该网络通道与互联网 ISP 的边界。

4　缩略语

VPN　虚拟专用网　(Virtual Private Network)
SQL　结构化查询语言　(Structured Query Language)
ISP　互联网服务提供商　(Internet Service Provider)

5　国家电子政务外网安全监测体系

5.1　技术框架

国家电子政务外网安全监测体系技术框架如图1所示。

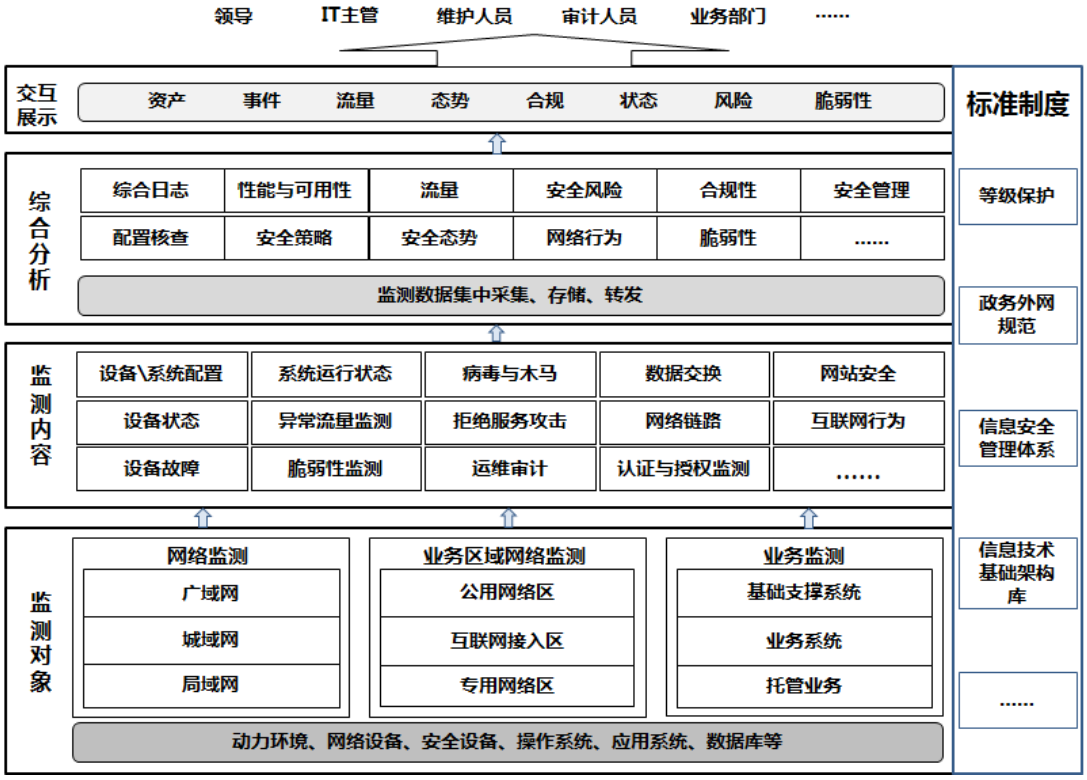


图 1　国家电子政务外网安全监测体系技术框架图

国家电子政务外网安全监测体系技术框架主要内容包括：

a) 监测对象层：确定国家电子政务外网安全监测的对象与范围，网络监测包括广域网、城域网、局域网监测，业务区域网络监测包括公用网络区、互联网接入区、专用网络区监测，业务监测包含基础支撑系统、业务系统、托管业务监测；

b) 监测内容层：根据监测目标，确定重点监测内容。监测内容包括设备与系统配置监测、设备状态监测、设备故障监测、系统运行状态监测、异常流量监测、脆弱性监测、病毒与木马监测、拒绝服务攻击监测、运维审计监测、数据交换监测、网络链路监测、认证与授权监测、网站安全监测、互联网行为监测；

c) 综合分析层：实现监测数据的集中采集、存储和转发，为综合分析提供基础元数据。利用综合日志分析、性能与可用性分析、安全管理分析、安全策略分析、风险分析、脆弱性分析、安全态势分析等技术，对监测内容进行综合分析，同时实现安全态势、知识库等的共享；

d) 交互展示层：根据决策者、管理人员和运维人员不同的需求和关注重点，将系统的风险、安全态势、脆弱性、流量、合规性等统计分析结果以报表、图形等直观的方式进行展示；

e) 标准制度：安全监测体系所涉及的信息系统要符合国家安全等级保护的相关要求和标准规范以及国家电子政务外网相关标准规范，同时在运维过程中遵循信息安全管理体系、信息技术基础架构库等体系要求，提升运维与管理水平。

5.2 监测分类

国家电子政务外网安全监测主要包括以下几种类型：

a) 安全事件监测：通过多种方式对各类安全事件进行监测，并对事件进行分类、分级。通过对事件的分析并发现问题，形成安全事件的上报与处理机制。

b) 状态信息监测：实现对安全设备、网络设备和系统的运行状态监测，掌握各类设备和系统的可用性状态信息。

c) 运维监测：实现对安全设备、网络设备和系统的运维操作审计，发现违规行为或误操作。

d) 脆弱性监测：实现对安全设备、网络设备和系统的脆弱性监测，发现资产所面临的安全风险。

e) 互联网行为监测：实现对接入单位的上网行为监测，发现访问互联网的违规行为或安全事件。

f) 流量监测：实现对网络流量的监测，掌握流量的分布与应用情况，发现引起流量异常的安全问题。

5.3 监测对象与内容

5.3.1 网络监测范围与内容

5.3.1.1 广域网

a) 监测范围：中央、省、地市三级纵向广域网；

b) 监测对象：各级核心路由器、下级接入路由器、广域网链路；

c) 主要监测内容：

1) 路由器：配置监测、设备状态监测、设备故障监测、运维操作审计监测、脆弱性监测；

2) 广域网链路：异常流量监测。

5.3.1.2 城域网

a) 监测范围：中央、省、地市、县各级城域网，各级政务单位接入边界；

b) 监测对象：城域网核心网络设备和安全设备、接入单位的接入设备、城域网链路；

c) 主要监测内容：

1) 城域网核心网络设备和安全设备、接入单位的接入设备：配置监测、设备状态监测、设备故障监测、运维操作审计监测、脆弱性监测；

2) 城域网链路：异常流量监测、病毒与木马监测。

5.3.1.3 局域网

用户单位接入政务外网的局域网络及信息系统的安全防护与监测，由接入单位按照信息安全等级保护相关要求和国家标准进行自主建设和管理。

5.3.2 业务区域网络监测范围与内容

5.3.2.1 公用网络区

a) 监测范围：公用网络区的公共基础设备、重要信息系统；
b) 监测对象：网络设备、安全设备、重要信息系统；
c) 主要监测内容：
   1) 网络设备和安全设备：配置监测、设备状态监测、设备故障监测、运维操作审计监测、脆弱性监测；
   2) 重要信息系统：病毒与木马监测、系统运行状态监测、脆弱性监测、拒绝服务攻击监测、身份认证与授权监测、配置监测。

5.3.2.2 互联网接入区

a) 监测范围：互联网统一出入口、互联网数据中心；
b) 监测对象：互联网统一出入口的设备、互联网数据中心的业务系统；
c) 主要监测内容：
   1) 互联网统一出入口：异常流量监测、病毒与木马监测、互联网链路监测、互联网行为监测；
   2) 互联网数据中心：业务系统的运行状态监测、脆弱性监测、配置监测。

5.3.2.3 专用网络区

a) 监测范围：为特定需求的部门或业务设置的MPLS VPN网络区域。用户单位通过专用网络区接入的业务及信息系统的监测，由接入单位自主建设和管理；
b) 监测对象：网络设备、链路；
c) 主要监测内容：网络设备状态监测、异常流量监测、病毒与木马监测。

5.3.3 业务监测范围与内容

5.3.3.1 基础支撑系统

a) 监测范围：支撑网络运行的重要信息系统，包括DNS系统、网络管理系统、安全管理系统、安全接入平台、跨网数据交换系统等；
b) 主要监测内容：
   1) 系统运行状况监测、设备运行状态监测、重要信息系统操作行为监测、配置监测、脆弱性监测；
   2) 安全接入平台：VPN隧道状态监测、认证与授权监测、病毒与木马等监测；
   3) 跨网安全交换系统：认证与授权监测、数据交换监测。

5.3.3.2 业务系统

a) 监测范围：国家电子政务外网的业务系统，包括：门户网站系统、安全邮箱系统、数据共享与交换系统等；
b) 主要监测内容：
   1) 设备运行状态监测、系统运行状态监测、用户访问行为监测；
   2) 门户网站的安全监测：网页篡改监测、挂马监测、拒绝服务攻击监测、跨站脚本监测、SQL注入监测。

5.3.3.3 托管业务

a) 监测范围：为托管单位提供的网络设备、服务器、链路；
b) 主要监测内容：

1) 网络设备运行状态监测；
2) 服务器运行状态监测；
3) 链路带宽监测：带宽使用率监测。

5.4 分析与展示

5.4.1 分析

应对采集到的信息进行比对分析，发现安全事件或问题。

a) 基于采集的信息，根据国家电子政务外网的安全要求和场景，采用多种关联分析技术进行综合分析，发现病毒感染、恶意代码、数据泄露、攻击入侵、设备故障、系统状态变化、人员违规行为与误操作等安全事件或问题；
b) 综合分析可借助安全管理系统、态势感知系统、综合审计系统等多种信息安全分析系统完成；
c) 综合分析可依靠专家团队进行；
d) 综合分析可结合安全知识库、专家决策系统，实现安全监测体系自动化分析；
e) 综合分析可采用专家分析法、层次分析法、机器学习、统计分析、自定义的数学模型分析等多种分析方法。

5.4.2 展示

将采集到的安全信息和分析后的安全问题进行实时可视化展示。

展示内容包括：

a) 实时展示物理环境状态、拓扑状态、运行状态、安全状态等信息；
b) 展示日志、事件和告警信息，以及事件之间的关联关系；
c) 可查询追溯事件的相关原始信息；
d) 展示安全信息统计分析图形、报表。

5.5 级联监测

通过中央、省、地市三级安全监测系统上下互联以及安全监测系统与网络管理系统互联，实现实时监测信息、安全预警信息在各级系统间传递与共享，形成覆盖中央、省、地市、县四级安全监测体系。

本级安全监测系统将监测信息上报给上级安全监测系统，上报信息包括：设备运行状态、风险状况、安全策略修改情况、漏洞、告警、重大安全事件、合规性分析以及信息安全统计指标等信息。下级安全监测系统可从上级系统中获取相关推送信息。

6 实施指南

6.1 实施原则

在建设国家电子政务外网安全监测体系过程中，应遵循“统一规划、分期建设、分级实施、分级管理”的总体指导原则。

a) 由国家电子政务外网管理中心对全网安全监测体系进行统一规划和指导；
b) 各级政务外网建设运维单位负责本级监测体系的建设、运维和管理；
c) 分阶段推进安全监测体系建设和实施。

6.2 实施目标

建设中央、省、地市三级安全监测平台，结合相应的制度规范与运维流程，形成覆盖中央、省、地市、县的政务外网四级安全监测体系，实现如下目标：

a) 实现全网的安全运行状态监测和安全趋势分析；
b) 提高信息安全事件处理效率及质量，实现政务外网日常安全运维以及管理工作的流程化、制度化，为政务外网的信息安全事件监测、安全风险分析等提供技术支撑；

c) 提供安全知识库的管理能力，通过建设全网共享知识库，提供安全知识库、漏洞库、补丁库、安全通告、事件案例库等内容，并在此基础上进行数据挖掘和分析；

d) 通过部署基于云计算的安全监测服务平台，面向本级或下级政务外网建设运维单位和接入单位提供安全监测服务。

6.3 实施阶段划分

国家电子政务外网安全监测体系建设实施分四个阶段进行：

第一阶段：中央、省级政务外网分别建立并完善安全监测系统；

第二阶段：实现中央、省级安全监测系统的级联，并推进地市级政务外网安全监测系统的建设，实现中央面向各级政务外网的知识共享；

第三阶段：通过中央、省、地市三级安全监测系统的级联，形成政务外网安全监测体系，实现面向全网的安全态势监测与分析。县级政务外网可根据自身情况建设安全监测系统，并与上级系统级联；

第四阶段：建立全网信息安全事件预警和应急处理机制。

6.4 实施内容

各级政务外网建设运维单位根据自身的管理需求建设安全监测系统，安全监测系统的建设内容分为基础型监测和增强型监测两种模式，其中基础型监测需优先实施。各级政务外网建设运维单位根据本级建设情况按表1所列项目适当选择建设内容。

表1 政务外网安全监测系统建设主要内容

	中央级	省级	市级	县级
基础型监测	■ 广域网、城域网核心设备及链路监测 ■ 骨干网流量监测 ■ 互联网链路监测 ■ 拒绝服务攻击监测 ■ 病毒与木马监测 ■ 网站安全监测 ■ 互联网行为监测 ■ 信息系统监测 ■ 认证与授权监测 ■ 核心设备性能监测 ■ 原始日志存储	■ 广域网、城域网核心设备链路监测 ■ 骨干网流量监测 ■ 互联网链路监测 ■ 拒绝服务攻击监测 ■ 病毒与木马监测 ■ 网站监测 ■ 互联网行为监测 ■ 信息系统监测 ■ 认证与授权监测 ■ 核心设备性能监测 ■ 原始日志存储	■ 广域网、城域网核心设备链路监测 ■ 骨干网流量监测 ■ 拒绝服务攻击监测 ■ 病毒与木马监测 ■ 网站监测 ■ 信息系统监测 ■ 互联网行为监测 ■ 认证与授权监测 ■ 核心设备性能监测 ■ 原始日志存储	■ 核心设备监测 ■ 骨干网流量监测 ■ 病毒与木马监测 ■ 互联网行为监测 ■ 认证与授权监测 ■ 原始日志存储
增强型监测	■ 脆弱性监测 ■ 服务器工作性能监测 ■ 运维操作审计 ■ 僵尸网络监测 ■ 配置监测	■ 脆弱性监测 ■ 服务器工作性能监测 ■ 运维操作审计 ■ 配置监测	■ 脆弱性监测 ■ 服务器工作性能监测 ■ 运维操作审计	■ 脆弱性监测 ■ 服务器工作性能监测 ■ 运维操作审计

6.5 实施方式

安全监测系统主要有三种实施方式，包括：

自建自维：政务外网建设运维单位根据统一规划自行建设安全监测系统，并且自行承担系统维护和日常监测分析工作；

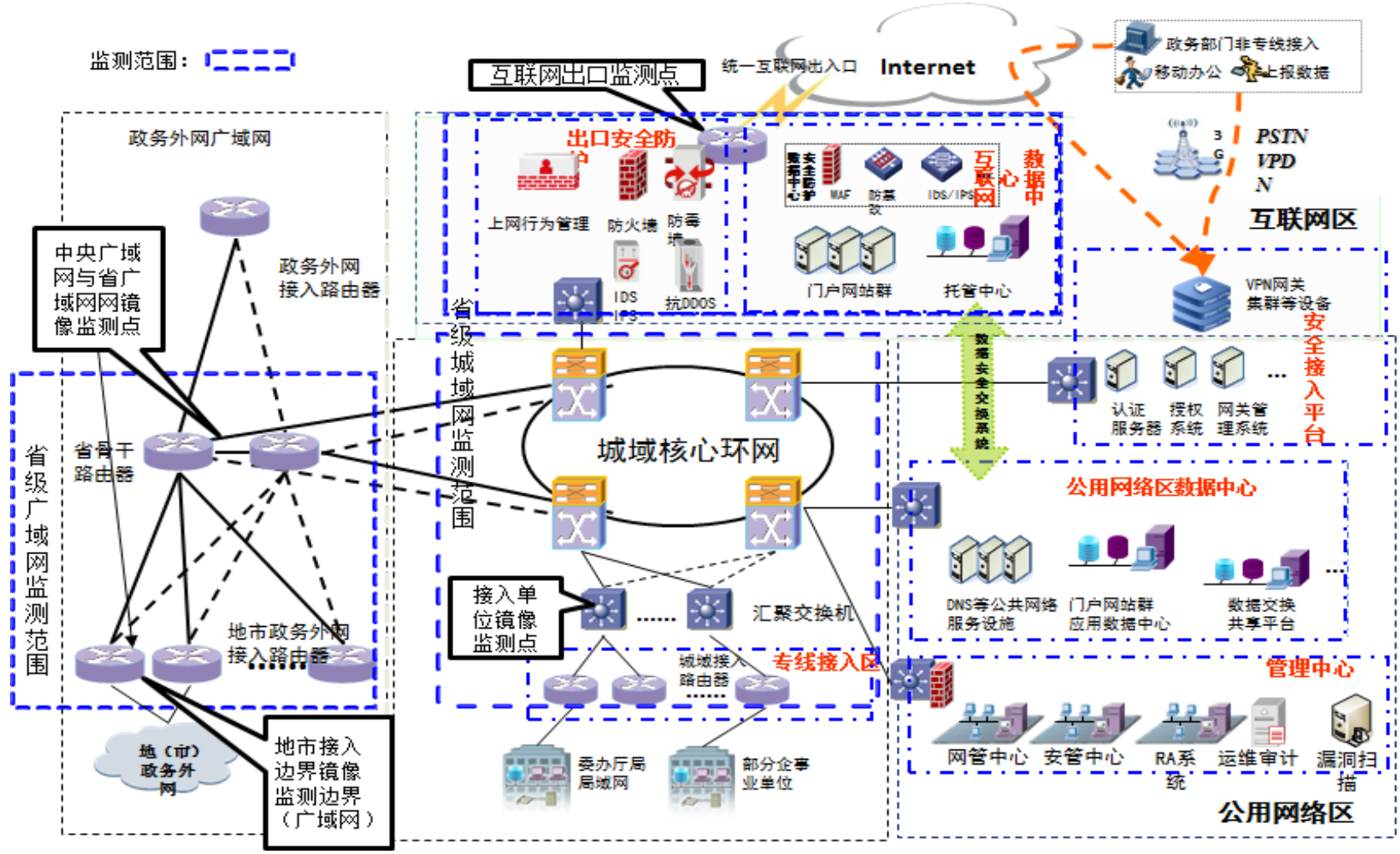
自建代维：政务外网建设运维单位根据统一规划自行建设安全监测系统，但委托第三方机构（如监测系统建设方、厂家或安全服务商）进行系统维护和日常监测分析；

代建代维：政务外网建设运维单位以购买安全监测服务的方式实现对本级政务外网的安全监测，可选择提供安全监测云服务的上级政务外网建设运维单位，也可选择安全监测服务企业等第三方机构。所选择服务对象应将系统部署于政务外网，系统应符合政务外网相关标准的要求，并在政务外网公用网络区进行监测数据分析，不允许带出数据进行远程或离线分析。

附　录　A

（规范性附录）

省、地市级政务外网广域网与城域网安全监测范围示意图



附　录　B
（规范性附录）
安全监测体系产品支撑

为满足安全监测体系相关监测需求，可以参考采用（不限于）如下安全产品作支撑：

监测需求	安全产品参考
系统运行状态	IT 资源管理系统、网络管理系统、系统日志软件
设备状态监测	网络管理系统、安全管理系统、终端管理系统、资产管理系统
设备与系统配置监测	配置核查系统、安全基线系统、漏洞扫描系统、日志分析系统
设备性能监测	网络管理系统、安全管理系统、终端管理系统、资产管理系统
设备故障监测	网络管理系统、安全管理系统、日志分析系统
流量监测	流量监测设备、流量控制系统、网络管理系统、APT 检测系统
网络链路监测	流量监测设备、深度包检测系统、设备日志软件、网络管理系统
链路负载监测	网络管理系统、流量监控管理系统、负载均衡设备
脆弱性监测	漏洞扫描系统
互联网行为监测	互联网行为监控系统、网络审计系统、Web 应用防火墙、终端安全管理系统、入侵检测系统
认证与授权监测	系统日志软件、堡垒机、AAA 系统、身份认证与授权系统
SQL 注入监测	Web 应用防火墙（WAF）、入侵检测系统
病毒与木马监测	防病毒网关、防病毒软件、入侵防御系统
拒绝服务攻击监测	流量清洗设备、抗拒绝服务系统
网站安全监测	Web 应用防火墙、网页防篡改系统、网站安全监测与恢复系统
运维审计监测	堡垒机、网络审计系统、终端管理系统、AAA 系统