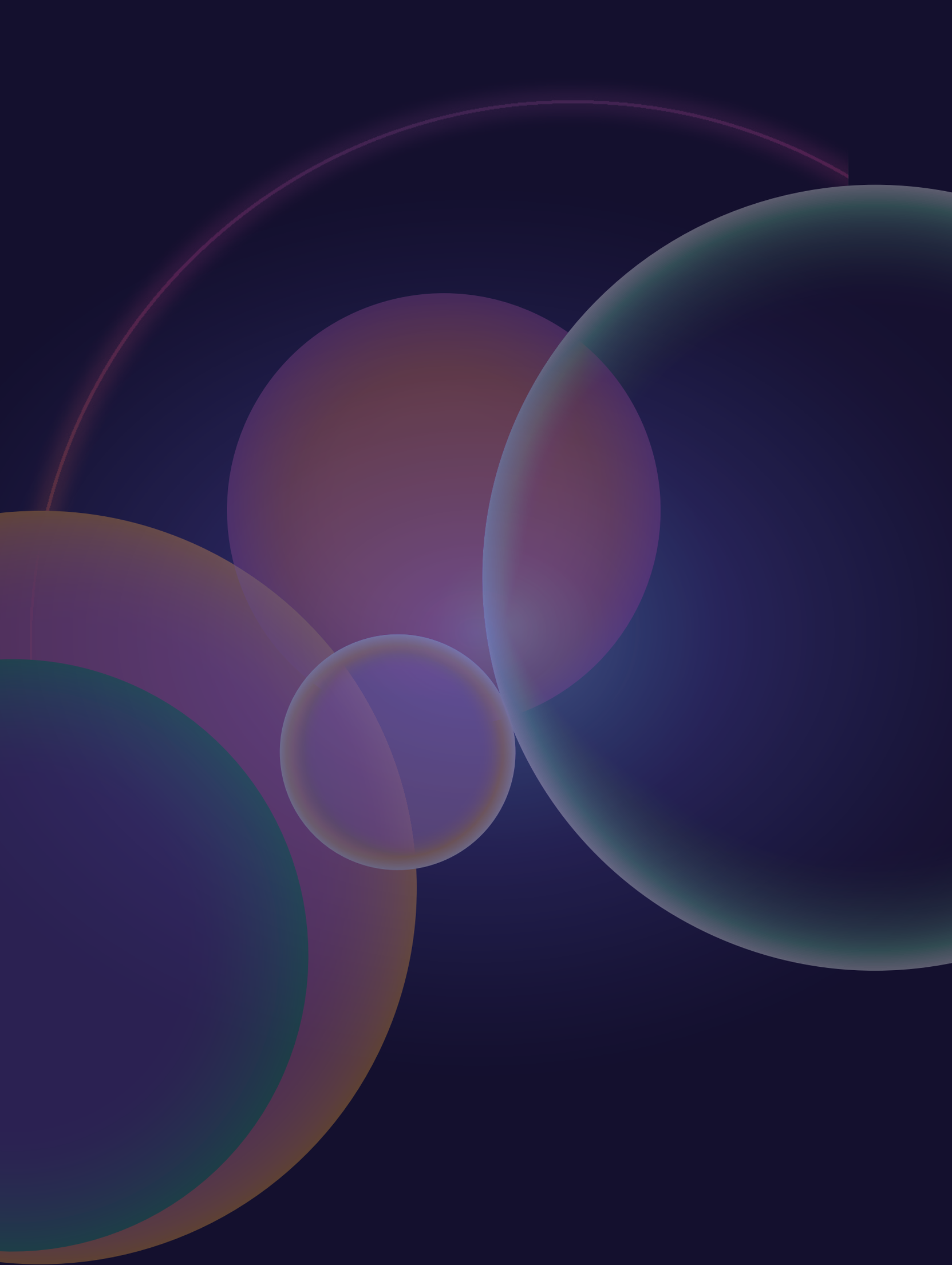
亚马逊云科技 marketplace

构建新格局
共赢云时代

全球技术合作伙伴解决方案集锦



亚马逊云科技 marketplace

介绍 INTRODUCE

亚马逊云科技 Marketplace 利用您熟悉和信任的软件来简化和加速推进现代化

加快采购速度，改善对第三方解决方案的管理水平，优化 IT 支出，一站式即可完成。

在当今快速发展以及变化的环境下，客户的转型、现代化和迁移正呈现出加速势头，基于云的技术使得软件的开发和运行比以往更加容易。除了早期采用者之外，我们看到了很多企业正在从传统的IT模式转向云模式，我们希望帮助这些企业尽可能轻松、快速地实现转型。这需要在安全性、合规性和速度之间找到一个平衡点。企业需要尽快对机会做出反应，却缺乏快速实施新技术的能力。与此同时，企业希望利用新的应用程序提升自己的客户体验，但需要维持并提高其IT支出的透明度。我们看到了这些挑战，并希望借助我们的技术助力客户加速和简化云迁移和转型。

在过去的几年，亚马逊云科技已经帮助成千上万的企业客户迁移到云端。在这个过程中，我们依靠广泛的软件和咨询合作伙伴帮助客户成功实现转型以及应用程序的现代化。这些合作伙伴的解决方案和服务是基于云而构建的，因此提升了客户转型的速度和敏捷性。为了更好的帮助企业客户轻松找到合适的第三方产品和服务，亚马逊云科技构建了亚马逊云科技 Marketplace。

亚马逊云科技 Marketplace 是一个精挑严选的数字化产品目录，企业客户通过它轻松查找、购买、部署和管理第三方软件于服务，完善了企业用户的云迁移之旅，帮助企业轻松找到合适的产品和服务，将治理和透明度放在优先位置，并优化 IT 成本和交易。亚马逊云科技和我们的合作伙伴帮助企业客户简化并加速云迁移，从企业客户的需求出发确立最佳的现代化战略。

亚马逊云科技 marketplace

安全

伴随云计算技术的快速发展，云安全问题备受关注，传统的信息安全技术已经不能满足云计算时代的信息安全要求。合作伙伴们基于亚马逊云科技的技术架构，为客户打造的下一代防火墙、WAF 和边缘安全、云基础架构安全等解决方案，既为客户提供安全环境，又能有效提高敏捷性、可伸缩性，降低成本，让客户获得3大安全收益：

- 快速采购和部署，在保证响应速度的同时快速发现和解决漏洞，以减少入侵对正常业务造成的干扰；
- 能与亚马逊云科技其他安全工具轻松集成，提升操作体验；
- 从迁移到日常管理，亚马逊云科技合作伙伴可为客户提供适合不同发展阶段的安全解决方案，以持续拓展客户对安全架构的需求。

亚马逊云科技 marketplace

paloalto NETWORKS

容器安全解决方案

Prisma Cloud Compute -为 DevOps 和 SecOps 团队提供了可视性和安全性，并具有先进的"安全前置（shift left）"与中央 CI/CD 策略管理功能，以及其他一些主机安全功能和架构改进特色。这些增强功能使企业能够在任何云和软件栈的 DevOps 全生命周期中实现云安全，并最终将先前划分的业务部门统一到一个共同目标上来：实施一种开发安全运营（DevSecOps）方法来推动安全的业务创新、扩展和增长。

客户挑战

传统的安全工具和方法不适合保护开发人员驱动的、与基础架构无关的、多云模式的云原生应用。这是因为：

- 开发人员和 DevOps 团队在构建和部署云原生应用方面起着至关重要的作用，他们通常在传统安全的视野之外进行操作。这需要与开发人员主导的基础架构和工具集成的安全性。
- 各企业使用的计算方案比以往任何时候都多，包括混合和多云部署，以及使用主机虚拟机 (VM)、容器、Kubernetes®、容器即服务 (CaaS) 和无服务器功能的组合。
- 云原生环境不断地发生巨大的变化。安全团队需要使用自动化来保护企业使用的数量不断增长而又不断变化的微服务。

Palo Alto Networks 产品

Prisma Cloud 计算版提供了灵活的部署选项，无论您选择在何处部署工作负载和应用，都可以保护它们。防御程序保护独立的虚拟机，Docker 容器，K8s 集群，容器即服务 CaaS，关键应用服务上的 PaaS 应用和无服务器应用。防御程序通过将应用行为加入白名单和防止发生异常操作来进行保护。深度防御将核心云原生防火墙与运行时防御结合，以保护东西向流量，并利用机器学习了解未知的应用行为。

适用场景

企业持续不断地实现其软件开发生命周期的现代化，并采用现代工具和流程，例如 DevOps、容器和其他云原生架构。这种增长伴随着不断增加的多样化云足迹同步发生，最终使生产和整个应用生命周期中需要保护的实体数量成倍增加。
安全团队需要持续监测保护该基础设施以上设备（虚拟机、容器和无服务器）以保证安全稳定运行，Prisma Cloud 提供了一个统一的代理框架来保护所有这些工作负载和架构。

客户收益

Prisma Cloud 是一个全面的云原生安全平台，在整个开发生命周期以及跨混合云和多云环境中，为应用、数据和整个云原生技术堆栈提供了业界最广泛的安全性和合规性覆盖。这种集成方法消除了围绕云原生体系结构的安全约束，而不是试图掩盖它们，并且还瓦解了整个应用生命周期中的安全操作隔阂，实现了 DevSecOps 的采用，增强了对云原生架构不断变化的安全需求的响应能力。

主要优势：

- 通过端到端安全解决方案，运营团队无需在浪费时管理和集成多种不同工具,大大降低安全运营成本。
- 以 DevOps 的无缝集成自动实现安全保护，授权开发人员和 DevOps 团队尽快进行部署，以向客户交付商业价值。
- 加快云原生应用架构的使用，帮助企业数字化转型进程。
- 囊括您喜欢的任何云原生技术，使您的基础架构决策永不过时。为任何给定的应用组件选择正确的工作负载，并了解您所涉及的安全平台。
- 在云原生环境中根据情境确定风险的优先级。在整个云原生基础架构中和整个软件生命周期期间，利用持续的漏洞情报和风险优先级，包括实时连接图和运行时威胁数据。
- 以 DevOps 速度自动实现安全保护。授权开发人员和 DevOps 团队尽快进行部署，以向客户交付商业价值，并改善安全防护效果。

产品功能

计算资源保护方面

全面的漏洞管理

持续监控主机的漏洞，将强大的风险优先级划分和 10 大漏洞列表结合，查看对于映像和容器漏洞的准确见解。10 大漏洞列表提供了所有已知 CVE 的风险优先级，并通过修复指导和按层映像分析提供支持。

合规性检查

利用 400 多项合规性检查，包括 Docker®、Kubernetes、Linux、Windows 配置和 Istio® 的 CIS 基准测试。预构建、可定制的框架支持 PCI DSS、HIPAA、GDPR 和NIST SP 800-190。

CI/CD 安全

集成安全作为 CI/CD 工作流的一部分。设置细粒度漏洞阈值，以对易受攻击的映像发出警报或阻止，或发出合规性策略相关警报或强制执行合规性策略。

运行时安全

通过跨流程、网络和文件系统传感器自动创建运行时策略，保护正在运行的应用，确保安全方案可以随应用扩展。强大的自定义运行时规则增强了容器化应用的安全性。

网络可视化

实时查看容器和 Kubernetes 的所有网络通信。

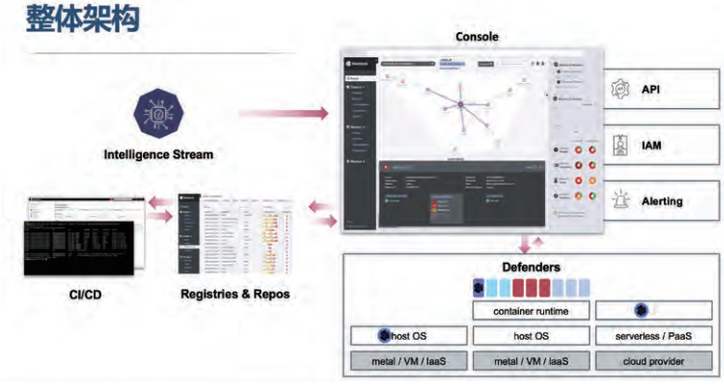
访问控制

跨底层主机、Docker 和 Kubernetes 建立和监视云原生应用的访问控制措施，同时集成身份和访问管理 (IAM) 与加密管理工具，以及其他核心技术。

Web 应用及 API 安全

在任何公有云或私有云中抵御第 7 层和 OWASP 十大威胁。

整体架构



方案特点

Prisma Cloud 是一个全面的云原生安全平台，在整个开发生命周期以及跨混合云和多云环境中，为应用、数据和整个云原生技术堆栈提供了业界最广泛的安全性和合规性覆盖。这种集成方法消除了围绕云原生体系结构的安全约束，而不是试掩盖它们，并且还瓦解了整个生命周期中的安全操作隔阂，实现了 DevSecOps 的采用，增强了对云原生架构不断变化的安全需求的响应能力。

- 提供 IaaS, PaaS, CaaS, Serverless 不同计算资源安全支持保护避免不同产品工具的带来的复杂性。
- 提供无缝集成到 CI/CD 安全插件支持，保证应用开发生产环境安全的同时，避免流水线开发效率造成影响。
- 可以与 PA 的 VM Series, Cortex XSOAR 产品进行联动集成，提供统一完整的解决方案，同时提供开放 API 接口，可以和其他三方平台做集成对接。

虚拟机安全功能

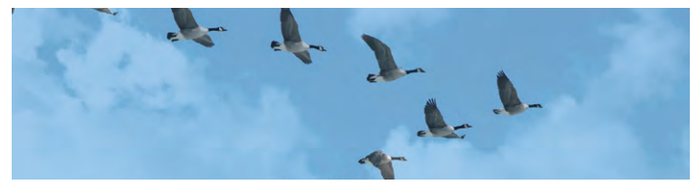
亚马逊云机器镜像（AMI）扫描：企业希望确保对其镜像进行审查以符合漏洞和合规性标准，并从可信来源进行部署。现在，此最新版本中的漏洞管理功能包括扫描亚马逊云机器镜像（AMI）功能，类似于 Prisma Cloud 扫描任何容器注册表或无服务器存储库的方式。这样，开发运营与安全团队就可以在部署 AMI 之前进一步了解其 AMI 的安全状况。

容器安全

Prisma Cloud Container Security 保护在公有云或私有云上运行的容器和 Kubernetes，针对 Amazon EKS 容器业务平台，可以提供端到端的全生命周期的保护、主要包括漏洞管理、合规性检查、运行时安全，网络可视化及 CI/CD 安全。

无服务器安全功能

查看 Amazon Lambda 上正在运行的功能的实时雷达可视化效果。查看功能触发器，持续监控漏洞和合规性状态，并查看所有连接的 Amazon 和 Amazon 服务，如 CloudWatch、ElasticCloud Compute (Amazon EC2®) 和 DynamoDB®，保护正在运行的 Amazon Lambda 功能免受不需要的流程、网络或文件系统活动的影响。



扫一扫访问
亚马逊云科技 Marketplace
了解更多 Palo Alto 解决方案

亚马逊云科技 marketplace

API 安全 - 新一代 WAF

F5® Advanced WAF 无需改造应用，能够帮助企业快速实现抵御针对 BOT 防护、应用层加密、API 及行为分析的攻击，防止凭证泄漏的安全方案。

客户挑战

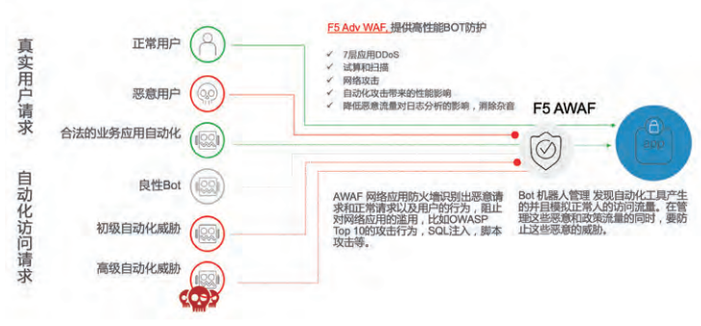
云中部署的应用类型不同，所需的安全策略也随之改变。需要一套完整的 WAF 解决方案部署在应用前端，提升应用的整体安全。

客户收益

- 对传统 WAF 的补充，能够实现基于特征、机器学习、主动挑战的 BOT 防御；
- 帮助亚马逊云科技用户加密登录凭证，防止被窃取滥用。

方案特点

- 帮助可以快速识别 BOT，提前防止对业务系统的攻击和资源滥用；
- 降低资源消耗，减少基础设施投入成本；
- 加密登录凭证，防止凭证泄漏导致的钓鱼、滥用、仿冒等攻击；
- 无需改造应用，快速实现 BOT 防护和凭证加密，降低安全维护成本。



扫一扫访问
亚马逊云科技 Marketplace
了解更多 F5 解决方案

适用场景

提供基于主动式防御的 BOT 防御和凭证加密平台，帮助客户快速识别 BOT 攻击，同时对用户输入凭证进行加密，防止凭证被窃取，保证用户资产安全。

F5 产品

F5® Advanced WAF 通过行为分析，主动式机器人防御和敏感数据的应用程序层加密来保护您的应用程序。F5 Advanced WAF（API 安全 - 新一代 WAF）通过反机器人功能动态防护应用，以按键加密的方式防止键盘监控引起的身份失窃，通过综合性机器学习和行为分析提高应用层 DDoS 嗅探能力。

产品功能

Web 入侵防御

- 最新 OWASP TOP10 威胁防御
- 提供设备指纹识别，识别隐藏攻击
- 安全威胁的全面可视化

抵御 BOT 网络

- 提供主动行为和特征相结合的 BOT 防护策略
- 提供深度网络爬虫防御
- 唯一提供针对 APP SDK 的 BOT 识别和防护

登录凭证保护

- 唯一提供应用层加密的登录凭证保护
- 多层级暴力破解防御
- 实时撞库防御

抵御应用层的 Dos

- 基于行为分析和应用压力智能形成防护模型
- 快速精确防御应用层 DDoS

Silverline® Shape Defense

F5® Silverline® Shape Defense 借助人工智能和机器学习，客户端检查工具和专家的 SOC 团队服务，阻断级别更高的自动化攻击，降低欺诈等恶意风险。

适用场景

Shape 保护企业的 WEB 应用免受自动 BOT 攻击，防止大规模欺诈所导致的运营成本虚高、知识产权被盗窃等行为的发生，避免企业因分析与事实不符的应用数据所造成损失、或因恶意攻击所导致与最终用户产生的摩擦。

客户挑战

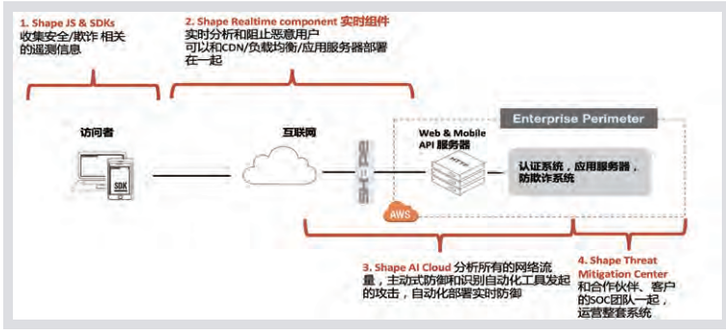
- 企业需要实时防御来自机器人，欺诈者，聚合器，抓取工具的攻击。
- 自动 BOT 攻击，大规模欺诈将导致企业运营成本上升，业务数据失真，进一步造成决策失误。又或者因恶意攻击导致数据被窃取或者被修改造成最终用户的损失。

客户收益

- 为企业提供一站式的防 BOT、防欺诈等服务，从而提高可见性，优化业务，提升用户体验。
- 全面的托管式的安全服务，可保护企业的 WEB 应用程序免受自动化的 BOT 攻击，防止大规模欺诈，以及降低最终用户的运营成本。

方案特点

- 提供了可见性和缓解选项,以保护基于 HTTP 的 API 免受自动化和其他攻击。
- 自动化按需定制的服务,与技术客户经理进行高质量的全方位服务管理。它通过收集环境、行为和网络信号来识别和减少不需要的合成流量,从而提供请求合法性的决策，以用于阻断恶意的请求。



F5 产品

Shape 是防止 WEB 和移动应用程序欺诈和滥用领域的领导者，基于 SaaS 的安全托管服务实现网站安全，部署于 EC2 的 roxy 会将 Hash 后的流量信传到 F5 位于海外的集中安全分析服务器进行分析。

产品功能

传统的安全措施(如设备 ID、WAFs、IPS)通常是基于签名的，无法抵御复杂的、重新装备的攻击者。

Shape 可以帮助企业防止以下攻击类型：

- 账户窃取/撞库
- 信用卡欺诈
- 虚假账户创建
- 高级别的爬虫和 IP 窃取
- 会员活动滥用/薅羊毛等
- 市场活动欺诈

扫一扫访问
亚马逊云科技 Marketplace
了解更多 F5 Silverline® 解决方案

亚马逊云科技 marketplace

FORTINET

网站安全解决方案

作为一款可以灵活配置，按需部署的 Web 应用安全解决方案，FortiWeb 能够帮助用户进行针对 Web 和 API 的精细化威胁防御。FortiWeb 的机器学习可以准确地检测异常，更重要的是识别出哪些是真正的威胁。

适用场景

无论是对公众开放还是仅对内部开放访问的 Web 应用，都需要使用 Web 应用防火墙来保护其 Web 服务和相关联的 API 安全。从业务层面可以分为：基础网站安全通用保护，针对指定网页和站点的特殊防护，针对恶意爬虫的高级网站内容保护，针对盗链的高级网站内容保护，针对网站页面被篡改的高级防护，针对电商类网站的高级业务安全保护，针对应用层 DDoS 攻击的防护，针对暴力破解和撞库攻击的防护。

客户收益

基于双模型机器学习结合高度灵活规则定制的 Web 安全解决方案，能够为用户交付近乎于100%精准度的威胁检测能力，防御 Web 和相关的 API 威胁，用户可以有如下收益：

- 无需投入很大精力来运维 WAF，并基于预配置的 Amazon CloudFormation 模板进行自动创建高可靠 HA 和 Auto Scaling Group。
- 无需担心大规模告警和产生的大量误报，基于行为的机器学习引擎能够有效降低误报，提升检测精确度。
- 无需担心 0Day 攻击，此方案可以检测针对未知漏洞的攻击，并可以针对已知漏洞但无法打补丁的情况提供虚拟补丁。
- 业务信息不会被机器人和爬虫进行恶意窃取，也无需担心通过 Web 上传到应用内的文件含有病毒，从而影响应用安全。
- 无缝对接 Amazon API Gateway，在开放更多 API 进行交互的同时，能够保证足够的安全性。

客户挑战

Web 应用的漏洞是导致数据泄露的最主要的原因，面对如今黑客攻击成本低廉的局面，所有的 Web 安全都将面对黑客的攻击和扫描。

IPS 只能防御网络和系统层面的已知漏洞，不能检测针对 Web 服务和应用的已知和 0Day 攻 击，企业要符合相关行业的安全评估标准，PCI DSS 或者等保。

保护 Web 应用免遭已知和未知漏洞利用攻击，最小化检测带来的大量误报，降低安全运维负担，而单靠特征和规则已经很难达到全面的 Web 安全防护。

传统 Web 安全方案在规则可定制性方面存在不足，有时无法满足客户的特殊需求。威胁可能会隐藏在上传到 Web 服务的文件中，而传统 Web 安全方案可能无法察觉。

现代化的 Web 应用通过 API 进行交互，提供更丰富的能力和能好的用户体验，也带来了更多的攻击入口。

Fortinet 产品

基于机器学习的下一代 Web 应用防火墙解决方案，Gartner Web 应用防火墙魔力象限挑战者，综合排名全球第四位，NSS Labs 推荐级 Web 应用防火墙。

- 此方案基于双层机器学习模型，可以防止 SQL 注入、跨站脚本、命令执行等常见攻击以及被挂马，博彩，被篡改；
- 可以防止恶意爬虫爬取相关内容及恶意程序访问网站，如：恶意刷票/抢票，刷赞，恶意注册，撞库等；
- 可以防止重要静态页面被篡改、对 Web 程序的恶意漏洞扫描，对 Web 应用 API 的恶意调用、病毒植入；
- 可以快速应对未知攻击，基于采取双层机器学习和沙箱、下一代防火墙联动实现对于 0day 攻击快速响应，如：挖矿程序，勒索软件等。

产品功能

标准安全能力

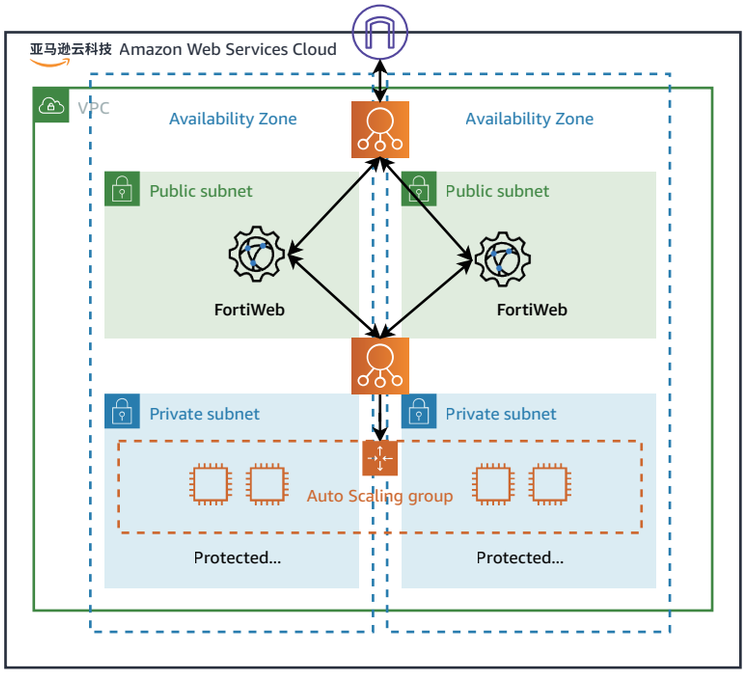
- 防护 OWASP TOP10 威胁：内置多种防护策略，可以选择防护 SQL 注入，XSS 跨站，Web Shell ，后门，命令注入，非法 HTTP 协议请求，常见 Web 服务器漏洞攻击，核心文件非授权访问，路径传阅，扫描防护等等。
- 威胁情报：海量恶意 IP 黑名单，包括僵尸网络，匿名代理，钓鱼网站，垃圾邮件，TorIP 等恶意的 IP 封禁能力。
- 防护基础恶意爬虫：封禁 libcurl ，Python 脚本等构造的恶意访问。
- HTTP/HTTPS 访问控制：IP 访问控制，URL 访问控制，目标系统管理后台保护。

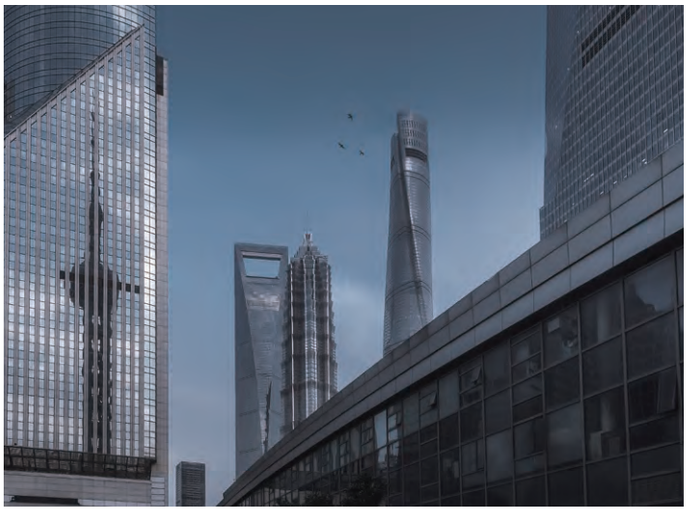
高级安全能力

- 防止恶意 CC 攻击：基于 HTTP 访问请求频率/TCP 连接频率/人机识别等综合智能分析有效拦截 CC 攻击。
- 0day 高精准安全防御：基于双层机器学习引擎构建异常威胁检测模型，对 Web 攻击具有较高的精准识别能力，可以自动发现 0day 等未知攻击，有效减少攻击误报。

业务安全能力

- 高级防爬虫：基于 user-agent ，IP，客户端事件及 AI 的人机识别技术精准识别爬虫。
- 防盗链：避免网站资源被其他网站恶意链接、使用。
- 防漏洞扫描：检测攻击则采用工具对网站进行漏洞扫描，并通过人机交互进行精准确认，最终准确拦截攻击者。





方案特点

具备三种机器学习模型

机器学习建立正向异常检测模型；支持联动 FortiGuard 威胁情报生成的机器学习威胁模型；支持基于机器学习建立自动识别机器人（Bot）动态检测模型。

能够提供虚拟补丁

帮助用户保护无法打补丁的老旧应用，或提供更长的补丁开发窗口期。

灵活可靠部署

结合 Amazon ELB 支持 AP/AA 模式的高可靠部署，并支持 Auto Scaling Group 进行弹性扩缩容。

Gartner 魔力象限挑战者

NSS Labs 评测推荐级，并且提供 Top 级产品中最好的性价比。

在公有云上 WAF 部署的最佳实践为“三明治”架构，
即 ALB-FortiWeb-ALB 的三层架构。

入向流量通过 ALB 负载，并基于内容分流，WAF 专注于管理高级 WEB 安全配置，在访问流量清洗完成后，再通过内部 ALB 将流量分发给应用所在的计算资源，即被保护的 Web 应用服务器。

为了满足用户对Web安全高可用性及冗余性的要求，FortiWeb 提供了Active-Active（A/A）及 AutoScaling 两种高可用解决方案。

扫一扫访问
亚马逊云科技 Marketplace
了解更多 Fortinet 解决方案

亚马逊云科技 marketplace

安恒信息 DAS-SECURITY 安全中国

一站式云安全方案

安恒一站式云安全解决方案为用户提供针云场景下的一站式云安全解决方案，基于等保2.0“一个中心，三重防护”的理念，为云上业务系统提供完整的云安全等保合规产品服务及方案，满足用户云上业务多样化的安全需求。

安恒产品

- 明御 Web 应用防火墙
- 明御运维审计与风险控制系统
- 明御数据库审计与风险控制系统
- 明御综合日志审计平台
- 明御主机安全及管理系统

适用场景

可用于企业客户、金融客户、医疗客户、教育客户、运营商客户、互联网客户等，覆盖以下应用场景：

云上业务满足等保2.0合规场景

安恒云安全为客户提供多样化、自服务化的安全能力及等保2.0合规套餐，满足客户对安全建设的合规性需求。

云内资产安全运维场景

在资产运维层面，用户往往有以下需求：外包企业运维安全监管、等级保护合规，内部运维统一管理等，安恒堡垒机实现资产全覆盖，运维精细化管理无死角的全生命周期运维内控审计解决方案。

数据库访问数据监控审计场景

安恒数据库审计帮助用户加强数据安全的管控，数据库审计系统可对核心数据库的访问情况进行监控，并对非常规操作进行预警，对所有的访问的追踪溯源。

WEB 应用安全防护场景

用户的 WEB 业务系统包含了大量的用户信息和大量有价值的数据，WAF 可构建WEB应用的防护体系，可有效防范网页篡改、网站恶意攻击导致信息泄漏，有效保障网站安全可靠的运行。

勒索病毒查杀，主机安全防护场景

在勒索病毒、挖矿病毒等造成重大破坏前，通过部署主机安全，批量下发各种配置策略，及时隔离病毒防止扩散并快速查杀，守护主机安全。

客户挑战

云上合规建设难

安全边界从清晰变得模糊，资产从单一变得多元，等保2.0时代，等保合规建设成为用户云上业务安全建设的痛点

传统安全建设方式难以适用云环境

传统的等保合规安全建设方式往往存在实施部署难度大、运维管理混乱、资源利用率低等问题，满足不了云内的等保合规需求。

企业内部安全运维管理日益复杂

据统计70%的安全事故来自企业内部运维管理，在日常云上资产运维的过程中，安全运维成为云上安全建设面领的重要一环。

云主机安全问题对业务的影响面扩大

用户云环境中的云内资产数众多，云主机或操作系统层面都不可避免的存在软硬件漏洞，一旦有云主机被感染，将使云平台业务瘫痪。

云上业务应用系统安全问题仍然存在

云上业务应用层面的脆弱性最为复杂，大量安全漏洞都可能成为被攻击者所利用，从而对云平台本身造成严重的危害。

云上数据安全问题日益突出

云平台上的业务数据均存储在云端，所以在数据层面的脆弱性也就因此产生。

客户收益

等保2.0标准快速落地，云上业务快速合规

安恒一站式云安全解决方案提供等级保护二级、三级合规能力，帮助用户快速满足等级保护要求，业务合规。

安全能力服务化，安全服务按需订购

为云上的不同用户提供全方位的基于“安全云”的安全保障服务能力，用户可以自行选配，灵活使用，最终建设形成自有的云内业务系统安全解决方案，覆盖事前、事中、事后的全方位安全防护。

可以快速构建安全防护系统

安恒一站式云安全解决方案具备丰富的云安全防护能力，涵盖主机网络、应用、数据多层安全保障能力用户直接用户在亚马逊云科技上订阅就可以实现一键交付，降低安全建设的难度，提升安全管理的效率。

可实现云上业务系统纵深安全保障

安恒一站式云安全解决方案为用户提供具备强有力竞争力的安全产品，从外部攻击防御到内部安全管控两方面提升云安全水平，建设可供用户放心托管的云基础设施环境。

方案特点

核心安全能力业界领先

等保 2.0 更加偏重对事前、事中、事后的安全管理闭环，要求有强大的审计能力和事后追查、溯源、处置能力，安恒信息在安全防护、安全审计、运维审计、等方面具备业绩领先的优势。

等保 2.0 经验丰富

安恒信息参与等级保护国家、行业标准撰写，是公安部等级保护推广推荐单位，具备丰富的等保建设经验，客户覆盖广，安恒信息承接了政府、企业、金融等众多客户的等级保护工程建设，均取得了很好的测评成绩，切实协助客户落实了等级保护要求、推动了客户网络安全工作；

安全能力丰富

安恒一站式云安全解决方案具备丰富的云安全能力，可以帮助用户一键构建云安全等保合规防护体系，帮助用户省心、省力。

安全能力弹性可扩展

安恒云安全能力秉承云计算的核心理念，安全能力具备弹性扩容能力满足用户业务弹性扩展的特性。

产品功能

明御® Web 应用防火墙

拦截针对网站的各类攻击，帮助用户应对网站运营中的安全风险，为 Web 应用提供全方位防护，构建覆盖全生命周期的 Web 应用安全防护解决方案。

明御运维审计与风险控制系统

为用户提供运维审计能力，全程记录运维操作行为，并通过录像方式回放，帮助用户满足业务等保合规要求，实现资产全覆盖，运维精细化，管理无死角的全生命周期运维内控审计解决方案，解决云上业务安全运维难题。

明御® 数据库审计与风险控制系统

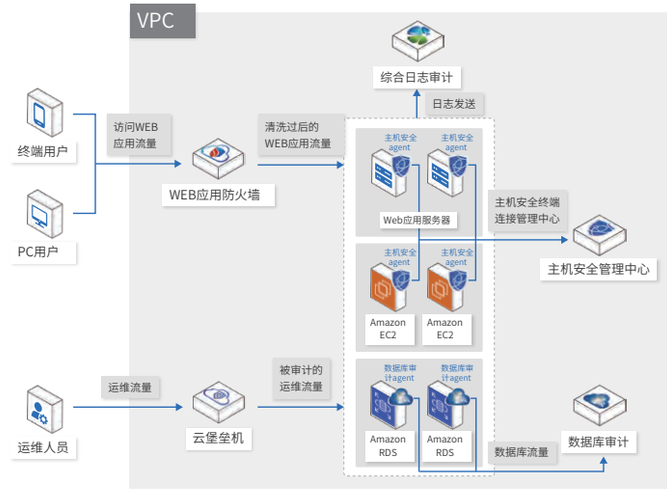
为用户提供数据库审计与监控能力，对数据库风险操作行为进行实时记录与告警，提供数据库权限管控、事后行为审计能力，满足云上等保合规要求。

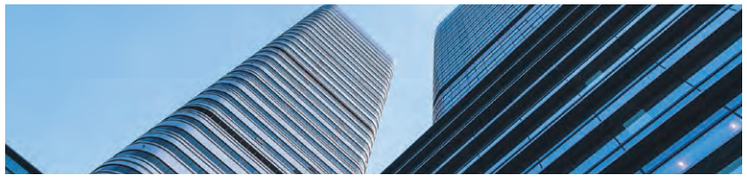
明御® 综合日志审计平台

提供全维度、跨设备、细粒度的日志关联分析，透过事件的表象真实地还原事件背后的信息，为用户提供真正可信赖的事件追责依据和业务运行的深度安全监控，协助用户全面审计信息系统整体安全状况。

明御® 主机安全及管理系统

提供主机系统防护与加固、主机网络防护与加固等功能，具备业界领先的勒索专防专杀、网页防篡改、网络隔离与防、补丁修复、外设管控文件审计、违规外联检测与阻断等主机安全能力,帮您快速发现网站潜在安全隐患。





扫一扫访问
亚马逊云科技 Marketplace
了解更多安恒信息解决方案

亚马逊云科技 marketplace

radware

Radware CNP 云原生安全防护服务

Radware CNP 云原生安全防护服务为企业提供了全面的云端安全解决方案，可以强化云配置，减少受攻击面，增强安全态势，并在发现攻击后立即响应，从而帮助企业保护云环境安全。

适用场景

全球越来越多的垂直行业将面临来自云端新的威胁。因此，所有迁移到亚马逊云科技或云原生的企业用户，需要对其云基础架构和云应用面做全面的安全防护。

客户收益

采用 Radware CNP 云原生安全防护服务的客户可以享受以下优势：

- 对用户的云资产具有全面的可视性，并了解有哪些资产以及数据可能暴露的地方，防止因云资产意外曝光而引发的数据泄露；
- 保护亚马逊云科技账户不被窃取和账户滥用；
- 避免混杂权限，进而限制用户账户入侵引发的潜在威胁；
- 通过智能 AI 分析来识别可疑行为和检测黑客攻击，并在攻击发生和数据泄露之前将其拦截；
- 通过拦截数据泄露，密码挖掘等关键矢量，来描绘整体云环境安全态势，并提供重要的取证信息来满足合规需求，从而帮助企业满足等保、PCI 、HIPAA 和 GDPR 等合规标准。

产品功能

Radware CNP 为全面保护用户的亚马逊云科技云资产提供了一种无需代理端的云原生解决方案，不仅可以保护云环境的整体安全态势，还可以保护单个云工作负载免受云原生攻击矢量的影响，满足用户在云端的安全和合规需求，包含以下功能：

- 云基础设施的权限管理(CIEM)
- 云安全态势管理(CSPM)
- 云威胁的检测和响应
- 跨云的全视图监控

扫一扫访问
亚马逊云科技 Marketplace
了解更多 Radware 解决方案

客户挑战

企业将工作负载迁移到公有云环境会将企业用户暴露在一系列原先在本地数据中心中不存在的新的云端原生攻击威胁中。

- 安全和运维团队难以对公司的所有云资产，云账户和使用状况做持续和全面的监控和权限管理；
- 安全和运维团队需要对云原生的威胁和攻击做出及时和准确的检测以及快速的响应；
- 企业用户需要确保其云端的业务符合多种安全合规标准，如等保，GDPR , HIPAA 和 PCI 等。

方案特点

- 跨云的全视图监控：用户通过 CNP 一个控制仪表盘就可以对亚马逊云科技上的所有工作负载提供集中的安全管理。在这个仪表盘中可以对云资产清单做自动发现，并对跨多个账户、区域和环境的云资产提供统一的视图；
- 满足法规遵从性要求：更好的遵守区域或行业法规，如等保，GDPR PCI 或 HIPAA ；
- 强化云安全态势与错误配置检测：通过 CNP 智能的加固建议和风险优先级警报，在安全漏洞出现之前防止它们；
- 消除过多的权限：通过分析预先定义的权限和实际使用的权限之间的差距，消除不必要的权限，且不中断业务流程；
- 阻止数据盗窃企图：通过 CNP 先进的攻击检测和智能分析连接单个事件的关联功能，可以展现出一个单一的，统一的攻击-杀伤链的演进；
- 用户无需安装代理端，可直接使用的 SaaS 产品。

亚马逊云科技 marketplace

网络

云时代，网络速度备受关注，用户需要在任何时间以安全的方式访问和部署生产力应用，亚马逊云科技提供了一套具有高可靠性、安全特性和高性能的全球最广泛、最深入的联网服务使合作伙伴可以为用户提供的高可靠性、高性能、广泛覆盖全球的联网服务，一站式覆盖全球生产力提升、满足未来网络架构发展的解决方案，以满足用户加速和安全的双重需求：

- 预置专属逻辑隔离网络，为 VPC /服务和本地应用程序提供专用链接，快速地设置、保护和监控网络安全。通过广泛的基础设施，在全球建立骨干网络，为用户提供低延时、超高速的稳定连接
- 集中配置并管理防火墙规则，保护在亚马逊云科技上运行的应用程序免遭 DDoS 攻击，保护 Web 应用程序免遭常见 Web 漏洞的攻击

亚马逊云科技 marketplace

利用 Cisco CSR1000v 搭建 Transit VPC

思科 CSR100 0v 云服务路由器可在亚马逊云科技中提供企业级网络服务和 VPN。此 AMI 支持所有四个 CSR 技术软件包。CSR是功能齐全的 Cisco IOS XE 路由器（即 ASR1K）的云服务版本。企业 IT 部门能够在亚马逊云科技中部署与企业内部网络相同的企业级网络服务。

客户挑战

- 未来几年的网络架构需要考虑企业站点数量的增加、上云业务流量的增大、云端业务 VPC 数量的扩展，以及网络中路由表数量的变大。如何设计满足未来几年的网络架构？
- 利用 CSR1000v 构建的 Transit VPC 如何与亚马逊云科技的 VGW、TGW、VPC Peering、DX、DXGW 等各网络组件实现互联互通，共同组成一个满足各种用户需求的云网络系统。
- 如何实现互联网线路或专线上进行传输数据的加密及实现网络应用的可视化。
- 如何保证从私有化数据中心向云端迁移的过程中，不修改应用服务器的 IP 地址？

客户收益

- 利用 CSR1000v，帮助客户构建高性能、高安全、高可靠性、高扩展性的 Transit VPC。可以为私有数据中心、企业总部以及各分支机构提供扁平化的接入网络，并提供高速可靠的加密数据通道，同时还可实现同 Region 或跨 RegionVPC 之间的互通。
- 亚马逊云科技Marketplace 上架的 Transit VPC 解决方案基于 CSR1000v，支持“即插即用”的部署体验，借助于 CloudFormation，可以实现Transit VPC 的自动化部署。
- 利用 CSR1000v 构建的 Transit VPC ，不仅仅实现了云中心和企业各站点的互联，并且实现了迁移过程中不需修改 IP 地址，并继续沿用客户已有的网络及应用可视化系统和网络管理运维系统，迁移前后使用无差别。
- 降低企业的组网及运维成本。通过 CSR1000v 构建的扁平化网络，企业各级接入站点只需就近接入到就近的 Amazon Region，就能实现与其他 Region 内 VPC 的互联互通，而无需租建昂贵的长途线路甚至国际线路。

适用场景

企业应用系统迁移到云端之后，数据流量的访问关系及安全性要求都与传统网络架构产生了很大的变化，具体表现在如下几个环节：

网络扁平化的要求

企业上云之后，流量模型转换为从总部和各级分支机构直接到云数据中心。出现网络扁平化的要求，从各级分支机构到达云数据中心的流量不再需要经过总部或私有数据中心，而是直接上云。

网络流量加密的要求

为了保证数据在互联网上传输的安全性，对数据的加密成为一个重要的技术要求。

网络高扩展性的要求

从企业 IT 系统扩展性的角度考虑，必然要求网络需要有一个清晰的层次和架构，并能够支持未来几年内站点数量的扩展、流量规模的增 大，以及网络规模的平滑扩展。

网络及网络应用的可视化

在企业上云之前，大部分企业内部都已经部署了网络和应用的可视化工具，可以非常清晰的看到整个网络的拓扑、线路的状态和传输质量、网络中传输了哪些应用以及各应用的传输效果如何。

网络的集中自动化管理

在企业上云之后，企业的网络运维部门系统仍然希望采用原有的网络管理运维系统和工具，对整个网络实现集中的管理和自动的业务开通和变更。

思科产品

思科 CSR1000v 云服务路由器可在亚马逊云科技中提供企业级网络服务和 VPN。此 AMI 支持所有四个 CSR 技术软件包。CSR 是功能齐全的 Cisco IOS XE 路由器（即ASR1K）的云服务版本。企业IT部门能够在亚马逊云科技中部署与企业内部网络相同的企业级网络服务。CSR 支持企业级路由，VPN，防火墙，高可用性，IP SLA，AVC，WAN Opt 等。熟悉的 IOS XE CLI 和 RESTful API 可确保轻松部署监视，故障排除和服务编排。

产品功能

构建高带宽、高安全、高可靠、高扩展的Transit VPC

高带宽：每台 CSR1000v 可提供最高 4.5G 的 IPSEC 吞吐量，支持多个IPSEC 隧道 Active-Active 工作模式，实现流量的负载分担

高安全：CSR1000v 自身支持 IPSEC 等丰富数据加密技术，同时内嵌基于状态防火墙、入侵侦测等高级网络安全特性

高可靠：Transit VPC 通过在2个AZ中分别部署 CSR1000v，可提供1+1冗余能力

高扩展：每台 CSR1000v 支持2400万条IPv4路由，1000个 IPSEC 隧道、4000个VRF、512000 条 NAT 表项、40万条BGP 路由、65000 条 ACL 表项，完全可以支持超大型网络的扩展性需求。

多个业务 VPC 之间的隔离与互通

CSR1000v 自身支持流量隔离技术（Traffic segregation），可以根据策略实现多个业务 VPC 之间的相互隔离以及互通关系，而无需配置 VPC Peering 或 TGW。

跨 Region 部署

通过在每个 Region 分别部署 Transit VPC，并将 Transit VPC 之间通过 IPSEC 连通，可以方便的搭建跨多 Region 的业务 VPC 互联平台，同时用户站点的接入也无需通过昂贵的长途线路连接到远端 Region 而只需要就进接入 Region 的 Transit VPC，就能实现与全网业务 VPC 的互联互通。

与私有数据中心之间大二层延伸

通过启动 CSR1000v 内部的 LISP 控制协议，可以实现亚马逊云科技中心与企业私有数据中心之间的大二层延伸，云中心和私有数据中心之间共享一个 IP 地址段，帮助用户在向云端迁移的过程中，无需修改原有服务器 IP 地址，方便企业完成迁移。

基于性能的横向扩展

通过监控 CSR1000v 实时的网络吞吐量，实现 CSR1000v 的横向扩展并自动实现多台 CSR1000v之间的流量负载分担，无需人为参与。

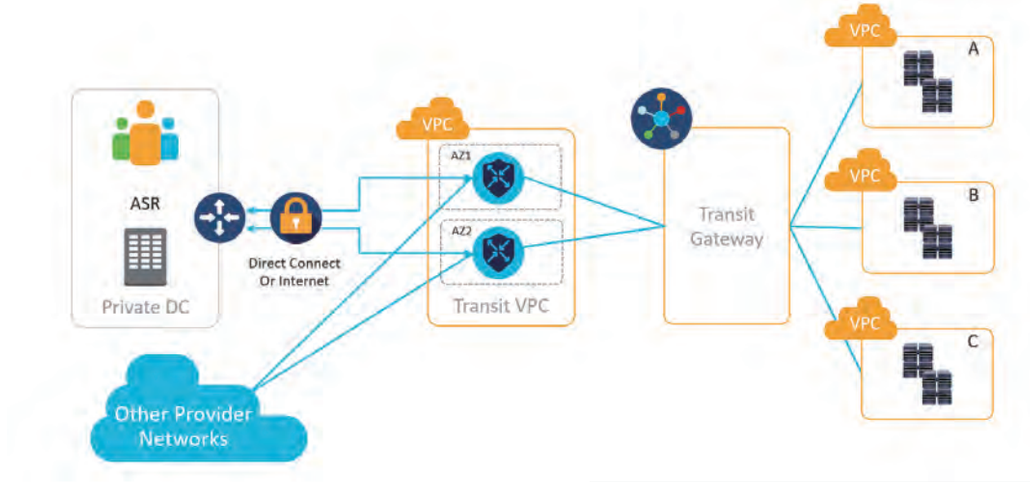
Security VPC

通过在 Transit VPC 中启动 CSR1000v 内嵌的防火墙、入侵侦测等高级网络安全功能，可以平滑将 Transit VPC 升级为 Security VPC，保持云数据中心安全 DMZ 架构与传统数据中心不变，沿用企业原有网络安全运维策落和运维体系不变。

方案特点

- 业界云端路由器部署案例最多，全球市场份额排名第一。
- 功能和特性最为丰富云端边缘路由器，不仅提供边缘路由功能，同时支持应用自动识别及可视化、下一代防火墙等高级网络安全特性等。

  高性能云端路由器，通过升级许可，可以方便实现高达4.5G的 IPSEC 吞吐量。
- 开放式路由平台，初了支持传统路由功能外，CSR1000v 自身支持容器技术和 Python 运行环境，企业可以根据自身需求在 CSR1000v 上运行自定义的脚步或其他程序（如网络流量监控探针等），而无需单独启动 EC2。



扫一扫访问
亚马逊云科技 Marketplace
了解更多 Cisco 解决方案

亚马逊云科技 marketplace

zenlayer

全球智能加速器

全球智能加速器 GIA，帮助业务解决全球用户访问卡顿或者延迟过高的问题，赋能企业最短的时延、最稳定的质量，让全球任意位置的终端用户畅享极速连接，无忧连接到客户的应用服务。

客户挑战

- 终端用户在访问企业网站、应用、内容（游戏平台、直播平台、交易引擎、电商网站、企业内部系统）的时候出现卡顿，访问不流畅，用户体验差。
- 企业跨境从服务器下载数据时间过长，出现下载多次中断无法正常完成的情况。
- 云上与云下，企业面临各区域云中的服务器之间数据同步时间长短，同步时间是否在业务允许范围内等问题。

客户收益

降本增效

用最短的时延、最优的路由、最稳定的质量，让全球用户连接到您的应用服务。

提高收益

赋能游戏、直播、在线教育、金融交易引擎、电商网站、企业内部系统等实时内容传输流畅，使用户体验得到大幅提升，提高用户留存率，为客户带来持续稳定的收益。

节约成本

动态扩展边缘节点，使客户服务更接近最终用户，无需将源站内容复制到过多地区，有效节约客户建设成本。

高效运营

管理数据稳定和高速传输，减少网络运维人员及开发人员的精力消耗，避免大量时间浪费在重连及等待中。

适用场景

分布在全球各地的企业，面临终端用户访问慢，时延过高，稳定性差，丢包过高等用户体验问题，从而造成企业运营与协作效率低，终端用户流失及增长缓慢、留存少且直接产生经济损失。Zenlayer 全球智能加速器 GIA，帮助企业实现全球用户快速、稳定地访问部署在亚马逊云科技的服务。

Zenlayer 产品

全球智能加速器 GIA，依托 Zenlayer 全球节点之间的高速通道与智能路由技术，实现各地终端用户的就近接入，通过低时延高速通道直达 亚马逊云科技全球各个源站区域，帮助业务解决全球用户访问卡顿或者延迟过高的问题。赋能企业最短的时延、最稳定的质量，让全球任意位置的终端用户畅享极速连接，无忧连接到客户的应用服务。

方案特点

- 低时延、高质量、高可用、易部署。
- 技术领先：多年优化与加速的行业实践与技术积累，通过技术研发创新（就近接入、骨干调度、协议优化、智能选路、应用识别）提升全球用户访问性能。
- IP 透传：获取用户真实 IP 信息。保障 IP 有效透传，满足业务对数据分析的需求。
- 下单灵活：整套解决方案均可通过海外亚马逊云科技 Marketplace 直接部署与采购，流程便捷。
- 计费友好：同时支持带宽计费与流量计费。

产品功能

网络能力

- 广泛覆盖：与中国和全球运营商达成广泛网际对等直连和规模性覆盖，网络一跳可达内容；
- 最低时延：骨干资源覆盖亚洲、欧洲、南美洲、北美洲、大洋洲，节点采用 LVS 负载，直接 FULLNAT 模式，全球 GSLB 调度系统；
- 智能选路：线路质量实时探测，应用级别的智能选路调度与切换机制。
- 亚马逊云科技无缝对接：与亚马逊云科技在全球多个区域通过云专线预部署打通，真正做到一步上云。

协议优化

- 协议支持：支持域名接入，支持4/7层协议，包含 TCP/UDP、websocket、socket(5)、HTTP(s)、FTP、ICMP、TLS（支持 1.3 向下兼容）SSH、SPS 等私有协议，支持4层 TCP option ，支持 Proxy 协议 v1/v2。
- 协议优化：结合 FEC、弱网优化等技术，屏蔽互联网质量不佳的问题，优化最后一公里的连接质量。支持单边加速、图片压缩、字节流缓存等技术，优化 TCP 传输质量，进一步提高用户使用体验。
- 内核支持：自研4.14内核优化 BBR，自研4.14内核 TOA 模块，自研4.14内核 TCP 大文件下载模型，自研4.14内核 TCP 小文件下载模型。
- 双向加速：支持双向加速（C2G，G2C），源站在海外或中国，均可以实现全球用户访问的加速效果。

赋能安全

- 安全特性：IP 黑白名单/ HTTPS 自助证书。

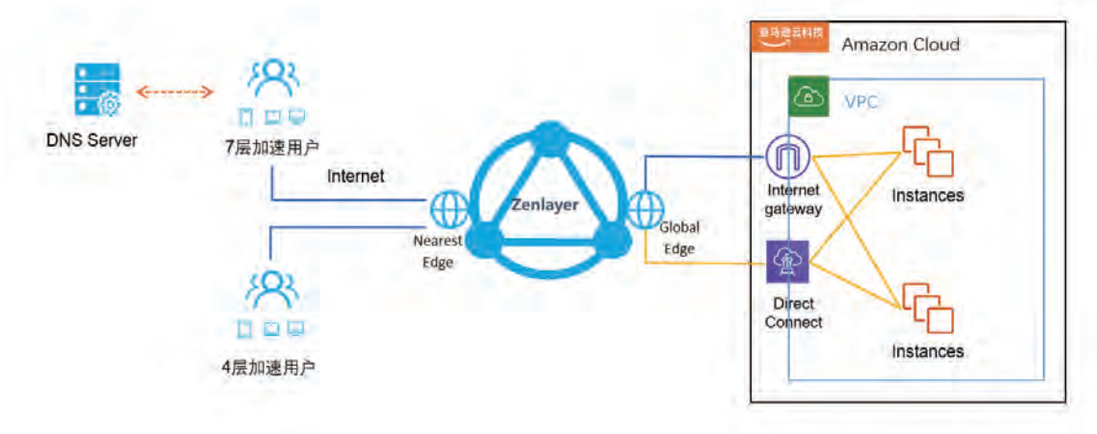
服务特点

全球连接

Zenlayer 全球180+IDC，25Tbps 容量储备，与全球运营商达成广泛网际直连和规模性覆盖。在全球6个大洲建立起连接全球的自有骨干网络，为用户提供高速稳定的连接。

超预期服务

专业技术支持团队，7x24 中英文双语支持 NOC 中心，低于15分钟的故障响应时间，95%以上的用户故障在4小时内解决，骨干网 SLA 达到99.99%。



扫一扫访问
亚马逊云科技 Marketplace
了解更多 Zenlayer 解决方案

亚马逊云科技 marketplace

FORTINET zenlayer

全球加速解决方案

Fortinet 与 Zenlayer 联合解决方案-全球智能加速为用户提供一站式覆盖全球的生产力提升解决方案。

唾手可得的办公神器，客户可以在任意位置、任何时间以优异的体验安全访问部署在全球任何地方的生产力应用。可以同时满足用户在全球加速和安全方面的双重需求。

适用场景

企业行业链条长，跨度大，用户在使用时普遍存在较差的体验，如延迟高甚至导致无法访问，视频的卡顿和掉线，或者页面加载时间过长，点击后响应超时，文件上传下载缓慢，配置保存不及时，超长的等待时间。

客户收益

唾手可得的办公神器

化繁为简，让办公应用发挥原有价值，让客户无忧访问、更加聚焦全身心投入自身业务。安全、省钱、省心，做到无忧上云、极速云间互通，各类办公应用访问高效稳定，无卡顿、花屏、掉线等问题。文件传输及 Web 页面加载速度大幅提升。全面提升协作效能，提高办公效率。

客户挑战

- 办公效率受阻，在使用海外应用系统或 SaaS 服务作为生产工具的企业在日常沟通、协作、生产的效率受到影响，生产力不足。
- 传统解决方案在场景支持方面受限，无法同时支持针对用户端和服务端的加速。比如无法全面覆盖移动端、PC 端、办公室、数据中心、VPC 等场景。
- 针对多平台、多环境、多应用的加速通常使用不同的解决方案，带来很高的管理复杂度。
- 针对可能分布在全球的 IaaS/SaaS 或其他应用服务没有针对性的路径优化，导致体验优化不明显。

Fortinet 与 Zenlayer 产品

- 智慧协同、化繁为简、以人为本，Zenlayer+ Fortinet 颠覆你和世界的连接方式！
- 唾手可得的数字化转型办公神器，客户可以 在任意位置、任何时间以优异的体验安全访问部署在全球任何地方的生产力应用。可以同时满足用户在全球加速和安全方面的双重需求。
- 作为网络安全与边缘云服务两大领域的全球领导者，Fortinet 与 Zenlayer 联合解决方案-全球智能加速为用户提供一站式覆盖全球的生产力提升解决方案。
- 无缝对接：骨干网中引入更多内容，与各类型 SaaS 在全球多个区域实现直连，真正做到一跳访问，全程可控。与亚马逊云科技在全球多个区域通过云专线预部署打通，一步上云。
- 兼收并蓄：同一平台融合完善的 SD-WAN 与安全能力，实现加速的同时保障安全。
- 下单灵活：整套解决方案均可通过中国和海外 Amazon Marketplace 直接部署与采购，流程便捷。

方案特点

网络

- 全智能高速网络，传输 PoP 之间骨干0丢包
- 本地链路，云连接专属网络，结合全球骨干网与协议优化，实现端到端全栈加速
- 全链路实时监控、故障切换、冗余集群、全球智能负载与智能调度
- 传输协议优化与内核优化，可用性99.99%，性能提升200%+
- 支持 TLS 1.3、支持单双证书、IP 黑白名单、Referrer 和时间戳防盗链、回源校验、URL 加密

SD-WAN 设备

- 5500+应用识别，覆盖几乎全部主流 IaaS，SaaS 和办公应用
- 开箱即用的 SD-WAN 规则（最大性能、最低开销、质量最好）
- 健康检查协议支持全面：ping, tcp-echo, udp-echo, http, twamp, dns, tcp-connect, ftp
- 基于延迟、抖动、丢包三大关键指标检测，并支持自定义健康指标可接受阈值，以及检查周期和切换规则
- 针对语音视频应用的质量优化（前向纠错 FEC，逐包均衡）
- 集成入侵防御，反病毒，URL 过滤等下一代防火墙功能
- 零接触部署，运维管理简单，且支持部署在企业办公网，数据中心，Amazon VPC 等环境

终端软件

- 支持部署在 Android，macOS，iOS，Windows，Linux
- 可选 VPN 版和集成应用控制、反病毒、URL 过滤、漏洞扫描的全功能版
- 可与企业现有身份管理平台集成，并实现 SSO 单点登录

产品功能

网络

全球连接：Zenlayer 全球 180+IDC，25Tbps　容量储备。在全球6个大洲建立起连接全球的自有骨干网络，为用户提供超低时延、超高速的稳定连接。

最低时延：低时延路由资源覆盖亚洲、欧洲、南美洲、北美洲、大洋洲，节点采用 LVS 负载，直接 FULLNAT 模式，全球 GSLB 调度系统。

智能选路：线路质量实时探测，应用级别的智能选路调度与切换机制

广泛覆盖：与中国和全球运营商达成广泛网际对等直连和规模性覆盖，逻辑一跳可达应用。

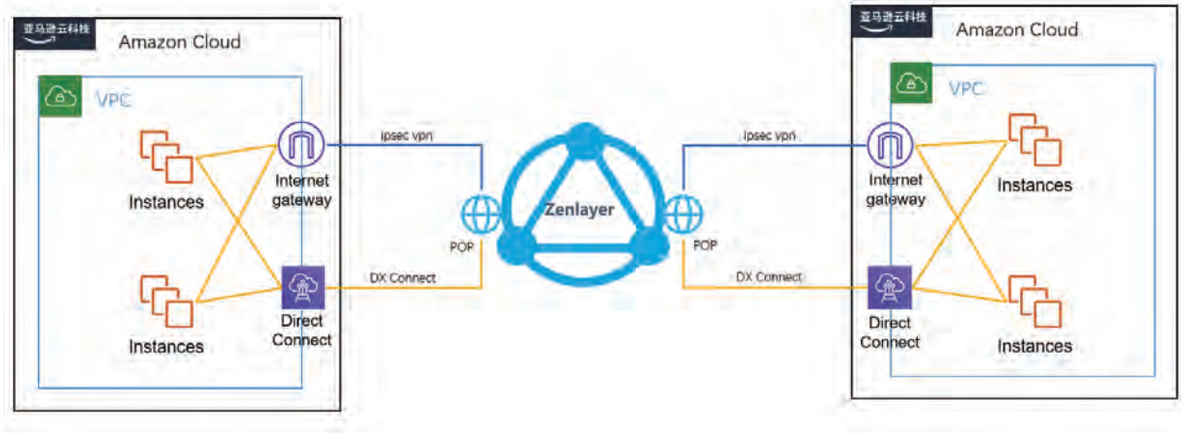
SD-WAN 设备

性价比高：支持 c5n 系列和 SR-IOV 性能优化，且 VPN 无额外授权

全球领先的 SD-WAN 能力：智能选路，应用识别，集中管理，简便易用。

缕获行业高度认可的病毒检测能力，入侵防御能力与应用识别能力保障企业全面安全

终端软件：一体化终端安全软件（可选纯 VPN 版），功能丰富，平台覆盖完善。



通过 DX Connect 打通 Zenlayer 骨干网到亚马逊云科技各个 Region 的连接通道，与亚马逊云科技全球所有 Region 全部已打通。
Zenlayer POP 支持标准 IPSec 接入，在亚马逊云科技云中安装 vpn 设备，通过 ipsec vpn 也可以连接到 Zenlayer 全球骨干网络中。
快速建立亚马逊云科技不同 Region 之间的连接，骨干全程专线，数据传输质量更稳定，屏蔽互联网连接的抖动丢包等问题。

扫一扫访问
亚马逊云科技 Marketplace
了解更多 Zenlayer 解决方案

亚马逊云科技 marketplace

数据分析

数据已成为企业的无形资产，企业需要快速存储、处理和缝隙数据，快速采取行动，有效提升业务。如何通过数据和分析解决方案获得更深入的洞察力、增强决策制定并实时采取行动，是企业用户最关注的问题。亚马逊云科技 Marketplace 为您提供众多数据解决方案，在较短的时间内收集、存储、处理和分析数据，方便有效地管理业务和数据以帮助客户构建一个完整的数据视图，充分挖掘数据的价值：利用云的可扩展性和灵活性为企业搭建现代化分析平台，帮助其快速实现业务洞察，发现数据价值。

- 提供安全地数据仓库，保障多用户访问统一数据不受影响以及数据安全与合规认证。
- 解决数据孤岛问题，统一数据口径，及时精准地通过数据定位企业管理及业务问题。

亚马逊云科技 marketplace

Tableau on Amazon Web Services

亚马逊云科技和 Tableau 共同创建了强大的云分析平台，企业可以通过亚马逊云科技 和 Tableau 产品，在企业范围内执行分析之旅，顺利完成包括数据收集、转换、存储和分析在内的各个步骤。

客户挑战

- 组织收集、存储和整理的绝对数据量持续以惊人的速度增长。虽然数据的变革潜力几乎难以限量，但绝大多数公司仍然无法充分实现其数据的价值。
- 随着越来越多的工作负载转移到云端，企业需要一个现代化的分析平台来利用云的可扩展性和灵活性，帮助其以远低于传统方法的成本更快地实现业务洞察。

客户收益

强大的分析能力

交互式的可视化分析让企业能够解决棘手的业务问题，并快速获得推动业务发展的见解。在具有专利的 VizQL 技术的支持下，Tableau 为企业提供强大的分析功能，让企业可以提出更深层次的问题，并获得更有意义的答案。

大规模的快速应用

无论是在构建工作簿和仪表盘，还是对他人发布的分析提出自己的问题，或是负责让数据成为每个人工作中更有用的一部分，Tableau 都能让企业轻松地从数据中获得价值。

适合企业的环境

企业的特定数据需求是独一无二的。因此，我们构建了具有灵活性的 Tableau，可在企业架构和数据生态系统中完美运行，不论是连接到您存储在本地或云端的数据，还是进行实时查询或使用数据提取，以及在内部或云端进行部署，完美兼容 Windows、Linux 或 macOS。

任务关键型平台

当数据对您的业务至关重要时，您的分析平台就需要做到安全、治理、可扩展和可靠。从合规性和安全性到管理和监控，Tableau 提供了一整套强大的内置功能来满足企业的业务需求。

适用场景

Tableau 平台是现代商业智能市场的首选产品。该平台之所以广为人知，就是因为它能够从几乎所有系统接收任何类型的数据，然后快速方便地将这些数据变成可指导行动的真知灼见。用户只需执行简单的拖放操作即可。无论客户处于云分析旅程中的哪个阶段，或身处世界上的哪个地点，Tableau 和 Amazon Web Services (亚马逊云科技) 都致力于在客户的云分析旅程中与他们开展合作。用户可以建立与亚马逊云科技数据源的本地连接，还可以通过经过优化的流程在 Amazon Elastic Compute Cloud (EC2) 上部署 Tableau Server，因此在亚马逊云科技上启动敏捷的端到端分析平台比以往任何时候都更加快捷。

Tableau 产品

数据的理想平台，其提供了兼具深度和广度的功能，可确保能够安心地将数据部署在整个企业中。Tableau Server 可在亚马逊云科技的云基础架构中无缝运行，确保喜欢在 Amazon Web Services 上部署应用的组织可以从 Tableau 获得完整的解决方案。

产品功能

- Tableau 和亚马逊云科技将数据可视化和云服务联合起来，致力于为企业客户打造现代云分析平台。
- 连接—— Tableau 能够直接连接 Amazon Redshift、Amazon Aurora、Amazon Athena 和 Amazon EMR 数据服务。
- 部署 —— Tableau Amazon 快速入门、参考架构和 Tableau Online 可以在几分钟内部署到任何亚马逊云科技可用区域的数千名用户。
- 规模—— 用户和连接到大型、高速和多样化的数据集，以进行交互式分析。

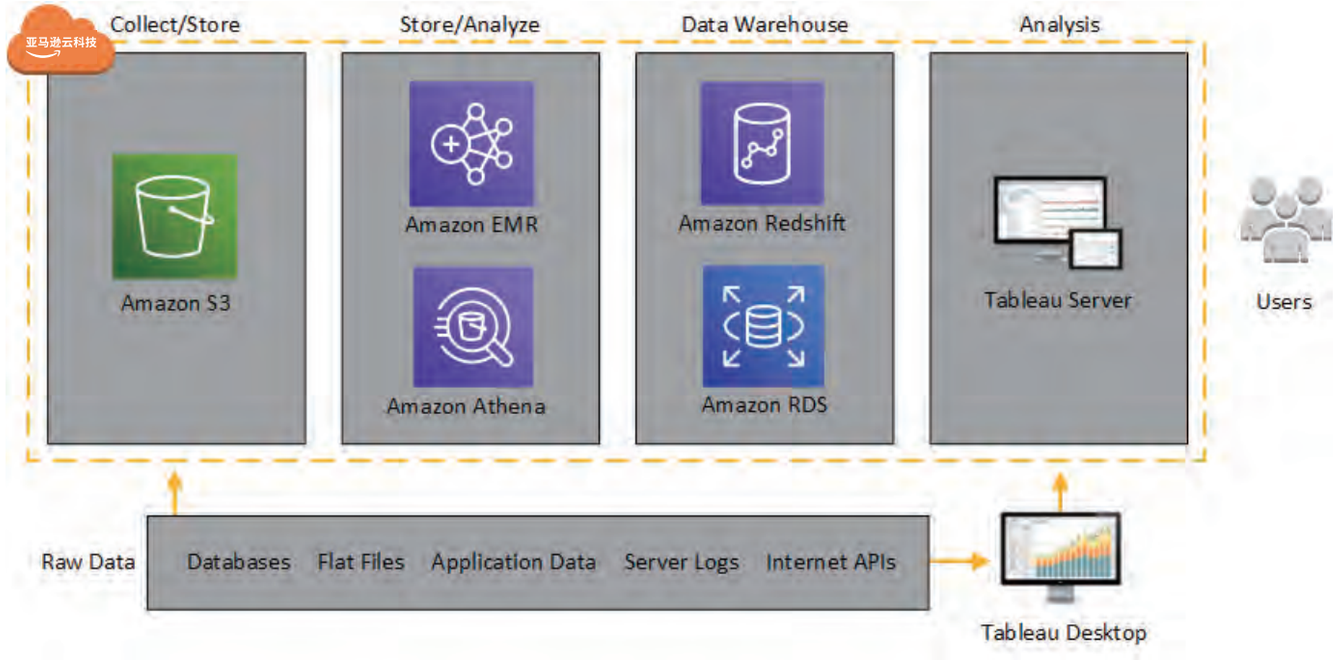
方案特点

连接存储在任意位置的数据

直接连接到企业本地和基于云的数据，或使用内存中的数据提取以优化性能。利用从 Tableau 到一系列包括 Amazon Redshift、Amazon S3（通过 Amazon Athena 或 Redshift Spectrum）、Amazon Aurora、Amazon EMR 或各种 Amazon RDS 数据库在内亚马逊云科技服务的本机连接，无需脚本或编码。

快速、安全的部署

自助部署 Tableau Server on Amazon Web Services，激活 Tableau Online 站点，使用亚马逊云科技市场，或利用 Tableau Server on Amazon 快速启动，按照 亚马逊云科技 和 Tableau Software 的最佳做法，在亚马逊云科技云上部署功能完备的 Tableau Server。只需点击几下，即可在全球任何亚马逊云科技区域启动 Tableau Server 在几分钟内实现全球化。



扫一扫访问
亚马逊云科技 Marketplace
了解更多 Tableau 解决方案

亚马逊云科技 marketplace

snowflake

数据仓库即服务

如今的数字化业务，企业的数据积累来源，大头来自于外部不断变化的数据，比如用户行为日志，点击流，移动设备，IoT 传感器设备等半结构化数据（JSON，Avro，Parque等），同时各个行业甚至国家地区对于用户隐私和数据合规监管越来越严格。用 Amazon Global region，不希望花太多精力运维，但是对于数据仓库有需求的客户。

客户挑战

大部分的数据解决方案都建立在必须雇佣专业的 admin 进行调试和维护的假设上。事实上，企业不应过多投入到自己不擅长的技术领域，而应该专心于业务上的开发以创造价值。相反，数据平台则应该尽可能多地担任自动化的角色，涵盖底层服务，面对用户提供最简单易用的功能。

基于云资源自建数据仓库，通常基于开源方案，用户负责底层资源的创建和管理，所有的配置工作，国内很多客户在 IDC 上采用这种模式，计算存储通常无法解耦，集群规模相对固定无法弹性扩展，数据安全、性能等需要额外的团队资源持续投入。

当不同的用户同时访问同一数据时，如何保证性能不受影响是并发必须解决的问题。数据要求越发实时性，安全需求更加复杂，都给数据仓库的建设提出新的挑战。数据安全对客户而言非常重要，数仓安全性，至少需要考量网络访问安全，账号和用户认证授权，对象（用户，数据库，表等）访问安全，数据安全以及合规认证。

适用场景

如今的数字化业务，企业的数据积累来源，大头来自于外部不断变化的数据，比如用户行为日志，点击流，移动设备，IoT 传感器设备等半结构化数据（JSON，Avro，Parque等），同时各个行业甚至国家地区对于用户隐私和数据合规监管越来越严格。

Snowflake 产品

Snowflake 作为一个数仓即服务的 SaaS 解决方案，本身是多租户模型，因此，第一层也是 Snowflake 公开演讲中比较复杂的 Cloud Service 一层（大脑层），包含共享的元数据管理，基础设施管理，认证和访问，事务，查询优化，安全，统计数据，监控等等模块。

Snowflake 扩展了标准的 SQL 类型来支持半结构化数据：VARIANT、ARRAY 和 OBJECT；VARIANT 可以保存任何标准的 SQL 数据类型（日期，字符串等）以及 ARRAY 和 OBJECT（Map）类型，比如类似 MongoDB 文档型对象 JSON，XML或 Avro/ORC/Parquet 等；ARRAY 和 OBJECT 是 VARIANT 的进一步具体化；底层都是一样的格式，自描述，压缩的二进制序列化，支持高效的键值查询，以及高效的数据类型测试，对比以及哈希计算。

客户收益

Snowflake 在技术架构上将存储和计算彻底分离，从本质上解决了以往架构的痛点，在性能、并发性和易用性方面都具有非常大的优势，最大化体现出了云原生架构的特点。

现代化数仓，尤其是面向云构建的数据仓库服务，更多聚焦数据生产者和消费者解耦，计算存储分离，计算资源可弹性伸缩，无限扩展不用担心容量的数据湖存储，数据安全以及较少的运维工作和整体拥有成本三层中每个组件服务都是多可用区部署，允许单个服务节点故障并自动恢复的能力。

从架构设计上来看，Snowflake 不限制用户并发数量，某一个用户可以并行跑尽可能多的查询分析任务，只需要扩展更多的 集群，或垂直提升集群计算能力；

Snowflake 以及其它云数据仓库服务都提供了访问控制（数据湖基于 Policy 最小权限设定，内置 SQL 的基于角色的访问控制等），数据加密，数据传输加密，多因素认证机制保障客户数据安全。

产品功能

开始就以 S3 为数据湖构建整个技术栈，数据存储在对象存储上，自动扩展，按实际使用付费，用户不需要担心存储扩展问题和数据持久性问题；由于采用集中的数据湖存储，也就不存在数据孤岛问题，企业数据更好的融合在一起；

计算存储分离，计算层以 Virtual Warehouse 为单位，同一份数据，不同部门和角色，根据不同的任务类型，可以用多个并行的 Virtual Warehouse 来扩展计算性能，并且该功能在高级版本中是自动实现，不需要客户管理；拉起一个新 Virtual Warehouse 集群只需要秒级的耗时；

用户不需要选择、安装和配置任何软件组件

用户不需要任何维护，集群管理和性能调优，一切交给 Snowflake 进行自动化进行

低成本，计算存储分离，计算层可以单独扩展，甚至停止，完全的云原生按使用付费

方案特点

Snowflake 解决方案具有可伸缩性、易操作、多云、多地区、易于集成、可快速启动和运行、节约成本方面的特点。

计算层（肌肉层）基本单位是 Virtual Warehouse（VW），就是一组 EC2 实例，并由独立可扩展的服务来管理（创建，销毁，按需垂直和横向扩展），用户可以在同一时间，运行多个 VM，每个独立的 VW 都可以访问所有数据，但拥有隔离的互不影响的性能；当用户没有分析任务时，可以停止所有的 VW 资源；为了满足不同工作负载对性能的要求，计算大小被标准化成 XS 到 4XL 类似 “T-Shirt” 大小的选项，独立于云平台的计算实例细节，不同的云平台采取不同的价格策略，而且不断迭代；为了降低计算节点跟对象存储之间的网络通信，每个计算节点本地 SSD 缓存部分热点表数据，比如过往查询过的 S3表文件；Snowflake 团队称他们的架构为 “多集群，共享数据架构“。

共享的、无限的数据湖存储意味着用户可以共享和集成所有数据，同时不同用户可以拥有相互独立的 私有计算资源 避免各团队之间不同工作负载的相互影响；比如定期拉起按需的 VW 集群用来处理大批量数据加载，同时不同的组织部门拥有多个 VW 集群用来处理查询分析任务；

VW 集群中的每个工作节点都在本地磁盘上维护一个热点数据的缓存，缓存的内容是该节点上执行过的查询所访问的 S3 表文件数据

Snowflake 还支持在线升级，正常一周一次；无论是 Cloud Service（大脑层）还是 VW（肌肉层）服务都被设计成允许多个版本同时在线；所有的状态数据（元数据）都利用事务特性的 K-V存储保障一致性，当团队需要更新元数据 Schema 的时候，必须保证向后兼容历史版本；其它服务组件都是无状态服务；如果服务需要升级，团队会先部署一个新版本，同时保留旧版本，用户所有新查询都会落在新版本服务上，并允许旧版本上的查询继续执行完成，一旦旧版本服务上所有查询都执行完成，该服务就会被销毁（类似蓝绿方式进行在线升级）。

扫一扫访问
亚马逊云科技 Marketplace
了解更多 Snowflake 解决方案

亚马逊云科技 marketplace

神策数据
SENSORS Data

神策数据数字化运营闭环解决方案

神策数据是国内专业的大数据分析和营销科技服务提供商，为企业提供神策营销云、神策分析云、神策数据根基平台三大产品方案通过全渠道的数据采集与全域用户 ID 打通，全场景多维度数据分析，全通道的精准用户触达，帮助企业实现数字化经营。

客户挑战

- 数字化转型无落地方案；
- 用户标签画像创建和管理成本高且维度少
- 用户行为数据缺乏，难以形成有效的用户感知，运营策划多半靠空想只能“参考竞品”或拍脑袋决定
- 不知业务流程真实现状的切入点选择与决策制定， 导致策略决定一错再错
- 运营策略落地像一场漫长的战役，必须“协同八方”才能落地一个简单的策略，运营效率极低
- 活动上线后数据反馈滞后，深度下钻的分析需求难实现，无法形成效果评估后迭代策略质量的运营闭环
- 自建试错、升级、优化、维护等成本高

客户收益

活跃用户数提升，突破流量增长制约，重新定义增长曲线

拒绝盲目砸钱，精准获客；找准时机刺激价值转化，持续跟进新用户落地体验，推动产品面向新用户激活场景的迭代优化；在用户全生命周期各个环节埋下运营伏笔，化被动为主动，增强存量用户依赖

营收/收益增长

让更多用户付钱：找到合适的商业变现点，优化流程与匹配效率。让付费用户享受舒适的权益体验，从此付费转化成自然

让用户付更多钱：拉长用户生命周期、自动化运营培育，提升用户对平台的黏性和复购习惯，实现 ARPU 自增长

适用场景

- 数字化转型，私域流量运营
- 线上+线下业务数据资产采集
- 全域客户数字资产 oneID 打通
- 统一客户数据视图
- 广告投放&引流数据监测
- 消费者消费旅程及转化监控
- 用户标签分群支撑实现精准营销
- 全平台数据中台建设
- 自动化智能化营销平台建设

神策产品

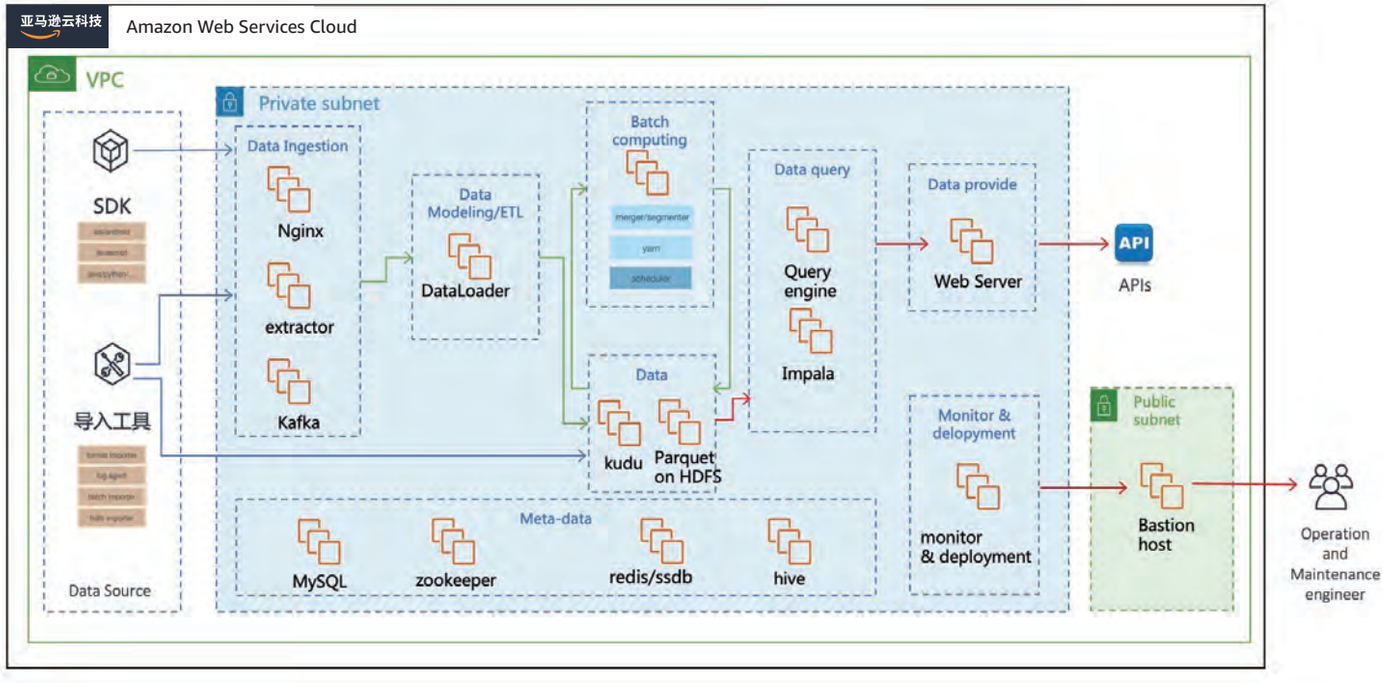
神策数据立足大数据及用户行为分析的技术与实践前沿，提出基于数据流的企业运营框架——SDAF，即 Sense（感知）、Decision（决策）、Action（行动）、Feedback（反馈）的数据闭环，并致力为客户打造基于 SDAF 运营框架的数据闭环。业务现已覆盖以互联网、品牌零售、金融、融合媒体、企业服务、高科技、汽车、互联网+ 等为代表的 30 多个主要行业，并可支持企业多个职能部门，目前已服务付费客户 1500 余家。公司总部在北京，并在上海、深圳、合肥、武汉成都、西安、中国台北等地均拥有本地化的服务团队，覆盖全国及东南亚市场，同时，公司拥有专业的服务团队，为客户提供与营销和大数据相关的咨询、解决方案和专业服务。

产品功能

- 数据驱动闭环：基于数据采集与整合，一站式实现看数据、分析数据、业务干预、效果评估的完整闭环，真正实现数据驱动业务迭代和增长
- 业务赋能　敏捷迭代：可视化操作与管理，实时、自助的数据洞察和业务验证，跨越数据与业务的鸿沟，释放业务生产力和想象力，提高运营效率
- 全渠道触达与管理：支持微信、企微、短信、Push　等全运营场景，兼备强大的渠道对接与策略规则引擎配置能力，让全渠道触达与多触点运营成为现实
- 可私有部署　PaaS　平台：基于成熟的平台化产品，具备完善的私有化部署方案及权限管理体系，交付快、质量高，快速满足业务应用诉求

方案特点

- 完整数字化运营平台闭环能力实施验证
- 标准产品实现批量化交付，支持客户依据实际业务逻辑和使用习惯进行个性化配置
- 成熟的私有化部署方案，可实现天级别部署
- 各行业 TOP 级企业合作经验，独立行业化体系服务，实施咨询能力丰富，赋能式实施服务



扫一扫访问
亚马逊云科技 Marketplace
了解更多神策数据解决方案

亚马逊云科技 marketplace

帆软 让数据成为生产力

企业级 BI 解决方案

为企业发展的不同阶段提供一站式大数据 BI 解决方案

客户挑战

- 企业数据分析过程中，各业务系统数据隔离，存在数据孤岛。
- 手工处理导致了数据时效性差、数据口径不一致、分析方式单一、数据安全难以管控等问题。
- 无法及时、精准的通过数据定位到企业管理问题。

客户收益

- 数据统一：数据统一分析、管理效果显著，节约大量的数据处理时间
- 效率提升：解决原有系统数据时效性和准确性问题
- 自助分析：用户探索式分析，实现数据驱动业务发展的方向

方案特点

- 多系统关联分析能力：打通多个业务系统数据，完成手工报表到自动化报表的建设；通过 FineReport 高度自定义的能力，实现线下报表线上化的场景功能全覆盖；
- 敏捷的分析能力：IT 配置化开发+业务自助性分析组合统一的数据分析平台，助力企业快速提升分析效率，随时随地多终端查看企业运营数据，辅助决策。
- 强大的性能支撑：通过 FineBI 的强大性能支撑能力和数据管理策略，服务业务多场景分析需求，降低数据分析门槛，提升用户体验和业务支撑性；
- 高度开放性：支持基于企业业务实际需求的定制化能力，支持从前端展现到后台功能的自定义开发功能，满足各类定制化场景。

适用场景

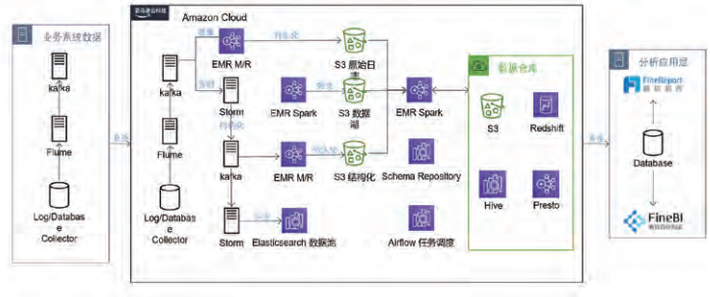
企业中的数据部在做的事情，都是加工数据，让数据转变成信息；加工信息，让信息转变成知识；利用知识，撬动变现的杠杆。在目前的信息时代，借助类似于 FineBI 的这些工具，可以让企业加速融入企业数据分析的趋势。

帆软产品

- 报表自动化：通过 FineReport 设计器完成报表自动化输出设计，解决手工报表时效问题、解放50%以上的人工生产力。
- 分析可视化：通过多种类可视化图表，提高数据的查看便捷性。实现可视化看板、大屏展示场景。
- 分析数据完整性：通过数据补录离线数据，线下目标与线上业务发生过程的数据结合，实现 KPI 式管理；
- 业务自助化：通过 FineBI 实现 IT 向业务的数字化赋能，实现业务人员灵活分析。

产品功能

- 报表自动化：通过 FineReport 设计器完成报表自动化输出设计，解决手工报表时效问题、解放50%以上的人工生产力。
- 分析可视化：通过多种类可视化图表，提高数据的查看便捷性。实现可视化看板、大屏展示场景。
- 分析数据完整性：通过数据补录离线数据，线下目标与线上业务发生过程的数据结合，实现 KPI 式管理；
- 业务自助化：通过 FineBI 实现 IT 向业务的数字化赋能，实现业务人员灵活分析。



扫一扫访问
亚马逊云科技 Marketplace
了解更多帆软解决方案

亚马逊云科技 marketplace

DevOps

在开发和运维的不同生命周期，开发者需要持续提升应用程序和基础架构的可靠性，使用以云为中心的 DevOps 技术和工具，为有效的端到端服务所有权积累知识和技能帮助企业以更敏捷的方法突破原有性能，提升云基础设施的使用效率：

- 降低成本，实现云计算资源按需获取，具备弹性伸缩特点，使资源合理。
- 通过机器学习技术将复杂的工具以及多维度数据进行汇总分析。
- 提升用户体验，加速企业数字化转型，快速优质地发布软件，为客户提供最佳数字体验。

亚马逊云科技 marketplace

splunk>

Splunk Enterprise

Splunk Enterprise 是从机器数据中汇总、分析和获取企业运营答案的最快方法。通过挖掘机器数据的价值，帮助用户提高企业生产力、企业网络安全性、业务盈利能力和竞争力所需的实时洞察力。

Splunk 产品

相对于其他开源技术或单一应用领域的产品，Splunk 对于大中型企业提供了一站式的机器数据采集分析解决方案。基于下列优势，Splunk 是旨在应对所有数据挑战并帮助组织将基于数据的决策和行动带到一切事务的唯一解决方案。

客户挑战

- 企业利用机器数据的挑战首先在于它们的格式五花八门，难以预测，且传统的监测和分析工具难以有效应对此类数据的种类、速度、数量或多变性。
- 对于机器数据的利用，不仅包括调查和监控，还有分析和行动。几乎每个数据问题都需要这些技能的结合，如今大多数公司拥有多个工具，在整个组织中独立运行。
- 安全数据工具与 IT 相分离。在每个部门中，会发现针对特定用例的特定工具，每个工具看起来都是完成这项工作的最佳选择，但它们的单独使用无法发挥四项技能的合力。

客户收益

世界各地的客户通过 Splunk 产生的价值：

- 调查事故的速度提高了90%；
- 开发报告、表盘和应用程序的速度提高了90%；
- 减少高达82%的业务影响；
- 将数据泄露、ID 盗窃和欺诈的风险降低50%；
- 缩短了50%的上市时间。

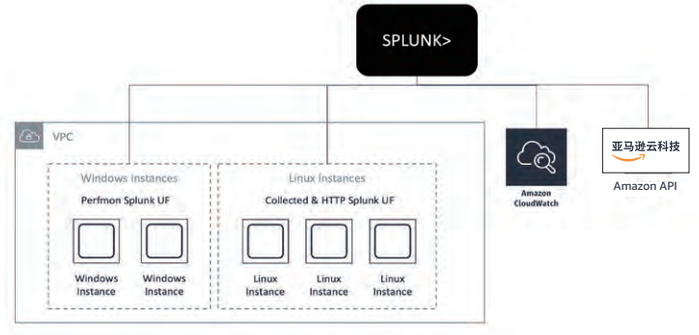
扫一扫访问
亚马逊云科技 Marketplace
了解更多 Splunk 解决方案

产品功能

- 精准洞察数据：将机器运营数据分析转化为答案，实现实时洞察，以提升业务成果；
- 实时可见性：实现对企业运营至关重要的实时机器数据的收集、索引和警报的自动化系统；
- 深入您的数据：从所有数据可视化分析结果中发现可操作的企业运营见解，无论是结构化或非结构化；
- 可操作的情报：通过机器学习提供人工智能分析运营数据，以做出更快更明智的决策。

方案特点

- 实时收集和索引任何来源、任何位置、任何类型的机器数据，并将其转换为一系列事件，您可以立即查看和搜索这些事件。
- 独特的读时建模技术，无需在数据收集阶段考虑数据的结构，而只需在数据搜索使用时按需建模。
- 强大的搜索处理语言（ SPL ）提供高度灵活的搜索过滤条件，内置数百个查询指令和函数，并且搜索结果可直接进行可视化展现，以报表和仪表板的形式呈现。
- 使用 Splunk Enterprise 可以关联跨数据源的复杂事件，关联类型包括基于时间的关联，基于事务的关联以及子查询、查找表、Join 等。
- Splunk Enterprise 的高度可扩展性支持收集和索引每天数十 TB 的数据，并且原生的集群技术为关键数据提供高可用性支持。
- 集成机器学习技术，集成的工具和命令由开源算法支持，可以收集、清理、可视化分析和发布数据洞察。



Appdynamics 提供全面的性能可视化分析能力

Appdynamics 从应用到基础架构全栈应用性能监控解决能力，帮助 亚马逊云科技客户加快云迁移的速度和质量，保证运行在亚马逊云科技云上的应用保持企业级的端到端性能，比较和验证云迁移前后的从客户到业务的优化。

适用场景

亚马逊云科技作为全球第一的公有云服务提供商，提供从云基础架构到原生云应用的体系化云解决产品和方案。亚马逊云科技云基础架构和应用微服务为企业 IT 带来新的灵活性和优势的同时，也带来了新的架构复杂性和管理挑战。在客户向亚马逊云科技云做迁移的过程中，如何保证客户应用的持续优化，是决定迁移成功的关键。市场调查结果表明，应用性能可视化已经成为客户对云迁移的主要顾虑，仅次于对安全和合规的顾虑。

客户挑战

- 缺乏混合云环境下的无缝监控视图，全面的理解和掌握应用的端到端的整体性能视图，以及下钻到局部查看细节的能力。
- 缺乏客户体验、业务、应用和基础架构的关联影响分析。无法根据业务和客户体验的变化趋势，作出优化的资源调度决策，提高防患未然的运维能力。
- 缺乏 DevOps 统一视图，无法满足在云环境下开发和运维之间的协同效率，不能保证应用的快速交付和高性能。

思科产品

思科的 Appdynamics 在复杂的混合云环境中为客户提供如下能力：

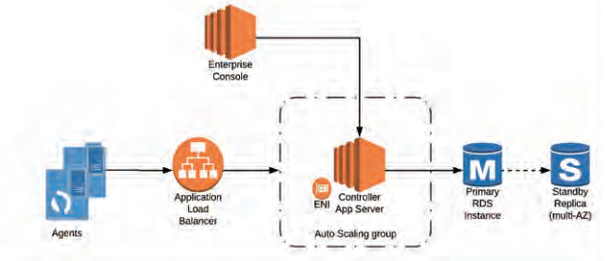
- 掌握从客户前端到服务器后端的业务交易执行路径中的关键节点的性能和状态，统一监控不同类型的应用组件（客户体验，应用，数据库，网络）的资源使用和性能。对应用组件性能对异常变化可以快速发现，快速定位。全面的理解和掌握应用的端到端的整体性能视图，以及下钻到局部查看细节的能力。
- 关注客户体验，从业务的角度了解用户执行业务交易时的实际性能体验自动发现关键的业务交易的可用性和性能
- 主动运维，实时掌握应用组件的资源使用和性能，并对标到业务和客户体验的变化趋势，自动作出最优化的资源调度决策，提高防患未然的运维能力。提高应用性能和客户体验，保证业务稳定和增长。

产品功能

Appdynamics 从应用到基础架构全栈应用性能监控解决能力，帮助亚马逊云科技客户加快云迁移的速度和质量，保证运行在亚马逊云科技云上的应用保持企业级的端到端性能，比较和验证云迁移前后的从客户到业务的优化。

- 在复杂的混合云架构中确保性能无论环境如何（传统，混合或本地云），都可以进行一致的端到端应用程序监视，自动发现跨云的应用拓扑和追踪交易全流程，对不同客户端、应用语言、基础架构、云架构都能保持相同的监控深度和可视化分析能力，提高管理人员的效率。有能力快速发现性能问题，避免影响业务和客户。
- 快速适应云原生的应用架构，隔离亚马逊云科技上不同的原生的应用架构，包括 Amazon EC2, Amazon ECS, Amazon EKS, Amazon Fargate and Amazon Lambda 提供一致的应用监控能力和界面。无缝地监控大规模的微服务和无服务器服务应用架构。通过基线分析和智能根因分析，快速定位微服务和容器环境里的性能瓶颈。
- 业务影响分析，把客户体验，业务产出和应用性能关联起来，打通 IT 部门和业务部门之间的隔断，IT 的优化目标和业务的目标联动起来保障业务的持续成功和优化。

在全球 Appdynamics 提供 SaaS 和数据中心本地部署。在中国，Appdynamiacs 支持本地部署和 Amazon PasS



扫一扫访问
亚马逊云科技 Marketplace
了解更多 Cisco 解决方案

亚马逊云科技 marketplace

dynatrace

面向未来应用的云原生监测

Dynatrace 不仅仅是应用程序性能监控（APM）解决方案，更是一个提供软件智能的平台。可在整个数字生态系统中为企业提供可见性，并提供由 AI 支持的答案，包括用户的数字体验、数字业务分析、应用程序和基础架构的性能以及 IT 运营（AIOps）。帮助企业提升 IT 运营效率，实现数字化转型，并提升业务绩效。

适用场景

- 应用程序性能监控：Dynatrace 为跨复杂企业云环境的应用程序提供自动化的代码级可见性和根本原因答案。
- 基础设施监控：Dynatrace 提供简化的自动化基础架构监控，可在主机、VM、容器、网络、事件和日志之间提供广泛的可见性。
- AIOps：Dynatrace 实时收集高保真数据并映射依赖关系，以便 Dynatrace 可解释的 AI 引擎 Davis? 能够显示问题或异常的确切根本原因，从而实现快速自动修复和智能云编排。
- 数字体验管理（DEM）：Dynatrace DEM 为每位客户的旅程提供真实用户监控（RUM），跨全球网络进行综合监控，以及 4K 类似电影的会话重播。
- 数字业务分析：通过将业务指标和 KPI 与已经被我们监控的应用程序性能和数字体验模块的数据绑定，实时获得由 AI 支持的关键业务问题的答案。

Dynatrace 产品

- 软件智能监控平台，可简化企业云复杂性并加速数字化转型。借助 Davis（Dynatrace AI 因果关系引擎）和完整的自动化功能，Dynatrace 一体化平台提供有关应用程序性能、底层基础架构和最终用户体验的答案，而不仅仅是数据。
- Dynatrace 用于实现企业云运营的现代化和自动化，更快地发布更高质量的软件，并为您的组织客户提供最佳的数字体验。Dynatrace 将基础设施和云，应用程序性能和数字体验监控无缝集成到由人工智能提供支持的一体化自动化解决方案中。Dynatrace 通过为开发，运营和业务团队提供共享的平台、指标来协助提高业务绩效。

客户挑战

IT 专业人员需要为用户提供完美的用户体验，对软件的监控和可观察项面临着5大挑战：

- 由于软件驱动的不仅仅是应用程序，因此有更多的失败可能性和更多的问题隐藏点。
- 容器和微服务的爆炸式增长。传统工具根本无法在微服务的复杂生态系统中工作。数字中断不仅比以前更昂贵，而且还会导致更多的问题。
- Web 规模。今天的环境可能跨越多个 Amazon zone，这使得寻找问题的根源比以往任何时候都更加困难，超出了人类可能的范围。

  企业在采用 DevOps 的情况下，更改的频率和速度使得监控非常难以保持最新。
- 尽管用户体验的重要性似乎显而易见，但事实是大多数组织都是盲目的。组织的可观察性工具和实践完全忽略了最终用户，并且没有将应用程序和基础设施性能放在业务结果的上下文中。

客户收益

弹性运维

减少停机时间、问题减少、MTTI 减少、战争会议室每次事件时间减少、IT 运营识别问题速度比传统 APM 快75%.(Forrester研究)

员工工作效率

更少的性能事件和更快的处理故障，安装和升级节省大量时间；

节约成本

有单个平台取代过个工具；与自己制定解决方案相比，实施 Dynatrace 更快、更便宜；与其它解决方案相比，Dynatrace 所需的硬件更少；企业使用 Dynatrace 更自信的加速云迁移，从而为基础设施运营节约成本，更快实现价值；

业务敏捷性

开发为市场提供服务的速度提升；提高内部和外部用户满意度；部署 Dynatrace，新项目提前得到业务成果；放弃率减少，转换率提高。

产品功能

真实用户监控

真实用户监控分析所有用户与应用程序交互的性能，无论交互是在浏览器中还是在移动设备上进行。支持应用程序可用性监控、验证 UI 元素的正确显示、第三方内容提供商性能分析、后端服务性能分析（下到代码级别）以及所有基础结构的性能分析。

移动用户监控

监控本机移动应用的用户体验的过程与监控基于浏览器的 Web 应用程序有着根本的不同。移动应用程序监视涉及到一个监视库和您自己的移动应用程序包的编译、打包和发送。Dynatrace 支持 Android 和 iOS 平台。

服务端服务监控

Web 应用程序由 Web 服务器（例如 Apache Tomcat）和 Web 容器（例如 ,Docker）提供服务的网页组成。Dynatrace OneAgent 可以提供有关哪些应用程序或服务与哪些其他服务交互以及特定服务调用哪些服务或数据库的详细信息。

网络、进程和主机监控

Dynatrace 能够监视您的整个基础设施，包括您的主机、进程和网络。提供详细的拓扑信息，以便哪些进程在哪些主机上运行，以及进程是如何相互关联的。

云和虚拟化监控

Dynatrace OneAgent 监视整个堆栈，包括私有，公共和混合云环境。可以与虚拟化基础架构集成，从而可以从数据中心 vCenter，以及其上的虚拟机、进程、服务、应用纵向堆栈关联起来。

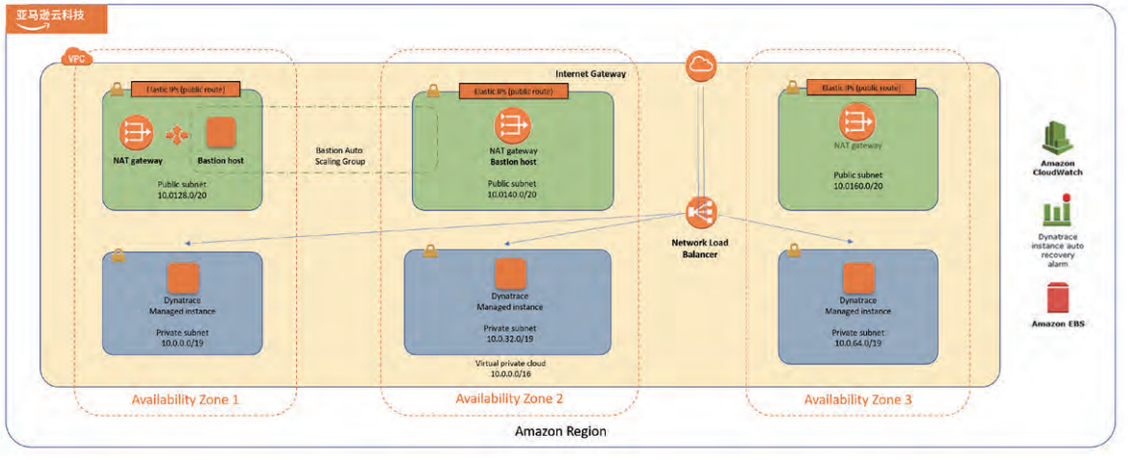
容器监控

Dynatrace 与现有 Docker 环境无缝集成，并自动监视您的容器化应用程序和服务。Dynatrace 挂接到容器中，并自动深度监控容器内的应用程序和服务，甚至到代码级。

方案特点

与其他监控工具相比，Dynatrace 的方法截然不同。以下是四个关键区别：

- 自动：从部署到检测、发现、依赖项映射、基线、问题识别和根本原因，Dynatrace 是完全自动的。只需在主机上安装 Dynatrace OneAgent 即可。
- 完整堆栈：Dynatrace 提供了上下文。这包括从上到下，从最终用户体验到基础结构，了解和映射所有关系和相互依赖性。
- AI 在核心：虽然其他解决方案已经"启动"机器学习，以减少警报噪音，但 Davis AI 引擎是平台的核心，在几毫秒内处理数十亿个依赖项，提供远远超出人类能力的精确答案。
- Web 级规模：Dynatrace 软件智能平台采用云原生架构构建，可无限制地扩展。Dynatrace 面向大型全球团队提供基于角色的治理、跨基础架构、云平台和应用程序的自动化企业部署和全堆栈覆盖，专为要求最苛刻的企业云环境而设计。



扫一扫访问
亚马逊云科技 Marketplace
了解更多 Dynatrace 解决方案

亚马逊云科技 marketplace

SpotMax

云成本优化综合解决方案

SpotMax 提供一套云成本优化的综合解决方案，帮助企业提升云基础设施的使用效率，节省多至90%的用云成本。

适用场景

从全球化大型企业到快速发展的初创企业，SpotMax 都可以帮助客户有效降低用云成本。对于拥有大量用户请求、需要快速响应、与用户体验极为相关的场景，以及希望解决流量快速变化带来的用云成本不稳定的问题，SpotMax 的作用更为突出，例如广告技术、电子商务、社交媒体、游戏、高性能计算等行业。

客户挑战

- 业务架构与云计算基础设施不匹配：无法真正实现云计算资源的按需获取，导致资源浪费；
- 不能充分使用 Spot 实例：由于担心稳定性受到影响，没有大规模应用 Spot 实例。

方案特点

- 能够在预测资源紧张时通过兼容机型或按需实例进行集群容量预补偿，并在 Spot 资源恢复时及时换回这些替代者；
- 能够与常见的负载均衡及服务发现机制协同工作；
- 可以与容器编排平台（Kubernetes）协调，实现 Pod 的无缝迁移；
- 利用大数据及机器学习技术对不同类型实例的回收率进行预估，并以此持续优化集群构成，大大降低集群实例中断的发生；
- 通过实时学习预测大规模中断，预先替换包括按需实例在内的稳定型实例，提前获取将有效避免资源紧缺时的无法补偿。

扫一扫访问
亚马逊云科技 Marketplace
了解更多 SpotMax 解决方案

SpotMax 产品

- MaxChaos：利用混沌工程有效评估系统容错能力，持续提高可用性及弹性；
- MaxArch：构建“云原生”架构，适应云基础设施弹性伸缩的特点，更好使用高性价比弹性资源；
- MaxGroup：智能弹性集群管理，提升 Spot 实例集群的可用性和效率降低云成本。

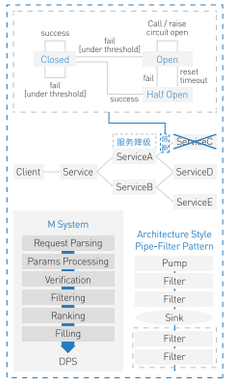
产品功能

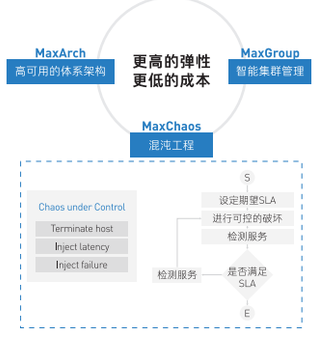
极致的云成本节省：

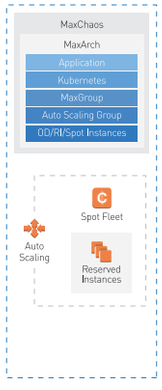
- 保证稳定性：动态调整高性价比可用资源，持续优化集群构成，使“省钱”与“稳定”二者兼得；
- 本地化支持：提供全方位的本地化技术支持和培训，无缝对接；
- 操作简单：开箱即用，易于操作；
- 适用范围广：通过云原生技术和最佳实践，根据实际情况进行 server 或 serverless 全球化部署。

客户收益

- 优化后的架构更适应云基础设施弹性伸缩的特点，从而提升云使用效率，充分享受云计算按需使用的优势；
- 通过全局历史数据和本地线上数据综合分析，在保证稳定性的同时，充分使用价格最优惠的 Spot 实例，极大节省了用云成本。







亚马逊云科技 marketplace

容灾备份

随着云端功能的不断强化，企业正将越来越多的数据和工作负载迁移到云端，保护数据不止要时刻防范风险，更要借助 IT 资源优化方案，提供数据备份等服务。亚马逊云科技合作伙伴通过不断技术构建，为客户提供一键式灾难恢复功能，确保正确高效还原数据库，为客户打破数据边界，应对云上数据挑战：

- 数据实时上云，帮助用户灵活管理混合云灾备，满足用户复杂场景才的混合云灾备需求。
- 减少迁移时间，利用广泛兼容性，解决本地与云端的链接及异构平台风险，缩短停机时间降低风险。
- 为企业提供颗粒度为微秒级的数据恢复，减少用户因数据丢失而造成的业务中断和经济损失。
- 轻松实现异地备份，灵活按需灾备演练。

亚马逊云科技 marketplace

COMMVAULT®

备份及存储解决方案

针对日益复杂、爆炸式增长的数据进行不同安全级别的数据保护帮助企业提供自动化的数据上云、云中备份、多云管理、云上云下数据迁移等能力，最大限度的降低数据管理成本、加速企业上云和保护云中数据资产。

适用场景

数据作为企业的重要资产，其重要性与日俱增。但是人为误操作、恶意删除、软硬件故障、勒索病毒以及自然灾难等诸多因素，均有可能造成业务数据的丢失，从而造成无法估量的损失。所以，建立一个完善的多云统一管理的备份和灾备系统便成了必然的选择。且客户自己建设和管理灾备中心成本很高，可以借助于云存储降低灾备投资和运维成本，并有效防止数据丢失。

客户收益

统一管理云上、云下数据，实现数据可视化，降低成本并提高管理效率

Commvault 解决方案能覆盖各种主流数据库、文件、虚拟化和云平台，实现云上、云下及多云环境的统一数据管理，降低管理成本和提高效率。

提高数据安全性，有效防范各种数据丢失风险和威胁

借助与亚马逊云科技的云资源整合，有效防范勒索病毒攻击和数据破坏并可以防止本地数据中心灾难造成的数据失效和业务宕机。

降低本地数据存储和管理成本

利用亚马逊云科技的云存储资源存储较少访问或需要长期合规保留的历史数据，有效降低本地存储和运维管理成本，并借助云资源的弹性扩展提升了业务扩展能力。

提高数据利用和管理效率，激活数据

与亚马逊云科技的云存储资源和云计算资源整合，方便为业务部门快速提供业务数据，满足数据分析，报表展现，研发测试等场景以及快速交付生产数据的需求。

客户挑战

企业数字化转型以及云计算的加速落地对用户基础架构和应用带来了前所未有的挑战，组织需要采用新的商业模式和新的体系架构来解决新的问题。Commvault 创新的数据管理解决方案，将能有效帮助用户保护并管理本地数据中心以及云环境中的数据。

- 线下数据备份、归档、复制到亚马逊云科技：将本地中心需要保护的数据直接写入外部的云存储中（D2C）；或者先把数据备份/归档在本地存储，再将本地副本复制到外部云存储中（D2D2C）。这种情况都适合短期和长期保留配置。
- 亚马逊云科技中应用数据备份：在公有云环境中提供保护及恢复工作负载及数据，把本地数据中心和公有云结合起来，实现集中数据保护及恢复。
- 数据中心应用容灾或迁移到亚马逊云科技：把本地应用恢复或迁移到云中心，当把本地应用数据备份到云中心后，如果本地出现灾难，可以利用云中心的备份数据和云中的虚拟机恢复应用。

Commvault 产品

Commvault 是一家全球技术领先的数据保护及信息管理解决方案供应商，旨在帮助全球各地的用户管理并应用数据，以增加数据的价值和商业洞察力。Commvault 直接或通过一个覆盖全球的合作伙伴及服务提供商网络为广大用户提供其解决方案和服务。Commvault 的解决方案涵盖一系列数据管理功能：数据保护及恢复、虚拟化和云平台保护及恢复、灾难恢复、数据归档、信息检索、文件同步及共享。作为独立、值得信赖的行业专家， Commvault 凭借其技术愿景、创新精神和执行力赢得了广大客户和第三方的赞誉。Commvault 专注数据管理平台的研发及推广，并吸引了各行各业、各种规模的企业的信赖，其解决方案被广泛部署在数据中心、移动平台和云平台上，并为用户提供一站式服务。

产品功能

全面的数据保护能力

数据保护方案全面支持多数据中心和多云环境的统一数据管理：包括物理服务器和虚拟机、数据库和应用、NAS 系统、私有云、公有云、混合云、个人终端数据及移动设备。

多种数据保护方式

能采用多种方式进行数据保护，包括：备份、归档、快照、复制及数据副本管理（CDM）。满足防止物理错误、防止逻辑错误、数据长期保留、灾难恢复多种需求，单一操作界面和平台满足企业客户对数据保护的各种的 SLA、RPO 和 RTO 要求。

灵活的数据恢复选项

对保护的数据能提供多种灵活的恢复选项：完全恢复、小颗粒蛋卷、单文件或单表恢复、应用时间点恢复、异机恢复、跨虚拟化或云平台恢复、灾难恢复、直接访问保护数据等等。

简便的管理操作

利用单一控制台实现全中文操作和管理，包括备份策略制定、软件安装和更新、统一报告和告警监控、统一浏览和恢复、集中许可管理、备份存储配置和监控等等。

高效的存储管理

透明的使用磁盘、磁带、云存储以及超融合，数据能在各种介质间进行转换并内置纯软件重复数据删除功能，极大节省了存储空间，简化管理操作，简化灾难备份管理。

智能快照管理

与业界所有主流存储设备集成，调用存储快照接口进行快照管理，自动创建具有应用感知的硬件快照，实现快速数据保护并确保应用数据一致性。

全面的虚拟化和云数据管理

对业界所有主流的虚拟化环境、私有云、公有云及混合云的数据进行保护，直接调用虚拟化或云平台数据保护接口或协议实现数据保护，效率高，操作简便，提供多种数据保护方式：即时复制、快照、备份及归档等等。并提供多种灵活的恢复和迁移策略，比如将本地数据中心的 VMware 或 Hyper-v 的虚拟机自动恢复或迁移到 Amazon EC2，将本地 SQL 或 Oracle 数据库迁移到 Amazon EC2 或 RDS；也能够将亚马逊云科技中的 EC2 或 RDS 数据库备份后恢复到本地数据中心或 MS Azure 的 VM 或数据库环境。实现云上、云下的统一数据调度和集中数据管理。

严格的安全管理

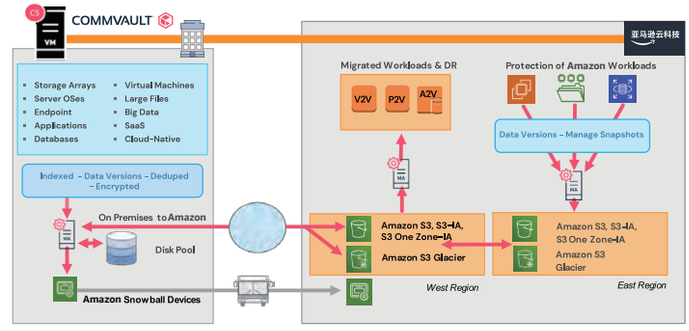
基于角色的功能权限管理，并能与 AD 相结合，支持多种数据加密算法，支持多种防火墙模式，内置勒索病毒检测和防护、确保数据安全。

基于策略的自动化

通过策略制定或工作流的编写，对数据保护、灾难备份、数据校验、恢复演练、灾难恢复等操作实现自动化，极大提高管理效率，降低劳动强度。

方案特点

- 一体化数据管理平台完成不同服务级别数据的复制、备份、快照、归档、容灾和数据副本管理（CDM）；
- 数据保护平台借助亚马逊云科技服务可以通过广域网对企业多分支机构、多云环境进行数据保护、应用迁移和管理；
- 针对勒索病毒等攻击提供有效的自动检测和数据安全防护，确保企业数据资产安全可靠；
- 基于角色管理 的权限模式和可扩展的功能模块，可以轻松帮企业实现数据保护服务化；
- 可以通过平台自带的流程编辑器流程化数据保护、恢复、数据验证、容灾演练等业务，确保数据高可靠；
- 可以对备份数据进行激活使用和快速交付。



扫一扫访问
亚马逊云科技 Marketplace了
解更多 Commvault 解决方案

亚马逊云科技 marketplace

VERITAS
云数据保护解决方案

数字化转型是新时代下企业CIO/CEO所最为关注的IT发展趋势。公有云平台提供的基于大数据、人工智能、物联网等创新能力为数字化转型提供核心支撑。企业为获取相应能力，纷纷打破传统数据边界，在公有云上部署业务和数据。

客户挑战

在平台云化的各个阶段中，从数据和业务的管理角度来看，还是依然有不少挑战的，整个业务都放在云上，那云上的数据怎么管理?要不要备份，怎么备?要不要拿到本地，又怎么拿?对带宽有没有要求，对我们业务的访问有没有影响。

还有，现有数据中心的业务向云上迁移过程中，如何考虑迁移路径，如何衡量迁移的业务逻辑关系，如何让整个 IT 的传统业务，在业务较小感知的情况下，甚至于说是零感知的情况下，迁移到云环境中去。

最后，当整个云上的架构完整，各业务板块以及企业系统都在云上，数据中心如果有部分经过评估后保留的业务，那这两者之间的业务以及数据是否能够统一管理?毕竟对 IT 管理团队而言，是不希望有两套不同的管理体系，也不希望看到两边的数据被割裂，更不愿意看到的是没有手段了解我们现有数据在各平台，各存放空间的使用和存放情况，需要一张完整的视图，确认我们那些数据在具体的什么地方，由谁使用，是属于哪个系统，它的冗余数据在哪儿；那些业务目前又是跑在什么地方，是否有合理的可靠性 plan 等等。有了这些信息，会极大的帮助我们减少管理的复杂性。

适用场景

对于如今的数据驱动型企业而言，仅仅“够好”还远远不够。随着云端功能的不断强化，企业正将越来越多的数据和工作负载迁移到云端，充分利用云托管解决方案的优势。这使得全方位数据管理和保护变得比以往任何时候都更为重要。云的各个发展阶段互不相同，不过 Veritas 能将所有阶段贯穿起来。这是因为我们关注的是您的信息，而非存储位置。云体系结构并非坏事。IDC 最近的一篇报告指出，85% 的企业 IT 部门致力于实现云体系结构。

Veritas 产品

数字化转型是新时代下企业 CIO/CEO 所最为关注的IT发展趋势。公有云平台提供的基于大数据、人工智能、物联网等创新能力为数字化转型提供核心支撑。企业为获取相应能力，纷纷打破传统数据边界，在公有云上部署业务和数据。

Veritas 帮助企业由传统数据中心向公有云的转型的主要途径包括：

- 通过本地虚拟化改造并维持混合云环境；
- 逐步向云迁移，或采取混合云容灾模式；
- 在云上构建全新的应用。无论采取何种模式，Veritas 都可在亚马逊云科技的云上提供服务。

产品功能

解决客户的重大数据保护难题为使命：

- 勒索软件：保护企业远离这类以加密或锁定重要数字文件为手段来勒索企业赎金的恶意软件。
- 现代化的工作负载：支持 Nutanix、Hadoop、VMware 等工作负载，尽在 NetBackup。
- 软件定义存储：SDS　可提高灵活性，扩大选择面，实现企业级服务水平并优化成本效益。
- 云上云下数据整合：跨各主流平台实现数据保护和可用性

客户收益

第一点

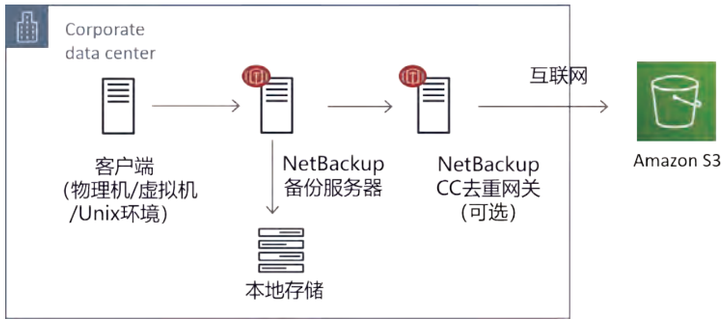
对 IT 建设者而言，公有云的一个显著优势就是弹性扩展，弹性部署。因此，构建方案的时候，这是一个首要考虑点，就是要确保方案对资源弹性部署的适配。Veritas 产品在方案构建的时候，支持云中的 ECS 和 S3，以及 Glacier，我们通过对这几个存储单位的级联部署，以及灵活调整，使性能和容量按需增加，以最大化的减少一次性投入。

第二点

Veritas 数据管理产品的架构和技术非常适用于大规模业务，在传统模型中的很多成熟技术很好的扩展到了云中。

第三点

有的客户在本地依然有数据中心，如果单一的仅仅将数据放在云端，这很难满足数据要异地存放的合规要求。因此，可以利用了 Veritas NBU AIR 的技术，将数据异地传输到本地中心。大家都知道，公有云的一个特点就是，数据下行是要收费的，所以这个技术实现必须要考虑带宽的因素。在 AIR 的异地传输实现过程中，我们经过测算，保守估计节省了约70%的带宽消耗。



方案特点

业务

业务成本效益化，低成本运维及投入，提供高效业务服务。优势点如下：

- 1.按需、快速　2. 实时、可靠　3.效能兼顾。

数据

数据需要了解在哪儿，存放必须安全，能够快速获取优势点如下：

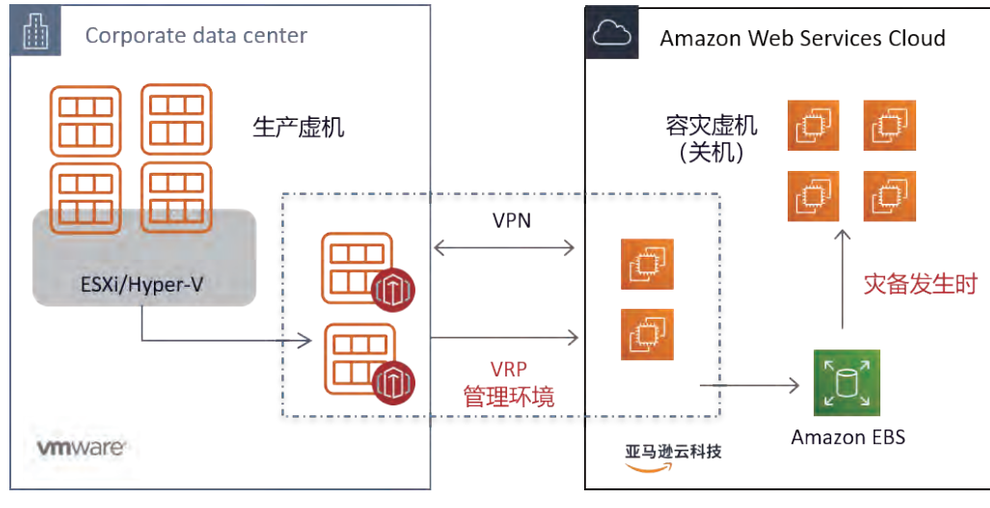
- 1.知其所在　2.存则安妥　3.取必速达

容灾

- 支持 AZ 内或 AZ 之间容灾（AZ：可用区）
- 支持公有云的跨区域容（例如北京区与宁夏区）
- 支持在不同公有云之间容灾

备份

- NBU 支持对公有云上数据进行备份
- 可支持将重删后的数据复制到 S3 存储，降低整体成本
- 通过应用一致性的快照对云上应用提供备份保护
- 可部署在一个公有云或多个公有云，实现多云数据备份的集中管理



扫一扫访问
亚马逊云科技 Marketplace
了解更多 Veritas 解决方案

亚马逊云科技 marketplace

information2 Double Information Double Value | 英方云 i2yun.com

英方软件
企业级混合云灾备解决方案

企业涉及云场景下的数据级、应用级灾备保护，i2CDP 持续数据保护软件，细粒度数据持续保护，可恢复至任意历史时间点。

客户挑战

- 企业生产数据如何实现实时上云；
- 一旦生产系统不可用，企业如何尽快实现数据恢复；
- 恢复之后的数据企业是否立即可用。

information2 产品

上海英方软件股份有限公司持续数据保护与恢复软件 i2CDP，把数据的变化以日志方式保存在灾备服务器。当生产服务器的数据被误操作或感染病毒时，用户可以指定时间将数据恢复到故障前一刻，确保生产服务器能够继续正常运行。

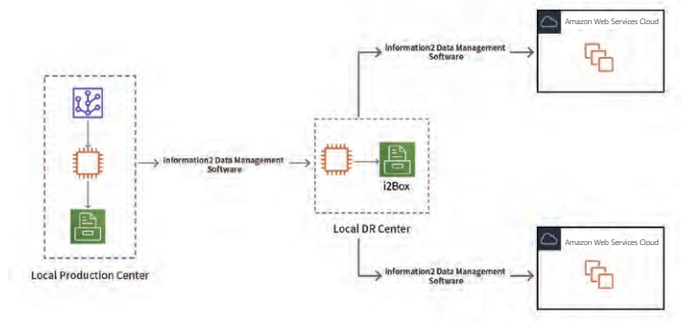
客户收益

- 基于混合云解决方案的核心数据复制技术——字节级数据复制技术，用户将获得无备份时间窗口的生产数据实时上云，且由于传输量小，整个备份过程对带宽消耗不大，大大降低用户资源的投入。
- 一旦生产系统发生逻辑错误、勒索病毒攻击等突发事件之后，提供颗粒度为微秒级的数据恢复，RPO 为零。恢复后的数据可立即用于生产，减少用户因数据丢失而造成的业务中断和经济损失等。

扫一扫访问
亚马逊云科技 Marketplace
了解更多英方软件解决方案

产品功能

- 帮助用户灵活管理混合云灾备，如设定数据保护所需的时间范围和存储空间；自动合并、删除历史数据副本等；
- 满足用户复杂场景下的混合云灾备需求，支持物理机、异构虚拟化平台间、异构云平台间的部署，实现任意到任意间的持续数据保护（P2V、P2P、V2P、V2V）；
- 图形化管理页面，自定义持续数据保护策略；恢复时，选取数据变更时间轴上的任意点，快速定位并将数据恢复到原机或其他。



方案特点

- i2CDP 以字节为数据捕获的最小单位，极大地减少了需复制的数据量；序列化传输方式在窄带宽、异地传输场景下，效率远高于传统备份传输。同时，企业可设置网络限速，保证带宽优先满足生产系统和业务应用。
- 以百万分之一秒的精度，将数据变化过程（包括实际数据、所有者、权限等属性的改变）以日志形式记录下来，分析并计算出变化部分，保存于 CDP 数据保护区。恢复时，指定时间点和目标位置，快速恢复，保持业务连续性。

Veeam Cloud Mobility

Veeam 的云迁移能力，帮助企业制定整体的应用上云、数据上云的解决方案，识别复杂系统上云风险，并辅以专业的技术力量，帮助企业有序、安全、便捷地进行迁移，保证业务的可用性、安全性、业务连续性，解决云迁移所面临的挑战。

适用场景

帮助客户从 On-Premise 将物理、虚拟环境，直接迁移到 Amazon EC2 云环境

客户挑战

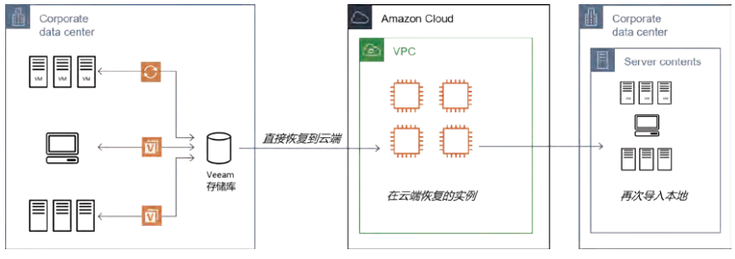
- 迁移停机时间漫长：系统停机，业务中断、迁移周期不可控，会使迁移进程延后
- 解决异构平台风险：异构平台技术适配，厂商的锁定，应用厂商失联，都会使迁移受阻碍
- 云间网络链路复杂：云端与本地网络连接复杂，网络速度成为不可控因素

客户收益

- Veeam 可以帮助企业缩短迁移过程中的停机时间，使客户按需进行迁移。
- Veeam 可以在大多种平台之间迁移，加大了企业迁移的自由度。
- Veeam 不需要通过 VPN，云端无预置主机，可以直接将主机迁移到亚马逊云科技云，减少了企业迁移成本和网络的复杂性。

方案特点

- Veeam Cloud Mobility 包含在全新 Veeam Availability Suite V10 中，是全新的备份数据利用方式，可将任何主机的备份迁移到亚马逊云科技云端，从而实现无缝的迁移过程。云数据管理的核心要务之一是简化云基础架构的采用，并充分利用云的强大力量快速实现现代化。
- Veeam Cloud Mobility 轻松将任何内部或云端工作负载移植和恢复至亚马逊云科技，并支持反向操作。通过将数据保留到云端降低存储成本。自动化存储分级将较旧的备份数据转移到成本较低的云目标。支持多个云厂商这意味着可以避开厂商限制。



Veeam 产品

利用 Veeam 云数据管理解决方案，帮助用户实现业务连续性与按需要迁移的功能。一方面，为企业的数据保护提供了强大的解决方案。另一方面，为云服务提供商增加了业务范围，继续扩大了云灾备托管的收益。

产品功能

- 广泛兼容：Veeam Cloud Mobility 具有广泛的兼容性，可以支持物理、虚拟平台上的大部分 Windows 和 Linux 主机产品。
- 自动调度：Veeam Cloud Mobility 可以与 自动化工具或是 Veeam 原生的 VAO 相结合实现自动化迁移。
- 效果预览：Veeam Cloud Mobility 可以实现迁移效果雨预览，用户可以随时回退迁移过程。
- 自由互联：Veeam 不需要通过 VPN，云端无预置主机，可以直接将主机迁移到亚马逊云科技云，减少了迁移成本和网络的复杂性。
- 安全还原：Veeam 可以自动化的调度杀毒软件，在迁移数据在亚马逊云科技云之前，将病毒木马都查杀一遍，保证了迁移的安全性。
- 业务连续：在迁移之后，Veeam 还提供免费的 VPN 工具，Veeam Power Network，可以保证迁移后的云上主机的可访问性。

扫一扫访问
亚马逊云科技 Marketplace
了解更多 Veeam 解决方案

如果您有任何问题，欢迎拨打亚马逊云科技热线电话：

亚马逊云科技海外区域：**1010 0866**
亚马逊云科技中国（宁夏）区域 - 由西云数据运营：**1010 0966**
亚马逊云科技中国（北京）区域 - 由光环新网运营：**1010 0766**

- **1键**-申请账号及产品咨询
- **2键**-合作伙伴(仅由海外区域热线支持)
- **3键**-账号帐单问题
- **4键**-备案咨询（仅由(宁夏)区域和(北京)区域热线支持）
- **5键**-培训与认证
- **6键**-市场活动查询
- **8键**-Marketplace 产品咨询

扫描二维码访问
亚马逊云科技 Marketplace
海外区

扫描二维码访问
亚马逊云科技 Marketplace
中国区

亚马逊云科技 marketplace

亚马逊云科技 marketplace

如果您有任何问题，欢迎拨打亚马逊云科技热线电话：

亚马逊云科技海外区域：**1010 0866**
亚马逊云科技中国（宁夏）区域 - 由西云数据运营：**1010 0966**
亚马逊云科技中国（北京）区域 - 由光环新网运营：**1010 0766**

- **1键** - 申请账号及产品咨询
- **2键** - 合作伙伴(仅由海外区域热线支持)
- **3键** - 账号帐单问题
- **4键** - 备案咨询（仅由(宁夏)区域和(北京)区域热线支持）
- **5键** - 培训与认证
- **6键** - 市场活动查询
- **8键** - Marketplace 产品咨询

扫描二维码访问
亚马逊云科技 Marketplace
海外区

扫描二维码访问
亚马逊云科技 Marketplace
中国区