青藤云安全

让安全更有效

自适应的主机安全解决方案

QINGTENG

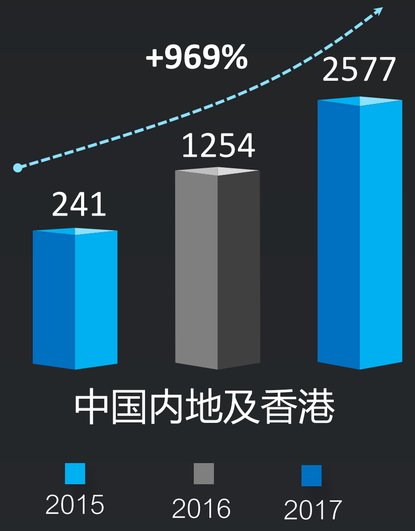
2018年8月

CONTENTS

网络安全现状

随着信息化的迅速发展，业务变得越来越开放和复杂，固定的防御边界已经不复存在；网络攻击行为向着分布化、规模化、复杂化的趋势发展，仅仅依靠防火墙、入侵检测、防病毒等单一的网络安全防护技术，已不能满足企业安全防护需求，迫切需要新的技术，及时发现网络中的异常事件，实时掌握网络安全状况。

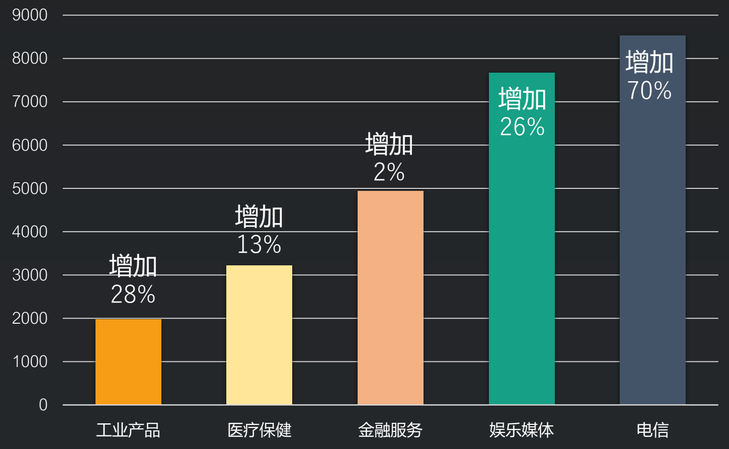
《2018年全球信息安全状况调查》



2017年中国企业检测到的信息安全事件平均数量是去年的两倍，比2015年更是增长了969%

数据来源：Gartner

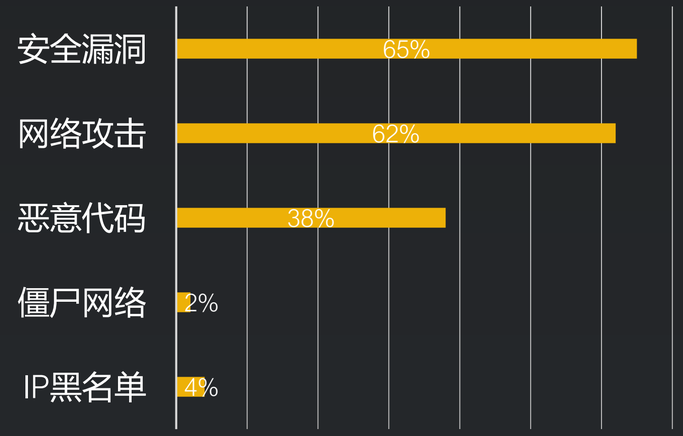
过去12个月内安全事件平均数



2017年12个月内安全事件频发，其中电信、娱乐媒体、金融服务、医疗保健、工业产品行业增长如右图所示，电信行业受攻击增加最为迅猛。

数据来源：Gartner

企业安全风险占比

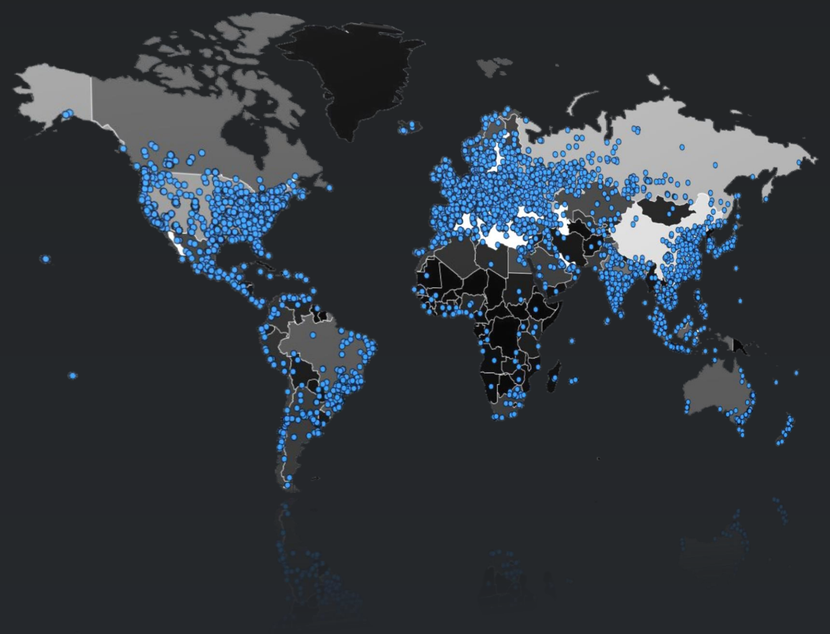


通过对2018年1月到6月企业内部安全风险的统计，安全漏洞、网络攻击、恶意代码入侵依然排在了安全风险总占比的前3名，安全威胁不容小觑。

数据来源：Gartner

WannaCry勒索病毒席卷全球

采用古代的城堡式的网络安全体系已经不能适应新兴木马病毒的攻击。勒索病毒主要以邮件、程序木马、网页挂马的形式进行传播。该病毒性质恶劣、危害极大，一旦感染将给用户带来无法估量的损失。2018年3月，国家互联网应急中心通过自主监测和样本交换形式共发现23个锁屏勒索类恶意程序变种。



5月9日

网页挂马方式进行传播，影响范围小

5月12日

利用445漏洞，“蠕虫”方式进行传播

5月13日

黑客继续开发，将WannaCry修改为WannaSister

5月14日

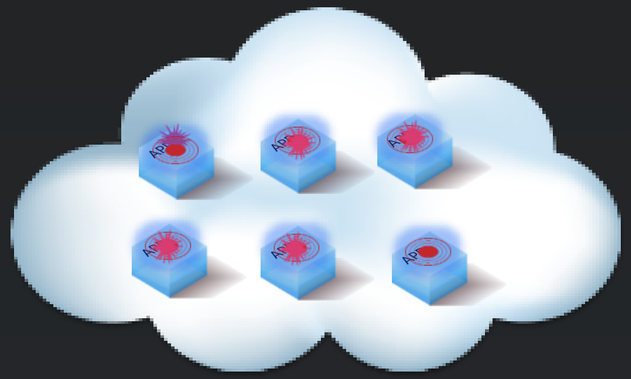
多种对抗手法，加壳、伪装、反调试、加签名的样本变种，躲避分析和查杀

未来

针对病毒的演化与变种，我们将持续关注

云环境面临的安全风险

东西向流量威胁



传统边界防火墙无法提供数据中心内部安全保护
缺乏应用之间的安全防护功能
以内部安全薄弱设备为跳板发起安全攻击

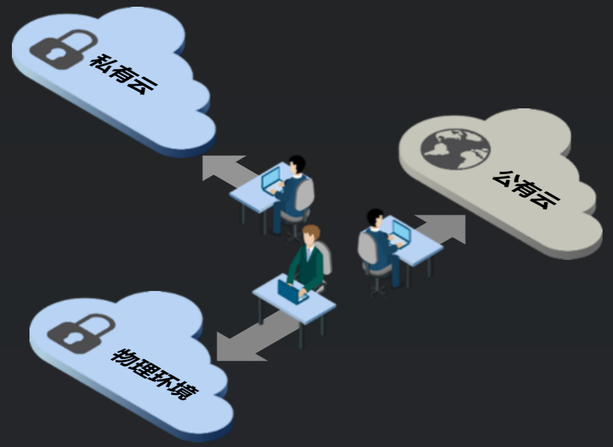
最新恶意软件可以通过内部流量感染其他主机，同时从一个应用传播到其他应用

数据中心结构快速变化

新业务通过预制备模板快速上线
虚拟应用实时迁移，IP地址频繁改变
大量处于休眠状态的虚拟主机可能随时开启

传统基于静态的安全保护方式已经无法满足新一代数据中心要求

复杂的云安全管理环境



物理机、虚拟机、私有云、公有云共存
安全管理策略需要全网统一
安全防护能力需要全网统一

在复杂的云环境下如何统一安全管理

主机安全防护存在的挑战

在应用云服务、软件定义的基础设施和移动计算后，您的系统安全吗？

拦截和防御的“城墙”越垒越高，可是下一次的定向攻击或持续攻击，会不会再次绕过防火墙和基于黑白名单的预防机制？

人员增长快

正式员工

外包员工

合作伙伴

投资公司

设备类型多

台式PC

笔记本

Mobile

IPAD

Win

MAC OS

Linux

IOS

Android

业务应用杂

办公应用

业务应用

移动APP

.....

安全防护难

定向攻击

持续攻击

高级木马

.....

传统安全防御体系痛点

边界模糊

网络规模及网络架构越来越庞大，多层面的网络安全威胁和安全风险也在不断增加，无法对业务系统进行深度防御.

资产难梳理

绝大多数企业缺乏自身数据资产的清点信息，或者清点不够全面透彻，企业无法实时掌控数据资产的全面情况.

安全检测频率低

安全频率太低，无法应对瞬息万变的安全内外环境，企业在完成测试的下一秒，外部安全形势可能就会发生变化.

难溯源

发生安全风险时，一般的日志或审计信息无法确定是人为因素或是系统自身因素造成的，且无法对安全事件进行溯源和追责.

无法联动

采购的各厂商安全产品无法进行有效联动形成纵深防御体系，且硬件产品很难快速更迭，很难适应最新的安全攻击特点.

缺乏外部情报

难以形成对资产变化、安全薄弱点和外部安全态势的联动分析和准确认知，更无法指导未来安全建设的实施推进.

安全建设思路的转变

面对传统的基于流量或规则的检测方式，已经无法检测新型未知威胁或最新的网络病毒；最合理的方案是企业要持续、动态地监控自身安全，并加强快速分析和响应能力，最终做到安全工作清晰、可衡量。

基于边界、流量或规则的传统检测方式已经无法检测新型或未知威胁。

持续监控和分析，通过系统“微指标”发现异常行为，并快速响应。

自适应安全架构

自适应安全是Gartner首次在2014年提出的面向未来的下一代安全架构，理念源自Gartner对美国一线安全厂商未来发展调研；核心思想是从防御转向持续监控和分析。

主机自适应安全平台

青藤主机自适应安全平台，采用Gartner在2014 年提出的自适应安全架构，有效解决传统专注防御的被动处境，为系统添加强大的实时监控和响应能力，帮助企业有效预测风险，精准感知威胁，提升响应效率，保障企业安全的最后一公里。

核心思想

- 将思维模式由“应急响应” 切换到“持续响应”，持续监控和分析。
- 构建自适应安全架构来应对高级威胁。
- 加大投入检测、 响应和预测能力。
- 建立情景感知的网络和终端和应用安全防护平台。
- 建立持续监控、 持续防护威胁的安全运营中心。

问题

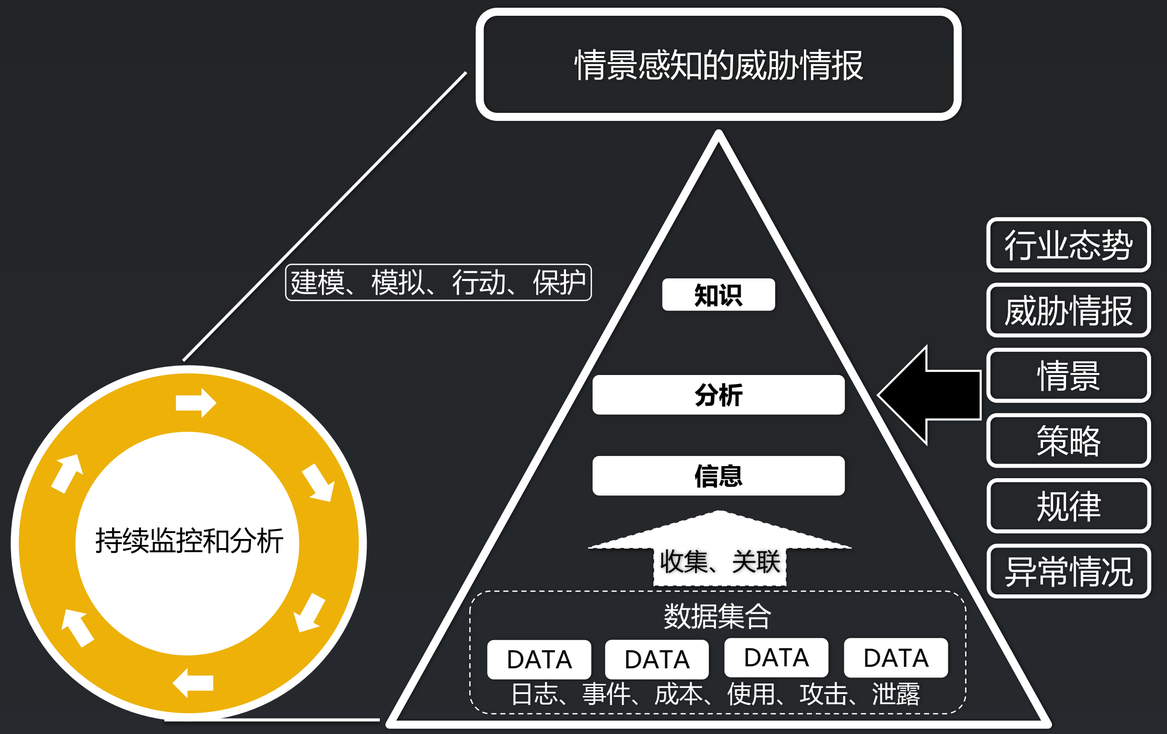
- 当前的防护功能难以应对高级定向攻击或持续攻击，持续防御能力明显不足

手段

- 12项关键能力

目标

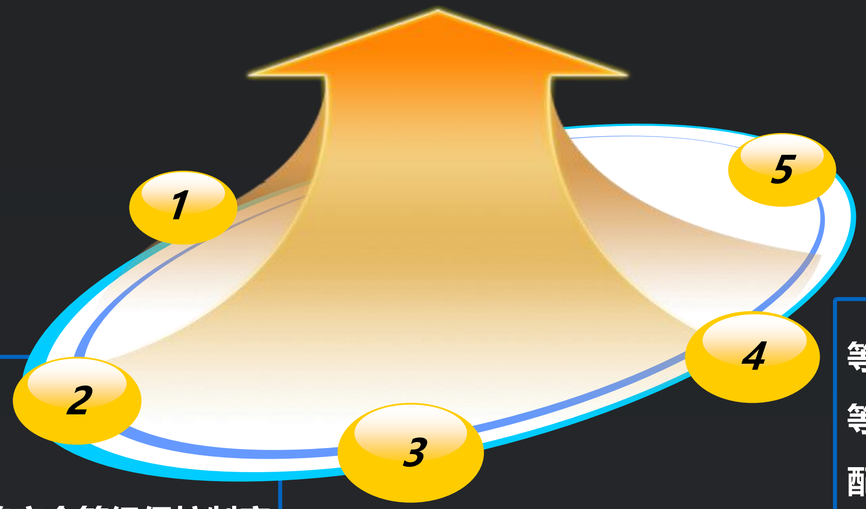
- 集防御、检测、响应和预测于一体的自适应安全架构应以智能、集成和联动的方式应对各类攻击。



助力等级保护2.0

新形势下的等级保护

网络安全引起空前关注。
■作用：辅助系统 - 支撑平台 - 基础设施；
■关注：信息安全 - 信息保障 - 网络安全；
■重视：《网络安全法》千呼万唤终颁布。



等级保护标准体系进一步提升适用性和可操作性。
核心标准启动修订
基本要求等标准扩展要求

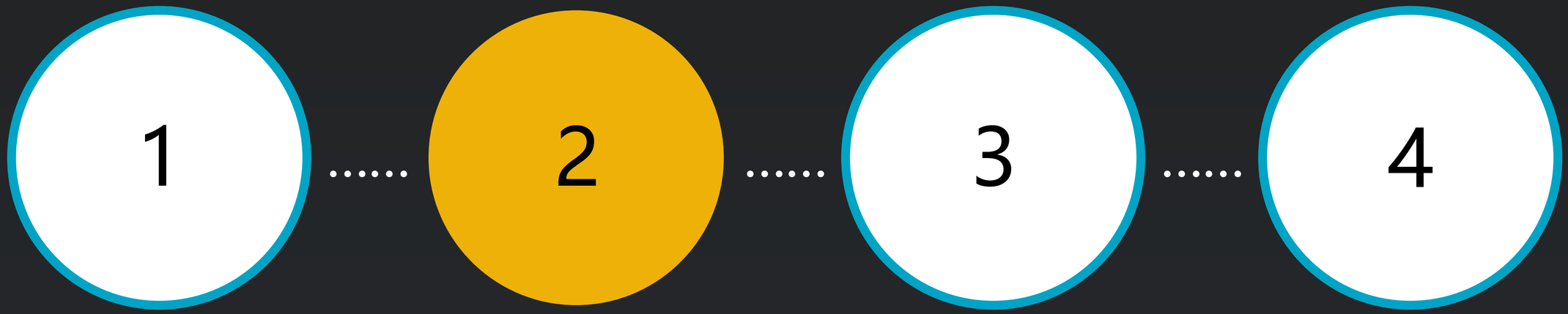
《网络安全法》确立制度地位。
21条规定：国家实行网络安全等级保护制度。
31条规定：国家对关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。

等级保护政策体系进一步细化和完善。
等级保护管理条例 / 关键信息基础设施保护条例启动制修订；
配套管理规范 / 细则启动编制。

等级保护外延进一步丰富和完善。
等级保护对象形态不断扩充（工业控制系统、云计算平台等）；
工作内容更加完善（供应链安全、通报预警等）。

“等级保护”是以**法律形式**确立的网络空间安全基本制度，其核心是“**划分等级，重点保护**”。

CONTENTS



现状及趋势　解决方案　增值服务　公司介绍

平台架构

青藤的核心平台架构，主要由Agent，Server，Web 三部分构成，为产品服务提供基础的、灵活的、稳固的核心能力支持。上层组件化产品模块，采用插件化的系统结构，实现功能的智能协同；底层的核心平台架构，是下一代主机安全能力引擎。

- 支持上层插件化的构建方式，具备灵活、快速和轻量的扩展能力；
- 支持各功能模块无缝联动；
- 支持分布式的部署；
- 支持大量任务下发和大型攻击来临的海量数据分析处理。
- 预留接口，可以与第三方威胁情报结合，使用情报库里的信誉、黑白名单等资源

资产清点

目标：实时掌握所有主机情况，快速搭建灵活有效的纵深防御体系。

自动化构建资产信息

通过安装Agent，可在15 秒内，从正在运行的环境中，反向自动化构建主机业务资产结构，上报中央管控平台，集中统一管理；确保安全覆盖无死角。

资产变化实时通知

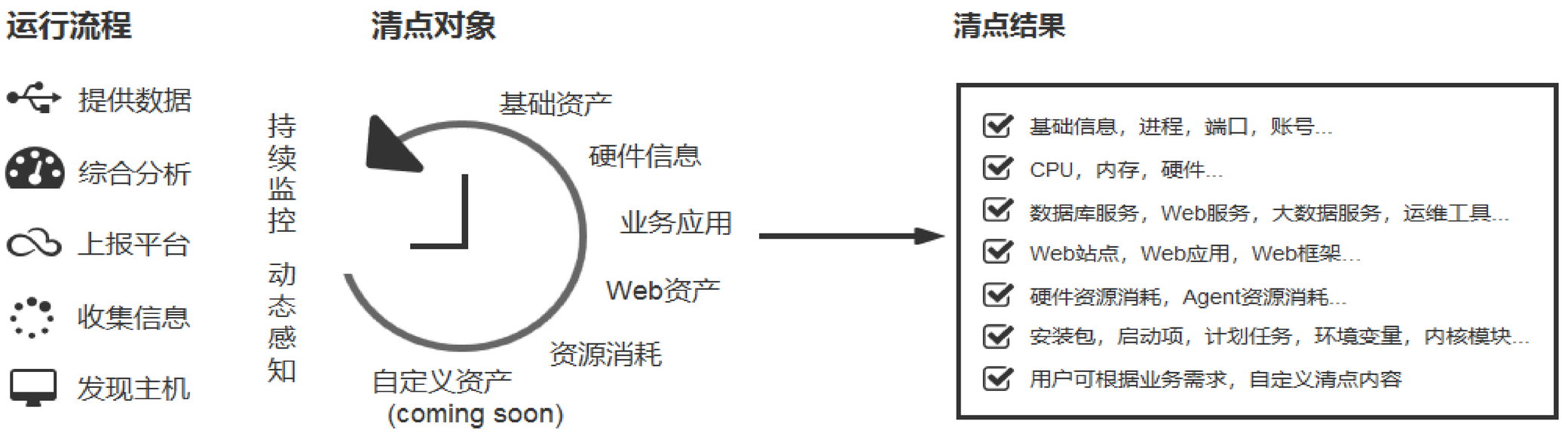
平台在清点资产后，将保持对资产持续监控，保证监控数据与实际业务数据一致；对一些需要特殊关注的敏感资产发生变化，将提供实时或定时通知。

灵活快速检索定位

参考大量国外先进产品经验，结合通用安全检查规范与安全事件的数据需求，形成细粒度资产清点体系；利用多维度的视图，引导用户轻松获得需要的资产信息；借助多角度的搜索工具，帮助用户快速定位关键资产信息。

资产清点

资产清点数据平台



精确识别10余类主机关键信息清点，200余类业务应用识别

结合通用安全检查规范与安全事件数据需求，构建业务型资产对象

支持绝大部分主流操作系统，支持本地环境、虚拟环境、云环境等混合业务架构环境

作为数据支撑，已与平台中的风险发现和入侵检测系统全面关联，实现一键查看

风险发现

目标：持续的进行风险检查和修复，将风险控制在较低水平。

提高攻击门槛

全面发现潜在风险及安全薄弱点，根据多维度的风险分析和精确的处理建议，用户可及时处理重要风险以限制黑客接触系统、发现漏洞和执行恶意代码。

企业风险可视化

持续性监测所有主机的安全状况，图形化展现企业风险场景，为安全管理者动态展示企业安全指标变化、安全走势分析，使安全状况的改进清晰可衡量。

持续性监控分析

主动、持续性地监控所有主机上的软件漏洞、弱密码、应用风险、资产暴露性风险等，并结合资产的重要程度进行风险分析，准确定位最急需处理的风险，帮助企业快速有效解决潜在威胁。

风险发现

风险总览 **安全补丁** **漏洞检测** **弱密码检查** **对外访问性**

应用风险 **系统风险** **账号风险** **Web风险文件**

① 全面系统脆弱性发现

全方位检测 IT 系统存在的脆弱性，发现信息系统存在的安全补丁、安全漏洞、安全配置问题、应用系统安全漏洞，检查系统存在的弱口令，收集系统不必要开放的账号、服务、端口，形成整体安全风险报告。

② 白盒角度发现风险

Agent 探针式的扫描机制，建立了自内而外的白盒视角。极低的误报率精准发现软件漏洞、发现更多更全的弱密码账户等。

③ 比传统扫描器更快

传统的扫描器每次扫描均需要将远程接入各级网络，部署相对麻烦且不能持续性扫描防护，而基于Agent 由内而外的扫描方式，一条命令即可一键部署，部署成功后即可持续为企业安全保驾护航。

④ 资产数据自动关联

基于主机环境资产全面清点的基础上进行的持续性风险扫描，能对主机环境资产进行持续性防护。支持在发现了风险之后，一键查看对应的资产情况，为风险的下一步处理提供有效信息。

入侵检测

目标：实时监控系统异常操作行为，第一时间发现入侵行为。

实时发现失陷主机

通过多维度的感知网络叠加能力，对攻击路径的每个节点都进行监控，并提供跨平台多系统的支持能力，保证了能实时发现失陷主机，对入侵行为进行告警。

发现未知黑客攻击

结合专家经验，威胁情报、大数据、机器学习等多种分析方法，通过对用户主机环境的实时监控和深度了解，有效发现包括“0day”在内的各种未知黑客攻击。

对业务系统“零”影响

Agent 以其轻量高效的特性，在保证对用户主机安全监控的前提下，不对其业务系统产生影响，为用户的主机安全提供了高效可靠的保护。

提供最准确的一线信息

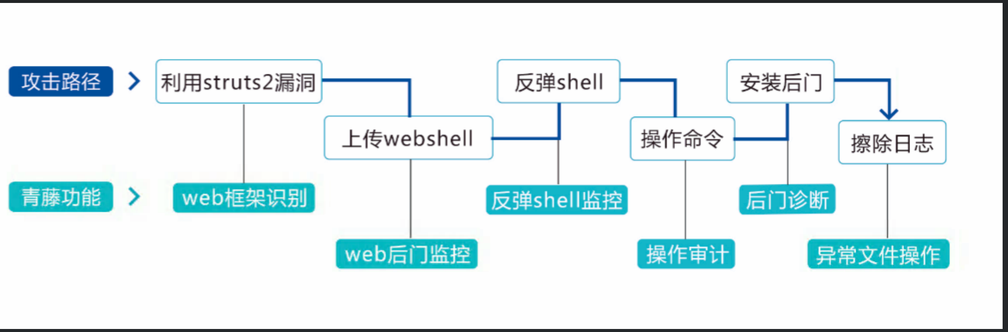
在独有的资产管理能力支持下，我们不只能发现入侵，更能够提供深入详细的入侵分析和响应手段，从而让用户精准有效地解决问题。

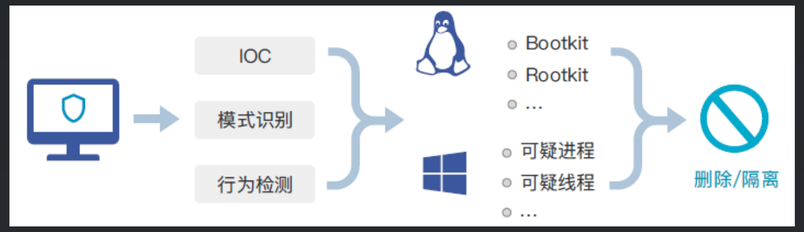
入侵检测

APT攻击链发现的设计思路——结合资产状态和风险状态，精准定位APT攻击并实现预警。

青藤的入侵检测技术基于行为模型学习的异常行为识别，通过设立特征锚点、分析行为模式、建立关系模型等手段，帮助企业在第一时间发现入侵，并联动其他功能模块迅速做出响应处理。

- 暴力破解（封IP）
- 异常登录诊断
- 反弹Shell监测
- 本地提权监控
- 系统后门（Rootkit诊断）
- 动态蜜罐（开放钓鱼端口并监测）
- Web后门（自研算法）



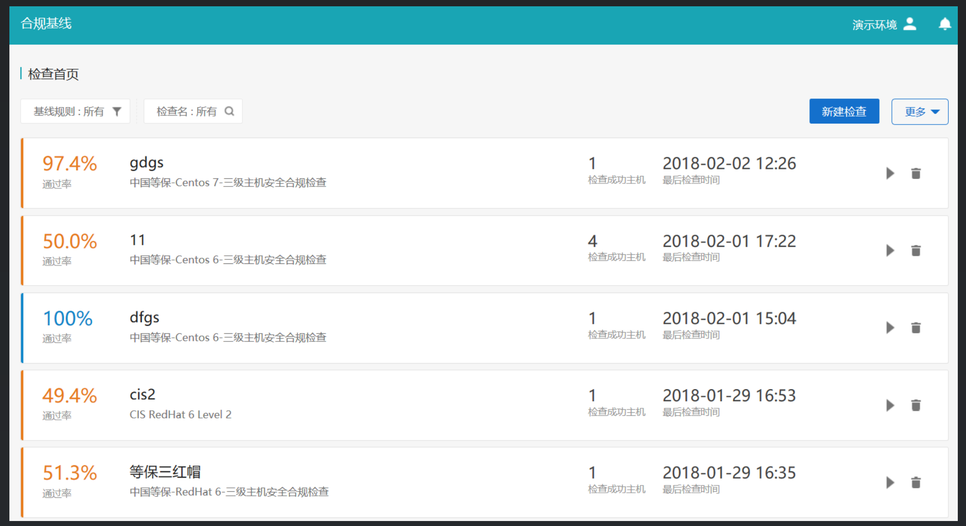


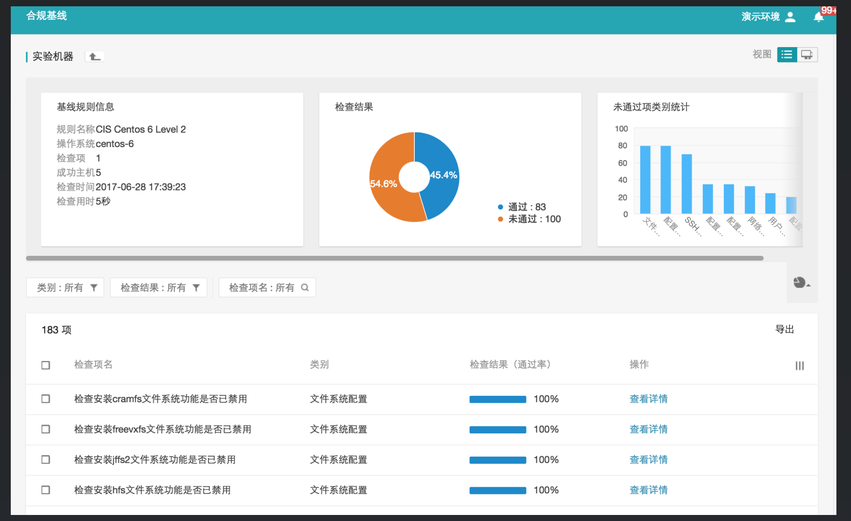
合规基线

目标：提供多种内置模版并支持自定义配置 ，实现主机层面精准的自动基线检查，检测时长只需3 ~ 5秒。

- 系统基线
- 应用基线
- 等保合规检查
- CIS合规检查

覆盖等级保护二级、三级技术要求主机安全检查330项。

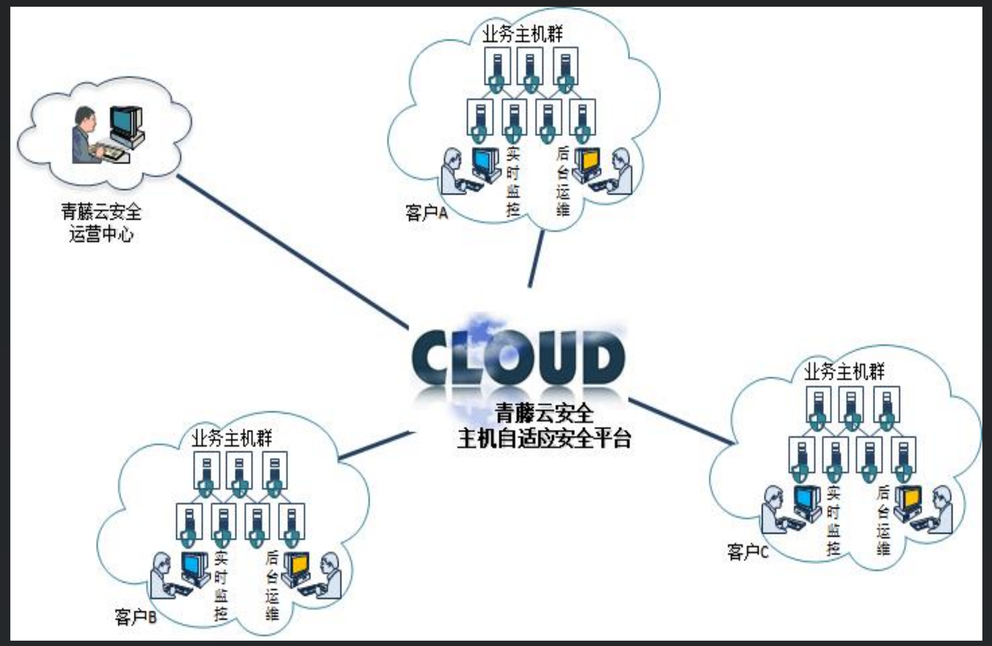




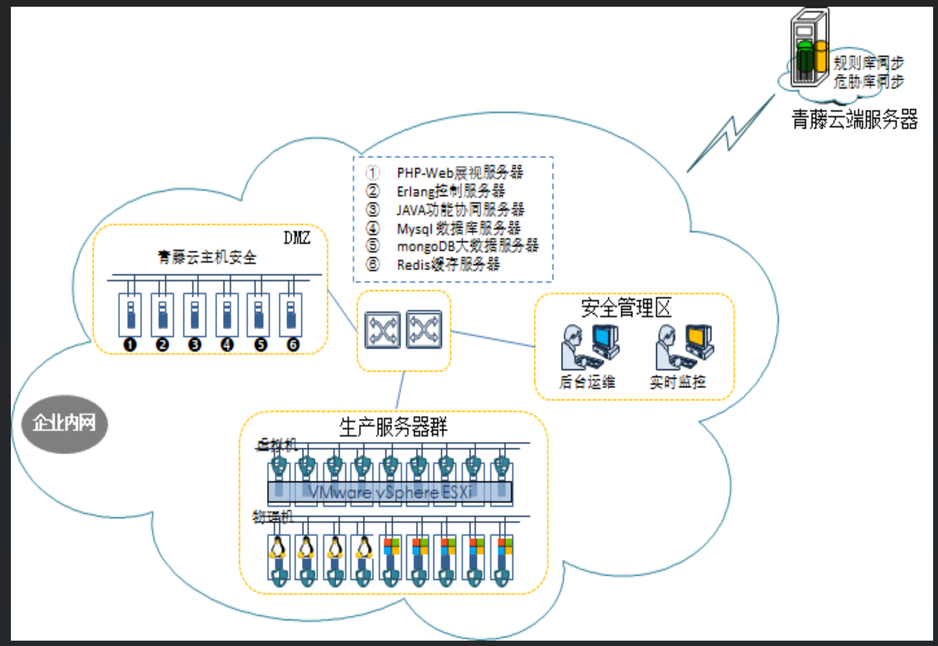
无需任何人工干预，全自动高效清点，一旦安全配置被修改迅速响应并可定位到具体的主机及负责人，最大限度减少风险暴露的同时有效降低员工再犯可能。

部署方式

青藤云安全产品从部署的方式来看，具有“SaaS（软件即服务）”服务模式和“独立部署”自建模式。 “SaaS”模式适合公有云或能够外网连接的网络环境客户，“独立部署”自建模式适合安全要求高内网部署的网络环境客户。



SaaS形态的部署方案仅包含青藤云安全Agent的实施，部署安装完成后，Agent会自行连接青藤云安全云端服务器，实现云主机的入侵检测和响应。



“独立部署”形态的部署方案包括Agent和主机自适应管理平台两部分，同时需依据Agent数量不同选择合适的服务器资源，以云主机数量100台为基准，服务器的推荐配置是8核CPU，64G内存，1T硬盘。

方案价值

① 产品核心

准确圈定保护范围 -- 以业务端安全为核心，轻量级、跟随式保护，青藤Agents的CPU占用率<3%，内存占用率<5%，稳定率高达99.998%

② 适用环境

适用于云环境、虚拟机和传统IDC，可以随着工作负载的启动自动加载

③ 超精细数据

已涵盖40,000多个软件漏洞，10,000多个WebShell规则，12,000多个Web漏洞，100,000多种弱口令及组合，合规检查相多达11,000个。

01

主机风险可视化展示，全面了解主机、业务、风险等关键信息

02

形成主机安全基线，让管理者清晰的知道安全现状，让运维人员有一个明确的安全工作方向

03

第一时间精准发现黑客的攻击行为，全面帮助客户发现系统内存在的安全风险

04

完整的安全运维闭环流程，体系化的产品架构 + 自动化的安全功能，降低对人的要求

05

符合等级保护2.0云计算安全扩展要求，满足国家政策要求

CONTENTS

1 现状及趋势

2 解决方案

3 增值服务

4 公司介绍

增值服务

等级保护咨询服务	安全评估阶段	资产调研	通过信息资产调研具体、有形的系统组成的调研过程以及管理调研、咨询等过程完成对系统信息资产进行调研，分析网络结构，进行业务影响的评估。	高级安全工程师
		威胁分析	对系统可能面临的威胁进行分析。	高级安全工程师
		技术脆弱性评估	通过漏洞扫描、手工检查、渗透测试等技术手段对系统的技术脆弱性进行评估。	高级安全工程师
		管理脆弱性评估	通过现场访谈、问卷调查、策略审计等手段对系统的管理脆弱性进行评估。	高级安全工程师
		风险分析与风险评估报告	对前期获得的数据进行分析，形成风险评估报告，为后期差距分析提供数据基础。	高级安全工程师
	差距分析阶段	差距分析报告	依据等保等级要求对系统的差距进行分析，形成差距分析报告。	高级安全工程师
		整改方案	依据等保等级要求及实际业务与安全需求，形成整改方案。	高级安全工程师
		信息安全技术培训	对整改可能设计的安全技术和产品进行培训。	高级安全工程师
	整改实施阶段	整改自检	依据等保三级要求对整改后系统进行自检，确保通过测评。	高级安全工程师
	测评阶段	第三方测评机构测评费用	邀请第三方测评机构对系统进行测评。	第三方测评机构
		第三方测评机构测评	协助通过等保三级测评。	高级安全工程师

增值服务

安全评估 （技术脆弱性评估）	安全漏洞扫描	安全漏洞扫描	使用安全厂商的远程安全评估系统或者已经部署的青藤的agent对评估范围内目标进行安全扫描，对目标设备的漏洞、用户名与口令、安全策略等方面进行评估。本次服务范围：服务器数量*台、网络设备*台、安全设备*台。	安全工程师
	安全渗透测试	灰盒渗透	通过真实模拟黑客使用的工具、分析方法来对网站进行模拟攻击，验证当前的安全防护措施，找出风险点，提供有价值的安全建议。服务范围为按照域名评估工作量按照人天工作量付费。	高级安全工程师
	代码审计	代码审计	使用白盒(White Box)测试对信息系统的源代码进行审计，找出编程缺陷，并提供改进建议及最佳安全编码实践，提高应用系统的安全性和健壮性，避免编程缺陷对系统和业务的正常运行造成影响。	高级安全工程师
	移动应用类安全评估	app安全分析测试	对提供的app进行安全测试，包含本地端的信息泄露测试、app加壳抗逆向测试、报文加密破解测试、通讯安全传输测试，本地端安全测试，业务逻辑安全测试，篡改注入测试等，同时包含B/S方式的安全测试。测试范围包含安卓以及IOS的应用，根据业务的复杂度进行评估付费。	高级安全工程师
	IoT智能硬件安全	智能硬件安全测试	针对智能硬件安全进行测试，范围包含IoT类的硬件，如网络安全设备（提供虚拟镜像环境如堡垒机、漏洞扫描器）、智能门禁系统、智能停车系统、物联网监控系统、电视盒子、智能硬件、工控设备等进行专业的的安全分析和测试。	高级安全工程师

增值服务

信息安全运维服务	定期安全巡检服务	安全产品以及设备检查	检查安全产品包括青藤以及其他安全设备的升级情况、设备的健康状况、设备的运行状况	安全工程师
		安全设备日志分析	对安全产品以及设备的日志进行分析	高级安全工程师
		安全扫描	收集、汇总新的漏洞信息，对目标设备进行漏洞挖掘工作	安全工程师
		安全加固	对巡检中发现的安全问题进行修补	高级安全工程师
	应急响应服务	入侵响应分析	在接到应急响应服务请求后，青藤安全专家依据安全事件的分类与应急响应的目标，及时提供远程或现场应急响应，协助客户对安全事件进行响应和分析对入侵来源、入侵路径、修复意见和意见进行系统性的梳理并给出详细的技术分析报告。	高级安全工程师
	日常安全通告	安全通告类	在第一时间向提供最新系统漏洞信息及解决方法，最新病毒、木马爆发警告及其解决方法信息，最新攻击方式以及防御措施信息和最新的安全事件通报。	高级安全工程师
	日常安全咨询	日常咨询	根据需求，青藤安全专家结合实际的问题进行分析，从安全新技术和安全策略等方面，向提供技术咨询服务。	高级安全工程师
	日常驻场支持	技术人员驻场支持	根据客户需求，青藤提供安全技术驻场人员针对青藤云安全产品的部署、安装、使用、安全分析、事件响应处理、维护等进行驻场的安全服务，驻场人员同时可以支持企业的其他安全产品的使用和日常安全技术支持等工作，根据客户需求驻场人员进行定期的驻场支持。	安全工程师

增值服务

安全培训服务	Web安全培训	主要针对流行的Web攻击如OWASP top 10攻击手法提供专业的安全的培训以及实际演练，通过理论知识、实验操作、攻击原理分析攻击对抗等进行专业的Web安全测试培训服务。	高级安全讲师
	Web安全开发培训	针对Web软件开发过程可能遇见的安全漏洞或缺陷进行讲解，对常见Web安全漏洞进行详细解说其原理、利用方式以及开发中如何避免这些问题做详细讲解。	高级安全讲师
	移动App安全测试培训	针对主流的移动APP的漏洞介绍如命令注入、逆向分析、重写保护、加密算法分析等进行整套的移动App安全体系分析培训，同时提供现场实验实验，理论和实践结合的方式开展专业的培训。	高级安全讲师
	应急响应与安全事件处理	主要讲解应急响应和安全事件的基本概念，介绍当前国内和国际应急组织的现状，企业如何发现和处理安全事件，如何对安全事件发生后进行最佳解决并结合案例进行说明。	高级安全讲师
	恶意样本取样与分析	主要针对流行的rootkit、木马、webshell、后门等样本从安全的角度进行取证与样本分析培训，培训会介绍流行的样本种类、具体的黑客攻击使用的方法、恶意样本的特征分析方法等	高级安全讲师

CONTENTS

1 现状及趋势

2 解决方案

3 增值服务

4 公司介绍

国内首家自适应安全公司

QINGTENG

青藤云安全以主机安全为核心，采用自适应安全架构，将预测、防御、监控和响应能力融为一体，为用户提供持续的安全监控、分析和快速响应能力。

青藤云安全总部位于北京，在上海、深圳、武汉设有分部。

- 青藤云安全成立 — 真格、云天使、丰厚资本600W投资
- 2015年6月发布产品Beta版，获得第一批种子客户
- 2015云计算大会上首次对外推出青藤自适应安全理念
- 2016年12月，获得宽带资本、红点创投的6000万人民币A轮投资，刷新企业安全创业融资记录
- 2016年1月产品2.0上线，用户规模扩大
- 2016年6月成为阿里云首批安全SaaS合作伙伴
- 2017年1月通过ISO9000质量认证体和ISO20000质量管理体系
- 2018年3月，获得红杉资本中国领投、红点创投中国基金、真格基金、宽带资本CBC参投的B轮2亿元人民币融资，再次刷新安全行业单笔融资新高

行业资质及品牌荣誉

行业资质
北京互联网金融行业协会会员
北京信息安全行业协会会议
北京市软件行业协会会员
上海信息安全法律专业委员会会员
北京市信息安全行业协会会员
中国中小企业协会会员
获奖记录
创业邦《2017中国信息安全创新公司50强》
2016“中国移动安全科技创新奖”
2016“中关村科技创新奖”
GMIC香港创新创业决赛三强
2017年入选可信云大会，并获得技术创新奖。
2018年度成功入围中央政府采购网。
2018年入选国家计算机网络应急中心创新产品和创新技术成果

行业资质及品牌荣誉

入选2017年全球最酷厂商

入选Gartner 2017 CWPP市场指南

青藤成为十年来第一家也是唯一入选 *“Gartner全球安全指南”* 的中国初创公司

青藤的客户

青藤产品已经获得**政府，金融，企业，运营商，互联网，云厂商，直播**等多个领域的行业标杆客户中认可

客户案例 – 雪亮工程

客户名称：朝阳区

所属行业：政府

项目名称：朝阳区公共安全视频监控建设联网应用示范工程

建设时间：2017年

部署模式：独立部署模式

用户需求：

采用主动式安全管理与预警，能够在威胁发生前进行事前安全管理，结合外部漏洞情报，实现多维度安全态势感知

能够对平台设备数据进行采集，对服务器/虚拟机、进行网络连通性、硬件性能及运行状态实时监测。

能够对全网服务器资产进行统一管理、统一维护，当发现系统设备发生故障或出现异常时，应能发出告警提示信息。

能够对服务器设备运行情况的统计分析，显示正常、故障、离线等状态信息，并可查看设备的详细信息。

系统能够提前获悉可能遭受的攻击和威胁、及其潜在的受影响范围

能够对系统内的服务器执行自动巡检，从而展现异常设备相关信息状况，能将异常设备、信息进行EXCEL导出。

客户案例 – 雪亮工程

解决方案

主动式安全管理	针对安全威胁进行实时监测，主要功能包括：安全威胁预警、漏洞扫描管理、配合安全核查。通过主动安全管理模式，系统提前获悉可能遭受的攻击和威胁、及其潜在的受影响范围，资产和业务系统中存在的安全漏洞和配置缺陷，有助于管理人员提前做好防范。
安全态势感知	系统将为用户提供基础的态势感知呈现能力。通过资产感知、漏洞感知、攻击感知这三个维度和安全态势总揽作为态势感知基础的实现框架，通过这三个维度有助于把庞大复杂的态势感知信息处理体系进行不同维度的理解和构建。
集成威胁情报	系统自动同步/导入/抓取来自内外部的威胁情报并予以利用，提高威胁分析的实效性和准确性。威胁情报主要包括恶意IP、恶意域名、恶意URL和恶意email，可来自公开的外部安全机构和社区，也可以来自商业威胁情报机构。
持续性监控分析	主动、持续性地监控所有主机上的存在的脆弱性，发现信息系统存在的安全补丁、安全漏洞、安全配置问题、应用系统安全漏洞，检查系统存在的弱口令，收集系统不必要开放的账号、服务、端口，形成整体安全风险报告。
设备集中管控	通过Web管理页面，直观展现所有设备的实时信息，使管理员可以全方位地了解设备的运行状况。结合通用安全检查规范与安全事件的数据需求，形成细粒度资产清点体系；利用多维度的视图，借助多角度的搜索工具，帮助用户快速定位关键资产信息。
自动化运维监测	通过持续性监测所有主机的安全状况，图形化展现企业风险场景，为安全管理者动态展示企业安全指标变化、安全走势分析，使安全管理人员快速了解主机资源的运行状态，并辅助定位主机故障。

客户案例 – 天翼云

客户名称：天翼云

所属行业：运营商行业

项目名称：天翼云主机安全防护合作项目

建设时间：一期（201x.xx-201x.xx），二期正在启动中

部署模式：独立部署模式，部署的Agent数量超过5000个

客户简介：天翼云是中国电信旗下云计算品牌，于2016年被中国电信注册，用于中国电信股份有限公司云计算分公司，是中国电信旗下的的云计算服务提供商。 2016年电信携手华为，发布“天翼云3.0”，凭借其“云网融合”、“安全可信”和“专享定制”等优势，为政企云提供一站式解决方案。

用户收益：天翼云通过和青藤云安全合作，为云上的企业用户提供服务器安全实时监控，可以发现攻击和入侵行为，保护核心系统和敏感数据安全，并因此扩大了在天翼云的租用量。

客户案例 – 中国移动政务云

客户名称：移动苏研院

所属行业：运营商行业

项目名称：苏研院政务云主机安全防护合作项目

建设时间：一期（201x.xx-201x.xx

部署模式：独立部署模式，提供API，将界面嵌入云平台，部署的Agent数量超过1000个

客户简介：中国移动苏州研发中心是中国移动通信集团公司2014年成立的全资子公司，是中国移动推动战略转型、实现向移动互联网业务和信息消费拓展的重要布局。以打造“产品研发能力、产品交付能力、产品服务能力”为主线，加速建立云计算、大数据和IT支撑系统领域核心竞争能力，围绕三大产品线自主研发了一系列核心产品

用户收益：移动政务云通过和青藤云安全合作，为云上的政企用户提供服务器安全实时监控，租户反馈的使用心得：

1. 能够准确地检测到WebShell等入侵攻击，客户会第一时间响应处理；

2. 能够及时发现弱口令、系统漏洞、不安全的配置等系统风险，对于定期安全巡检，提高服务器安全有较大的作用

Thank you

ppt规范

大标题

大标题　字号：88pt | 字体：苹方-简

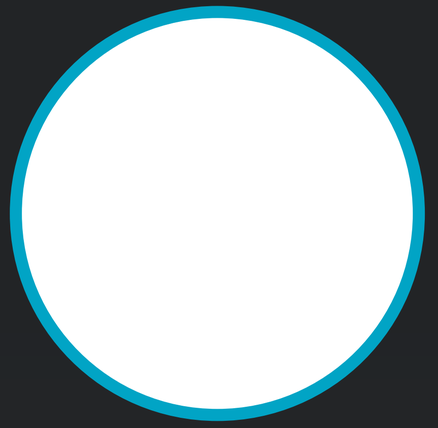
副标题

副标题　字号：30pt | 字体：苹方-简

标题

标题　字号：60pt | 字体：苹方-简

标题线　高度：0.2cm | 宽度：2.8cm



图形　图形里填充内容
边框：9磅

标题

标题　字号：40pt | 字体：苹方-简

文章内容文章内容文章内容
文章内容文章内容文章内容
文章内容文章内容文章内容
文章内容

文章　字号：24pt | 字体：苹方-简 | 行间距：1.5倍

青藤成为十年来第一家也是唯一入选“Gartner全球安全指南”的中国初创公司

青藤成为十年来第一家也是唯一入选“Gartner全球安全指南”的中国初创公司

注释两种表达形式：
1.品牌色边框 边框：4.5磅
2.白色透明底 透明度：90%

字体主色　色号：＃FFFFFF　标题主色　色号：＃03A4C5　辅助色　色号：＃014D90　点缀色　色号：＃EDB107