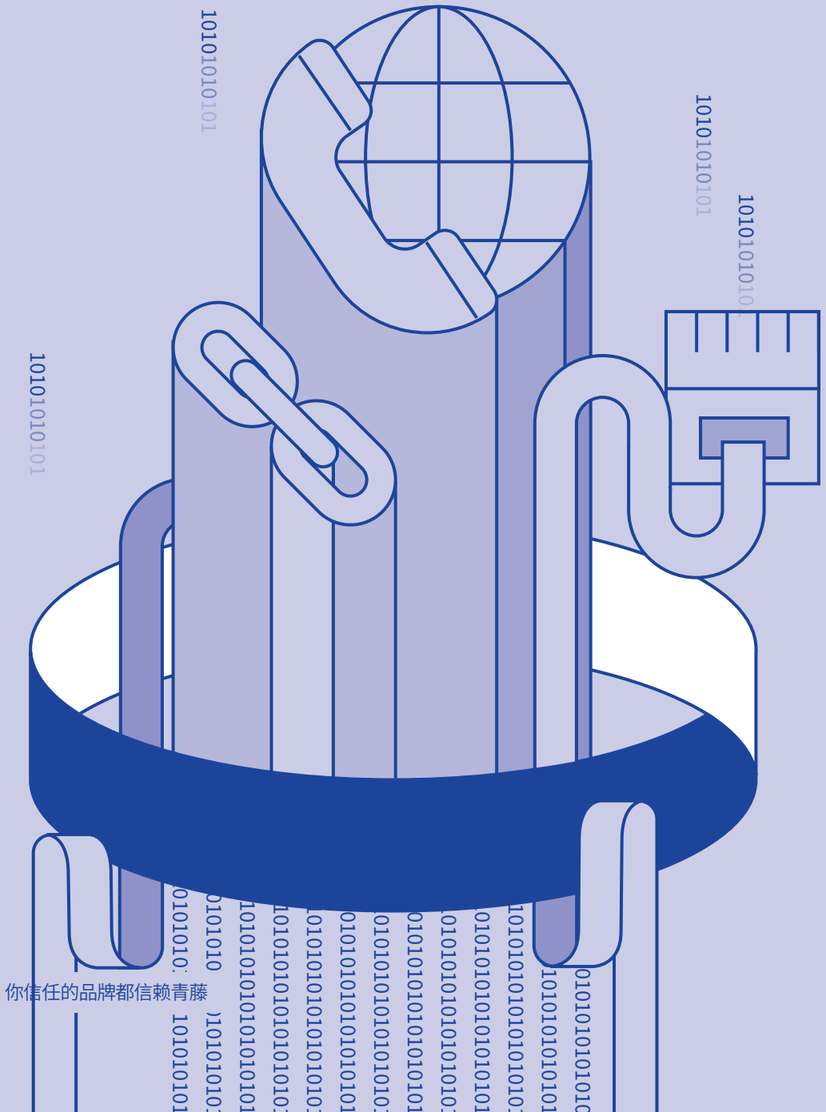
运营商
Telecom Operators



3 大运营商

全部覆盖

40 +

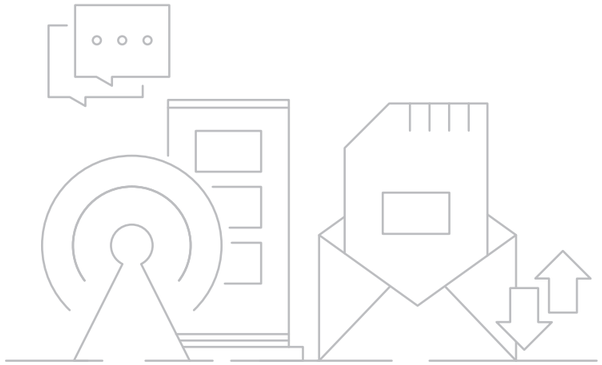
运营商省级分支机构及子公司

< 24 小时

平均风险漏洞响应时间

250,000 +

行业Agent 部署量



运营商作为通信类关键信息基础设施，与其他行业产生了大量交集，汇集了大量的客户信息。为了加强运营商网络安全，相关监管部门出台了大量的监管要求和标准，例如《电信和互联网行业数据安全标准体系建设指南》《电信网和互联网安全防护管理指南》《电信网和互联网安全等级保护实施指南》等。在此背景下，运营商行业面临安全合规压力大、安全运营和重保任务繁重、入侵威胁严重等安全挑战。

青藤 产品协同满足运营商合规要求，安全运维

风险分析：

青藤通过对运营商大型数据中心海量安全日志的集中分析处置，对风险进行全面监测、准确研判、及时处置、有效溯源。

无签名检测：

通过机器学习、行为分析和集成威胁情报实现高级无签名保护，精准抓住入侵威胁。

合规要求：

青藤全面地指导运营商信息系统的安全配置及加固工作，并实现自动化的安全配置核查，帮助客户满足监管合规要求。

中国移动某省子公司云主机资产风险可视化方案

背景概述

中国移动某省子公司隶属中国移动通信集团公司，是中国移动有限公司的全资子公司，在全省拥有 11 个市分公司和 62 个县（市）分公司。该客户一直是全省移动通信服务的主要提供者，并始终保持领先地位。

> “我们在2020年9月选择青藤作为安全合作伙伴，快速建设了一套自动化、智能化的云内网络性能健康度监控工具，获得了全面的资产可见性，发现了以前没有意识到的威胁。”

客户需求

随着客户信息化建设不断加快，网络规模逐渐增大，导致云内网络成为黑盒，相关风险系数激增，运维复杂度增加。

缺少网络流量的可视化信息

目前客户运维人员人工管理的方式，难以对网络流量实现可视化监控，无法及时发现来自内部、外部的安全隐患。

风险威胁监测能力弱

客户现有防护体系，缺乏网络威胁监控能力以及性能分析能力，影响业务的持续稳定运行，也不利于信息化建设。

智能化运维能力不足

由于大量的人工配置工作，导致运维人员管理压力大，而且经常出现因为配置错误、流程失误、监控管理缺失等带来的安全隐患和安全事件。

解决方案

通过青藤零域·微隔离安全平台，实时采集主机、虚机和容器节点之间的网络连接，并进行可视化呈现。

一个Agent集成主机安全能力和微隔离能力，自动化梳理主机资产信息，及时发现来自内外部的风险入侵行为。

通过统一的管理平台实现自动化运维，支持主机和虚机环境Agent约2500个、容器环境Agent约6000个，对所有服务器进行集中安全管理。

客户收益

01 获得云内网络连接清晰可视化信息

青藤零域支持在同一管理平台呈现多个数据中心、多个资源池的网络连接全景，客户获得依据互访关系生成的全面清晰的网络拓扑。

02 实时监测发现系统风险和入侵威胁

客户获得实时的系统风险分析结果，持续修复业务环境内的高危漏洞补丁风险。并对攻击路径的各个节点实时监控，及时发现入侵。

03 自动化运维降低人力成本

业务访问关系全部依赖自动化智能学习分析，无须人工介入，而且随业务或IT环境变化，可自适应调整发布到主机的策略，实现自动化运维，减少人力成本和犯错可能。

中国电信某省分公司集约化合规安全管理方案

背景概述

中国电信某省分公司是中国电信首批在海外上市的四家省级公司之一，是省内规模最大、历史最悠久的电信运营企业，在网络、品牌、技术、人才等方面独具优势，位列全国前茅。公司下辖 11 个市分公司、62 个县（市、区）分公司、1 个直属单位、2 个专业分公司。

> “我们通过青藤的安全解决方案，对物理机、虚拟机、容器等各种环境中的主机资产进行统一管理，对当前的主机安全状况进行实时地监测和感知，安全团队可以有效预测风险，精准感知威胁，提升响应效率。”

客户需求

缺乏对多种环境中的主机资产统一管理能力

在云计算的背景下，该运营商主机资产数量高速增长，导致各种不可控的业务风险频频出现，迫切需要建立起覆盖各种环境的统一安全管理体系。

资产数量庞大，难以全面清点资产

该运营商客户业务系统繁杂多样，对云主机、虚拟机、容器等资产查询统计非常困难，无法精准了解查询结果。

需要有效识别与安全规范不相符的安全配置

细化系统配置要求，规范设备上线和日常运行的安全配置核查流程，并实现自动化的基线管理等问题是该运营商亟需解决的难题。

解决方案

- 通过自动化批量部署，对客户近千台服务器部署青藤Agent ，支持本地环境、云环境业务架构的统一安全管理。
- 利用青藤自适应主机安全平台，支持对业务层资产信息的精准识别和动态感知，让保护对象清晰可见。
- 结合青藤合规基线，帮助客户快速进行内部风险自测，发现问题并及时修复，以满足监管部门要求的安全条件。

客户收益

01 实现对各种环境资产的统一安全管理

青藤的产品充分适配客户主流的 Linux / Windows 系统，对混合业务架构下的各种资产采用集中式管理模式，帮助客户实现统一安全管理。

02 自动化构建细粒度资产信息，减轻安全人员压力

客户获得超细粒度资产信息，在资产变化时安全人员可实时获得通知，并且通过灵活的检测方式，可快速定位关键信息，减轻安全人员复杂的管理操作。

03 快速完成安全配置检查整改，满足合规要求

客户实现自动化基线配置，一键任务化检测，提高安全配置检查效率，节省时间成本，全面满足等保 2.0 、工信部等监管单位的合规要求。

中国移动某省子公司智能化、自动化主机安全建设方案

背景概述

中国移动某省子公司负责中国移动在某省的网络建设维护和业务经营。该公司以“移动信息专家”为目标，网络覆盖全面、技术领先、业务丰富、功能完善、管理先进、智能化程度高。

> “我们在2018年与青藤正式签约合作。通过青藤万相·主机自适应安全平台，全面清点、实时监控资产信息，持续监测系统入侵行为，极大地提高了主机层的风险感知和响应防御能力。”

客户需求

网络攻击手段多样化，出现了许多传统安全防护体系无法应对的问题，企业所面临的安全挑战不断增加。

主机层防护体系缺失

目前攻击手段逐渐转向针对主机层的攻击，主机侧数据的缺失导致安全分析和响应不及时。

缺乏威胁入侵的感知和防御能力

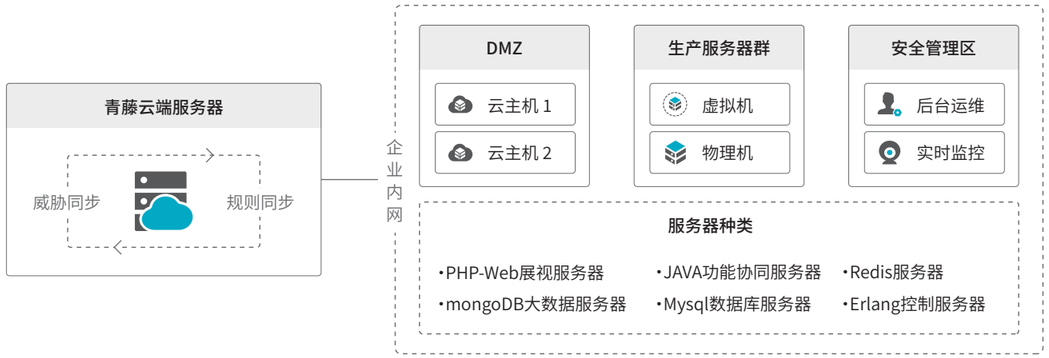
随着业务更新加快，业务复杂度不断升级，攻击者更可能趁虚而入，而且手段多样、隐蔽性高，现有的安全措施难以实时感知威胁，无法实现有效防御。

缺乏智能化实时分析能力

随着业务复杂度不断提升，客户需要智能化运维手段，提升安全事件实时分析能力，减轻运维压力。

解决方案

- 通过 Agent 端分别部署在不同主机节点上，动态清点服务器资产信息，收集细粒度的主机侧数据。
- 基于机器学习和行为关系模型持续监测精准感知威胁，为系统添加强大的实时监控和响应能力。
- 主机安全平台接受来自Agent的数据信息，通过关联分析，形成可视化的威胁态势，通过与风险发现功能配合工作，实现智能化的资产脆弱性管理。



客户收益

01 精准识别和动态感知资产风险

青藤资产清点能力支持对业务层的资产信息进行精准识别和动态感知，让客户资产清晰可见，并与风险和入侵事件自动关联，提供灵活高效的回溯能力。

02 有效缩减90%攻击面

客户精准发现内部风险，并获得详细的资产信息、风险信息以供分析和响应。青藤风险发现平均漏洞反应时间小于 24 小时，有效缩减攻击面。

03 基于机器学习和智能分析快速发现入侵

通过基于行为的智能关联分析，青藤产品能够在15s内完成入侵告警，快速定位发现失陷主机，实现自动化威胁发现，大大降低人力成本。

中国联通某院大型数据中心加强型主机安全防护方案

背景概述

中国联通某院是中国联通集团的全资子公司，主要承担中国联通信息化系统的 IT 软件研发工作，致力于提升核心系统自主研发水平，培育自有研发力量，全面推进中国联通的信息化建设。

> “青藤帮助我们在主机安全层面建立起了一个实时有效的防护体系，升级了大型数据中心安全防御能力，搭建起更高效、更精准和更智能的安全防护屏障。”

客户需求

随着业务的快速增长及变化，客户各系统和支持平台的规模逐步扩大，但对关键系统及重要服务器缺乏必要的安全防护能力。

缺乏资产全量梳理能力

目前，客户在主机侧缺乏有效的资产自动梳理工具，在日常业务运行过程中，无法对现有资产进行全量梳理。

风险发现能力不足

客户缺少对主机服务器内部风险的自动化扫描工具，无法第一时间发现来自主机服务器内部的安全隐患。

需要实时监控及时发现攻击

在业务运行过程中，客户针对外部的恶意攻击和访问缺少实时监控能力，针对外部攻击的溯源能力不完善。

解决方案

采用服务端+Agent方式，系统客户端为轻量级 Agent ，一条命令快速安装，安装完毕后自动化进行资产清点。

解决方案覆盖客户总部各大数据中心重点网络区域和重点核心系统主机，全面发现系统风险解决安全隐患。

通过为客户部署青藤万相·主机自适应安全平台，将预测、防御、监控和响应能力融为一体，形成安全闭环，快速精准地发现安全威胁和入侵事件。

客户收益

01 动态清点服务器资产信息

客户实现自动化构建并快速定位资产信息，各类资产清晰可见，获得重要资产实时变化通知，实现资产动态保护。

02 准确定位弱点和漏洞

客户实现持续性地监测风险，化被动为主动，发现大量系统内部暴露的弱点和漏洞，并有效处理，从而提高攻击门槛。

03 实时感知威胁行为

客户通过青藤态势感知衡量系统安全状态，实时监测威胁行为，第一时间发现入侵，减少安全事故损失。