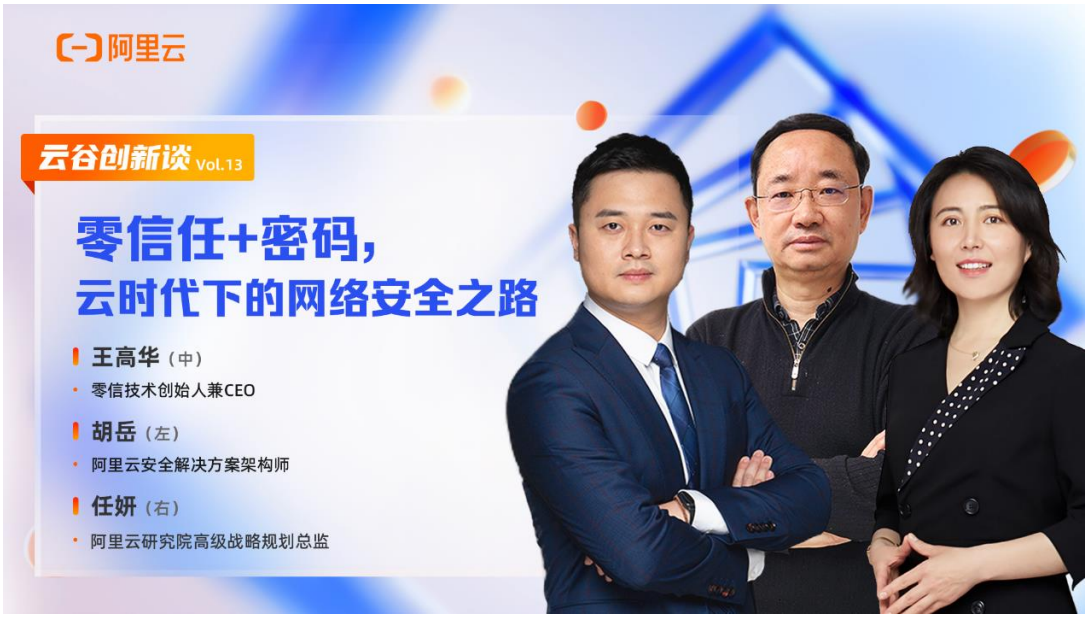
# 云谷创新谈 NO.13 | 零信任+密码，云时代下的网络安全之路

本文转发自 2023 年 3 月 6 日"阿里云在线访谈节目-云谷创新谈第 13 期"，邀请零信技术创始人王高华，与阿里云共同探讨“零信任+密码技术+云计算”究竟为下一代网络安全发展指向何方。




传统网络安全防护是基于“防火墙”的物理边界防御，主要借助软硬件在内网和外网之间构建一道安全屏障，外部用户只要获得认证就能访问内网。伴随着云计算、大数据、物联网、5G 等技术革新，远程办公、云办公等工作模式开始普及，网络环境的内外边界日益模糊，这道防火墙体系在云时代已经力不从心，不能识别谁才是真正“可信任”的用户。

如何保证用户、设备、系统等各种主体的访问安全，实现业务连续和数据安全，是技术服务商和各领域客户都正面临的问题。

2010 年，John Kindervag 提出了“零信任”的概念，其核心是“持续验证，永不信任”，任何人与物在网络中均不可信，基于身份认证和授权重新构建访问控制的信任基础，需对其访问请求进行不断验证。零信任颠覆了传统的安全认证理念，经过多年的发展，涌现出多种支撑技术和实现方式。

本期云谷创新谈邀请了零信技术（深圳）有限公司 CEO—**王高华**，由阿里云研究院高级战略规划总监—**任妍**，阿里云安全解决方案架构师—**胡岳**共同主持，就“**零信任+密码**”话题，一起分析零信任行业的国内外发展态势；从发展战略层面解读零信任技术的走向以及对政企系统的影响；共同探讨在云原生时代，零信任技术在商业化落地中的机遇与挑战。

## 01 解读国内外零信任市场信号，零信技术的破局“密码”

根据 Gartner 的数据，2022 年全球网络安全市场规模增长至 1691.56 亿美元。安全市场非常大，但同时比较分散庞杂，王高华选择了“零信任”作为突破口。

在互联网与信息安全领域深耕三十多年，王高华从事过政务信息系统建设、CA 运营、密码技术、软件研发等工作，早在 2002 年，他就创立了沃通 CA 及其子公司密信技术，后被 360 集团收购。

这位 IT 老兵时隔二十年后再次创业，于 2021 年成立零信技术，继续未了的数字证书及密码应用事业，这一次他将**密码技术与“零信任”安全理念相融合**，开启了新一轮网络安全实践。

“零信任”需要解决多个层面的安全问题，当中最核心的问题是：如何让正确的人，在正确的时间，访问正确的资源，获取正确的数据。**王高华认为，零信任是基于 PKI 体系来实现数字信任。**“PKI 是安全这个木桶的底板，如果桶底没了，就一滴水都没有了。”

PKI 指的是公钥基础设施，这是一种遵循既定标准的数字证书管理平台，为网络应用提供加密和数字签名等密码服务及其必备的**密钥和数字证书管理体系**，广泛应用于网上银行、电子商务、电子政务等领域。而 PKI 中最基础的应用是 SSL 数字证书，具有身份验证和数据传输加密功能，几乎所有的网站、APP 都要使用 SSL 证书。

那零信任应该在一个怎样的具体框架下进行网络安全防护？王高华和胡岳带我们从国内外网络安全战略中解读政策信号。

美国在 2021 年颁布的“联邦零信任战略”中，就提出了零信任的五大支柱：**身份、设备、网络、应用和工作负载、数据**，并通过协同自动化系统进行监管，为零信任的发展给出了具

体方向。看回国内，从网安法到 2020 年制定并正式实施的《密码法》，我国近年来也接连发布一系列推动零信任落地的政策。

王高华认为基于五大支柱的零信任框架，对于我国政企建设零信任体系，保障云上用户安全也有着重要的借鉴意义。同时指出，我国的《密码法》在零信任体系中启动基础性作用，尤其在政务信息的保密和安全方面发挥重要作用。

国家愈发关注信息安全建设以及关键基础设施的商用密码使用规范，而零信任模式作为一种新的安全模型逐渐进入大家的视野，业界也在积极探讨如何将零信任的理念助力国家信息安全能力建设。

## 02 从理念走向实践，“零信任”面临的挑战与机遇

零信任从理念走向实践的过程中，仍面临着重重困难，胡岳认为目前问题主要集中在三个维度：

**其一，考验管理者的认知度与决策力。**管理者在选择零信任前，需要有清晰的认知：建立信任到底能为企业解决什么问题。

**其二，考验执行者的魄力。**零信任的建设会打破企业当前业务习惯甚至于部门的协作关系，会对原有的经营模式发起挑战。坚定的战略定力是考验管理者的一个门槛。

**其三，传统模式下零信任实施难度大。**在零信任工程建设中，企业不仅需要对系统的资源现状有清晰的认知，包括梳理访问入口、明确保护对象、明确保护范围等，同时需要建立可信终端、可信网关、统一认证、统一鉴权、应用集中授权等一系列的改造才能落地零信任的技术模式。

同样，王高华认为零信任仍然处于生态分散化野蛮生长中，不同主体对零信任的基本概念、技术路径等认知差别较大，市场对于零信任的认知存在几个误区。企业如何选择适合自己的零信任建设方案？

胡岳表示：“身份、设备、网络、应用、数据”这五个方面，单独一点都能延伸出很多的话题和方案，企业可以根据自身的业务现状裁剪方案。全局部署的零信任方案对于企业来说，

在管理上和技术上都要面临不小的挑战，企业不妨可以从最急迫的几个点入手，进行零信任的能力建设。”

当前，以谷歌、亚马逊、Cloudflare 等为代表的国际科技公司已经在进行零信任理念实践，他们在零信任和密码结合方面进行了很多创新，为国内的企业零信任建设提供了很多借鉴。

在这些企业代表身上，王高华关注到了“云”的能力，表示：“我们可以将把密码产品和服务同云服务融为一体，为用户直接提供所需的产品和服务。”

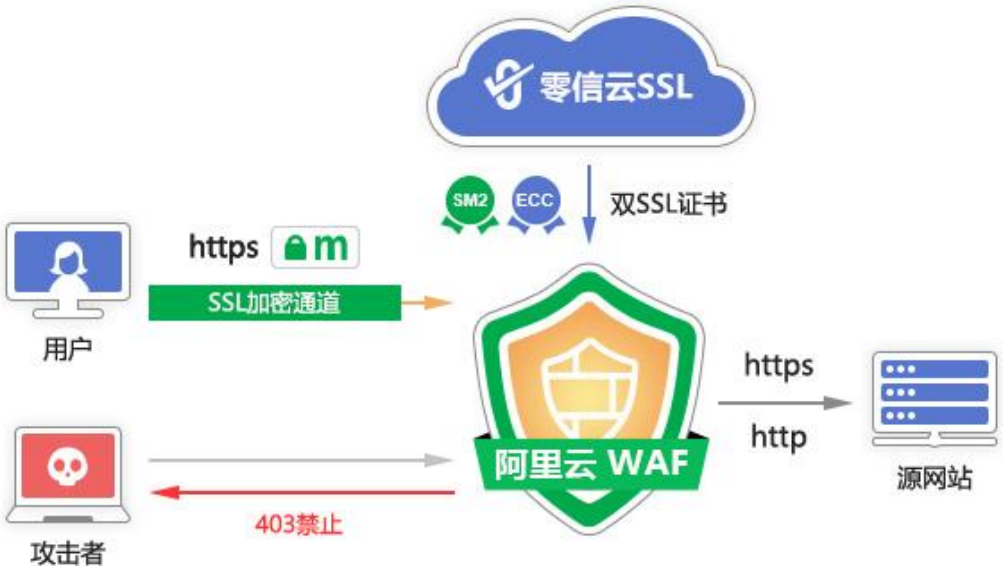
云服务成为了零信技术的新着力点。零信技术开始构建集端云一体的服务体系，与阿里云开始了一次“密码+云服务”的创新实践，基于本地端存放用户关键数据及信息，包括密钥、数字证书等，同时依托云服务完成自动化加密、防护和证书签发工作。

## 03 “端云一体”零信任解决方案

在上云过程中，王高华的考虑主要有两方面，一方面是数据和信息的安全性；另一方面是操作的便捷度。

他提出：零信任的内核是“**永不信任、始终验签、始终加密**”，密码技术就像一把自动锁，既能实现身份验证，又可以对明文加密，保障数据安全。同时，零信技术提供的端云一体的零信任解决方案，通过融合云服务，尽可能减少用户操作环节，帮助用户一键实现数据加密(如 https 加密)。

在 2022 年乌镇世界互联网大会上，零信技术发布了网站安全云服务。将阿里云的 WAF 产品与零信任的云 SSL 服务相结合，用户下单购买网站安全云服务，只需做 2 到 3 次域名解析即可为用户提供 https 加密、云 WAF 防护、CDN 分发、网站可信认证等四位一体的网站安全服务，用户不需要分别向阿里云购买 CDN/WAF 服务、向 CA 申请 SSL 证书，一键即可完成。同时零信技术已完成升级支持国密 SSL 证书，自动化实现国密 https 加密。




（零信技术网站安全云服务—国密云 WAF 服务）

随着中小企业上云的持续深化，还需要继续降低中小企业的零信任建设门槛。对此，王高华提出了他对于云服务的考量，更看重集成化的能力。“以建站为例，用户肯定希望一键完成操作，通过云服务可以实现自动化配置 SSL 证书，并直接实现通过 https 访问网站。”

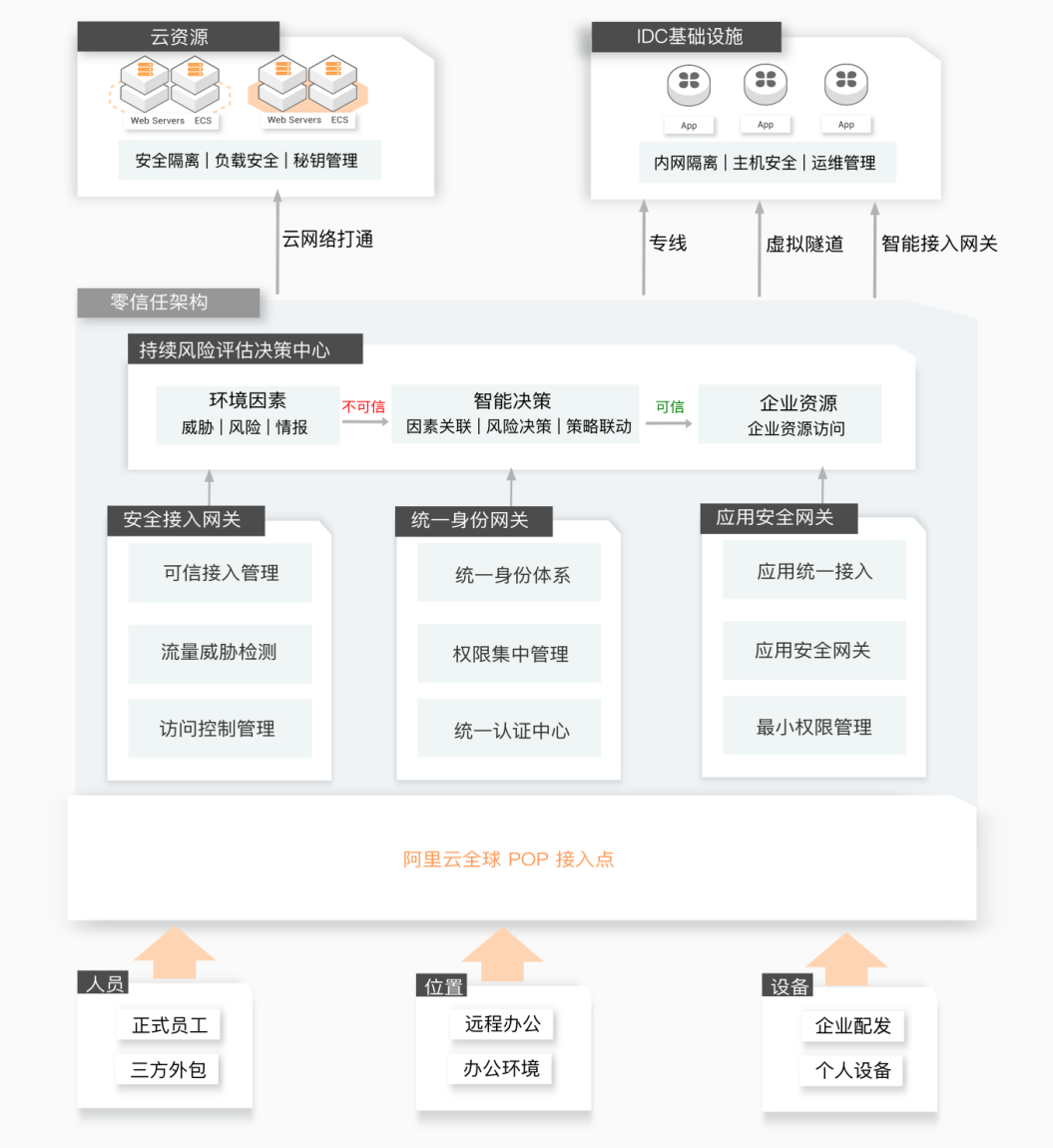
对此，阿里云安全发挥云计算的优势，利用安全即服务的理念，大大降低零信任的建设难度和门槛。阿里云提供的零信任安全解决方案基于零信任安全框架的指导思想和原则进行设计，通过零信任架构对访问主体向企业资源的请求进行安全验证，使得默认不可信的访问请求在经过身份、设备、网络和应用权限的验证后能够安全访问企业资源。

基于高效的零信任网络，阿里云在全球布局多个 pop 节点（入网节点），结合阿里云自身多年的网络攻防经验，能够在 pop 点为企业提供实时的访问、入侵监测和保护。基于阿里云的全球网络建设，可提供全球的办公应用安全加速服务。

默认采用云原生的零信任框架，遵循整个零信任线上原则，构建访问的可信链路，通过云延伸的边缘安全接入点和网关进行身份设备网络情报的安全校验，以及最小化的权限授权，帮助企业构建可信的安全框架。基于云原生架构，可提供天然的高可用及网关自身的防护能力。

通过 SaaS 化安全服务实现快速灵活部署，企业无需部署和投入硬件资源，快速搭建零信任网络框架，并支持云混合部署形态，减少企业重复建设工作，降低运维压力。

此外，阿里云借助当前比较强大的机密数据和流量分析能力，对办公网的外发下载行为进行识别和途径分析，帮助企业获取敏感数据使用的地图，并进行告警和监控，从而保护企业的机密数据不被损害。




（阿里云零信任安全解决方案架构）

零信技术与阿里云的合作，形成了一次零信任的建设范例，帮助用户降低零信任技术体系的复杂度，提升了云上安全防护水平。随着云原生技术的深入，以及零信任理念的进一步普及，安全市场对零信任服务需求表现更多元化。如何实现零信任在更多安全防护场景应用，获得更多用户的信赖，是每一个服务商接下来需要思考的命题。

---

请关注公司公众号，实时推送公司 CEO 精彩博文。