

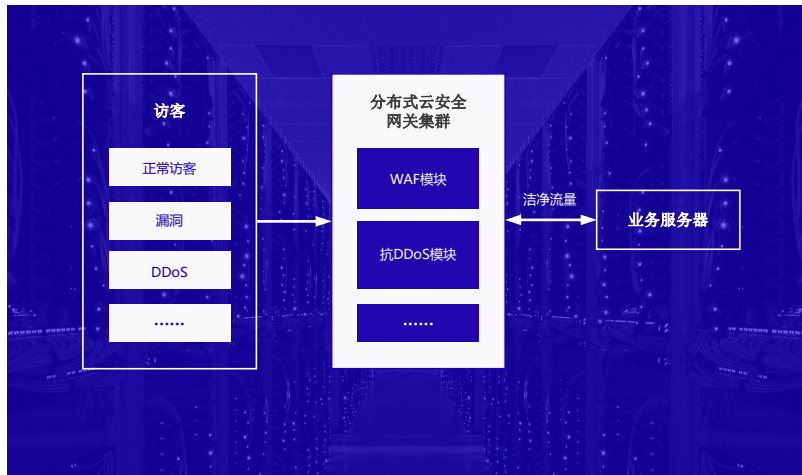
云原生应用零信任实践

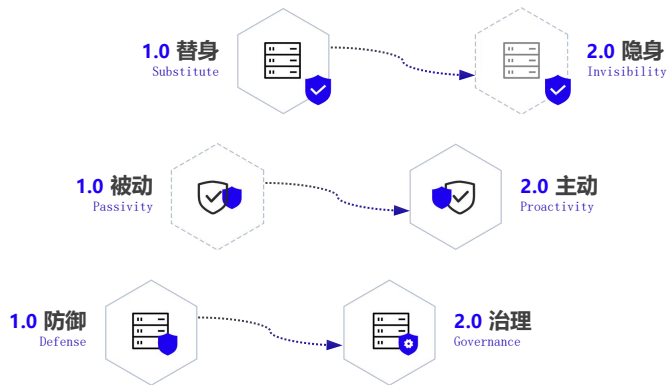
上海云盾信息技术有限公司

主讲：胡金涌（CTO）

1、主张替身安全

2、隐藏被保护对象，针对源 实现了替身式云防护





Emergence of Software Defined Perimeters (SDP)

1. 网络隐身(Information Hiding):

隐藏服务器地址、端口，无法被扫描发现

2. 预验证 (Pre-authentication):

在连接应用之前，先验证用户和设备的可信性

3. 预授权(Pre-authorization):

最小粒度授权，终端只能看到被授权访问的应用

4. 应用级的访问控制(Application Layer Access):

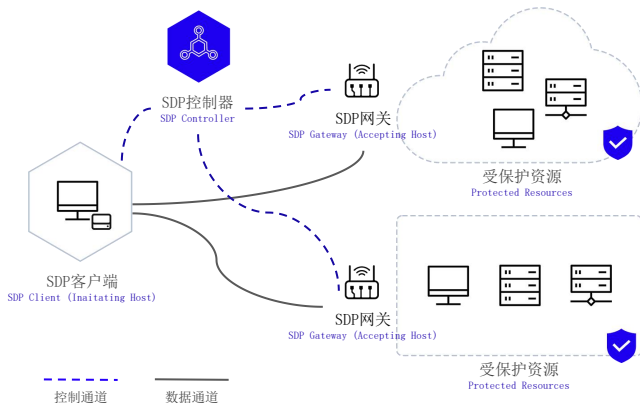
用户只有应用层的访问权限，无网络级的访问权限

5. 可视化(Visualization):

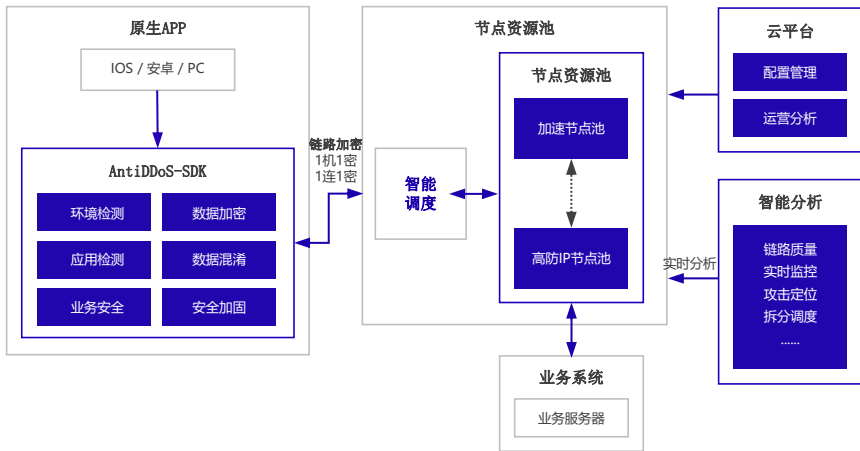
策略可视化、流量行为可视化

6. 扩展性(Extensibility):

基于标准协议，易与其它安全系统集成



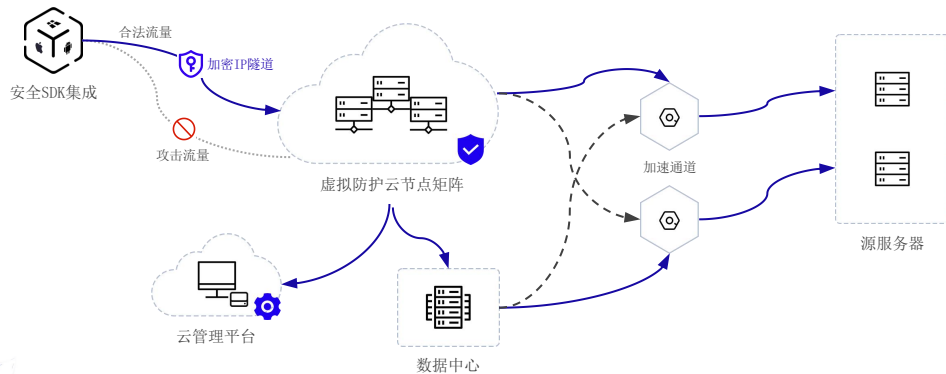
1. 以全新算法、终端风险检测、大数据分析技术、海量分布式节点为基础，游戏、金融、电商等行业的APP应用推出的端安全解决方案
2. 通过SDK端环境的信息收集、决策、调度等手段，与黑客在DDoS攻防上再也不是硬碰硬。基于数据，可以通过动态调度策略动态将黑客隔离，让黑客找不到攻击目标



YUNDUN基于零信任的抗D方案架构

AntiDDoS Solutions Architecture

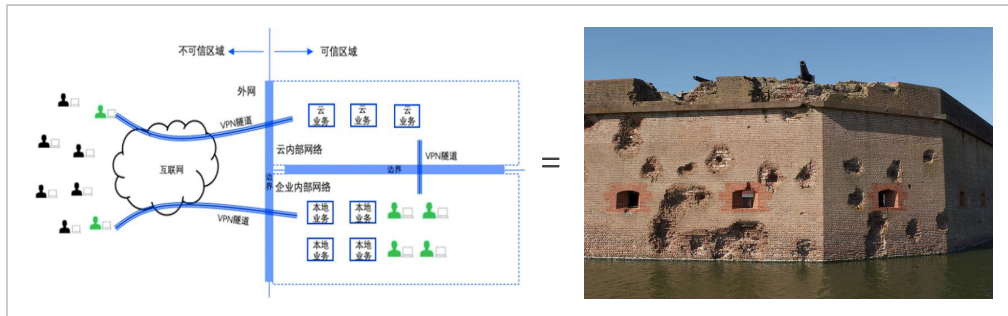
www.yundun.com



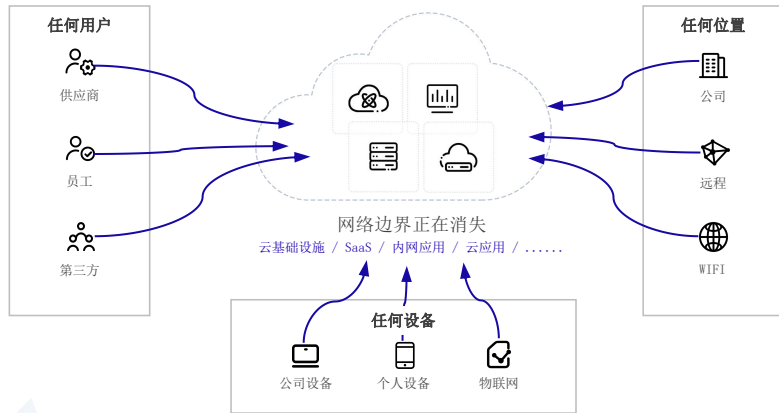
以为只要筑起城墙，城墙足够的深厚就可以抵御威胁

传统模式的问题

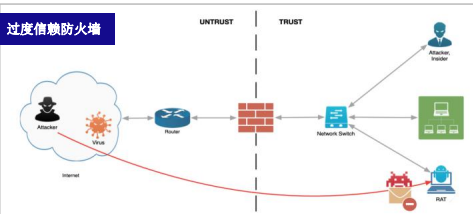
无法应对场景、攻击武器和战术不断变化



移动办公、远程访问等形式突破了企业的物理网络边界，边界消失已经成为必然



企业同时面临这安全与效率的双重挑战



业务上云后，攻击面积扩大



档案系统



邮件系统



财务系统



OA系统

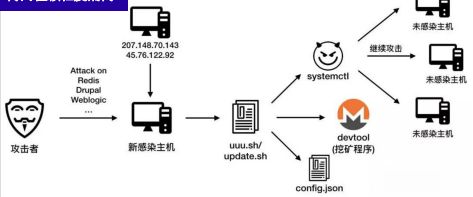


审批系统



办公系统

内网粗颗粒度隔离



内部安全问题：弱口令/敏感数据泄露

全球数据泄露事件统计

泄露事件	泄露日期	泄露数据类型	泄露用户数量
MySpace数据泄露	2008年数据泄露 / 2015年数据泄露	网络公司	2.4亿
LinkedIn数据泄露	2012年	招聘和社交平台	1.7亿
VK.com数据泄露	2012年数据泄露 / 2015年数据泄露	社交平台	9400万
Kayak数据泄露	2012年	旅行服务公司	150万
Replayr.com数据泄露	2012年	成人内容提供商	140万
Myapp数据泄露	2012年	社交应用程序	200万
23andMe数据泄露	2012年	基因检测	500万
Ku!ra!数据泄露	2012年	黑客论坛	80万
Phone.me数据泄露	2012年	电话号码目录	220万
Avira! Webmail数据泄露	2012年	成人内容网站	2000万
Bank of America数据泄露	2012年	银行数据	5万
ESurance数据泄露	2012年	国外保险代理	120万
Vindex数据泄露	2012年	成人内容网站	400万
Adult Friend Finder数据泄露	2012年	成人内容网站	70万
MyWay数据泄露	2012年	搜索引擎	110万
Reel! Hot! Photo数据泄露	2012年	成人内容网站	200万
OnDemand数据泄露	2012年	成人内容网站	1.5万
Shutterstock数据泄露	2012年	设计平台	400万
Mail.com数据泄露	2012年	邮件服务提供商	400万
Forums数据泄露	2012年	论坛平台	100万
Audio数据泄露	2012年	音频平台	400万
Adobe Photoshop数据泄露	2012年	软件服务提供商	1.5万

中国互联网用户常用弱口令排行

1	123456	16	1234	31	qazwsx@	48	001122	61	andrew	79	qaz123
2	123456789	17	12345678	32	asdfgh	49	100000	62	1a1b1c1d	77	456789
3	111111	18	qazwsx@123	33	123456789	50	11111111	63	123456789	78	aaaaaa
4	123123	19	123123123	34	00000000	51	123456	64	asdfgh	79	11111111
5	000000	20	004321	35	88888888	52	qq123456	65	123456789	80	and123
6	12345678	21	147258369	36	asdfghjkl	53	123456789	66	000000	81	0000000000
7	123456789	22	password	37	123456	54	77777777	67	123456789	82	456789
8	00011111	23	888888	38	123456	55	111111	68	123456789	83	000123456
9	1234567	24	7777777	39	147258	56	180000	69	000001	84	163.com
10	123321	25	123	40	551514	57	222222	70	12345678910	85	333333
11	112233	26	112233	41	qwerty	58	789456	71	123456789	86	123456
12	11111111	27	aaaaaa	42	111111	59	000000	72	000000	87	221214
13	12341234	28	12345678	43	77777777	60	0123456789	73	00000000	88	0000000000
14	00000000	29	123456	44	121212	61	199199	74	1111	89	0001408
15	33333333	30	001054321	45	123456789	62	999999	75	111222	90	0001408

安全问题

www.yundun.com

一场疫情改变了我们的工作模式

居家隔离告知书

尊敬的居民朋友：

配合做好疫情防控工作关乎您和家人及全社会的健康，是每一位公民应承担的责任和义务。2020年2月1日，本公寓一位住户经新型冠状病毒检测阳性，存在很大的传染风险。为最大限度阻断疫情传播，保障居民人身安全，按照《中华人民共和国传染病防治法》及《自治区新型冠状病毒感染的肺炎疫情防控工作方案》等相关规定要求，自2020年2月1日起至2020年2月14日，需对本公寓居民实施隔离。特殊情况由不得外出。

上海市：

1月27日，上海市发布《上海市人民政府关于延迟本市企业复工和学校开学的通知》，要求本市区域内各类企业不早于2月9日24时前复工。

重庆市：

1月29日，重庆市新型冠状病毒感染的肺炎疫情防控工作领导小组办公室发布通知，明确本市各类企业复工、复产时间不得早于2020年2月9日24时。

河北省：

1月30日，河北省发布《关于延迟企业复工复业的通知》要求，河北省行政区域内企业复工复业时间不得早于2020年2月9日24时。

远程办公通知

为深入贯彻落实中央、省委、省政府关于疫情防控工作要求，确保疫情防控工作顺利开展，现就远程办公有关事项通知如下：

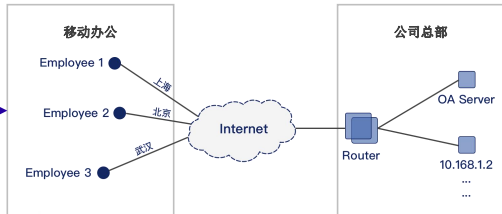
一、适用范围：本通知适用于公司全体员工。

二、工作要求：全体员工应严格按照公司规定的时间和要求，通过远程办公系统开展工作。如有特殊情况，请及时向部门负责人报告。

三、保障措施：公司将提供必要的技术支持和保障，确保远程办公系统稳定运行。

四、其他事项：本通知自发布之日起生效，如有未尽事宜，另行通知。

办公模式的改变



在无边界网络环境下，确保所有的业务访问都是由可信的人、终端或系统用可信的方式访问可信的资源和数据

原则

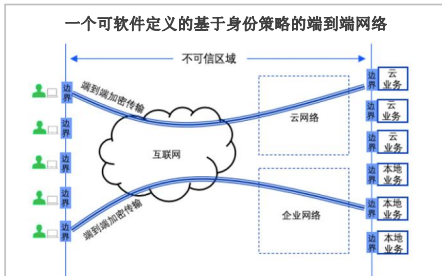
- NEVER TRUST
- ALWAYS VERIFY
- CONTINUOUSLY MONITOR

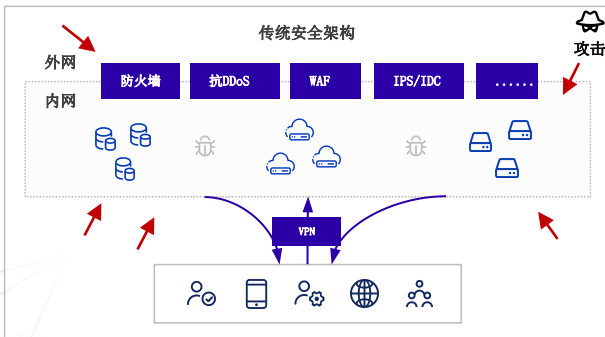
特点

- 基于请求的持续检测
- 细粒度强认证和全网加密
- 最小特权和可变的信任

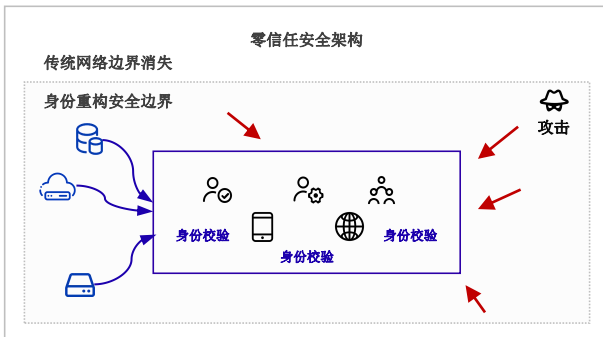
组件

- 基于应用的认证/授权
- 基于设备的认证/授权
- 信任/威胁评分（云端）





- 信任基于访问请求来自的网络位置
- 默认内网环境是可信任的
- 内网内部安全防护薄弱
- 一旦攻破网络边界，整个体系就会处于高度威胁之中

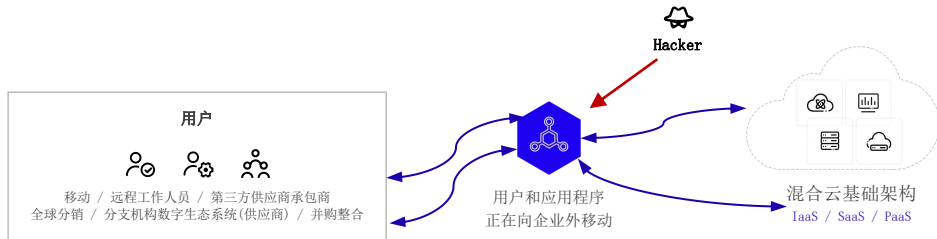


- 身份作为唯一验证
- 无处不在的最小特权访问
- 任何用户都不被信任
- 每个访问请求都必须验证

云WAF+零信任 (背景)

疫情问题下 IT 新的挑战

- 内网应用没有支持公网环境访问
- 应急将应用发放公网的安全顾虑
- VPN访问慢不稳定急需扩容

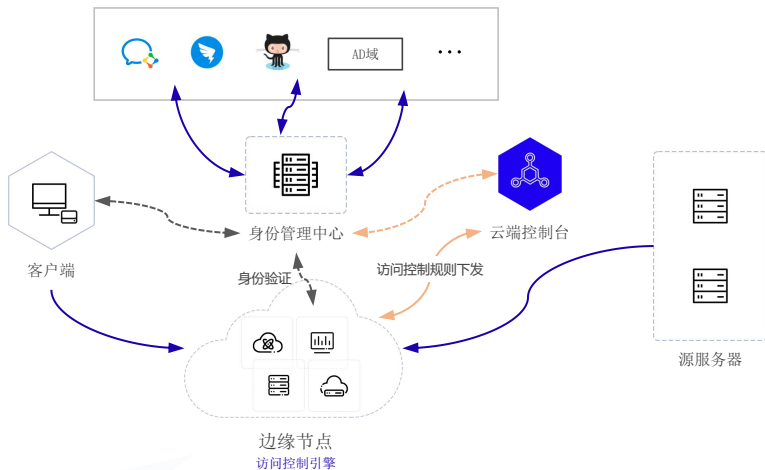


云原生零信任-应用可信访问

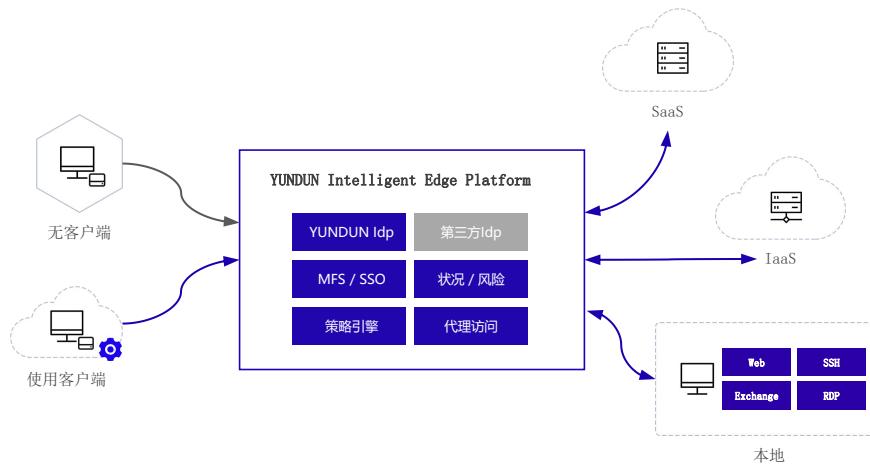
边缘安全加速节点

集成身份认证和访问控制

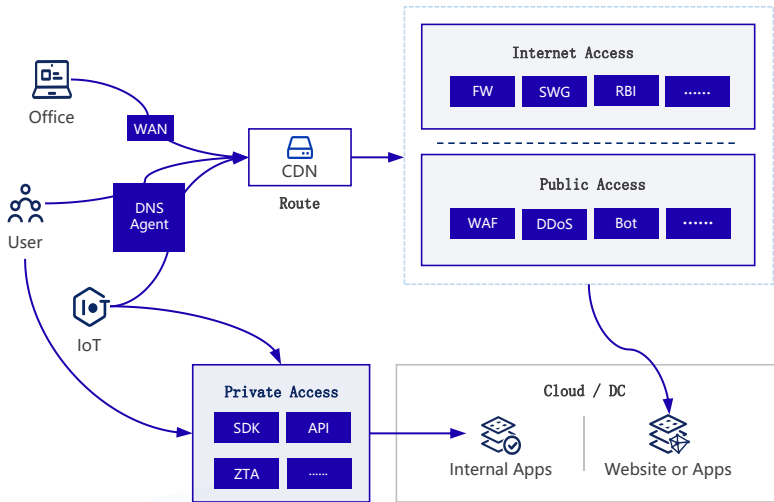
- 资产集中收敛、统一工作入口，隐藏资产攻击面
- 替代内部VPN
- 内网应用快速SaaS化
- 提供综合的解决方案级产品
- 降低建设IT+安全复杂性
- 安全检测分析平台联动



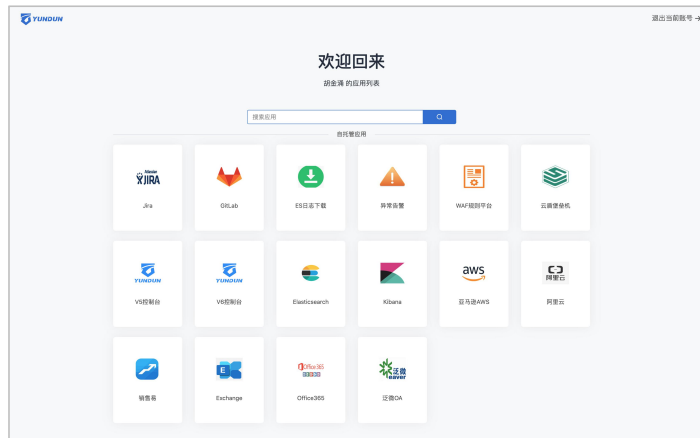
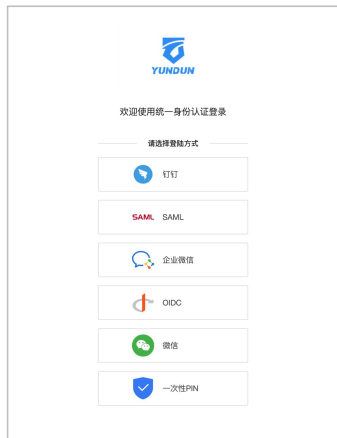
YUNDUN零信任架构



云原生安全CDN+云原生零信任



云原生安全CDN+云原生零信任



互联网即企业WAN

存粹基于互联网的连接和访问。所有企业应用程序都可以通过边缘访问，解放了企业的安全边界。边界不必存在于数据中心的硬件盒子中，而是在企业需要的任何地方。员工、外地员工、第三方人员，甚至物联网设备，都可以自由地安全访问。

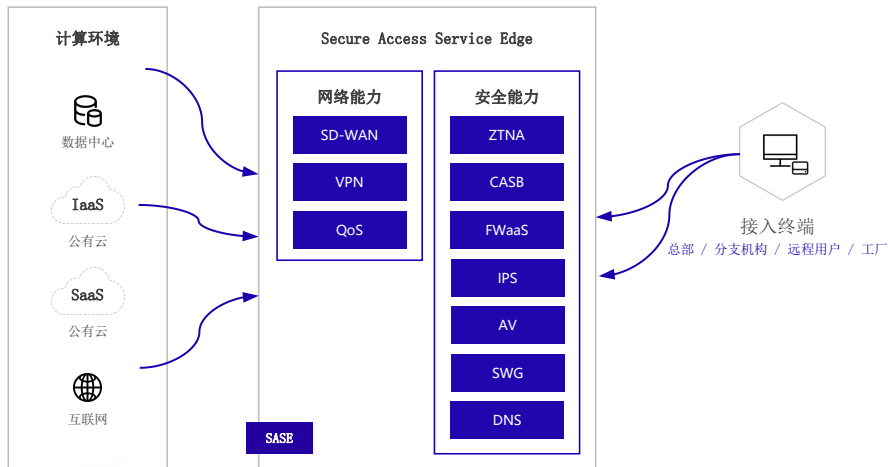


由零信任看到未来的趋势：SASE

www.yundun.com

SASE的理念就是借助SD-WAN搭建起来的虚拟化架构去集中化，将核心能力附加到边缘，以满足当前和未来云上和移动业务的动态需求

SASE是端到端安全。SASE平台上的所有通信都是加密的。包括解密、防火墙、URL过滤、反恶意软件和IP在内的威胁预防功能都被集成到SASE中，并且对所有连接的边缘都可用





THANKS

