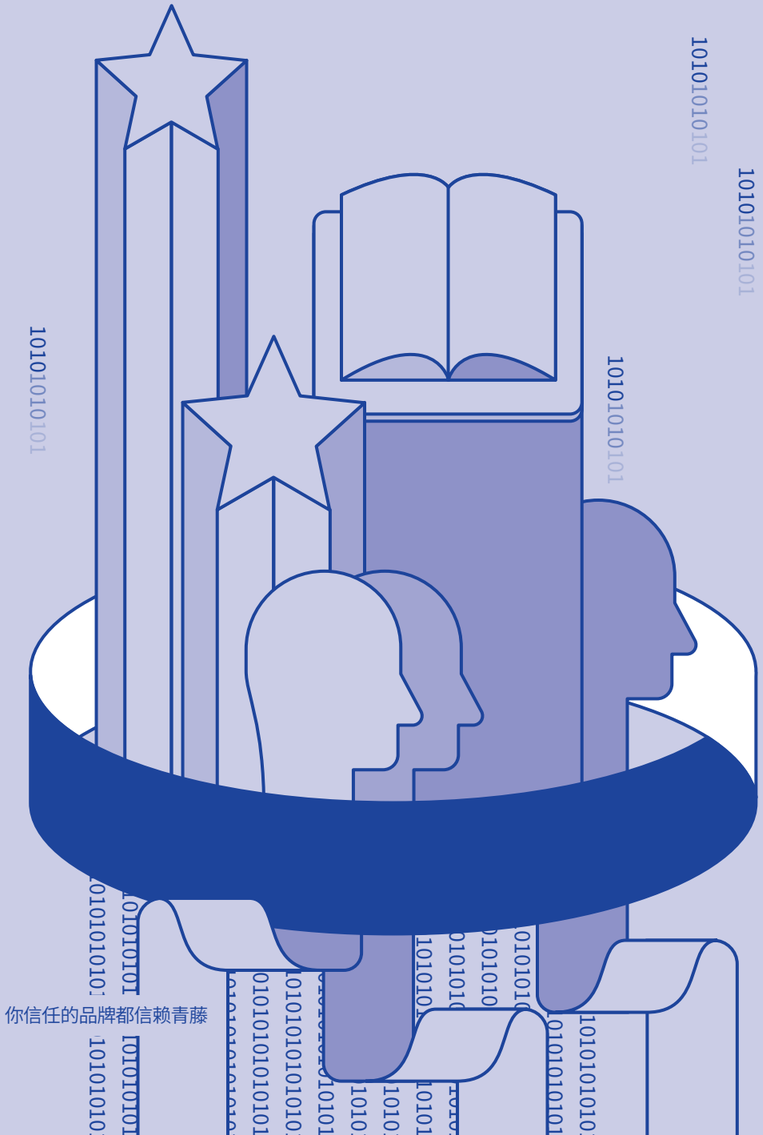
政府机构
Government



100+

从中央部委到地方行政机构

100+

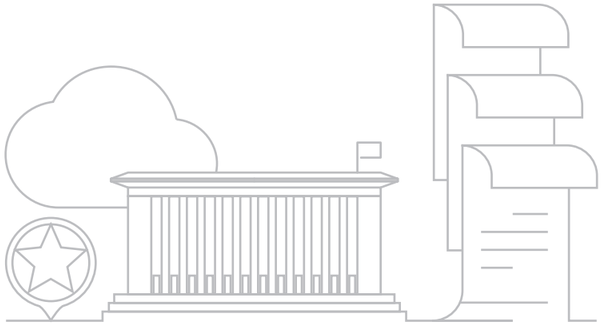
累计支持大型重保活动

1个

轻量级Agent无限扩展

500,000+

行业Agent 部署量



政务信息系统是政府高效履职的重要支撑，是以信息化推进政府治理能力的重要载体。国家“十四五”时期持续推进政务信息化建设，加快建设数字政府，提升政务服务水平。相关监管部门相继出台《政务云安全要求》《国家政务信息化项目建设管理办法》《信息安全技术 政务信息共享数据安全技术要求》等政策标准，对国家政务信息化项目的建设管理提出了系统全面的要求。

青藤 安全方案助力智慧政府信息化进程，前沿创新

快速实现安全：

青藤Agent是一款轻量级探针，可在几小时内部署到近万台主机上，快速实现安全能力。

及时响应威胁：

通过持续监控，对恶意活动进行快速检测和响应，以阻止已知和未知的风险威胁。

满足合规要求：

提供有效的安全产品和专业的安全服务，帮助政府机构满足最严格的安全合规要求。

中国地震局跨区域主机安全防御体系建设方案

背景概述

中国地震局不仅为中央和各级地方政府，以及高铁、核电等国家重大基础设施行业提供专业的地震信息，也为社会公众提供便捷、易懂的地震信息服务。地震局网络资产是重要的信息基础设施，也是地震部门开展地震监测、预报、科研的网络基础平台。

> “地震局为了准确地预报地震信息，离不开庞大的业务系统支持，而在背后守护这个业务网络的，正是青藤主机自适应安全平台。我们通过青藤安全解决方案，大幅提高了风险发现和响应能力，充分满足监管层的合规要求。”

客户需求

地震局管理全国地震监测预报工作，保护承载核心业务的服务器安全是开展工作的基础，但目前在主机安全方面存在几个突出的问题。

缺乏区域安全防护能力，安全问题难解决

地震局整个网络如同一个大的交换网在工作，近年来跨区域的网络攻击事件逐年增加，影响范围也逐步扩大，往往是一个小漏洞，需要全网应对。

网络安全意识有待加强，缺乏风险发现能力

缺乏良好的运维团队和安全系统的支撑，往往在发生安全事件后才进行安全应急工作，结果常常是小问题引发了大问题。

整体安全建设不足，无法满足等保三级要求

缺乏对登录操作系统和数据库系统的用户进行有效的身份鉴别，也无法很好地对重要用户行为、系统资源的异常使用等情况进行审计，不满足等保合规要求。

解决方案

- 青藤利用自动化运维工具实现2分钟/百台Agent部署，快速实现去中心化行业局域网内服务器安全保障能力。
- 在地震局业务网和台网中心网络两个核心业务系统上都部署了青藤Agent，通过模型分析计算，实时发现风险威胁。
- 通过专家远程在线咨询、现场支持服务做到安全策略风险的深度剖析、跟踪、处理、关闭，形成安全管理闭环。

客户收益

01 安全高效运维，减少人力成本

客户轻松实现海量服务器的安全管理，解决大规模业务网和台网中心网络运维安全问题，提高运维人员的工作效率，降低运维成本。

02 第一时间发现各种入侵行为，保障损失最小化

客户实现对攻击路径的各个节点实时监控，通过细粒度数据分析，清楚梳理恶意行为链路，快速有效响应入侵，减少损失。

03 建立合理的安全防御体系，满足等保合规要求

客户在青藤安服人员的协助下，利用合规基线产品，分析核心业务系统的合规基线策略，构建起安全防御体系，在主管部门检查中获得合规肯定。

中国煤炭地质总局云安全高级攻击防护方案

背景概述

中国煤炭地质总局是国务院国资委管理的中央勘查企业，是煤炭、化工资源勘查及煤炭、化工地质单位的行业管理机构。中国煤炭地质总局下辖中化地质矿山总局、省（区）煤炭地质局、专业局（中心、院）、干部学校、《中煤地质报》社等 18 个直属单位。

> “随着云时代的来临，业务变得越来越开放和复杂，黑客的攻击手段越来越多样化，我们通过青藤的主机安全解决方案建立起整合、联动、集约化的安全防护体系，能够持续感知业务端的运行状态，第一时间识别出攻击并迅速做出响应。”

客户需求

对主机安全风险无法持续检测和有效识别

当大量的业务、海量数据都集中在服务器中，客户需要建设持续监控、分析并可实时响应风险的主机安全能力。

高级威胁检测分析能力不足

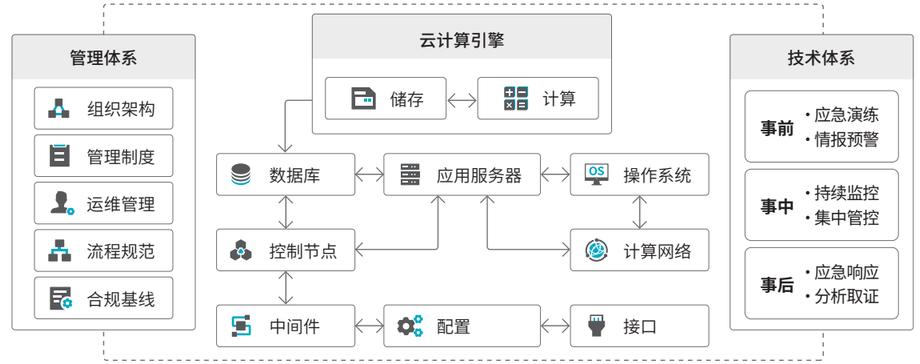
客户特殊的行业属性导致其经常面对来自黑客持久性、高度针对性的攻击，如何了解这种恶意事件的来龙去脉，以及如何提升对恶意事件的检测能力，是安全人员面临的一大难题。

建立云计算时代云安全风险防御手段

随着云计算时代数据价值的提升，各种非法之徒通过绕过传统的安全防护体系直接进入数据层，一些 APT 攻击很难用传统手段加以防护，客户需要解决云计算的安全问题。

解决方案

- 将青藤 Agent 部署在客户的虚拟机、容器等计算节点上，协助客户对云主机进行实时监控，了解其安全状态。
- 青藤万相以智能、集成、联动的方式应对各类攻击，通过协同打破数据孤岛和鸿沟，对攻击进行快速分析、溯源、响应。
- 针对云计算的安全问题，通过青藤入侵检测解决方案，实时准确地感知入侵事件，发现失陷主机，并提供对入侵事件的响应手段。



客户收益

01 持续检测主机安全状况，全面发现系统脆弱性

客户清晰了解内网所有主机实时情况，并通过全方位检测IT系统存在的脆弱性，先于攻击者发现安全问题，及时进行修补。

02 获得高级威胁的入侵分析和响应手段

结合青藤的专家经验，以及对主机环境的实时监控和深度了解，有效发现包括“0 Day”在内的各种未知黑客攻击，并通过详细多维分析，实现精准有效地解决高级攻击问题。

03 提升云安全防护能力,符合安全监管要求

客户通过智能化、自动化的安全管理平台，极大减少安全人员管理工作量，并建立云安全防御体系，满足了政府信息系统安全监管要求。

某政府单位大规模网络安全风险感知能力建设方案

背景概述

某政府单位信息网络系统已经实现行业全覆盖，包括47个国家或省级、直属单位等一级网络中心及近千个二级网络节点，为各类政府单位观测业务、数据处理业务、信息服务业务提供支撑与保障。

> “通过青藤提供的解决方案，我们全面提升了网络安全态势感知和风险检测预警水平，建立健全了安全保障体系，并通过青藤的安全培训服务，增强了组织人员安全意识，整体提升了风险防范和应急处置能力。”

客户需求

虽然该政府单位在系统网络安全和信息化工作中已经取得了一定的进展，但是在主机安全防护、风险感知、安全意识等方面还存在一定的漏洞和风险隐患。

清晰梳理众多资产

该客户信息化业务发展迅速资产剧增，客户意识到资产识别能力的重要性，需要从多层次、多角度、多粒度详细梳理资产的安全性。

提升网络安全状态和薄弱环节感知能力

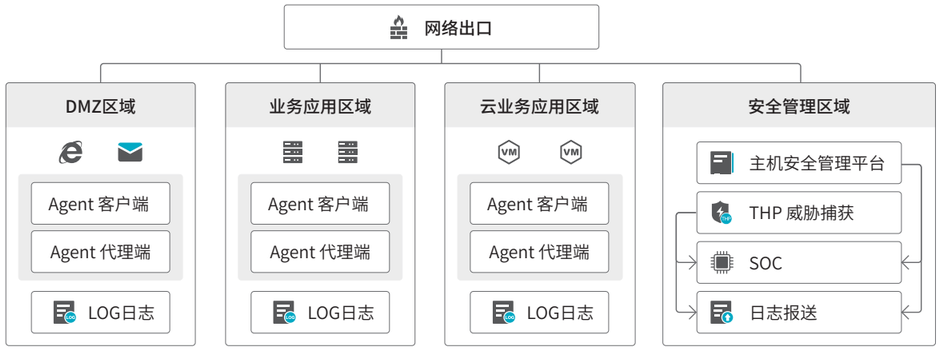
客户的系统架构越来越复杂，资产本身的漏洞、配置缺陷以及由于缺乏安全意识导致的弱口令等安全问题更是难以排查。客户需要高效地进行网络安全状态和脆弱性评估治理。

增强安全意识，缓解安全运营压力

增强公司内部防御能力和人员安全意识，缓解人员漏洞风险和安全运营压力，是客户急需解决的重要问题。

解决方案

- 通过部署4台服务器，实现约2000台Agent主机持续监控和管理，多维度、细粒度清点资产安全情况，以图、表等可视化形式展现给用户。
- 结合该单位网络系统架构特点，采用“控制中心 - 控制端”安全管理架构。各控制端全面排查安全风险问题，评估系统脆弱性，控制中心全面管理与控制风险状况。
- 青藤通过立体的安全服务和有效的安全产品，对客户人员进行全面的安全意识培训，并结合安全基线、威胁情报和知识库对客户系统进行多维度安全分析,对发现的漏洞和脆弱性及时处置。



客户收益

01 结合最新资产信息，及时发现威胁并快速响应

客户持续进行系统监控和分析，获得实时详细的资产信息，从而更精准地进行风险评估和威胁预测，提高对威胁的溯源和实时处置能力。

02 增强主机安全防护能力，提高了攻击门槛

客户对漏洞、弱口令、风险账号等安全风险，获得了可行的修复建议，有效提高了服务器的安全系数，降低了内外部攻击风险。

03 通过顾问式安全服务，提高整体安全意识

青藤的顾问式服务和安全培训，使该客户员工整体安全意识有效提升，大幅减少人员漏洞风险。

青海卫健委利用多维数据风险分析响应实践方案

背景概述

为贯彻落实《“健康中国2030”规划纲要》要求，青海卫健委开始加强顶层设计，加快建设信息平台，强化信息安全和标准规范管理、推进和规范医院的信息化建设。

> “我们通过青藤主机自适应安全平台，对各个子域、虚拟机进行安全防护与监控，相比于其他的解决方案总部署时间减少了 90 %，快速实现了‘拿不走、打不瘫、可预测、可追溯’的主动防御目标。”

客户需求

在国家相关政策指导下，青海卫健委信息化工作组对重要应用系统及核心关键数据的安全提出了严格的要求，构建全面的信息安全保障体系迫在眉睫。

利用多维事件信息对入侵威胁全面溯源分析

目前，在系统内部发生安全风险时，依赖片面的传统日志或审计信息，无法快速地对安全事件进行溯源和响应，使得威胁持续扩大。

全面识别复杂系统及设备的安全风险

如果对于自身信息系统情况都无法做到充分了解，则安全防护就无从说起，客户需要对资产进行全面的调研梳理和风险评估，识别出核心业务系统在不同层面、不同领域面临的安全威胁。

安全管理措施需要全网统一

客户需要对主机涉及文件、目录、进程、注册表和服务的访问控制建立统一的安全管理措施和安全基线配置。

解决方案

基于青藤Agent底层技术的主机解决方案，对主机进行实时监控，收集详细的资产信息和日志信息，快速发现威胁，同一个Agent可持续扩展其他安全能力。

对于复杂环境，精准、快速、全面发现系统风险，并从“识别、分析、处置、验证”全流程对风险进行闭环管理。

通过统一的管理平台，全面管理安全策略，从安全角度引导客户对日志进行查询与分析，对接主机层六大类事件采集数据，发现黑客入侵的蛛丝马迹，还原攻击现场。

客户收益

01 有效解决安全体系“信息孤岛”“数据烟囱”等问题

客户通过青藤独有的关键事件数据，凭借多维度的关联信息分析，提升可疑问题验证及恶意事件检测能力。

02 发现应用配置缺陷导致的安全问题

客户通过青藤风险发现功能自动识别应用配置缺陷，发现并处理存在的问题，有效解决潜在安全隐患，大大降低被入侵的风险。

03 实现统一安全管理及自定义基线检查

青藤产品充分适配客户各种业务环境，帮助客户实现资产的统一安全管理，并且客户可根据实际的使用场景，自行定义基线的检查项，以满足企业多样化的内部监管要求。