深圳市智博通电子有限公司

网络安全等级保护2.0

智博通路由解决方案

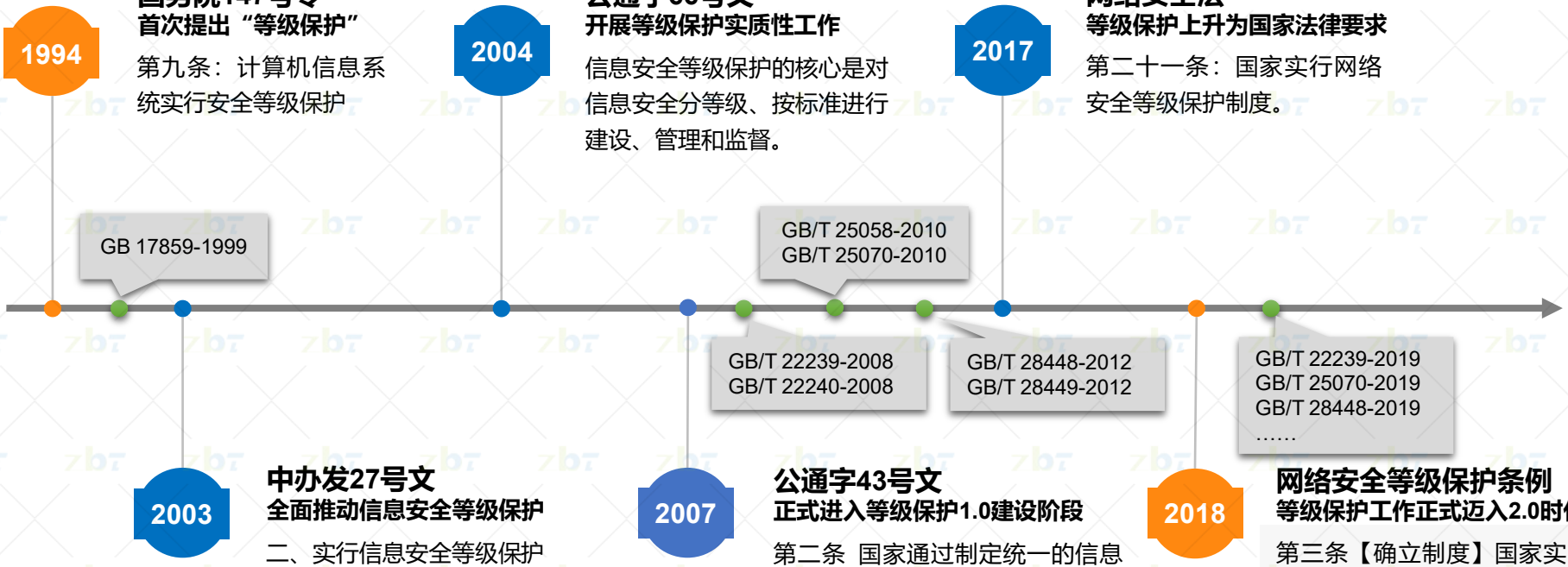
共同打造智能、安全、高效的未来网络服务平台

2020/7/7

目录

CONTENTS

网络安全法等级保护发展历程



目录

CONTENTS

等保2.0相对等保1.0的升级

强制执行力度加大

确立法律地位，法律责任实质化

保护能力等级提升

- 第三级对象（重要网络）范围扩大；
- 安全保护能力提升

安全保护措施强化

- 技术措施趋向主动、动态；
- 测评尺度更为精准、严格

保护对象范围扩大

- 更多网络运营者被纳入等保监管；
- 覆盖云、移、物、工、大等新场景

工作内容要求细化

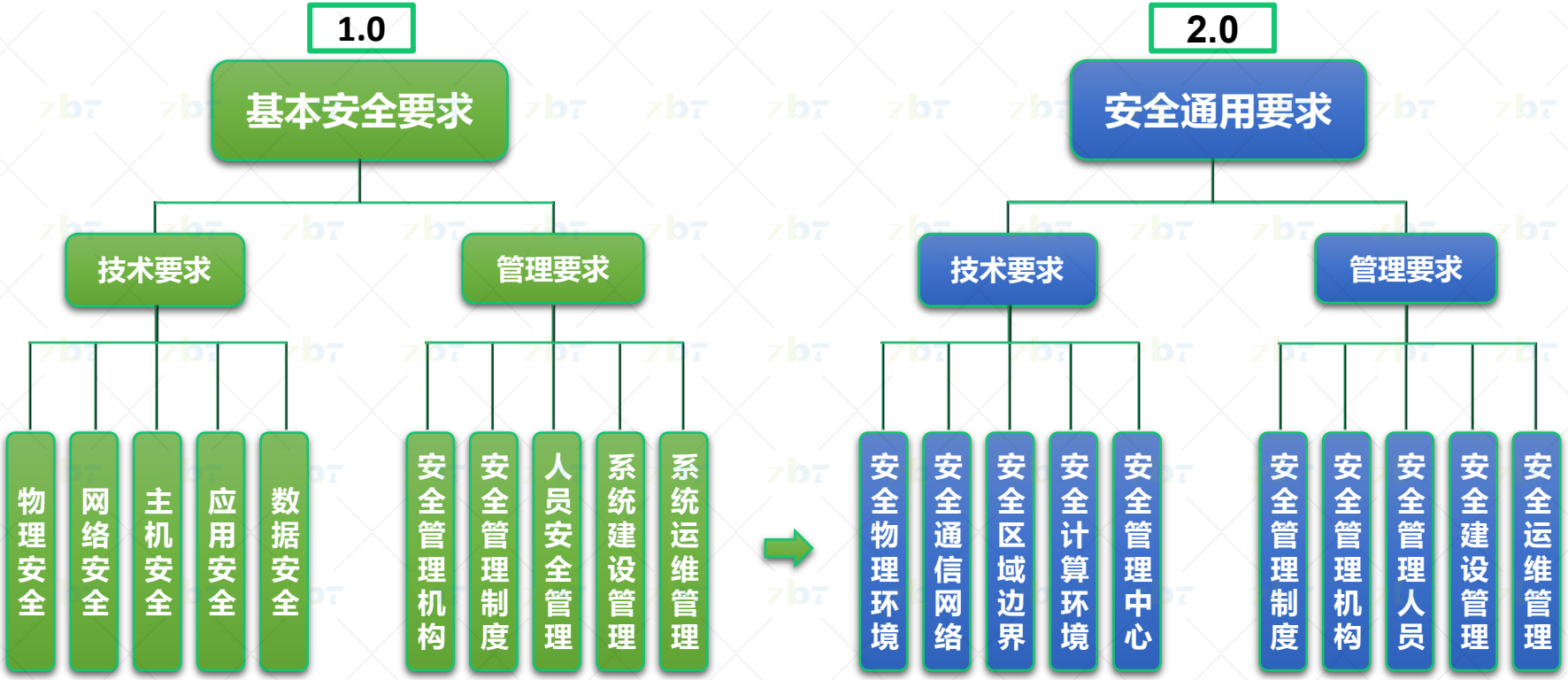
- 五个规定动作+三同步；
- 增加监测预警、应急处置等要求

强制执行力度加大

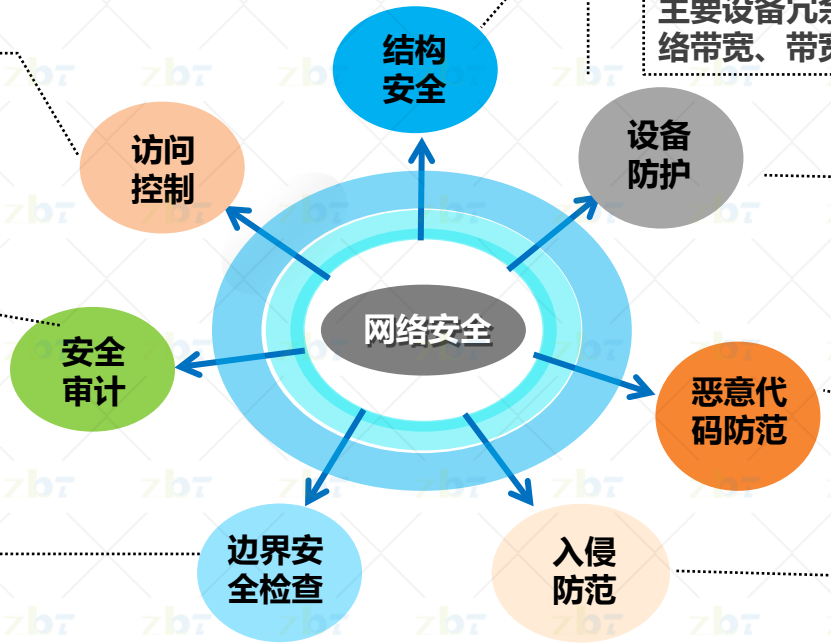
我国山西、广东、上海、四川、重庆、安徽、黑龙江、湖南等地已经出现了网络安全等级保护相关案例，涵盖教育、互联网、医疗、公共服务等领域。被处罚对象发生了**未定级备案**、**未按期进行等级测评**、**未按规定留存网络日志**、**未采取防范网络威胁的技术措施**、**未采取数据保护措施**等违法行为。

序号	时间	处罚行为	处罚对象	处罚措施	执法机关	处罚依据
1	2017.6	未采取防范网络攻击、害网络安全施。存在S严重威胁网				
2	2017.7.20	三级以上系期开展网络				
3	2017.7.22	未进行定级评。存在高站发生被黑				
4	2017.8.1	未依法留存网络日志				
5	2017.8.12	未进行网络定级备案、				
6	2017.8.30	未按照网络安全等级保护制度的要求落实网络安全主体责任，存在高危安全漏洞并被黑客攻造成严重后果	哈尔滨方正县农业技术推广中心设立的“方正农	责令整改，并处	黑龙江省哈尔滨市公安局网安支	《网络安全法》第21条、第
7	2017.9.28	未建立网络安全措施、网络日志六个月，未采取重要数据备份施，致使系统存生身份信息泄露				
8	2017.10.17	未落实网络安任，网站被入侵病毒				
9	2017.12.12	未进行网络安全的定级备案、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	浏阳市烟花爆竹总会网站系统	警告、责令改正	长沙市公安局网技支队、浏阳市公	第21条、第25条、第59条第1款
				的主管人员处5000元罚款		
10	2017.12.13	未落实网络安全等级保护制度。附属医院协同办公系统存在任意文件上传等隐患漏洞情况	湖南省长沙医学院	警告、责令改正	湖南省长沙市、县（区）两级公安网安部门	《网络安全法》第21条、第59条第1款
11	2018.3.26	未落实网络安全等级保护制度，未履行网络安全保护义务	湖南中科智谷教育科技有限公司	约谈法人代表及网站系统管理员； 警告、责令改正	湖南省株洲市、区公安网安部门	《网络安全法》第21条、第25条、第59条第1款
12	2018.1.12	未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，致使网站遭到攻击	河南省新乡市封丘县图书馆网站	对封丘县图书馆给予罚款20000元、对直接责任人处以警告，并罚款5000元	封丘县公安局、封丘县文化广电旅游局	《网络安全法》第21条、第59条第1款

安全控制措施分类结构的变化



等级保护安全解读



要点：
主要设备冗余空间、安全路径控制、整体网络带宽、带宽优先级、重要网段部署

要点：
端口控制、防地址欺骗
协议过滤、会话控制
最大流量数及最大连接数

要点：
组合鉴别技术
特权用户权限分离

要点：
审计记录
审计报表
审计记录的保护

要点：
记录、报警、阻断

要点：
非授权设备接入
非授权网络联出

要点：
记录、报警、阻断

目录

CONTENTS

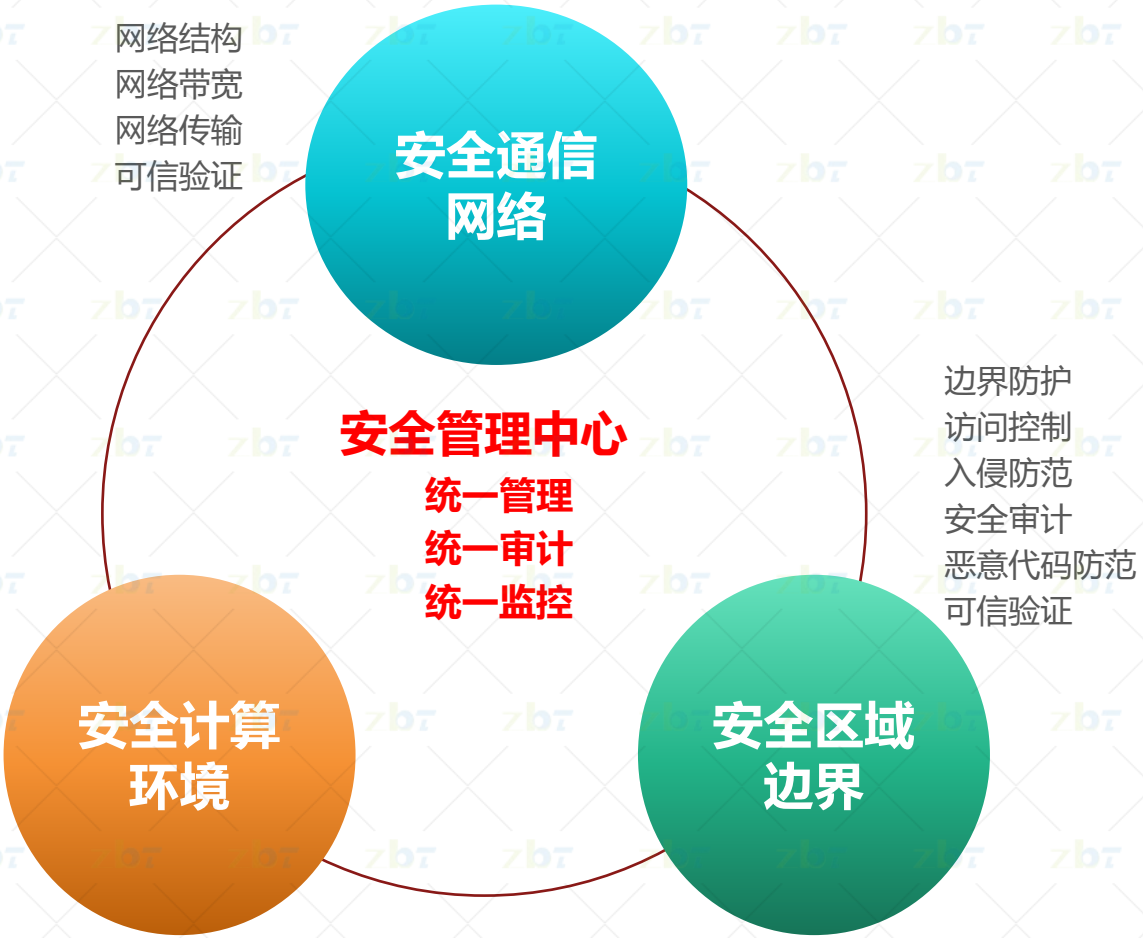
等级保护防护框架

建设“一个中心”管理、“三重防护”体系，分别对计算环境、区域边界、通信网络体系进行管理，实施多层隔离和保护，以防止某薄弱环节影响整体安全

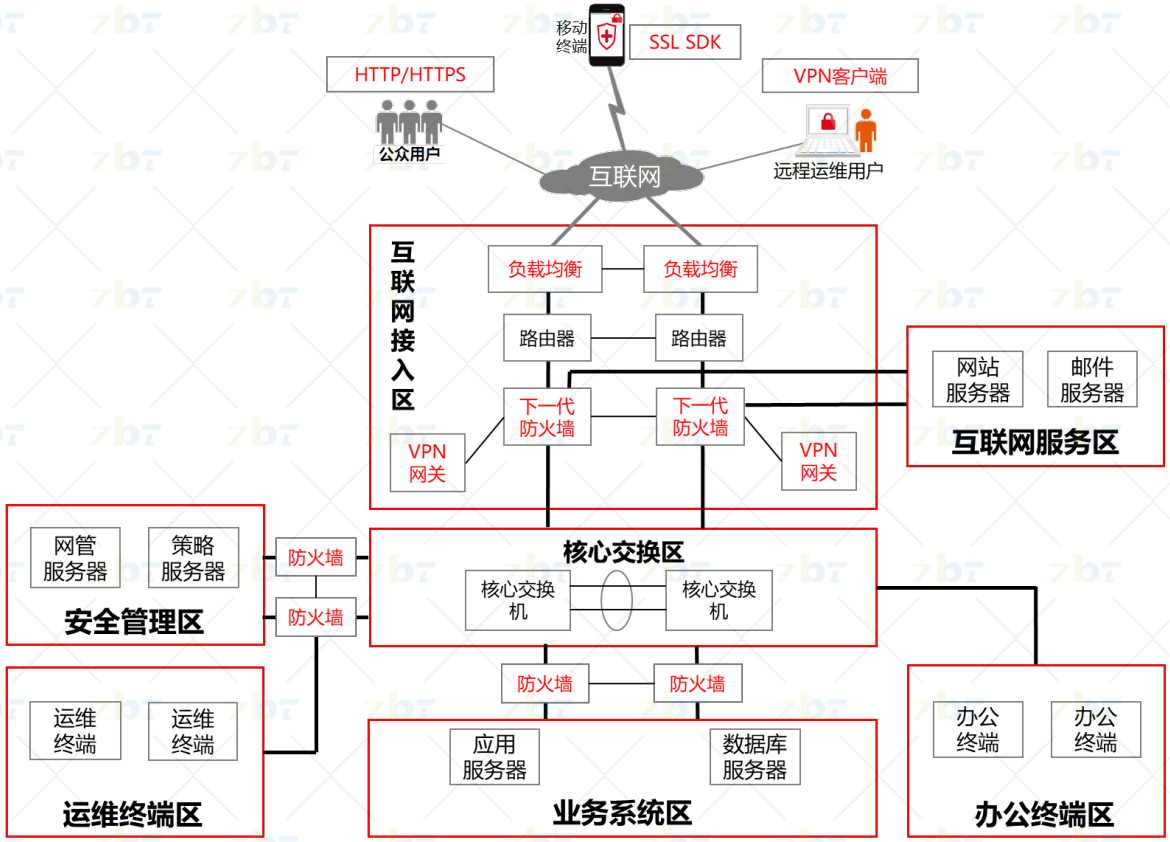
重点对操作人员使用的终端、业务服务器等计算节点进行安全防护，控制操作人员行为，使其不能违规操作，从而把住攻击发起的源头，防止发生攻击行为

分析应用系统的流程，确定用户（主体）和访问的文件（客体）的级别（标记），以此来制定访问控制安全策略，由操作系统、安全网关等机制自动执行，从而支撑应用安全

一个中心、三重防护


网络结构
网络带宽
网络传输
可信验证
安全通信网络
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
保密性
数据备份恢复
个人信息保护等
安全管理中心
统一管理
统一审计
统一监控
边界防护
访问控制
入侵防范
安全审计
恶意代码防范
可信验证
安全计算环境
安全区域边界

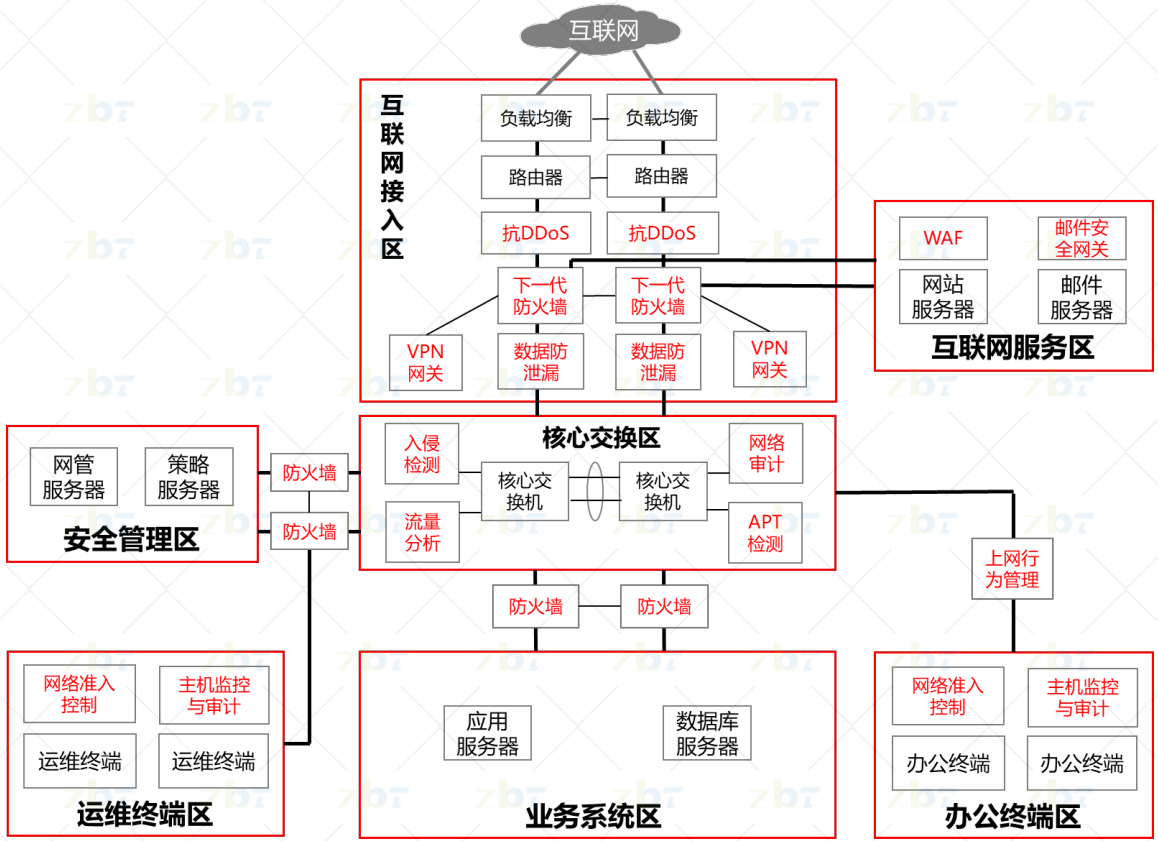
安全通信网络



安全通信网络建设要点

- 路由器、交换机、防火墙等网络设备的业务处理能力满足业务高峰期需要；
- 网络带宽满足业务高峰期需要；
- 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；
- 重要网络区域与其他网络区域之间采取可靠的技术隔离手段；
- 采用密码技术保证通信过程中数据的保密性及完整性。

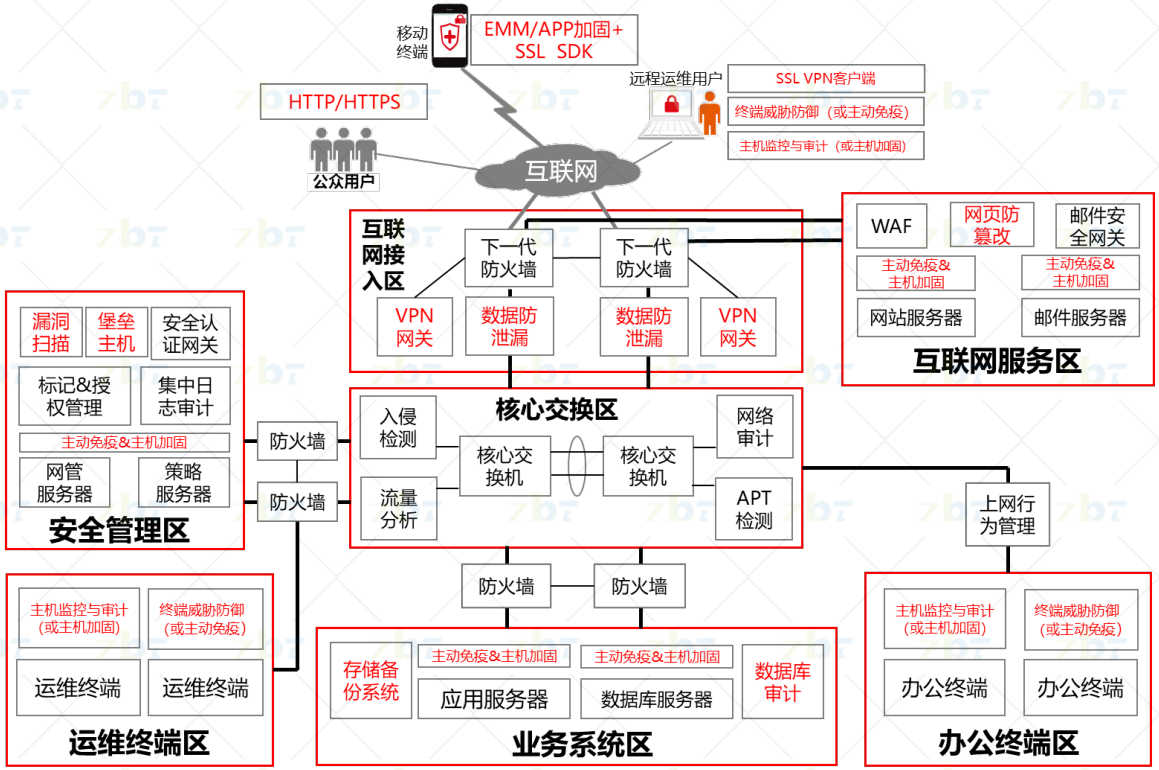
安全区域边界



安全区域边界建设要点

- 对非授权设备私自联到内部网络的行为进行控制；
- 对内部用户非授权联到外部网络的行为进行控制；
- 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；
- 在关键网络节点处检测和/或防御从外部/内部发起的网络攻击行为；
- 对网络攻击特别是新型网络攻击行为进行检测分析，事件告警；
- 对垃圾邮件进行检测和防护，并及时升级和更新；
- 对用户的远程访问行为、互联网访问行为等进行审计和数据分析。

安全计算环境



安全计算环境建设要点

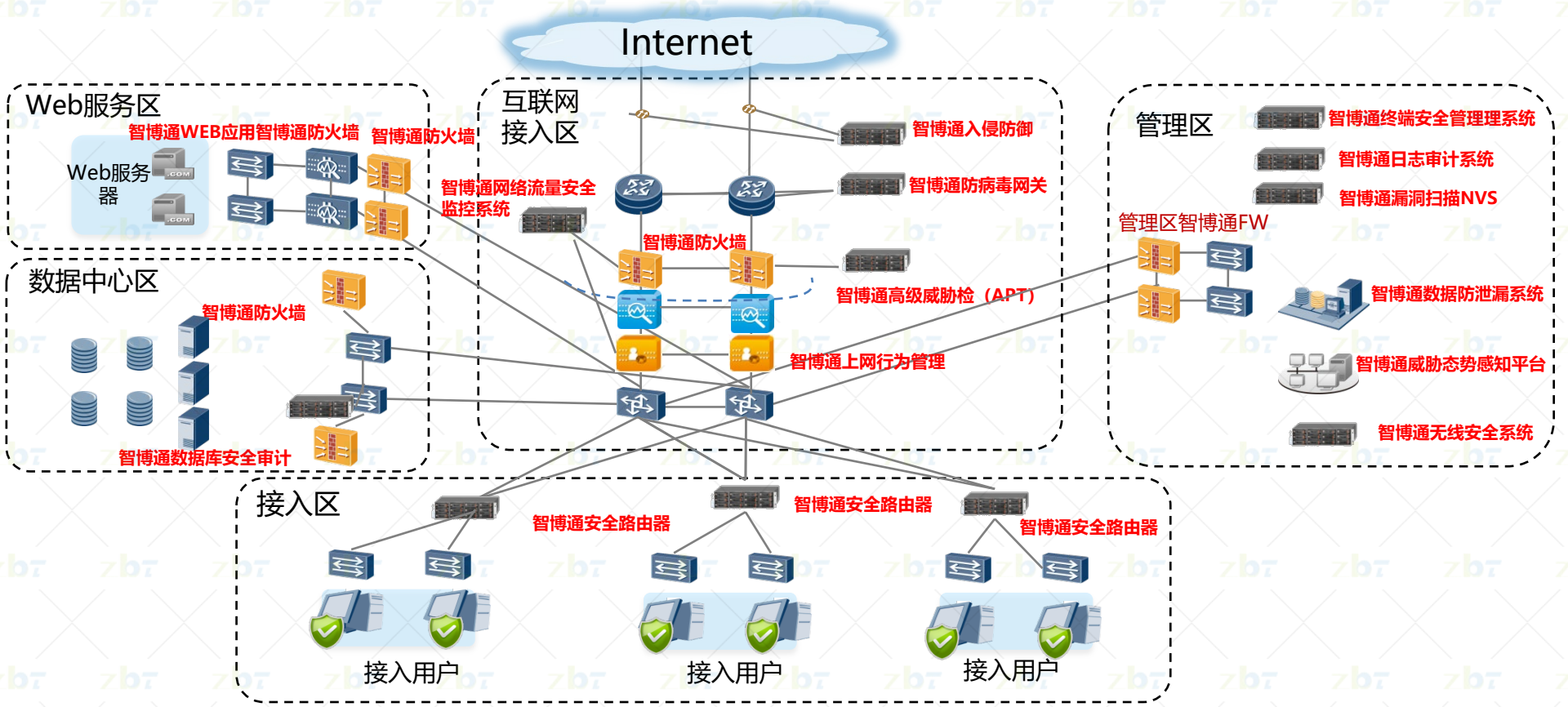
- 采用口令或生物技术结合密码技术对用户进行身份鉴别；
- 采用基于角色/属性或安全标记的访问控制技术对操作系统、数据库、应用用户进行权限管理；
- 对重要的用户行为和重要安全事件进行集中审计；
- 采用漏洞检测、终端管理结合补丁管理、终端威胁防御、主动免疫可信验证、主机加固等技术保障终端及服务器等计算资源的安全；
- 采用密码技术、容灾备份技术等保障重要数据的完整性、保密性、可用性；
- 网页防篡改；
- 敏感数据和个人信息保护。

安全管理中心

安全管理中心建设要点

- 划分不同管理角色，并提供集中的身份鉴别、访问授权和操作审计；
- 对网络和信息基础设施的运行状况进行集中监控；
- 对分散在网络中的审计数据进行收集汇总和集中分析；
- 对安全策略、恶意代码、补丁升级等进行集中管理；
- 部署态势感知和安全运营平台，支撑安全监测、分析、预警、响应、处置、追溯等安全管理和运维工作。

整体解决方案


Internet
Web服务区
Web服务器
智博通WEB应用智博通防火墙
智博通防火墙
数据中心区
智博通防火墙
智博通数据库安全审计
互联网接入区
智博通网络流量安全监控系统
智博通入侵防御
智博通防病毒网关
智博通防火墙
智博通高级威胁检（APT）
智博通上网行为管理
管理区
智博通终端安全管理理系统
智博通日志审计系统
智博通漏洞扫描NVS
管理区智博通FW
智博通数据防泄漏系统
智博通威胁态势感知平台
智博通无线安全系统
接入区
智博通安全路由器
智博通安全路由器
智博通安全路由器
接入用户
接入用户
接入用户

二级/三级等保（基础版）套餐设计

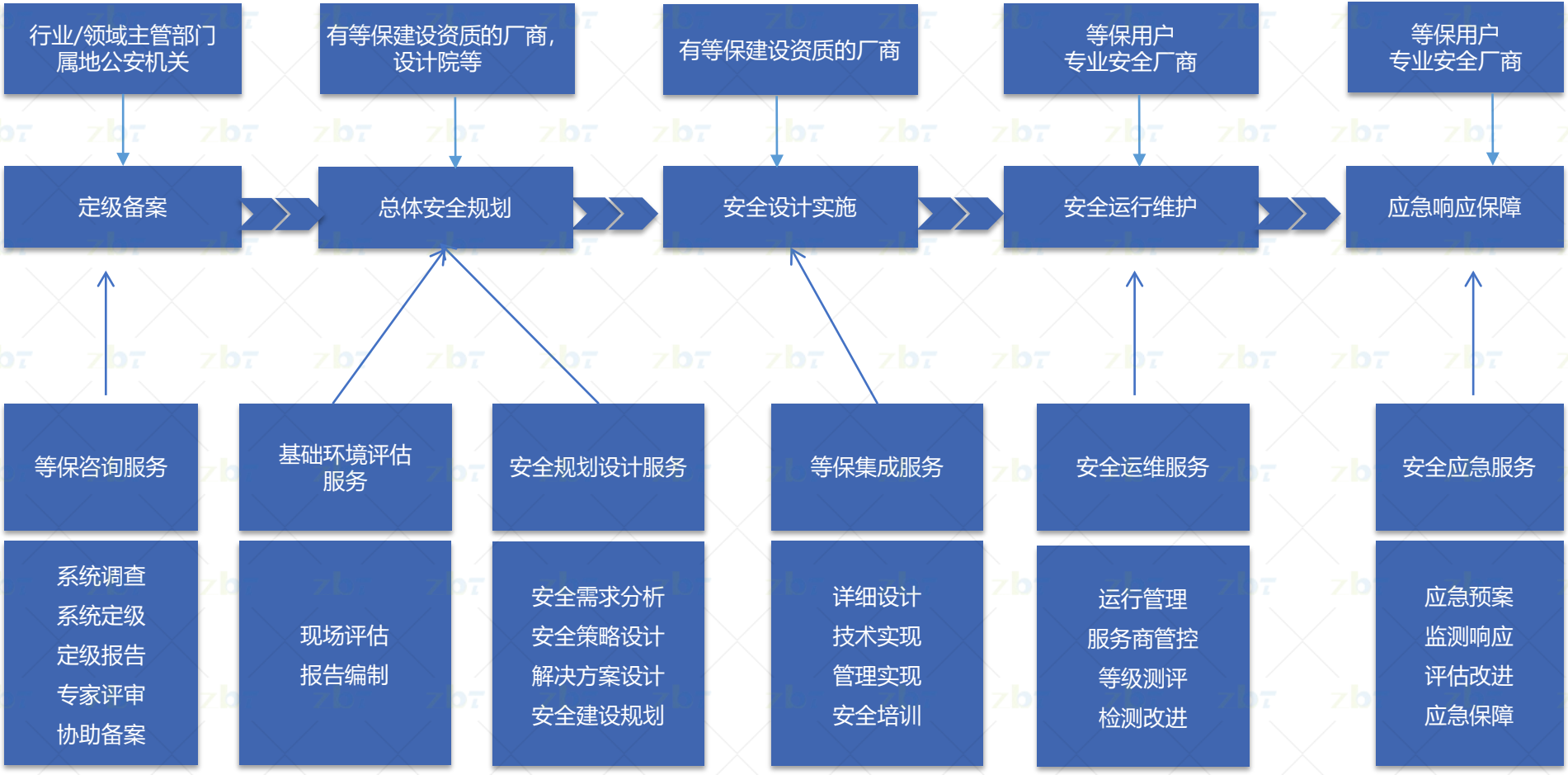
二级等保（基础版）套餐	
智博通防火墙/智能网关	必选
智博通入侵防御IPS	必选
智博通日志收集与审计分析系统	必选
智博通网络流量安全监控系统	必选
智博通终端安全管理系统	必选
智博通上网行为管理UBA	可选
综合评分	**75+**

三级等保（基础版）套餐	
智博通防火墙	必选
智博通安全路由器	必选
智博通日志收集与审计分析系统	必选
智博通网络流量安全监控系统	必选
智博通终端安全管理系统	必选
堡垒机	必选
智博通漏洞扫描NVS	必选
智博通上网行为管理UBA	必选
智博通WEB应用智博通防火墙	可选
智博通数据防泄漏	可选
综合评分	**80+**

三级等保（增强版）套餐设计

三级等保（增强版）套餐			
智博通防火墙/智能网关	必选	智博通主机入侵防御HIPS	可选
智博通入侵防御IPS	必选	智博通数据防泄漏	可选
智博通DDoS防护系统	必选	IAM身份鉴别平台	可选
智博通上网行为管理UBA	必选	智博通网络空间资产治理系统	可选
智博通APT	必选		
智博通日志收集与审计分析系统	必选		
智博通网络流量安全监控系统	必选		
智博通漏洞扫描NVS	必选		
智博通终端安全管理系统	必选		
智博通威胁态势感知平台	必选		
智博通WEB应用防火墙	必选		
运维堡垒机	必选		
网络准入控制系统	必选		
综合评分		85+	

建设流程

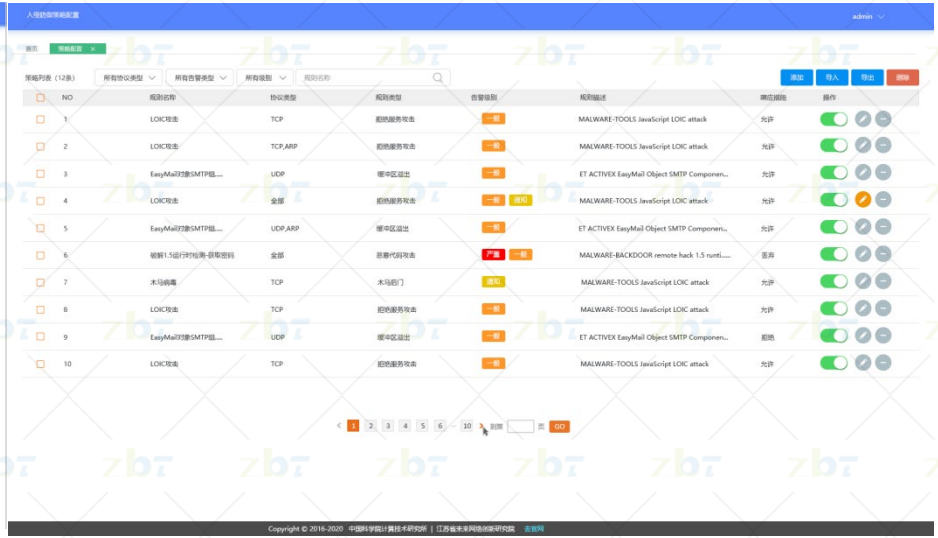


目录

CONTENTS

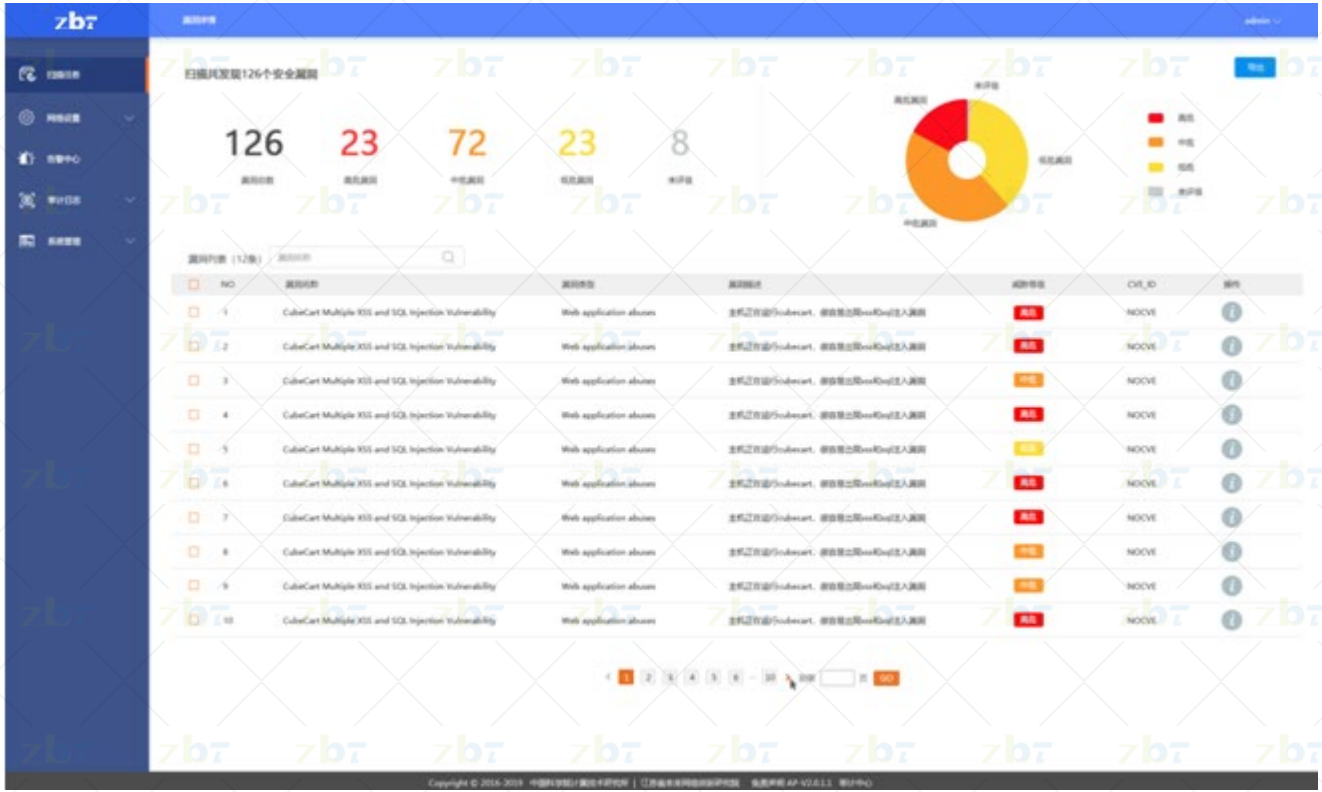
1、智博通入侵防御/检测（IPS/IDS）

- 记录并保存拦截到的入侵事件，对异常流量进行监测并告警，
- 仅限于指定的授权用户访问事件数据，禁止其他用户对事件数据的操作。
- 覆盖35个大类5W+种攻击行为，用于区域边界与计算环境的入侵防御、智博通入侵防御。



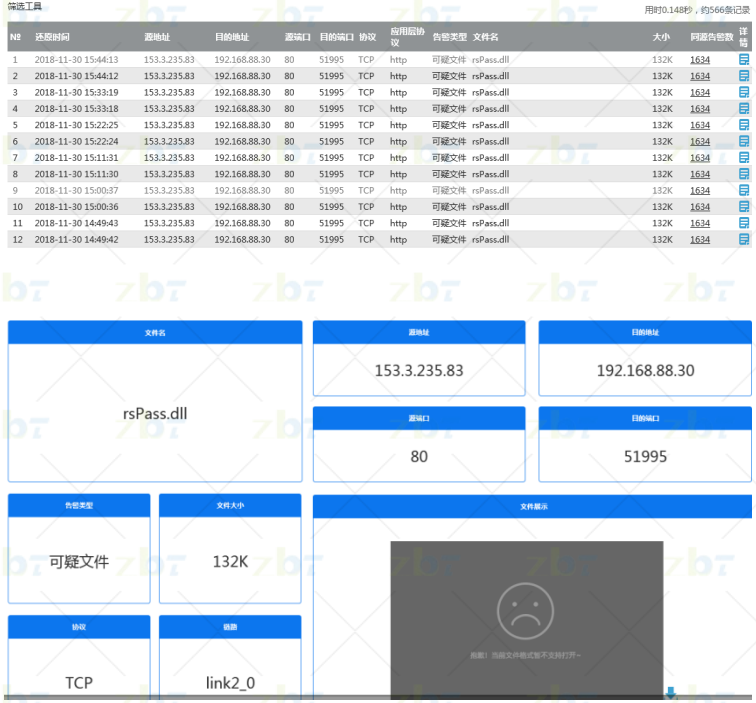
2、智博通漏洞扫描NVS

- 拥有漏洞扫描知识库包含5W+的漏洞规则，10W+CVE漏洞记录，用于内网资产安全管理。



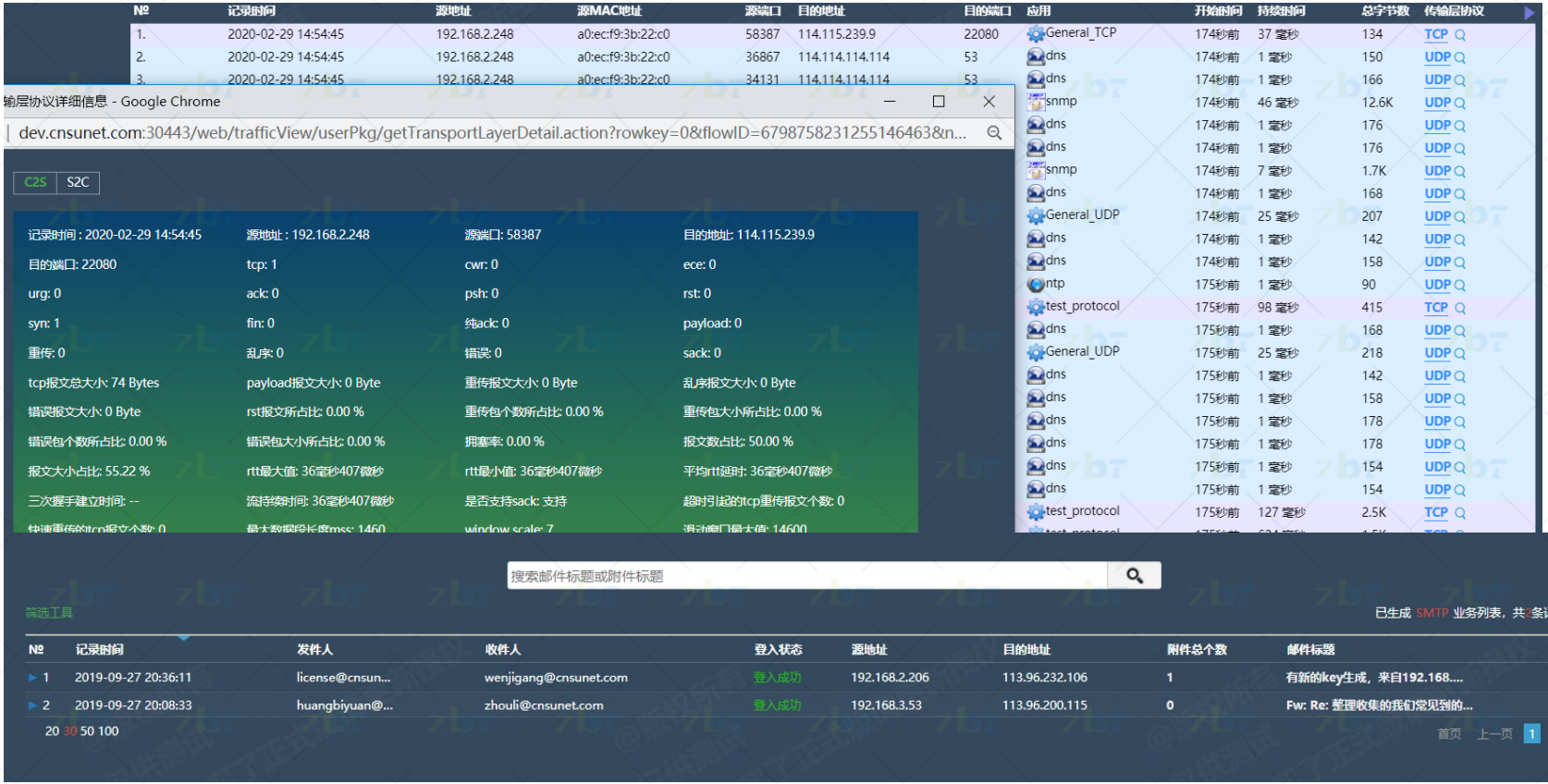
3、智博通防病毒网关UTM

支持文件还原和病毒检测，病毒库规模800W+，用于恶意代码防护与清除，桌面病毒防范。



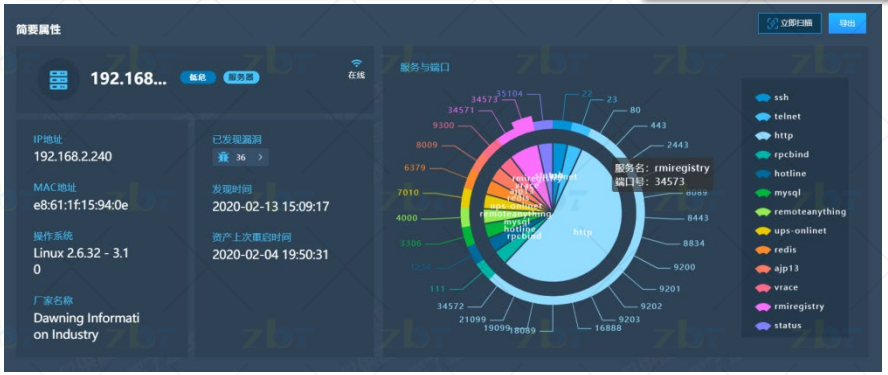
4、智博通日志收集与审计分析系统

支持WEB、流媒体、语音、邮件、文件等业务系统操作记录分析与事件审计。



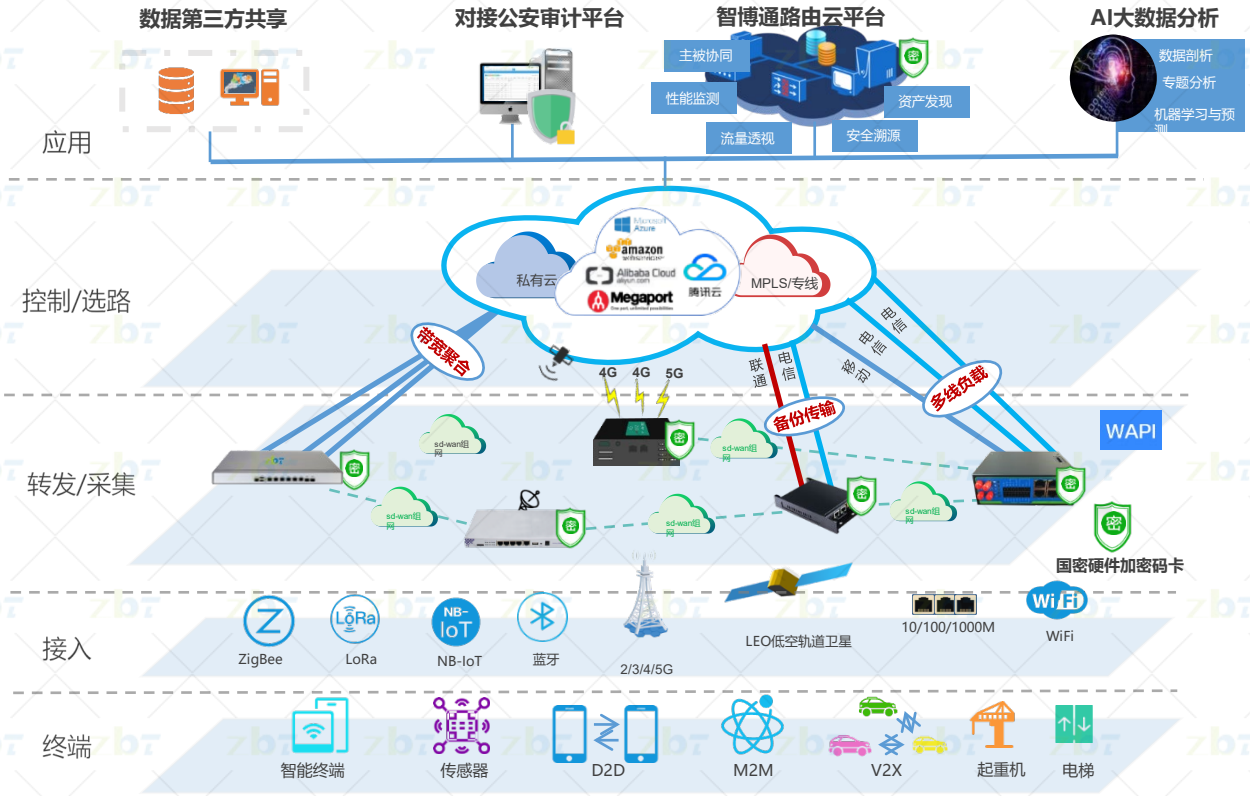
5、智博通网络流量安全监控系统

- 识别主流网络应用2500种以上，支持的资产业务种类大于2300种，用于数据采集分析与异常流量检测。



6、智博通安全路由器

接入管控 + 多重加密 + 安全防护 + 云平台统一管理



泛在接入，资产发现	资产感知/漏洞扫描
带宽聚合/传输优化	入侵防护/未知威胁检测
行为管理，智能流控	智博通防火墙、防毒墙
SD-WAN/VPN	WAPI/国密加密
多业务切片隔离	安全审计/第三方审计
AI鉴别，智能分析	海量挖掘AI智能分析

应用功能软件定义化
按需定制加载

云平台统一管理

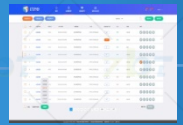
7、智博通虚拟专用网VPN

- 通过加密通道的方式实现异地间安全可靠的连接自组网
- 身份鉴别、访问控制、可信验证、日志审计、数据加密
- 支持网关/隧道状态监控与告警

组网小四步

1 设备通电

2 本地管理复制设备信息



3 粘贴至云平台

4 云平台选择设备组网

通过云平台关联设备即可选择设备组网，**方便快捷**，无需聘请专业IT人员运维。

8、智博通回溯分析系统

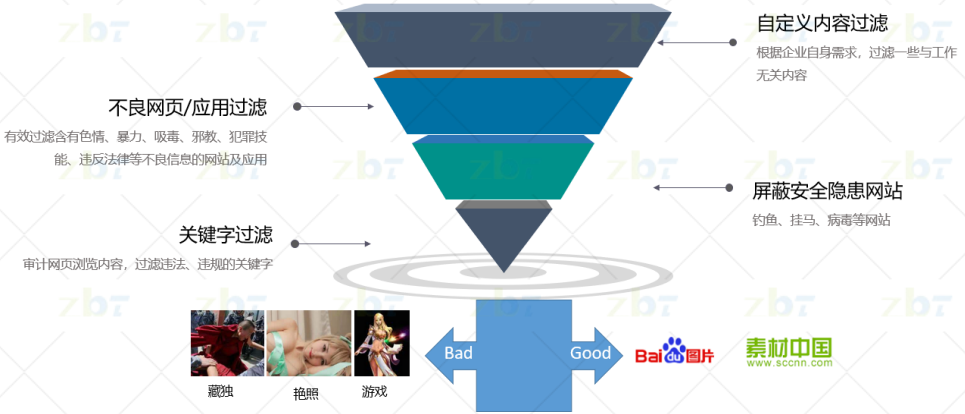
支持2-7层全流量保存与在线解码分析，实现数据保存、取证分析。

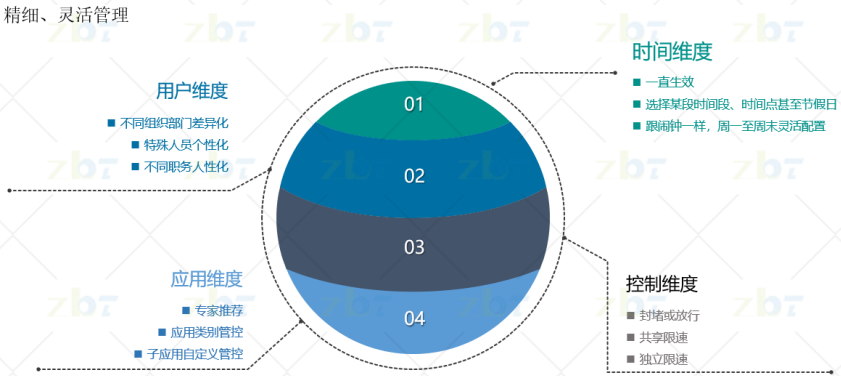
9、智博通防火墙

连接数控制、FTP动态开放端口、DDOS防御及扫描防御、病毒检测等多项功能。

10、智博通上网行为管理UBA

支持身份鉴别、接入认证、安全检测、实名审计、行为管控等多项功能。





11、智博通安全审计平台（综合型）

符合公安部82号令的审计。实现日志采集、储存、分析各系统的人员操作维护信息，及时发现非法、越权操作；同时，可对高危操作实现实时分析、实时监控和阻断。

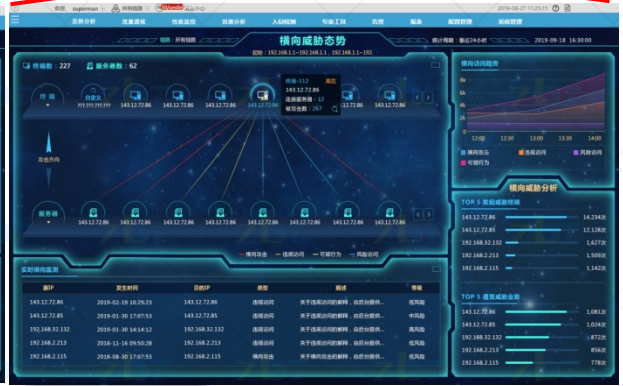
- ✓ 数据捕获和过滤，分析用户上网行为和内容，舆情监控；
- ✓ 细粒度审计环境，网络行为解析、数据库操作记录和预警；
- ✓ 多维检索与关联，还原精确数据，便于追溯取证。
- ✓ 支持海量数据存储，便于安全取证、文件还原和溯源分析

12、智博通态势感知平台

资产态势

外联态势

横向威胁



网络性能

安全态势

13、智博通综合管理系统

对全网的安全设备、安全事件、安全策略、安全运维进行统一集中的监控、调度、预警和管理。对安全管理员进行身份鉴别，根据权限进行操作及操作审计。

14、智博通工控安全检测系统

- 可对异常工控协议报文进行匹配检测，并定位可其中攻击行为，对安全隐患进行直观的分析。
- 系统内置50000+安全规则库，提供全局数据安全检测分析，包括对工控指令攻击、病毒、木马、攻击参数篡改等攻击行为。

开始时间	持续时间	源IP	源端口	目的IP	目的端口	工控协议	详情
2018-11-30 14:16:16.162	83 毫秒	192.168.0.10	51192	192.168.0.2	102	s7	
2018-11-30 14:16:01.89	44 毫秒	192.168.0.10	51181	192.168.0.2	102	s7	
2018-11-30 14:15:59.572	727 毫秒	192.168.0.10	51180	192.168.0.2	102	s7	
2018-11-30 14:15:54.628	1 秒 420 毫秒	192.168.0.10	51179	192.168.0.2	102	s7	
2018-11-30 14:15:51.375	72 毫秒	192.168.0.10	51178	192.168.0.2	102	s7	
2018-11-30 14:15:51.251	104 毫秒	192.168.0.10	51177	192.168.0.2	102	s7	
2018-11-30 14:15:42.881	101 毫秒	192.168.0.10	51176	192.168.0.2	102	s7	
2018-11-30 14:14:38.112	543 毫秒	192.168.0.10	62431	192.168.0.1	102	s7	
2018-11-30 14:14:36.351	329 毫秒	192.168.0.10	62430	192.168.0.1	102	s7	
2018-11-30 14:14:35.489	62 毫秒	192.168.0.10	62429	192.168.0.1	102	s7	
2018-11-30 14:14:23.627	17 毫秒	192.168.0.10	62422	192.168.0.1	102	s7	
2018-11-30 14:14:10.094	538 毫秒	192.168.0.10	62401	192.168.0.1	102	s7	
2018-11-30 14:14:08.322	332 毫秒	192.168.0.10	62400	192.168.0.1	102	s7	
2018-11-30 14:14:07.519	62 毫秒	192.168.0.10	62399	192.168.0.1	102	s7	
2018-11-30 14:13:44.398	533 毫秒	192.168.0.10	62386	192.168.0.1	102	s7	
2018-11-30 14:13:43.09	325 毫秒	192.168.0.10	62385	192.168.0.1	102	s7	
2018-11-30 14:13:42.31	46 毫秒	192.168.0.10	62384	192.168.0.1	102	s7	
2018-11-30 14:13:22.608	166 毫秒	192.168.11.15	49295	192.168.11.10	53548	opc	
2018-11-30 14:12:48.994	40 秒 527 毫秒	192.168.11.10	62529	192.168.11.15	49237	opc	
2018-11-30 14:12:48.696	442 毫秒	192.168.11.15	49295	192.168.11.10	53548	opc	

0 100

首页 上一页 1 2 3 4 5 下一页

期待与您的合作!