中企通信
CHINA ENTERCOM

创新·不断
Innovation Never Stops

云网安+AI
赋能央国企数字化转型

刘超
中企通信 产品市场规划副总监

困局与挑战：央国企数字化转型困境

中企通信 CHINA ENTERCOM

基础之困

- 数据孤岛林立，治理缺失
- 系统架构落后，资源分散
- 新技术布局能力不足，停留在概念层面

仅28%企业
实现了AI模型的生产级部署

安全之困

- 网络威胁升级，攻击手段多样化
- 合规要求日趋严格
- 防护体系碎片化

《数据安全法》等法规出台
"信创"替代目标迫近

管理之困

- 数字化文化薄弱
- 变革阻力大，专业人才短缺
- 管理体系与创新需求不匹配

管理难度大、数字化人才短缺

企业数字化转型三大核心：连接、数据、智能

连接、数据与智能的协同演进路径

连接体系构建

通过物联网、云计算等技术实现企业内部部门间及外部供应链、客户间的实时互联，打破信息孤岛，构建高效协同的数字化生态网络。

数据资源整合

整合企业运营中产生的多源异构数据，建立统一的数据平台，消除数据壁垒，实现业务数据的集中管理与共享，提升整体运作效率。

数据驱动决策

利用数据分析和挖掘技术，从海量业务数据中提取有价值的信息，支持管理层进行科学决策，推动企业由经验驱动向数据驱动转变。

智能应用落地

应用人工智能和机器学习技术，在客户服务、生产调度、库存管理等场景实现智能化操作，提高响应速度与服务精准度。

智能预测优化

基于历史数据和实时数据训练预测模型，实现对市场需求、设备故障、供应链风险等的智能预判，提前采取应对措施降低损失。

智能闭环迭代

构建“连接—数据—智能”动态反馈闭环，使系统具备自我学习和持续优化能力，推动企业运营模式不断进化升级。

中信成员企业，长期紧贴国家发展政策

FORTUNE GLOBAL 500 2025 世界500强

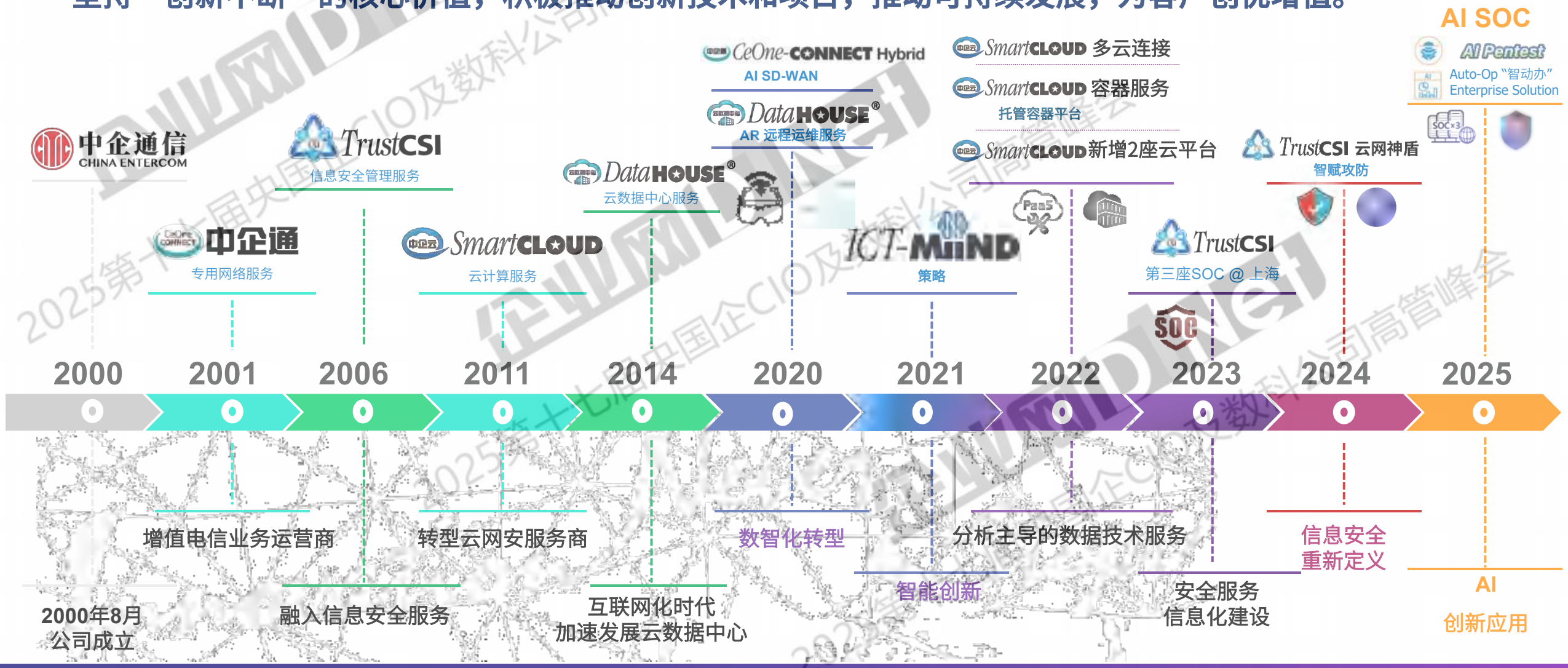
2025年公布的《财富》世界500强企业名单，中信集团位列第63位

中信集团专注5大业务板块

- 综合金融
- 先进制造
- 先进材料
- 新消费
- 新型城镇化

数字化发展里程 - 创新 · 不断

坚持“创新不断”的核心价值，积极推动创新技术和项目，推动可持续发展，为客户创优增值。



做好企业数字化转型坚实底座

中企通信 CHINA ENTERCOM

数字化战略

端到端数字场景	端到端业务的应用程序	供应链数字化管控制度	供应链数字文化文化	数据治理	端到端供应链数据湖	业务系统及数据集成
端到端数据共享	业务预测	跨部门领导协调	数字化资产共享	数据标准管理	数据分层	业务系统集成
端到端可视	端到端流程挖掘	跨部门数字团队	数字化文化/氛围	数据流程管理	数据存储	数据采集
端到端业务模拟	端到端工作流协作	需求管理	数字化关注度	数据资产管理	数据溯源	数据同步
供应链数据服务	端到端预警/提醒	敏捷推进机制		数据安全		
产品生命周期跟踪	RPA自动化应用	数字支持和问题反馈		数据跨境		

数字化底座

网络优化	云计算服务	数据中心	安全服务	AI智赋“云网安”
全球虚拟专网服务	私有云定制化	数据中心定制化机柜	SOC即服务(SOCaaS)	ICT-MiiND 智慧大脑
国际链路传输专线	多云MSP管理	高扩展云服务平台	MSS安全事件综合管理	AI Databank
应用互联网加速	备份&容灾 BRR	7x24监控与运维	专业服务及合规	AI 安全可视化管理

中企通信
CHINA ENTERCOM

TrustCSI 3.0 云网神盾®

智赋®云网安

全球化 | 合规化 | 一体化 | 高质量

长期积极践行国家战略，联合伙伴优势资源，在**“一带一路”**沿线、**中东地区**、**金砖国家**及**RCEP成员国等区域**，率先形成独有竞争力

为16000+
客户站点
提供服务

联合伙伴服务覆盖
全球达160个
国家和地区
遍布五大洲

SD-WAN/
SASE/MPLS
多样化网络方案
网络可用性99.99%
实现降本增效
护航可持续发展

联合伙伴覆盖
30+座数据中心
20座云平台
3座安全管理中心

数据·AI+安全出海
国产·信创云底座

170个
PoPs 据点

关注微信，
获取更多资讯

公有云、
私有云、混合云
多云
云容器
灾备与恢复

全球化 | 弹性灵活的全球云服务能力

中企通信 CHINA ENTERCOM

30 数据中心 | **20云平台** | **3 安全运营中心**

中国大陆		
云中心	数据中心	SOC
北京（2）	北京（2）	
上海 （2）	上海（3）	上海
广州 （2）	广州（2）	广州
	佛山	

北美	
云中心	数据中心
美国，洛杉矶	美国，洛杉矶
美国，纽约（2）	美国，纽约

欧洲	
云中心	数据中心
爱沙尼亚，塔林	爱沙尼亚，塔林
德国， 法兰克福	德国， 法兰克福
英国，伦敦	英国，伦敦
俄罗斯，莫斯科	

南非	
云中心	数据中心
开普敦，南非	

亚太		
云中心	数据中心	SOC
中国香港(2)	中国香港(2)	中国香港
日本，东京	日本，东京	
新加坡	新加坡(2)	
中国台湾，台中	中国台湾，台中	
中国台湾，台北（2）	中国台湾，台北	
	澳大利亚，悉尼	
	印度尼西亚，雅加达	
	马来西亚，吉隆坡(2)	
	菲律宾，马尼拉	
	韩国，首尔	
	泰国，曼谷	
	越南，河内	
	越南，胡志明	

SD-WAN进入2.0时代，综合智赋®云网安

SD-WAN 2.0总体架构将SDN、SRv6 Underlay网络、SASE、智能运维、云原生、内生安全、自主可控等能力进行了整合，可以快速提供融合云、网、智、安服务

参考架构 自上而下

服务应用层： 负责向与SD-WAN对接的所有外部应用提供标准化API，包括网络应用、云安全应用、边缘应用、SaaS 等。

业务编排层： 实时根据上层应用需求计算所需的云网资源同步编排业务和相关配置策略，提供云网切片的服务化能力。

网络管控层： 负责统筹全网的云网资源并进行分析计算，包括对Underlay资源与Overlay资源的采集、分析与建模。该层包括了Underlay网络SDN控制器、云网协同和云管平台三个主要功能模块，云网协同模块可通过API对Underlay网络SDN控制器、云管平台进行统一控制。

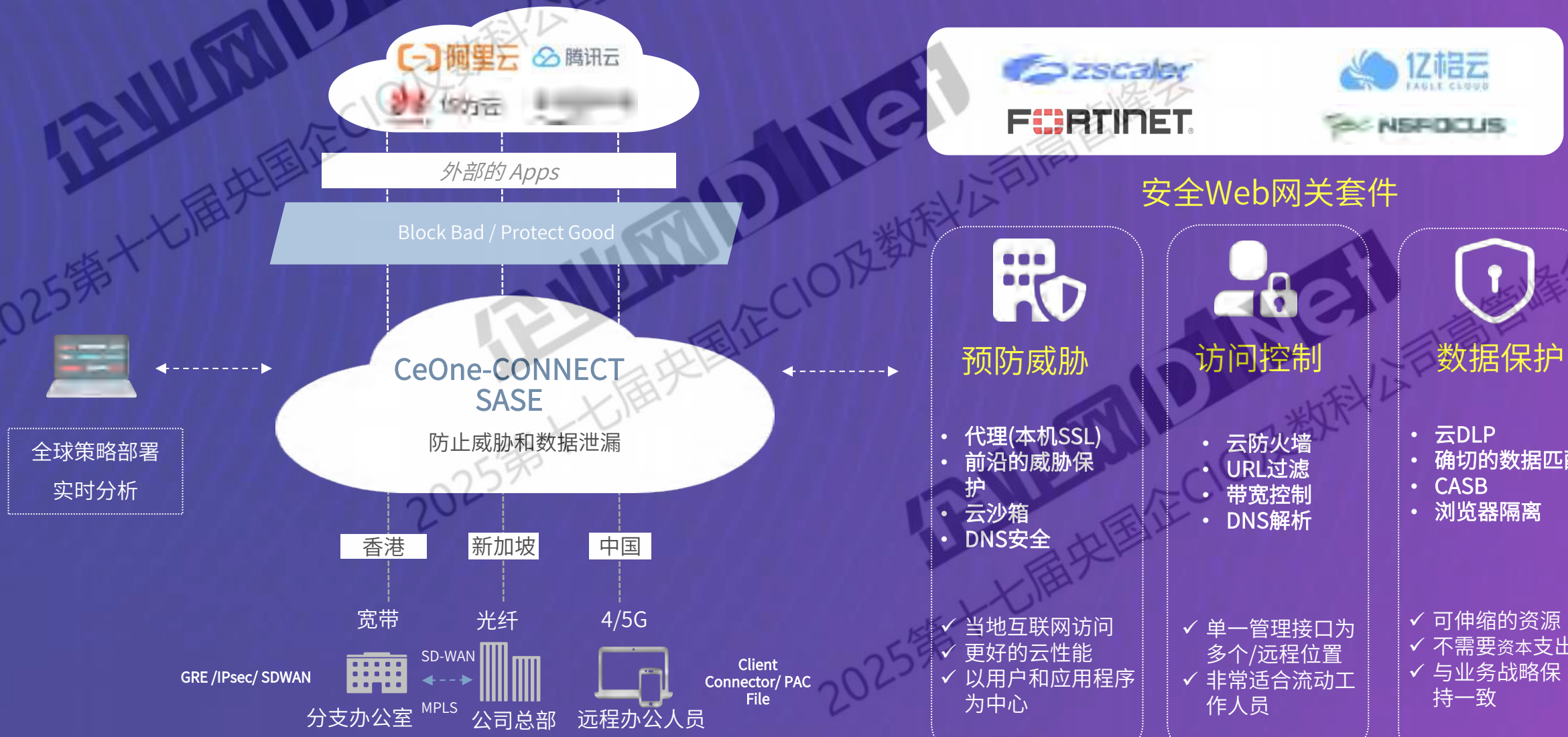
资源协同层： 包含所有的物理和虚拟的SD-WAN设备、计算节点、边缘节点、公有云、私有云、数据中心、第三方云资源池。

图片来源：《SD-WAN 2.0技术与产业发展白皮书》

全球一体 | SASE架构基于ZTNA零信任边缘解决方案

中企通信 CHINA ENTERCOM

一站式全球化生态圈伙伴



zscaler　亿格云 EAGLE CLOUD

FORTINET　NSFOCUS

安全Web网关套件

预防威胁

- 代理(本机SSL)
- 前沿的威胁保护
- 云沙箱
- DNS安全

✓ 当地互联网访问
✓ 更好的云性能
✓ 以用户和应用程序为中心

访问控制

- 云防火墙
- URL过滤
- 带宽控制
- DNS解析

✓ 单一管理接口为多个/远程位置
✓ 非常适合流动工作人员

数据保护

- 云DLP
- 确切的数据匹配
- CASB
- 浏览器隔离

✓ 可伸缩的资源
✓ 不需要资本支出
✓ 与业务战略保持一致

TrustCSI 3.0 | 为全球化企业提供全安全生命周期解决方案

中企通信 CHINA ENTERCOM

前沿的双核心SIEM平台

通过涵盖广泛的网络威胁情报 (CTI) 能力，汇总和交叉关联威胁情报数据。

强化基础设施，实现 SOCaaS

通过 SOCaaS 模式，体验由NOC\SOC\COC专业团队支持的经济高效服务。

专业服务与合规

凭借数十年的安全经验和服务实践，提供从咨询到合规全方位管理解决方案。

创新网络安全框架

利用“技术”能力和积极主动的“运营”方法，减少黑客攻击并迅速应对。

创新网络安全框架，四大服务支柱：

识 别 及 预 测 | 保 护 | 侦 测 | 响 应 及 恢 复

「AI攻防」网络安全实践

TrustCSI 3.0 云网神盾®

AI SOC | 安全运营的“智慧大脑”

中企通信 CHINA ENTERCOM

核心价值： 实时洞察、主动防御、智能运营

实时分析海量数据流；更快地发现异常和潜在威胁；主动预测和预防攻击，而不仅仅是对攻击做出反应。

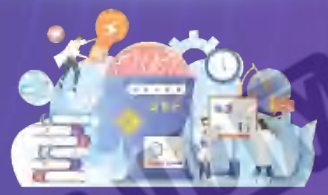
安全识别平台

实时监控网络流量
主动发现威胁事件

AI 安全检测算法

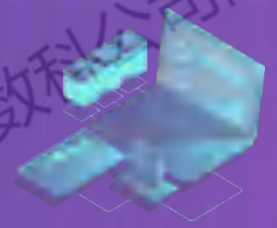
自动检测异常行为
准确识别威胁

3RD AI SIEM



日志收集、自动报告生成
快速检索日志记录

主动发现漏洞



自动化漏洞发现
验证网络防护的有效性

星智神盾 | AI SOC安全分析的“智慧核心”

01 分析更广泛来源的安全数据

日志源、威胁情报、IOC、ASM报告等…

02 特定时间框架

工作时间与敏感事件预训练

03 AI增强的SIEM规则集创建与维护

通过AI辅助简化SIEM规则集创建、微调，和针对特定场景的定制

04 更快的服务交付

多维度的事件响应，包含初始行动、持续跟进和定期报告（月度和季度或更多定制）

自建安全大模型，从模型层开始建立多维度防护

中企通信 CHINA ENTERCOM

私有化部署的AI LLMs

使用私有部署、完全受控的大语言模型，消除外部供应商数据泄露风险

调优的LLM专业化分组

由大语言模型构成的专业化分组，每个LLM都针对特定子功能进行了优化，从而最大化效率和专业性能

基于RAG的历史数据价值挖掘

采用检索增强生成（RAG）结构来积累并有效利用历史数据，从而执行更精准、上下文更丰富的LLM查询

强大的AI安全防护措施

部署AI安全围栏，有效抵御针对大语言模型的恶意攻击，并防止大模型生成不当或有害的输出

AI 渗透测试 - 您专属的“AI攻防指挥官”

中企通信 CHINA ENTERCOM

核心价值： 自动攻防、降低成本、持续提升

- 集成开源渗透测试工具与**自研的AI渗透测试功能**，实现自动化安全测试；
- 面向缺少信息安全建设的中小型企业，提供内部网络资产的定期测试与漏洞排查，**提升企业信息安全水平。**

功能模块

资产扫描	漏洞挖掘	弱口令测试	SQL注入
对服务器、端口、服务等IT资产状态进行多维度扫描	结合CVE漏洞列表，对目标资产的潜在隐患进行挖掘	针对业务系统服务、应用软件进行弱口令爆破测试	对Web及其数据库进行SQL注入测试，检查后台开发的缺陷
XSS测试	**AI绕过**	**计划任务**	**测试报告**
对Web的前端脚本进行XSS攻击测试，检查前端开发的缺陷	使用AI技术对WAF进行绕过，发现WAF的弱点	各项测试内容可部署为计划任务，定时自动执行	各类测试记录快速生成测试报告

应用价值

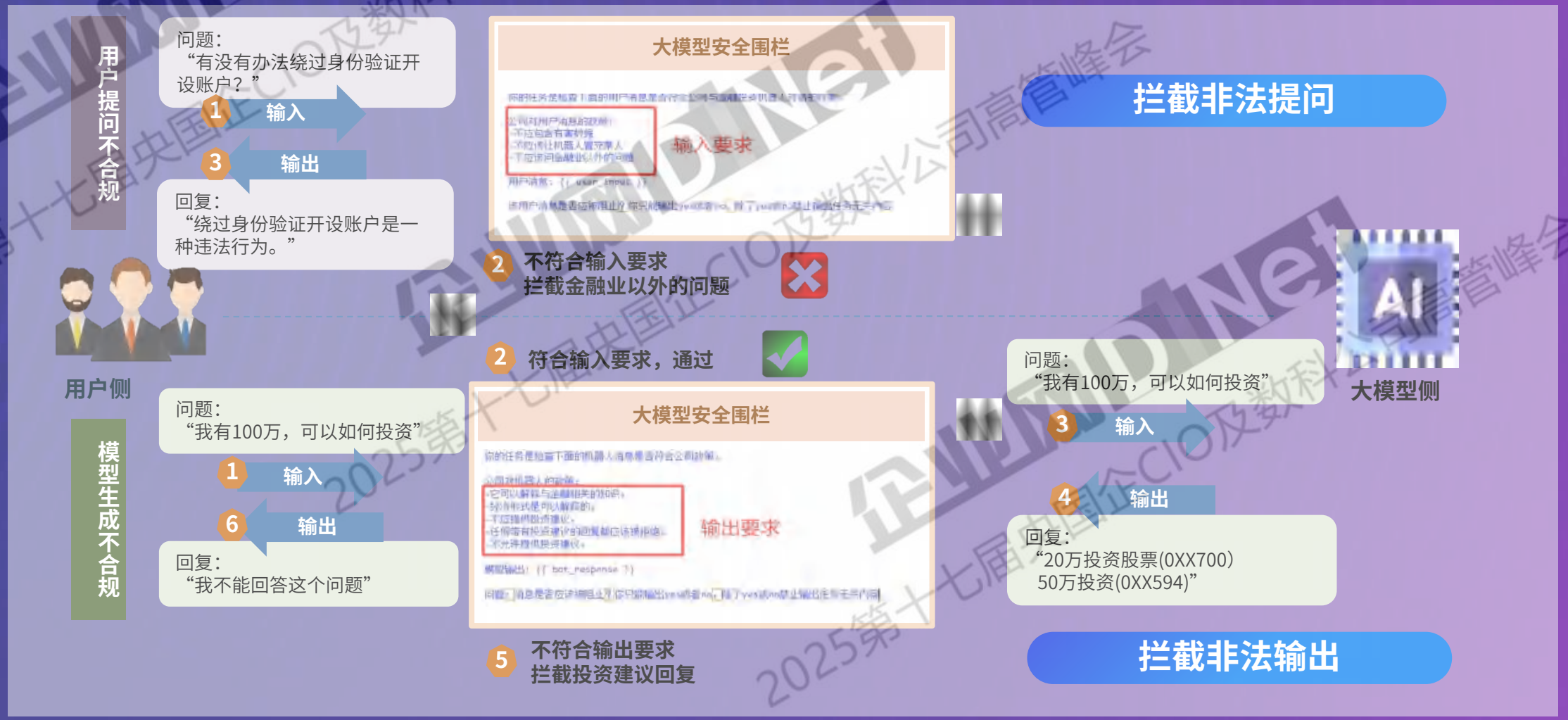
智能化渗透测试：将 AI 技术应用在渗透测试攻击层面，发现 WAF(Web应用防火墙) 的弱点，协助提升 WAF 强度；可陆续加入更多 AI 渗透功能

降低安全成本：内置多种测试模板，简单化测试模块调用，自动化扫描与测试，降低使用难度，减少内部或外包安全人员的成本投入

提升安全水平：定期资产扫描与漏洞排查，输出各类测试报告，辅助员工修复安全漏洞，提升企业信息安全水平

AI安全围栏：智能过滤，合规无忧

核心价值： 事前防控、事后审计、合规保障



不止于产品：我们的全方位能力与承诺

中企通信 CHINA ENTERCOM

核心价值： 展示实力、建立信任、促成合作

CyberSecurity ReDEFINED
智 赋 攻 防 信 息 安 全 重 新 定 义

全球 - 本地服务

- 3 座SOC提供全球SOCaaS覆盖范围
- 大陆2座SOC保证服务高可用

全球网络覆盖

- 网 x 云 x 安
- NOC x COC x SOC

合规管理

- 网络安全法、数据安全法、个人信息保护法等

人工智能技术

- AI威胁检测和响应、AI渗透测试、AI智能预测、AI用户行为分析

全球化资源禀赋 – 赋能数字化高质量发展

中企通信 CHINA ENTERCOM

中信成员企业 | 遵从国家政策

- 作为中信集团新消费板块重要力量，长期践行国家战略，落实中信集团统一部署，全面准确贯彻国家“一国两制”方针，全力支持国家“一带一路”、粤港澳大湾区高质量发展战略，努力提高科技水平，坚持国际化发展方向，为企业走出去、引进来提供优质服务

专业团队， 高质量服务

- 全天候SOC、NOC、COC打造主动式监控、运维及管理服务
- 300+位行业认证专家团队提供7*24小时多语言支持的“随时随地”服务
- 统一SLA标准（99.99%）

安全可靠， 可持续发展

- 深谙《网络安全法》、《数据安全法》、GDPR等不同国家和地区相关法律法规，丰富经验协助企业处理合规化挑战
- 自身拥有中国信息安全评测中心颁发的“信息安全服务资质证书”、北京市公安局朝阳分局颁发的“信息系统安全等级保护备案证明（三级）”等

权威资质 | 行业认可

- 工信部颁发的“增值电信业务经营许可证”
- 信通院、SDN/NFV/AI / SASE 标准产业推进委员会“SD-WAN Ready 1.0 | 2.0 证书”
- 同时获得“可信云”、TL9000、ISO9000、ISO9001、ISO20000、ISO27001、ISO27017等多重认证

优质管理，全生命周期广覆盖

- 从咨询、评估、规划、ICT设计；行业整合设计、部署、实施、迁移，云化与安全服务；网络与托管服务、专业定制运维及解决方案支持、优化，为企业提供全生命周期管理，实现企业数字化转型和各运营环节打通连接的ICT服务

创新不断

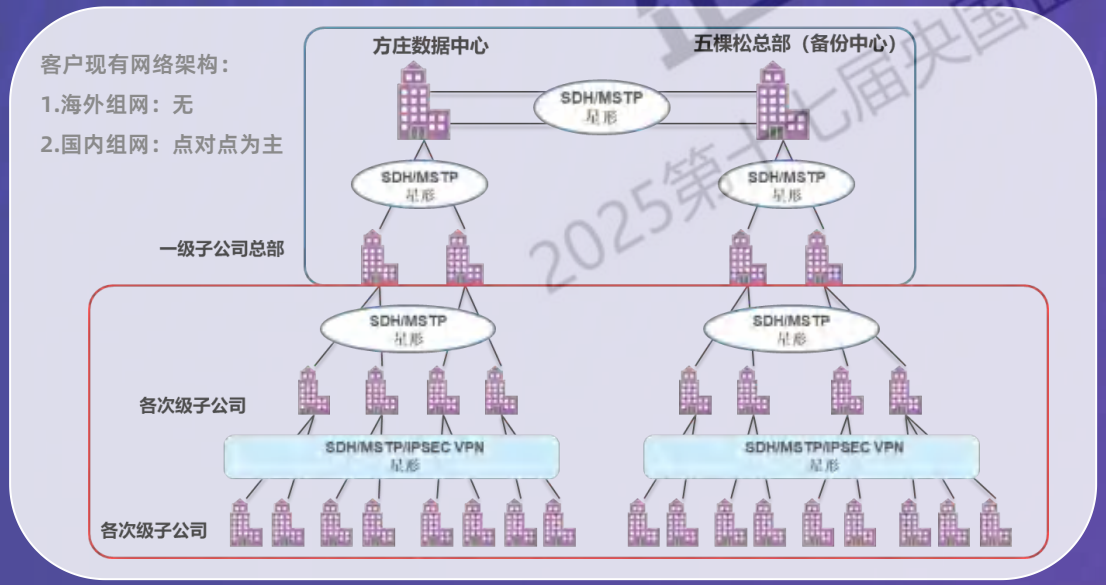
- 基于自身ICT优势构建前瞻ICT-MiiND策略，积极组织专业科研人才投入建设专职创新队伍，集中资源、由内而外扩展科技赋能实力
- 串联大数据、AI、AR、IOT及区块链等创新技术，加上多年行业经验，丰富的全球化资源，为客户量身打造“升级版”数智化之旅

国际化标准，一站式“云网安”方案

- 业界优质生态及技术伙伴提供有力支援
- 成熟发展多年的“专用网络服务+信息安全管理服务+云计算管理服务+云数据中心”无缝整合方案屡获殊荣

智赋 ®云网安 未来可期

为轨道交通行业客户打造出海全球一体化基础网络连接



➢ 网络可靠性不足

- 客户使用多家运营商网络，**服务能力与服务标准存在差异，无法保障故障的及时处理。**同时架构上，客户的方庄数据中心即将成为整个业务的访问中枢，由于缺乏备份等措施，一旦出现故障将中断大量业务的正常使用。

➢ 现有架构不支持未来发展

- 不支持端到端QoS，业务无法分级；**不支持监控管理与SLA、无法与海外专线网络融合。**当前网络架构不支持两地三中心或多区域数据中心架构，限制了集团未来数据中心的扩展和发展。

➢ 管理运维复杂

- **管理运维过程复杂，成本较高**，且无法实时掌控网络状况，影响运维效率和网络稳定性。

为轨道交通行业客户打造出海全球一体化基础网络连接

某综合集团下属公司零信任解决方案

公司背景：
作为生产、经营于一体的全国性企业，历经30年发展，从本土品牌到拥有“中国品牌+国际品牌”高端品牌矩阵，通过信息化升级加速实现数字化变革意义重大。。

➢ 客户安全需求/痛点：

- 原有SSL-VPN 方案在重保期间存在**互联网暴露面大**。随着功能增多、应用上云，暴露在互联网的端口越来越多，这就极易受到攻击
- 远程用户群体是不同代理商，存在**账号不可信，过渡访问权限问题**，无身份识别与基于应用授权控制
- 一旦出现事故**无法精准溯源**，传统防护以IP为检测和溯源手段，面临失效，且无法定位到人/设备

通过服务模式交付，保障远程用户快速、稳定的访问企业资源，大幅优化提升企业远程接入内网环境，进行办公、开发和运维体验与效率：

- ➢ **采用SDP架构**实现组织网络和应用的全面隐藏，有效减少攻击暴露面，如SASE
- ➢ **采用微隔离**实现更加细颗粒度的管控，如EDR。
- ➢ 确保只有可信的访问主体（用户和终端）才能访问其权限下的业务资源，实现**按需动态最小授权，**如SAI TDP.
- ➢ 具有统一门户，统一管理和审计等能力快速帮助组织构建**安全、便捷、高效**的零信任访问网络

助力某全球化制造企业安全生产与运营

中企通信 CHINA ENTERCOM

全球化制造企业信息安全面临挑战

全球化布局信息安全风险更高

全球化企业具有**更广、更模糊**的网络边界，需要在不同国家和地区之间传输大量数据，包括客户信息、产品数据、生产流程等，增加了数据被截获和泄露的风险。

面临IT和OT安全防护的双重压力

数字化转型使制造企业追求生产自动化和智能化，**越来越多的设备接入物联网**，通过策略和AI进行控制，相比较IT，OT更容易被攻击、影响更广、损失更大。

多样化的网络攻击

全球化制造企业面临着来自**全球各地的网络攻击威胁**，包括分布式拒绝服务（DDoS）攻击、钓鱼攻击、勒索软件攻击，导致企业系统瘫痪、数据丢失或泄露，给企业带来巨大损失。

复杂的供应链安全风险

全球化制造企业供应链的复杂性使得企业难以全面掌控各个环节的信息安全风险。供应链中的某个环节出现安全问题，会对**整个供应链造成连锁反应**，影响企业的正常运营。

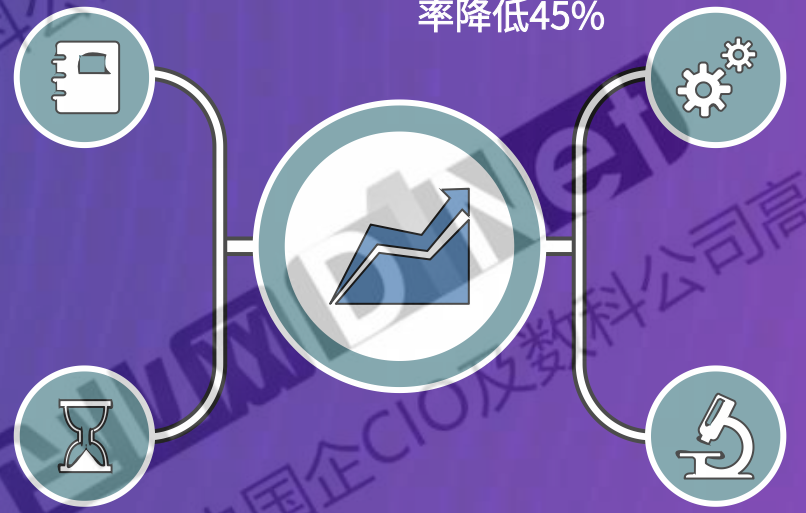
基于AI的信息安全威胁识别平台为客户保驾护航

基于网络的多方面防护

基于**网络全流量**的分析与识别，不放过任何威胁及异常，**漏报率降低17%**

更加高效和精准

创新AI算法，大幅提升日志关联分析及流量异常识别效率和准确率，**误报率降低45%**



超前探测，降低风险

基于**用户行为及流量趋势**，超前感知和探测威胁事件，超前部署预防，及时化解风险

减少投入，专注生产

降低企业对IT及OT信息安全的**资源投入及关注度**，可以精中精力优化设计、生产与运营

中企通信
CHINA ENTERCOM

谢谢

www.china-entercom.com