SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

深信服等级保护2.0解决方案

持续保护，不止合规

深信服 智安全

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

目录

《网络安全法》带动安全建设上升到国家战略高度

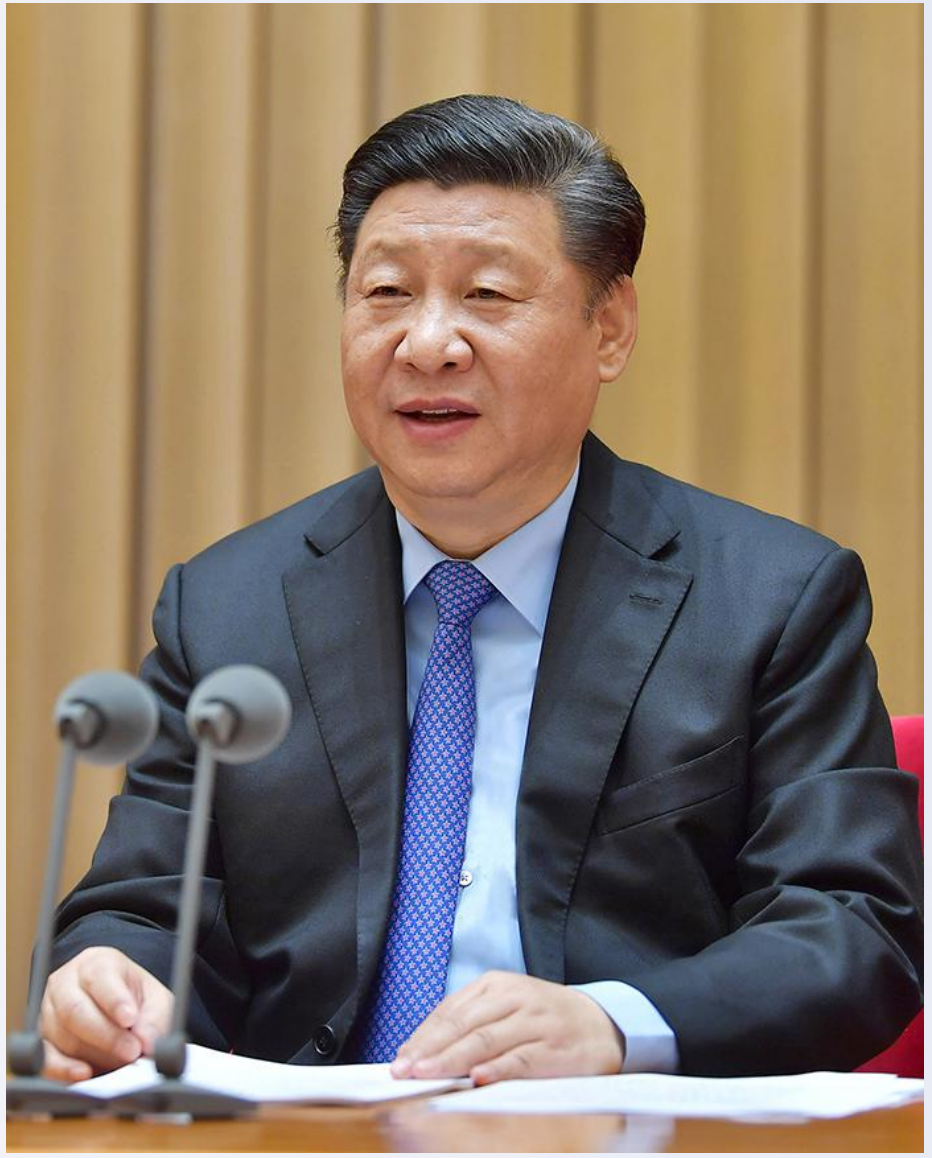
SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

2019年
国家网络安全宣传周

- 国家网络安全工作要坚持网络安全为人民、网络安全靠人民，保障个人信息安全，维护公民在网络空间的合法权益。

全国网络安全和信息化工作会议

- 没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。
- 要落实关键信息基础设施防护责任，行业、企业作为关键信息基础设施运营者承担主体防护责任，主管部门履行好监管责任。



《网络安全法》

《网络安全等级保护条例》（报批稿）

《关键信息基础设施安全保护条例》（报批稿）

安全影响面更广

安全建设深入各行各业，各种场景

关基重点保护

关键信息基础设施实行重点保护

《网络安全法》之等级保护

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

一审		二审			三审	发布
十二届全国人大常委会第十五次会议	公开征求意见	十二届全国人大常委会第二十一次会议	公开征求意见		十二届全国人大常委会第二十四次会议	
2015.6.26	2015.7.6	2015.8.5	2016.6.28	2016.7.5	2016.8.4	2016.10.31	2016.11.7

第二十一条

- **国家实行网络安全等级保护制度。**网络运营者应当按照网络安全等级保护制度要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

第三十一条

国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的**关键信息基础设施**，在网络安全**等级保护制度的基础**上，**实行重点保护。**

第五十九条

- **网络运营者不履行**本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。
- **关键信息基础设施的运营者不履行**本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致后果的，处十万元以上一百万元以下罚款，对直接负责主管人员处一万元以上十万元以下罚款。

不做等保就是违法！

配套法规之《网络安全等级保护条例》

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

法律效力

- 根据**《行政法规制定程序条例》**第五条：行政法规的名称一般称“条例”，国务院各部门和地方人民政府制定的规章不得称“条例”
- 《信息安全等级保护管理办法》是依据行政法规制定的**部门规范性文件**，而《网络安全等级保护条例》属于依据国家法律制定的**行政法规**，**自身法律效力或法律依据的效力位阶**均高于等保1.0

保护等级

受侵害的客体	对响应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	**第三级**
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

测评周期

信息安全等级保护管理办法

- 第三级：每年至少一次
- 第四级：每半年至少一次
- 第五级：依据特殊安全需求测评

网络安全等级保护条例

- **第三级以上**的网络运营者应当**每年**开展**一次**网络安全等级测评

配套法规之《关键信息基础设施安全保护条例》

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

第二条

本条例所称关键信息基础设施，是指支撑国家经济社会运行，一旦遭到破坏、丧失功能、数据泄露，会严重危害**国家安全**、**国计民生**和**公共利益**的**网络设施、信息系统、数字资产**等

第六条

在**网络安全等级保护制度基础上**，进一步采取技术保护措施和其他必要措施，**及时有效应对网络安全事件，防范网络攻击和违法犯罪活动**，保障关键信息基础设施安全稳定运行，维护数据的完整性、可用性和保密性。

第九条

根据对经济社会运行的重要程度、信息化水平，以及遭到破坏后产生的危害影响，确定关键信息基础设施行业和领域范围如下：

（一）**公共通信和信息服务，包括电信、互联网、广播电视**等

（二）**金融，包括银行、证券、保险**等

（三）**能源，包括电力、石油、石化、天然气**等

（四）**交通，包括民航、铁路**等

（五）**水利**

（六）**公共服务，包括医疗卫生**等

（七）**国防科技工业**

（八）**国家机关**

违法案例

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

政府行业违法案例

事件4：山西忻州市某省直事业单位网站不履行网络安全保护义务被处罚

今年6月至7月间，山西忻州市某省直事业单位网站存在SQL注入漏洞，严重威胁网站信息安全，连续被国家网络与信息安全信息通报中心通报。根据《中华人民共和国网络安全法》第二十一条第二款之规定，网络运营者应当按照网络安全等级保护制度的要求，采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；第五十九条第一款之规定，网络运营者不履行第二十一条规定的网络安全保护义务的，由有关主管部门责令改正，依法予以处置。山西忻州市网警认为该单位之行为已违反《网络安全法》相关规定，忻州市、县两级公安机关网安部门对该单位进行了现场执法检查，依法给予行政警告处罚并责令其改正。

执法机构：山西忻州市、县两级公安机关网安部门
处罚行为：未按照网络安全等级保护制度的要求，采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施
处罚措施：警告并责令其改正
法律依据：《网络安全法》第21条、第59条

教育行业违法案例

怀远一学校网站未履行网络安全保护义务 分管副县长被约谈

8 月 12 日，蚌埠怀远县教师进修学校网站因网络安全防等级保护制度落实不到位，遭黑客攻击入侵。蚌埠市公安局网安支队调查案件时发现，该网站自上线运行以来，始终未进行网络安全等级保护的定级备案、等级测评等工作，未落实网络安全等级保护制度，未履行网络安全保护义务。根据《网络安全法》第五十六条之规定，省公安厅网络安全保卫总队约谈怀远县教师进修学校法定代表人、怀远县人民政府分管副县长 这是自《网络安全法》实施以来，首次由省级人民政府公安部门履行网络安全监督管理职责，约谈网络运营者的法定代表人及相关责任人。

蚌埠市局网安支队依法对网络运营单位怀远县教师进修学校处以一万五千元罚款，对负有直接责任的副校长处以五千元罚款。

医疗行业违法案例

近日，重庆永川公安经核实发现，某私立医院因未按照网络安全等级保护制度的要求履行安全保护义务造成业务瘫痪——医院 HIS、LIS、PACS 和 EMR 等后台系统业务以及医院网站等主要系统业务全部放置在同一套服务器中，未安装边界防护设备、未安装日志行为审计设备、未设置数据安全备份策略等其他的网络安全技术措施，使得黑客可以通过互联网攻破医院系统后植入勒索病毒，导致医院业务停摆。

针对此案，公安部门对医院按照《中华人民共和国网络安全法》第五十九条之规定，对医院处以罚款一万元，对直接负责的主管人员处以罚款五千元的行政处罚。

企业单位违法案例

事件3：汕头某公司未及时履行网络安全义务，网警依据网安法责令改正

2017年7月20日，广东汕头网警支队在对该市网络安全等级保护重点单位进行执法检查时发现，汕头市某信息科技有限公司于2015年11月向公安机关报备的信息系统安全等级为第三级,经测评合格后投入使用，但2016年至今未按规定定期开展等级测评。

该公司之行为已违反《信息安全等级保护管理办法》第十四条第一款和网络安全法第二十一条第（五）项规定，未按规定履行网络安全等级测评义务。根据网络安全法第五十九条规定，广东汕头网警支队依法对该单位给予警告处罚并责令其改正。

发布于：
http://www.thepaper.cn/newsDetail_forward_1755140

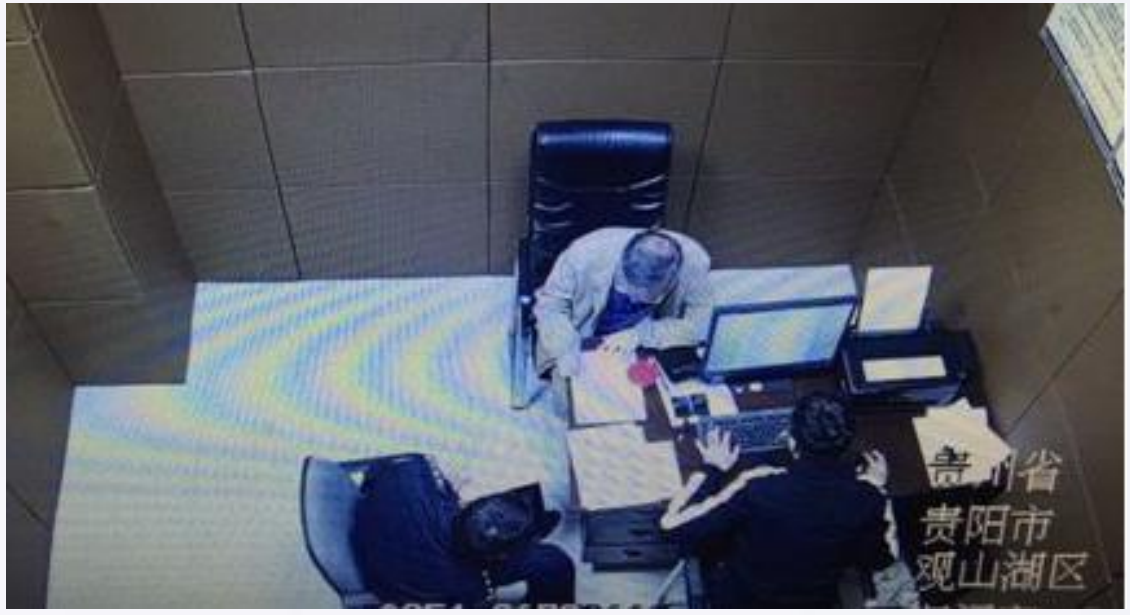
执法机构：广东汕头网警支队
处罚行为：未按规定履行网络安全等级测评义务
处罚措施：警告并责令其改正
法律依据：《网络安全法》第21条、第59条第1款

违法案例-教育行业

某高校不履行网络安全保护义务案

【案例】贵阳一高校网站主页遭遇黑客攻击，登录页面被非法篡改为违法有害信息，影响恶劣。贵阳网警获悉后，立即展开调查。经查，该高校网站平台未留存web访问日志，服务器系统日志、安全日志留存时间不满6个月留存时限，未开展网络安全检测，平台内共发现10余个木马后门，技术防护措施极为薄弱。

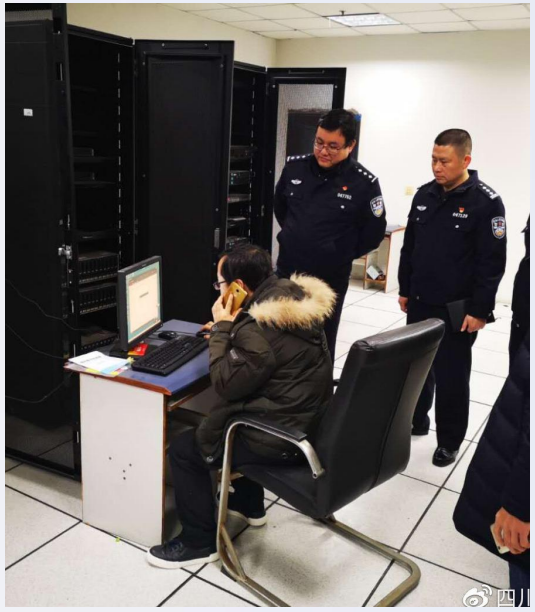
【处罚】2019年10月19日，贵阳观山湖区警方根据《中华人民共和国网络安全法》第21条、第59条之规定，依法对该高校及高校负责人分别处以10万元和5万元的行政罚款。



某学院不履行网络安全保护义务案

【案例】2019年1月，宜宾学院图书馆因网络安全责任意识淡薄、联网备案制度和网络安全等级保护制度落实不到位，导致“移动图书馆馆藏书目查询平台”的页面被攻击篡改。

【处罚】宜宾市翠屏区公安分局网安大队依据《网络安全法》第五十九条，对宜宾学院作出罚款80000元，对直接负责的主管人员作出罚款10000元的处罚；依据《计算机信息网络国际联网安全保护管理办法》第二十三条，对学院“移动图书馆馆藏书目查询平台”未履行备案职责，作出停机整顿六个月的处罚。



违法案例-医疗行业

某私立医院不履行网络安全保护义务案

【案例】2019年5月，重庆永川某私立医院服务器突然陷入瘫痪，医院业务全面“停摆”，重庆永川公安接警后立即按照“净网2019”工作要求，启动网络安全应急响应预案，详细了解相关情况，经过民警和技术专家调查核实，该私立医院因未按照网络安全等级保护制度的要求履行安全保护义务。医院HIS、LIS、PACS、EMR等后台系统业务以及微信公众号后台、医院网站等主要系统业务全部放置在同一套服务器中，医院未安装边界防护设备、未安装日志行为审计设备，未设置数据安全备份策略等其他网络安全技术措施，使医院业务在互联网上长期处于“裸奔”状态。黑客通过互联网攻破医院系统后植入勒索病毒，导致医院业务全面“停摆”。

【处罚】针对此案，永川公安按照公安部“一案双查”工作要求，对医院未按照网络安全等级保护制度的要求履行安全保护义务的行为进行查处，并按照《中华人民共和国网络安全法》相关规定，对医院处以罚款一万元、对直接负责的主管人员处以罚款五千元的行政处罚。

违法案例-政府与事业单位

某事业单位不履行网络安全保护义务案

【案例】2019年3月泰州某事业单位集中监控系统遭黑客攻击破坏。经查，该单位网络安全意识淡薄，曾因存在安全隐患、不落实网络安全等级保护制度被责令整改。整改期满后，未采取有效管理措施、技术防护措施。

【处罚】泰州警方依据《网络安全法》第21条、第59条规定，对该单位予以6万元罚款，对相关责任人予以2万元罚款，同时责令该单位停机整顿，开展定级备案、测评整改等网络安全等级保护工作。

某水闸管理局不履行网络安全保护义务案

【案例】“净网2019”专项行动工作发现，宿迁某水闸管理局未按照网络安全等级保护要求，落实安全管理和防护工作。鉴于该管理局隶属水利部淮委沂沭泗局，是沂沭泗河洪水东调南下工程体系中的重要组成部分，属关键信息基础设施，其网络安全问题事关社会稳定和群众切身利益。

【处罚】2019年8月，宿迁警方依据《网络安全法》第21条、第31条、第59条规定，对该水闸管理局予以警告，责令限期整改，落实网络安全等级保护制度。

违法案例-企业行业

某网络科技有限公司不履行网络安全保护义务案

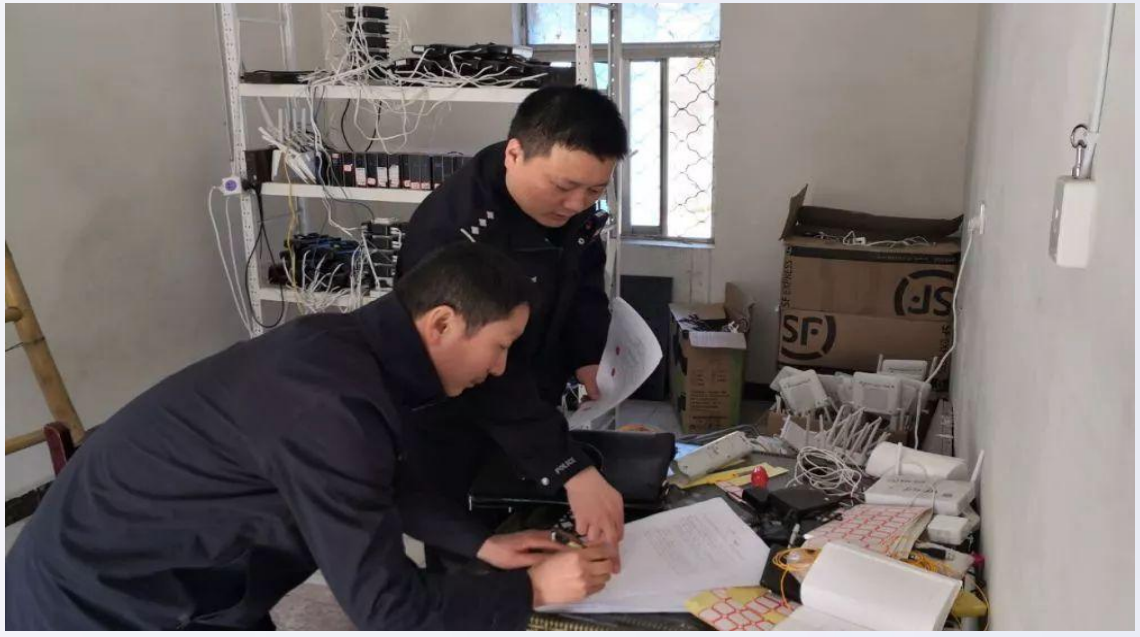
【案例】 “净网2019”专项行动工作发现，无锡某智慧便民服务有限公司建设运营的应用导航系统，遭黑客攻击破坏造成不良影响。经查，该公司未落实网络安全等级保护制度，未制订网络安全事件应急处置预案等。

【处罚】2019年7月，无锡警方依据《网络安全法》第21条、第25条、第59条规定，对该公司予以罚款5万元，对公司主管人员予以罚款2万元，责令限期整改，落实网络安全等级保护制度。

某网络公司不履行网络安全保护义务案

【案例】 “净网2019”专项行动工作发现，连云港某网络公司在提供互联网服务过程中未履行网络安全保护义务，未采取监测、记录网络运行状态、网络安全事件的技术措施，未按照规定留存相关的网络日志等。2019年3月22日，连云港警方依法责令该公司限期整改，并予以警告。4月3日，复查中发现该公司存在拒不整改情形

【处罚】警方依据《网络安全法》第21条、第59条规定，对连云港某网络公司予以罚款5万元，对该公司法人毛某某予以罚款2万元，责令其落实网络安全等级保护制度。



落实等级保护制度的意义

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

满足合法合规要求，明确责任和工作方法，让安全防护更加规范

提高人员安全意识，树立等级化防护思想，合理分配网络安全投资

明确组织整体目标，改变以往单点防御方式，让安全建设更加体系化

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

目录

等级保护发展历程

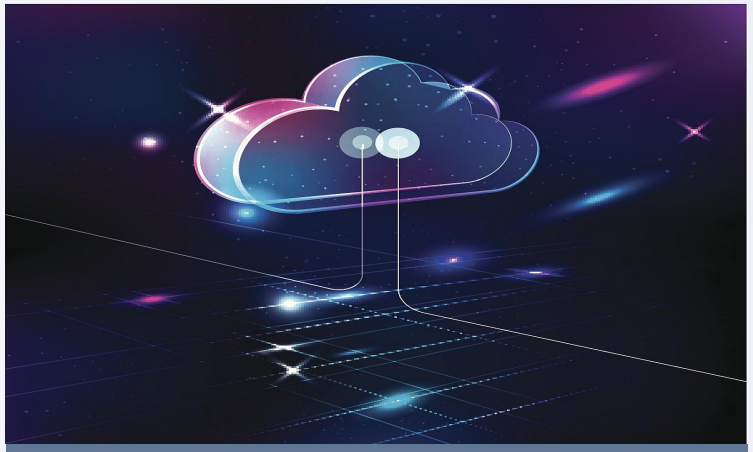
SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

1994	1999	2003	2004	2007	2017	2019
国务院令第147号	GB17859	中办发[2003]27号	公通字[2004]66号	公通字[2007]43号	网络安全法	等保2.0核心标准
第九条“计算机信息系统实行安全等级保护”首次提出了等级保护的概念	强制性标准：本标准规定了我国计算机信息系统安全保护能力的五个等级	信息安全保障纲领性文件，明确指出“实行信息安全等级保护“主要任务	进一步明确了信息安全等级保护制度的职责分工和工作的要求等基本内容	明确了信息安全等级保护的五个动作，为开展等级保护工作提供了规范保障	第二十一条“国家实行网络安全等级保护制度”，从法规上升到法律层面	《基本要求》《安全设计技术要求》《测评要求》《实施指南》

等级保护2.0修订背景

传统安全思维难以应对新型攻击

以“勒索病毒”为代表的新型攻击席卷全球，使传统安全防护手段已经难以有效保护网络空间安全，网络安全保护体系需要全面升级。



适应新型的系统形态和网络架构

新技术、新业务下的产品与服务不断创新与升级，云大物移工等新技术广泛应用，使网络安全范畴进一步拓展，要求网络安全的保护体系也随之升级。

现有等保体系需要完善升级

等保1.0相关系列标准已使用多年，为配合《网络安全法》的实施，对原有等保体系进行修订，在适用性、时效性、易用性、可操作性上进行升级。

等级保护2.0的典型变化

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

两个全覆盖

- 一是**覆盖各地区、各单位、各部门、各企业、各机构**，也就是覆盖全社会。除个人及家庭自建网络的全覆盖。
- 二是覆盖**所有保护对象，包括网络、信息系统，以及新的保护对象，云计算平台、物联网、工控系统、大数据、移动互联**等各类新技术应用。

三个特点

- 等级保护2.0基本要求、测评要求、安全设计技术要求框架统一，即：**安全管理中心支持下的三重防护结构框架。**
- 通用**安全要求+新型应用安全扩展要求**，将云计算、移动互联、物联网、工业控制系统等列入标准规范。
- 把**可信验证**列入各级别和各环节的主要功能要求。

等级保护2.0主要变化

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

名称变化

《信息安全技术 信息系统安全等级保护基本要求》

↓

《信息安全技术 网络安全等级保护基本要求》

定级对象变化

信息系统

↓

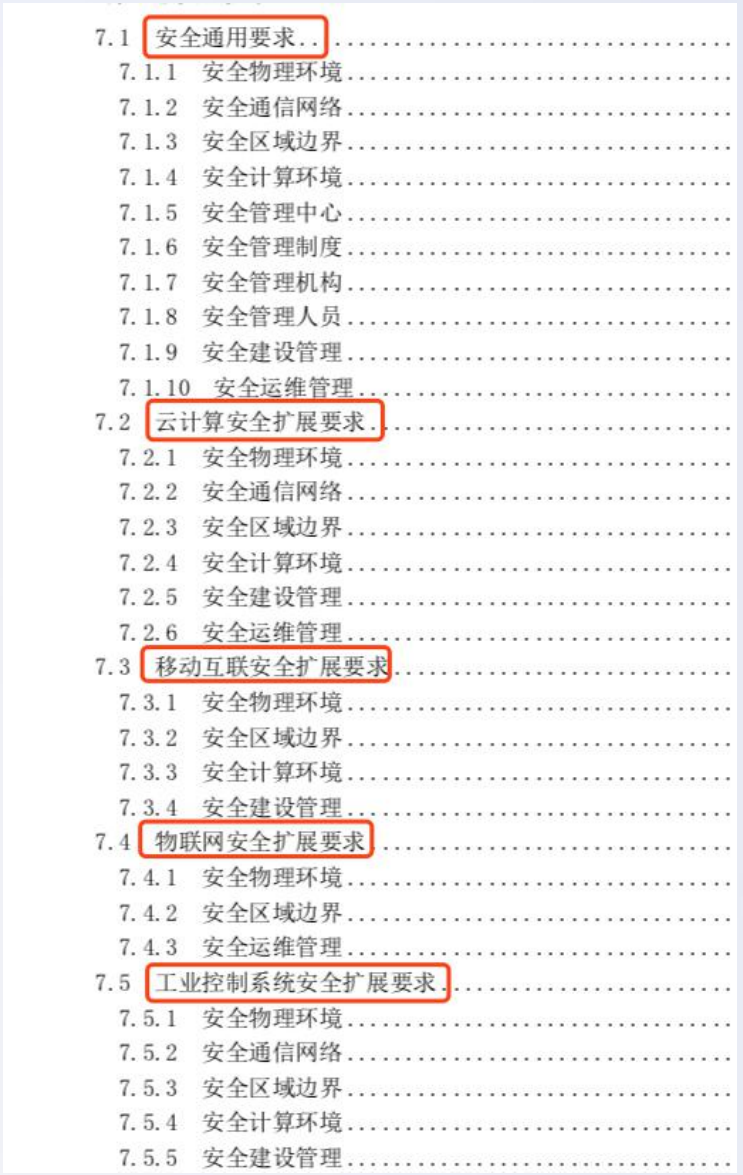
信息系统、基础信息网络、云计算平台、大数据平台、物联网系统、工业控制系统、采用移动互联技术的网络等

安全要求变化

安全要求

↓

安全通用要求+安全扩展要求



7.1 安全通用要求
7.1.1 安全物理环境
7.1.2 安全通信网络
7.1.3 安全区域边界
7.1.4 安全计算环境
7.1.5 安全管理中心
7.1.6 安全管理制度
7.1.7 安全管理机构
7.1.8 安全管理人员
7.1.9 安全建设管理
7.1.10 安全运维管理
7.2 云计算安全扩展要求
7.2.1 安全物理环境
7.2.2 安全通信网络
7.2.3 安全区域边界
7.2.4 安全计算环境
7.2.5 安全建设管理
7.2.6 安全运维管理
7.3 移动互联安全扩展要求
7.3.1 安全物理环境
7.3.2 安全区域边界
7.3.3 安全计算环境
7.3.4 安全建设管理
7.4 物联网安全扩展要求
7.4.1 安全物理环境
7.4.2 安全区域边界
7.4.3 安全运维管理
7.5 工业控制系统安全扩展要求
7.5.1 安全物理环境
7.5.2 安全通信网络
7.5.3 安全区域边界
7.5.4 安全计算环境
7.5.5 安全建设管理

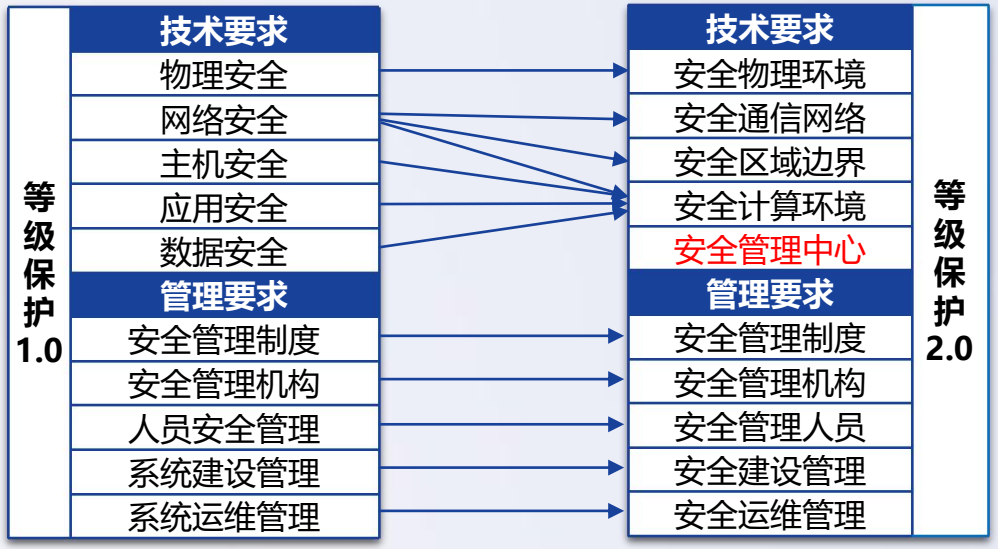
等级保护2.0主要变化（续）

控制措施分类结构变化

技术（物理、网络、主机、应用、数据）+管理

↓

技术（物理环境、一中心三防护）+管理



内容变化

等保五个规定动作

↓

五个规定动作+新的安全要求

等级保护1.0

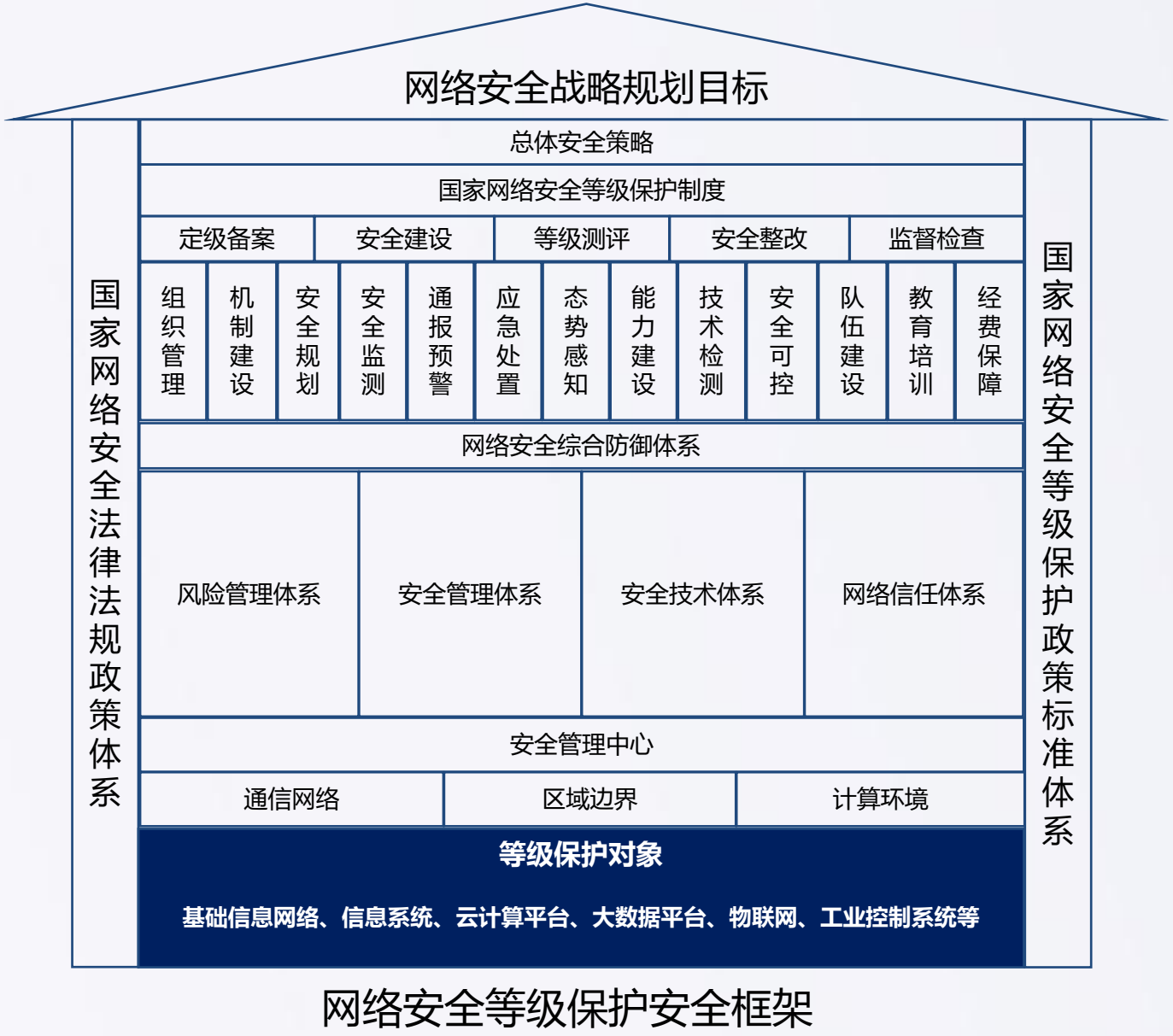
- 定级
- 备案
- 建设整改
- 等级测评
- 监督检查

内容变化 →

等级保护2.0

- 定级
- 备案
- 建设整改
- 等级测评
- 监督检查
- 安全检测
- 通报预警
- 案事件调查
- 数据防护
- 灾难备份
- 应急处理
- 风险评估

等级保护2.0安全框架和关键技术



网络安全等级保护安全框架

防护框架：

- 以“一个中心”管理下的“三重防护”体系框架，构建整体安全防护体系；
- 最终做到整体防御、分区隔离；积极防护、内外兼防；自身防御、主动免疫；纵深防御、技管并重 。

部分关键安全预防措施理解：

- 传统威胁：对于传统威胁，要做到快速、精准的防护；
- 新型网络攻击：对于新型网络攻击，要做到智能检测与分析；
- 建设和加强入侵防护等技术检测与防护是网络安全防护的重要工作；
- 维护网络安全，感知网络安全态势是网络安全防护中最基本、最基础的工作。

等级保护基本要求框架（以三级为例）

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

技术要求

安全管理中心

- 系统管理
- 审计管理
- 安全管理
- 集中管控

安全计算环境

- 身份鉴别
- 访问控制
- 安全审计
- 入侵防范
- 恶意代码防范
- 可信验证
- 数据完整性
- 数据保密性
- 数据备份恢复
- 剩余信息保护
- 个人信息保护

安全区域边界

- 边界防护
- 访问控制
- 入侵防范
- 可信验证
- 恶意代码和垃圾邮件防范
- 安全审计

安全通信网络

- 网络架构
- 通信传输
- 可信验证

安全物理环境

- 物理位置选择
- 物理访问控制
- 防盗窃和防破坏
- 防雷击
- 防火
- 防水和防潮
- 防静电
- 温湿度控制
- 电力供应
- 电磁防护

管理要求

安全管理制度

- 安全策略
- 管理制度
- 制定和发布
- 评审和修订

安全管理机构

- 岗位设置
- 人员配备
- 授权和审批
- 沟通和合作
- 审查和检查

安全管理人员

- 人员录用
- 人员离岗
- 安全意识教育和培训
- 外部人员访问管理

安全建设管理

- 定级和备案
- 安全方案设计
- 产品采购和使用
- 自行软件开发
- 外包软件开发
- 工程实施
- 测试验收
- 系统交付
- 等级测评
- 服务供应商选择

安全运维管理

- 环境管理
- 资产管理
- 介质管理
- 设备维护管理
- 漏洞和风险管理
- 网络和系统安全管理
- 恶意代码防范管理
- 配置管理
- 密码管理
- 备份与恢复管理
- 变更管理
- 安全事件处置
- 应急预案管理
- 外包运维管理

等级保护2.0差异变化

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

新增扩展要求

分类	一级	二级	三级	四级
安全通用要求	55	135	211	228
云计算安全扩展要求	11	29	46	49
移动互联安全扩展要求	5	14	19	21
物联网安全扩展要求	4	7	20	21
工业控制系统安全扩展要求	9	15	21	22

通用要求变化

安全类	控制点	主要变化
安全物理环境	物理位置选择	取消机房场地在顶层或地下室的限制
安全通信网络	通信传输	加强了通信传输的保密性要求
	可信验证	新增控制点
安全区域边界	边界防护	新增对非法外联的管控 针对无线网络要有边界防护设备
	访问控制	新增对内容的访问控制
	入侵防范	新增从内到外的攻击检测 新型网络攻击行为的分析
	恶意代码和垃圾邮件防范	新增垃圾邮件方案要求（针对三级及以上）
	可信验证	新增控制点

安全类	控制点	主要变化
安全计算环境	可信验证	新增控制点
	数据完整性	新增对于密码技术的使用
	数据保密性	加强数据保密性要求 三、四级要求使用密码技术
	数据备份恢复	加强备份要求，二级异地备份 三、四级要求异地实时备份、数据处理系统热冗余
	个人信息保护	新增控制点
安全管理中心	系统管理	新增要求，二级以上有要求
	审计管理	新增要求，二级以上有要求
	安全管理	新增要求，三、四级要求
	集中管控	新增要求，三、四级要求

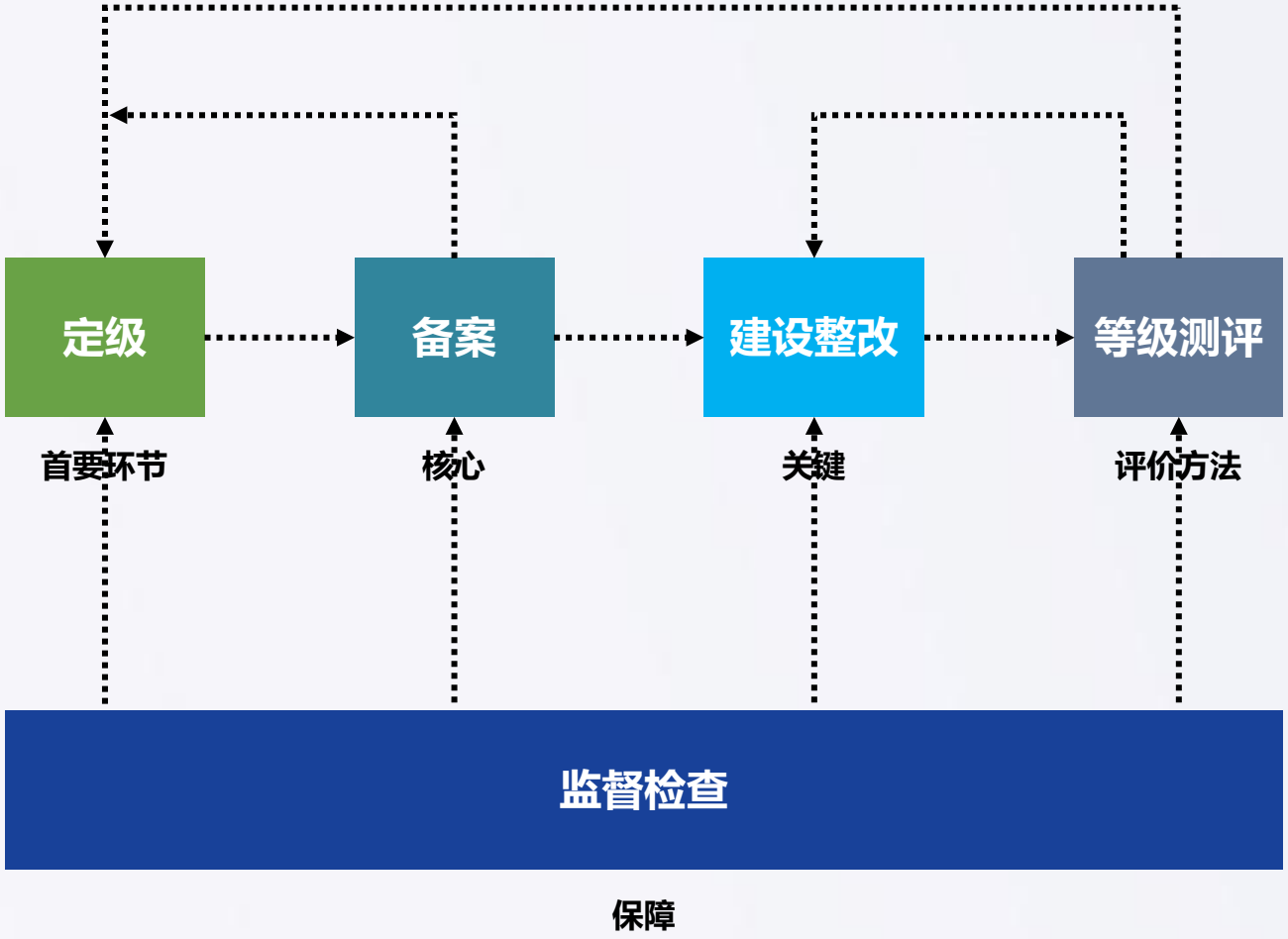
等级保护2.0通用要求相关产品和措施（三级）

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

安全类	安全控制点	相关产品和措施
安全物理环境	物理位置选择	合理选择机房位置
	物理访问控制	电子门禁系统
	防盗窃和防破坏	防盗报警系统、视频监控系统
	防雷击	防雷保安器、过压保护装置
	防火	火灾自动消防系统
	防水和防潮	防水检测仪表、元件
	防静电	静电消除器、防静电手环
	温湿度控制	机房空调
	电力供应	稳压器、过电压防护设备、UPS
	电磁防护	屏蔽柜、屏蔽机房
安全通信网络	网络架构	负载均衡、流量控制、网管软件、防火墙、路由器、交换机
	通信传输	VPN
	可信验证	采用可信产品或技术措施
安全区域边界	边界防护	防火墙、终端接入控制系统、云盾、网闸、路由器和交换机、
	访问控制	下一代防火墙、上网行为管理、云盾、网闸、路由器和交换机
	入侵防范	下一代防火墙、潜伏威胁探针、安全感知平台、全流量威胁分析系统、云端抗DDoS、云盾
	恶意代码和垃圾邮件防范	下一代防火墙、云盾、邮件安全网关
	安全审计	日志审计系统、堡垒机、网络安全审计、基础级防火墙、VPN
	可信验证	采用可信产品或技术措施

安全类	安全控制点	相关产品和措施
安全计算环境	身份鉴别	网络设备、安全设备、服务器、应用配置项、VPN、堡垒机、终端接入控制系统、统一身份管理
	访问控制	网络设备、安全设备、服务器、应用配置项
	安全审计	网络设备、安全设备、服务器、应用配置项、日志审计系统、堡垒机、网络安全审计
	入侵防范	网络设备、安全设备、服务器、应用配置项、终端接入控制系统、堡垒机、下一代防火墙、云盾、基线核查系统、云镜、云眼、终端检测响应平台、潜伏威胁探针、安全感知平台
	恶意代码防范	终端检测响应平台
	可信验证	采用可信产品或技术措施
	数据完整性	网络设备、安全设备、服务器、应用配置项、VPN、CA
	数据保密性	网络设备、安全设备、服务器、应用配置项、VPN、数据加密软件、数据库加密系统
	数据备份恢复	容灾备份系统、重要数据处理系统热备冗余
	剩余信息保护	服务器、应用配置项
	个人信息保护	应用配置项
安全管理中心	系统管理	堡垒机、集中管理平台、安全感知平台、XSec集成安全平台
	审计管理	数据库审计系统、日志审计系统、网络安全审计、堡垒机
	安全管理	堡垒机、集中管理平台、安全感知平台、XSec集成安全平台
	集中管控	网管软件、堡垒机、安全感知平台、XSec集成安全平台、日志审计系统、数据库审计系统、集中管理平台、终端检测响应平台

等级保护工作流程



定级

步骤：确定定级对象，初步确定安全保护等级，**专家评审，主管部门审核、**公安机关备案审查

备案

持定级报告和备案表到当地公安机关网安部门进行备案，获取备案证明

建设整改

参照网络安全等级保护相关标准及规范要求，对信息系统进行整改加固

等级测评

委托具备测评资质的测评机构对信息系统进行等级测评，形成正式的测评报告

监督检查

向当地公安机关网安部门提交测评报告，配合完成对信息安全等级保护实施情况的检查。

等级保护工作角色分工

网络安全等级保护工作包括**定级、备案、建设整改、等级测评、监督检查**五个流程。在等级保护全流程中，涉及到四个不同的角色，分别是：运营使用单位、公安机关、深信服、测评机构。等级保护各工作流程内容及角色分工如下：

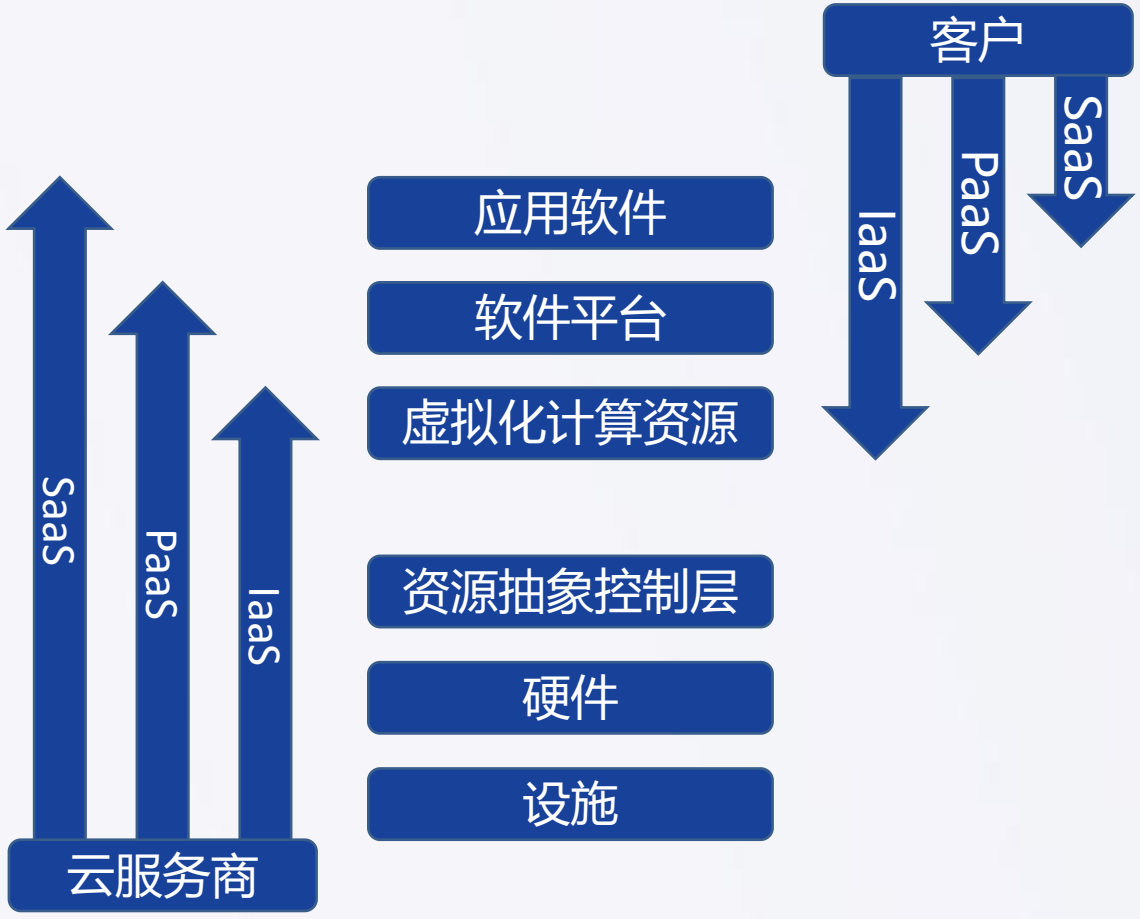
流程 \ 角色	运营、使用单位	公安机关	深信服	测评机构
定级	确定安全保护等级，填写定级备案表、编写定级报告		协助运营、使用单位确认定级对象，为其提供定级咨询服务，辅导运营、使用单位准备定级报告，并组织专家评审（二级以上）	可承接运营、使用单位的定级咨询服务
备案	准备备案材料，到当地公安机关备案	当地公安机关审核受理备案材料	辅导运营、使用单位准备备案材料和提交备案申请	可承接运营、使用单位的备案服务
建设整改	建设符合等级要求的安全技术和管理体系		依据相应等级要求对当前实际情况进行差距分析，针对不符合项以及行业特性要求进行个性化的整改方案设计，协助运营、使用单位完成建设整改工作	
等级测评	准备和接受测评机构测评		在测评阶段会指导运营、使用单位配合测评中心开展等级测评工作，并保障顺利通过等保测评获得测评报告	对等级保护对象符合性状况进行测评
监督检查	接受公安机关的定期检查	公安机关监督检查运营、使用单位是否按要求开展等级保护工作	根据运营、使用单位需要配合完成自查工作，协助运营、使用单位接受检查和进行整改	

等级保护基本要求框架

云计算等级保护=安全通用要求+云计算安全扩展要求

云计算服务模式与责任划分

《信息安全技术 云计算服务安全应用指南》GB/T 31167-2014中将云计算分为IaaS、PaaS、SaaS模式。不同模式下云服务商与云服务客户的控制范围不同。



云计算服务模式与控制范围的关系

- **应用软件层：**为客户提供业务系统所需的应用软件
- **软件平台层：**编译器、函数库、工具、中间件
- **虚拟化计算资源层：**虚拟机、虚拟存储、虚拟网络等
- **资源抽象控制层：**虚拟机资源监视器（Hypervisor）
- **硬件层：**物理计算资源、存储资源、网络资源
- **设施层：**物理环境、通信线路等

云计算平台及云服务客户保护对象划分

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

服务模式	安全层面	保护（测评）对象
SaaS	安全计算环境	云产品（服务）
		云产品（服务）数据
PaaS	安全计算环境	虚拟机、数据库服务器、中间件、容器、云应用开发平台、云产品（服务）等
IaaS	安全计算环境	云操作系统、虚拟机监视器、云业务管理系统、云产品（服务）
		虚拟化网络/安全设备、虚拟机镜像
		云产品（服务）服务器（虚拟机）、宿主机、终端、运管平台服务器
		网络设备、安全设备
		配置文件、鉴别信息、系统数据、审计数据、镜像文件、快照数据、个人信息
	安全通信网络	网络架构、物理链路、通信数据
	安全区域边界	物理网络边界、虚拟网络边界
	安全管理中心	云管理平台、云平台监控系统
	安全管理	安全相关人员、机房、介质以及管理文档和制度
	安全物理环境	物理机房、云计算基础设施部署的相关机房及技术设施

云计算平台不同服务模式下的保护对象

服务模式	安全层面	保护（测评）对象
IaaS	安全计算环境	云服务客户业务应用系统
		虚拟机、数据库、中间件
		虚拟网络设备、虚拟安全设备
	安全通信网络	虚拟网络架构
	安全区域边界	虚拟网络边界防护服务（措施）
PaaS	安全计算环境	容器，数据库
	安全管理中心	安全管理平台
	安全管理	全相关人员、介质以及管理文档
SaaS	安全计算环境	业务数据
		业务应用系统
	平台侧安全	云计算平台等级测评结论/云服务符合性评价

云服务客户业务系统不同服务模式下的保护对象

云等保定级备案

	云服务商	云服务客户
备案地点	负责云计算平台备案，备案地点为运维管理端所在地	负责云上业务信息系统备案，备案地点工商注册地或实际经营所在地
备案系统	大型云计算平台应将云计算基础设施与辅助系统（运维系统、运营系统）分别定级	在云端的业务应用系统
备案等级	关键信息基础设施云计算平台≥3级； 不低于承载的等级保护对象的安全保护等级	参照《网络安全等级保护定级指南（报批稿）》
备案时间	对外提供服务前	云计算平台完成备案后

材料准备

- 等级保护备案表
- 拓扑图及说明
- 安全组织机构及管理制度
- 安全产品销售许可证明

专家评审

- ≥2级均应进行专家评审
- 评审定级报告，获得专家评审意见

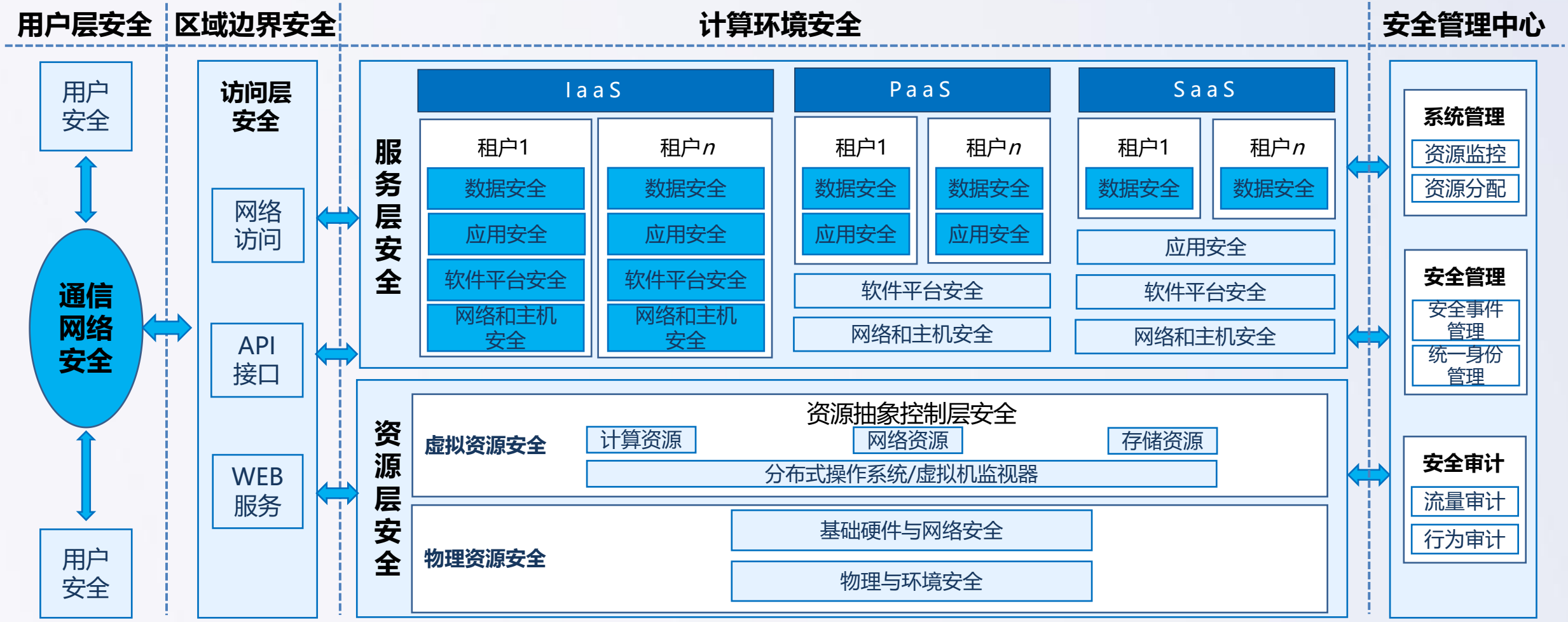
主管部门审核

- 定级结果报行业主管部门或上级部门进行审核

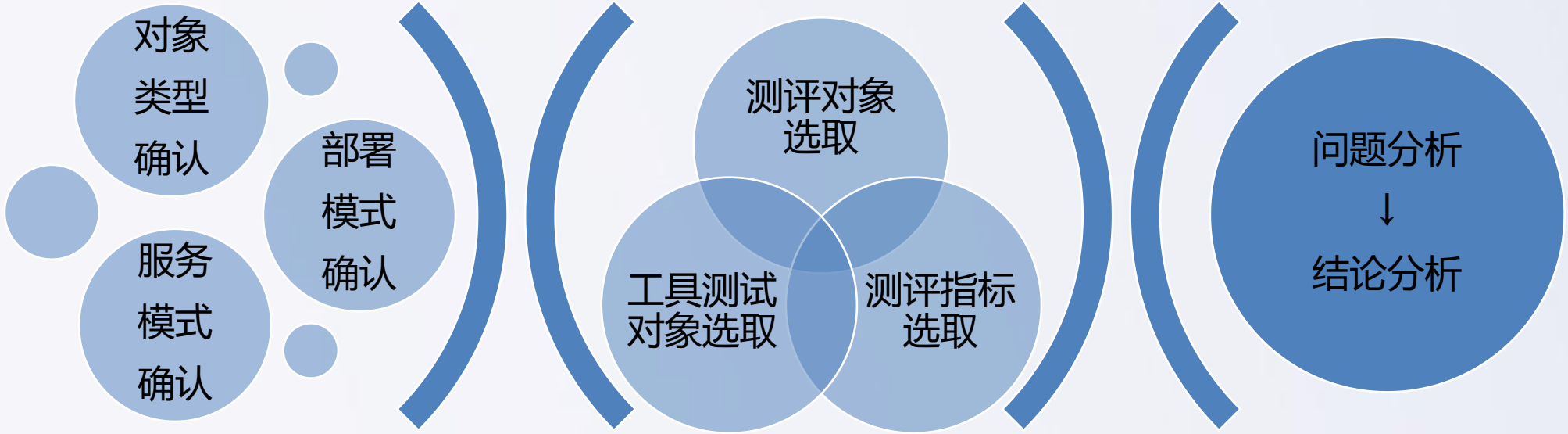
公安机关备案审查

- 提交相关材料至县级以上公安机关
- 获得备案证明

云计算等级保护安全技术设计框架



云等保测评流程



	调研阶段	准备阶段	实施与分析阶段
云服务商	1.填写信息调研表；	1.根据测评机构对象选取结果准备设备； 2.准备管理制度及相关表单。	1.配合测评机构完成现场测评及验证测试； 2.根据测评结论进行整改。
云服务客户	1.要求云服务商提供云计算平台的备案证明； 2.填写信息调研表。	1.要求云服务商提供《等保测评报告》结论页、云计算系统测评结论扩展信息表； 2. 根据测评机构对象选取结果准备设备； 3.IaaS和PaaS模式下需准备管理制度及相关表单。	1.配合测评机构完成现场测评及验证测试； 2.根据测评结论进行整改。

云等保测评结论

测评对象	等级保护测评判别依据	等级保护测评判定结论
云计算平台	云计算平台存在的问题中无中、高风险项，且得分不低于90分。	优
	云计算平台存在的问题中无高风险项，且得分不低于80分。	良
	云计算平台存在的问题中无高风险项，且得分不低于70分。	中
	云计算平台存在的问题中**存在高风险项**，**或**得分**低于70**分。	差
云服务客户业务应用系统	云计算平台等级测评结论为优，云服务客户业务应用系统存在的问题中无中、高风险项，且得分不低于90分。	优
	云计算平台等级测评结论为良，云服务客户业务应用系统存在的问题中无高风险项，且得分不低于80分。	良
	云计算平台等级测评结论为中，云服务客户业务应用系统存在的问题中无高风险项，且得分不低于70分。	中
	云计算平台等级测评结论为优、良、中，云服务客户业务应用系统存在的问题**存在高风险项**，或得分低于70分；云计算平台等级测评结论为**差**，则**不考虑云服务客户的等级保护测评结论。**	差

注：使用云计算技术的应用系统等级保护测评结论参照通用系统结论

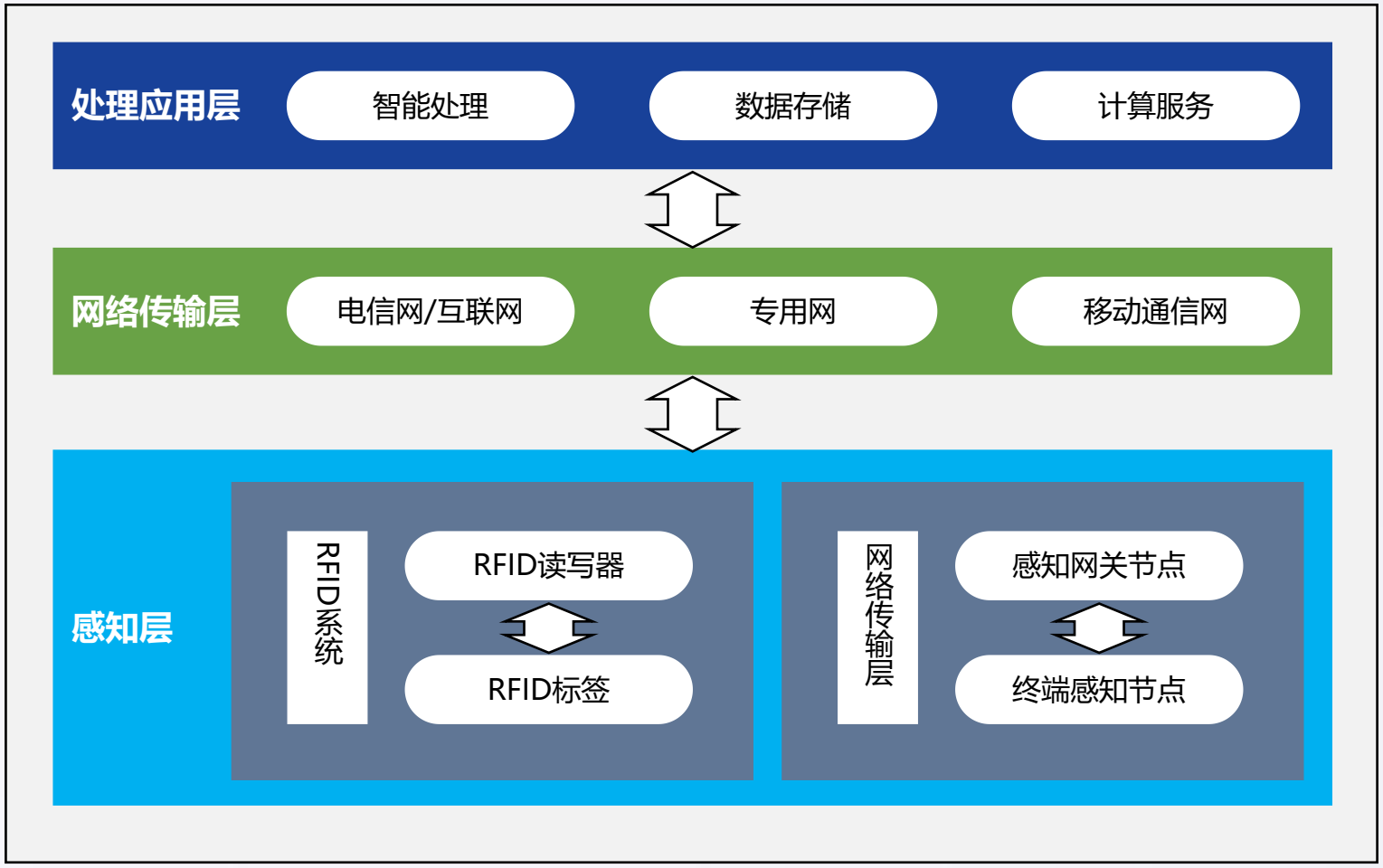
移动互联安全扩展要求

移动互联安全扩展要求章节针对移动互联的特点提出特殊保护要求。对移动互联 环境主要增加的内容包括“无线接入点的物理位置”、“移动终端管控”、“移动应用管控”、“移动应用软件采购”和“移动应用软件开发”等方面。

安全要求项	一级	二级	三级	四级
安全通用要求	55	135	211	228
移动互联安全扩展要求	5	14	19	21

- 针对采用移动互联技术的等级保护对象其移动互联部分提出特殊保护 要求。移动互联部分通常由移动终端、移动应用和无线网络三部分组成。
- 移动互联部分涉及的对象不单独定级，与后台应用一起整体进行定级。

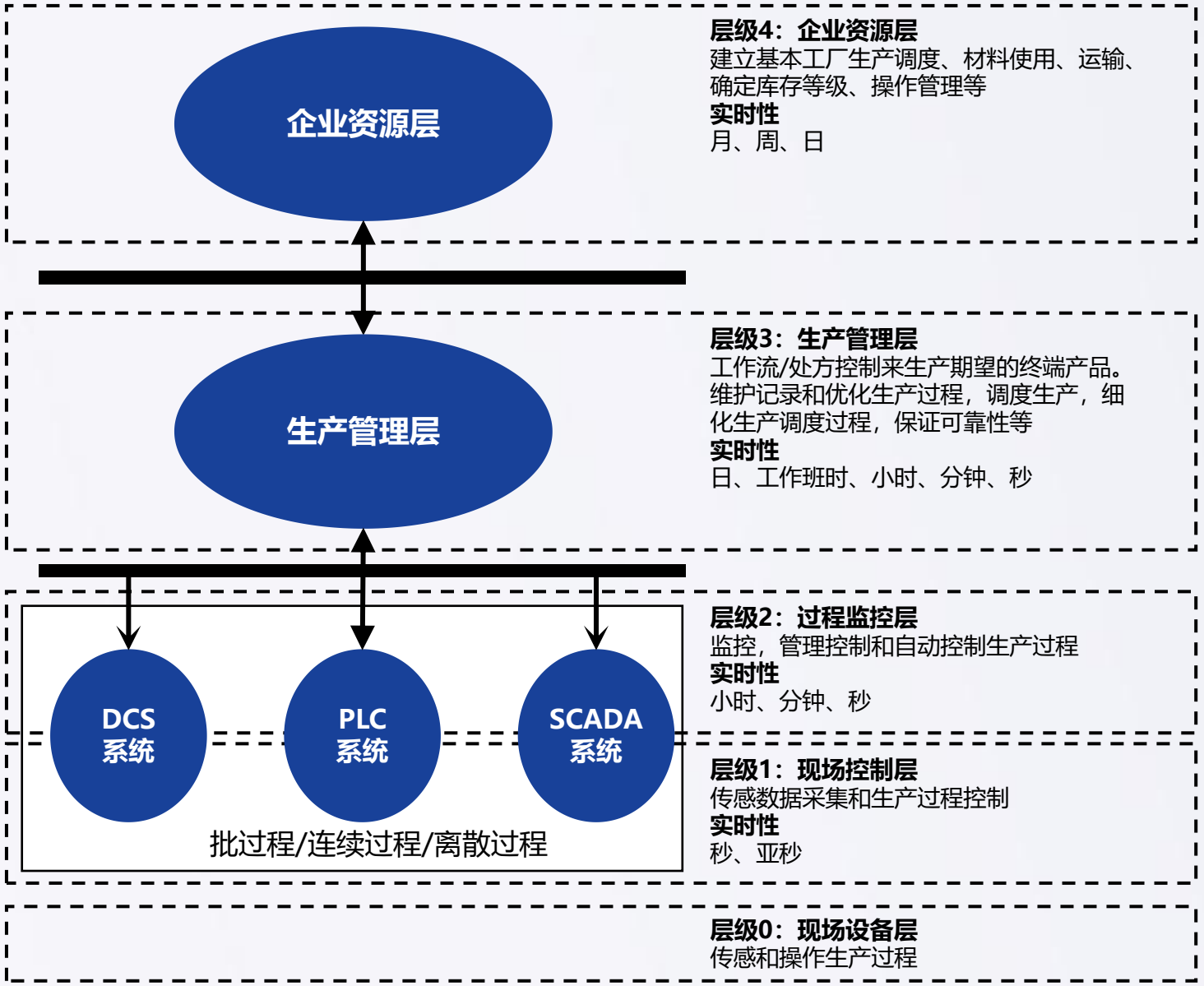
物联网系统层次模型



- **处理应用层**主要包括对感知数据进行存储与智能处理的平台，并对业务应用终端提供服务
- **网络传输层**主要包括将这些感知数据远距离传输到处理中心的网络，包括互联网、移动网等，以及几种不同网络的融合
- **感知层**主要包括传感器节点和传感器网关节点，或RFID标签和RFID读写器，也包括这些感知设备及传感网网关、RFID标签与阅读器之间的短距离通信（通常为无线）部分

各个层次实现等级保护基本要求的差异

工业控制系统层次模型



- **企业资源层**主要包括ERP系统功能单元，用于为企业决策层员工提供决策运行手段；
- **生产管理层**主要包括MES系统功能单元，用于对生产过程进行管理，如制造数据管理、生产调度管理等；
- **过程监控层**主要包括监控服务器与HMI系统功能单元，用于对生产过程数据进行采集与监控，并利用HMI系统实现人机交互；
- **现场控制层**主要包括各类控制器单元，如PLC、DCS控制单元等，用于对各执行设备进行控制；
- **现场设备层**主要包括各类过程传感设备与执行设备单元，用于对生产过程进行感知与操作。

各个层次实现等级保护基本要求的差异

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

目录

深信服等级保护2.0价值主张

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

安全可视

采用可视化设计，提供多维度安全报表为安全决策提供数据支撑，提升组织安全管理效率。

协同防御

参照防御/检测/响应的安全模型，加强云防护/威胁情报的联动，构建本地协同、云端联动的动态保护体系。

持续检测

对企业核心资产、各类威胁与违规行为，网络东西向、南北向流量进行持续检测分析，提升网络整体安全保护能力。

深信服等级保护2.0建设规划框架

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

持续保护，不止合规

安全可视能力　持续检测能力　协同防御能力

安全价值

安全保障

安全体系

技术体系

安全管理中心	系统管理 审计管理 安全管理 集中管控
安全计算环境	身份鉴别 访问控制 安全审计 入侵防范 恶意代码防范 可信验证 数据完整性 数据保密性 数据备份恢复 剩余信息保护 个人信息保护
安全区域边界	边界防护 访问控制 入侵防范 恶意代码和垃圾邮件防范 安全审计 可信验证
安全通信网络	网络架构 通信传输 可信验证
安全物理环境	物理位置选择 物理访问控制 防盗窃和防破坏 防雷击 防火 防水和防潮 防静电 温湿度控制 电力供应 电磁防护

管理体系

- 安全管理制度
- 安全管理机构
- 安全管理人员
- 安全建设管理
- 安全运维管理

运营体系

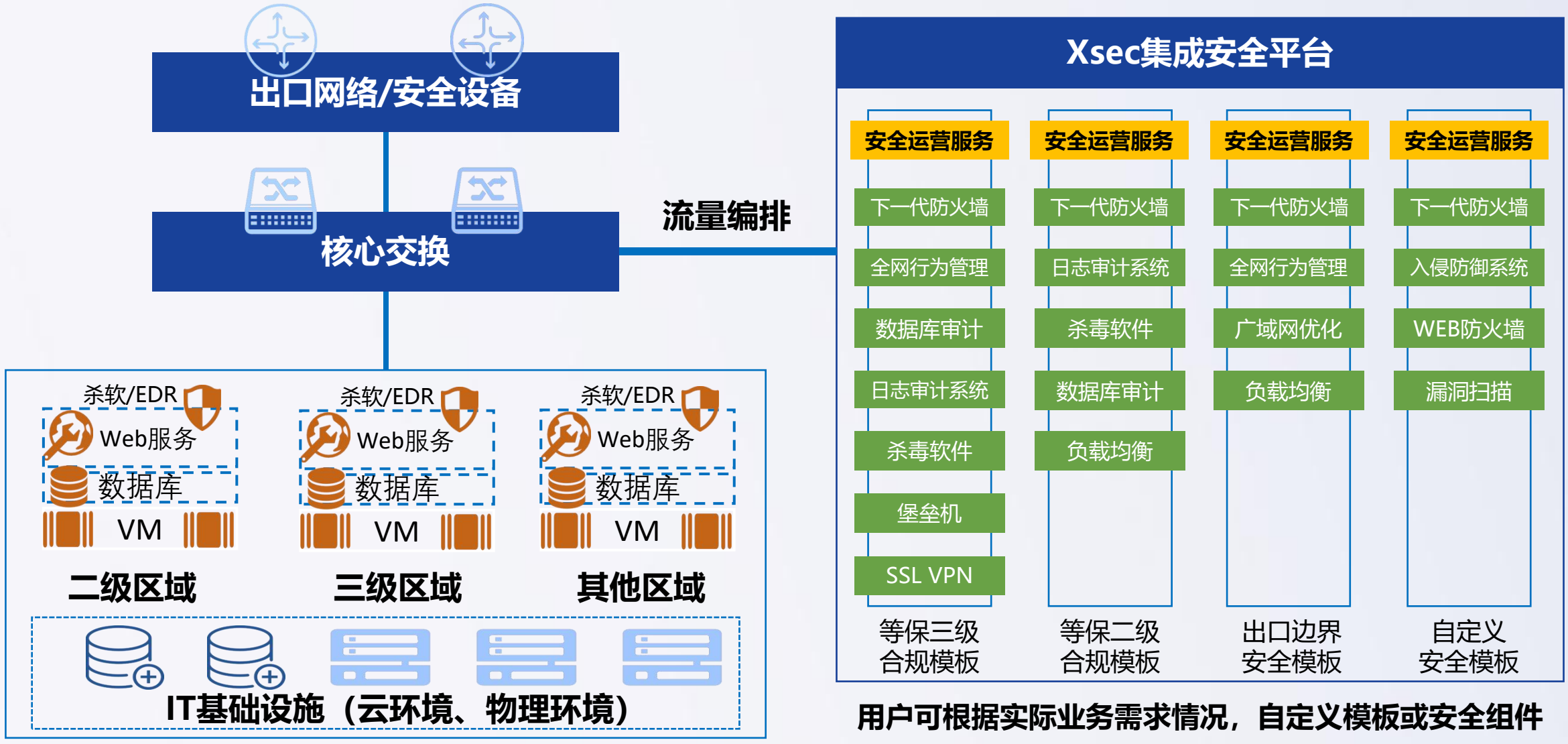
- 风险评估
- 渗透测试
- 漏洞扫描
- 基线核查
- 应急响应
- 应急演练
- 安全培训

能力支撑

能力模型

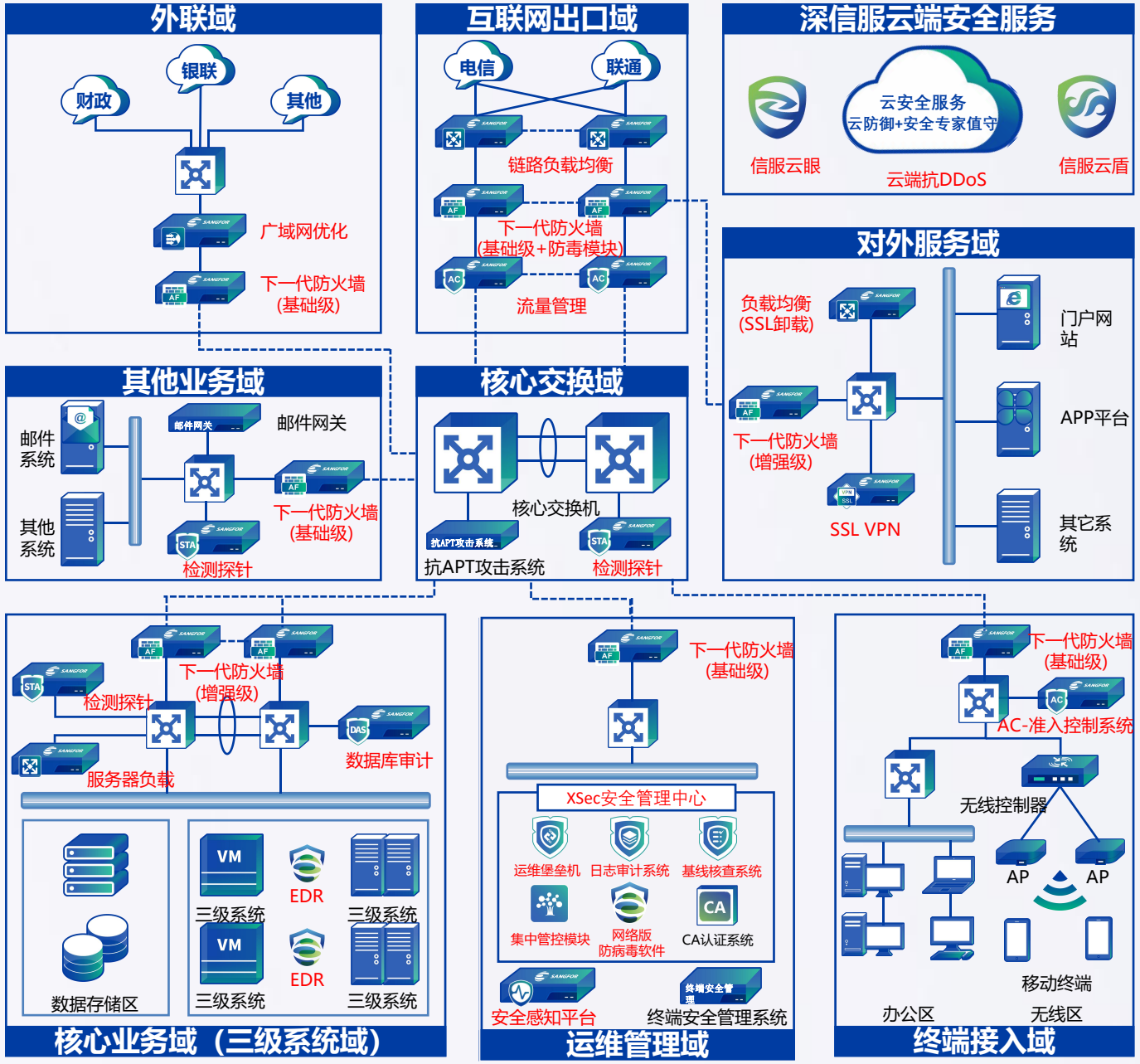
智能(A)	智能流量分析 智能文件分析 日志关联分析 安全数据基线 安全云脑 威胁情报 机器学习
防御(P)	网络防御 应用防御 零信任
检测(D)	已知威胁 未知威胁 安全监测
响应(R)	应急演练 应急处置 调查取证
运营(O)	资产发现与暴漏面监测 漏洞识别与优先级排序 威胁狩猎 风险评估 安全加固 攻防演练 安全意识 7×24保护

深信服“XSec集成安全平台”创新方案



用户可根据实际业务需求情况，自定义模板或安全组件

实践思考一：等保2.0通用方案解决方案



二级等保安全产品（服务）列表

必选	建议	可选
下一代防火墙	SSL VPN	数据库审计
网络版防病毒软件	上网行为管理	堡垒机
日志审计系统	检测探针+感知平台	云端安全服务
	XSec安全管理中心	风险评估服务

三级等保安全产品（服务）列表

必选	建议	可选
下一代防火墙	SSL VPN	广域网优化设备
网络版防病毒软件	堡垒机	风险评估服务
日志审计系统	负载均衡	测试渗透服务
上网行为管理	检测探针+感知平台	应急响应服务
数据库审计	基线核查系统	应急演练服务
XSec安全管理中心	云端安全服务	
	邮件网关	

说明：

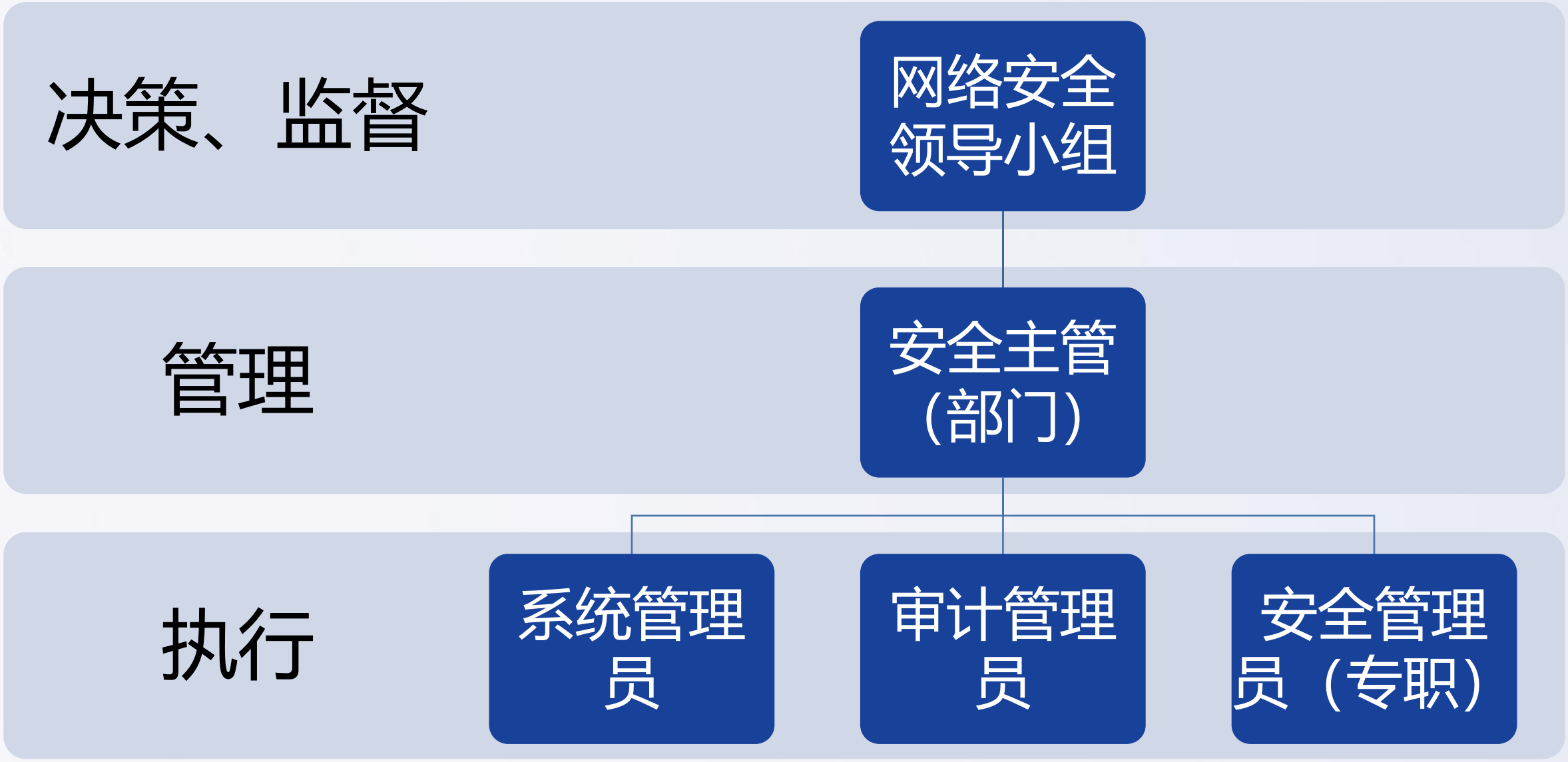
- ✓ 产品（服务）列表主要针对左侧通用场景拓扑情况；
- ✓ XSec安全管理中心产品中的数据库审计、日志审计、堡垒机、漏洞扫描、网管中心、BBC、补丁管理等安全组件可根据用户情况选择

“XSec集成安全平台”界面展示

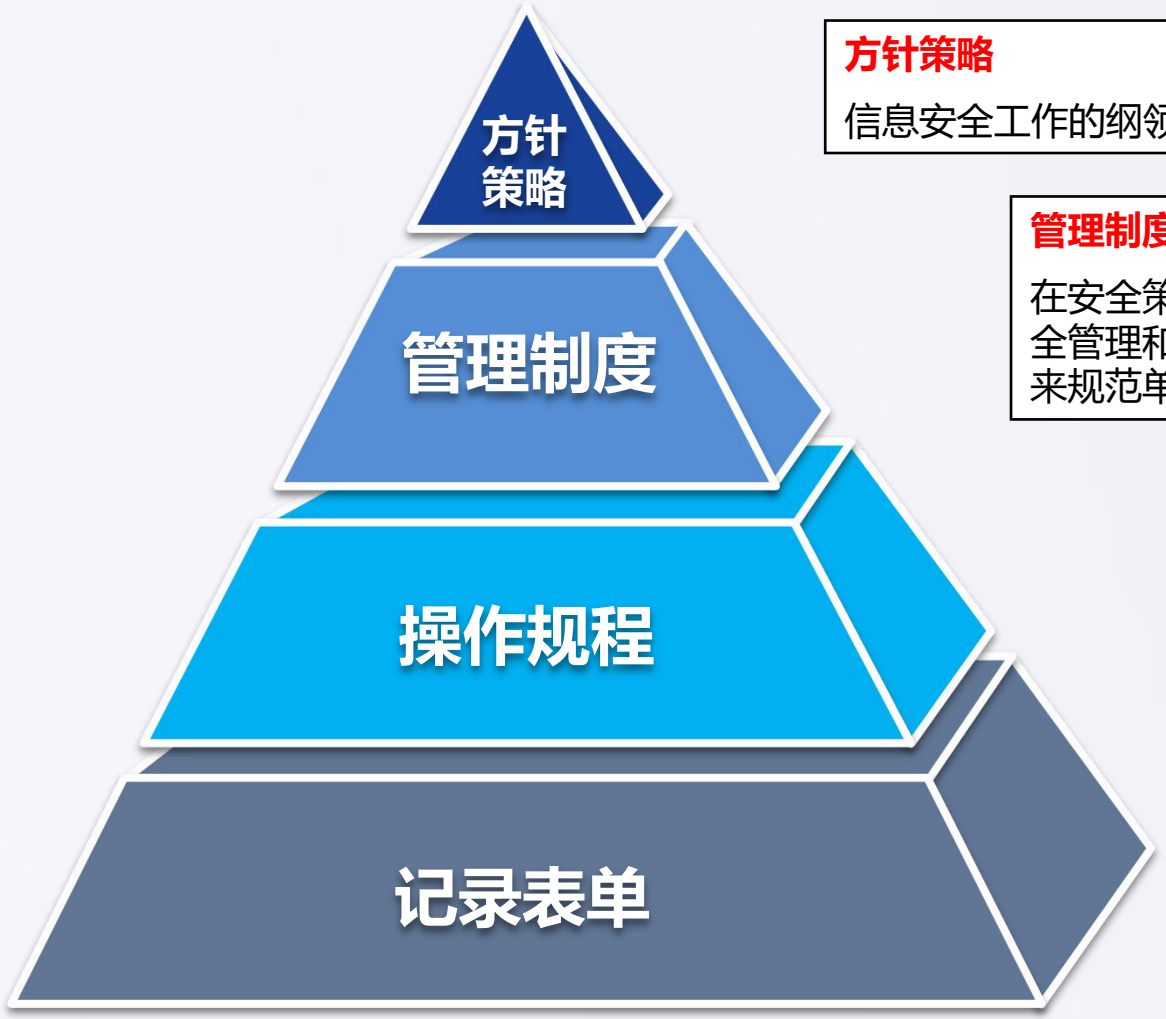
SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

安全平台首页 → 多场景模板选择 → 安全组件自定义 → 第三方组件大融合

安全管理体系建设-高效的安全管理机构



安全管理体系建设-体系化的管理制度



方针策略

信息安全工作的纲领性文件。

管理制度

在安全策略的指导下，制定的各项安全管理和技术制度、办法和准则，用来规范单位各部门处室安全管理工作。

操作规程

细化的实施细则、管理技术标准等内容，用来支撑第二层对应的制度与管理办法的有效实施。

记录表单

记录活动实行以符合一、二、三等级的文件要求的客观证据，阐明所取得的结果或提供完成活动的证据。

安全管理体系文件（参考）

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

控制类	安全控制点	文档名称
安全管理制度	安全策略	《网络安全工作的总体方针和安全策略》
	管理制度	《物理环境安全管理制度》 《通信网络安全管理制度》 《办公终端和主机设备安全管理制度》 《应用系统安全管理制度》 《数据安全管理制度》 《安全建设管理制度》 《安全运维管理制度》等
		《设备操作规程》等
	制定和发布	《制度制定、发布、评审和修订管理制度》
	评审和修订	
安全管理机构	岗位设置	《网络安全组织机构管理办法》
	人员配备	《网络安全组织机构管理办法》
	授权和审批	《授权和审批管理制度》
	沟通和合作	《沟通与合作管理制度》
	审核和检查	《安全审查和检查管理制度》
安全管理人员	人员录用	《人员安全管理制度》
	人员离岗	《人员安全管理制度》
	安全意识教育和培训	《网络安全培训管理制度》
	外部人员访问管理	《外部人员访问管理制度》

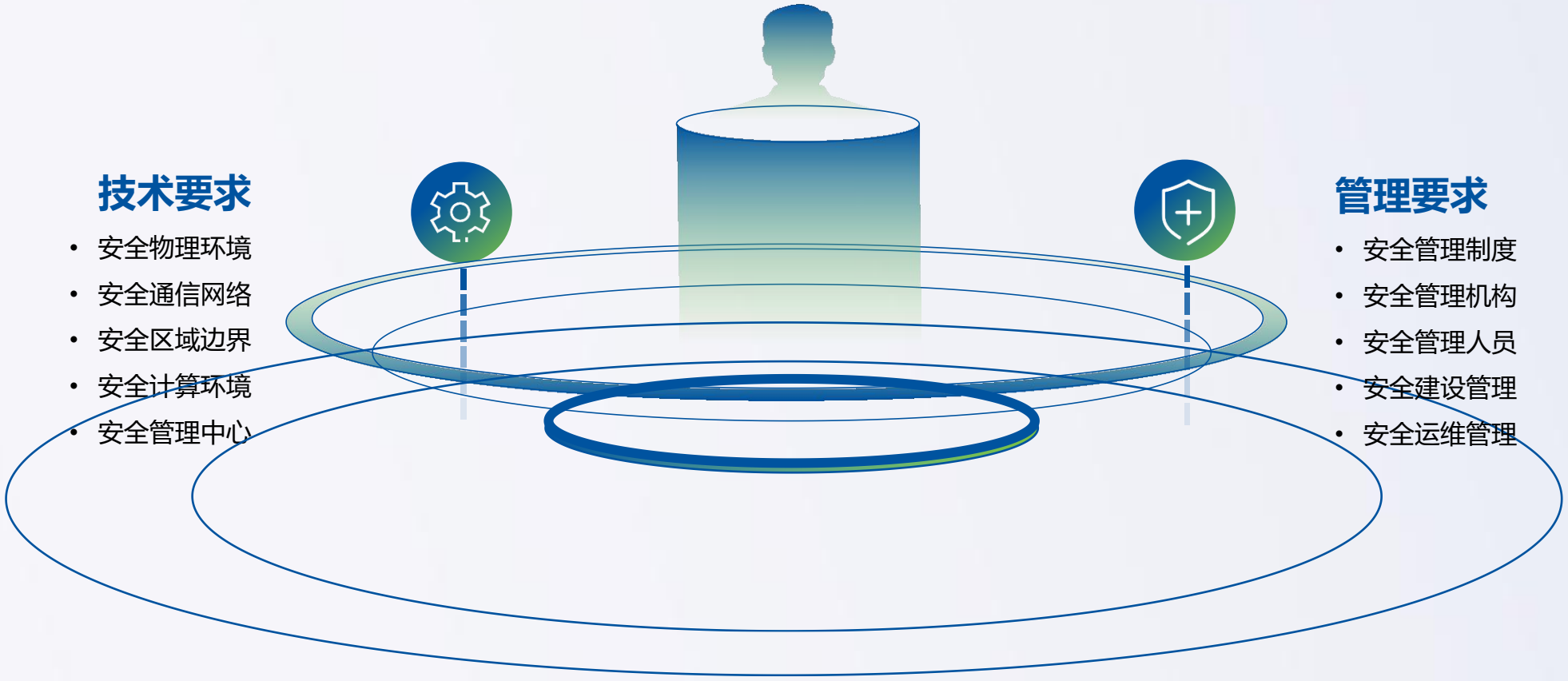
控制类	安全控制点	文档名称
安全建设管理	定级和备案	《网络安全等级保护管理规定》
	安全方案设计	《网络与信息系统安全设计规范》
		《等级保护2.0解决方案》
	产品采购和使用	《IT产品采购管理制度》
		《密码产品与服务的采购和使用审查表》
	自行软件开发	《软件开发管理制度》
		《代码编写安全规范》
		《软件开发文档指南》
		《软件开发管理制度》
	外包软件开发	《外包软件开发管理规范》
	工程实施	《工程实施管理规范》
		《安全工程实施方案》
	测试验收	《工程测试验收方案》
		《安全测试报告》

控制类	安全控制点	文档名称
安全运维管理	环境管理	《机房安全管理制度》
	资产管理	《信息管理制度》 《资产信息分类文档》 《信息资产管理办法》
	介质管理	《介质安全管理规定》
	设备维护管理	《设备维护管理制度》
	漏洞和风险管理	《风险评估管理制度》 《漏洞管理规定》
	网络和系统安全管理	《网络安全管理制度》 《系统安全管理制度》 《账户、密码及权限管理制度》 《变更运维审批记录》
	恶意代码防范管理	《恶意代码管理制度》
	配置管理	《基本配置信息记录》
	密码管理	遵循相关的国家标准和行业标准要求
	变更管理	《变更管理制度》
	备份与恢复管理	《备份与恢复管理制度》
	安全事件处置	《网络安全事件与应急管理制度》
	应急预案管理	《网络安全应急预案》

技术要求与管理要求落地保障

安全运营

把安全当作一项业务，通过运营把
等级保护2.0中的技术和管理要求落地



技术要求

- 安全物理环境
- 安全通信网络
- 安全区域边界
- 安全计算环境
- 安全管理中心

管理要求

- 安全管理制度
- 安全管理机构
- 安全管理人员
- 安全建设管理
- 安全运维管理

深信服安全SaaS网站安全托管服务

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

网站/APP

企业网站

企业网站或OA系统上云

信服云盾 信服云眼

深信服安全云

合作安全机构

攻击产业化

执法常态化

持续监测、安全防护与处置

风险评估 防护托管 事件监测 应急响应 专家

持续加固 持续检查 持续响应

公众账号、微信群、邮箱等

企业运维人员

黑客 监管/主管单位

防扫描 防篡改 防被黑 零运维 全程可视 人机共智 7×24小时服务

安全SaaS网站安全托管服务价值

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

WEB安全托管闭环解决方案价值

7*24小时持续监测

- 安全SaaS平台对网站集群进行篡改监测、漏洞扫描、网站可用性监测，针对网站挂马等安全问题及时告警

动态防护

- 安全SaaS平台对网站集群进行整体安全防护，如SQL注入等，实时阻断威胁，自动化替身等处置高危安全事件

主动应急响应

- 后台专家7×24小时运营服务，出现安全事件后，及时告警、处置及响应（自动切换至安全的缓存页面）

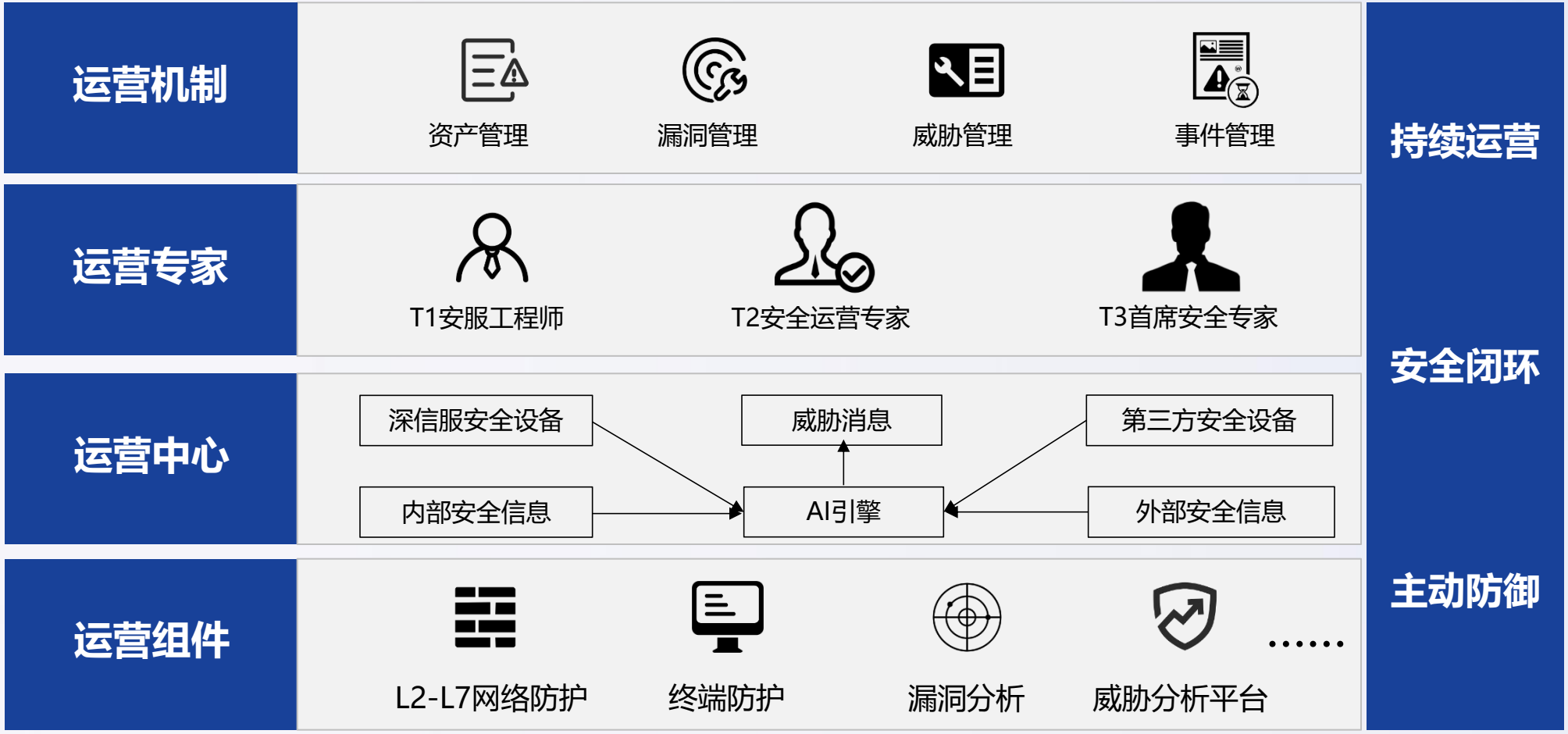
全程保障

全程可视，随时掌握安全态势

专家在线，保障安全效果

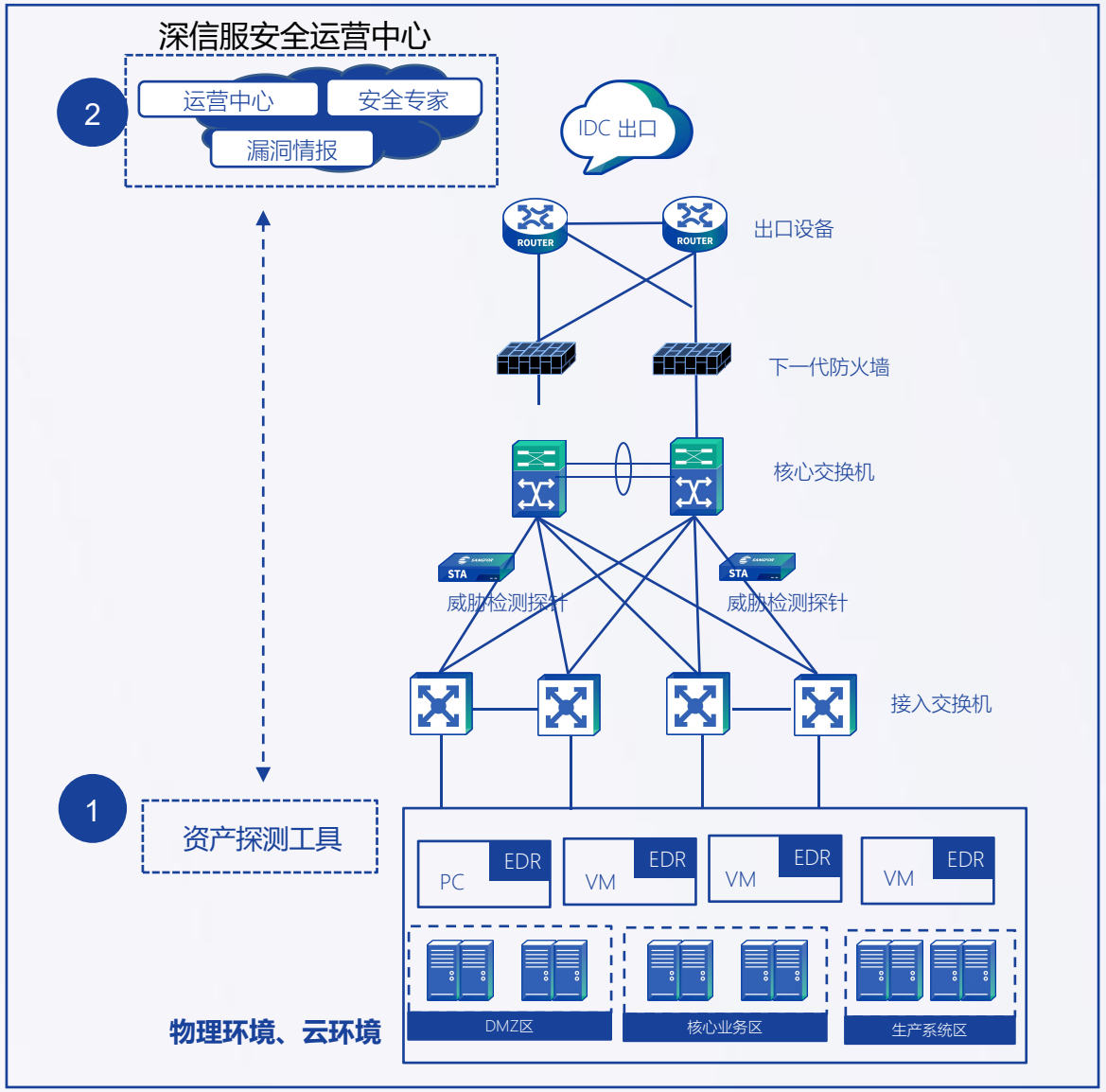
托管式服务交付

人机共智的安全运营架构



人机共智的安全运营架构，7×24小时持续为用户提供有效的安全保护

持续运营：资产管理



资产管理五步法

Step1 组件部署：设置相关策略

Step2 资产梳理：梳理台账、主动探测

Step3 资产发现：监测影子资产、变更资产

Step4 资产分级：对发现的资产进行重要性分级

Step5 资产台账：完善资产管理台账

全面梳理、主动探测、变更通知、持续管理

持续运营：漏洞管理

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

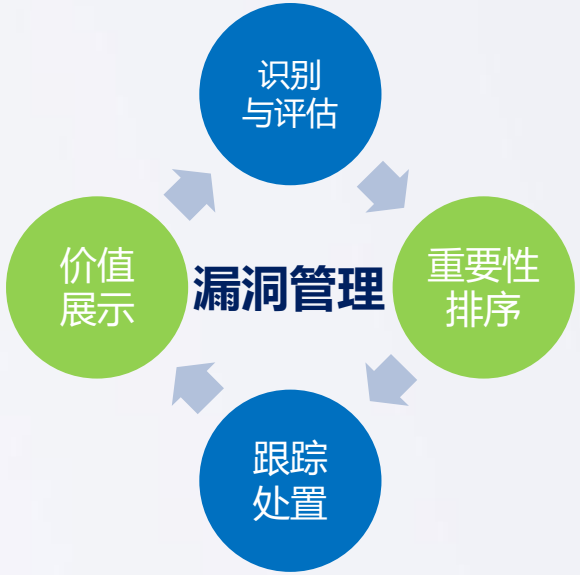
措施

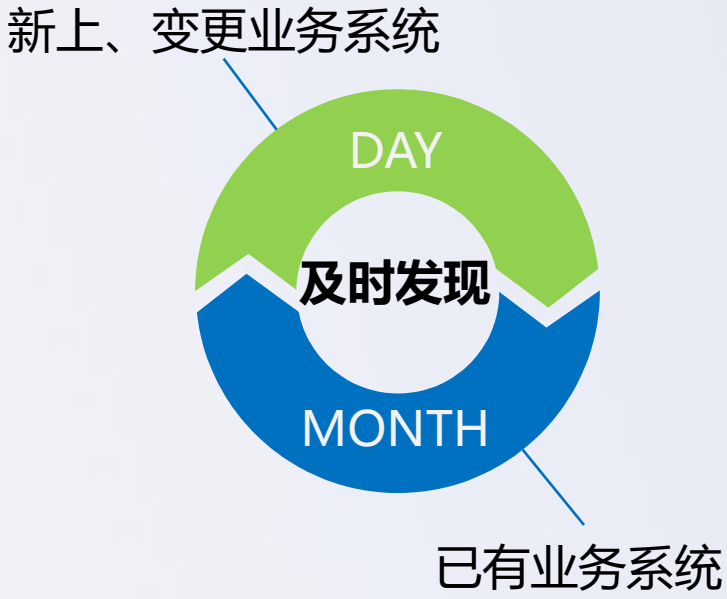
客观的优先级修复建议

可落地的漏洞修复方案

标准化的漏洞闭环管理

最新漏洞的预警与响应





实现资产漏洞全生命周期管理，预防漏洞引发的安全事件

持续运营：威胁管理

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

前期准备

安全用例设计

根据以往经验设定不同安全用例（USECASE），通过这些安全用例可以实时关联分析海量的安全日志，提炼更需要关注的安全信息；

持续服务

安全威胁监测

基于安全用例，进行7*24小时对安全日志的监测分析；同时也对客户侧的互联网网站进行7*24小时监测分析；

专业分析及定位

高级安全专家进行研判验证。一旦被认为是真实的威胁，将迅速确定后续处置计划，并立即进展进一步分析，如横向影响面分析。

处置

基于安全用例，提供可落地的处置建议；必要时，根据内部操作规范进行威胁处置工作。

总结汇报

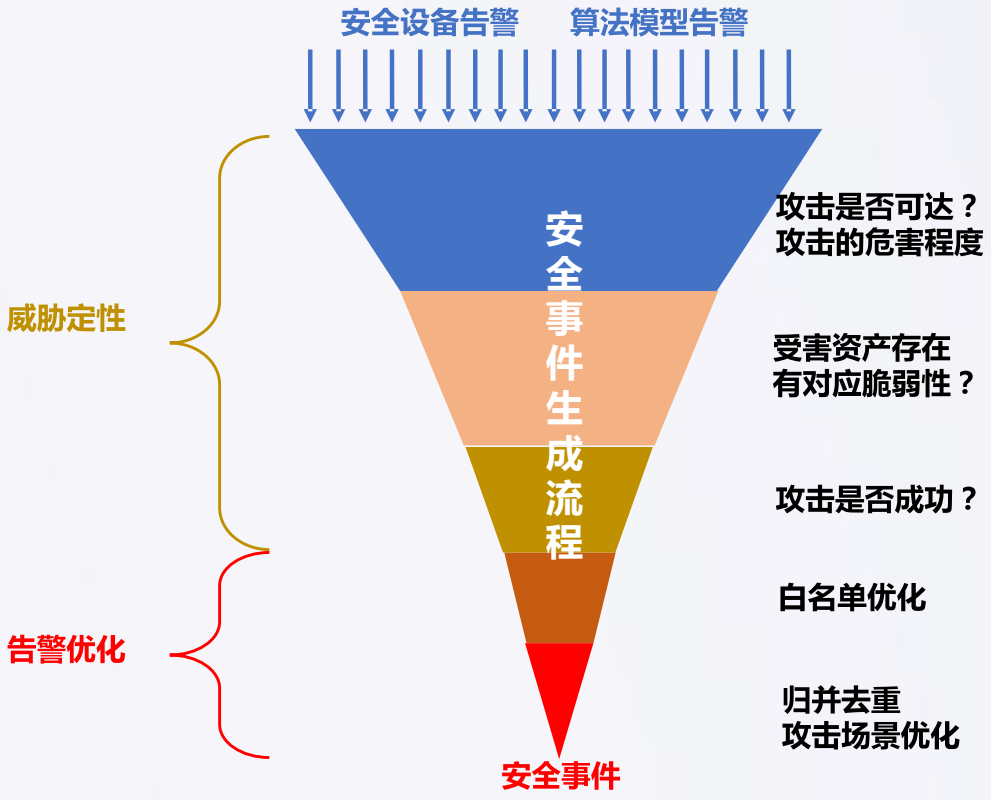
周期性分析威胁管理措施有效性，并提供未来安全建议及规划建议。

7×24小时持续监测、专家研判，精确处置，持续服务

持续运营：事件管理

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

主动监测安全事件



积累上千类安全事件处置实例

在线团队快速响应

主动监测，快速响应，过程可视

安全运营优势价值

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

持续运营

通过持续监测，动态发现问题，及时通报，并协助处置，实现持续运营

安全闭环

通过线上线下三级安全专家，对发现的问题进行快速响应，实现安全闭环

主动防御

主动发现问题、处置问题，优化网络安全体系，实现主动防御

深信服安全服务

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

安全运营类服务

- 安全运营
- 漏洞管理
- 威胁监测与主动响应
- 安全事件响应
- 安全通告

安全评估类服务

- 风险评估
- 渗透测试
- 漏洞扫描
- 基线核查
- 代码审计
- APP检测
- 无线安全评估

安全培训类服务

- 安全意识培训
- CISP培训
- CISAW培训

安全运维类服务

- 安全日志分析与响应
- 安全加固
- 驻场运维
- 应急演练
- 应急响应

安全规划咨询服务

- 等保建设咨询
- 安全规划咨询

等保建设咨询服务能力-服务商资质

全国首批

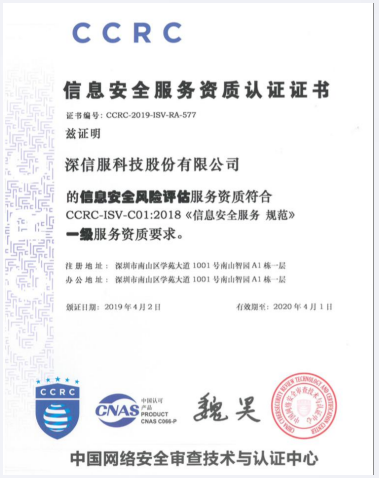
信息安全等级保护安全建设服务机构能力评估合格证书

安全工程类一级

国家信息安全测评信息安全服务资质证书

国家级

网络安全应急服务支撑单位证书

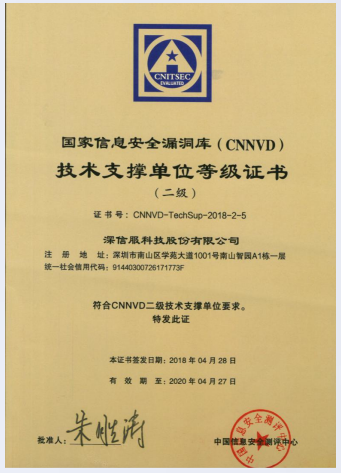


风险评估（一级）

信息安全风险评估服务资质认证证书

应急处理（一级）

信息安全应急处理服务资质认证证书



支撑单位（二级）

国家信息安全漏洞库(CNNVD)技术支撑单位等级证书

等保建设咨询服务能力-人员资质

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

国家重要信息系统保护人员证书

等级保护安全建设专业技术人员

注册信息安全专业人员（CISP）

信息安全保障人员（CISAW）

注册信息系统安全专家（CISSP）

深信服智安全产品/服务全景图

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

有效保护的安全产品

边界安全

- 下一代防火墙 AF
- 入侵防御系统 IPS
- Web应用防火墙 WAF

终端安全

- 终端检测响应平台 EDR
- 企业移动管理 EMM

云安全

- XSec集成安全平台
- 网站安全托管服务 SaaS

身份与访问安全

- 全网行为管理 AC
- SSL VPN
- 统一身份管理 IDtrust

威胁检测

- 安全感知平台 SIP
- 全流量威胁分析 NTA

安全审计与运营

- 安全云图 X-Central
- 数据库审计 DAS

合规类安全产品

合规审计

- 运维堡垒机 OSM
- 日志审计系统 LAS

风险评估

- 基线核查系统 BVT

安全隔离

- 网闸 GAP/光闸 FGAP

人机共智的安全服务

运营类

- 安全运营
- 威胁检测与主动响应
- 漏洞管理
- 安全事件响应

评估类

- 风险评估
- 渗透测试
- 漏洞扫描

培训类

- 安全意识培训
- CISP/CISAW培训

咨询类

- 等保建设咨询
- 安全规划咨询

运维类

- 安全日志分析与响应
- 应急演练/应急响应

深信服智安全优势

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

多款安全产品市场占有率第一

- 硬件VPN产品市场份额第一
- 上网行为管理产品市场份额第一
- SSL VPN产品市场份额第一
- 广域网优化产品市场份额第一
- 下一代防火墙产品在综合类防火墙品类中市场份额第二

国际认可

- ICSA防火墙认证
- 中国唯一获NSS Labs “Web攻击防护”最高评价“推荐”
- OWASP测评四星
- AC、WOC、SSL VPN是唯一入围国际Gartner魔力象限的国产品牌

广泛的生态合作

战略合作伙伴

Microsoft、intel、redhat、NVIDIA、腾讯云、阿里云、aws、Baidu 百度、HUAWEI、inspur 浪潮

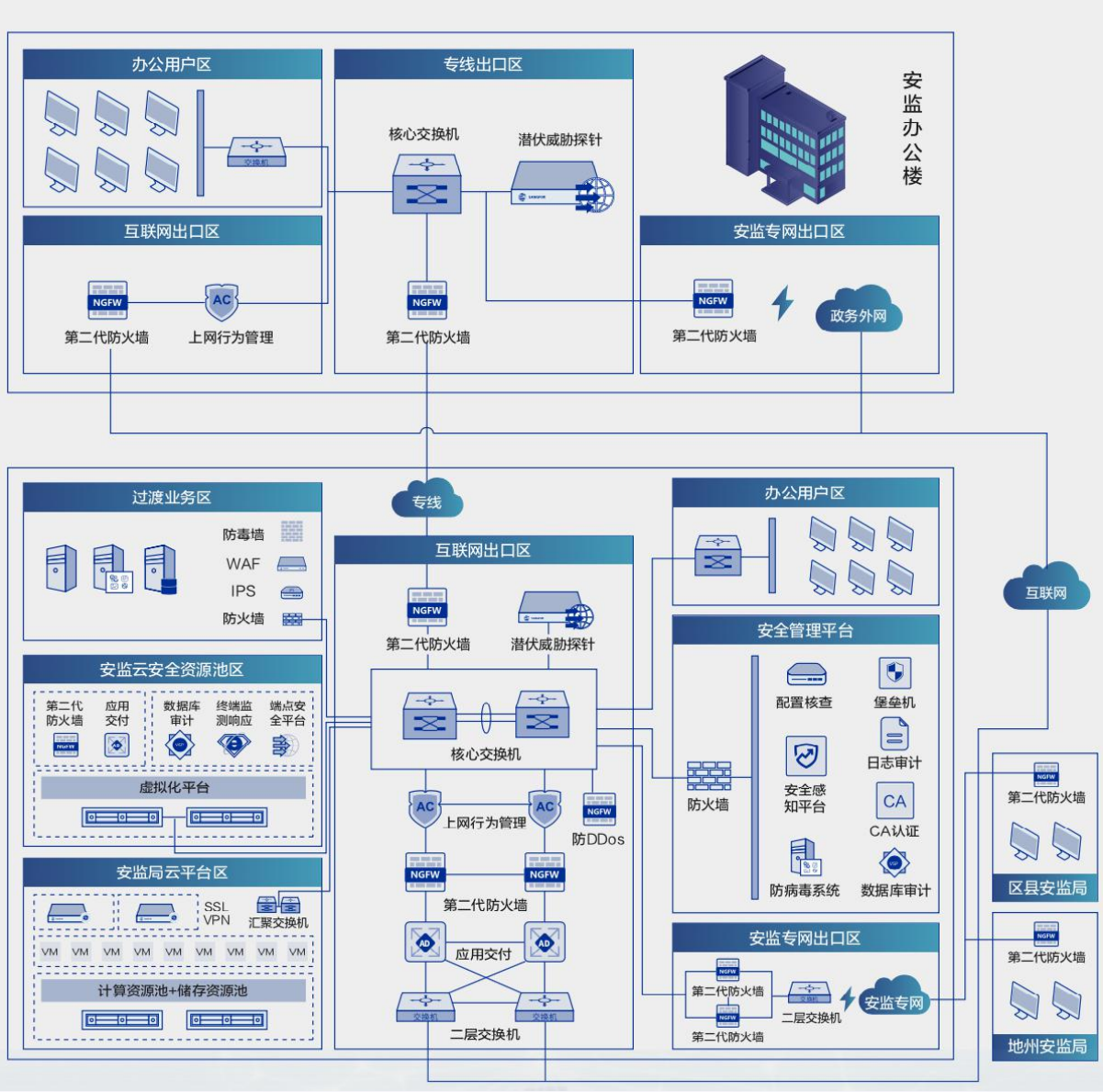
安全解决方案合作伙伴

吉大正元、Avira、KASPERSKY、RISING 瑞星、火绒安全 www.huorong.cn、JIANGMIN 江民科技、圣博润 SBR-info、思福迪 SAFETY、建恒信安 JIAN HENG XIN AN、云安宝、WebRAY 盛邦安全、JUMING 聚铭、安盟信息 SECURITYUNION、victory-idea 伟思信安、联软科技 LEAGSOFT、Infogo 盈高科技、Softnext 守内安信息科技、ANTIY 安天、兰云科技 LANYUN TECHNOLOGIES、兰德网络 LANDE NETWORK | 摩卡 Mocha、6cloud 六方云、THNWIN、Oplead

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

目录

案例分享-政府



一、项目背景

XX应急管理厅（原安监局）主管根据原国家安监局下发的《关于印发全国安全生产“一张图”地方建设指导意见书的通知》的要求，建设XX“安监云”应用及大数据平台。

二、需求分析

1. 需要满足三级等保合规要求；
2. 侧重防御，缺乏检测响应手段；
3. 设备使用年限长，无法发挥应有价值。

三、方案设计

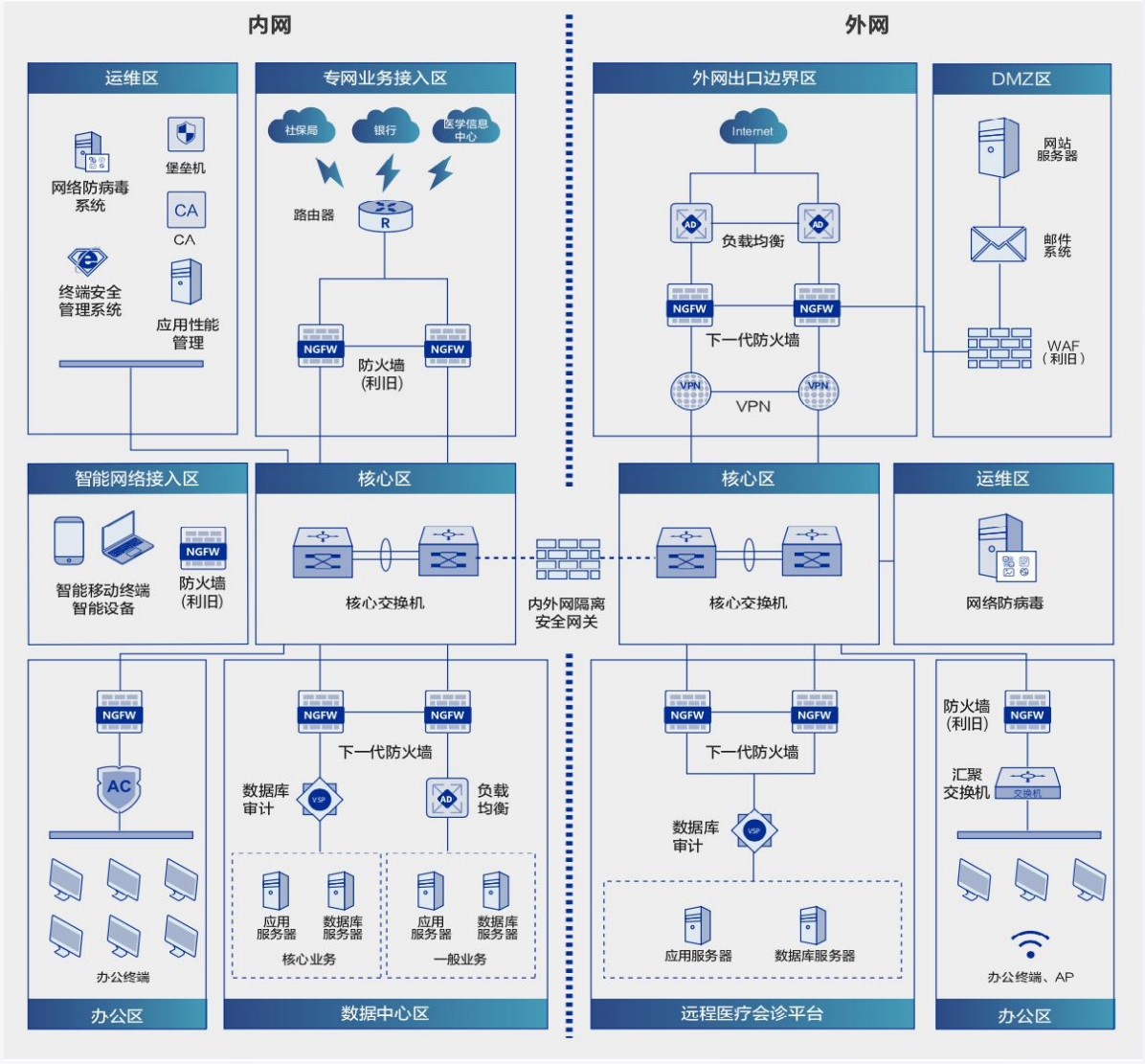
1. 网络边界安全：在各个重要网络节点部署下一代防火墙，提供L2-L7层全面的防护，构建融合防御体系；

2. 安全接入：部署深信服商密SSL VPN，实现端到端的安全接入，符合等级保护2.0移动互联安全建设要求；

3. 云平台安全：部署了集成服务平台，实现租户自助申请、自由组合安全组件，合规的同时满足个性化安全需求；

4. 安全运维管理：部署安全感知平台，帮助用户实时掌控全网安全态势，及时预知、处置安全事件。

案例分享-医疗



一、项目背景

XX医科大学附属医院作为市属公立医院，属于三级甲等医院，在新院区建设过程中，需要同步开展网络安全规划和建设工作。

二、需求分析

1. 充分保障系统运行安全和数据安全，具备新型高级威胁防御能力；

2. 按照三级等保要求进行网络规划设计。

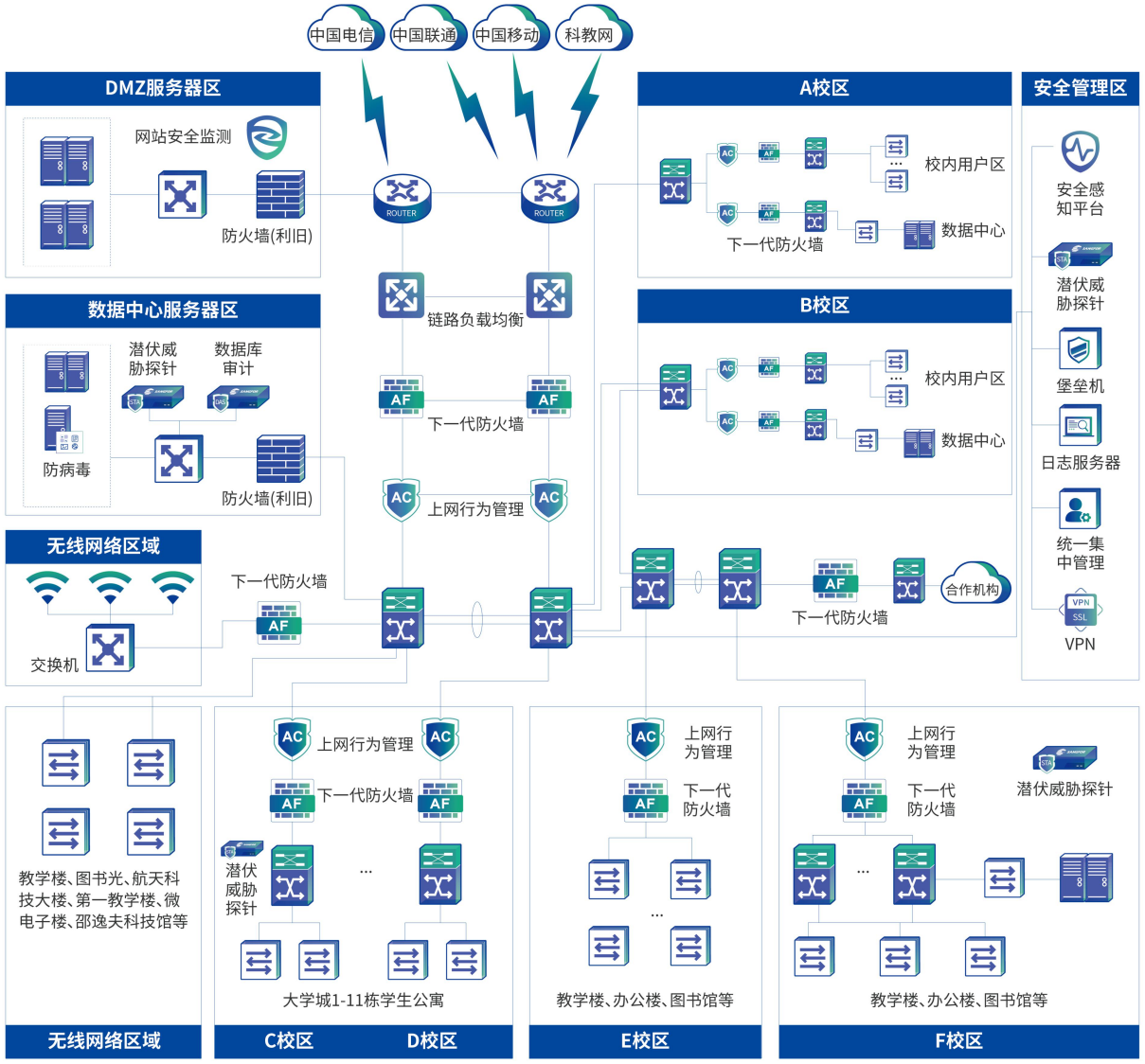
三、方案设计

1.两套网络：内外网部署两套逻辑隔离网络；

2.分级分域：实施边界安全隔离防护；

3.安全感知平台和潜伏威胁探针：二期加强检测能力、可视化能力，辅助快速响应，有效应对新型威胁。

案例分享-教育



一、项目背景

XX大学由教育部直属、中央直管，是中国著名顶级学府之一。XX省教育厅和公安厅在2015年开始就明确各高校需要针对业务系统进行分批次等级保护建设。

二、需求分析

1.需要满足等级保护相关要求；

2.网络攻击无法及时有效定位。

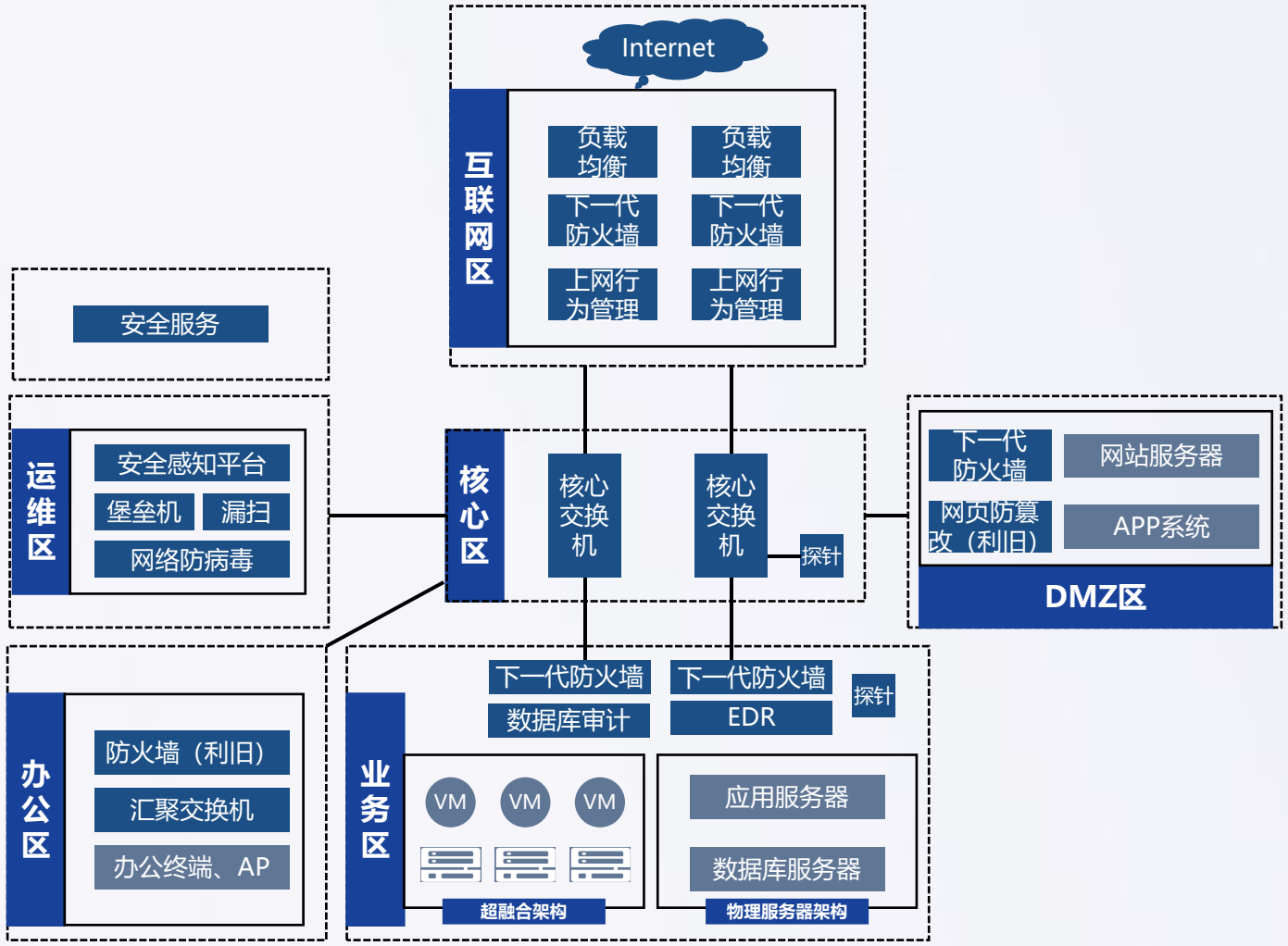
三、方案设计

1. 下一代防火墙：部署在教科网出口和核心数据中心出口，确保数据中心核心业务系统安全防护满足三级要求;

2. 安全感知平台：部署在运维管理区，针对经过数据中心的数据进行持续性检测，保障核心数据安全；

3. 应急分析与处置服务：在防御、检测的基础上，配套安全服务，在发现问题后可以实现快速响应，最大程度降低事件造成的影响。

案例分享-企业



一、项目背景

某央企集团作为XX集团旗下的重点单位，随着网络安全法的实施，积极响应国家号召，对于等级保护保持着空前关注，包含网站、项目管理系统等都纳入规划。

二、需求分析

1. 业务调整和政策法规对安全提出了更高要求；
2. 缺乏快速发现潜在威胁的能力；
3. 运维能力弱，无法形成安全闭环；
4. 业务云化带来新的安全挑战。

三、方案设计

1. 云上安全：通过部署EDR，解决云内东西向流量可视及访问控制问题，对于云内流量状态进行实时展示；

2. 全网态势感知：部署安全感知平台，通过设备联动并结合“人机共智”安全运维，对告警进行及时响应。

行业成功案例（部分）

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

政府

- 中华人民共和国交通运输部
- 国家气象局
- 中国环境监测总站
- 国家粮食局
- 国家知识产权局
- 陕西省人民政府
- 河北省人民政府
- 浙江省经济和信息化委员会
- 新疆维吾尔自治区应急管理厅
- 贵州省安全生产监督管理局
- 吉林省人力资源和社会保障厅
- 中华人民共和国福建海事局
- 陕西省人社保障厅
- 江西省省委党校
- 甘肃省交警总队
- 内蒙古司法厅
- 北京市民政局
- 天津市住房公积金管理中心
- 大连市政法委
- 乌鲁木齐市司法局
- 深圳市电子政务资源中心
- 成都市人力资源和社会保障局
- ……

医疗

- 北京博爱医院
- 山东大学齐鲁医院
- 中南大学湘雅医院
- 青海省第五人民医院
- 安徽省中医药大学第二附属医院
- 中山大学附属第二医院
- 浙江省新华医院
- 云南省肿瘤医院
- 湖南省肿瘤医院
- 南方医科大学深圳医院
- 深圳大学学府医院
- 延安市中医院
- 保定市第二人民医院
- 商丘市第一人民医院
- 同煤总医院
- 深圳市孙逸仙心血管医院
- 深圳市南山区人民医院
- 怀化市第一人民医院
- 西藏自治区卫健委
- 广西医科大一附院
- 厦门大学附属心血管病医院
- ……

教育

- 复旦大学
- 武汉大学
- 郑州大学
- 东北大学
- 山西医科大学
- 内蒙古医科大学
- 天津医科大学
- 中央民族大学
- 山东财经大学
- 广西师范大学
- 乌鲁木齐职业大学
- 扬州职业大学
- 武汉工程大学
- 华北电力大学
- 香港中文大学（深圳）
- 河北工业职业技术学院
- 贵州工商职业学院
- 福建工程学院
- 北京政法职业学院
- 云南文山学院
- 红河卫生职业学院
- 浙江财经学院
- ……

公检法

- 中华人民共和国公安部
- 广西壮族自治区公安厅
- 浙江省公安厅
- 黑龙江省公安厅
- 北京市公安局丰台分局
- 重庆市公安局
- 厦门市公安局
- 西安市公安局
- 广西壮族自治区高级人民法院
- 内蒙古自治区高级人民法院
- 合肥中级人民法院
- 阳泉市中级人民法院
- 遵义市中级人民法院
- 六盘水市中级人民法院
- 杭州市中级法院
- 深圳市龙岗区人民法院
- 河北省高级人民检察院
- 山西省人民检察院
- 深圳市检察院
- 杭州市人民检察院
- 梅州市人民检察院
- 开封市人民检察院
- ……

企业

- 中建三局
- 中冶南方
- 中国中车
- 中国二十二冶集团有限公司
- 中国检验认证集团有限公司
- 威海市水务集团有限公司
- 核工业建设集团
- 金川集团
- 中建八局第一建设公司
- 东风柳州汽车有限公司
- 上海机场集团
- 中国电建市政建设集团有限公司
- 呼和浩特市白塔机场
- 中核燃料元件有限公司
- 利亚德光电股份有限公司
- 北京城市排水集团有限责任公司
- 上海城投资产管理(集团)有限公司
- 上海申通地铁集团有限公司
- 科大国创软件股份有限公司
- ……

行业成功案例（部分）

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

广电

- 国家广播电视总局
- 湖北省广播电视信息网络股份有限公司
- 广西广播电视信息网络股份有限公司
- 厦门广播电视智能网络有限公司
- 江苏省广电网络股份有限公司
- 大连广播电视台
- 山西省电视台
- 大连广播电视台
- 河北省电视台
- 南方电视台
- 广东广播电视台
- 内蒙古广电
- 云南广电
- 济南电视台
- ……

自然资源

- 中华人民共和国自然资源部
- 陕西省自然资源厅
- 湖南省自然资源厅
- 湖北省自然资源厅
- 江西省自然资源厅
- 河北省自然资源厅
- 安徽省自然资源厅
- 山西省自然资源厅
- 重庆市规划和自然资源局
- 青岛市自然资源和规划局
- 廊坊市自然资源和规划局
- 沈阳市自然资源局
- 郴州市自然资源局
- 揭阳市自然资源局
- 雅安市自然资源局
- 澄江县国土资源局
- 宁海县国土资源局
- ……

财政

- 江苏省财政厅
- 云南省财政厅
- 福建省财政厅
- 山东省财政厅
- 山西省财政厅
- 陕西省财政厅
- 河北省财政厅
- 湖北省财政厅
- 湖南省财政厅
- 新疆维吾尔自治区财政厅
- 北京市财政局
- 厦门市财政局
- 沈阳市财政局
- 廊坊市财政局
- 北京市丰台区财政局
- 上海市普陀区财政局
- 广东省潮州市财政局
- ……

电力

- 宁夏华电供热有限公司
- 中电热电
- 南方电网烽火平台
- 福建省电力有限公司
- 霞浦核电
- 昱光电厂
- 西山煤电集团公司
- 西山煤电德威煤业有限公司
- 大唐电力
- 大武口电厂
- 国电内蒙古电力有限公司
- 海南电网公司
- 华润电力控股有限公司（深圳）
- 广东电网深圳供电局
- 杭州杭联热电有限公司
- 国电宿迁热电有限公司
- 湄洲湾发电厂
- ……

其他

- 中国联合网络通信有限公司广东省分公司
- 中国电信股份有限公司福建分公司
- 中国电信股份有限公司佛山分公司
- 内蒙古烟草专卖局
- 山西省戒毒管理局
- 甘肃省监狱管理局
- 惠州监狱
- 山东省女子监狱
- 中国邮政报
- 武汉市审计局
- 赣州市审计局
- 廊坊市审计局
- 天津市市政公路信息中心
- 呼和浩特白塔国际机场
- ……

专业的等级保护2.0安全服务商

影响力

- 深信服承办等级保护2.0国家标准宣贯会，以及省级等保宣贯会议20+场，地市级200+场
- 协助近万家用户落地等保建设，并顺利通过测评

专业性

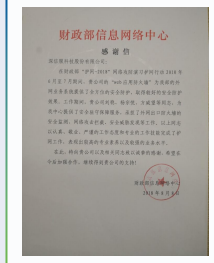
- 资质齐全：首批获得等级保护安全建设服务机构能力评估合格证书
- 人员专业：300+重要信息系统保护人员认证，分布全国各省、市
- 用户无忧：全流程“一站式”等保咨询与整改服务能力保障通过测评

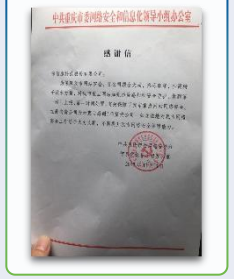
工具齐全

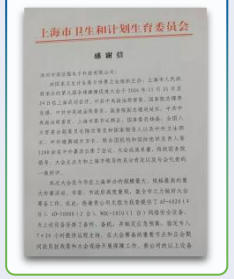
- 全流程服务：整理等保全流程材料模板与操作指引，含定级、备案、方案模板等工具
- 精品化方案：17+行业等级保护精品化方案素材、新技术（云移物工）等级保护方案素材

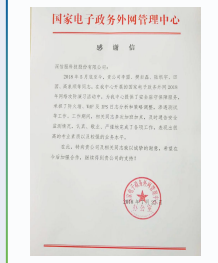
客户认可的网络安全服务商

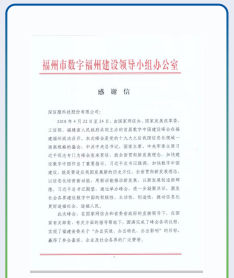
SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

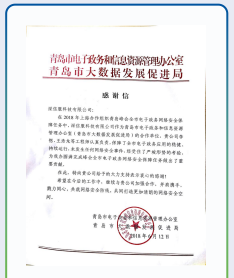


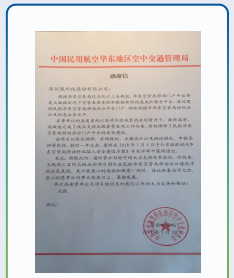


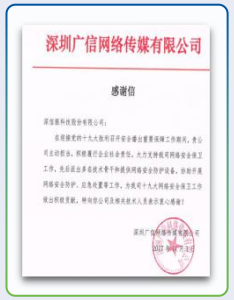


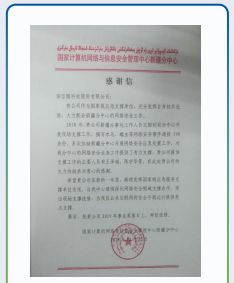












SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

THANK YOU

深信服 智安全