Ruijie 锐捷 Networks

企业信息安全解决方案 V2.0

看得见的安全 ● 信得过的网络

企业行业部

2022/6/30

1

Contents

为什么要实行等级保护

《网络安全法》第21条、第31条明确规定了网络运营者和关键信息基础设施运营者都应该按等级保护要求对系统进行安全保护，以法律的形式确定等级保护工作为国家网络安全的基本国策，并在法律层面确立了其在网络安全领域的基础、核心地位。

- 网络安全法的要求
- 是信息安全工作的基本制度、基本国策，是国家意志的体现
- 有利于在信息化建设过程中同步建设信息安全设施，保障信息安全与信息化建设相协调

等级保护政策演进

1994年国务院颁布《中华人民共和国计算机信息系统安全保护条例》

首次提出计算机信息系统必须实行安全等级保护。

2003年9月中办国办颁发《关于加强信息安全保障工作的意见》（中办发[2003]27号）

明确做等级保护

2004年11月四部委会签《关于信息安全等级保护工作的实施意见》（公通[2004]66号）

定义了五个保护级别、监管方式、职责分工和时间计划

2007年 四部委会签公通字[2007]43号文件《信息安全等级保护管理办法》

明确了等级保护的具体操作办法和各部委的职责，以及推进等级保护的具体事宜

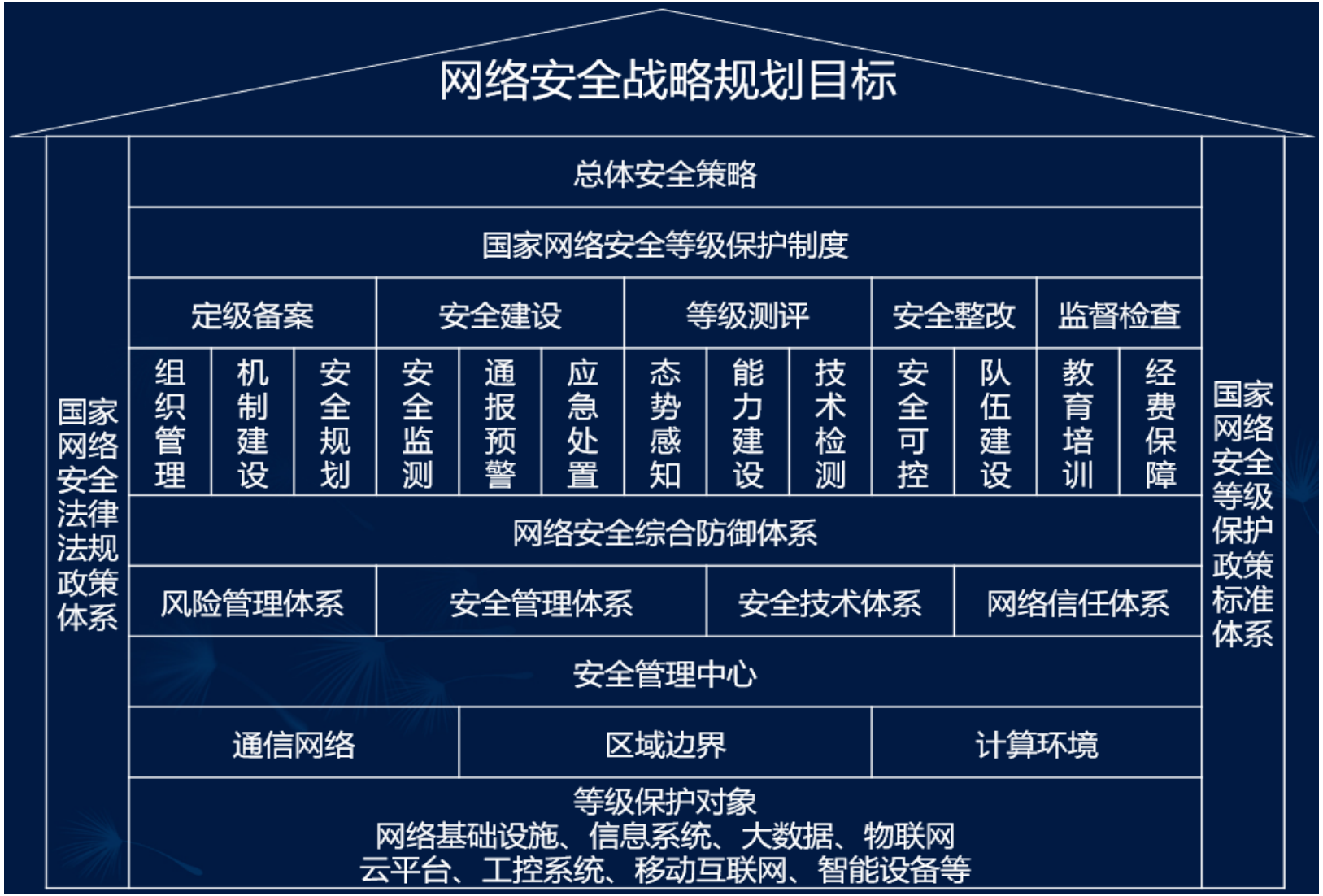
2007年7月16日 四部门会签公信安[2007]861号文件：四部门下发《关于开展全国重要信息系统安全等级保护定级工作的通知》

开始了等级保护的实质性工作的第一阶段

《GBT 22239-2008 信息安全技术 信息系统安全等级保护基本要求》
《GBT 25070-2010 信息安全技术 信息系统等级保护安全设计技术要求》
《GBT 28448-2012 信息安全技术 信息系统安全等级保护测评要求》
……
等保1.0时代

等级保护2.0

等级保护安全框架

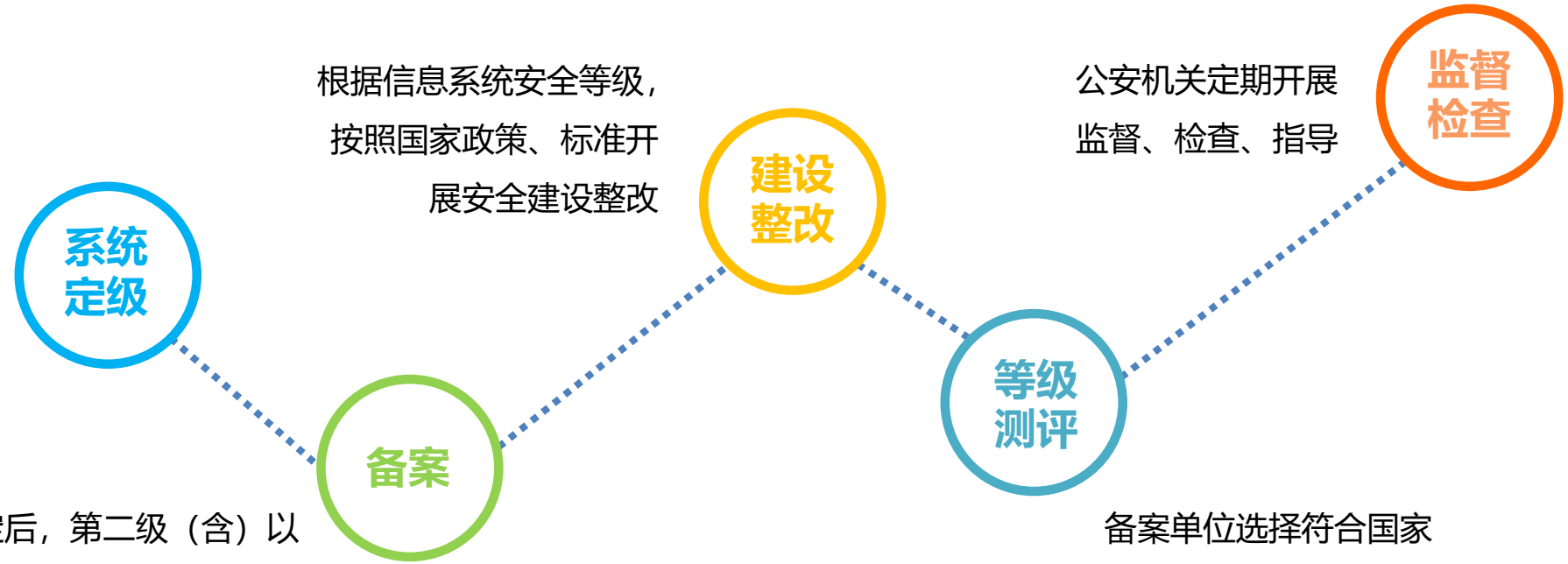


在开展网络安全等级保护工作中应首先明确等级保护对象，等级保护对象包括基础网络设施、信息系统、云平台、大数据平台、物联网、工业控制系统等。

确定了等级保护对象的安全保护等级后，应根据不同对象的安全保护等级完成安全建设或安全整改工作；应针对等级保护对象特点建立安全技术体系和安全管理体系，构建具备相应等级安全保护能力的网络安全综合防御体系。

应依据国家网络安全等级保护政策和标准，开展组织管理、机制建设、安全规划、通报预警、应急处置、态势感知、能力建设、监督检查、技术检测、队伍建设、教育培训和经费保障等工作。

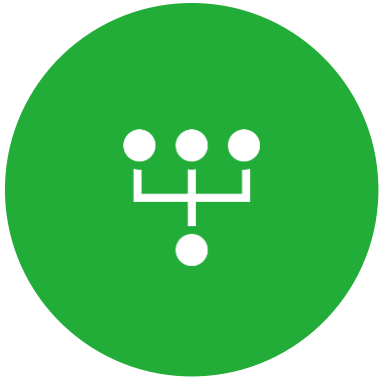
等级保护实施过程


将网络系统按照重要性和遭受损坏后的危害性分成五个安全保护等级
系统定级
等级确定后，第二级（含）以上信息系统到公安机关备案，公安机关审核后颁发备案证明
备案
根据信息系统安全等级，按照国家政策、标准开展安全建设整改
建设整改
备案单位选择符合国家规定条件的测评机构开展等级测评
等级测评
公安机关定期开展监督、检查、指导
监督检查

等级2.0关键变化

对象变化

“信息安全”→“网络安全”
引入移动互联、工控、物联网等新领域



结构调整

一个中心，三重防御

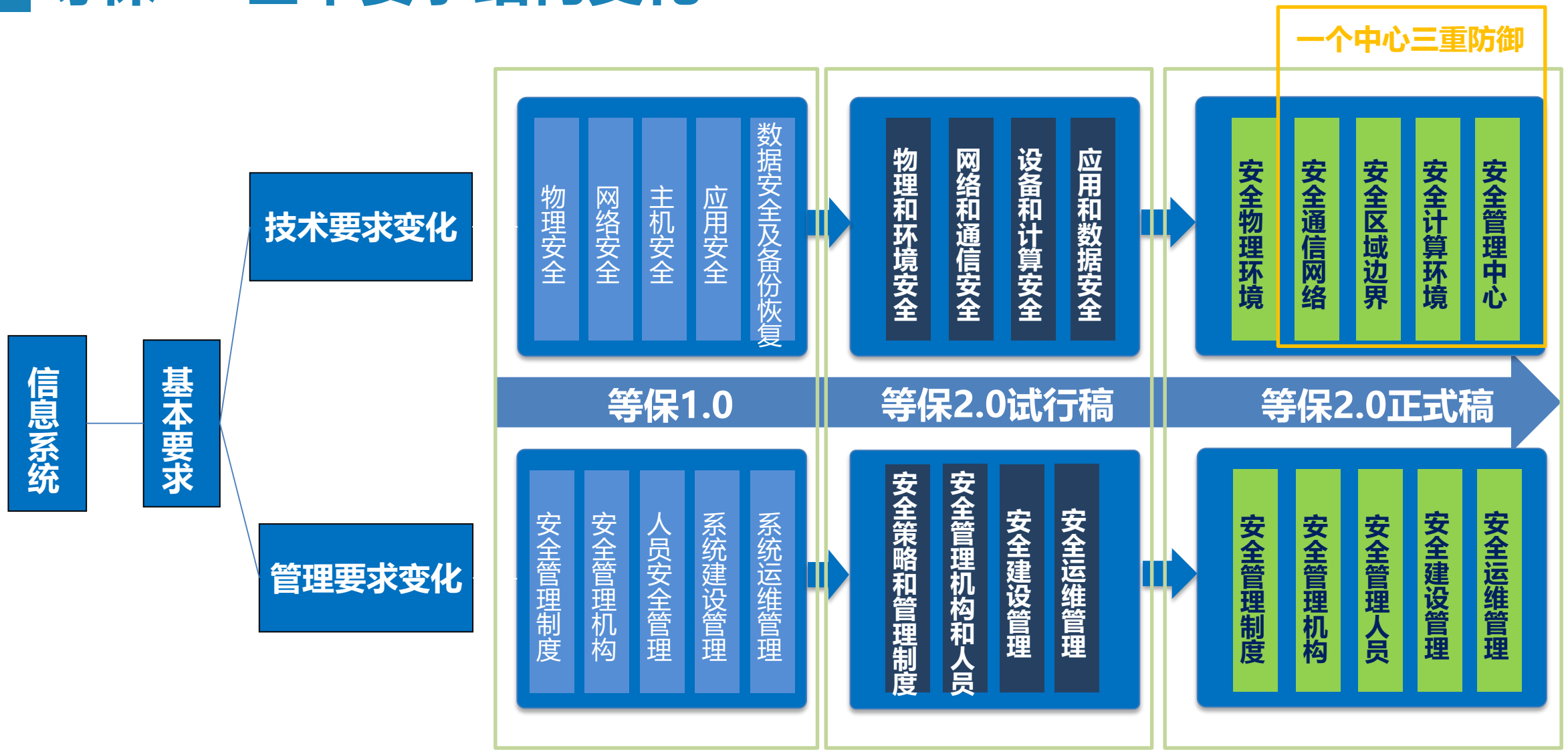
防御理念

被动防御→主动防御

“等级保护由1.0到2.0是**被动防御**变成**主动防御**的变化，依照等级保护制度可以做到整体防御、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。”

——中国工程院院士 沈昌祥

等保2.0基本要求结构变化



等保2.0第三级安全要求结构

安全通用要求	云计算安全扩展要求	移动互联安全扩展要求	物联网安全扩展要求	工业控制系统安全扩展要求
• 安全物理环境	• 安全物理环境	• 安全物理环境	• 安全物理环境	• 安全物理环境
• 安全通信网络	• 安全通信网络	• 安全区域边界	• 安全区域边界	• 安全通信网络
• 安全区域边界	• 安全区域边界	• 安全计算环境	• 安全计算环境	• 安全区域边界
• 安全计算环境	• 安全计算环境	• 安全建设管理	• 安全运维管理	• 安全计算环境
• 安全管理中心	• 安全管理中心	• 安全运维管理		• 安全建设管理
• 安全管理制度	• 安全建设管理			
• 安全管理机构	• 安全运维管理			
• 安全管理人员				
• 安全建设管理				
• 安全运维管理				

不管等级保护对象形态如何都必须满足安全通用要求。如果等保对象是云计算、移动互联、物联网和工业控制系统，则在满足安全通用要求的基础上还需满足安全扩展要求

2

Contents

等保2.0解读

智能制造下的企业信息安全现状

锐捷企业信息安全解决方案

锐捷企业安全典型案例

中大企业客户在安全方面的需求

■ 生产线病毒攻击问题

常见病毒接入：
1、USB接入；
2、IT&OT融合后带来的外部攻击。

生产线的终端、工控机的系统程序非常固定，几乎不能升级系统，安装非PLC相关的系统。
主系统一般为老旧的Windows系统。

自动化产线控制器

MES终端

工控机主机

典型安全事件

1. XX轴承企业，因互联网接入生产线，导致工控机中勒索病毒，直接经济损失0.5亿元，生产中断15天。【处理方法，断网、查毒、交钱还原系统 】
2. XX电子企业，因员工不慎将带病毒的U盘定入工控机，导致整个工业网中病毒，仅排查杀毒花了13天，经济损失巨大；【处理方法：断网、查毒、杀毒】
3. ……

中大企业客户在安全方面的需求

■ 研发场景信息安全问题

1、研发人员：USB、外部访问中病毒（勒索病毒、永恒之蓝等）

2、办公人员：误带入有病毒电脑入网，感染整个研发网络。

3、外部黑客：黑客攻击研发系统漏洞，通过勒索病毒攻击或者直接窃取核心机密。

4、网络感染：企业研发网安全不足，导致各种病毒、攻击可随意进入网络，并感染主机。

典型安全事件
XX电子信息企业，因某研发电脑中永恒之蓝病毒，而快速扩散，导致研发瘫痪一周，损失过千万；
XX电子企业，办公中勒索病毒，影响研发网，要求其每天交2万美元方为其解毒；
XX机械设计企业，受黑客攻击，设计图纸被盗取，导致新产品无法上市，损失不可估量；
……

中大企业客户在安全方面的需求

■ 企业办公场景信息安全问题

1、办公电脑中网络病毒：通过办公电脑上网、下载、浏览等方式中病毒，并感染整个办公网。

2、数据中心中病毒：因办公感染导致数据中心中病毒；因服务器对外访问，导致数据中心中病毒，从而影响内部办公、外网访问等业务。

典型安全事件

1. XX药企因办公网安全防御不到位，导致整个办公网中病毒，直接办公正常开展；
2. XX钢铁企业，办公网中勒索病毒，导致快速蔓延，企业办公无法正常进行
3. .....

中大企业客户在安全方面的需求

■ 政策类合规需求

关注 | 国资委：将网络安全纳入央企负责人经营业绩考核

中国信息安全

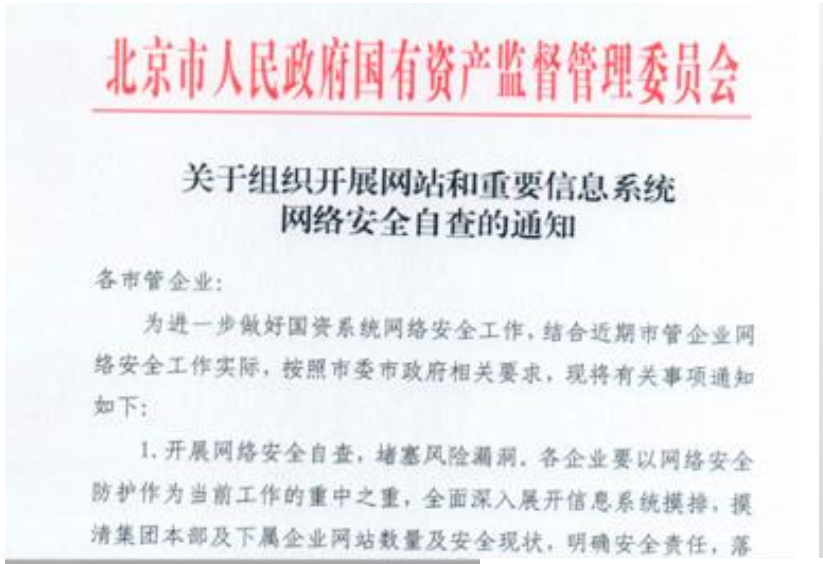
近日，国务院国资委修订印发了《中央企业负责人经营业绩考核办法》，办法多角度构建中央企业负责人年度与任期相结合的高质量发展考核指标体系，突出分类与差异化考核，强化国际对标、行业对标。

值得关注的是，办法首次将网络安全事件纳入考核范围，并视情节给予负责人相应的处分。这必将是促进我国网安事业发展的又一股力量，提高央企防范重大网络安全事件的能力和水平，保护国有资产不受侵害。

中央企业负责人经营业绩考核办法

第一章 总则

第一条 坚持以习近平新时代中国特色社会主义思想为指导，全面贯彻党的十九大精神和党中央、国务院关于深化国有企业改革，完善国有资产管理体制的一系列重大决策部署，切实履行企业国有资产出资人职责，维护所有者权益，落实国有资产保值增值责任，建立健全有效的激励约束机制，引导中央企业实现高质量发展，加快成为具有全球竞争力的世界一流企业，根据《中华人民共和国公司法》《中华人民共和国企业国有资产法》《企业国有资产监督管理暂行条例》等有关法律法规和《中共中央 国务院关于深化国有企业改革的指导意见》（中发〔2015〕22号）以及深化中央管理企业负责人薪酬制度改革等有关规定，制定本办法。



北京市人民政府国有资产监督管理委员会

关于组织开展网站和重要信息系统网络安全自查的通知

各市管企业：

为进一步做好国资系统网络安全工作，结合近期市管企业网络安全工作实际，按照市委市政府相关要求，现将有关事项通知如下：

1. 开展网络安全自查，堵塞风险漏洞。各企业要以网络安全防护作为当前工作的重中之重，全面深入展开信息系统摸排，摸清集团本部及下属企业网站数量及安全现状，明确安全责任，落

国家烟草专卖局文件

国烟办〔2014〕370号

国家烟草专卖局关于印发烟草行业信息化发展规划（2014—2020年）的通知

行业各直属单位，国家局、总公司机关各部门、各单位：

现将《烟草行业信息化发展规划（2014—2020年）》（以下简称规划）印发给你们，请认真贯彻执行。

各单位要深刻领会规划精神，准确把握以“一号工程”为基础，以“三流合一”为目标，以“一个平台、五大应用、五大保障”为基本框架，整合兼容、互联互通、共建共用、改造升级、推进一体化数字烟草建设的总体发展思路，要紧密结合实际情

设，切实抓好企业“十二五”信息化规划“回头看”工作，扎实推进各项工作落实。要系统思考谋划企业“十三五”信息化规划工作，既要满足行业管控要求，又要兼顾企业现实需求；既要注重技术先进性，又要处理好技术、业务与管理的融合互动关系；既要有效推进企业信息化重点项目建设，又要充分考虑并落实行业信息化重大工程建设要求，加快实现集成整合、协同共享，推进信息化与烟草产业的深度融合。

国家烟草专卖局

2014年11月13日

（不公开）

中华人民共和国工业和信息化部

Ministry of Industry and Information Technology of the People's Republic of China

工业和信息化部 新闻动态 信息公开 在线办事 公众参与 专题专栏

首页 > 工业和信息化部 > 机关司局 > 网络安全管理局 > 工作动态 > 正文

工业和信息化部关于《关于加强工业互联网安全工作的指导意见（征求意见稿）》公开征求意见的公告

发布时间：2019-04-15 来源：网络安全管理局

为贯彻落实《国务院关于深化“互联网+先进制造业”发展工业互联网的指导意见》，加快构建工业互联网安全保障体系，经广泛征求意见，反复研究修改，工业和信息化部会同有关部门起草了《关于加强工业互联网安全工作的指导意见（征求意见稿）》。为保障公众知情权和参与权，凝聚各界共识和智慧，现向社会公开征求意见。有关意见或建议请于2019年4月30日前通过电子邮件方式发送至(ayhlw409@163.com)，或传真至(010-68206187)。

附件：

关于加强工业互联网安全工作的指导意见

福建省烟草专卖局文

闽烟办〔2018〕50号

福建省烟草专卖局关于印发福建烟草商业系统网络安全建设技术规范及建设指导意见的通知

各设区市局（公司），进出口公司，海晟投资公司，各烟叶复烤企业：

现将《福建烟草商业系统网络安全建设技术规范》及《福建烟草商业系统网络安全建设指导意见（2019—2021年）》，印发给你们，请各单位遵照执行。

福建省烟草专卖局

2018年12月28日

（主动公开）

— 1 —

中大企业客户在安全方面的需求

企业信息安全问题分类

病毒攻击类

① 勒索病毒、永恒之蓝病毒等，瘫痪生产、研发网络及电脑；
② U盘病毒，影响生产、办公、研发体系；
③ 外部直接进行系统漏洞攻击、病毒攻击。
④ 网站安全，导致业务受损。

权限攻击类

① 生产、研发、办公网络权限不清晰，相互感染；
② 企业员工权限不清晰，导致文件、资料、信息泄密；

3

Contents

等保2.0解读

智能制造下的企业信息安全现状

锐捷企业信息安全解决方案

锐捷企业安全典型案例

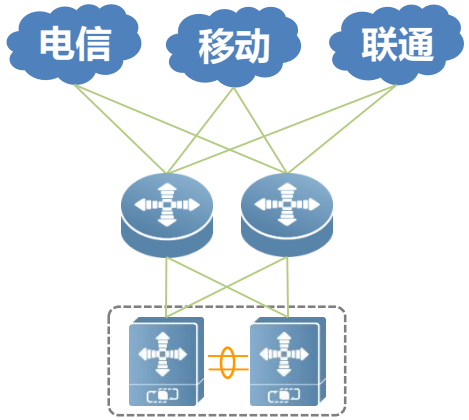
中大企业客户信息安全整体解决思路框架

等保2.0建设方案指导思想

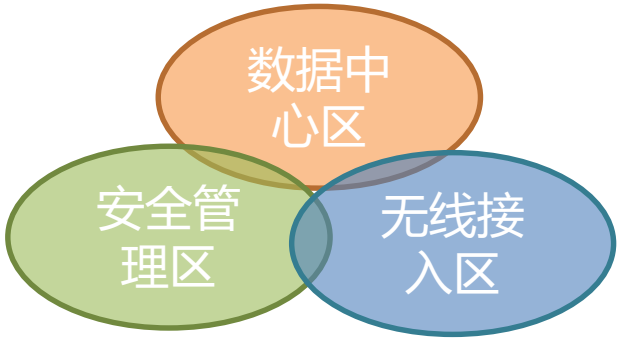
安全通信网络：建设要点（三级）

等保要求	控制点	对应产品或方案
安全通信网络	网络架构	防火墙、路由器、交换机、网络规划与配置优化、关键设备/链路/服务器冗余
	通信传输	VPN
	可信验证	可信计算机制

除红字部分外锐捷均可提供



主干网络链路及设备均采用冗余部署



基于业务管理和安全需求划分出有明确边界的网络区域

采用VPN或HTTPS等加密手段保护业务应用

安全区域边界：建设要点（三级）

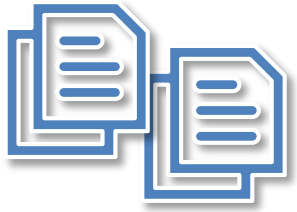
等保要求	控制点	对应产品或方案
安全区域边界	边界防护	防火墙、身份认证与准入系统、无线控制器
	访问控制	第二代防火墙、WEB应用防火墙、行为管理系统
	入侵防范	入侵检测与防御、未知威胁防御、日志管理系统
	恶意代码和垃圾邮件防范	防病毒网关、垃圾邮件网关，或 第二代防火墙
	安全审计	行为审计系统、身份认证与准入系统、日志管理系统
	可信验证	可信计算机制

除红字部分外锐捷均可提供

区域边界部署必要的应用层安全设备，并启用安全过滤策略

建立基于用户的身份认证与准入机制，启用安全审计策略

采用行为模型分析等技术防御新型未知威胁攻击



采集并留存不少于半年的关键网络、安全及服务器设备日志

安全计算环境：建设要点（三级）

等保要求	控制点	对应产品或方案
安全计算环境	身份鉴别	身份认证与准入系统、堡垒机、安全加固服务
	访问控制	身份认证与准入系统、安全加固服务
	安全审计	堡垒机、数据库审计、日志管理系统
	入侵防范	入侵检测防御、未知威胁防御、日志管理系统、渗透测试/漏洞扫描/安全加固服务
	恶意代码防范	杀毒软件、沙箱
	可信验证	可信计算机制
	数据完整性	VPN、防篡改系统
	数据保密性	VPN、SSL等应用层加密机制
	数据备份恢复	本地数据备份与恢复、异地数据备份、重要数据系统热备
	剩余信息保护	敏感信息清除
	个人信息保护	个人信息保护

除红字部分外
锐捷均可提供

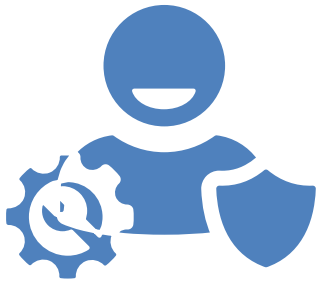
安全管理中心：建设要点（三级）

等保要求	控制点	对应产品
安全管理中心	系统管理	堡垒机
	审计管理	堡垒机
	安全管理	堡垒机
	集中管控	VPN、IT运维管理系统、安全态势感知平台、日志管理系统
安全建设管理	测试验收	上线前安全检测服务
安全运维管理	漏洞和风险管理	渗透测试服务、漏洞扫描服务

除红色字体部分外锐捷均可提供

系统管理员、审计管理员、安全管理员权责清晰，三权分立

设置独立安全管理区，采集全网安全信息，实施分析预警管理



借力专业安服人员，提供渗透测试等高技术要求安全服务

等保2.0技术条例推荐配置方案

序号	等保所需产品与服务	必备/可选(等保二级)	必备/可选(等保三级)	对应锐捷产品或服务名称
1	防火墙	必备	必备	RG-WALL
2	入侵防御	必备	必备	RG-IDP或防火墙开启IPS功能
3	日志审计与集中管理	必备	必备	RG-BDS
4	渗透测试服务	可选	必备	渗透测试服务
5	漏洞扫描服务	必备	必备	漏洞扫描服务或RG-SCAN
6	堡垒机	必备	必备	RG-OAS
7	上网行为管理	必备	必备	RG-UAC
8	WAF应用防火墙	可选	必备	RG-WG
9	终端准入系统	可选	必备	SAM或SMP系列
10	双因素认证	可选	可选	SourceID
11	数据库审计	可选	必备	RG-DBS
12	等级保护建设咨询	可选	可选	等级保护建设咨询服务
13	安全事件处置服务	可选	可选	安全事件处置服务
14	网站防篡改	可选	必备	RG-Wlock
15	机房运维管理软件	可选	可选	RIIL
16	新型攻击防御	可选	可选	RG-DDP、RG-APT
17	网络版杀毒软件	必备	必备	火绒终端安全（战略合作）
18	数据存储备份	必备	必备	第三方产品

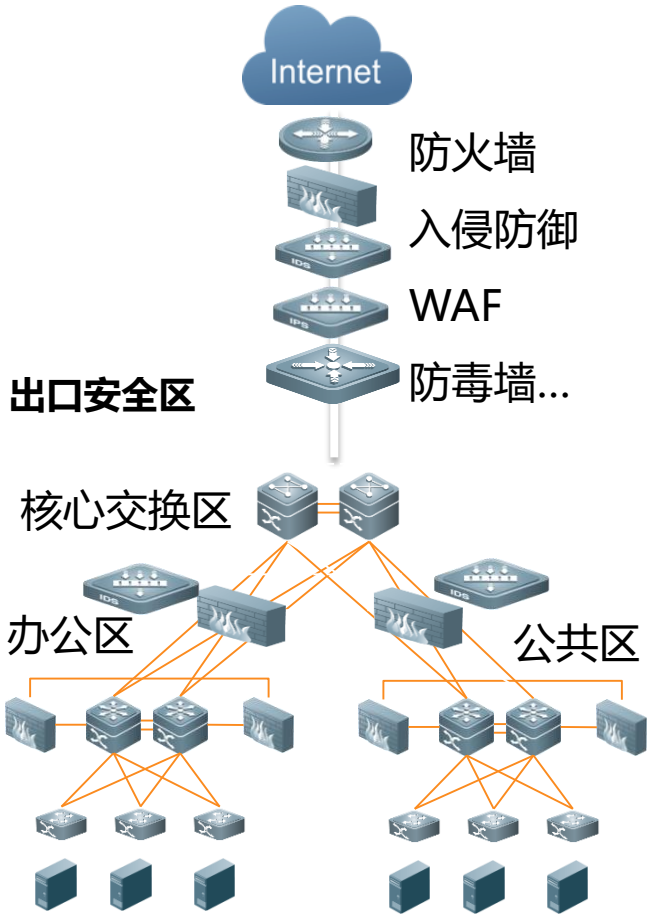
安全通信网络：建设难点和困惑

等保2.0规范关键要求

- 应保证网络设备的业务处理能力满足业务高峰期需要
- 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段
- 应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性

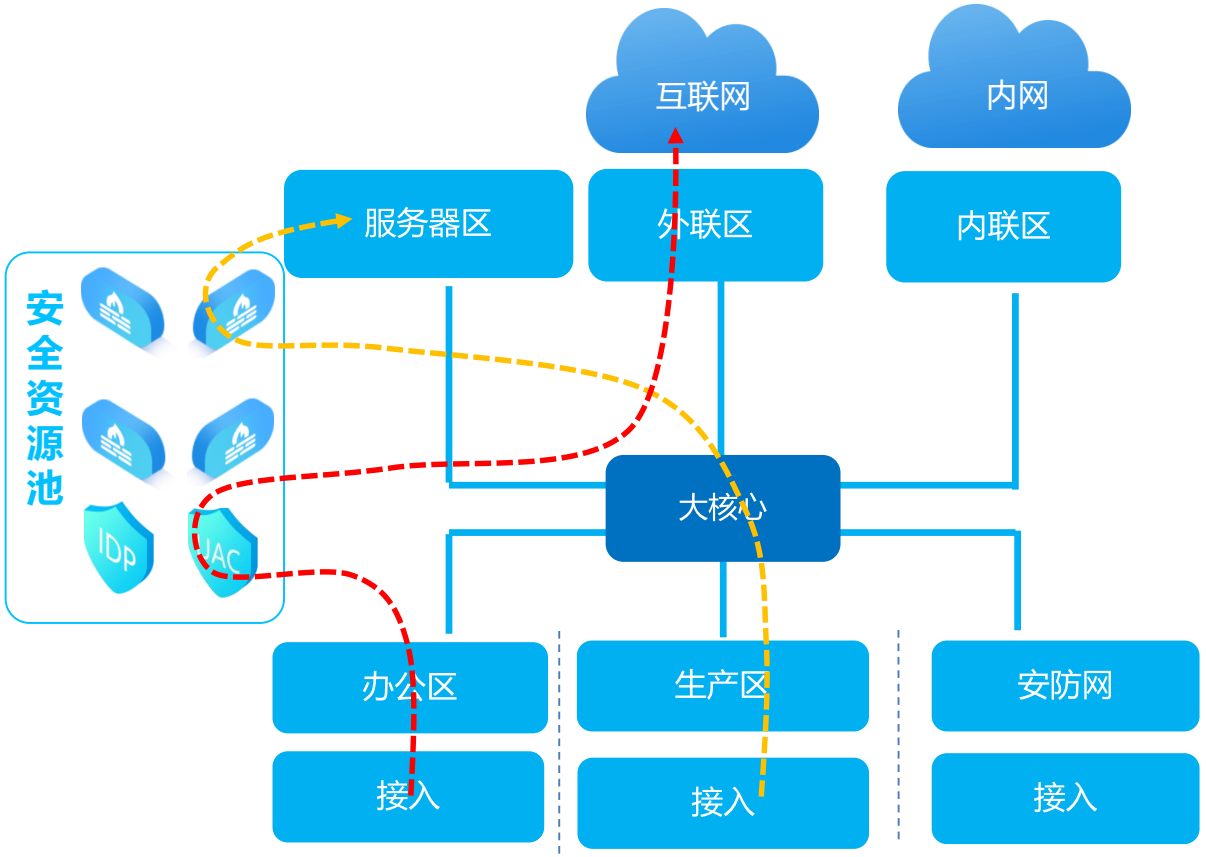
用户困惑

- 边界串接大量设备，带来极大单点故障风险，并且也因木桶效应造成性能瓶颈
- 多个不同区域边界需要重复部署设备实施安全隔离，建设成本高，利用率低
- 已有设备无法充分利用，无法实现跨厂商设备负载均衡



传统安全边界部署方案

安全通信网络：锐捷方案特色



基于SDN技术的ServiceChain，实现安全资源池化，灵活部署

- 区域边界无需直接部署物理设备，实现逻辑隔离，提高安全设备复用率
- 基于不同业务需求，灵活设计流量路径，分配给适当的安全设备
- 可进行跨厂商的安全设备冗余部署，实现负载均衡，充分满足性能需求
- 改变出口“糖葫芦串”部署模式，不再存在单点故障风险

安全区域边界：建设难点和困惑-1

等保2.0规范关键要求

- 应能够对非授权设备私自联到内部网络的行为进行检查或限制
- 应能够对内部用户非授权联到外部网络的行为进行检查或限制
- 应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络

用户困惑

- 无线网、物联网普及带来大量新增终端设备，难以准确定位用户位置和身份，且无法对物联网哑终端设备实施有效的认证准入管理
- 无线网络环境缺少针对性的安全管理手段
- 无法基于用户身份进行访问授权
- 传统准入认证手段大多只能进行简单的身份认证，难以实施对终端合法性的验证和管控

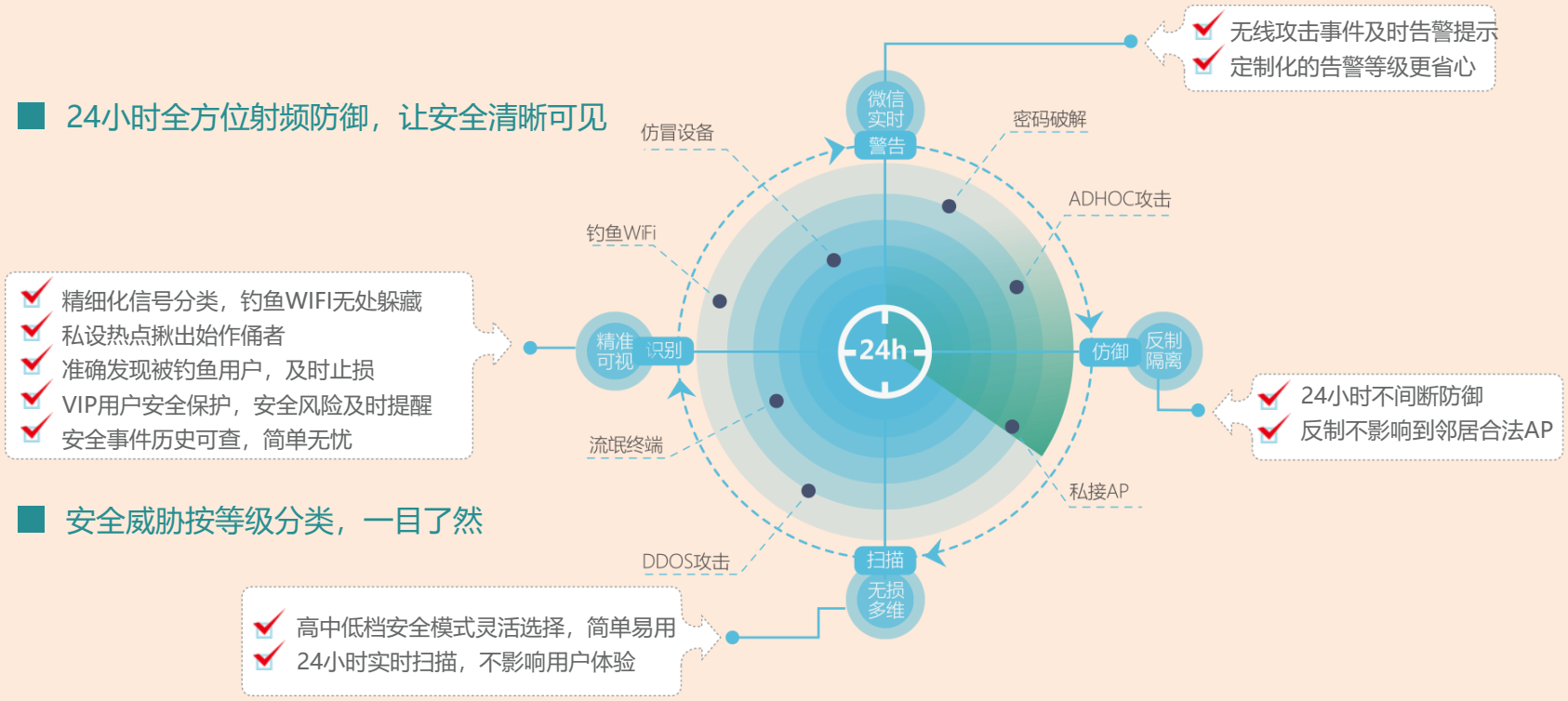
安全区域边界：锐捷方案特色-1

覆盖全网有线、无线、物联网终端的准入认证机制

- **智能发现全网终端设备**
- **安全事件与实名用户身份关联**
- **终端无感知实名认证**
- **不合规终端自动隔离**
- **基于用户身份的访问权限控制**

安全区域边界：锐捷方案特色-1

■ 24小时全方位射频防御，让安全清晰可见



- 无线攻击事件及时告警提示
- 定制化的告警等级更省心

- 精细化信号分类，钓鱼WIFI无处躲藏
- 私设热点揪出始作俑者
- 准确发现被钓鱼用户，及时止损
- VIP用户安全保护，安全风险及时提醒
- 安全事件历史可查，简单无忧

- 24小时不间断防御
- 反制不影响到邻居合法AP

■ 安全威胁按等级分类，一目了然

- 高中低档安全模式灵活选择，简单易用
- 24小时实时扫描，不影响用户体验

借助锐捷在无线领域丰富的技术积累，无线安全也全面融合进入整网安全体系，帮助用户实现无线接入安全

安全区域边界：建设难点和困惑-2

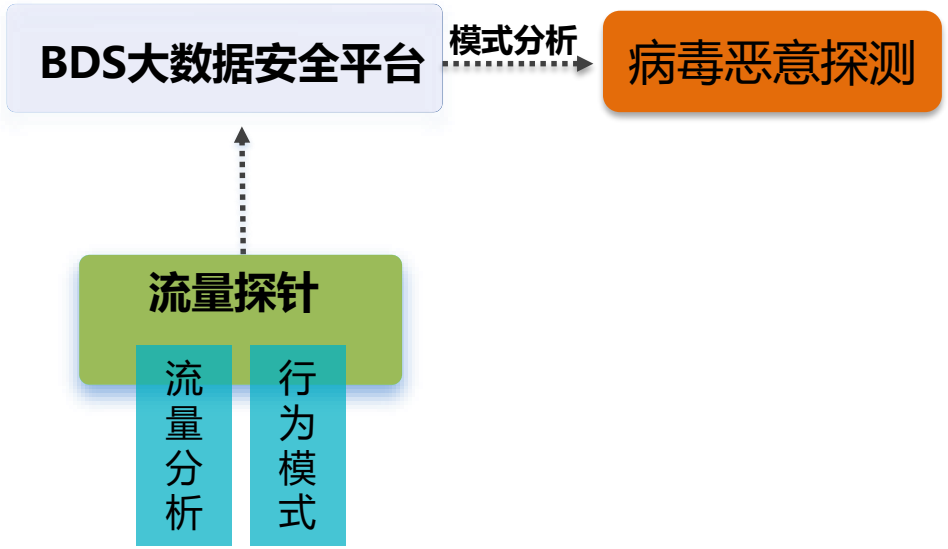
等保2.0规范关键要求

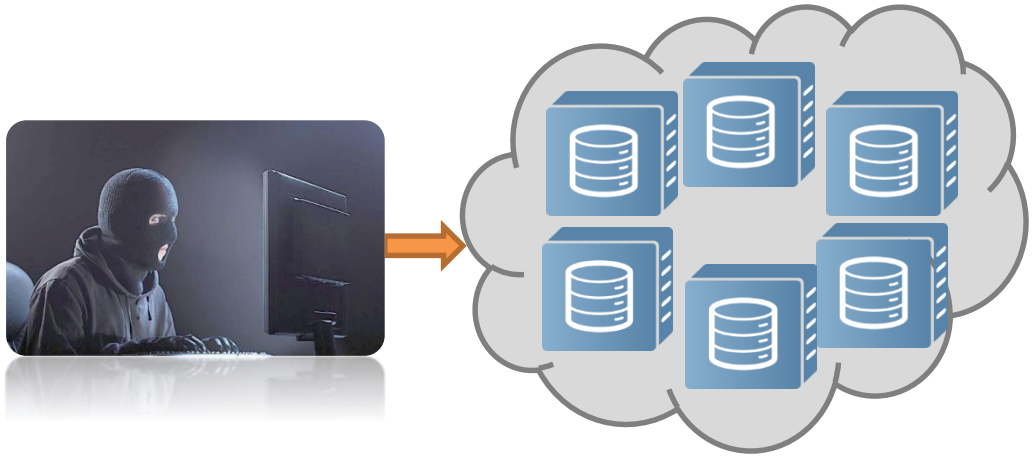
- 应在关键网络节点处检测、防止或限制从内部/外部发起的网络攻击行为。
- 应采取技术措施对网络攻击行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析

用户困惑

- 以勒索、挖矿病毒为代表的新型网络攻击行为，其显著特点就是变种多、变化快，传统的IPS、防毒墙、杀毒软件等基于特征库进行检测的手段往往严重滞后于攻击的变化，无法提供有效的防御能力。

安全区域边界：锐捷方案特色-2





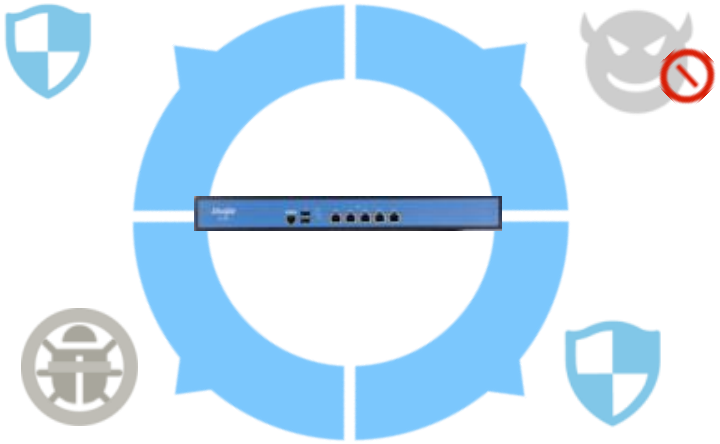
✓ **“RG-BDS + 流量探针”**基于“安全特征+ 行为分析”实现病毒恶意探测定位，除了基于已知“安全特征”，还可依靠“行为模型”去发现未知威胁和攻击。

✓**动态防御系统DDP**，无需依赖任何特征库，通过在网络中虚拟大量诱饵终端，迷惑攻击者的同时分析异常的流量行为模式，从而捕获攻击源

基于网络行为的未知威胁检测

安全区域边界：锐捷方案特色-2

动态防御系统DDP



XX钢铁企业实测案例

1. 2019年5月某一天，在拜访XX钢铁企业客户的路上，客户电话说中了勒索病毒，希望我们能协助解决，初步判断是3-6台电脑；
2. 当天我们快速安排测试样机到客户现场，不到1小时就发现了网络中10几台中病毒的电脑，还有几台没有爆发的潜伏电脑。而同时在测试的国内XX大型安全厂商，还仅发现了几台电脑。
3. 客户当即就不让我们撤下DDP，并计划采购……

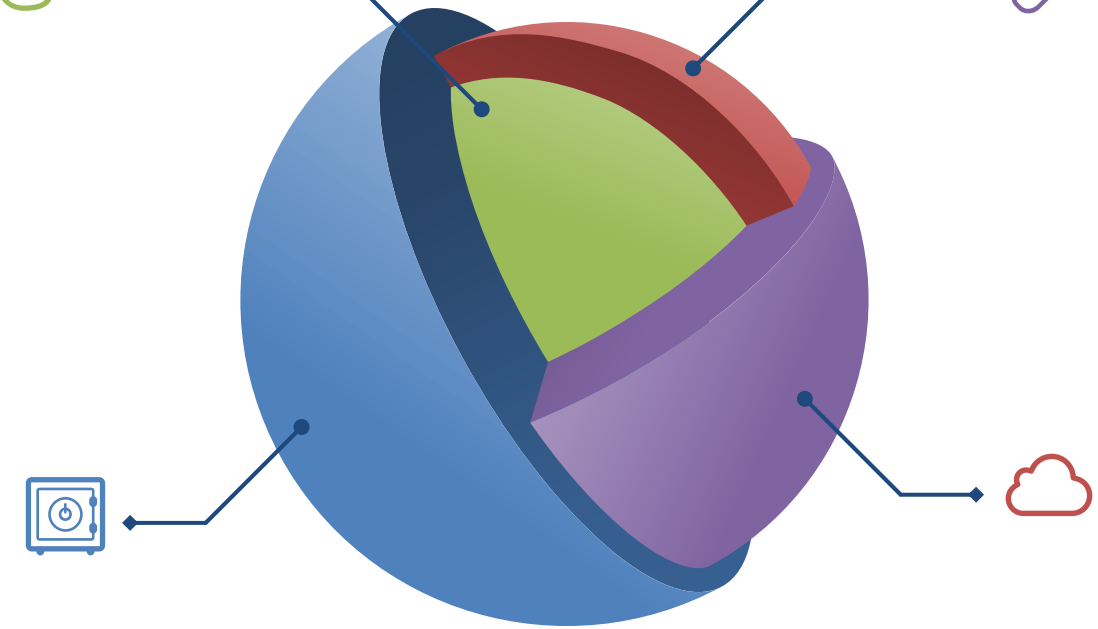
安全区域边界：锐捷方案特色-2

空间维度：DDP

通过虚拟大量“诱饵终端”对恶意攻击者进行诱捕

流量维度：探针

基于流量模型的异常发现分析能力



文件维度：沙箱

基于文件行为的动态恶意代码学习能力

主机维度：EDR

联动EDR提供基于主机的异常进程和病毒行为信息

锐捷安全态势感知平台

4+1 未知威胁防御

除了最基础的各类安全、网络和系统日志，增加主机、流量、文件、空间四大维度的安全数据来源，实现对未知威胁的态势感知

安全区域边界：建设难点和困惑-3

等保2.0规范关键要求

- 应在关键网络节点处检测、防止或限制从内部/外部发起的网络攻击行为。
- 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

用户困惑

- 传统安全建设方案里，网络安全事件监测往往缺乏用户身份认证与审计的配合，出现安全事件后无法定位到人。
- 对于检测到的安全攻击事件，特别是来自内部的攻击，缺少有效的响应机制，对攻击者实施及时的警告、隔离等处理。

安全区域边界：锐捷方案特色-3

采集全网安全流量+日志信息，智能发现安全威胁

安全事件智能处置，联动全网设备将风险排除在边界

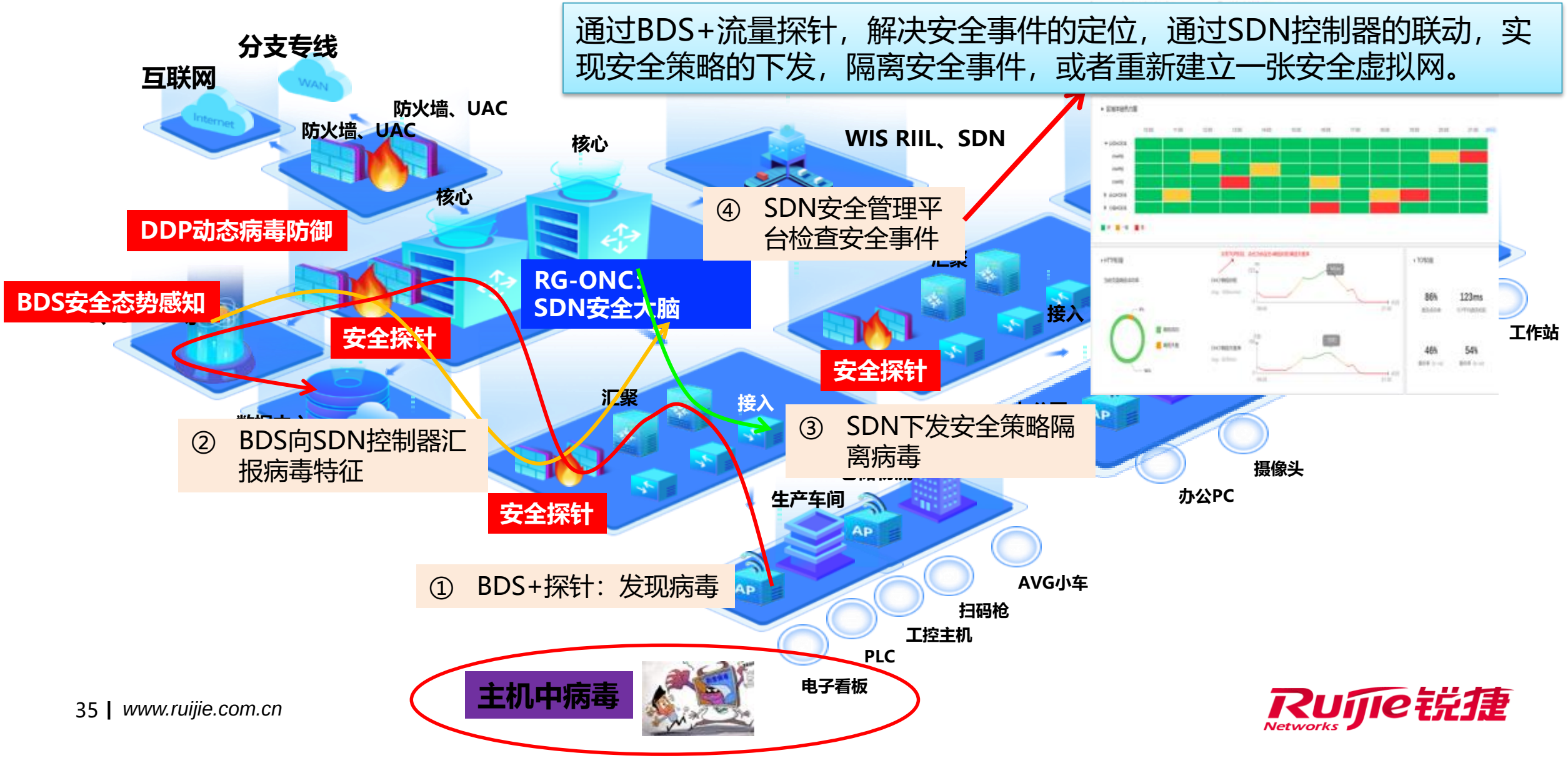
全网统一实名身份认证体系，实现用户级事件响应

3合1 主动安全防御

经态势感知+SDN+实名认证技术赋能，全网设备形成统一的安全体系，每一个交换机端口都能成为智能阻断入侵的防线，实现基于用户身份的安全事件响应处理

安全区域边界：锐捷方案特色-3

通过BDS+流量探针，解决安全事件的定位，通过SDN控制器的联动，实现安全策略的下发，隔离安全事件，或者重新建立一张安全虚拟网。



安全计算环境：建设难点和困惑

等保2.0规范关键要求

- 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换
- 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现

用户困惑

- 现实环境中，不少业务系统缺乏足够安全的用户身份认证机制，无法实现双因素认证的安全要求
- 内部大量业务系统各自独立认证，缺乏统一的身份管理体系，也增加了用户密码记忆和管理负担

安全计算环境：锐捷方案特色

✓ 密码、短信、APP、指纹……多重因素认证

✓ 单点登录，入网即认证，一次登录一网全通

面向业务的多元身份聚合能力

安全管理中心：建设难点和困惑-1

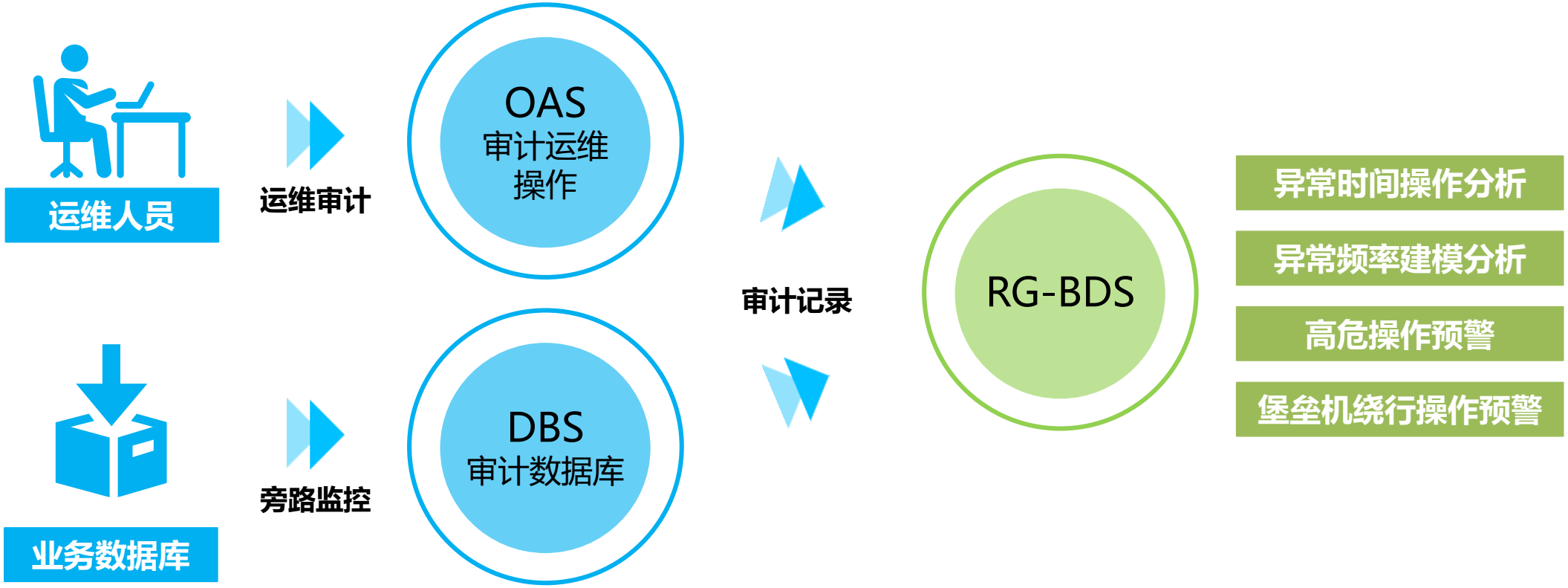
等保2.0规范关键要求

- 应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计。
- 应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等

用户困惑

- 堡垒机等运维审计设备一般采用类似代理服务器的工作原理，往往只能执行最基本的审计和告警策略，无法实现真正的访问控制，如果未设置有效的网络层访问控制机制。如果恶意用户绕过堡垒机直接访问系统，甚至直接物理登录操作，堡垒机对此无能为力。

安全管理中心：锐捷方案特色-1



基于大数据模型的安全审计

OAS堡垒机、 DBS数据库审计实现与BDS大数据平台联动，将重要审计记录实时同步到BDS，并结合服务器登录日志等信息源进行建模分析，对异常操作进行及时预警，实现敏感数据的安全监控需求

安全管理中心：建设难点和困惑-2

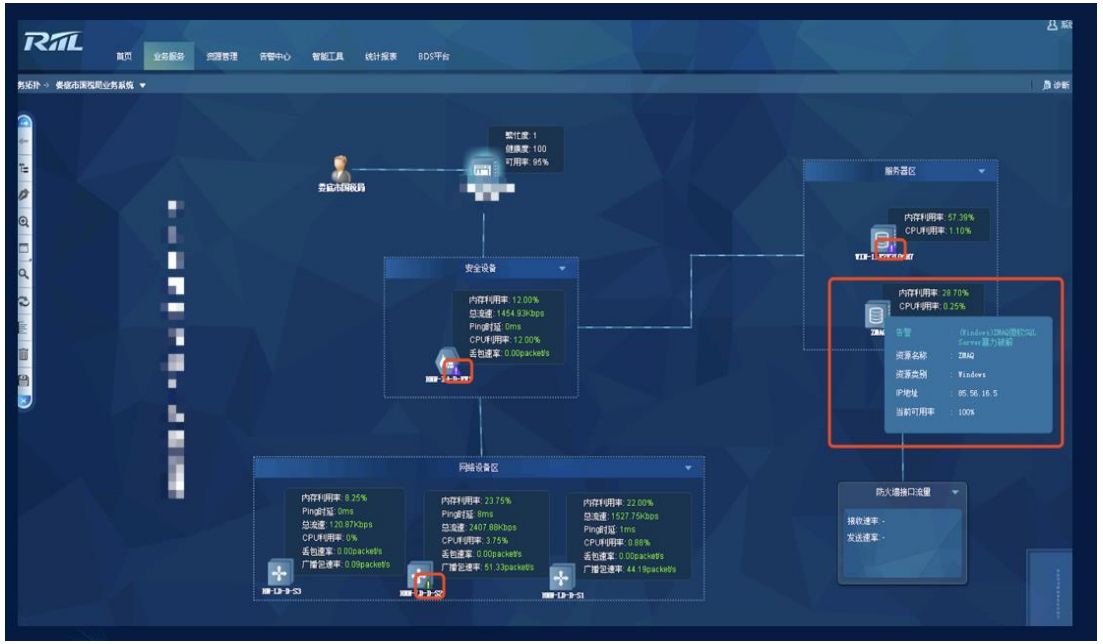
等保2.0规范关键要求

- 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；
- 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；
- 应能对网络中发生的各类安全事件进行识别、报警和分析。

用户困惑

- 常规的安全等保方案往往缺少针对IT运维层面的技术解决方案
- 传统的日志管理平台仅具备基本的日志采集功能，和基于日志的简单告警，无法胜任结合全网安全数据进行综合安全建模分析的要求
- 发生业务故障时，往往难以快速判断是网络故障、性能问题或是遭到攻击

安全管理中心：锐捷方案特色-2



安全+运维 统一管理

IT运维与安全运维无缝结合，实现统一高效管理

典型运维场景案例：

- 运维平台报告某业务系统CPU/内存资源占用>90% → 检查告警事件发现大数据分析高危挖矿行为 → 查询大数据关联分析报告，确认黑客入侵路径 → 进行针对性加固，问题解决

Ruijie Networks 锐捷

锐捷等保2.0方案特色总结：1+N 全网安全

网络 + 安全

等保2.0标准名称的变化，明确强调了安全体系的建设必须要跟网络架构设计紧密结合

锐捷等保2.0方案特色总结：1+N 全网安全

01

安全产品

完整的等保安全产品品类

02

网络产品

提供基于SDN技术的网络安全支撑体系

03

无线产品

全系列无线产品，形成有线无线全网统一安全体系

04

认证产品

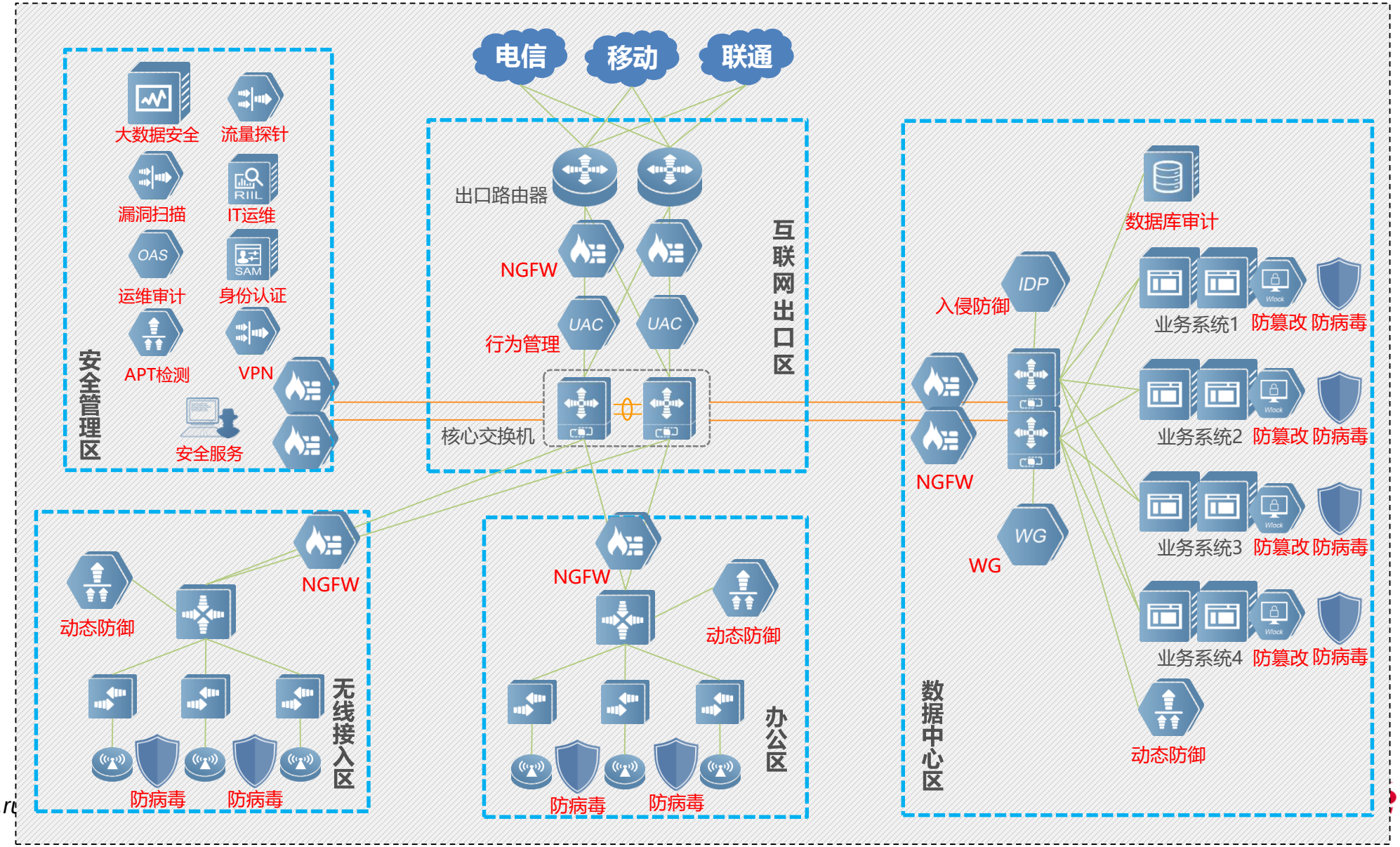
用户身份+应用鉴权

05

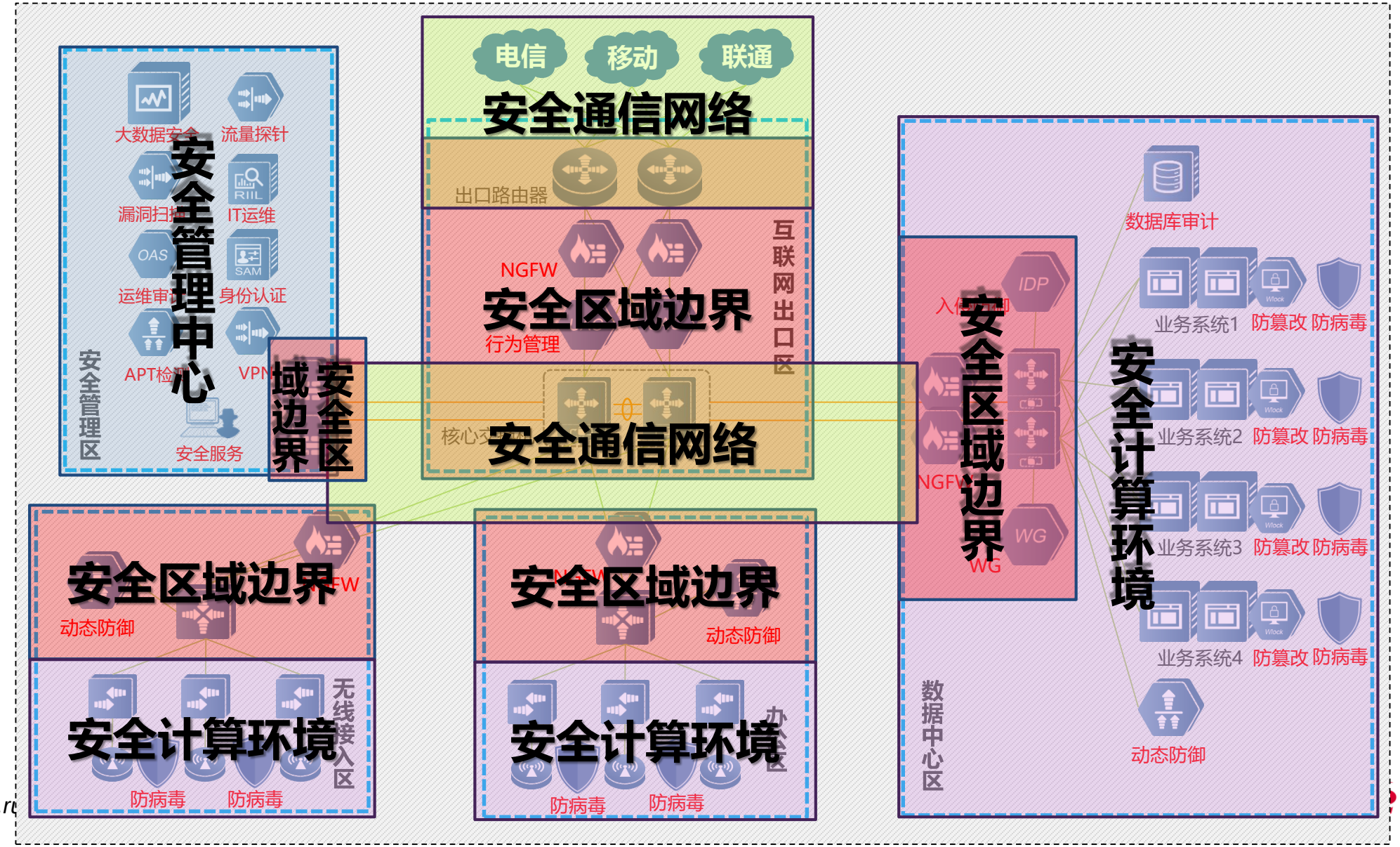
运维产品

IT运维管理的可靠支撑

一个中心三重防护 等保方案详细结构设计



一个中心三重防护 等保方案详细结构设计



安全管理中心

- 大数据安全 (流量+日志)
- IT运维管理
- 堡垒机
- 漏洞扫描
- WMS
- 等保建设咨询服务

安全通信网络

- 下一代防火墙
- VPN
- 路由器
- 交换机

安全区域边界

- 下一代防火墙 (防病毒+垃圾邮件)
- 入侵检测/防御
- 上网行为管理
- 安全沙箱
- 动态防御系统
- 身份认证管理
- 流量探针
- WEB应用防护

安全计算环境

- 入侵检测/防御
- 数据库审计
- 动态防御系统
- 网页防篡改
- 双因素认证
- 漏洞风险评估 (渗透+漏扫服务)
- 杀毒软件

建设要点

- 对安全进行统一管理与把控
- 集中分析与审计
- 定期识别漏洞与隐患

建设要点

- 构建安全的网络通信架构
- 保障信息传输安全

建设要点

- 强化安全边界防护及入侵防护
- 优化访问控制策略

建设要点

- 强调系统及应用安全
- 加强身份鉴别机制与入侵防范

4

Contents

等保2.0解读

智能制造下的企业信息安全现状

锐捷企业信息安全解决方案

锐捷企业安全典型案例

中国铁总通信中心——中心节点数据中心

该数据中心部署了包括3套大数据安全BDS-A等在内的防火墙、漏扫、安服等6大类接近20台锐捷安全设备，是全国铁路数据网络的中心节点，连接了18个铁路局和几万个车站的庞大网络，是全国铁路通信网络的大脑，承载着信号、通信、信息等上百个业务系统。

近两年各行业标杆性案例

全球净楼层第三高

中国尊

整网安全

（独家供应）

金融级总行

中国进出口银行

30台防火墙

（总行数据中心）

国家部委

国家信息中心

BDS+RIIL

（综合安全运维平台）

全国医院TOP10之一

华山医院新院区

整网安全

（高分通过等保三级）

锐捷典型客户案例

- 南京依维柯
- 阿里巴巴（中国）
- 苏酒集团
- 美亚柏科
- 福建省交通集团
- 上海华山医院
- 上海胸科医院
- 山东中医药大学附属医院
- 贵阳职业技术学院
- 黔西南州人民医院
- 南州中级人民法院
- 呼和浩特铁路局
- 河源市江东新区管委会
- 黑龙江农垦大学
- 贵阳职业技术学院
- ……

首批通过公安部等保建设专业认证

各类认证证书


CCRC

信息安全服务资质认证证书

证书编号：CCRC-2019-ISV-RA-594

兹证明

锐捷网络股份有限公司

的**信息安全风险评估**服务资质符合
CCRC-ISV-C01:2018《信息安全服务 规范》
三级服务资质要求。

注册地址：福建省福州市仓山区金山大道618号桔园洲工业园19#楼
办公地址：福建省福州市仓山区金山大道618号桔园洲工业园19#楼

颁证日期：2019年4月29日　　有效期至：2020年4月28日

中国网络安全审查技术与认证中心

中国·北京·朝外大街甲10号（100020）　www.isccc.gov.cn　证书通过此网站查询

S 001547


CCRC

信息安全服务资质认证证书

证书编号：CCRC-2019-ISV-ER-261

兹证明

锐捷网络股份有限公司

的**信息安全应急处理**服务资质符合
CCRC-ISV-C01:2018《信息安全服务 规范》
三级服务资质要求。

注册地址：福建省福州市仓山区金山大道618号桔园洲工业园19#楼
办公地址：福建省福州市仓山区金山大道618号桔园洲工业园19#楼

颁证日期：2019年4月29日　　有效期至：2020年4月28日

中国网络安全审查技术与认证中心

中国·北京·朝外大街甲10号（100020）　www.isccc.gov.cn　证书通过此网站查询

S 001546


QAC

中质协质量保证中心

质量管理体系认证证书子证书

注册号：00617Q20774R2L-4

兹证明

锐捷网络股份有限公司

ISO 9001:2015

认证范围

互联网接入设备、网络及通讯设备的设计、开发、生产和服务；网络技术及软件的设计开发、生产和服务；系统集成服务（依资质范围）

本证书有效期：2017年06月13日 至 2020年06月12日

IAF　CNAS


EWC

信息安全管理体系认证证书

证书号：0390161S

兹证明

锐捷网络股份有限公司

福建省福州市仓山区金山大道618号桔园洲工业园19#楼
福建省福州市闽侯县上街镇高新大道9号星网锐捷海西科技园

建立的信息安全管理体系符合标准：
ISO/IEC 27001:2013

认证范围

互联网接入设备、网络及通讯设备的
设计、开发、生产和服务；
网络技术及相关软件的设计、开发和服务；
计算机系统集成服务所涉及的信息安全管理活动

（适用性声明版本：V1.0）

认证有效期：2016年7月11日至2019年7月10日

确证日期：2016年7月11日

EWC 授权人：

CNAS


中国反网络病毒联盟
Anti Network-Virus Alliance of china

中国反网络病毒联盟成员单位证书

证书编号：ANVA-MEMBER-1905

锐捷网络股份有限公司：

根据签署的ANVA自律公约，认证贵单位为中国反网络病毒联盟成员单位，作为白名单工作组成员，有效期从2019年1月至2021年1月。

中国反网络病毒联盟
2019年1月


荣誉证书

HONORARY CREDENTIAL

锐捷网络股份有限公司

RG-BDS大数据安全平台

2017中国应急管理信息化产品技术创新奖

中国信息协会
二零一七年五月

Ruijie Networks 锐捷

安全全家福

覆盖应用、网关、审计、管理、
安服等**5大类17个**安全品类

应用安全

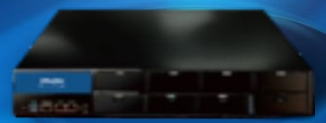
- RG-Wlock网页防篡改
- RG-WG WEB应用防火墙
- RG-WMS网站监控预警
- RG-Scan漏扫
- RG-IDP入侵检测防御
- RG-ISG视频监控安全网关

网关安全

- RG-WALL下一代防火墙(固化端口)
- RG-WALL下一代防火墙(模块化)
- RG-WALL-VPN安全网关

态势感知

- RG-BDS大数据安全平台
- 动态防御系统RG-DDP
- 安全沙箱RG-APT
- RG-PowerCache上网内容加速



审计安全

- RG-UAC上网行为管理
- RG-OAS堡垒机
- RG-DBS数据库审计

安全服务

- 等级保护建设咨询
- 渗透测试
- 漏洞扫描
- 安全事件处置
- 安全检测评估
- WEB安全现状分析
- 专家安全分析
- 安全策略优化

Ruijie 锐捷 Networks

THANKS

锐捷网络股份有限公司

地址：北京海淀区复兴路29号中意鹏奥大厦东塔A座11层　邮编：100036

Office Tel: 010-5171 5999　　Fax: 010-5171 5872

www.ruijie.com.cn