基于“动态安全”体系架构设计，构筑“网络+安全”稳固防线

锐捷网络等级保护2.0整体解决方案

如有疑问
扫一扫在线咨询

Ruijie Networks 锐捷

国家网络安全等级保护工作进入2.0时代

国家《网络安全法》于 2017 年 6 月 1 日正式施行，所有了网络运营者和关键信息基础设施运营者均有义务按照网络安全等级保护制度的要求对系统进行安全保护。随着 2019 年 5 月 13 日《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》标准的正式发布，国家网络安全等级保护工作正式进入 2.0 时代。

等保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

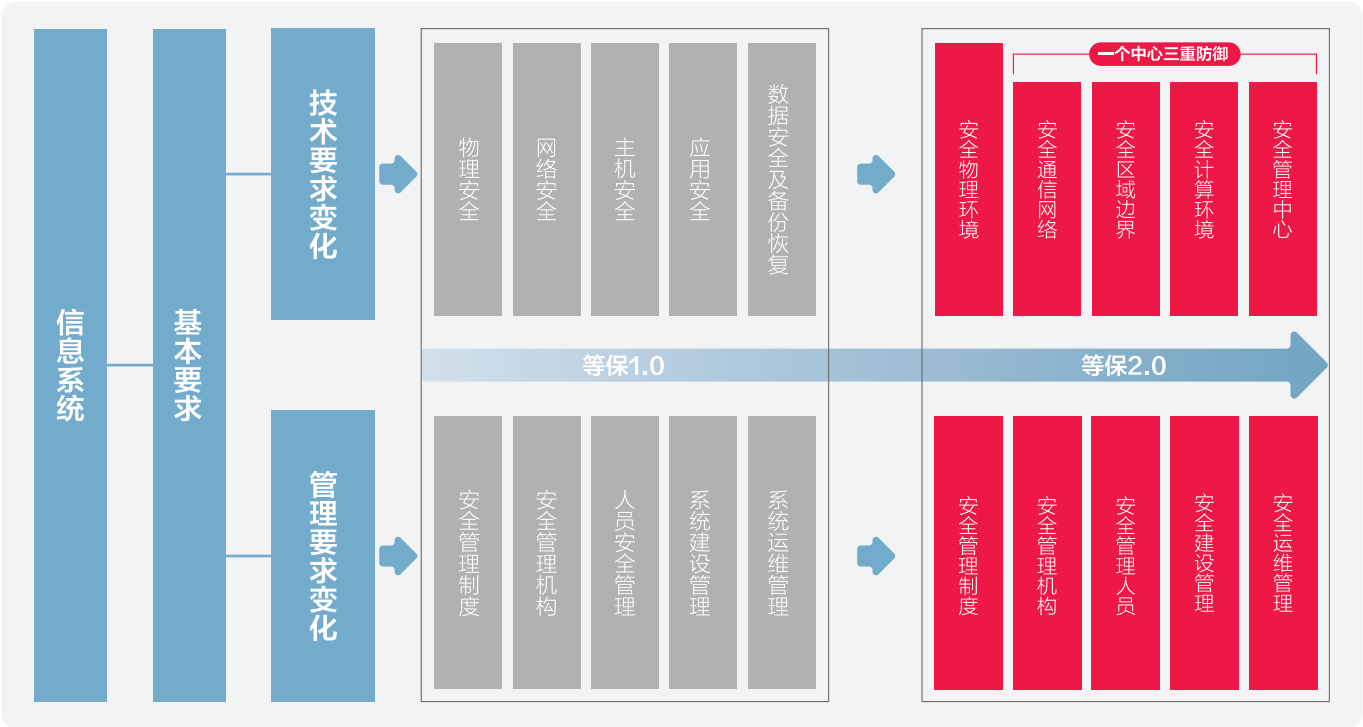
结构调整

一个中心，三重防御

防御理念

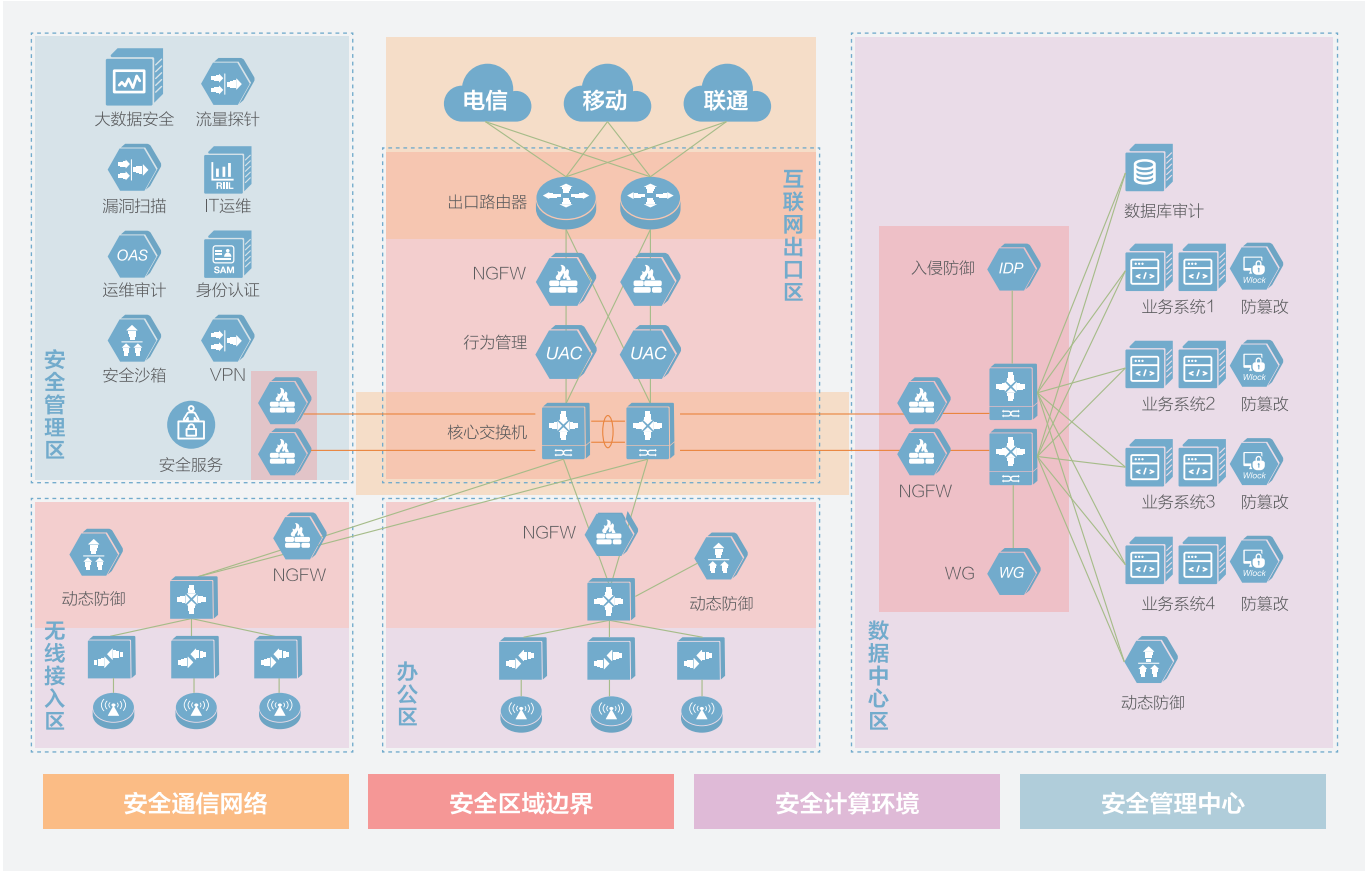
被动防御→主动防御

等保2.0基本要求结构变化



等保 2.0 充分体现了“一个中心三重防御“的思想。一个中心指“安全管理中心”，三重防御指“安全计算环境、安全区域边界、安全网络通信”，同时等保 2.0 强化可信计算安全技术要求的使用。

锐捷网络等保2.0解决方案拓扑图结构设计



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
- 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

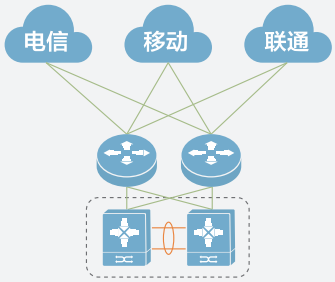
- 强调系统及应用安全
- 加强身份鉴别机制与入侵防范

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



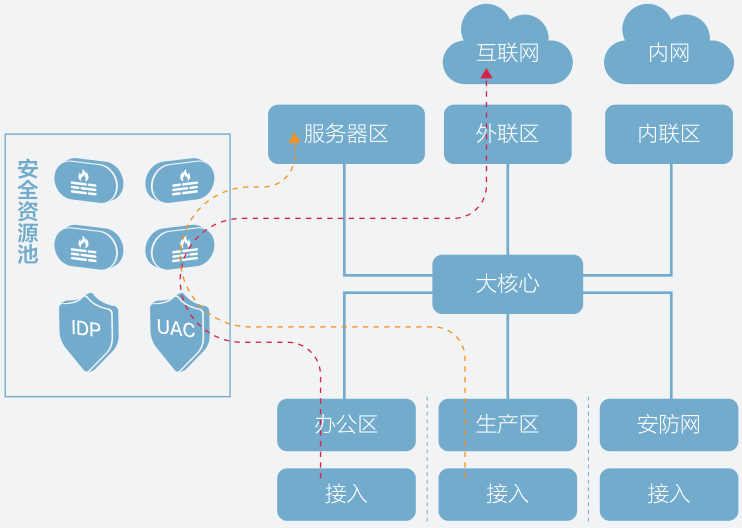
主干网络链路及设备均采用冗余部署

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

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

建设要点（三级）

等保要求	控制点	对应产品或方案
安全通信网络	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，启用安全过滤策略

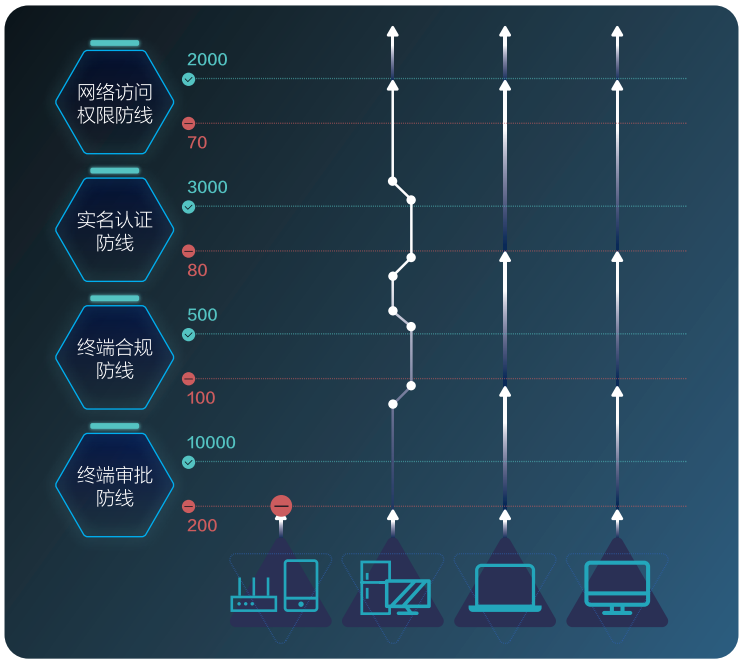
建立基于用户的身份认证与准入机制，启用安全审计策略

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

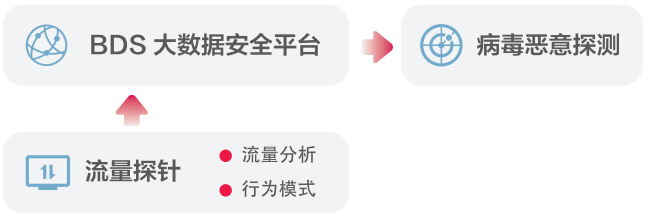
锐捷方案特色

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

基于网络行为的未知威胁检测



“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 RG-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。

4+1 未知威胁防御

除了最基础的各类设备日志，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。

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

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。

大数据安全态势感知

采集全网安全流量 + 日志信息，智能发现安全威胁

SDN 全网统一纳管

安全事件智能处置，联动全网将风险排除在边界

实名身份认证

全网统一实名身份认证体系，实现用户级事件响应

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

注：除红字部分外锐捷均可提供

锐捷方案特色

面向业务的多元身份聚合能力

● 密码、短信、APP、指纹……多重因素认证

● 基于用户组织统一灵活设置业务访问权限

● 单点登录，入网即认证，一次登录一网全通

与火绒安全达成合作
生态链合作产品融入锐捷整网安全体系

EDR 运营体系

- 全国唯一 EDR 运营体系
- 全网收集分析终端威胁情报，共享八百万用户情报分析能力

核心技术

- 深度融合“反病毒 + 主动防御 + 网络防火墙”
- 国内唯一“三合一”终端安全产品

产品成熟度

- 常规内存占用≤10M，CPU 占用≤3%
- 界面简洁，操作简单，几乎无弹窗，对用户打扰最少

服务能力

- 在线支持响应中心，30 分钟内答复客户支持问题
- 一对一客户建档，全程跟踪支持直至问题解决

● **等保2.0规范关键要求**

应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。

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

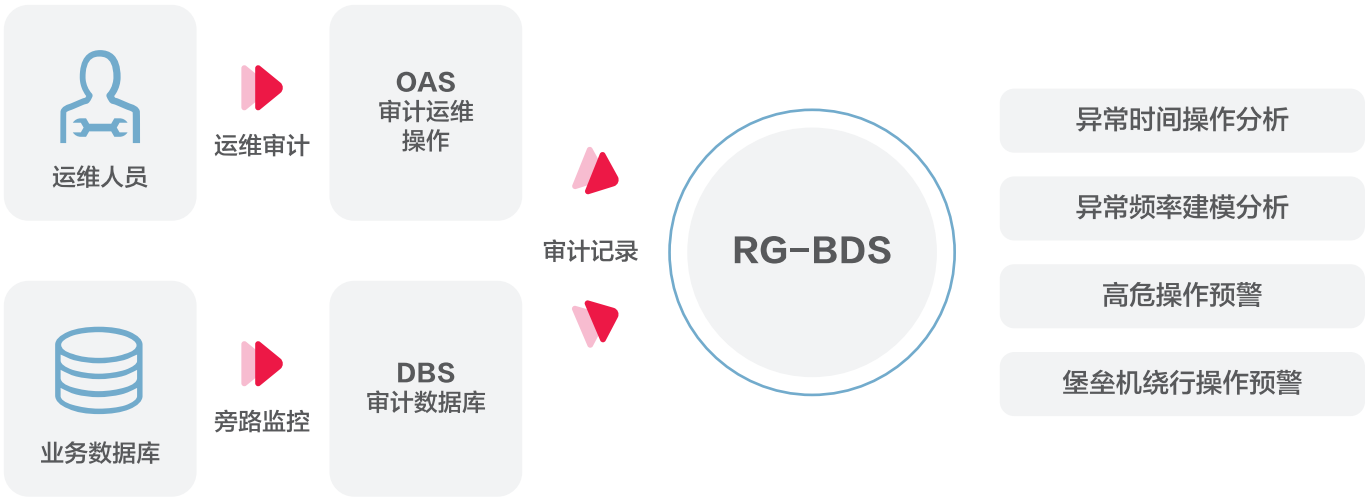
系统管理员、审计管理员、安全管理员权责清晰，三权分立

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

锐捷方案特色

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+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，分析黑客入侵路径，进行针对性加固 → 问题解决

锐捷等保2.0解决方案特色总结

1+N 全网安全

《网络安全等级保护》

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。

安全产品

完整的等保安全产品品类

01

02

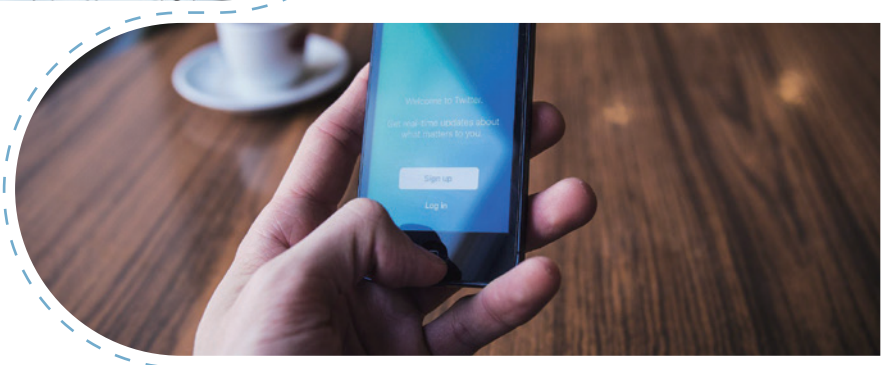
网络产品

提供基于SDN技术的网络安全支撑体系

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

03



04

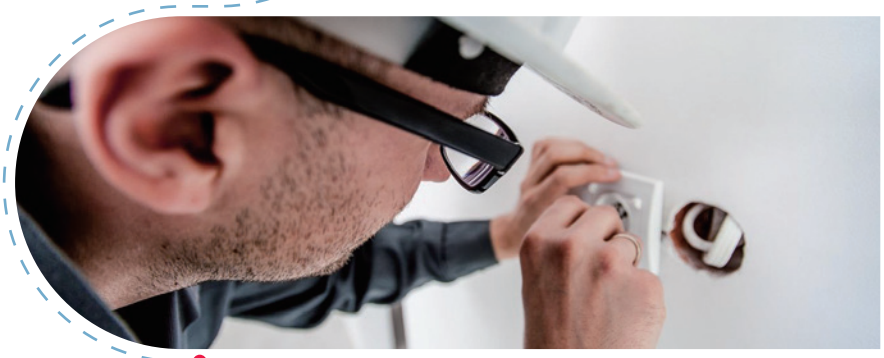
认证产品

用户身份+应用鉴权

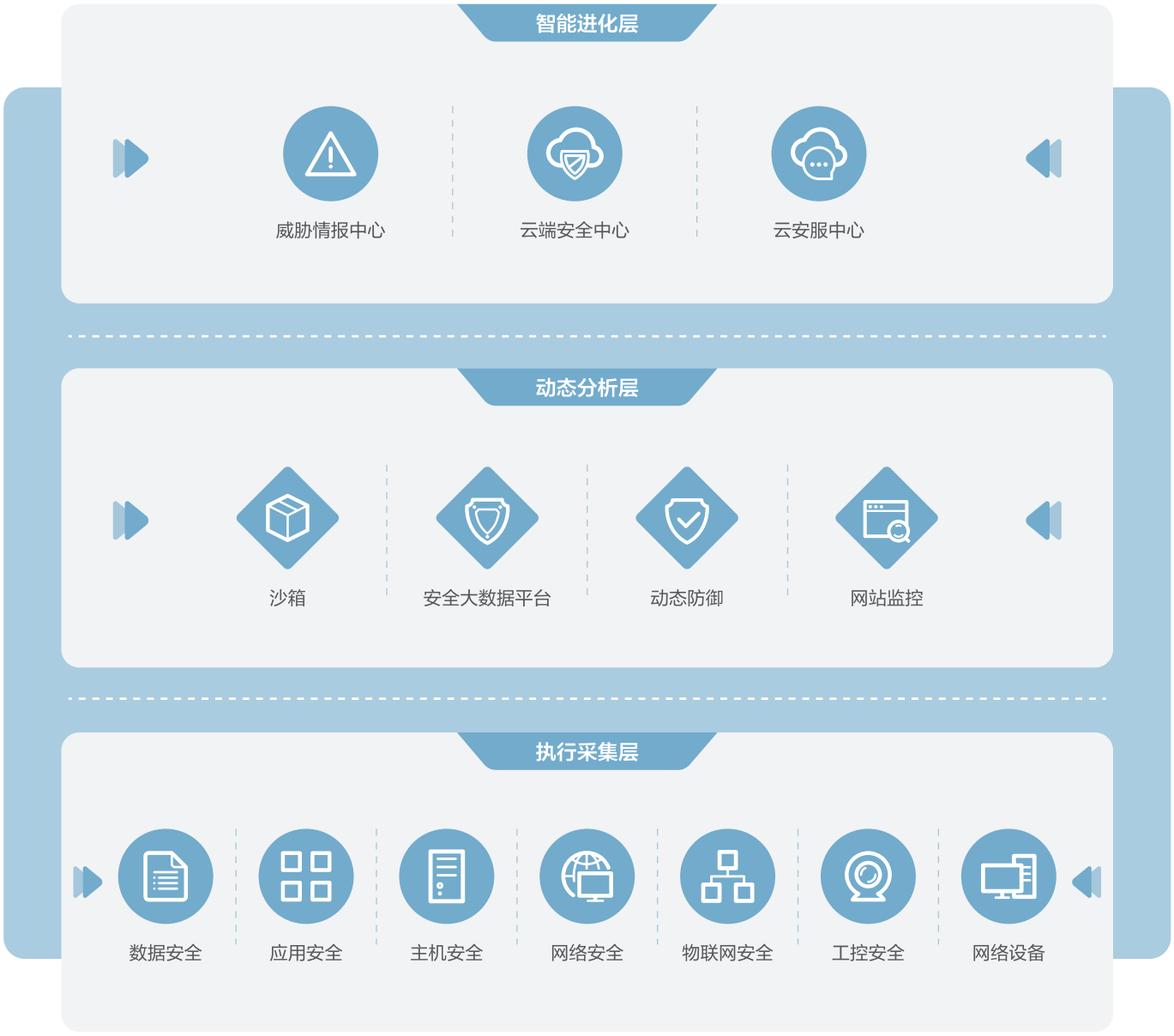
运维产品

IT运维管理的可靠支撑

05



锐捷方案整体架构：动态安全体系



智能进化层：
为“执行采集层”和“动态分析层”提供安全能力的持续增强，达成整网安全能力的可持续演进。

动态分析层：
对“执行采集层”提供的数据和信息进行分析，持续给出动态安全威胁和风险评估，让用户掌握整网最新安全状况，让“安全看的见”，必要时下发安全策略。

执行采集层：
执行网络所需的安全策略；采集各类日志、流量、文件等数据和信息供“动态分析层”分析。

变静态为动态，化被动为主动。

等保2.0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
01	防火墙	必备	必备	RG-WALL
02	入侵防御	必备	必备	RG-IDP或防火墙开启IPS功能
03	日志审计与集中管理	必备	必备	RG-BDS
04	渗透测试服务	可选	必备	渗透测试服务
05	漏洞扫描服务	必备	必备	漏洞扫描服务或RG-SCAN
06	堡垒机	必备	必备	RG-OAS
07	上网行为管理	必备	必备	RG-UAC
08	WAF应用防火墙	可选	必备	RG-WG
09	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	可选	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

等级保护实施过程

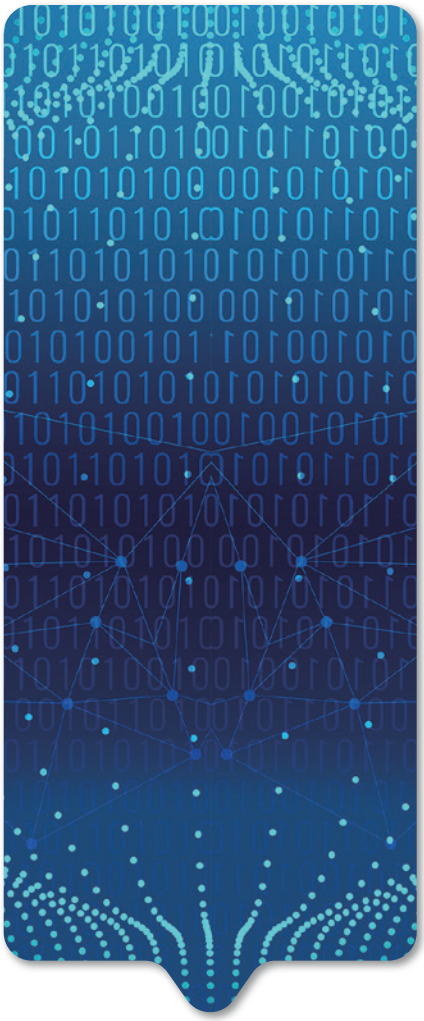
锐捷可提供等保全周期的安全咨询服务协助用户顺利通过测评。

系统定级

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

备案

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



建设整改

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

等级测评

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

监督检查

公安机关定期开展监督、检查、指导

Ruijie 锐捷
Networks

锐捷网络股份有限公司

欲了解更多信息，欢迎登录www.ruijie.com.cn，咨询电话：400-620-8818