长亭科技

下一代网络安全解决方案领导者

化繁为简 • 智能安全

目录

CONTENTS

关于我们

安全产品

安全服务

解决方案

合作生态

公司实力

01

ABOUT US

关于我们

关于我们

CHAITIN

长亭科技

国际顶尖的技术驱动型安全公司

全球首发基于智能语义分析的下一代Web应用防火墙产品

目前，公司已发布10余款自研技术驱动产品服务，形成以攻（安全评估系统）、防（下一代Web应用防火墙、高级威胁分析预警系统）、知（安全分析与管理平台、攻击面管理运营平台）、查（主机安全管理平台）、抓（伪装欺骗系统）为核心的新一代安全防护体系，并提供优质的安全测试及咨询服务，为企业级客户带来智能的全新安全防护思路。

10+

推出10余个产品
覆盖安全体系建设核心场景

100%

连续七年业绩翻番

1000+

为上千家客户提
供网络安全解决方案

长亭关键词

CHAITIN

长亭科技 CHAITIN

清华蓝莲花

国内最知名CTF攻防蓝莲花战队

硬核技术

第三代安全公司，唯一跨应用、终端、网络、运营技术域能力覆盖

云计算

深入理解云计算，从国内云安全成熟最佳实践最早探索者的技术演进

实战攻防

国内大型攻防演练前三成绩保持者

长亭大事记
CHAITIN

2014.7
- 公司成立
- 豪华技术团队阵容

2015
- 推出安全服务：渗透测试
- 几乎包揽国内黑客大赛冠军
- 首款产品原型亮相美国Black Hat大会军械库

2016
- 全球首发智能语义分析NGWAF：雷池（SafeLine）
- 国内首款商业化欺骗伪装系统：谛听（D-Sensor）
- 世界最高标准黑客大赛 DEFCON CTF 全球第二
- 形成攻、防、抓三位一体应用层解决方案

2017
- 商业化产品提名Gartner魔力象限报告
- 首个发现并预警全球重大安全事件永恒之蓝（WannaCry）
- 《华尔街日报》评价为改变世界网络安全的中国力量
- 《财富》中国创新大赛全国第一

2018
- 漏洞检测商业化产品洞鉴（X-Ray）发布
- Gartner《 Web应用防火墙魔力象限》报告再次提名
- 入围Gartner 2018《Web应用防火墙魔力象限报告亚太版》

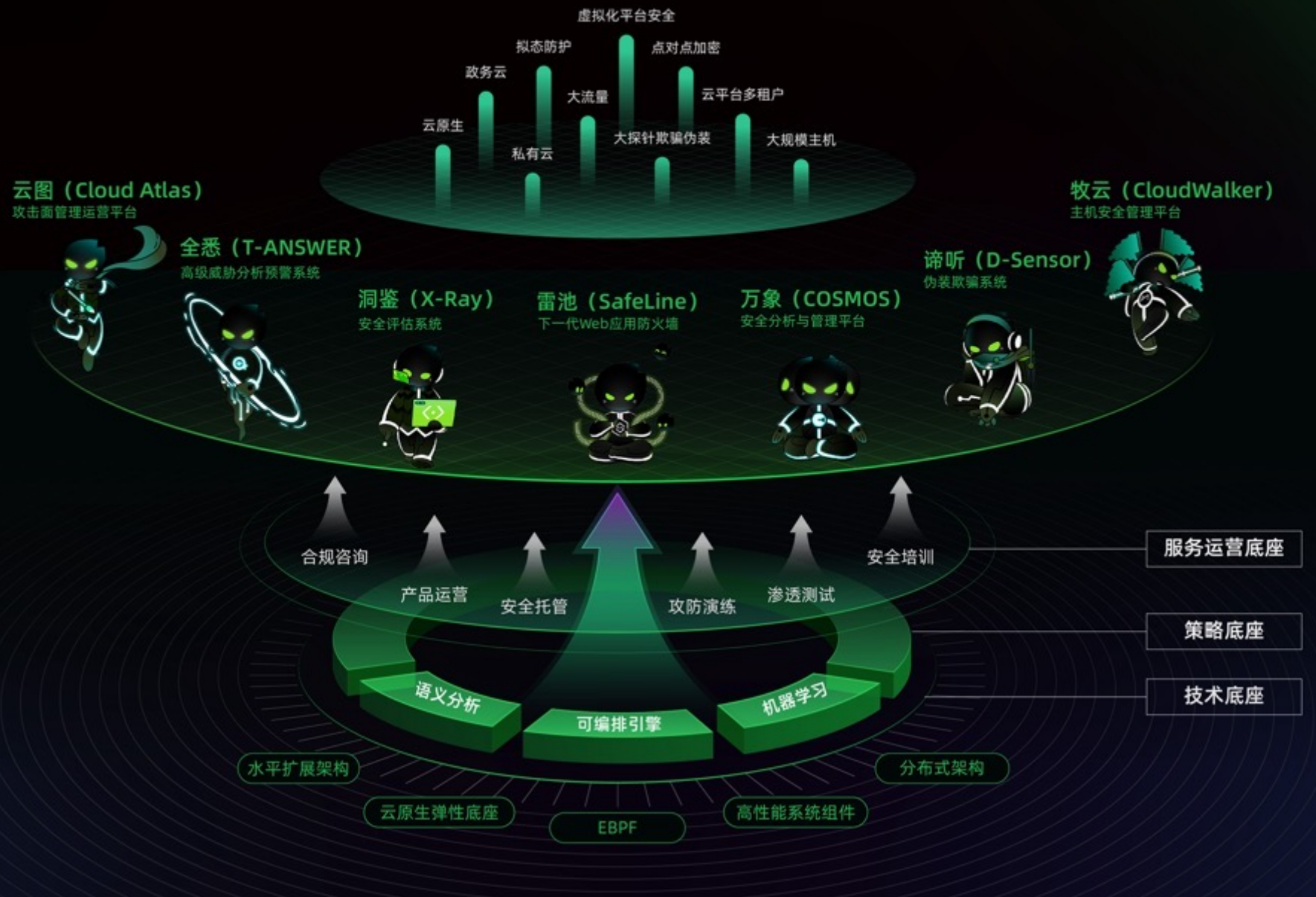
2019
- 入选Forrester《Now Tech：Web Application Firewalls, Q4 2019》报告
- 入选IDC《中国Web应用安全市场》潜力厂商
- 荣膺CNCERT网络安全应急服务支撑单位（省级）

2020
- 商业化布局终端侧安全产品-牧云（CloudWalker）
- 斩获“强网杯”网络安全挑战赛一等奖
- 发现并命名当年全球十大安全漏洞-Ghostcat（幽灵猫）

2021
- 首个安全运营平台产品万象（COSMOS）发布
- IDC 2020年中国硬件WAF产品市场份额报告中位列第四
- 近5年最大影响力安全漏洞 Apache Log4j2，国内首个推出免费检测工具
- 10项虚拟机漏洞获Oracle官方致谢

新一代安全防护体系

长亭科技新一代安全防护体系



02

PRODUCTS

安全产品

攻 洞鉴（X-Ray）安全评估系统

从资产视角出发
集Web漏洞扫描、主机服务漏洞扫描、基线合规检查于一体
实现资产风险闭环管理

自启发式漏洞检测
精准度高

分布式部署
匹配庞杂网络环境

智能调节扫描速度
适用多种业务场景

无害PoC原理检测
不影响业务稳定性

覆盖面广
不遗漏潜在风险

实时响应突发漏洞
小时级快速响应

核心功能
PRODUCTS

卡亭科技 CHAITIN

资产发现

识别主机服务**3000+**

应用指纹**8000+**

Web资产**1000+**

漏洞检测

自研高质量PoC或通用插件**700+**

原理扫描漏洞**1500+**

整体漏洞库**23万+**

基线配置核查

CIS**一级、二级**

等保**二级、三级**

资产风险闭环管理

多维度综合评估

建立资产风险集中化管理体系

漏洞扫描

主机&Web漏洞**一体化**自动检测

弱口令检测种类**20+**

模拟浏览器爬虫、多种被动检测模式

内置盲打平台，自动验证无回显漏洞

多租户分级管理

总分多级架构，容器化部署

组织单位数据**隔离划分**

用户权限精细化管理

应用场景

PRODUCTS

漏洞扫描工具

精准灵活探测漏洞

应对日常风险或突发漏洞排查

满足监管检查、等保合规等需求

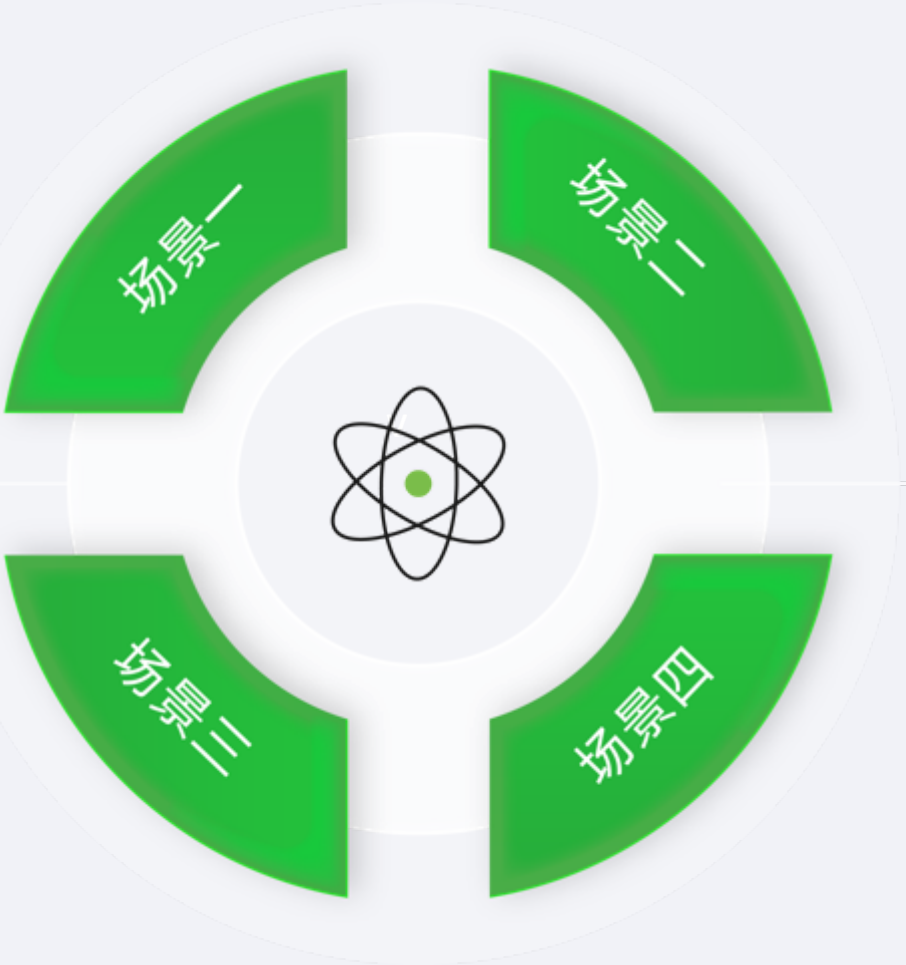
资产风险管理平台

资产视角风险梳理

定岗定人风险告警

资产风险生命周期追踪

打造自动化的资产风险管理闭环流程



云原生多租户

容器轻量化部署

弹性可扩展

高效集中管控云平台资产

租户端资产隔离、运营端统一管控

SDLC

嵌入研发流程

协助系统上线前风险排查

实现安全测试左移

降低漏洞修复成本

防 雷池（SafeLine）
下一代Web应用防火墙

全球首款基于人工智能语义分析引擎的下一代Web应用防火墙
用算法的迭代改变规则防护的现状，质变提升检测准确率
并对攻击防护难题——未知威胁有天然的抵抗力

FVM
机器学习
智能语义分析算法
容器化底层架构

核心技术

核心功能

- OWASP Top 10
- 0day防护
- API防护
- BOT管理
- Web访问控制
- 流量学习
- 可编程扩展插件

市场认可
PRODUCTS

2015年提出语义分析技术并实践落地，受邀美国Black Hat大会展示SQL Chop

2016年，雷池（SafeLine）基于语义分析引擎发布后至今，已连续6年实现100%增长

攻击拦截性能全球领先

抽样威胁检测误报率 **<0.87%**

漏报率 **<0.73%**

客户端访问延迟 **<5ms**

单日检测流量破**2000亿**

单个节点检测峰值访问请求超过 **200000 QPS**

全球三大权威咨询机构大满贯认可

Gartner

入围《亚太区Web应用防火墙魔力象限》
连续4年提名《Web应用防火墙魔力象限》

Forrester

入选2022年、2019年《Now Tech：Web Application Firewalls》报告

IDC

连续2年中国硬件WAF市场份额**位列第四**（2020-2021）

产品优势
PRODUCTS

长亭科技 CHAITIN

极准拦截
极低误报

还原经过层层伪装变形的攻击向量，并从编码的基因层面识别和判断其危害程度

主流漏洞检测覆盖率100%

01

发现未知威胁
变被动防御为主动识别

基于攻击语言代码的理解，提取同类攻击原理，对未知威胁有天然抵抗力

无需升级
防护70%以上0day

02

极简界面
简化操作流程

“傻瓜式”简易操作难度和友好界面，大幅降低使用成本

默认配置即可适用99%的业务后端

03

速度提升百倍
不影响正常业务

固定资源条件下，语义分析算法时间复杂度更低，处理能力更强

99%的请求1ms以内响应
90%的请求0.1ms以内响应

04

最灵活部署方式
应对最复杂的商业化场景

容器的底层架构天然的分布式和灵活特点，已具备同类产品中最全的部署方式

Kubernetes WAF的部署方式，
在当前国际范围内仅有不超过3家的厂商具备

05

防 全悉（T-ANSWER）高级威胁分析预警系统

聚焦智能、实战、集约构建的新一代网络流量检测、狩猎、溯源以及响应全流程的全流量威胁检测与响应平台

快速有效应对0day、变种威胁、APT攻击、加密流量攻击等不断蔓延升级的高级威胁风险挑战

产品优势
PRODUCTS

卡亭科技 CHAITIN

智能语义分析2.0威胁检测
算法升级有效检测0day、变种、APT等攻击

红队武器库检测
红队武器库检测与识别

攻防实战检测规则

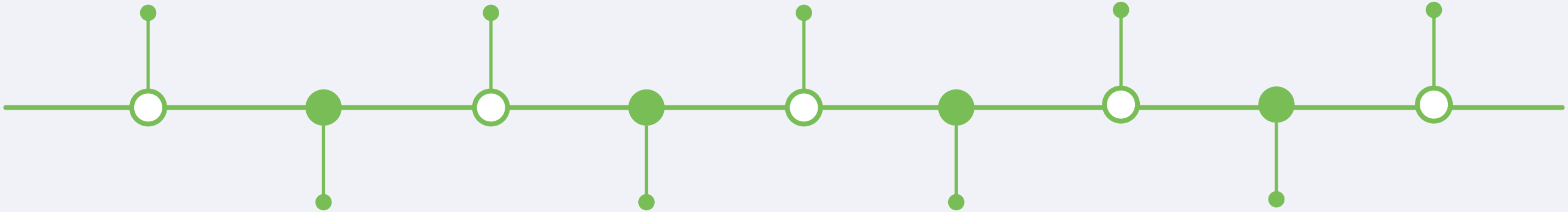
红队武器行为智能检测模型

威胁情报检测
内嵌威胁情报检测引擎

实时更新海量威胁情报

虚拟化平台威胁检测
精准检测针对VMware vCenter、 VMware ESXi等虚拟化平台的攻击

WebShell检测
结合动静态多种检测算法，深度检测WebShell关键恶意代码



AI恶意加密流量检测
有效检测加密反弹Shell、ICMP、 DNS、 HTTP隐秘隧道及多数工具加密入侵行为

Cyber-Kill-Chain检测
基于攻击链视角

全生命周期阶段的检测覆盖

内网渗透威胁检测
内网常见攻击手段

攻击手法的识别

智能恶意文件检测
动静态交叉检测病毒、木马、黑客工具、 Rootkit、挖矿程序等恶意文件行为

应用场景
PRODUCTS

高级威胁实战攻防对抗

- 智能语义分析、人工智能检测技术、文件检测、动态沙箱等技术融合
- 发现0day攻击、加密恶意流量、各种红队武器以及潜在的APT行为
- 攻击链覆盖，补足内网检测盲点
- 攻防视角对事件进行告警聚合分析，快速聚焦重点安全事件
- 日志数据存储，专职运营人员支撑分析

复杂业务架构威胁集约监控与管理

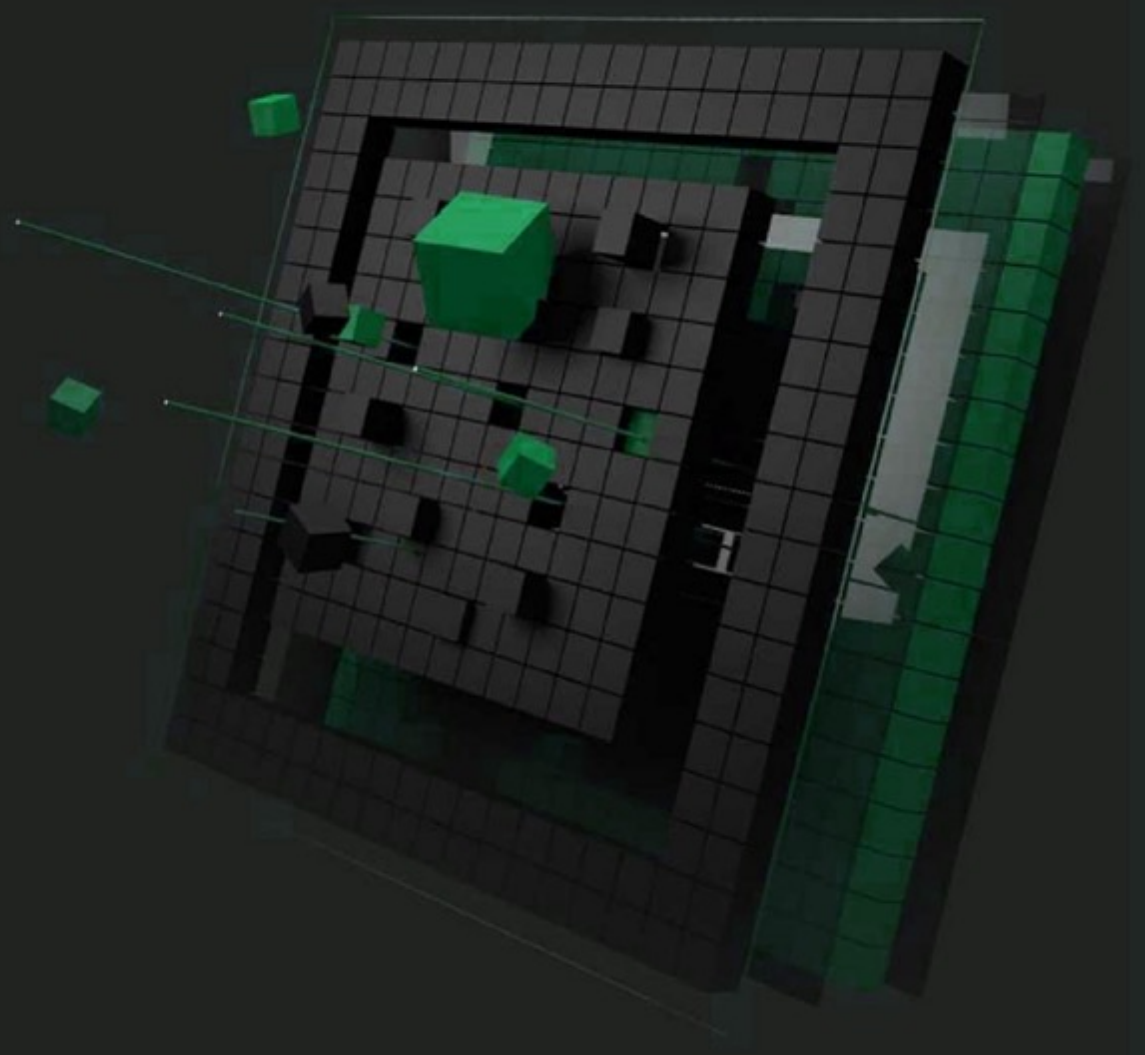
- 分布式部署实现流量采集、解析和分析
- 统一集中管理平台展示风险
- 输出威胁告警事件至态势感知平台，为态势感知监测提供数据来源

日常安全运营&等保合规

- 旁路部署方式接入企业现有网络架构，有效检测风险
- 发现内网存在的失陷、远控问题主机，并进行安全排查
- 满足等保2.0要求，识别检测未知威胁

知 万象（COSMOS）安全分析与管理平台

基于数据驱动、人+平台理念的安全大数据分析及NGSOC平台
以更宏观的视角，汇聚海量的安全事件、日志、IT基础信息等数据
通过多种告警处理动作、告警研判流程等，形成风险处置闭环
精准的分析出风险成果
通过可视化展示能力，让风险更直观、安全更便捷



核心能力
PRODUCTS

5

数据融合

全面采集企业IT、风险、
日志等多源相关数据

智能分析

实时、离线、基线学习多种分析模式
灵活、交互式分析规则配置
内置大量分析引擎、分析规则

风险研判

告警中心统一呈现及管理风险
国内最顶尖安服团队支撑风险
研判

威胁可视

多维度态势分析场景
多视角风险感知大屏
灵活可视化交互配置

协同响应

自动化联动、处置
SOAR：自动化编排与响应

应用场景
PRODUCTS

安全数据中心

- 汇聚多源、异构的安全类数据（安全设备日志、安全合规、操作日志、安全运行）、基础IT类数据（用户数据、资产数据）、威胁情报数据、流量数据等各类网络安全、IT支撑等数据
- 平台自主数据：全流量风险监测事件数据、资产发现及脆弱性监测事件数据、网站风险监测事件数据等

安全风险数据分析平台

- 通过深度理解、挖掘各类安全数据间相关度、关联方式、逻辑关系，帮助提升安全风险输出的可信度，站在整体视角综合分析，支持实时、离线输出更精准、更可信的安全风险
- 支持智能分析，包括基线学习、安全引擎等深度分析能力

安全策略分析工具

- 贴合不同企业安全业务，更灵活、可配置的安全数据处理、可视化分析的安全策略分析工具

企业安全运营管理机制

- 贯穿企业安全运营体系建设，逐步帮助用户建立数据分析、风险发现、风险处置、处置反馈/复查的安全风险闭环流程，管理企业安全资产数据，串联实际安全工作，形成企业安全运营管理机制

知 云图（Cloud Atlas）攻击面管理运营平台

绘制资产关联图谱，梳理真实攻击路径，持续性安全巡检，快速应急响应，从而大幅提升安全运营效率，让安全从被动防御变为主动出击

SaaS模式无需部署，自适应弹性扩容

平均发现**60%**的未知/隐藏资产
千万亿+攻击情报数据积累
10年+渗透测试经验积累
50000+安全社区/白帽情报源
从攻击者视角梳理完整攻击路径

核心能力
PRODUCTS

卡亭科技 CHAITIN

01 资产发现与管理

发现企业资产
绘制关联图谱

资产数据中台
自动资产盘点
未知资产发现
资产归属关联
资产生命周期管理
智能识别分析

02 攻击面分析

威胁情报集成
主动&被动发现

主动威胁检测
被动信息分析
云安全配置管理
数据集成与导入

03 持续安全巡检

从攻击者视角
持续性验证企业安全状况

规则策略自定义开发
灵活配置与运营
持续安全扫描
持续资产目录更新
定期巡检

04 优先级判断

不被无效噪音淹没

资产重要性分析
漏洞真实风险评估
攻击路径分析
攻击验证
威胁情报

05 风险告警与处理

风险管理效率显著提升

近乎实时的警报
联动集成防御
报警通知管理
统一报告输出
安全建议

应用场景
PRODUCTS

长亭科技
CHAITIN

统一管理多资产、高复杂环境风险

探查与分析企业资产、业务、暴露面等，定位攻击者视角下暴露的潜在风险

持续性攻防演练风险防控

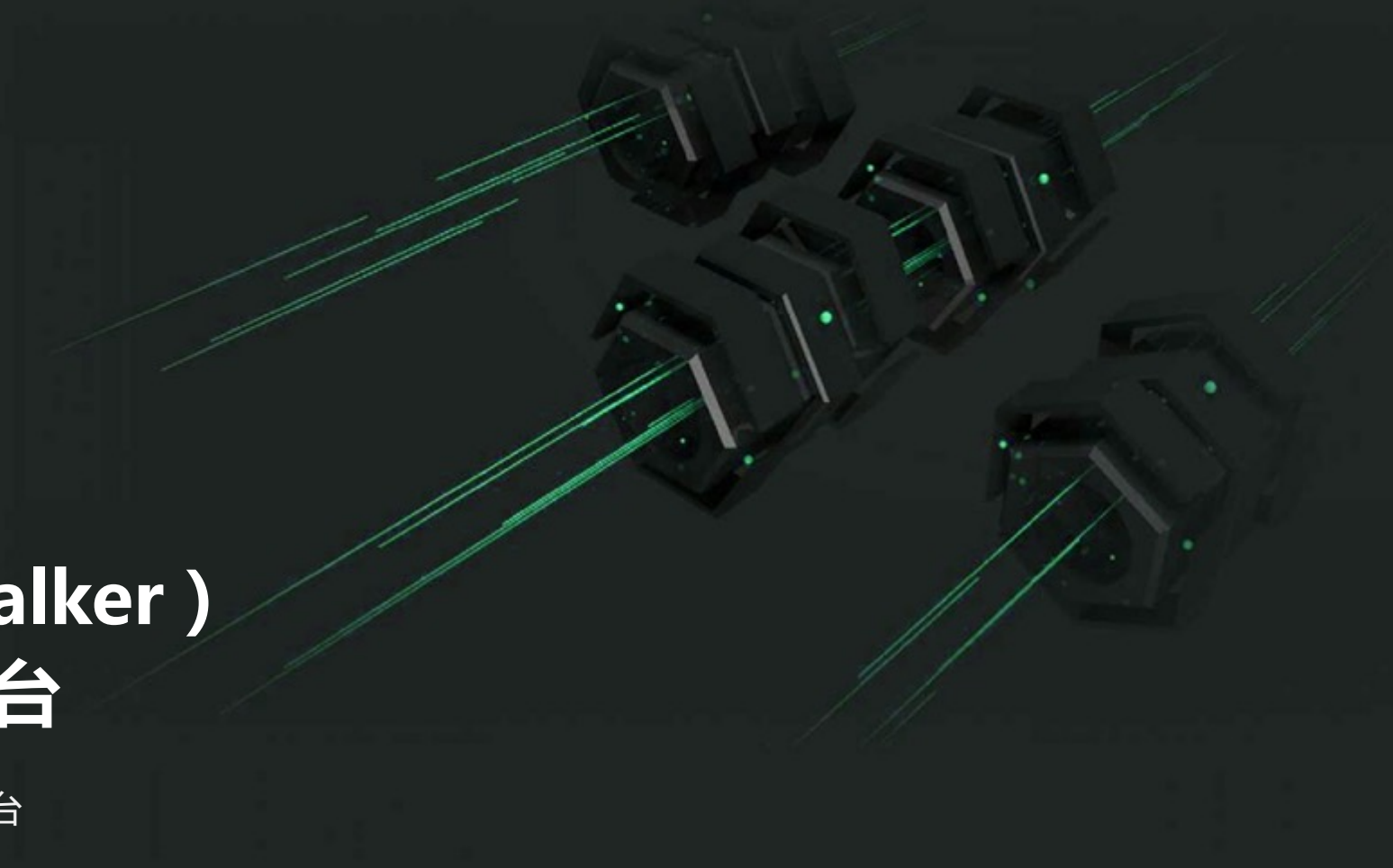
基于攻击者视角，结合资产重要性、漏洞利用情况，梳理排序风险，并持续监控与更新状态

风险快速扫描响应

有效识别企业内网、外网、云上资产、子公司、第三方供应商中存在的漏洞、配置错误、数据泄漏、影子资产等多种风险类型，并实时报警

提升安全运维效率

高效的自动化扫描能力，灵活的配置与运营，具备规则策略自定义开发能力



查 牧云（CloudWalker）主机安全管理平台

基于 Agent 的深度主机安全检测与分析管理平台
以资产安全为核心，以安全事件为驱动
在庞杂的混合云环境下
提供给用户一个不同的观察网络环境的安全视角
提升资产能见度并有效防御入侵

核心功能

PRODUCTS

资产全面清点

多维度收集并集中化管理主机资产
打造全面、清晰、详尽的资产图谱

深度风险感知

持续监控与分析主机资产的漏洞、补丁、弱口令、合规基线等脆弱性

实时检测入侵行为

依托对操作系统的动态监控
实时监控与扫描入侵行为

融合阿里云主机安全因子，适配云上云下多样防护场景

- 公有云
- 私有云
- 混合云
- 虚拟化
- 物理机

产品能力
PRODUCTS

1秒检测反弹Shell
10秒检测WebShell

Agent自定义CPU阈值
管理端灵活策略调度

主机、虚拟机、容器
全面覆盖Agent和端口
融合动态和静态数据

非Root权限探针，零负担
单服务器可支持5000探针
5分钟快速部署

卡亭科技 CHAITIN

历经实战检验
检测能力一骑绝尘

全网首发Log4j2专项检测工具
下载量**10000+**

发现并协助修复
6个隐藏数年 Linux 内核 0day

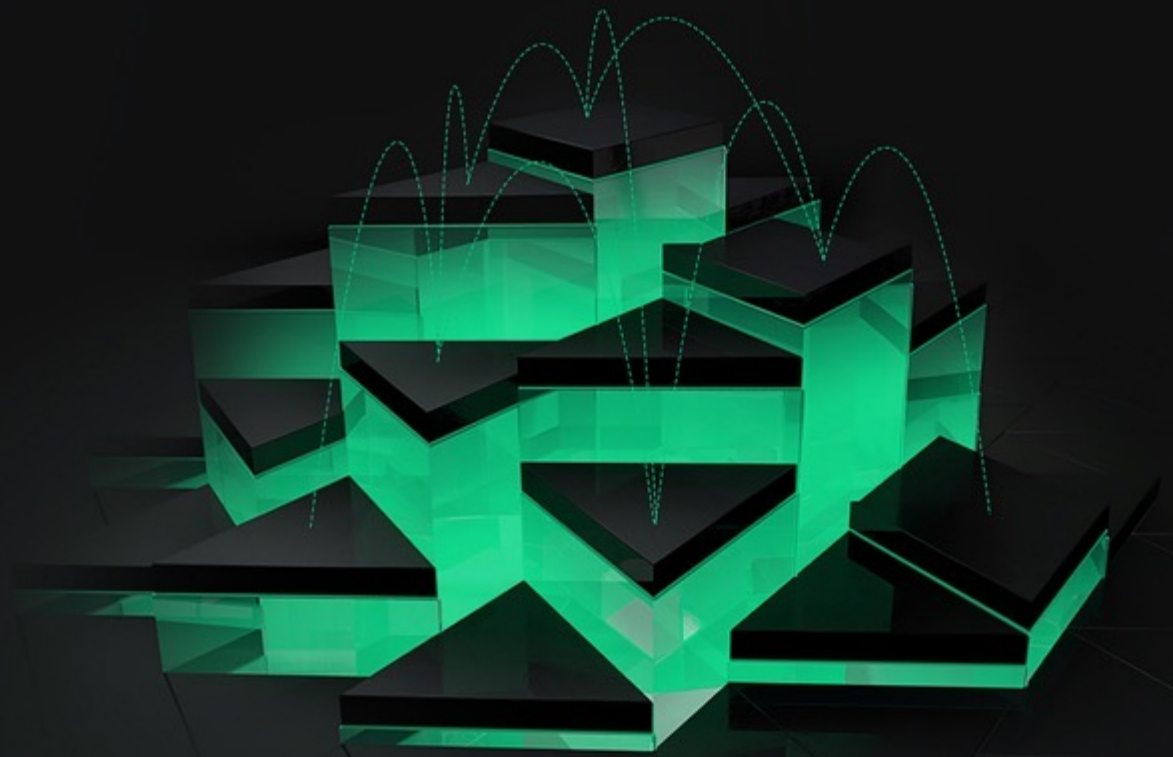
大型**重保期间**
为多家客户检出内存WebShell

多次检测出
冰蝎3.0、哥斯拉等工具特征入侵行为

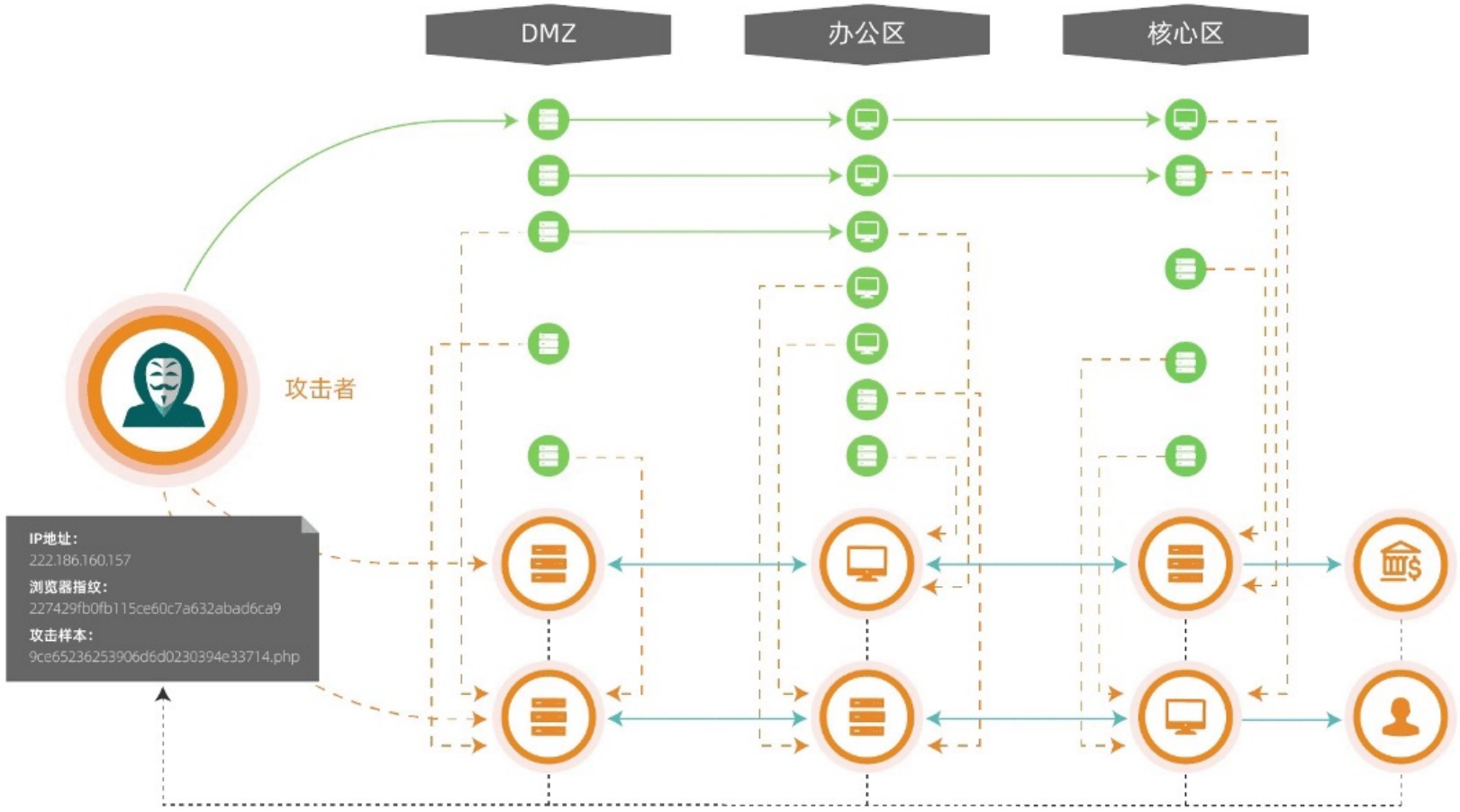
与高交互蜜罐联防联控
攻防演练现场摘得**数百分**

抓 谛听（D-Sensor）伪装欺骗系统

国内第一款基于Deception技术研发出的伪装欺骗系统
通过布置陷阱、诱敌深入、记录路径、溯源取证
解决网络防护难以察觉、难以明确、难以追溯三大问题



核心功能
PRODUCTS



- 异常流量监测与重定向
- 多IP全端口威胁感知覆盖
- 威胁感知与取证分析
- 攻击预警与行为分析
- 攻击者身份溯源与反制
- 威胁监控与展示

产品优势
PRODUCTS

伪装程度高

- 60余种蜜罐，覆盖客户使用的常见框架、服务、工控协议、5G核心网元等，仿真和交互程度高
- 自定义蜜罐页面和数据
- 多种具有真实漏洞或漏洞特征的蜜罐

威胁感知能力强

- 监听多个IP的UDP和TCP全部端口
- 内置自研语义分析引擎，感知多种攻击行为
- 监听Ping探测和ARP欺骗
- 检测容器逃逸行为

溯源精准，反制多样

- 网站账号溯源种类最多，溯源方式隐蔽
- 集成第三方威胁情报，溯源更精准
- 内置git、客户端、MySQL等多种反制方式，获取更多信息
- 完整还原攻击路径，完整记录攻击行为

部署和使用轻量化

- 完美支持云上虚拟化环境
- 蜜罐基于容器技术，使用灵活，占资源少
- 支持配置多IP，仅占用少量计算和网络资源，即可覆盖大规模网络

长亭网页防篡改系统

PRODUCTS

长亭科技 CHAITIN

采用第三代防篡改技术，高效解决网站被非法篡改问题
保障政府和企业业务正常进行

内核事件触发保护机制
实时监控，即刻阻断篡改行为

高安全强度 128 位加密技术
保证信息传输过程完整性及私密性

采用文件驱动级技术的系统
不受变化的内容影响

自动实时监控多个子文件夹
能够检测所有文件类型，
执行准确率高

实时防护大规模连续篡改攻击
检测到非法操作后主动阻断后续操作

先进算法高速上传备份
方便日常维护

长亭深度安全网关

PRODUCTS

长亭科技 CHAITIN

采用高性能多核架构，搭建接口丰富的硬件平台，结合多种检测防护技术
提供安全智能一体化防护体系

深度检测解析内容
让威胁无所遁形

多种检测技术
全面分析用户流量

安全问题闭环治理
多安全方案联动

事前、事中、事后
构建全流程防御体系

集成多样化安全能力
支持各种业务场景

集成防火墙、负载均衡、入侵防御等
功能于一体

结合全网威胁情报
防护未知风险

整合60+开源情报
提供一站式解决方案

多维智能分析
降低运维压力

一体化安全策略
综合分析和集中管理

长亭流量分析预警系统

PRODUCTS

长亭科技 CHAITIN

通过网络流量深度分析，有效实现对APT新型网络攻击的检测和响应，开箱即用
提升企业防护高级威胁攻击的能力，快速建立联防联动的自动化处置方案

核心能力

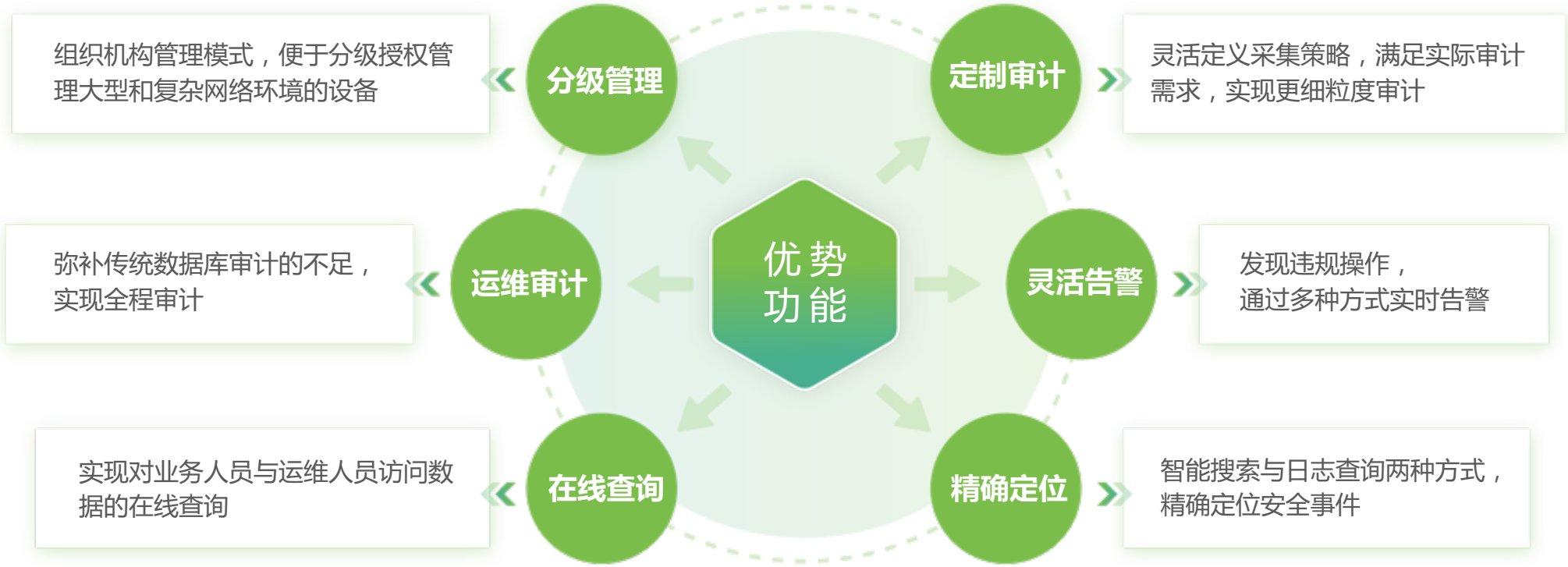
- 流量采集及文件还原
- 高级入侵植入检测
- 高级远程控制检测
- 可视化分析与预测
- 多维报告输出

长亭数据库审计平台

PRODUCTS

长亭科技 CHAITIN

通过协议代理和交换机旁路镜像的方式，全程对所有数据库运维操作进行管控
发现违规操作及时阻断，记录网络中一切对数据库的访问行为



产品价值

- 满足合规性要求 助力安全评测
- 简化业务治理 提高数据安全管理能力
- 完善纵深防御体系 提升整体安全防护能力
- 避免核心数据资产被侵犯 保障业务安全

长亭运维审计与管理平台

PRODUCTS

长亭科技 CHAITIN

集用户管理、授权管理、认证管理和综合审计于一体的集中运维管理系统

集中管理

IT资源统一管理
支持分布式多层级统一管理

系统扩展

多平台对接
丰富的自身管理功能

审计管理

运维行为审计
审计报表
事件追溯

认证管理

登录统一入口
强认证
多认证组合

权限管理

目录树层级管理
自定义管理权限
权限按组节点细分

账号管理

主、从账号同步
生命周期管理

资源管理

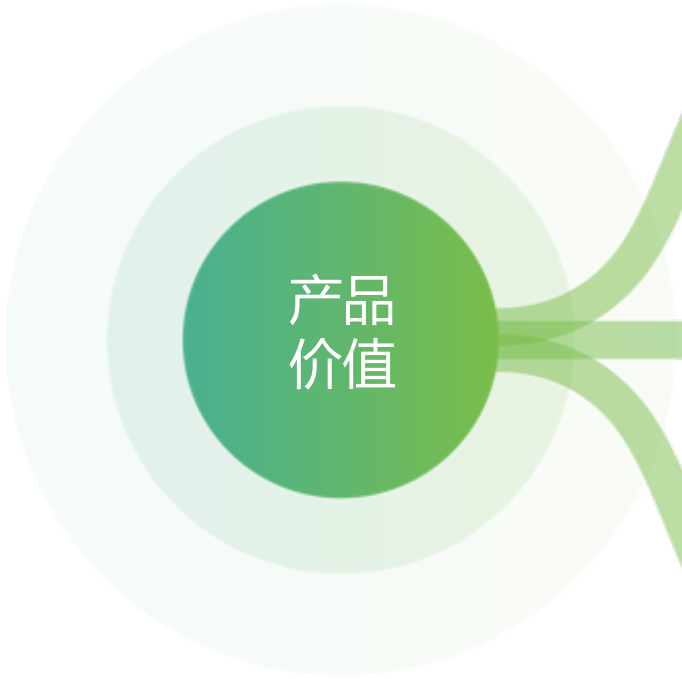
丰富的资源类型

授权管理

管理权限分配
行为权限分配
授权流程管理

长亭日志审计平台
PRODUCTS

集中采集、集中管理、集中审计
信息系统中的各类日志



对于安全管理员、安全分析员、安全运维人员

- 明确工作职责，协同合作
- 提升工作效率，及时应急响应
- 发生安全问题，事后调查有据可循

1

对于企业安全负责人

- 助力安全策略执行
- 持续有效分析安全事件
- 协助审计、取证分析和内部调查
- 统一存储日志与操作行为
- 自动产生各种分析报表和报告

2

对于企业和组织的领导层

- 为安全建设决策提供依据
- 整体安全防护水平
- 提升安全设施的投资回报率

3

长亭上网行为管理系统

PRODUCTS

长亭科技 CHAITIN

网络行为管理和内容审计

防止非法信息传播、敏感信息泄漏，具有实时监控、日志追溯、网络资源管理等能力

利用带宽管理与优化技术，控制过度使用网络资源的协议与用户，提高网络的接入用户数，改善用户上网体验

过滤非法上网行为，记录与审计上网的行为、内容和流量，遵从法律法规审计要求

分别对接公安网监和运营商数据审计接口，满足公安及运营商的数据审计要求

特色技术

精准而全面的协议识别

强劲的高性能与稳定性

完整有效的数据审计

精准智能的流量管理

03

SERVICE

安全服务

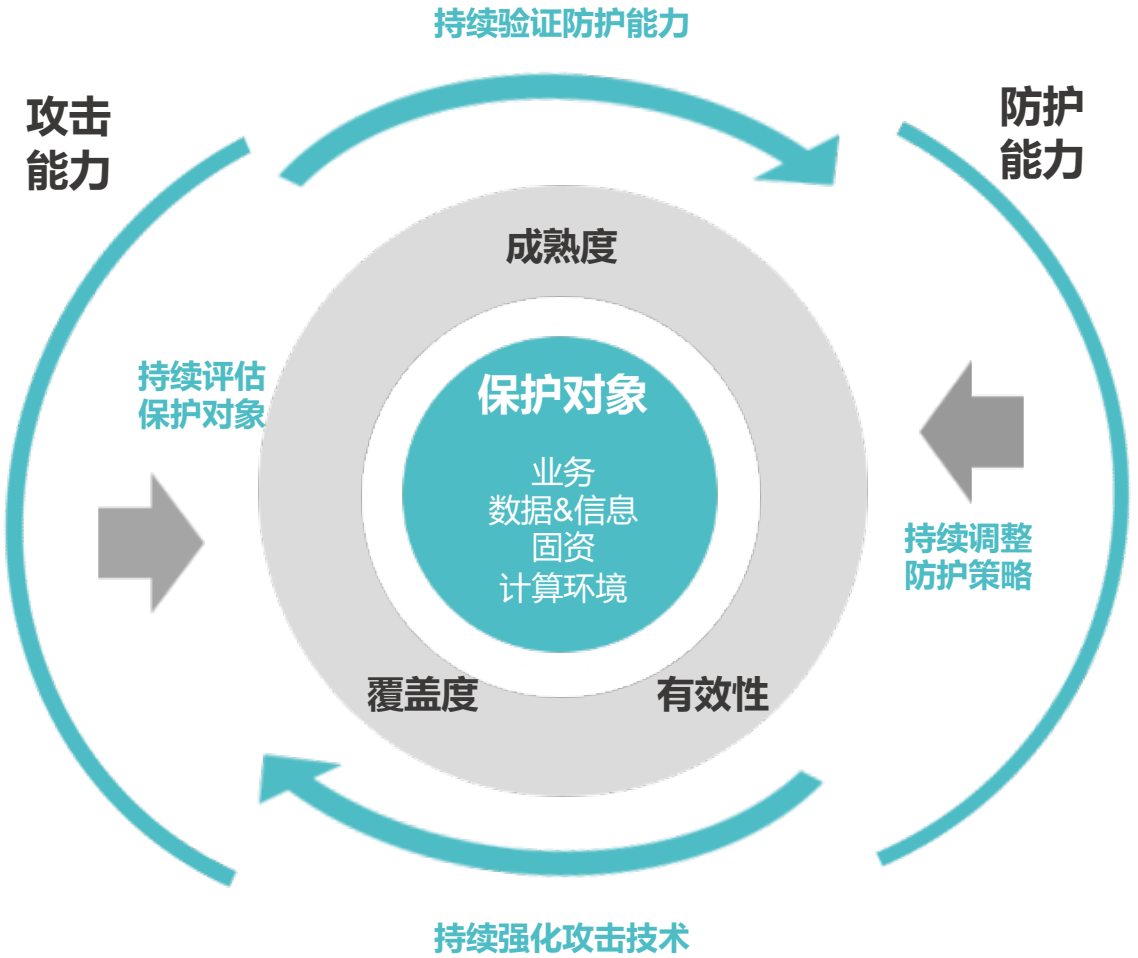
长亭安全服务理念：以攻量防，“敏捷”运营

SERVICE

	难点	解法	
软件开发	软件需求和软件bug随时产生	快速测试（功能+性能） 快速反馈，快速迭代	敏捷开发
安全运营	外部威胁和保护对象复杂多变	以攻量防（有效性+覆盖度） 持续度量，持续提升	“敏捷”安全运营

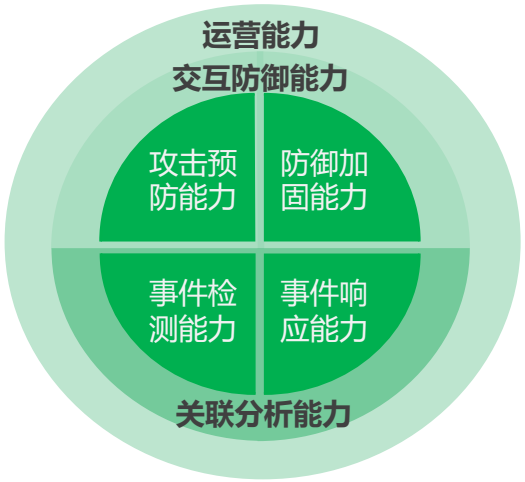
实现“敏捷”安全运营的三个关键点

- 安全度量体系
- 一体化攻防知识库
- 自动化工具平台



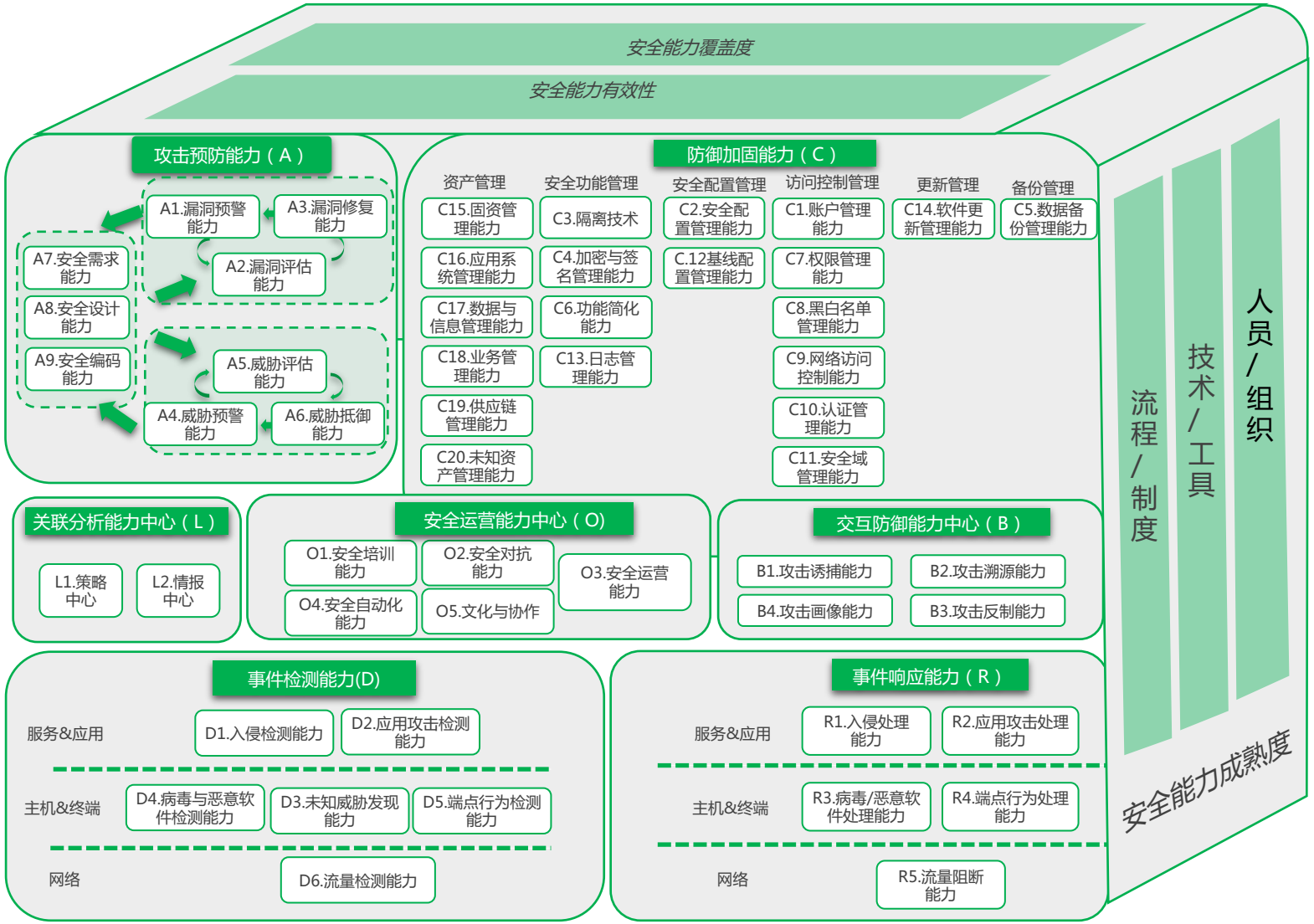
长亭安全能成熟度模型2.0：向运营能力度量延伸

SERVICE



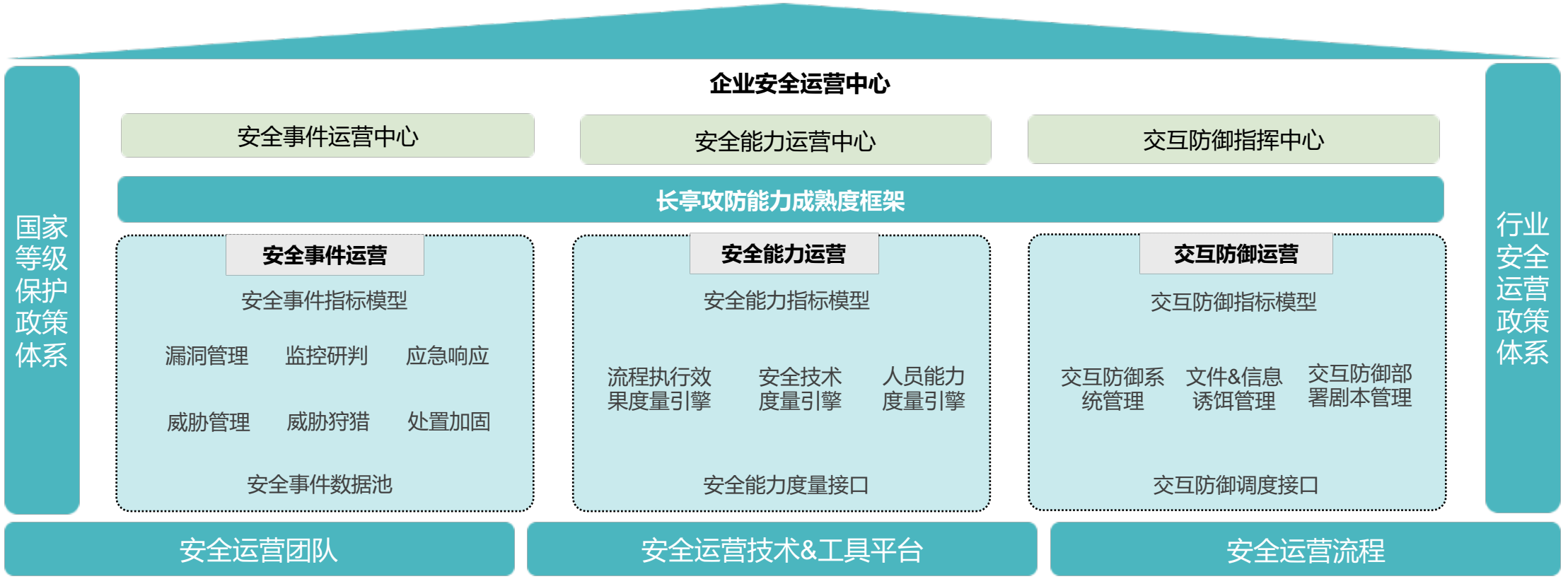
模型参考：

- WPDRRC
- MITRE-ATT&CK
- MITRE-ENGAGE
- ASA2.0
- CMM



长亭安全运营体系

SERVICE



一体

一套体系

即长亭攻防能力成熟度框架体系

两防

两类防御

即传统的被动防御与交互式防御

三中心

三个运营中心界面

分别对应“事件运营”、“能力运营”、“交互防御运营”

安全服务项目一览

SERVICE

综合解决方案

- 实战攻防演练整体解决方案
- 蜜罐运营解决方案
- 重要时期保障解决方案
- 沙盘演练解决方案

评估分析

- 渗透测试
- 专项评估
- 应急响应
- 基线分析
- 攻防演练

培训展示

- “安道场”蓝军专项培训服务
- “安道场”红军专项培训服务
- “安道场”竞赛专项培训服务
- CTF办赛服务
- 珂兰寺

安全咨询

- 等级保护咨询服务
- 商用密码安全评估服务
- 风险评估服务
- 企业信息安全规划服务
- 电子银行评估服务
- SDLC开发生命周期咨询服务
- 容器安全咨询服务
- 企业攻防能力成熟度评估服务

运营托管

- 长期驻场
- 实战攻防演练服务
- 蜜罐运营服务

优势服务

渗透测试服务

- 强大的漏洞储备
- 高效的工具平台
- 丰富的攻防经验
- 专业的服务团队
- 测试方向覆盖Web、APP客户端、PC客户端、无线等

已服务客户**400+**，获得广泛认可

攻防演练服务

- 顶尖国际信息安全大赛技术积累，具备黑客思维
- 丰富项目经验，了解不同场景下的安全诉求
- 定制化攻防演练方案，先攻击者一步发现脆弱环节

已服务客户**150+**

区块链安全服务

- 包含链源码审计、合约审计、区块链设计咨询服务、区块链监控产品等
- 长亭独立的区块链安全研究团队实施

已审计**上百份合约**，技术能力强，经验丰富

国家级攻防演练主防服务

- 融合企业安全攻防能力建设及关键时期安全运营的全部经验与理解
- 体系化设计、全面性保障、可灵活适配，覆盖企业安全建设的各个阶段

连续3年为**27家**客户提供主防服务，覆盖金融、能源、制造等多个行业，协助多家客户取得优异成绩

创新服务

企业攻防能力成熟度评估

- 基于长亭首创且自主开发的企业攻防能力成熟度模型开展的轻量级技术咨询服务
- 根据企业攻防能力成熟度量化指标，深入了解企业安全攻防所处的成熟度级别及与行业标杆的差距，提供完善方向和依据

服务客户**30+**，顺利完成落地

企业安全能力提升服务

- 集培训类运营服务、培训类咨询服务及培训类产品为一体的综合解决方案
- 根据实际情况，灵活构建针对人员能力提升的各类支持，专项解决人才培养的痛点问题
- 实操机会多，培训形式灵活

安道场3期课程，已服务客户**29+**，招收学员**1100+**

蜜罐运营

- 结合蜜罐产品与运营服务，基于实际业务环境，仿真业务系统，定制开发蜜罐
- 专人持续运营蜜罐，定期更新策略，保证蜜罐系统的威胁感知能力
- 提高蜜罐命中率和溯源准确度和成功率

服务客户**15家**

沙盘演练

- 基于对于国家级攻防演练中沙盘环节的经验和理解，结合实际业务情况推出的整体性咨询服务

已在**2家**客户侧完成落地并得到高度评价

在不断变化升级网络信息安全趋势下，长亭科技结合多年安全服务实践经验和技术积累，
以攻防为核心推出多个创新性安全服务

项目经验丰富

3500+个
累计交付项目

1500+家
累计服务客户

27个省 121个市
服务覆盖范围

8个
服务覆盖行业

7年
2015年开始提供服务

攻防能力强

33家
主防客户

236家
协防客户

Top3
国内大型攻防演练成绩

超过99%
防守率

100+家
客户感谢

深入安全研究

3大机构
CVE、CNVD、CNNVD

近万个
累计收录漏洞

16%
超危漏洞占比

63%
高危及以上漏洞占比

数百个
0day漏洞

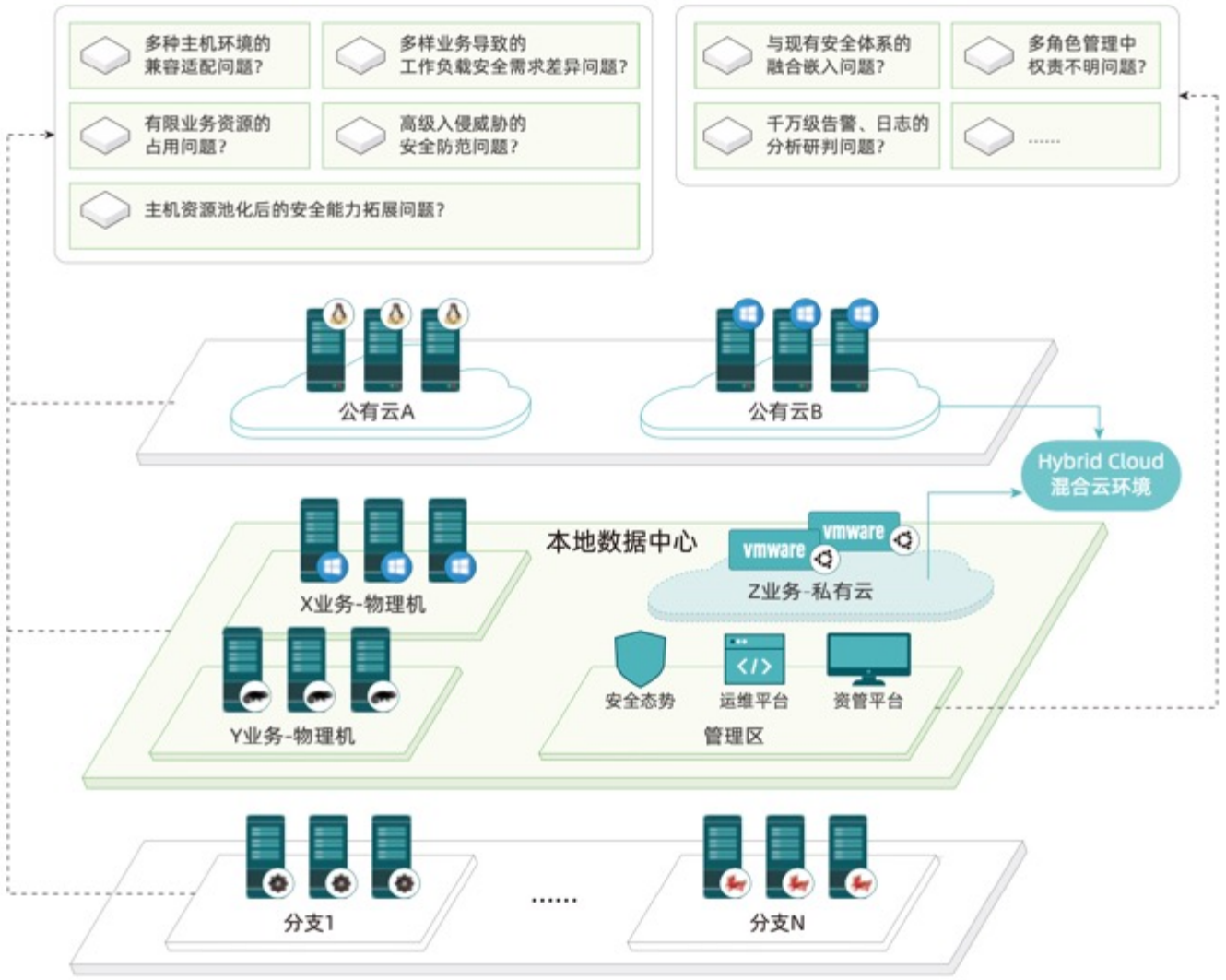
04

SOLUTIONS

解决方案

解决方案
SOLUTIONS

大规模主机资产风险管理解决方案



复杂业务架构下主机风险管理痛点

方案简介

数字经济蓬勃发展，在服务器规模扩张、云化进程推进、暴露窗口增多、攻击价值提升等因素影响下，大规模主机的资产风险管理面临多项挑战。

该方案通过**牧云（CloudWalker）主机安全管理平台**的集群部署，协助大规模主机管理者构建主机资产风险管理体系，满足合规、实战对抗等多种场景的安全要求。

方案优势

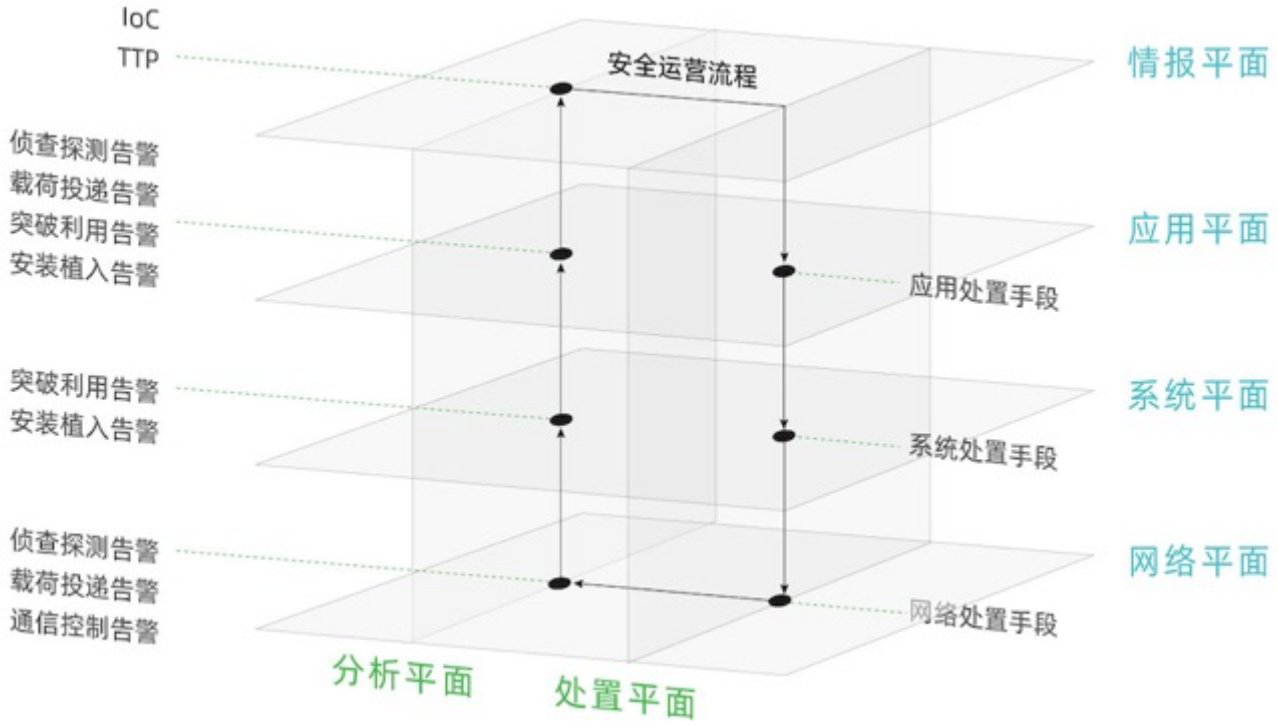
- 基于K8s的长亭分布式滑板车底座保障管理端自由伸缩、水平拓展
- 轻量化非root探针降低负载，灵活定义阈值
- 多种检测模式搭配选择，灵活策略满足业务需求
- 过滤筛选，支持安全事件的闭环管理
- 基于RBAC的灵活赋权满足多部门管理需求
- 开放的第三方联动，内嵌已有IT架构

攻防演练前线防守运营方案

方案简介

攻防演练活动日趋常态化，由于参演单位的组织架构、职能分配不同以及缺乏体系化的安全运营机制，导致“安全监控组”、“研判分析组”、“事件处置组”在实际工作执行中难以有效协同配合，防守工作低效，甚至影响防守成绩。

长亭科技通过大量的实战经验积累与理论模型参考，打造纵深式一体化的“点、线、面、体”实战防守运营体系，通过标准化梳理点状告警、高效推进分析研判流程、完善应急处置手段，帮助客户更加有效地展开攻防演练备战工作，提升战时防御水平。



方案优势

- 精准定位防守关键点，确保网络流量检测与防护设备覆盖到所有潜在攻击路径，快速收敛风险
- 动态关联所有点状告警信息、威胁情报，快速构建入侵分析流程，缩短应急处置窗口期
- 丰富的攻防实战经验积累和沉淀，补充处置过程中的欺骗和溯源反制能力，补齐安全短板
- 全面梳理防守单位组织架构和业务特点，提升安全监测响应、分析研判、应急处置及协作配合水平

SDL建设中“安全左移”方案

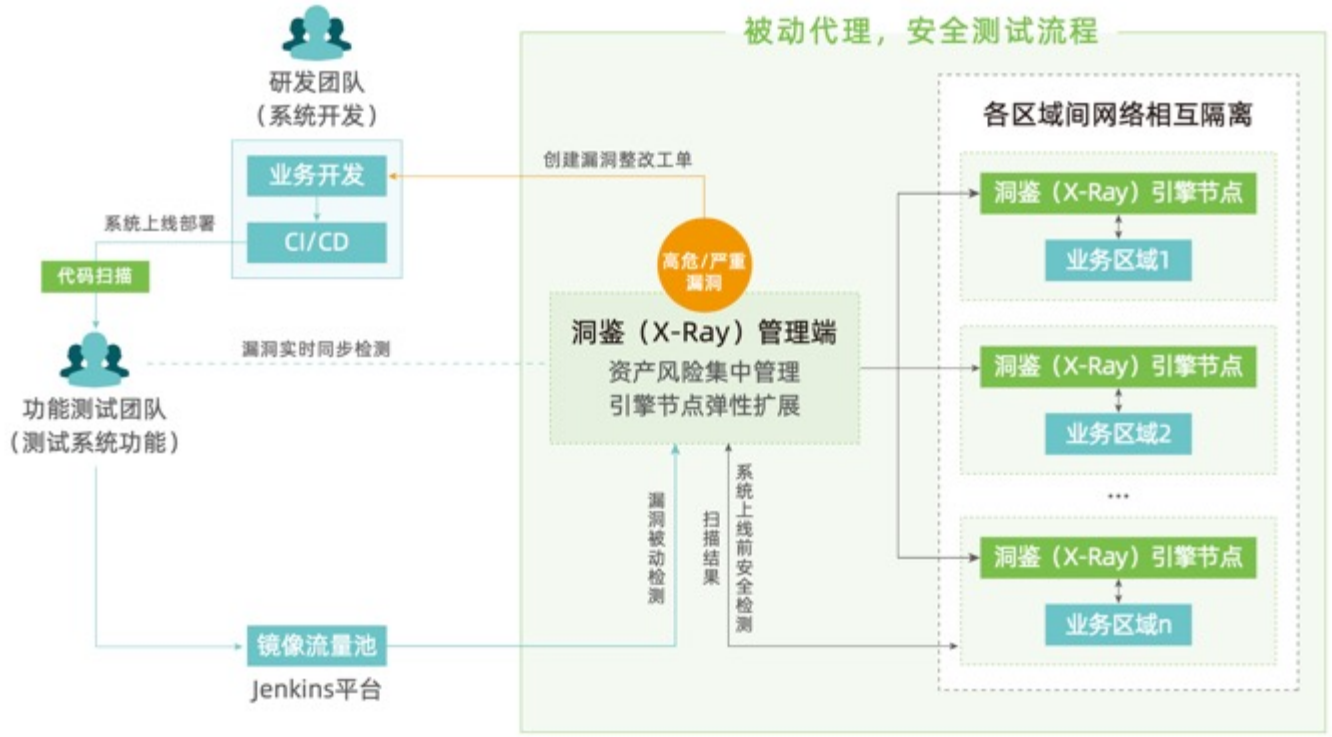
方案简介

早在2012年Gartner报告便提出：安全风险越靠近运维侧，则企业要花费的安全成本越高。但长期以来，业界的安全防护更多的侧重于软件上线后，而对研发阶段的安全投入不多。

洞鉴（X-Ray）可通过被动代理模式嵌入客户SDL流程，前置安全测试关口，为安全部门争取充足时间以保障安全检测效率，帮助客户在现有SDL流程架构下实现安全左移。

方案优势

- 实现更早的在SDL流程中执行安全测试，从而提高测试效率、加强业务系统安全性
- 创新性的PoC验证式漏洞检测技术自动完成漏洞探测过程，具有准确性高、误报率低的优势
- 提供针对主机和Web资产的主、被动探测能力，依托自主开发的扫描引擎，全面覆盖企业资产信息收集需求
- 针对目标资产进行全生命周期闭环管理，促进安全管理制度流程高效运转



SDL流程优化后业务上线流程示意图

特色业务场景
SOLUTIONS

政务云集约化安全建设方案
搭建应用安全塔防体系，实现政务云上安全防护能力的补充升级，满足在政府网站集约化中的安全合规要求，有效应对应用安全风险。

证券行业Web应用安全解决方案
以可用性为中心，建立多级熔断高可用机制、WAF流量处理效能双重保障机制，有效应对检测服务和流量处理问题，保障业务平稳运行。

手机银行加密数据安全检测方案
利用嵌入式SDK将完成解密的流量引流到WAF集群中，对数据进行研判，并通过SDK返回攻击判定结果，完成对应的检测/阻断动作。

常态化蜜罐运营服务方案
谛听（D-Sensor）伪装欺骗系统与常态化安全运营服务相结合，由剧本设计、定制蜜罐、平台部署、运营服务四个部分构成，通过蜜罐的常态化运营，最大化提升伪装欺骗效果。

云平台多租户资产风险管理解决方案
洞鉴（X-Ray）轻量化分布式部署模式，满足云端资产风险统一管理和租户侧弹性扩展、风险自查的需求，实现有效的资产风险管理。

大流量网站架构Web应用安全防护方案
雷池（SafeLine）下一代Web应用防火墙软件集群部署方案将功能模块化，能够把不同的功能组件部署至特定的服务器，根据企业实际需求进行组合，充分利用服务资源，满足大流量、高并发、可扩展的要求。

“大探针”全覆盖欺骗防御方案
谛听（D-Sensor）“大探针”通过网口配置在一个网络区域内实现多个IP和多个蜜罐绑定，在节约资源、成本的同时尽可能多地部署伪装欺骗节点，迅速扩大欺骗范围，实现快速威胁感知和诱捕。

金融机构重大活动安全保障方案
基于金融机构业务特点和防护要求，方案密切关注重点业务系统和网络基础设施，以梳理筹备、摸底评估、布防加固、模拟演练、值守保障、整改优化的工作步骤，提供一体化保障体系，协助完成重保任务。

金保信社保卡

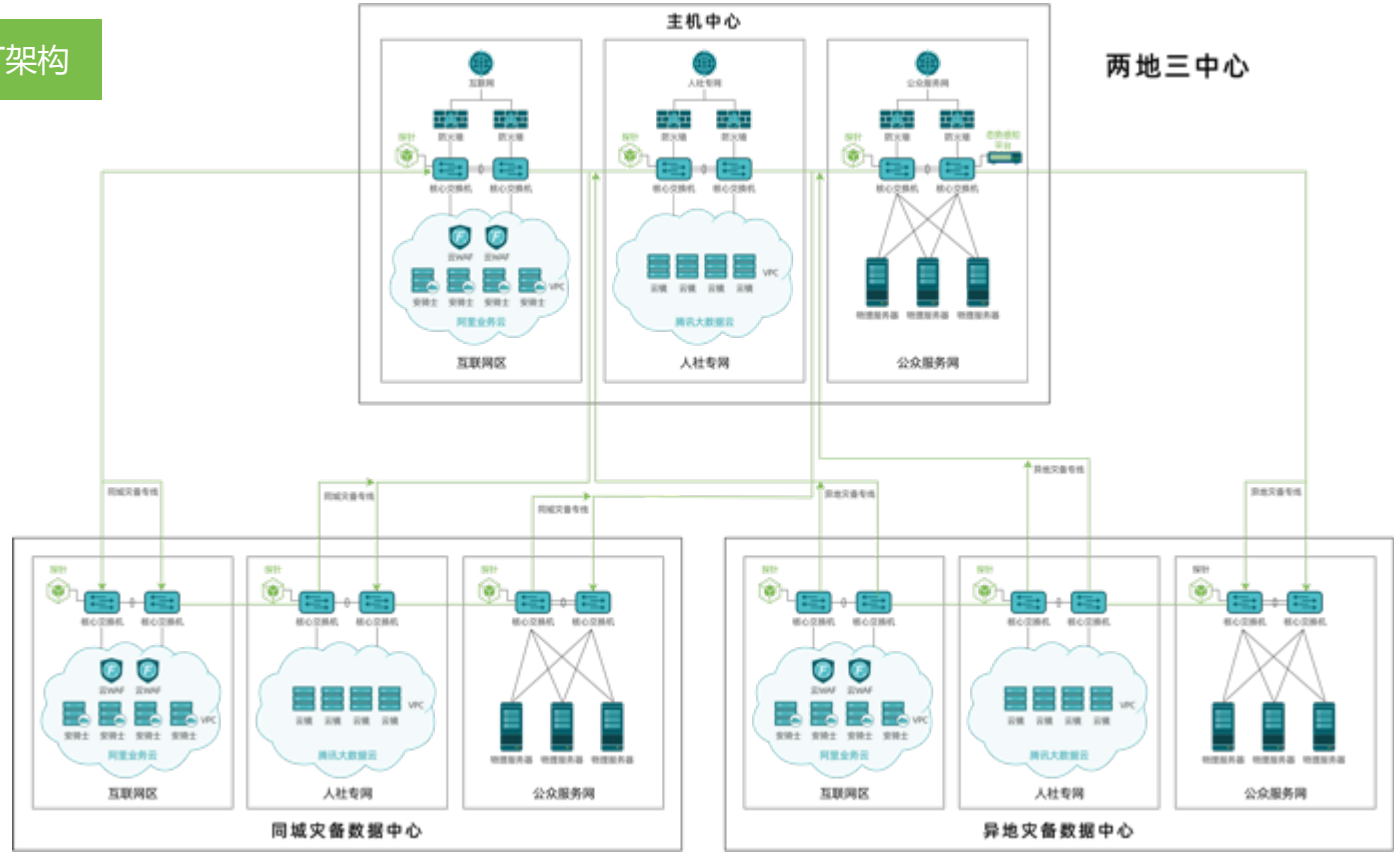
全国电子社保服务提供商 | 业务分布三朵云 | 两地三中心IT架构

服务内容

以长亭科技万象（COSMOS）安全分析与管理平台为底座，在公众服务网运维区域，接收来自互联网、人社专网流量探针和网络中安全设备的安全数据，提供一平台三探针覆盖主数据中心，同城灾备及异地灾备数据中心的态势感知持续扩张。

价值优势

- 提供高性能的底层平台
- 提供平台+服务的模式，解决高级别安全问题
- 数据聚合降噪能力处于业界领先水平
- 提供完整的同城灾备及异地灾备方案，具有可落地的实施步骤
- 提供友商的威胁情报对接接口
- 提供完整的SOAR能力，提供多种剧本，可根据客户现场环境进行



某部委单位

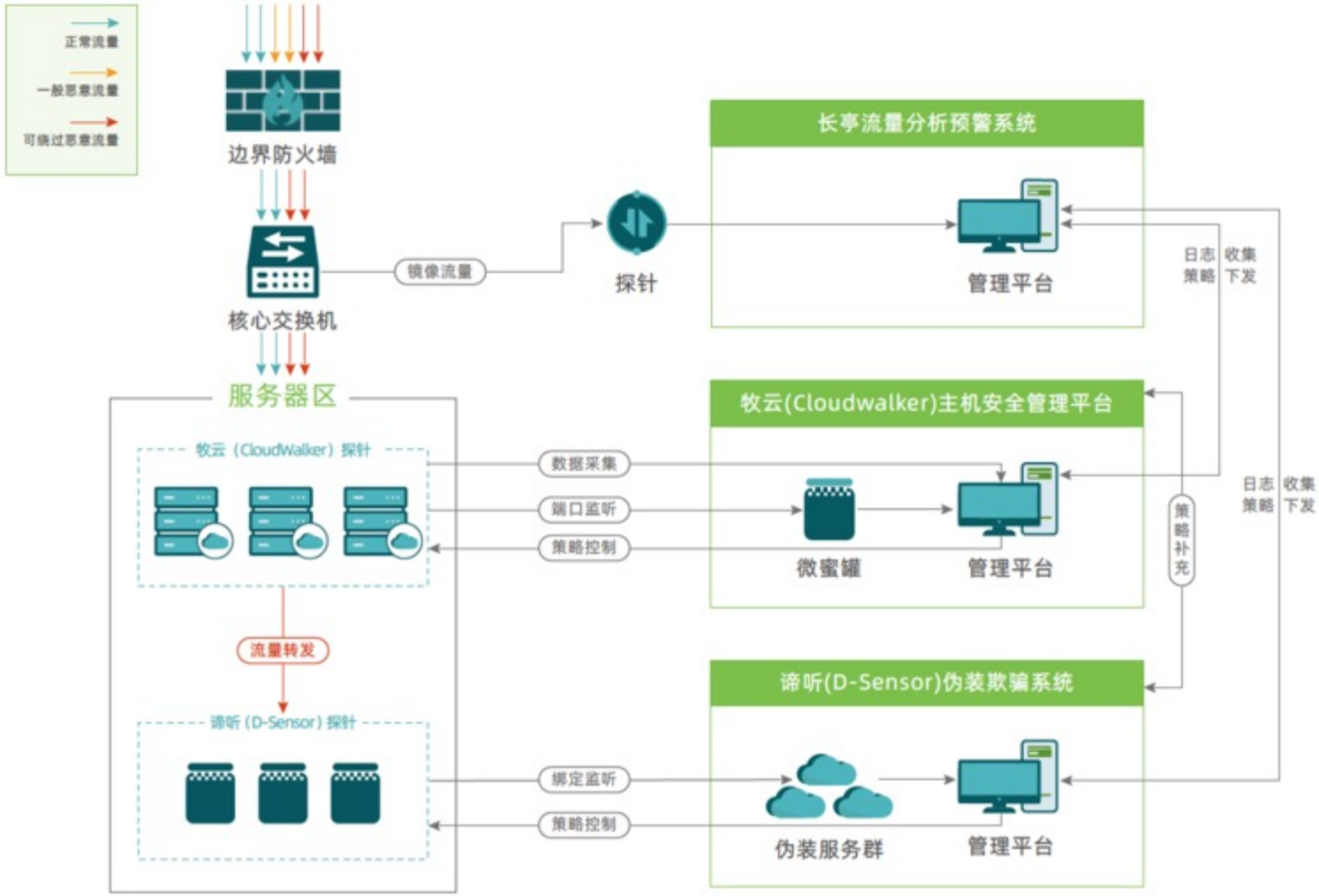
APT攻击对抗 | 国产化适配 | 内网入侵检测

服务内容

通过部署牧云（CloudWalker）主机安全管理平台、谛听（D-Sensor）伪装欺骗系统、长亭流量分析预警系统，形成蜜-网-端内网威胁监测体系，提供准确、全面、真实的入侵威胁告警信息，大幅提升APT攻击威胁的抵御能力。

价值优势

- 提升攻击监测能力，实现APT攻击的发现与处置（发现“海莲花”APT攻击并协助处置）
- 借助牧云（CloudWalker）微蜜罐功能，扩大谛听（D-Sensor）覆盖范围，形成全覆盖蜜网，提升内网入侵威胁检测范围
- 基于长亭流量分析预警系统的蜜-网-端架构，通过综合分析提升准确性，减轻运维负担
- 支持适配国产化环境，实现内网主机资产的统一风险管理



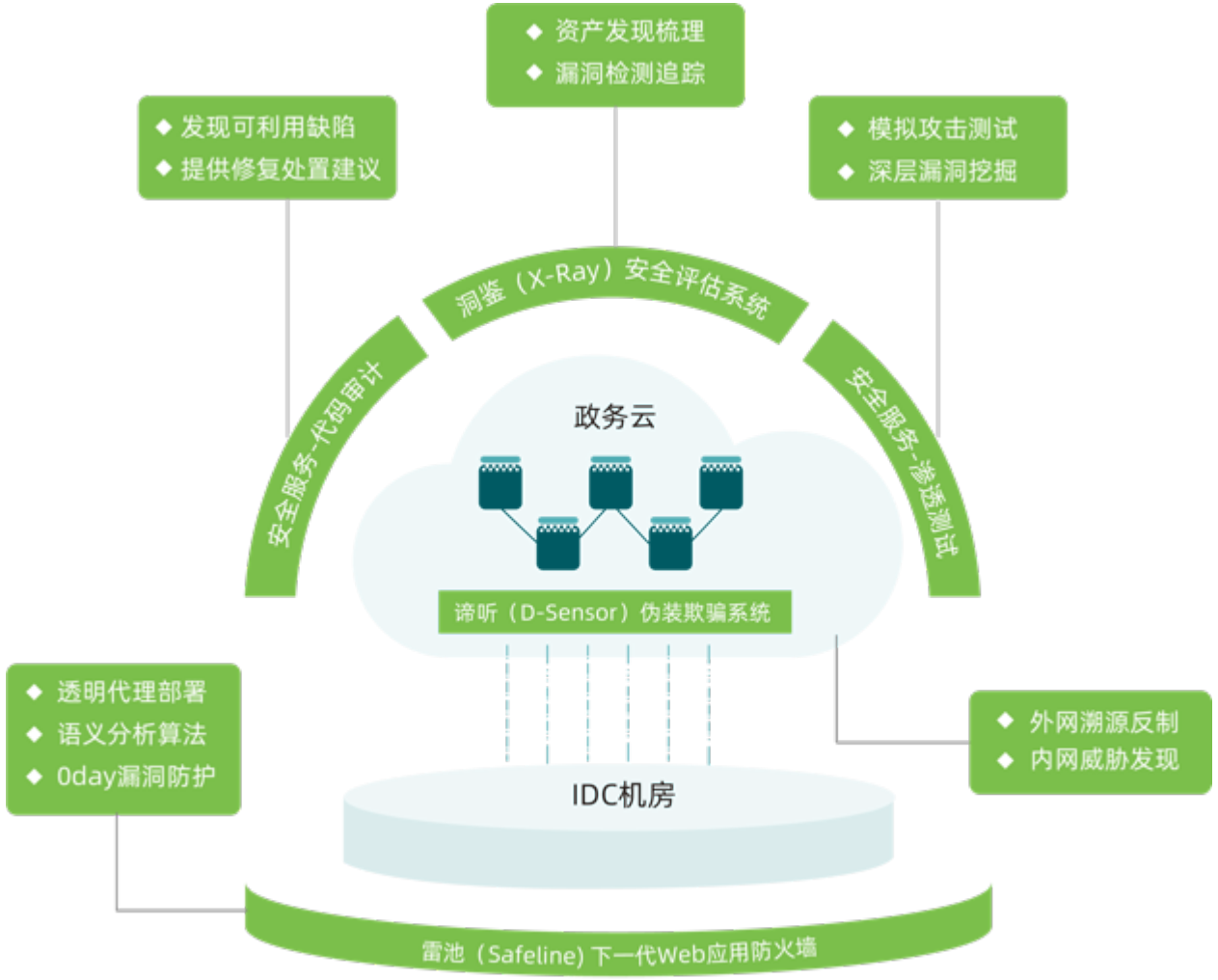
宁夏电信

政务云等“八朵云”· 云平台安全塔防体系

补充政务云缺失安全能力，初步构建安全塔防体系底座，
增强高级威胁应对能力。

价值优势

- 实现应用层防护能力、内网威胁检测、主动溯源反制、资产风险管理等能力的提升，完成安全塔防体系的初步构建，提升了高级威胁抵御能力
- 通过外部攻击视角、内部白盒视角双维度的深度安全检查，发现并整改大量系统缺陷，显著提升业务系统健康度
- 轻量化资源占用，有效减轻安全运维压力，紧急漏洞（Log4j2）协助应对处置，极大减轻应急响应压力



宁夏政务云平台网络安全塔防体系

大型金融机构

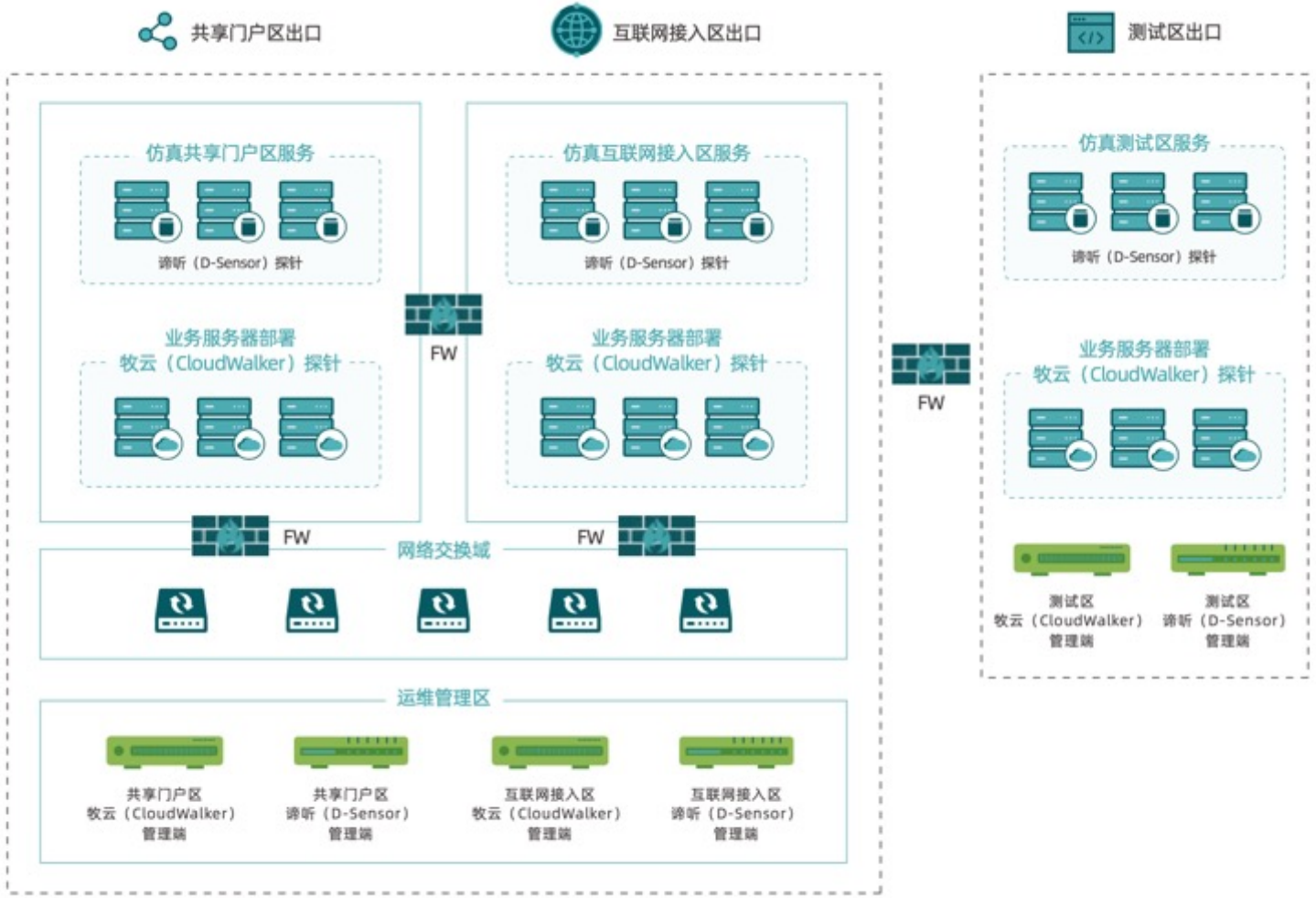
主机防护　蜜网体系　欺骗溯源

服务内容

生产网（互联网接入区、共享门户区）、测试网区部署长亭谛听（D-Sensor），并引入牧云（CloudWalker）对业务资产进行精细化自动梳理，提升主机侧安全预警、检测、防护、响应能力。同时牧云（CloudWalker）的微蜜罐与谛听（D-Sensor）管理端，共享情报，策略联动，形成主被动融合式蜜网防护体系，全面提升内网威胁检测与防御能力。

价值优势

- 提供持续实时入侵检测和响应能力，大幅提升了主机安全性
- 联防联控，打造主动+被动相结合的联动蜜网防护体系，全面阻击内网入侵
- 国家级攻防演习保障期间，蜜罐剧本精准获取攻击者设备指纹、社交信息、位置信息等，提供大量高价值的情报信息
- 连续两年通过谛听(D-Sensor)反制蜜罐反控场内攻击队， 帮助客户取得优异成绩



网络拓扑示意图

大型企业

Unilever
McKinsey & Company
吉利汽车 GEELY AUTO
CapitalOne
贵州茅台集团
BGI华大
绿网天下 green net world
SF EXPRESS 顺丰速运
雪球
PERFECT DIARY 完美日记
SHISEIDO GINZA TOKYO

消费电子

HUAWEI
Nikon
科大讯飞 IFLYTEK
vivo
Panasonic 松下电器
PHILIPS
MOREVFX

证券&保险

招商证券 CHINA MERCHANTS SECURITIES
国泰君安证券 GUOTAI JUNAN SECURITIES
兴业证券 INDUSTRIAL SECURITIES
国信证券 GUOSEN SECURITIES
中原证券
财富证券 FORTUNE SECURITIES
广发证券 GF SECURITIES
安信证券 ESSENCE SECURITIES
太平洋保险 CPIC

电子商务

美团
小红书
去哪儿 Qunar.Com
每日优鲜
度小满金融 Du Xiaoman Financial

互联网

ByteDance 字节跳动
滴滴出行
babytree 宝宝树
VIPKID
FACE++
KK

航空

中国南方航空 CHINA SOUTHERN
春秋航空 SPRING AIRLINES
河南机场集团

教育

清华大学 Tsinghua University
中山大学医学院
南开大学 Nankai University

能源

国家电网公司 STATE GRID
中国水利
中国石化 SINOPEC

国有大型银行

中国建设银行 China Construction Bank
中国工商银行
中国农业银行 AGRICULTURAL BANK OF CHINA
中国银行 BANK OF CHINA
交通银行 BANK OF COMMUNICATIONS

长亭科技 CHAITIN

股份制商业银行

平安银行 PING AN BANK
兴业银行 INDUSTRIAL BANK CO.,LTD
华夏银行 HUAXIA BANK
Bank 中国光大银行 CHINA EVERBRIGHT BANK
广发银行 CHINA GUANGFA BANK
中国民生银行 CHINA MINSHENG BANK
浦发银行 SPD BANK

城市、农村商业银行

汉口银行 HANKOU BANK
江苏银行 BANK OF JIANGSU
广西北部湾银行 GUANGXI BEIBU GULF BANK
桂林银行 GUILIN BANK
徽商银行 HUISHANG BANK
郑州银行 BANK OF ZHENGZHOU
柳州银行 BANK OF LIUZHOU
中原银行 ZHONGYUAN BANK
东莞银行 BANK OF DONGGUAN
浙商银行 CZBANK

政策性银行

国家开发银行 CHINA DEVELOPMENT BANK
中国农业发展银行

音视频网站

bilibili
快手
抖音
荔枝

运营商

中国移动 China Mobile
中国电信 CHINA TELECOM

政府

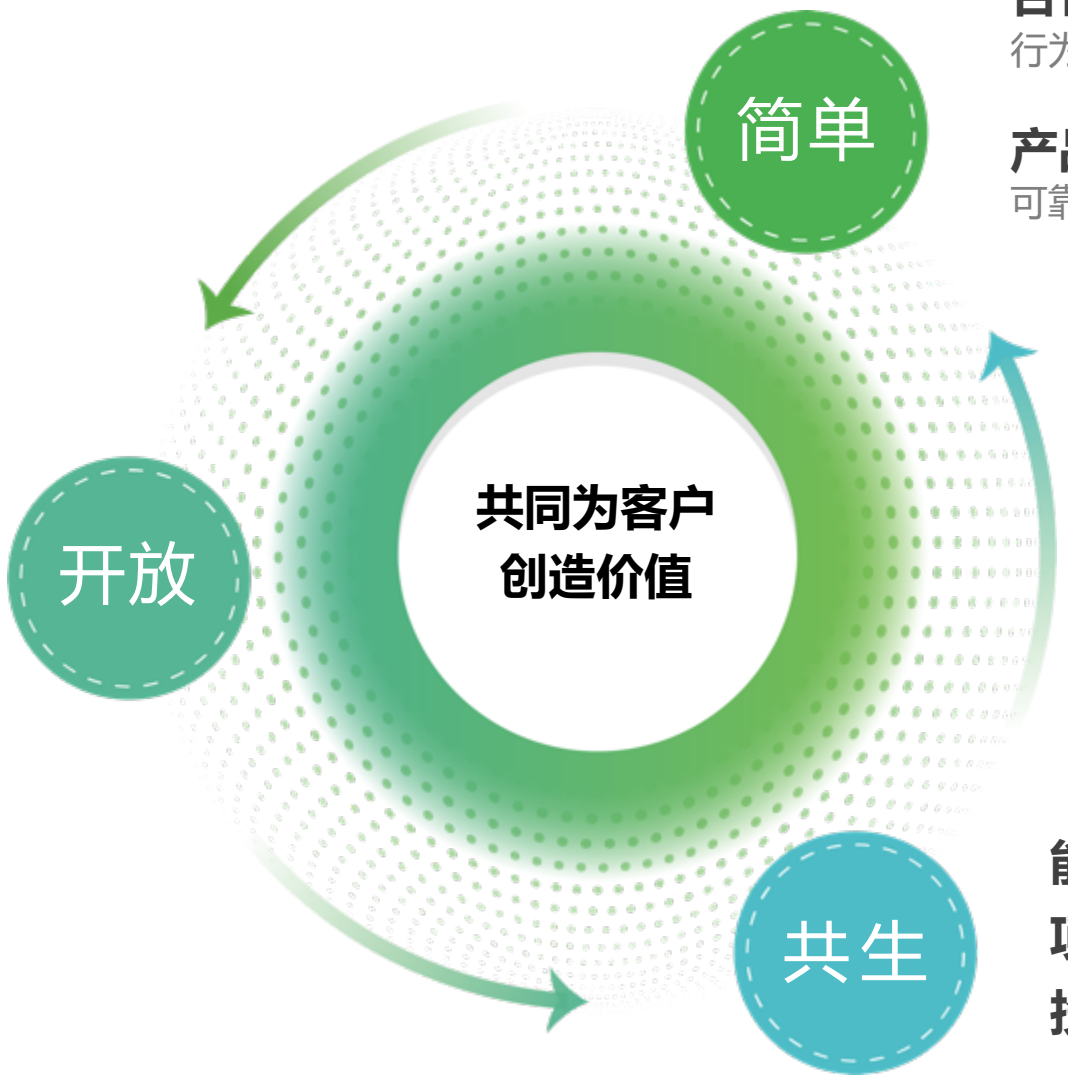
中华人民共和国工业和信息化部
中国科学院
中华人民共和国国家互联网信息办公室
国家体育总局
中华人民共和国公安部
中国地震局
中华人民共和国教育部
中共中央宣传部
中华人民共和国商务部
中国疾病预防控制中心
外交部
中华人民共和国水利部
中华人民共和国人力资源和社会保障部

05 PARTNERS

合作生态

“简单、开放、共生”伙伴关系

PARTNERS



合作简单透明
行为规范、秩序维护

产品简单省心
可靠性、易部署

全行业开放
不圈地
所有客户资源全开放

全能力开放
API接口、x-ray社区、长亭学堂
全开放

合作全开放
匹配不同类型渠道合作方式
合作模式全开放

能力共生
项目共济
投入共赢

合作体系
PARTNERS

镇星级、揽月级、逐日级合作伙伴
代理长亭科技产品和服务销售给用户

解决方案合作伙伴
和长亭科技共同打造联合解决方案或共同开发运营等合作

服务商合作伙伴
承载长亭科技产品技术实施交付服务

2000+

生态合作伙伴

31个

省市覆盖

1.5亿

签单业绩

06

CAPABILITIES

公司实力

技术影响力

CAPABILITIES

卡亭科技 CHAITIN

全球首次

- 发布语义分析检测引擎，打破20年历史检测规则，质变提升检测精准率
- 发现存在Tomcat中的漏洞，命名为“幽灵猫（GhostCat）”
- 完成VMwareESXi虚拟机逃逸
- 创造基于真实世界软件的全新CTF赛制，创办Real World CTF国际网络安全大赛

国内首个

- Log4j2专项检测工具，下载量1万+
- PS4远程越狱
- 原班人马从商业产品中脱胎出免费漏洞扫描工具x-ray，总用户数近10万
- 将Deception技术落地并成功商业化的欺骗伪装系统

5项规范编制

金融、私有云、区块链
深度参与

- 人民银行《金融安全Web应用服务安全测试通用规范》
- CNVD《2020年区块链安全态势感知报告》
- CNVD《区块链漏洞定级细则》
- 《国家广播电视总局关于引发区块链技术应用系列白皮书的通知》
- 安全牛《私有云环境下的安全能力构建》

5个联合实验室及基地

产、学、研

- 浙江泰隆商业银行信息安全联合实验室
- 无锡农商行联合安全实验室
- 光大科技联合安全实验室
- 中原消费金融联合安全实验室
- 中国海洋大学网络空间安全研究联合培养基地

自带云基因，研发思路与云原生高度一致

CAPABILITIES

安全能力与技术底座独立

- 普通资源实现“大能力”
- 200W级别的大流量检测能力

7层接入方式

天然集成云网络架构的业务模型：

- 7层：LB、Sidecar
- K8s：Ingress、LoadBalance

工程化+科学化思想

- 核心产品全部采用云原生弹性底座
- 全部业务都基于容器化方式交付

模块化，快速解耦&组合

- 专项工具应对紧急事件
- 引擎能力化
- 多种商业合作模式

深度集成云底座

- 适配云环境：云底座、高可用场景、云原生网络架构、云原生基础组件和中间件
- 适配云的业务场景和运营需求
- 适配多租户权限控制体系
- 和云上产品联动

1+1>2，释放安全能力

- 利用云上提供的稳定设施（EIP等）保障自身稳定性
- 云原生模式，检测云上业务的流量和云平台自身流量
- 透明接入模式，保障了云平台本身的安全性，又不影响云平台自身的可用性

全球三大权威咨询机构大满贯认可

CAPABILITIES

FORRESTER®

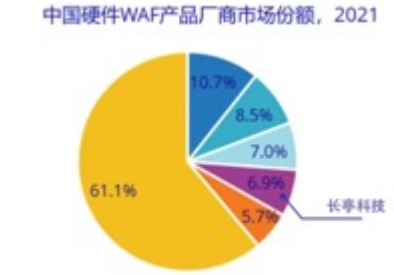
2次入围Now Tech报告 被评为WAF Specialist

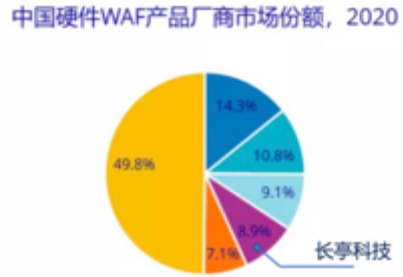
IDC ANALYZE THE FUTURE

入选《中国Web应用安全市场》潜力厂商

牌。最终入选本次报告的厂商包括（按照拼音字母顺序）：**阿里云、安恒信息、安全狗、长亭科技、迪普科技、Fortinet、绿盟科技、奇安信、启明星辰、瑞数信息、盛邦安全、深信服、腾讯云、新华三。**厂商评估结果基于IDC MarketScape模型以图像的形式呈现。

2020-2021中国WAF市场份额排名第四





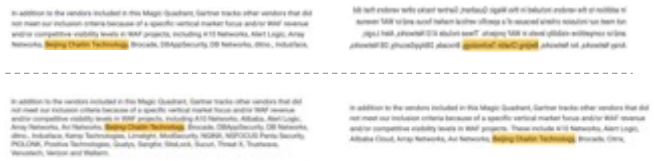
Gartner

入选2018亚太版WAF魔力象限

Asia/Pacific Context:
'Magic Quadrant for
Web Application Firewalls'

4次提名全球WAF魔力象限

2017年因技术先进性成为最年轻入选者
2018-2020年以技术创新WAF连续被提名



2021-2022 ICT报告，获云安全领域推荐供应商

屡次登榜国内研究机构榜单

CAPABILITIES

4次

年度安全厂商
100强

9次

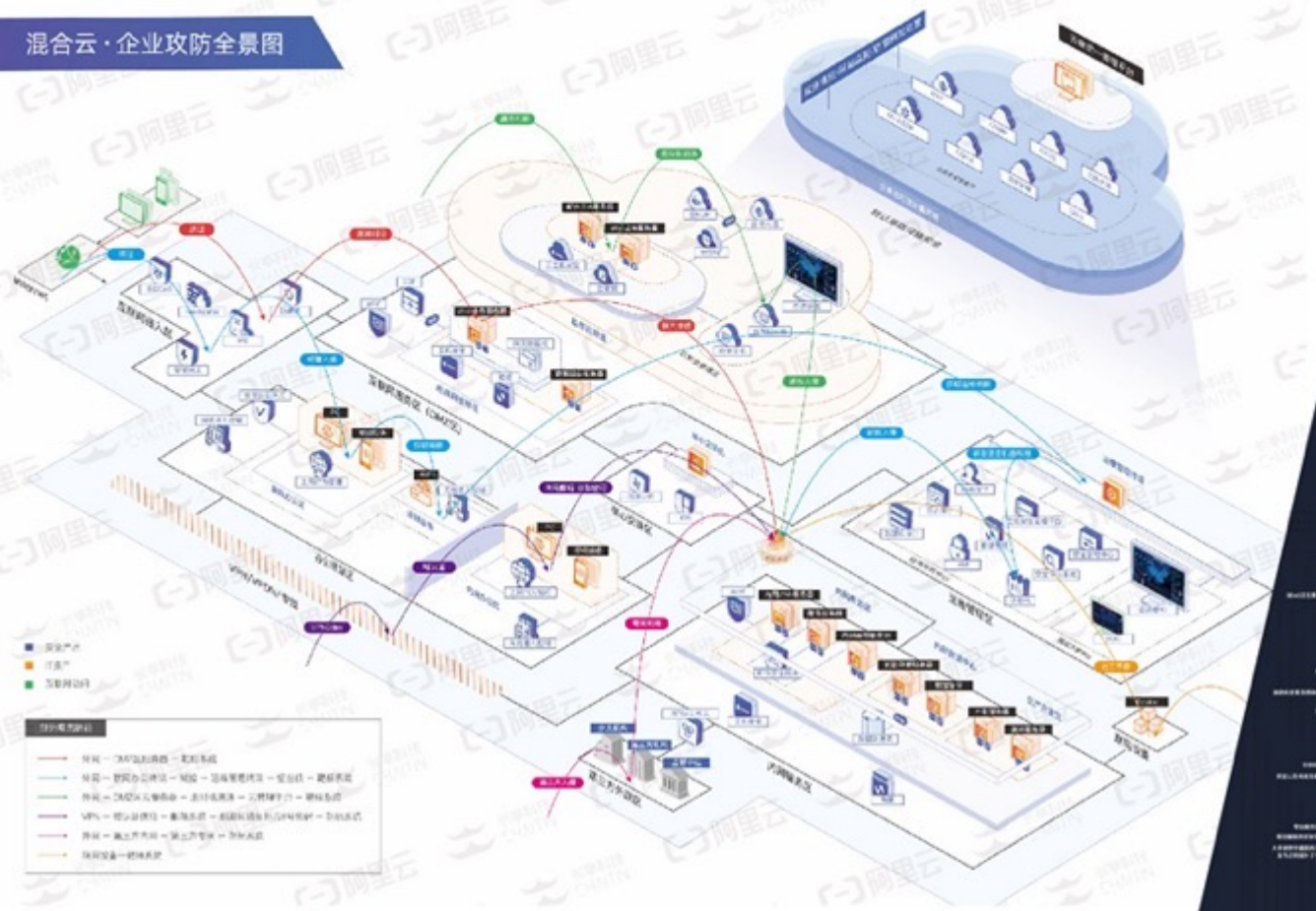
入选行业能力
全景图

排名24

2021年
安全牛百强

“酷厂商”

2018年度



首个

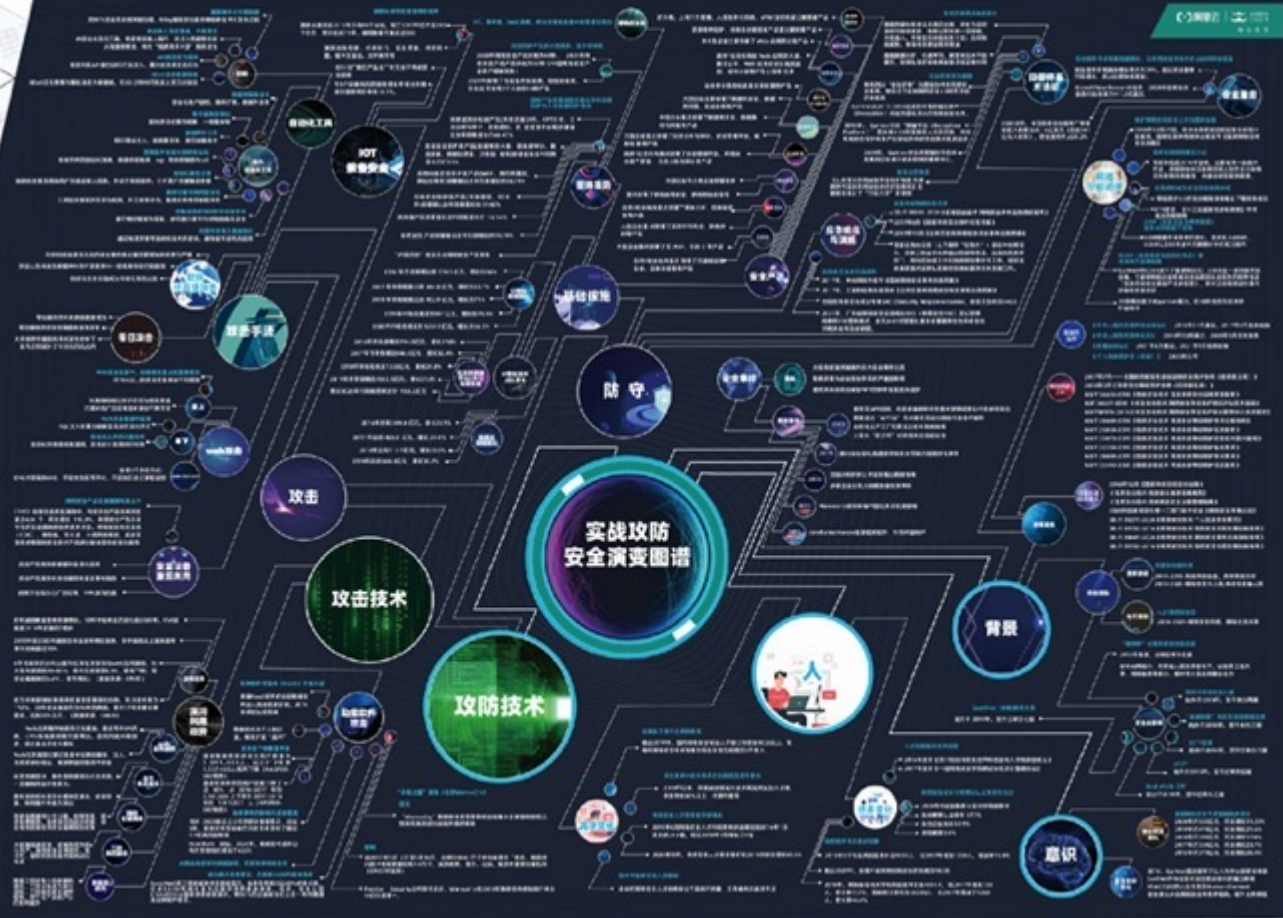
混合云视角攻击路径及布防思路

上帝视角描绘企业攻防全景图

全网首张

实战攻防安全演变图谱

近50余个细分维度展现最佳观察视角



技术成果出席国际赛事及顶级大会

CAPABILITIES

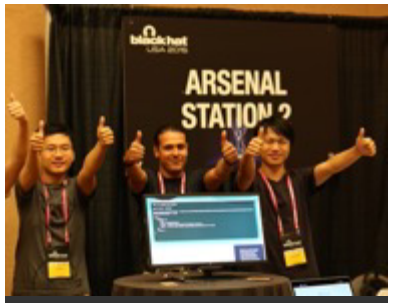
DEFCON 2014


Pwn2Own 全球第三

GeekPwn 2019


“强网杯”2021

“天府杯”2021



US Black Hat 2015


US Black Hat 2017

欧洲36 CCC

HITB 2021


广州《财富》论坛 2017


RSA Conference 2018


RSA Conference 2019


国家网络安全宣传周2022


乌镇 世界互联网大会 2021


4.29首都网络安全日 2021

荣获国内外十余个网络安全大赛冠军

CAPABILITIES

长亭科技 CHAITIN

10+

网络安全大赛冠军
几乎包揽国内知名安全竞赛一等奖

300W

比赛奖金（CNY）

2017年全球顶级
网络安全大赛Pwn2Own
现场唯一破解
全线操作系统的团队

- 2021 “强网杯”网络安全挑战赛特等奖
- 2020 **“强网杯”线上赛线下赛一等奖**
- 2019 “强网杯”网络安全挑战赛线上与线下赛一等奖
- 2018 **“网鼎杯”网络安全大赛二等奖**
- 2018 GeekPwn上海站最佳技术奖
- 2017 **Pwn2Own全球第三名**
- 2016 **GeekPwn中国第一名**
- 2016 第三届4.29首都网络安全日网络安全技术大赛 一等奖
- 2016 **Defcon CTF 全球第二名**
- 2015 GeekPwn2015一等奖
- 2015 第三届通信网络安全知识技能竞赛年度总决赛一等奖
- 2015 首都网络安全日网络安全技术赛一等奖

主办国际赛事
CAPABILITIES

Real World CTF国际网络安全大赛

全球首创基于真实世界软件的全新CTF赛制
集合CTF夺旗赛和Pwn赛的优势
所有赛题全部基于真实世界软件的修改或二次开发
广受好评

连续四年
CTFtime满分评价

超万人
同场竞技

单次集结
近2000支队伍

覆盖5大洲
10+个国家地区

世界强队悉数到场

R3kapig NeSE PPP
Sauercloud KalmarUnionen
p4 Balsn 0ops Nu1L ...

题目覆盖广

物联网 云安全 虚拟化 可信计算
办公安全 区块链安全 渗透测试
逆向工程.....

第一届　2018年 · 郑州

第二届　2019年 · 北京

第三届　2020-2021年 · 线上赛

正赛

第四届　2022年 · 线上赛

2022年，体验赛首次上线

面向：企业、高校新一代技术人才

难度降档
30%难度
入门体验更友好

质量不降
100%
同质量题目和考察范围

202支队伍
近1000人参赛

7大行业领域
金融、能源、教育、企业
交通、政府、通讯

50+知名高校
清华、复旦、北理、北邮
成都信息工程...

行业领先的完整资质认证
CAPABILITIES

ISO9001

ISO27001

国家高新技术企业

CNVD
支撑单位

CNNVD
技术支撑单位

CNCERT应急服务
支撑单位（省级）

CMMI5

信息安全服务资质认证
风险评估（一级）

信息安全服务资质认证
应急处理（一级）

通信网络安全服务能力
评定证书（风险评估一级）

通信网络安全服务能力
评定证书（安全培训一级）

信息安全服务资质证书
（安全工程类一级）

信息安全服务资质证书
（风险评估类一级）

从硬件、组件、中间、操作系统，自主可控

CAPABILITIES

操作系统&CPU

核心产品全面适配统信、银河麒麟、中标麒麟 、海光、中科方德等国产化生态，12类66款产品入围央采

基础组件&中间件

开发语言

Go　Lua　TS

依赖库

Vue.js　ECHARTS　Element

中间件

MINIO　redis　TiKV　engine

基础库

kubernetes　K3S

采用国际或国产开源组件，部分自研

硬件

适配国产化硬件、信创硬件

核心服务&技术

自研为主，核心组件申请专利或软著

品牌影响力
CAPABILITIES

长亭科技 CHAITIN

公司总部

北京

分支机构

10+

上海、南京、杭州、深圳、广州、长沙、武汉
成都、西安、郑州、沈阳、济南、乌鲁木齐.....

业务范围

覆盖全国省市行政区

34


卡奇科技
CHAITIN
THANKS
不可计算 无限可能