智慧校园下的等级保护建设

王鸿洋 湖南区产品主管
深信服科技

1 智慧校园建设趋势分析

2 等级保护标准演进

3 智慧校园下的等级保护建设

SANGFOR
深信服科技

信息化建设现状

基础网络建设

- 初步具有校园的网络环境
- 能实现简单的信息查询服务
- 应用系统较少或不能互联互通

教学应用信息化

- 具有较多的数字化资源
- 应用系统能集成
- 相关业务能整合
- 对教学教研管理和服务有一定的支持作用

业务系统资源整合

- 具有丰富的数字化资源
- 应用系统集成性强
- 相关业务高度整合
- 支持软件设施具有开放性和可扩展性
- 能较好的支持教学、教研、管理和服务

教育服务化

- 能有效支持教与学
- 丰富学校的校园文化
- 真正拓宽学习的时空纬度
- 以面向服务为基础的理念
- 基于新型网络技术构建业务流畅、资源共享、智能灵活的教育教学环境

大多数处于第二阶段向第三阶段过渡阶段

SANGFOR
深信服科技

落地保障-新技术助力智慧校园应用创新

1 智慧校园建设趋势分析

2 等级保护标准演进

3 智慧校园下的等级保护建设

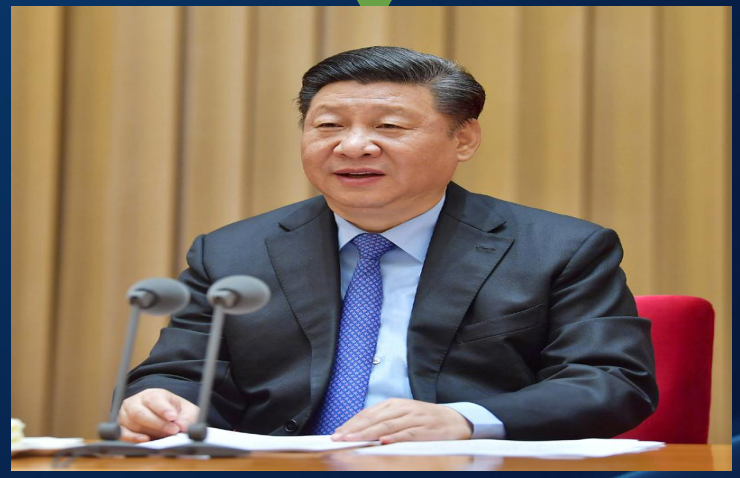
等级保护2.0时代标志

《关于加强社会治安防控体系建设的意见》

意见（七）加强信息网络防控网建设中要求“健全信息安全等级保护制度”

中央领导批示要求

习近平总书记等中央领导批示要求：健全完善以保护国家关键信息基础设施安全为重点的网络安全等级保护制度。



《中华人民共和国网络安全法》

《网络安全法》第21条明确要求：国家实行网络安全等级保护制度。

等级保护发展历程

1994年-国务院147号令

第九条：计算机信息系统实行安全等级保护。

1999年-GB 17859

强制性标准：规定了我国计算机信息系统安全保护能力的五个等级。

2003年-中办发27号文

信息安全保障纲领性文件。
第二条：实行信息安全等级保护。

2007年-公通字43号文

规定了等级保护基本内容、流程及工作要求等，为开展信息安全等级保护工作提供了规范保障 。

2017年-《网络安全法》

第二十一条：国家实行网络安全等级保护制度。
第三十一条 ： 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。

2018年-《网络安全等级保护基本要求》

新国标发布，等级保护建设正式进入 2.0时代。

《中华人民共和国网络安全法》--法律要求及责任

➢第二十一条： 国家实行网络安全等级保护制度。

➢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。关键信息基础设施的具体范围和安全保护办法由国务院制定。

关键信息基础设施[illegible]
不低于第三[illegible]

➢第五十九条

➢网络运营者不履行本法[illegible]第二十五条规定的网络安全保护义务的，由[illegible]警告；拒不改正或者导致危害网络[illegible]以上十万元以下罚款；对直接负责的主管人员处[illegible]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；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款；对直接负责的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！

(等级保护由基本制度、基本国策，上升为法律)

《中华人民共和国网络安全法》--各地正在执法

事件3：汕

2017年
法检查时发
安全等级为
评。
该公司
法第二十一
法第五十九
发布于：
http://www
执法机构：
处罚行为：
处罚措施：
法律依据：

事件5：四

2017年
到位，导致
网安部门在
级保护的定
全保护义务
训与教育研
师培训与教
发布于：
http://news
执法机构：
处罚行为：
处罚措施：
法律依据：

事件7：山西忻

今年6月至7
网站信息安全，
国网络安全法》
度的要求，采取
施；第五十九条
务的，由有关主
已违反《网络安
现场执法检查，
发布于：
http://weibo.co
id=2309404133
执法机构：山西
处罚行为：未按
网络侵入等危害
处罚措施：警告
法律依据：《网

哈尔滨i

8月30日，哈
立的“方正农业社会
该网站隶属于方正
作落实不到位，未
危安全漏洞并被黑
根据《网络安
业技术推广中心立
络安全法》案件。
发布于：http:
执法机构：方
处罚行为：方
络安全等级保护制
入侵。
处罚措施：责
法律依据：《

国内首例高校违法案例诞生，因未落实等保制度致学生信息泄露

9月28日，淮南市网络与信息安全信息通报中心接到国家网络与信息安全信息通报中心通报：淮南职业技术学院系统存在高危漏洞，系统存储的4000余名学生身份信息已经造成泄露。经查，确认淮南职业技术学院招生信息管理系统存在越权漏洞，后台登录密码弱口令，学院未落实网络安全管理制度，未建立网络安全防护技术措施、网络日志留存少于六个月，未采取数据分类、重要数据备份和加密措施，致使系统存储的4353名学生的身份信息泄露。

10月12日,安徽省淮南市网警巡查执法官方微博发布通报称，关于淮南职业技术学院未落实网络安全等级保护制度，导致4000余名学生身份信息泄露一事，淮南市公安局网安支队依法对该学院处以立即整改和行政警告的处罚措施。

发布于：http://server.zzidc.com/a/cio/2017/1013/2126.html

执法机构：淮南市公安局网安支队

处罚行为：淮南职业技术学院招生信息管理系统存在越权漏洞，后台登录密码弱口令，未落实网络安全管理制度，未建立网络安全防护技术措施、网络日志留存少于六个月，未采取数据分类、重要数据备份和加密措施，致使系统存储的多名学生身份信息泄露。

处罚措施：责令整改，警告

法律依据：《网络安全法》第21条、第59条第1款。

等级保护2.0-标准名称及定级对象变化

《信息安全技术 信息系统安全等级保护基本要求》

上升到了网络空间安全层面

《信息安全技术 网络安全等级保护基本要求》

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。

名称与《网络安全法》保持一致！

等级保护2.0-内容及管理策略变化

- 定级
- 备案
- 建设整改
- 等级测评
- 监督检查

内容变化

- 五个规定动作
- **风险评估**
- **安全监测**
- **通报预警**
- **态势感知**
- ……

- 自主定级
- 自主保护
- 监督指导

策略变化

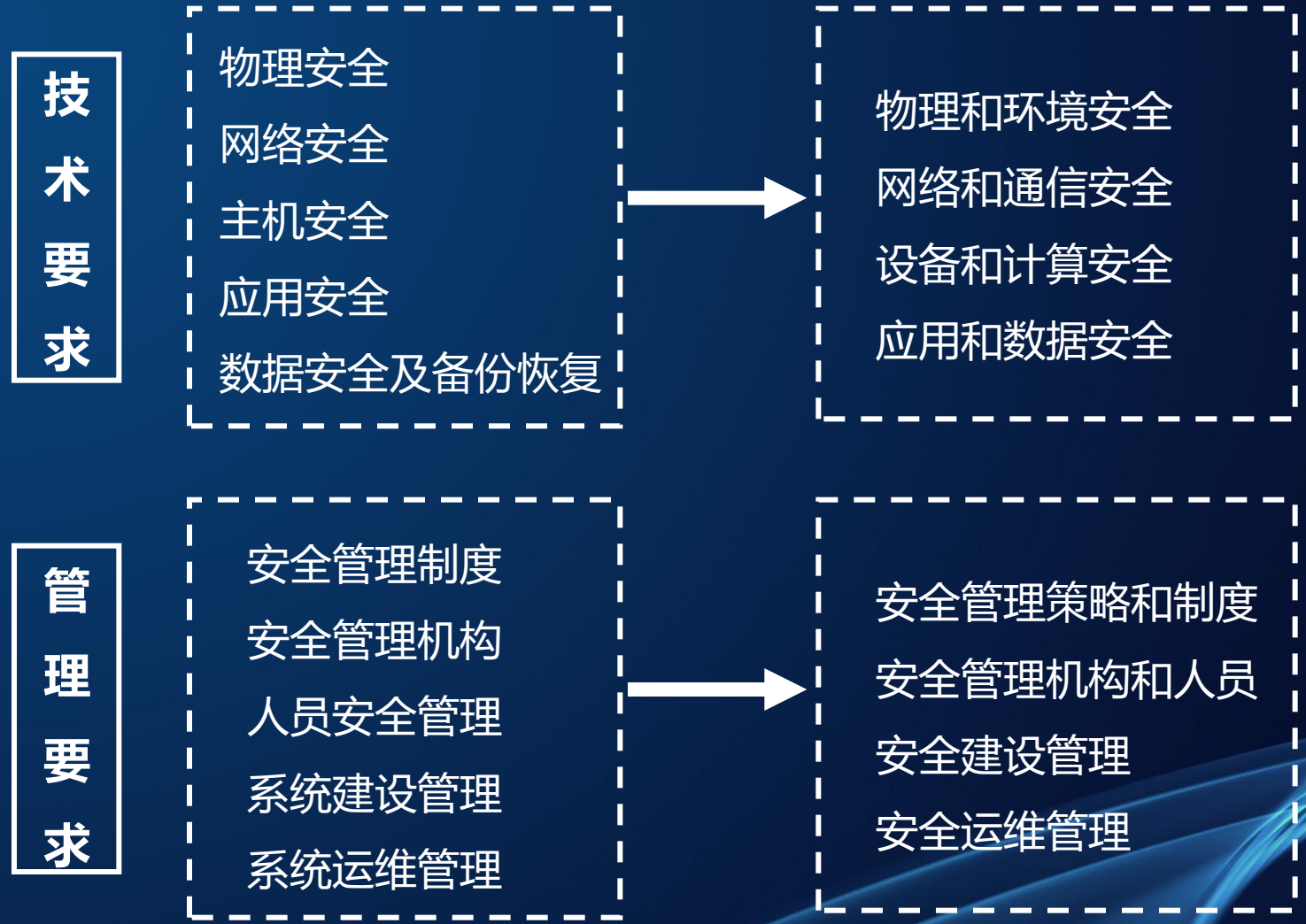
- **明确等级**
- **增强保护**
- **常态监督**

等级保护2.0-安全要求变化

安全要求 → **安全通用要求与安全扩展要求**

- 安全通用要求：针对共性化保护需求提出，等级保护对象无论以何种形式出现，必须根据安全保护等级实现相应级别的安全通用要求。
- 安全扩展要求：针对云计算、移动互联、物联网和工业控制个性化保护需求提出了特殊的技术要求，需要根据安全保护等级和使用的特定技术或特定的应用场景实现安全扩展要求。
- 安全通用要求和安全扩展要求共同构成了对等级保护对象的安全要求

等级保护2.0-控制措施变化



技术部分变化（1）应用层双向防御能力

控制措施	技术要求
网络和通信安全 网络架构	应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址； 应避免将重要网络区域部署在网络边界处且没有边界防护措施；
网络和通信安全 访问控制	应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级；
网络和通信安全 访问控制	应在关键网络节点处对进出网络的数据流实现基于应用协议和应用内容的访问控制（原来仅要求在关键网络节点处对进出网络的信息内容进行过滤，实现对内容的访问控制）；
网络和通信安全 入侵防范	应在关键网络节点处检测、防止或限制从内部和外部发起的网络攻击行为（原来仅要求单向防护）；
网络和通信安全 恶意代码防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新；

技术部分变化（2）威胁检测、分析与预警能力

控制措施	技术要求
网络和通信安全 入侵防范	应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析（新增）；
网络和通信安全 入侵防范	应在关键网络节点处检测、防止或限制从内部和外部发起的网络攻击行为（新增）；
网络和通信安全 恶意代码防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新（新增）；
网络和通信安全 集中管控	应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控（新增）；
网络和通信安全 集中管控	应能对网络中发生的各类安全事件进行识别、报警和分析（新增）；

技术部分变化（3）云计算、物联网、工控、移动互联等安全新技术

扩展要求	具体内容
云计算安全扩展要求	对云计算环境主要增加的内容包括“基础设施的位置”、“虚拟化安全保护”、“镜像和快照保护”、“云服务商选择”和“云计算环境管理”等方面。
物联网安全扩展要求	物联网环境主要增加的内容包括“感知节点的物理防护”、“感知节点设备安全”、“感知网关节点设备安全”、“感知节点的管理”和“数据融合处理”等方面
移动互联安全扩展要求	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。
工业控制系统安全扩展要求	工业控制系统主要增加的内容包括“室外控 制设备防护”、“工业控制系统网络架构安全”、“拨号使用 控制”、“无线使用控制”和“控制设备安全”等方面

管理部分变化：定期做风险评估、应急演练（强化）

控制措施	技术要求
安全管理机构和人员- 审核和检查	应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况； 应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等； 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。
安全运维管理- 漏洞和风险管理	应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。
安全运维管理- 应急预案管理	应规定统一的应急预案框架，具体包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容； 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练； 应定期对原有的应急预案重新评估，修订完善。

1 智慧校园建设趋势分析

2 等级保护标准演进

3 智慧校园下的等级保护建设

SANGFOR
深信服科技

智慧校园下的网络安全问题

问题一：资产上线、变动导致漏洞多，难以及时感知

- 高校安全管理工作和应用开发工作“两张皮“导致安全部门缺乏风险感知能力

- 学校级、院系级的业务系统升级、版本，更新迭代复杂

- 高校数据中心业务环境复杂、多样

现象:高校新增资产风险难以感知

导致：高校新增业务往往会产生大量漏洞

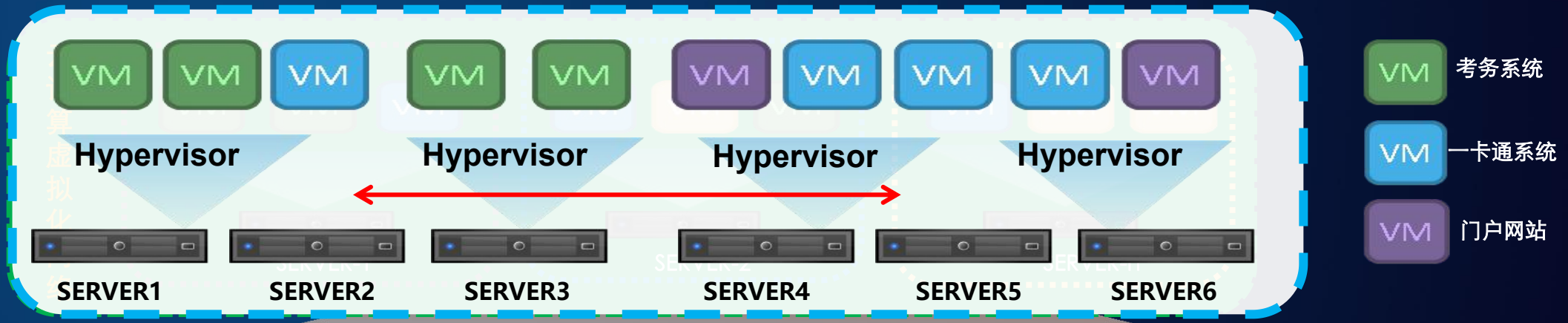
结果:如果不及时进行安全策略的加固，会造成漏洞暴露时间长、容易被利用及攻击

根据中国国家信息安全漏洞库（CNNVD）统计，截至2015年12月31日，CNNVD收录漏洞总量已高达80300个！全世界每年有大量的信息安全事件，就是因为新增资产漏洞更新不及时，被黑客利用造成的！

问题二：高校面临的信息安全监管压力增大

问题三：数据中心云化，物理边界消失了

新技术的运用使高校数据中心安全边界模糊



业务虚拟化后不同安全等级业务混合，边界消失

虚机之间通过Hypervisor调用通讯，流量不可视

一台主机失陷后，威胁横向扩散，影响其他主机

问题四：黑客突破边界接入校园内网，你都不知道？

攻击手段越来越多

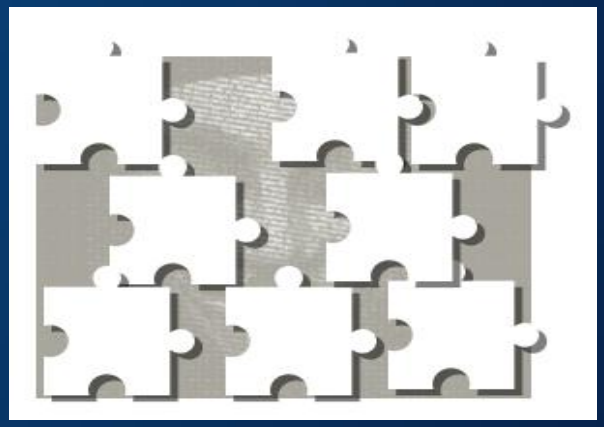
防御被轻易绕过

攻击者突破防线后难以被发现

等级保护1.0建设改进

堆叠设备，运维复杂

为满足合规性检查，盲目添加各种安全设备，安全状态情况不清晰，给运维带来巨大负担。



重防护，轻检测

安全设备上配置静态防御策略，对资产变化、攻击行为不能持续检测，表面安全的错觉。

本地防护，响应较差

本地防护措施能阻断大部分攻击，但对于紧急事件应变处置能力较差，导致资产、形象受损。

习主席4•19网信座谈会讲话

- **聪者听于无声，明者见于无形**

  维护网络安全，首先要知道风险在哪里，是什么样的风险，什么时候发生风险。

- **没有意识到风险是最大的风险**

  网络安全具有很强的隐蔽性，一个技术漏洞、安全风险可能隐藏几年都发现不了，结果是“谁进来了不知道、是敌是友不知道、干了什么不知道”。

- **网络安全是动态的，而不是静态的**

  网络安全的威胁来源和攻击手段不断变化，那种依靠装几个安全设备和安全软件就想永保安全的想法已不合时宜，需要树立动态、综合的防护理念。

等级保护建设思路

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

通过防御/检测/响应/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。

等保2.0时代合规的本质是安全建设的有效和简单。

定级对象安全保护环境

计算环境

区域边界

通信网络

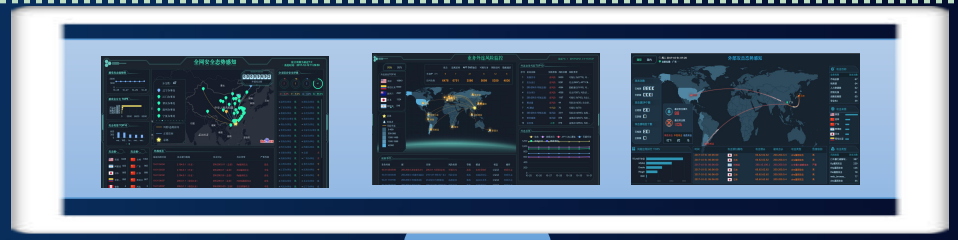
安全管理中心

定级对象互联

安全互联部件

跨定级对象安全管理中心

一个中心，三重防护保障合规



安全可视

预测

防御

自适应

响应

检测

协同防御

动态感知

本地协调云端联动

动态响应设备联动防御

企业安全大脑

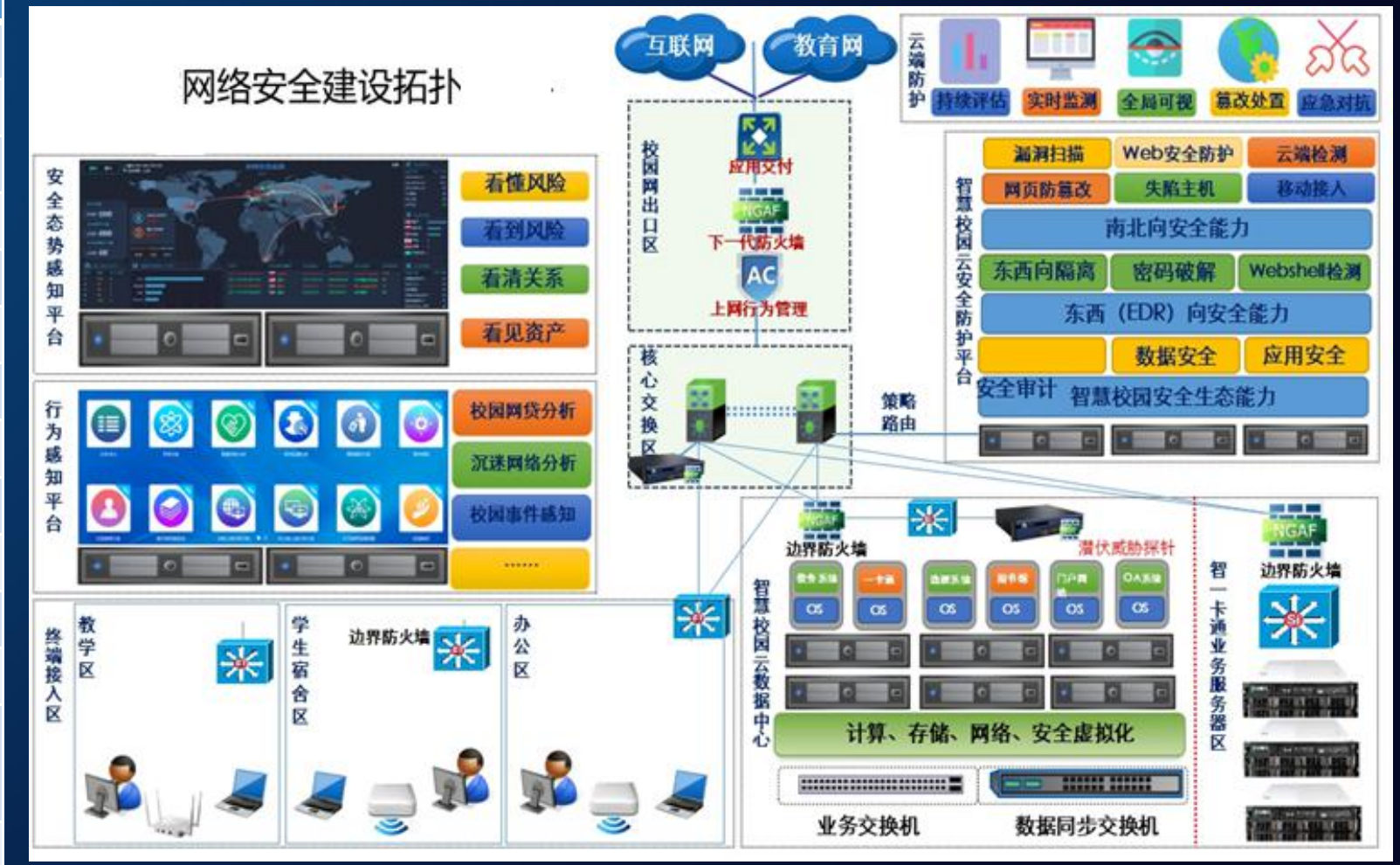
全网安全感知平台运营与情报中心

叠加三种能力，构建主动防御体系

等保2.0解决方案

序号	设备名称	
1	下一代防火墙	
2	上网行为管理系统	
3	应用交付（可选）	
4	VPN网关（SSL VPN、WOC、MIG等）	
5	等保一体机服务器（一体机硬件、管理平台）	
6	等保一体机组件	下一代防火墙
7		数据库审计系统
8		漏洞扫描系统
9		日志审计系统
10		运维审计系统
11		EDR系统服务端软件
12		EDR系统agent（部署在服务器上）
13	安全云服务	云端沙箱、云守、信服云眼、信服云眼、信服云镜、云端在线服务等
14	安全感知平台（SIS）	
15	潜伏威胁探针（STA）	
16	深信服敏捷安全服务（风险评估、渗透测试等）（可选）	

等级保护建设参考设备清单（可利旧）



安全可视辅助决策简化运维

全网安全态势可视 → 外部攻击可视 → 业务外连风险可视 → 业务脆弱性与风险可视

动态感知持续检测

清晰呈现业务视角 → 攻击检测并报警 → 攻击详情举证 → 攻击影响面分析

协同防御，多级联动

实时监测安全事件，3-5分钟内生成可视化报告，并告知用户

实时爬取站点资源

人工智能+安全专家

网页篡改监测
- 一级页面，每分钟一次
- 二级页面，30分钟一次
- 人工审核，确保零误报

0Day监测
- 24小时内，触发式检测

网马监测
- 每天一次

黑链监测
- 域名首页，每分钟一次

DNS监测
- 每15分钟一次

可用性监测
- 模拟访问，每分钟一次

微信预警

分钟级可视告警

等保一体机解决方案

合规仅仅是基础，等保建设需要一套**实用有效**的**一站式**解决方案！

防火墙　VPN　WAF　运维审计　漏洞扫描　数据库审计

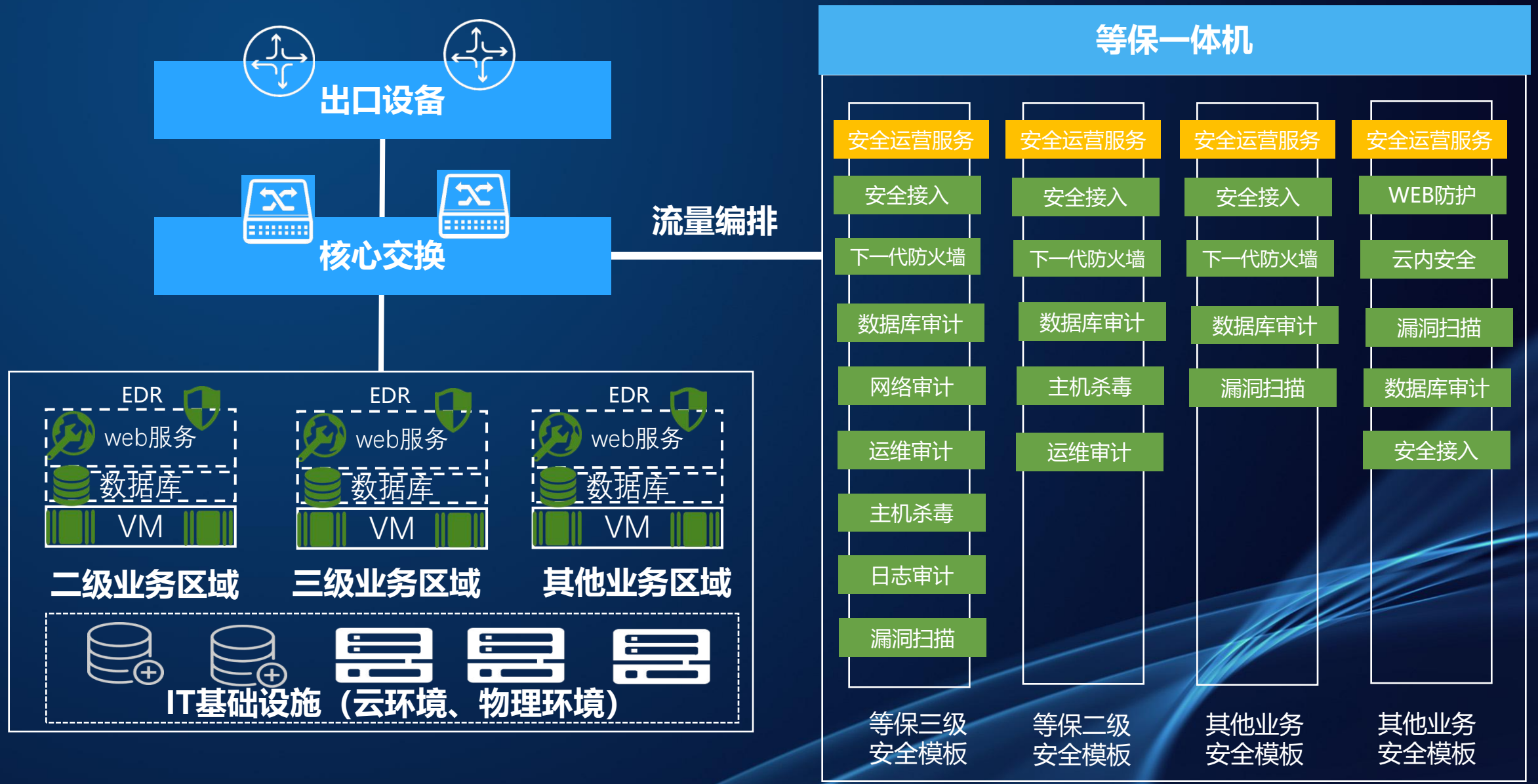
日志审计　配置核查　风险监测　端点安全

ALL IN 等级保护一体机

协同防御，多级联动

- **一键阻断：**自动阻断木马与黑客通信
- **用户提醒：**安全事件用户端告警

等保一体机方案架构


出口设备
核心交换
流量编排
EDR
web服务
数据库
VM
二级业务区域
三级业务区域
其他业务区域
IT基础设施（云环境、物理环境）
等保一体机
安全运营服务
安全接入
下一代防火墙
数据库审计
网络审计
运维审计
主机杀毒
日志审计
漏洞扫描
主机杀毒
运维审计
WEB防护
云内安全
漏洞扫描
数据库审计
安全接入
等保三级
安全模板
等保二级
安全模板
其他业务
安全模板
其他业务
安全模板

方案优势

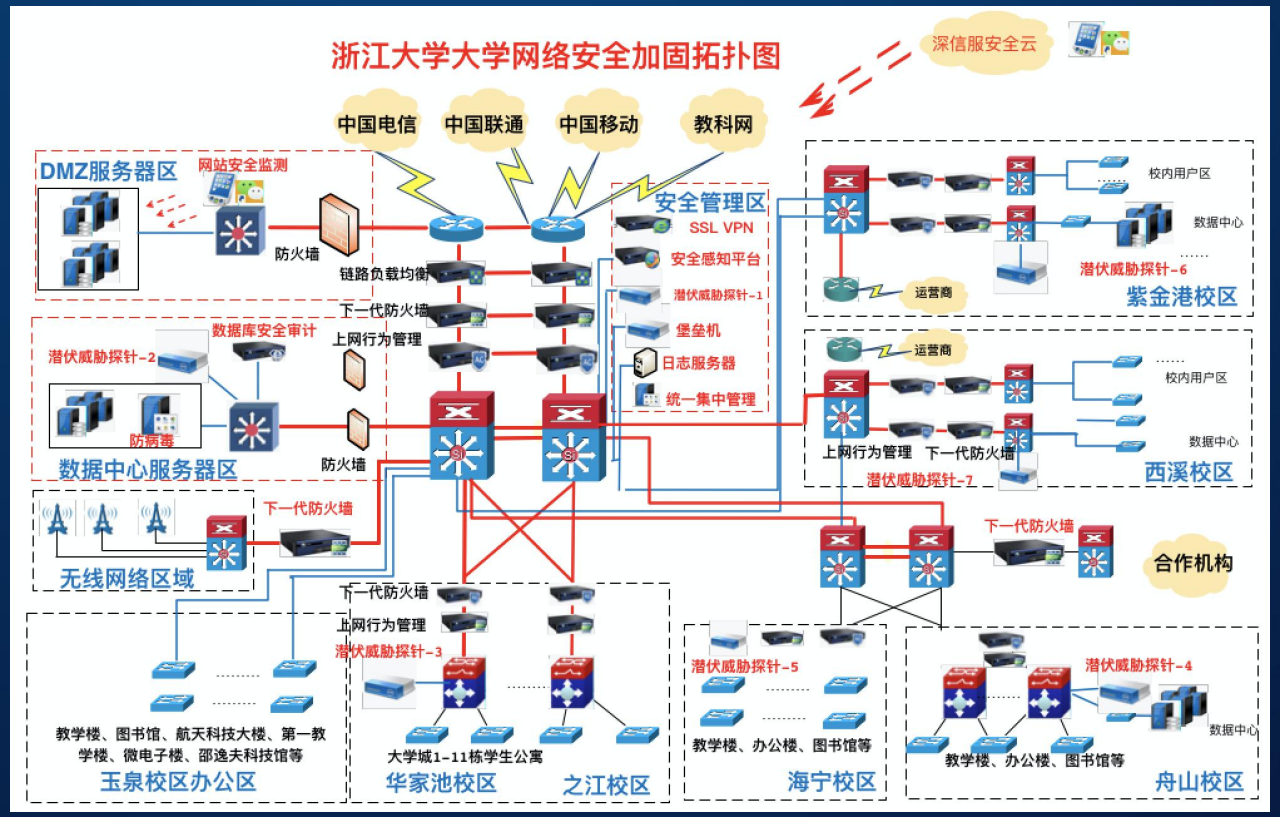
一体化交付，提供一站式的快速安全合规能力。

基于场景的交付，实现安全设备的统一高效管理

统一安全服务，实现安全持续闭环

基于软件定义的安全架构，弹性扩展随需而变

浙江大学等级保护建设项目



- **等级保护标准安全管理体系：**网络划分为不同的安全域，实现安全域风险内控隔离，有效避免风险不同区域间扩散，云平台环境下等保2.0趋势。
- **系统按照重要程度区别保护：**针对数据中心区域，需要部署功能强大，针对性强的数据中心应用防火墙，针对应用系统层的安全防御。普通系统和终端区则通过传统防御手段。区域划分，服务细化。
- **综合运维管理：**针对网络安全的管理提供多种手段，包括数据库审计、运维堡垒机、日志审计系统、云安全（虚拟化）。
- **校园网安全态势感知和校园大数据：**引入最新的技术，通过大数据和网络威胁情报系统预警校园网潜在风险，出现安全事件第一时间告知，降低安全事件产生的危害。

THANKS!