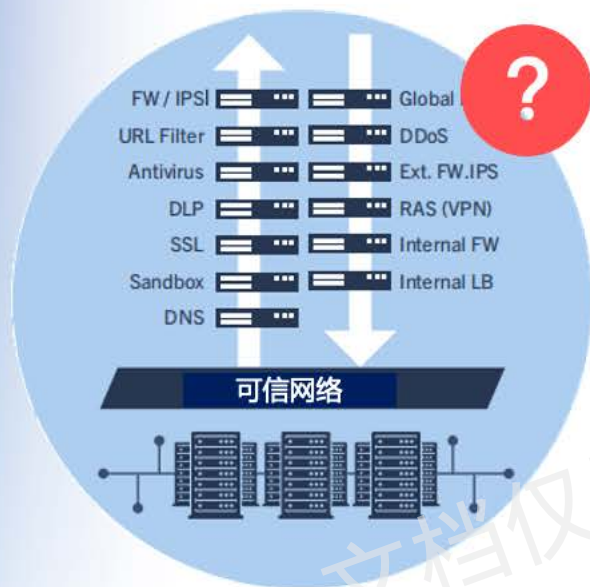


# 基于SASE的安全运营方案实践

北京瑞和云图科技有限公司

主讲人：董事长 周东



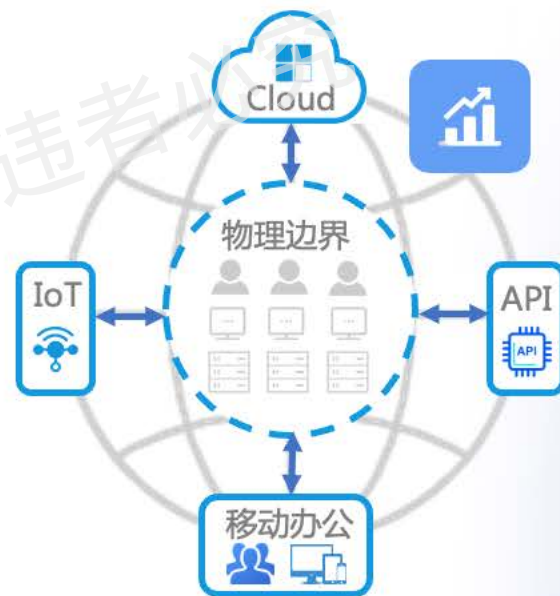
## 变革1：传统网络安全产品遇到挑战

网络环境不断复杂化，使传统网络安全环境、边界、通信等防护手段无法应对新型攻击，对防御的发现、响应和处置能力要求逐步提高。2020年HW行动中，VPN和传统安全设备0DAY漏洞频发。



## 变革2：传统网络安全边界消失

传统的物理网络安全边界消失，VPN、BYOD等提供了对于内部网络的不可信访问，APT攻击、勒索病毒等黑客技术的发展，带来了更多的安全风险，使得内网不再100%安全。



## 变革3：数字化转型升级

随着各行业数字化转型升级，云大物移智等新兴技术的应用使得IT基础架构发生根本性变化，平台、业务、用户、终端呈现多样化趋势，开放协同需求增加了数据的互联互通。

## 政策驱动

- 网络安全法、等保2.0等出台，安全无小事；
- 重要业务系统一旦出现网络安全问题，后果很严重；
- 来自上级主管、各级监管的考核要求。



## 安全事件层出不穷

- 2019年5月易到用车被巨额勒索
- 2017年11月天翼校园客户端携带后门病毒，众多校园网用户沦为挖矿肉鸡
- 伊朗核设施的震网APT攻击

## 安全建设投资大

- 企业网络安全的全面建设，需要十几种甚至几十种安全产品和方案；
- 大量安全产品的堆砌，大幅提升网络安全建设投资成本。

## 投入难有实效

- 安全应用投资80%在运维阶段；
- 安全相关知识，分析、调试、应急等均需要专业的安全人才；
- 2020年我国信息安全人才缺口140万人。



## 传统运营方式

安全产品堆叠

简单维护



- 安全产品堆叠
- 缺乏专业人员
- 无法安全联动
- 事件被动响应

## 云化安全一体运营服务

采集/阻断设备

云端服务



专业安全能力平台化，技能储备强、实操经验足的专家运维，借助云端平台实现高效服务交付

- 安全能力平台化，按需购买
- 7\*24安全运维，全量日志分析
- 主动发现基于流量全量安全问题
- 7\*24主动应急，威胁情报触发

科技发展强劲，安全和业务融合，**无边界安全**延生，风险防范要求持续走高  
网络安全正从“买硬件”转向“重实战”，“**云+边+端**”的防护能力升级  
满足合规要求的同时，维护业务动态安全，建立**安全运营中心**，动态全场景防护已成为趋势

## 成本降不下来

- 从客户买设备变成服务商提供设备，设备数量没有减少，硬性投入没有降低
- 从客户买人到服务商提供人，人力投入没有减少，大量的人力仍然需要到客户现场低效率消耗

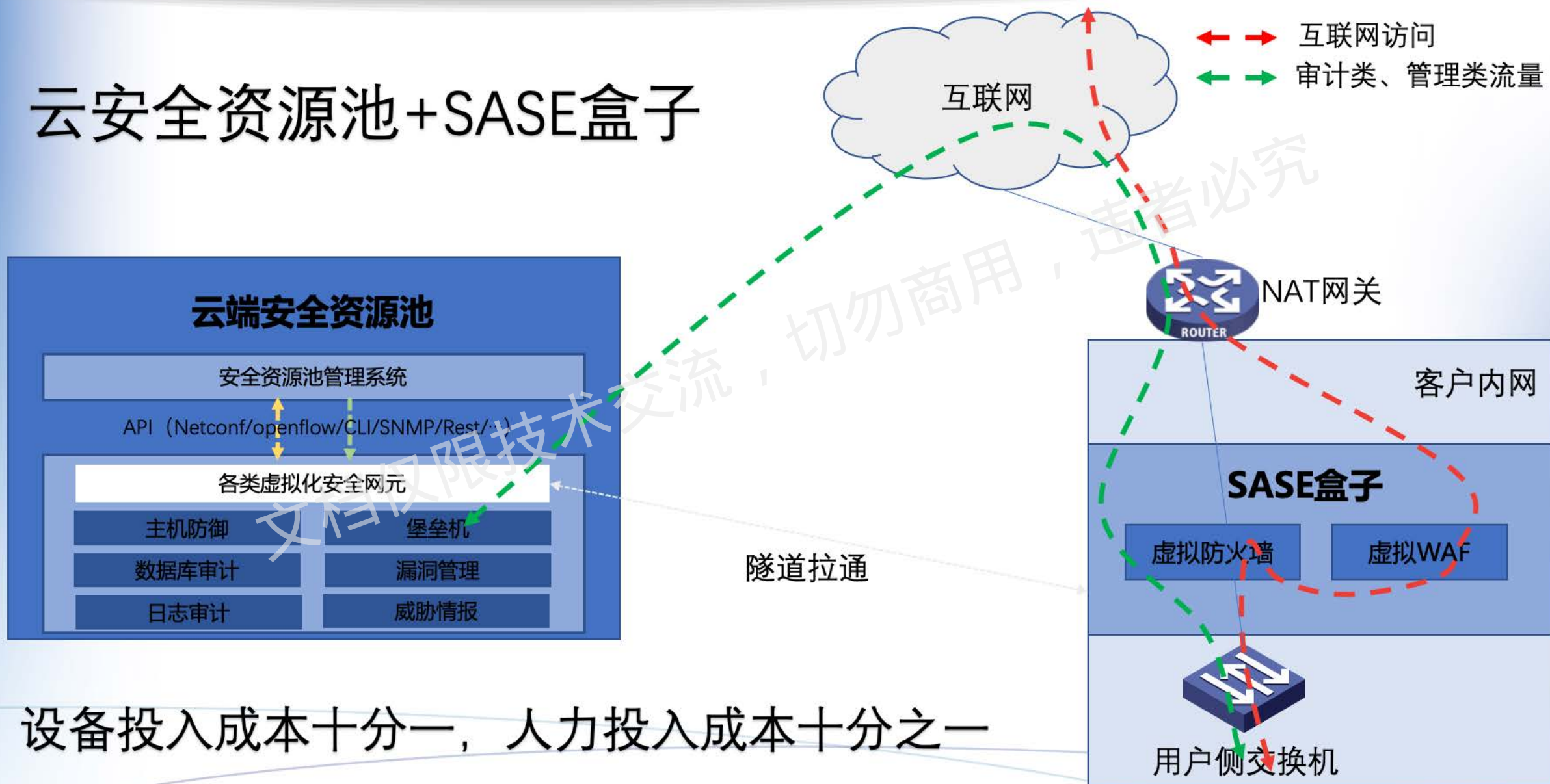
## 设备用不起来

- 设备的配置普遍不合理，很多功能没有真正发挥作用，无法捕获入侵攻击事件或者产生大量误报
- 整个安全防护体系的自动化程度低，不能让安全设备之间形成有效的协同联动和情报共享

## 解决问题能力低下

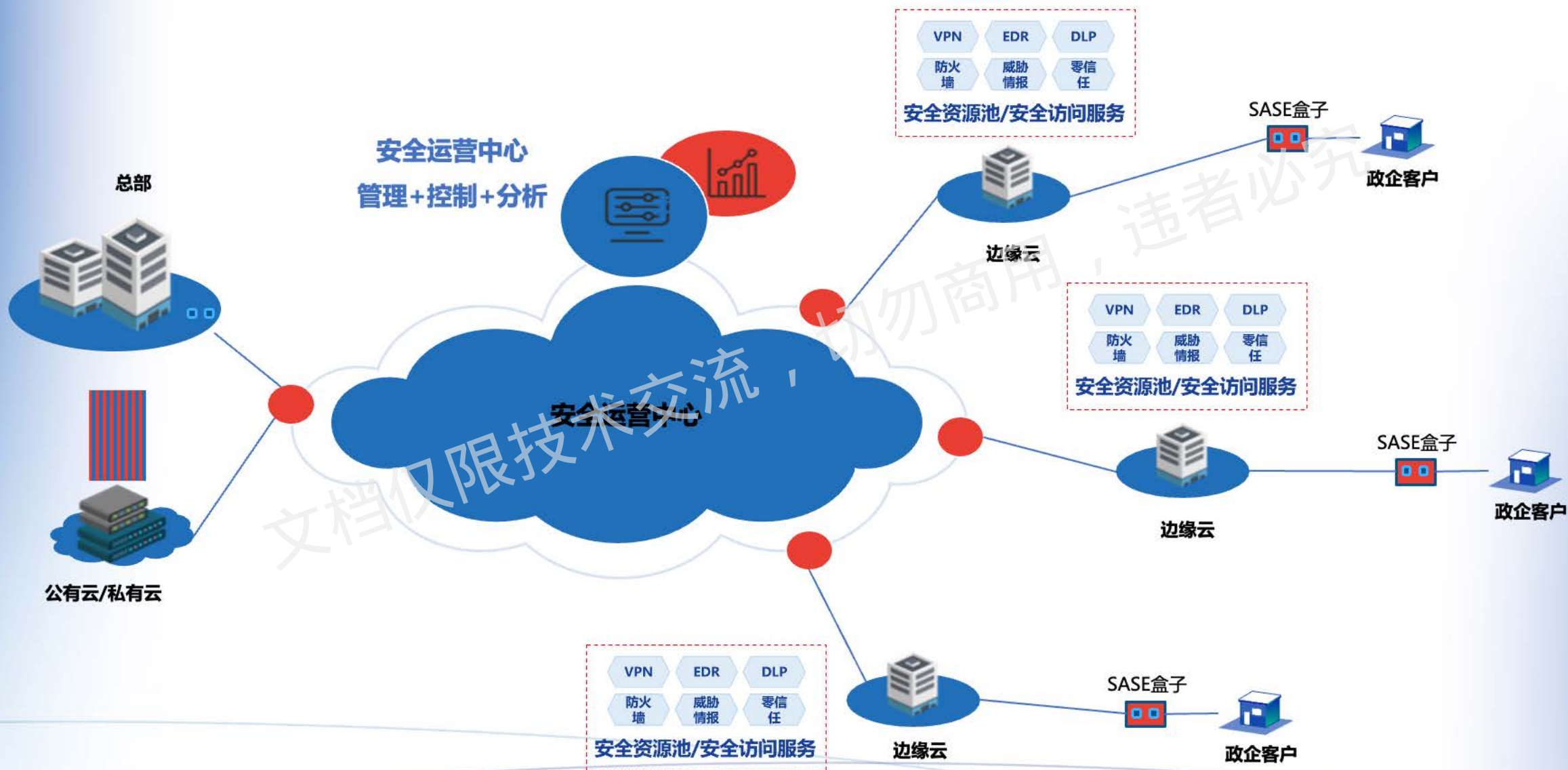
- 对安全事件缺少分析和处置的能力，面对大量安全告警不知道如何处置，更不具备处置高级安全威胁如APT和0day等攻击的能力
- 专业人员数量少，专业性不足、效率低下，不能保证能够输出安全分析结果和报告，无法及时对安全事件做出处置和响应

## 云安全资源池+SASE盒子



设备投入成本十分一，人力投入成本十分之一





## 云上安全能力

### 安全检测服务

#### 攻击检测服务

态势感知大屏服务

攻击日志服务

攻击检测周报服务

#### 漏洞扫描服务

漏扫周报服务

#### 流量分析服务

流量分析周报服务

### 安全防护服务

#### 防火墙服务

防火墙周报服务

#### IPS服务

IPS周报服务

#### 防病毒服务

防病毒周报服务

#### 上网行为管理和审计服务

上网行为管理和审计服务周报

#### WEB安全防护服务

WEB安全防护周报服务

#### 安全策略代维服务

### 其他增值服务

#### 抗DDOS服务

#### 网站安全监控服务

#### APT检测服务

#### 运维审计服务

#### 日志审计服务

#### 数据库审计服务

## 本地安全服务

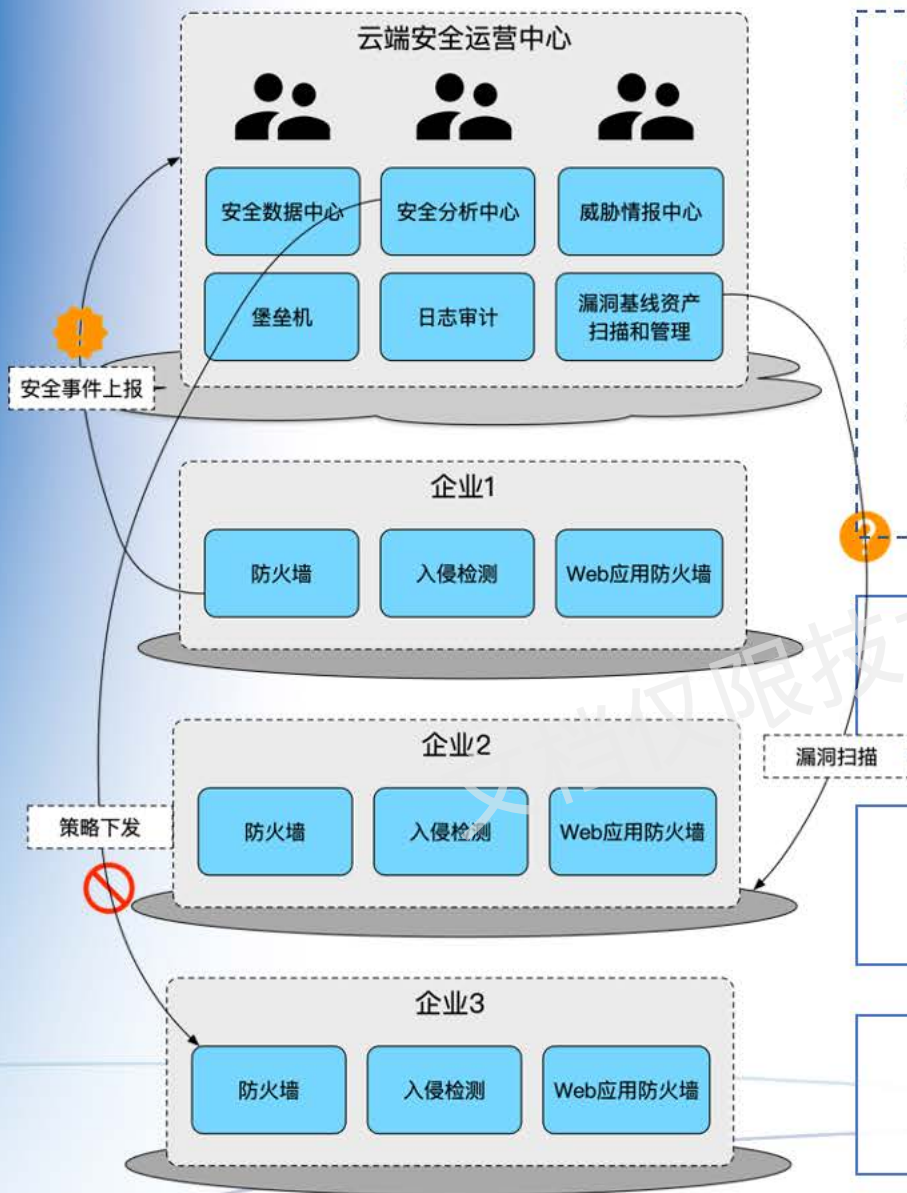
### 现场巡检服务

### 等级保护测评服务

### 安全培训服务

### 安全重保服务





## 安全运营的云服务模式解决了大规模安全运营的主要痛点

- 解决运营中心建设成本和运营成本问题：统一云端运营
- 解决人员成本问题：专业安全团队在云端提供专业的安全运营服务能力
- 解决安全设备成本问题：堡垒机、日志审计、资管漏管等SaaS化
- 解决高级安全分析系统的成本和使用门槛问题：由专业的安全团队来使用这些系统并向用户提供报告结果

### 扫描类安全产品和用户资产之间的一公里

- 堡垒机、漏洞扫描、基线核查等可SaaS化、云化部署的安全设备无法“看见”用户内网的网络和资产。

### 高级安全分析系统和安全事件数据之间的一公里

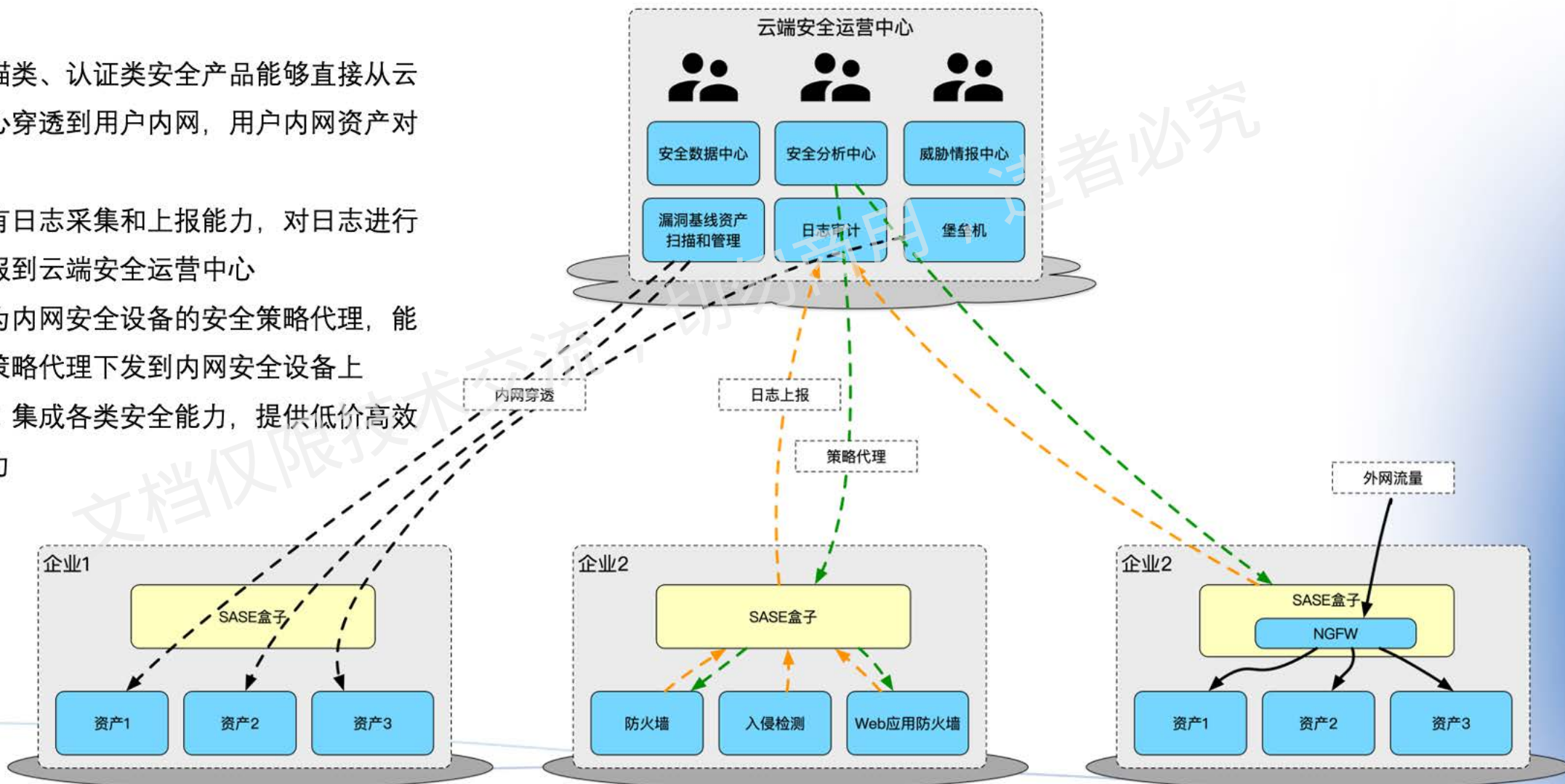
- 防火墙、入侵检测等安全设备产生了安全事件日志后无法送给部署在云端的态势感知、安全数据中心、高级安全分析中心等数据分析平台。

### 安全分析师、安全服务人员和防护类安全设备之间的一公里

- 在云端安全运营中心的安全分析人员通过安全研判做出处置结果后，无法把安全策略下发到安全设备上。

## 四大特性

- 内网穿透：扫描类、认证类安全产品能够直接从云端安全运营中心穿透到用户内网，用户内网资产对这些服务可见
- 日志上报：带有日志采集和上报能力，对日志进行加密压缩后上报到云端安全运营中心
- 策略代理：作为内网安全设备的安全策略代理，能够将云端安全策略代理下发到内网安全设备上
- 安全能力集成：集成各类安全能力，提供低价高效的安全防护能力

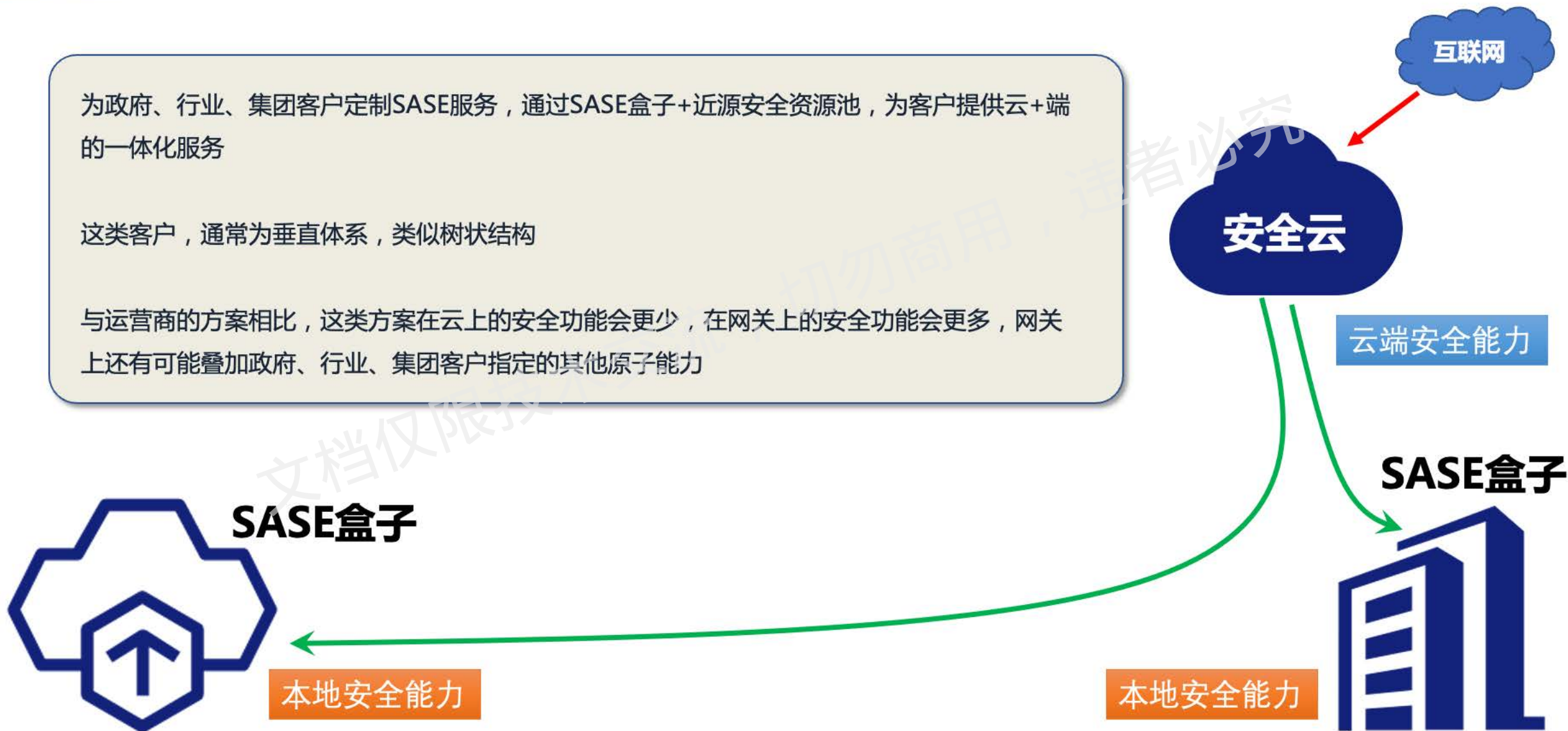




为政府、行业、集团客户定制SASE服务，通过SASE盒子+近源安全资源池，为客户提供云+端的一体化服务

这类客户，通常为垂直体系，类似树状结构

与运营商的方案相比，这类方案在云上的安全功能会更少，在网关上的安全功能会更多，网关上还有可能叠加政府、行业、集团客户指定的其他原子能力







- 一个机柜



## 安全业务编排功能



调度、编排、管理

## 安全原子能力池



## ● 软硬一体化

结构紧凑、场景化交付、各类安全产品  
统一高效管理

## ● 完备安全管理闭环

安全服务能力涵盖预防、防御、检测、  
处置等各环节

## ● 安全资源池化

高可用、快速部署、灵活扩展

## ● 一台2U/1U硬件



### 可视化安全集中管控界面

- 安全服务管理
- 安全态势感知
- 集中安全运维



二代防火墙



WAF



等级保护工具箱



主机安全



堡垒机



数据库审计



漏洞扫描



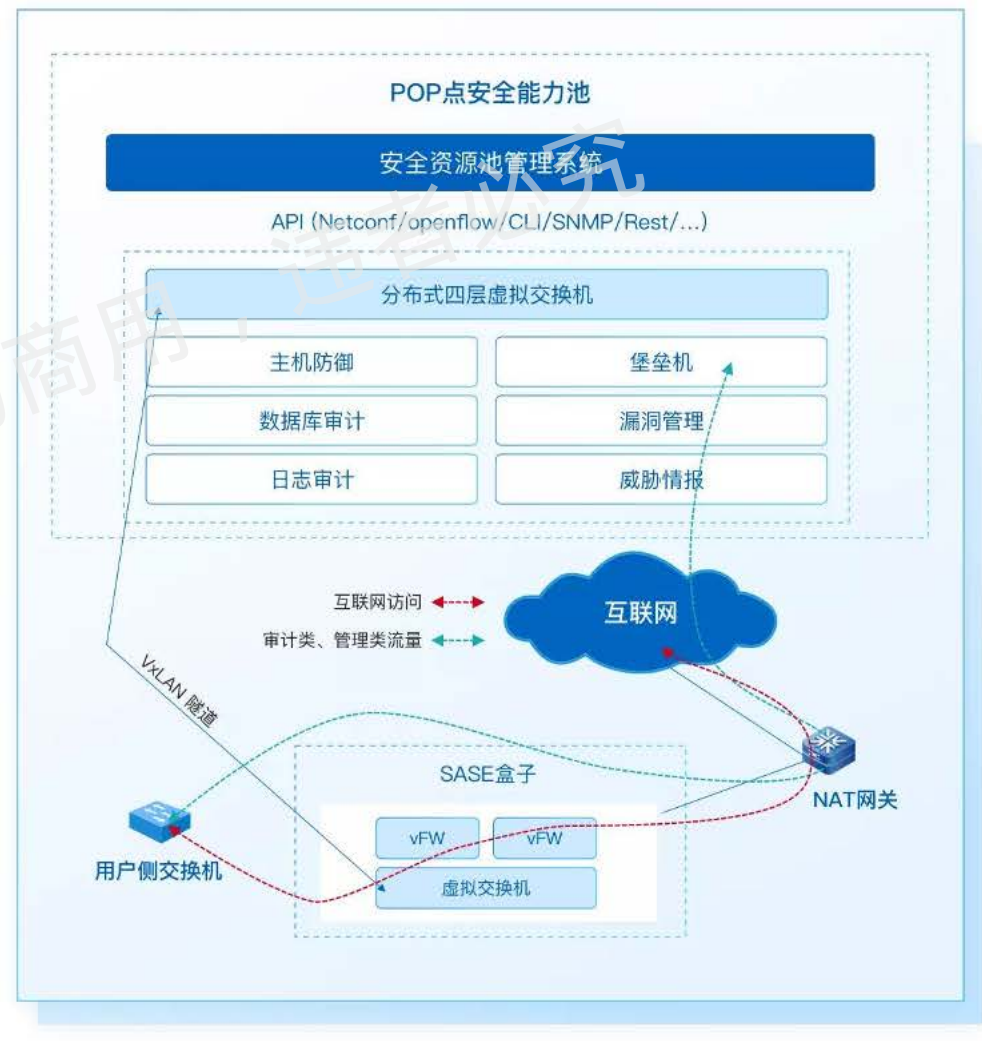
日志审计



SASE网关是一款安全接入边缘安全产品，采用标准硬件平台，提供丰富的安全接入能力，SASE网关与管理平台的所有通信都是加密的，包括防火墙、URL过滤、终端防护、病毒查杀和应用控制等防护功能都被集成到SASE终端硬件，通过分布广泛的POP点实现策略管理和所有边缘可用，并且相比传统架构，结构更加简单，更加安全，易于使用及维护。

## SASE网关解决方案亮点

- 软硬一体化交付，简化部署，透明部署，不改变用户现有网络；
- 业务上线简单，管理平台内置套餐、模板，业务快速开通；
- 高性能，多业务转发性能达千兆线速，无需引流，不增加带宽资源消耗；
- 高可靠性，透明部署，软件故障自动Bypass，不影响客户业务；
- 自身安全性保障，从SASE盒子到POP节点，所有管理、控制、监控等流量加密传输，保证传输安全可靠；
- SASE网关用户自主可控，SASE网关部署在用户侧，包括云端资源池安全能力，通过隧道打通，可以做到云端直接管理；







## 典型需求一：安全可视化

用户群体：

- 不懂安全，未部署任何安全措施（服务先给客户做体检）。
- 已部署了互联网边界安全设备，但是没有可视化手段。

随信息化程度  
加深，安全需  
求相应演进



## 典型需求二：需要边界安全

用户群体：

- 未部署边界安全设备（地市级以下客户普遍现象）
- 已部署边界安全设备但需要纵深防御（少量高端客户）

随信息化程度  
加深，安全需  
求相应演进






## 典型需求三：需要安全管控

用户群体：

- 网站有问题，被公安/网信办责令限期整改
- 关注上网行为，需对上网流量进行管控


## 1.安全监测套餐

-  专线攻击检测服务
-  专线流量分析服务
-  网站安全扫描服务



给用户做体检，让用户发现安全问题和隐患，用低价的方式吸引用户使用



## 2.基础安全防护套餐

-  专线防火墙服务
-  专线IPS服务
-  专线防病毒服务



含安全监测套餐，提供基础的安全防护能力，满足大部分用户普适性的安全需求

## 3.高级安全防护套餐

-  网站安全防护服务
-  专线上网行为审计服务



含安全监测套餐和基础防护套餐，提供高级安全防护能力，满足大部分用户更高的安全需求

## 态势感知

当前IP

VPC2021-呜呜

10.253.242.11

中国

全球

### 安全总评



### 当前威胁态势环比

708

今日攻击

0

昨日攻击

708

本周攻击

0

上周攻击

### 全部攻击类型 TOP5

详情 >



### 攻击源IP TOP5

详情 >

- 1. 1.15.98.178 (中国) 1
- 2. 1.169.26.29 (台湾.台北市) 1
- 3. 1.180.135.151 (内蒙古.乌海) 1
- 4. 1.197.170.4 (河南.南阳) 1
- 5. 1.57.163.130 (黑龙江.双鸭山) 1

### 漏洞



### 对外访问服务 TOP5

详情 >

暂无数据

### 安全评分变化

### 攻击趋势

24时

7天

30天

### 漏洞变化趋势

### 实时阻断攻击

详情 >

- 2021-08-08 21:57:32 病毒攻击 | 中  
攻击源IP: 113.215.119.53 (浙江)
- 2021-08-08 21:57:32 病毒攻击 | 中  
攻击源IP: 223.76.12.188 (湖北)
- 2021-08-08 21:57:32 病毒攻击 | 中  
攻击源IP: 106.93.64.243 (重庆)
- 2021-08-08 21:57:32 病毒攻击 | 中  
攻击源IP: 111.195.146.94 (北京)
- 2021-08-08 21:57:32 病毒攻击 | 中  
攻击源IP: 223.8.40.235 (山西)
- 2021-08-08 21:57:32 病毒攻击 | 中  
攻击源IP: 183.65.165.175 (重庆)
- 2021-08-08 21:57:32 病毒攻击 | 中  
攻击源IP: 60.165.170.170 (甘肃)

### 需要处理的威胁

详情 >

- 08-08 22:04:37 入侵攻击 | 中  
59.219.170.77
- 08-08 22:04:37 入侵攻击 | 中  
222.69.193.168
- 08-08 22:04:37 入侵攻击 | 中  
115.217.142.238



## 全局

1 资源池  
11 宿主机  
11 存活虚拟机  
8 模板  
3 租户  
3 供应商

## 运维告警

详情 >

## 运维认证

## 安全服务状态

NGFW	10.2.108.100	异常
NGFW	10.2.108.100	异常
Web应用防火	10.2.109.80	异常

## 全省CPU使用率-TOP 3

1 私有云11 0.00%

## 全省磁盘使用率-TOP 3

1 私有云 62.61%

## 全省内存使用率-TOP 3

1 私有云 73.08%

## 流量趋势变化

近一周

## 攻击趋势

近一周

异常包攻击

总流量 上行 下行

激活 Windows



运维大屏

资产池云管入口

资产

资产管理

资产类型

资源池

资源池管理

主机管理

虚拟机管理

安全实例分布

引流

镜像

安全网元镜像

供应商管理

系统

地址管理

平台配置

系统操作日志

## 主机管理

请选择资源类型 请选择省 请选择市 请选择资源池

主机

告警日志

请输入主机名称或...

检索

总资源池总量: 11 正常: 2 异常: 9 无流量: 0

新增主机

序号	主机IP	名称	位置	所属资源池	添加时间	主机状态	磁盘使用率	内存使用率	CPU使用率	当前拥有虚拟机	操作
1	10.2.109.64	10.2.109.64	福建省-	私有云11 (10.2.109.53)	2021-07-21 04:13:20	正常	74.03% (540G)	20.82% (503G)	14.10% (0核)	0	<a href="#">编辑</a> <a href="#">详情</a> <a href="#">网络配置</a>
2	10.2.3.4	jira3232222	福建省-福州市	私有云11 (10.2.109.53)	2021-07-22 01:53:32	异常	null% (nullG)	null% (nullG)	null% (0核)	0	<a href="#">编辑</a> <a href="#">详情</a> <a href="#">网络配置</a>
3	10.2.109.22	test1333	福建省-福州市	私有云11 (10.2.109.53)	2021-07-22 01:55:10	异常	null% (nullG)	null% (nullG)	null% (0核)	0	<a href="#">编辑</a> <a href="#">详情</a> <a href="#">网络配置</a>
4	10.2.108.100	安博通防火墙	福建省-福州市	私有云11 (10.2.109.53)	2021-07-22 02:17:05	异常	null% (nullG)	null% (nullG)	null% (0核)	0	<a href="#">编辑</a> <a href="#">详情</a> <a href="#">网络配置</a>
5	10.2.2.222	绿盟waf	福建省-福州市	私有云11 (10.2.109.53)	2021-07-22 02:44:28	异常	null% (nullG)	null% (nullG)	null% (0核)	0	<a href="#">编辑</a> <a href="#">详情</a> <a href="#">网络配置</a>
6	10.2.109.80	绿盟waf1	福建省-福州市	私有云11 (10.2.109.53)	2021-07-22 02:46:22	异常	null% (nullG)	null% (nullG)	null% (0核)	0	<a href="#">编辑</a> <a href="#">详情</a> <a href="#">网络配置</a>
7	10.2.109.36	http://10.2.109.36/		私有云11 (10.2.109.53)	2021-07-21 04:06:23	异常	null% (nullG)	null% (nullG)	null% (0核)	0	<a href="#">编辑</a> <a href="#">详情</a> <a href="#">网络配置</a>
8	10.2.5.100	abt防火墙		私有云11 (10.2.109.53)	2021-07-27 01:56:01	异常	null% (nullG)	null% (nullG)	null% (0核)	0	<a href="#">编辑</a> <a href="#">详情</a> <a href="#">网络配置</a>
9	10.10.1.156	堡垒机		私有云11 (10.2.109.53)	2021-07-27 02:04:30	异常	null% (nullG)	null% (nullG)	null% (0核)	0	<a href="#">编辑</a> <a href="#">详情</a> <a href="#">网络配置</a>
10	10.23.3.44	23213		私有云11 (10.2.109.53)	2021-08-04 09:53:20	异常	null% (nullG)	null% (nullG)	null% (0核)	0	<a href="#">编辑</a> <a href="#">详情</a> <a href="#">网络配置</a>

运维大屏

资产池云管入口

资产

资产管理

资产运营

资源池

资源池管理

宿主机管理

虚拟机管理

安全实例分布

引流

镜像

安全网元镜像

供应商管理

系统

地址管理

平台配置

系统操作日志

防火墙策略

策略

上网行为审计

日志分析

服务信息

1 第一步 配置防火墙策略

2 第二步 配置安全防护策略

下一步

1. 配置地址对象

2. 配置服务对象

3. 配置防火墙策略

新增

名称	地址	排除地址	描述	引用次数	操作
1221	12.22.3.3			1	删除
地址对象1	133.2.33.2			3	删除
22222	222.22.2.2		2222	0	编辑 删除
测试名称1	172.10.1.28		dfd	0	编辑 删除

共 4 条 < 1 > 10 条/页

文档仅限技术交流，切勿商用，违者必究

Copyright © 2019-2021 5G+云化安全能力平台

## 新建安全服务

安全服务列表

新建安全服务实例



### NGFW

二代防火墙，提供访问控制、入侵防御、防病毒、上网行为管理、应用流量控制等安全能力。

- |                   |       |
|-------------------|-------|
| • 全功能开启吞吐量200Mbps | 年/0 点 |
| • 全功能开启吞吐量400Mbps | 年/0 点 |
| • 全功能开启吞吐量600Mbps | 年/0 点 |
| • 全功能开启吞吐量800Mbps | 年/0 点 |
| • 全功能开启吞吐量1Gbps   | 年/0 点 |

新建安全服务实例

下载手册



### 系统漏洞扫描

针对服务器、操作系统、网络设备、中间件、数据库等执行漏洞扫描，发现资产脆弱性，帮助识别和控制资产风险。

- |               |       |
|---------------|-------|
| • 20个IP的扫描授权  | 年/0 点 |
| • 40个IP的扫描授权  | 年/0 点 |
| • 60个IP的扫描授权  | 年/0 点 |
| • 80个IP的扫描授权  | 年/0 点 |
| • 100个IP的扫描授权 | 年/0 点 |

新建安全服务实例

下载手册



### 主机EDR

针对PC终端，提供病毒查杀、主动威胁防护，并可针对PC终端执行集中策略配置、安全报表查看等。

- |                           |       |
|---------------------------|-------|
| • 2个Linux授权，10个Windows授权  | 年/0 点 |
| • 4个Linux授权，20个Windows授权  | 年/0 点 |
| • 6个Linux授权，30个Windows授权  | 年/0 点 |
| • 8个Linux授权，40个Windows授权  | 年/0 点 |
| • 10个Linux授权，50个Windows授权 | 年/0 点 |

新建安全服务实例

下载手册



### 数据库审计

针对服务器、操作系统、网络设备、中间件、数据库等执行漏洞扫描，发现资产脆弱性，帮助识别和控制资产风险。

- |                |       |
|----------------|-------|
| • 1个数据库实例的审计授权 | 年/0 点 |
| • 2个数据库实例的审计授权 | 年/0 点 |
| • 3个数据库实例的审计授权 | 年/0 点 |
| • 4个数据库实例的审计授权 | 年/0 点 |
| • 5个数据库实例的审计授权 | 年/0 点 |

新建安全服务实例

下载手册



### 堡垒机

对运维行为提供4A管理（账号管理、身份鉴别、授权管理、安全审计），对运维风险进行控制。

- |            |       |
|------------|-------|
| • 20个资产授权  | 年/0 点 |
| • 40个资产授权  | 年/0 点 |
| • 60个资产授权  | 年/0 点 |
| • 80个资产授权  | 年/0 点 |
| • 100个资产授权 | 年/0 点 |

新建安全服务实例

下载手册



### 日志审计

对数据中心内的各类IT组件进行集中的日志采集，归并处理，集中存储。在进行事故处理时提供必要的记录。

- |             |       |
|-------------|-------|
| • 20个日志源授权  | 年/0 点 |
| • 40个日志源授权  | 年/0 点 |
| • 60个日志源授权  | 年/0 点 |
| • 80个日志源授权  | 年/0 点 |
| • 100个日志源授权 | 年/0 点 |

新建安全服务实例

下载手册



### Web应用防火墙

集WEB防护、网页保护、负载均衡、应用交付于一体，事前主动防御，智能分析应用缺陷、屏蔽恶意请求、防范网页篡改、阻断应用攻击，全方位保护WEB应用。

- |                   |       |
|-------------------|-------|
| • 全功能开启吞吐量200Mbps | 年/0 点 |
| • 全功能开启吞吐量400Mbps | 年/0 点 |
| • 全功能开启吞吐量600Mbps | 年/0 点 |
| • 全功能开启吞吐量800Mbps | 年/0 点 |



### 主机防病毒

可通过中央主控制中心对网络内的服务器、客户机进行远程策略设置、病毒查杀、远程安装等各种管理操作，实现跨地区、跨平台的网络防病毒系统实施统一管理和监控。

- |                          |       |
|--------------------------|-------|
| • 2个Linux授权，10个Windows授权 | 年/0 点 |
| • 4个Linux授权，20个Windows授权 | 年/0 点 |
| • 6个Linux授权，30个Windows授权 | 年/0 点 |
| • 8个Linux授权，40个Windows授权 | 年/0 点 |



### IPS

可以对漏洞攻击、蠕虫病毒、间谍软件、木马后门、溢出攻击、数据库攻击、高级威胁攻击、暴力破解等多种深层攻击行为进行防御，有效弥补网络层防护产品深层防御效果的不足。

- |                   |         |
|-------------------|---------|
| • 全功能开启吞吐量500Mbps | 3年/10 点 |
|-------------------|---------|





已付款: 26

已完成: 216

全部订单: 242

开始日期 ~ 结束日期

全部服务

租户账号、订单号

搜索

序号	下单时间	购买服务	服务规格	数量	单价/元	订单金额/元	服务申请	付款方式	订单号	操作
1	2021/07/27 - 16:11	NGFW	全功能开启吞吐量1Gbps/1年	1	0	0	服务申请	线下付款	N202107271611158678410002	<a href="#">拒绝</a> <a href="#">同意</a>
2	2021/07/26 - 11:39	NGFW	全功能开启吞吐量1Gbps/1年	1	0	0	服务申请	线下付款	N202107261139272934390001	<a href="#">拒绝</a> <a href="#">同意</a>
3	2021/07/23 - 11:02	NGFW	全功能开启吞吐量1Gbps/1年	1	0	0	服务申请	线下付款	N202107231102057893310006	<a href="#">拒绝</a> <a href="#">同意</a>
4	2021/07/23 - 09:24	NGFW	全功能开启吞吐量1Gbps/10年	1	0	0	服务申请	线下付款	N202107230924145969880003	<a href="#">拒绝</a> <a href="#">同意</a>
5	2021/07/16 - 15:30	安全盒子	全功能开启吞吐量200Mbps/3年	1	10	30	服务申请	线下付款	N202107161530024657160010	<a href="#">拒绝</a> <a href="#">同意</a>
6	2021/07/16 - 15:29	主机EDR	10个Linux授权, 50个Windows授权/1年	1	0	0	服务申请	线下付款	N202107161529316951160008	<a href="#">拒绝</a> <a href="#">同意</a>
7	2021/07/16 - 15:28	数据库审计	5个数据库实例的审计授权/1年	1	0	0	服务申请	线下付款	N202107161528513706160006	<a href="#">拒绝</a> <a href="#">同意</a>
8	2021/07/16 - 15:27	NGFW	全功能开启吞吐量1Gbps/1年	1	0	0	服务申请	线下付款	N202107161527137559820004	<a href="#">拒绝</a> <a href="#">同意</a>
9	2021/06/21 - 10:47	系统漏洞扫描	20个IP的扫描授权/1年	1	10	10	服务申请	线下付款	N202106211047387145040014	<a href="#">拒绝</a> <a href="#">同意</a>
10	2021/06/21 - 10:47	系统漏洞扫描	20个IP的扫描授权/1年	1	10	10	服务申请	线下付款	N202106211047130922560013	<a href="#">拒绝</a> <a href="#">同意</a>

## 攻击检测总览

选择租户和网络: VPC2021-嘟嘟 10.253.242.6

攻击检测总览

攻击日志

统计周期: 近30天 近7天 近24时

### 攻击统计



0

异常包攻击

日志



204

扫描攻击

日志



0

入侵攻击

日志



0

病毒攻击

日志



3

WEB攻击

日志

### 各IP受攻击类型分布

全部





## 安全防护总览

选择租户和网络: VPC2021-呜呜 10.253.242.11

安全防护总览

阻断日志

统计周期: 近30天 近7天 近24小时

### 网元防护统计

1021  
防火墙

0  
IPS

0  
WAF

0  
漏洞数量(昨日)

### 防护分类统计

1021  
防护病毒攻击

0  
入侵攻击

0  
防护非法访问

2236  
异常包攻击  
(非阻断数据)

1200  
扫描攻击  
(非阻断数据)

### 防护服务态势

访问拦截

Web防护

www.aaa.com

拦截分时态势

非法访问IP-TOP5

拦截访问目标-TOP5

防护分时态势

安全工作台

态势大屏

攻击检测总览

出城流量总览

安全防护总览

选择租户和网络: ip段-IP段 租户下全部IP统计及每个IP

出城流量统计 出城应用流量统计

统计周期: 近30天 近7天 近24小时

分类应用流量统计



各应用流量统计

应用名称: 请输入应用 检索

应用名称	上行流量	下行流量	总流量
其他TCP	2.21K	2.21K	4.42K
其他UDP	0.00K	0.00K	0.00K



安全网关

主页

数据中心

策略配置

安全中心

网络配置

系统管理

入侵防御

病毒防护

安全防护

ARP攻击防护

异常包攻击防护

DoS攻击防护

防暴力破解

弱密码防护

非法外联防护

WEB防护

风险扫描

入侵防御 > 入侵防御配置

入侵防御配置

+ 新建

	名称	描述	防护等级	操作
1	All	最大事件集	低	<a href="#">编辑</a> <a href="#">删除</a> <a href="#">复制</a>
2	Common	常规事件集	低	<a href="#">编辑</a> <a href="#">删除</a> <a href="#">复制</a>
3	Application	应用事件集	低	<a href="#">编辑</a> <a href="#">删除</a> <a href="#">复制</a>
4	Attack	攻击事件集	低	<a href="#">编辑</a> <a href="#">删除</a> <a href="#">复制</a>
5	2		高	<a href="#">编辑</a> <a href="#">删除</a> <a href="#">复制</a>
6	防火墙保护者1号		低	<a href="#">编辑</a> <a href="#">删除</a> <a href="#">复制</a>

All -- 3776条

+ 添加事件 分类 安全类型 名称 启用 全部 级别 全部 日志 全部 动作 任何 查询

名称	级别	启用	日志	动作	操作
安全漏洞(1142)	-	✓	✓	-	<a href="#">编辑</a> <a href="#">删除</a> <a href="#">复制</a>
CGI攻击(209)	-	✓	✓	-	<a href="#">编辑</a> <a href="#">删除</a> <a href="#">复制</a>
缓冲溢出(809)	-	✓	✓	-	<a href="#">编辑</a> <a href="#">删除</a> <a href="#">复制</a>
木马后门(657)	-	✓	✓	-	<a href="#">编辑</a> <a href="#">删除</a> <a href="#">复制</a>
可疑行为(82)	-	✓	✗	-	<a href="#">编辑</a> <a href="#">删除</a> <a href="#">复制</a>
CGI访问(423)	-	✓	✓	-	<a href="#">编辑</a> <a href="#">删除</a> <a href="#">复制</a>
拒绝服务(145)	-	✓	✓	-	<a href="#">编辑</a> <a href="#">删除</a> <a href="#">复制</a>
网络数据库攻击(46)	-	✓	✓	-	<a href="#">编辑</a> <a href="#">删除</a> <a href="#">复制</a>