零信任的发展及其在安全远程访问中的应用

Contents

摘要

本白皮书首先介绍了“零信任”概念及其相关历史背景，并解释了近年来零信任为何越来越受欢迎。此外，白皮书讨论了零信任在当前网络安全实践中最引人注目的应用，接着聚焦其在远程访问中的应用，即零信任访问（ZTA）。最后，本文说明了腾讯如何在其T-Sec零信任访问控制（ZTAC）平台中实施ZTA。

零信任的时代已经到来

虽然零信任早在十多年前已经出现，但这种信息安全方法在过去三年中获得了发展动力，一个证明就是，越来越多的技术供应商在其市场活动中支持零信任概念并表示在其产品中融入了该技术。此外，针对该主题的网络研讨会、会议和白皮书数量激增都显示出，当前企业对零信任的兴趣比以往更加强烈。

近期，新冠疫情驱使全球数百万知识型工作者长时间居家办公。这引发了企业对安全远程访问的关注，以及对更安全的传统虚拟专网（VPN）方法替代方案的兴趣。零信任原则在此问题上的应用是零信任访问（ZTA）技术，我们将在白皮书后面的部分进行讨论。

首先，让我们考虑推动零信任兴趣的市场现实，接着研究这种针对安全的设计、实施和操作方法的核心原则。

威胁经济迅速发展

网络安全是IT方面唯一具有天然对立性的领域。尽管服务器、处理器、网络和应用厂商都在相互竞争来争夺业务和市场份额，但安全厂商不仅必须与彼此竞争，还必须面对企图规避其产品的攻击者。网络攻击者和防御者之间的竞争通常被恰当地比作“军备竞赛”，并且有明显迹象表明，在过去二十年，防御者一直处于劣势。

首先，它们正在保护的基础设施变得更加复杂。由于数字化转型、应用基础设施向云迁移以及越来越多的智能终端能够远程连接到企业资源等趋势，网络边界几乎已经消失。

在这一新情况下，客户面临着更大的敏感数据可能丢失的风险，而传统的网络安全架构（在基础设施可以被视为“城堡与护城河”时创建）无法应对该挑战。

攻击者的数量和种类大幅增多；曾经他们大多是希望获得同行认可的技术极客，而现在的情况已经发生了很大的变化。当前，全球各地都存在资金充裕的犯罪集团，并且存在具有政治动机的“黑客行动主义者”社区，例如匿名者（Anonymous），此外还有背靠国家支持的拥有丰富资源的攻击者群体。

同样，自世纪之交以来，这些群体可以利用的威胁基础设施迅速发展：

- 包含基础攻击代码的攻击工具包在暗网上的价格相对很低；
- 暗网上还存在一个线上的现成市场，提供有助于攻击者的各种数据，包括盗用的IP地址、盗用的信用卡详细信息和其它凭证；
- 伴随云计算的发展，保障匿名性的僵尸网络和代理等犯罪软件即服务基础架构大量出现。

除了21世纪迅速发展的“威胁经济”之外，还出现了合法的隐私举措，这些举措进一步推动了攻击者的活动。例如：

- Tor Project（基于The Onion Router浏览器）推出了免费的开源软件，该软件使互联网流量经过一个由全球志愿者免费提供，包含数千个中继的覆盖网络，从而隐藏用户的位置和使用，避免任何人进行网络监控或流量分析，最终实现匿名浏览和通信。
- 即时消息应用（如WhatsApp）已将加密作为一种标准做法，Telegram等类似WhatsApp的应用正为消息、视频通话、VOIP和文件共享提供“端到端”加密。

虽然这类技术并非天然为非法活动而设计，但显然，伴随合法用户寻求隐私和言论自由，它推动了非法活动的迅速发展。

对于网络犯罪的演变而言，另一个重要的发展是加密货币的出现。加密货币作为一种交易媒介，是数字资产或货币的电子形式，而且至关重要的是，加密货币不受任何中央权威的管制。

去中心化且独立的加密货币自然引起了网络犯罪分子的关注。虽然作为加密货币的支撑技术，区块链公开宣称的目标是成为一个不可篡改的分类账来保障身份识别，使所有交易都能被追踪，但有一种方法可以绕过这种追踪，称为“不倒翁”服务。该服务将可能被识别的加密货币资金与其它加密货币资金混合以掩盖通往资金源头的路径，这意味着在交易中可以保持匿名。据估计，在暗网上进行的非法活动中，高达 97% 都是通过比特币（最著名的加密货币）进行交易。

加密货币为网络犯罪分子提供了一些便利：

- **首先，比特币已成为勒索软件攻击中最受欢迎的交易形式，即通过比特币支付赎金。**
- **其次，加密货币交易平台对于犯罪分子来说是容易攻击的目标，而攻击的目的通常是窃取资金。**
- **由于缺乏监督交易的中央权威，加密货币也为毒品交易等非法活动的洗钱行为提供了便利。**
- **最后，挖矿是IT系统被入侵的主要驱动因素之一，犯罪分子可利用他人服务器（以及电力）来从事耗能的牟利活动。**

预防性安全方法无法承受越来越大的压力

以上这些技术的发展，导致原先主要的网络安全保护措施效力下降；我们可以将这个方法称为预防性方法，尽管该方法依赖“零号病人”受到网络病毒感染。

这是传统的杀毒（AV）软件，其工作方式如下：杀毒软件厂商的一个客户报告感染，这时该厂商将分析引发该问题的恶意软件并针对该病毒开发一个所谓的“签名”，然后立即将签名分发给所有其他客户，以防他们受到感染。许多杀毒软件厂商还将检测到的警告信息提供给VirusTotal等订阅式社区，以便其它厂商保护自己的客户。但是，病毒签名仍然是各个厂商的知识产权。

这种模式对于一些厂商来说很有效，其中一些厂商（赛门铁克和迈克菲）成长为价值数十亿美元的公司，同时为消费者和企业客户提供服务。然而很明显，在2010年，网络威胁领域的规模和速度占据上风，杀毒软件捕获的病毒百分比逐年下降。在2014年，杀毒软件市场的领导者赛门铁克向《华尔街日报》承认，杀毒软件“已死”，或至少“注定是要失败的”，它捕获到的病毒已不到50%。

三种新的安全方法——NGAV、XDR和零信任

随着传统的预防性安全方法承受越来越大的压力，安全行业广泛响应，采用了以下三种方式：

- **下一代杀毒（NGAV）**厂商寻求机器学习和威胁情报来增强预防性能力；
- **各种扩展的检测和响应（XDR）**：一些公司完全放弃了预防性方法，而是采取一种反应式方法，在客户基础设施中存在威胁时进行检测并做出响应。各种各样的技术正在涌现，首先是端点检测和响应（EDR），然后是网络检测和响应（NDR），并且现在Omdia发现了用于云的检测和响应技术（CDR）。这些服务统称为XDR。
- **零信任**是第三种方法，本质上它是一种规范性方法，通过让组织的受攻击面完全脱离互联网来缩小受攻击范围，仅将特定资产提供给单个用户（通常是员工或合作伙伴）和系统，并在他们获得访问权后监控和记录其行为。

所有这三种方法都取得良好发展，但阶段不同。NGAV在上一个十年的中期取得了一些成功，但其大多数支持者都被较大的安全厂商收购，从而将该技术融入到更广泛的产品组合中。另一方面，XDR不断发展壮大，如今不仅支撑着多个厂商的产品组合，还支撑着被称为MDR的管理服务产品。相比之下，零信任在过去三年才受到重视，尽管这个概念已经存在了十年之久。

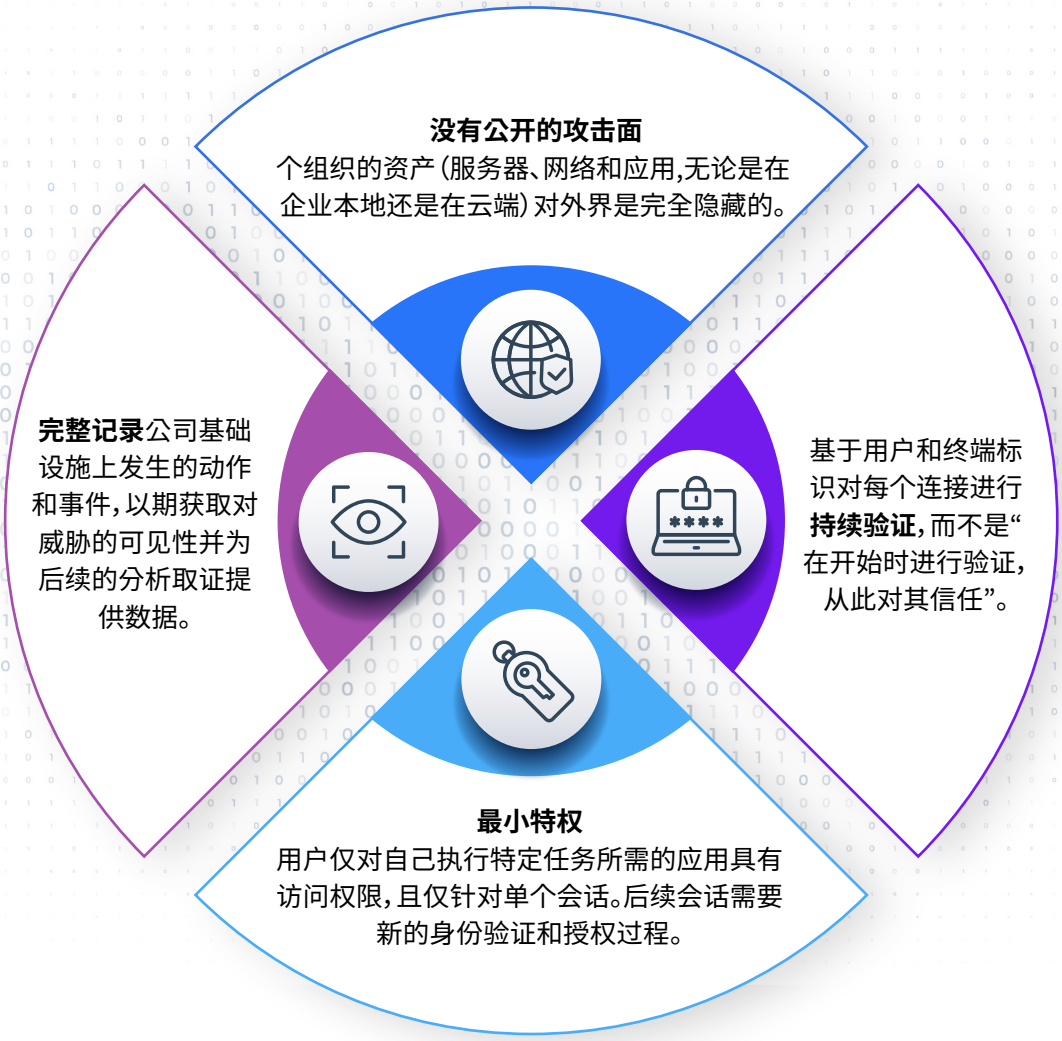
零信任概念的演进

零信任的历史可以追溯到21世纪初许多组织内部开展的工作，其中包括耶利哥论坛、美国国家安全局（NSA）以及谷歌等公司。这些举措的驱动力来自人们越来越意识到处于组织边界的预防性安全平台正败下阵来，因此需要一种更好的安全方法。例如，谷歌将许多零信任原则融入到为内部员工开发的远程访问平台BeyondCorp上。

当时使用了各种词语来描述这种新方法，包括“Black Cloud”、“de-perimeterization”和 “segment of one”，而“零信任”一词是在2010年由时任Forrester分析师的John Kindervag正式提出（现在他是Palo Alto Networks的区域首席技术官）。

“永不信任，始终验证”是零信任理念的一个常用口号，这使它能够很好地与之前的安全方法（即“信任，但也要验证”）区别开来。其核心原则如下方图1。

图1. 零信任的关键原则



资料来源: Omdia

零信任在现代安全领域中的应用

十年后的今天，我们可以发现在一些领域，零信任方法已经融入到网络安全技术中。

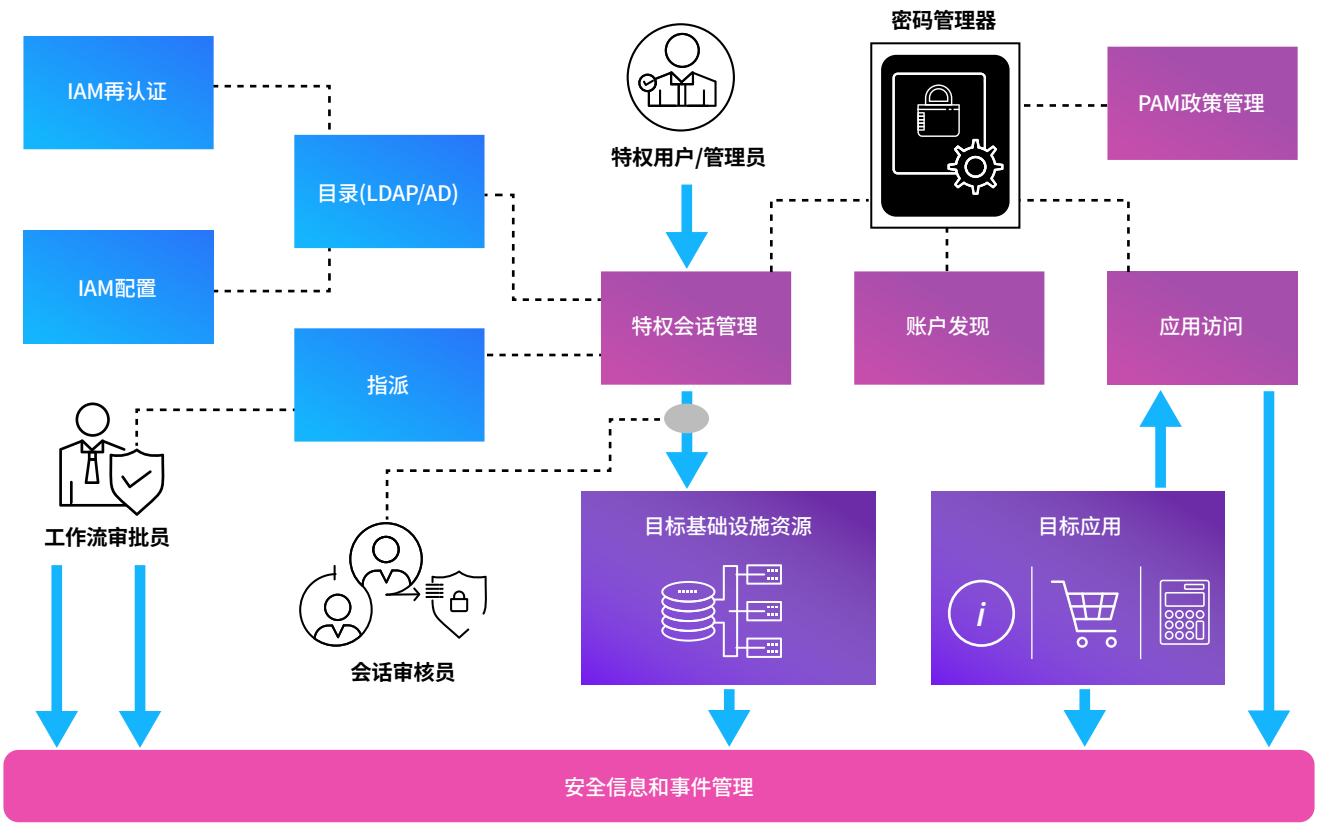
特权访问管理（PAM）采用最小特权原则

作为身份和访问管理（IAM）的一个分支，PAM在过去十年脱颖而出，因为显然，攻击者针对的是组织内拥有最广泛访问权限的用户（系统管理员、高管等），因此就要求对他们的凭证进行更严格的控制。

密码管理器是保证此类用户凭证安全性的首次尝试。然而，随着应用基础设施向云迁移并变得更加动态化，密码管理器的作用被削弱。因此，现在人们常常提到需要PAM系统来支持“最小特权”。通过该系统，特权用户（例如系统管理员）仅授权访问他们当前需要的应用，而不是像之前那样，在登录后享有对企业中所有系统的访问权限。当他们切换到另一个应用时，必须重新登录。

在易用性/用户体验和安全性之间，几乎总是需要进行权衡取舍，而显然最小特权首先考虑的是安全性。现在，由于系统管理员在采用每个新应用时需要再次登录，一些PAM系统试图简化这个单调乏味的过程，尽管这在一定程度上会不可避免地损害最小特权准则。它们让公司创建一小部分可以通过单点登录在一个会话中一起访问的应用程序；然而，以最小特权不可能全面访问组织的整个基础设施。

图2：特权访问管理



资料来源: Omdia

云权限管理（CPM）将零信任应用于数据存储

应用零信任原则的一类新兴技术是云权限管理（CPM）。CPM旨在解决“权限蔓延”的问题——

开发人员、管理员、服务帐户和应用权限因为权限蔓延问题（往往通过从属于某个特别工作组等间接方式）而能够随便访问公司在云端的应用和工作负载。

CPM技术调查了公司云端数据存储的访问权限，就在哪些地方减少访问权限提出了建议，并在客户希望的情况下，通过升级或自动方式采取补救措施。

零信任访问：零信任在远程访问中的应用

零信任的一个更广泛应用（不仅限于特权用户）正在兴起，即零信任访问技术，该技术可满足所有公司用户（员工、合约商和合作伙伴）的远程访问需求。它仅支持远程用户访问执行工作所需的特定应用或资源。公司网络的其余部分是不可见或不可选的。

显然，随着疫情的到来，安全远程访问问题急需解决。VPN是组织向企业最终用户提供远程访问的主要方式（另一种方法是基于服务器的计算，通常与瘦客户端技术结合使用，但是功能往往更少），因此ZTA是一种与之竞争的方法 。实际上，一些ZTA厂商将其定位为一种更安全的替代方案。

相比VPN，ZTA的优势是它提供了更大的安全性。VPN授予对整个公司基础设施的访问权限，这导致攻击者一旦得到允许，就可以植入代码来进行监视（通过所谓的东西流量），并找出有价值的资产，以便随后向指令和控制服务器渗透。ZTA支持用户访问完成工作所需的特定资产，并在用户得到允许后监控会话。

微隔离

零信任现在经常被用来保护工作负载，包括数据中心，特别是云环境。在这种情况下，可以看到许多公司提供的微隔离技术都采用了零信任原则，并作为云工作负载保护平台(CWPP)市场的组成部分。

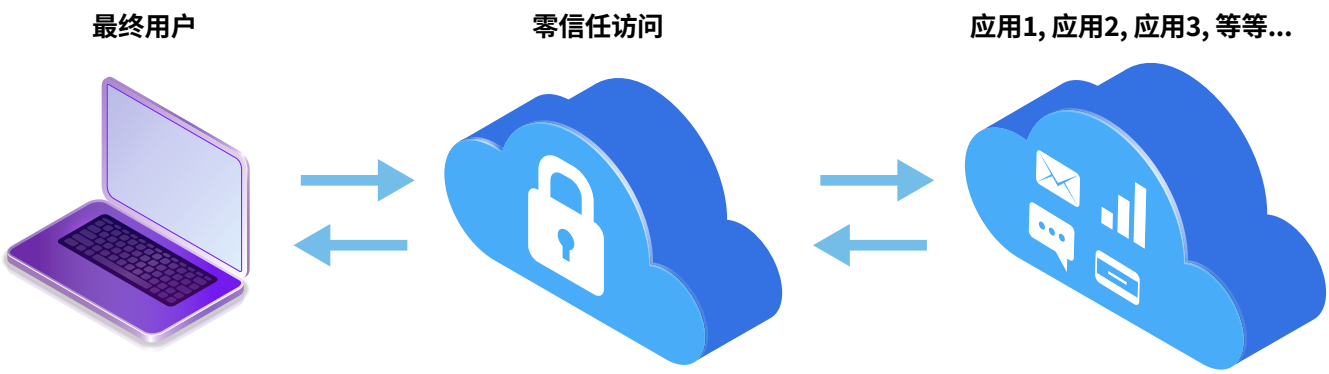
就云环境而言，微隔离方法针对基础设施和平台即服务（IaaS和PaaS）环境创建安全区域，使公司能够将工作负载彼此隔离并分别进行保护。

关键不在于人的访问，而在于系统到系统、工作负载到工作负载的流量，因为随着攻击者试图收集更多数据，或感染更多工作负载，成功的突破通常需要东西流量，即在云环境中的实例之间通信。因此，隔离每个工作负载并检查所有往返流量的能力使公司能够采用并实施特定于工作负载的安全政策。

此类功能通常需要在运行工作负载的主机上安装小型软件代理。代理会与可能位于客户本地或云端的“中央大脑”进行通信，以接收阻拦和允许等指令。代理通常通过与主机操作系统的原生防火墙功能（即Windows Filtering Platform，或者Linux系统中的iptables功能）集成来执行这些强制功能。

当然，在某些情况下无法部署代理，例如高频交易（该情况下，任何其它功能都会被禁止以避免增加延迟）。对于这些情况，微隔离供应商使其产品能够通过应用程序接口（API）与负载均衡器和防火墙集成，从而利用这些终端来实施功能。

图3：在安全远程访问方面，零信任访问是VPN的替代选项



资料来源: Omdia

两种ZTA架构

对于ZTA，值得注意的是，ZTA供应商提出了两种架构。

软件定义边界（SDP）

第一种架构是软件定义边界（SDP），其技术规范由云安全联盟（CSA）编写。SDP系统依赖于以下功能软件：

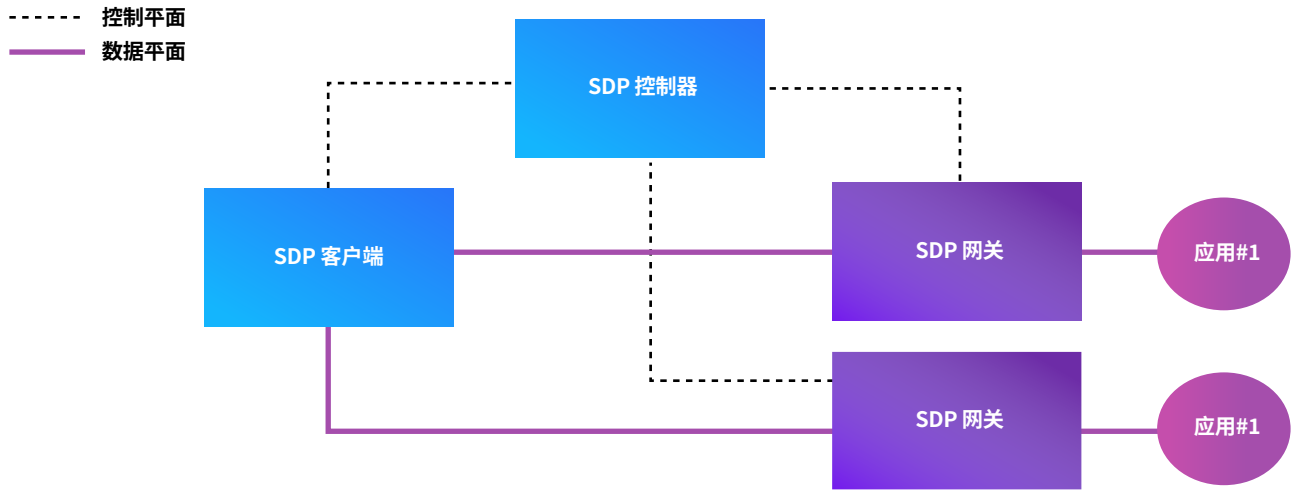
- SDP客户端软件，在最终用户的终端上运行
- SDP控制器，处于云端或客户本地，用于设置和实施访问政策。控制器位于最终用户与目标应用之间的控制路径中，而非数据路径中；
- SDP网关，通常在每个网段部署一个（或部署两个以实现高可用性），并在用户和后端的目标应用之间充当防火墙。网关位于最终用户终端与应用之间的数据路径中，而非控制路径中；
- 此外，SDP系统监控所有访问活动，并使用日志服务器来进行报告。

网关可以处于企业本地，也可以处于公有云或私有云中，具体取决于网关将授予访问权限的特定应用所在位置。

SDP控制器接收最终用户的访问请求，并根据Active Directory或LDAP等源验证其身份，并检查其登录的端点终端的安全状态。如果请求被接受，那么控制器会通知位于数据平面的网关，从而设置连接最终用户终端和应用的加密隧道。接着将进入直通模式，从而不在通信中添加任何延迟。

所有其它资产，无论是在公司本地还是云环境中，都将“隐身（blacked out）”（所以才会在开发此概念的早期阶段使用“Black Cloud”一词），无法访问，从而使围绕公司基础设施的特权升级或横向移动成为无效尝试。

图4：用于零信任访问的SDP架构

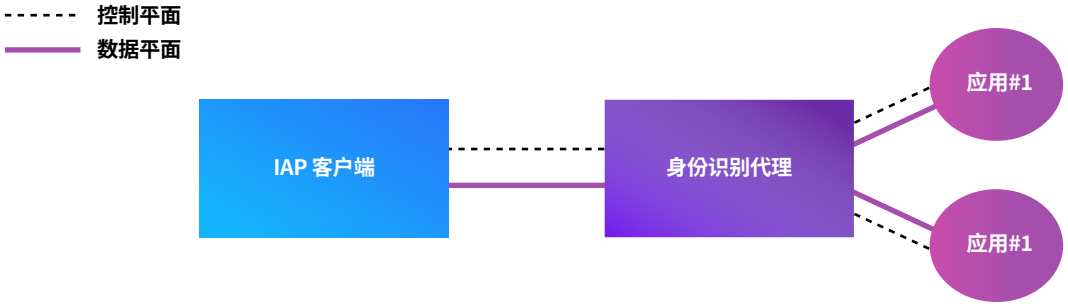


资料来源: Omdia

身份识别代理（IAP）

第二类架构称为身份识别代理（IAP）。在IAP中，代理既处于控制平面又处于数据平面，因此不仅作为访问请求的中介，还会在之后为最终用户和应用建立起加密隧道。

Figure 5: The IAP architecture for zero-trust access



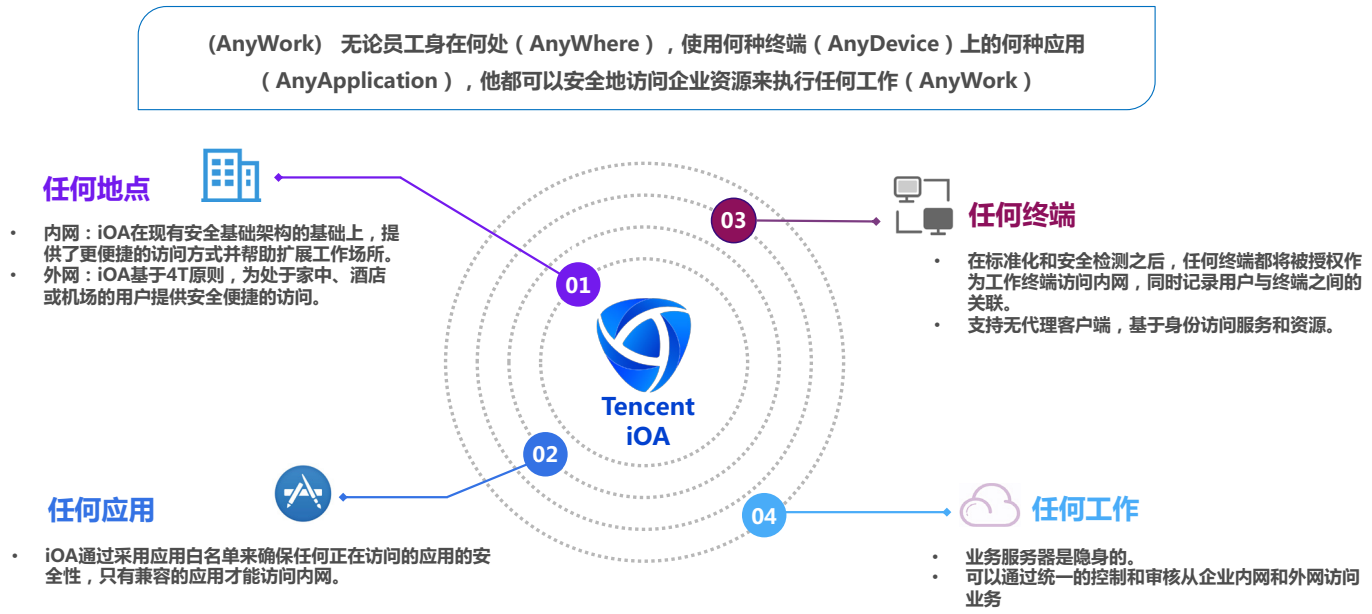
资料来源: Omdia

由于在数据平面中加入了一个额外的“插件（bump in the wire）”，这种方法有可能会增加延迟。因此，提供IAP的大多数供应商和厂商都在运行自己的网络，这使它们能够通过最佳路径选择等技术来改善延迟和其它性能方面的考量。相比之下，SDP通常作为软件提供给公司来部署和运营，也就是说，它不一定要作为一种服务。

腾讯的产品：ZTAC

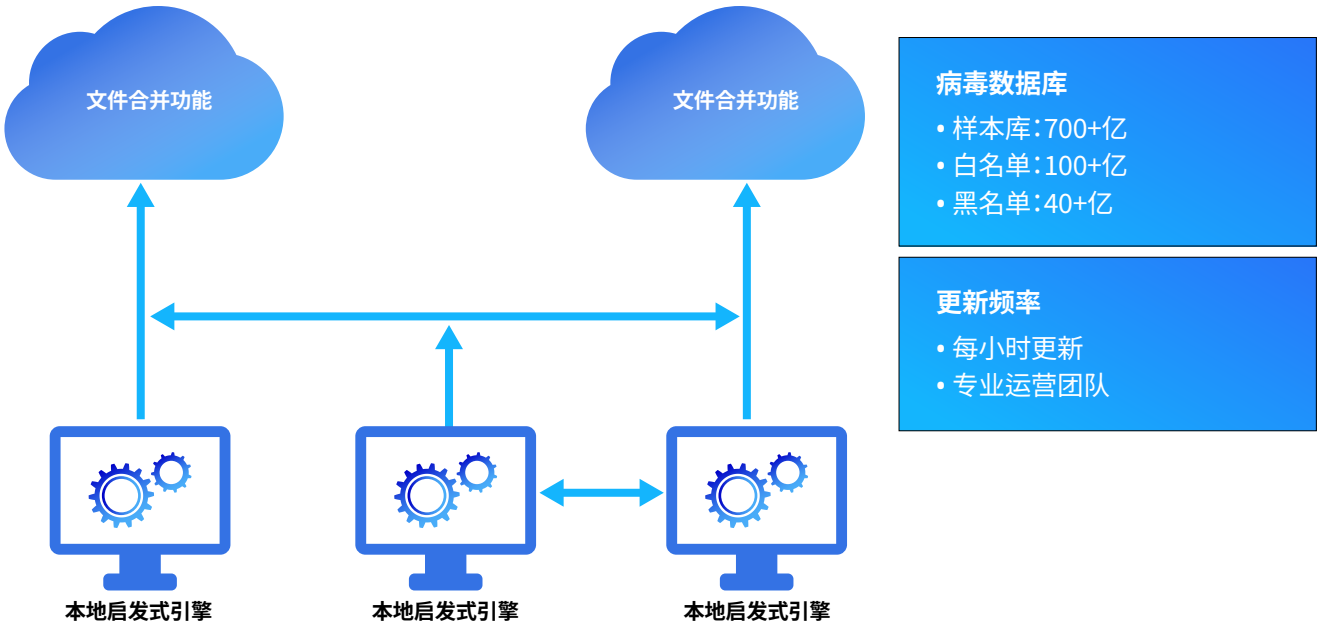
腾讯将零信任原则融入到一个“零信任安全管理系统”中，该系统名为腾讯iOA。腾讯将其针对iOA的设计愿景称为“4A”，具体可参考下方图6：

图6：腾讯iOA零信任架构的设计原则



资料来源: Tencent

图7：腾讯的病毒查杀功能



资料来源: Omdia

这四个A是：

- Anywhere, 无论用户身在何处（企业内网或外网），甚至处于其它国家，都可安全便捷的接入业务资源；
- Any Device，任何终端，是指支持属于公司和不属于公司的终端，这意味着终端设备在通过iOA（提供基于代理和无代理的运行模式）进行标准化和安全检测后，任何终端都可以作为工作终端来访问企业业务资源。腾讯还基于20多年的数据积累，支持病毒查杀和漏洞修补——利用自研的杀毒引擎清除已知病毒同时主动阻止未知病毒（见图7）。
- Any Application，任何应用，是指iOA可以对访问业务资源的任何应用进行管控，通过采用应用程序白名单来确保任何正在访问的应用程序的安全性，只有白名单内的应用程序才能访问企业业务资源。
- Any Work，任何业务，是指iOA将业务服务器隐藏，企业内外网业务均可接入，进行统一管控和审计。

iOA是腾讯零信任访问产品（称为ZTAC）的基础，它以两种部署模式提供：其核心功能可以处于客户本地（腾讯将其称为“私有化”模式，完全由客户管理），或者作为软件即服务（SaaS模式）交付。

如上所述，腾讯提供基于代理和无代理的ZTAC版本，基于代理的版本具有EDR和端点数据防泄漏（DLP）功能。架构方面，该平台可提供SDP和IAP两种模式：

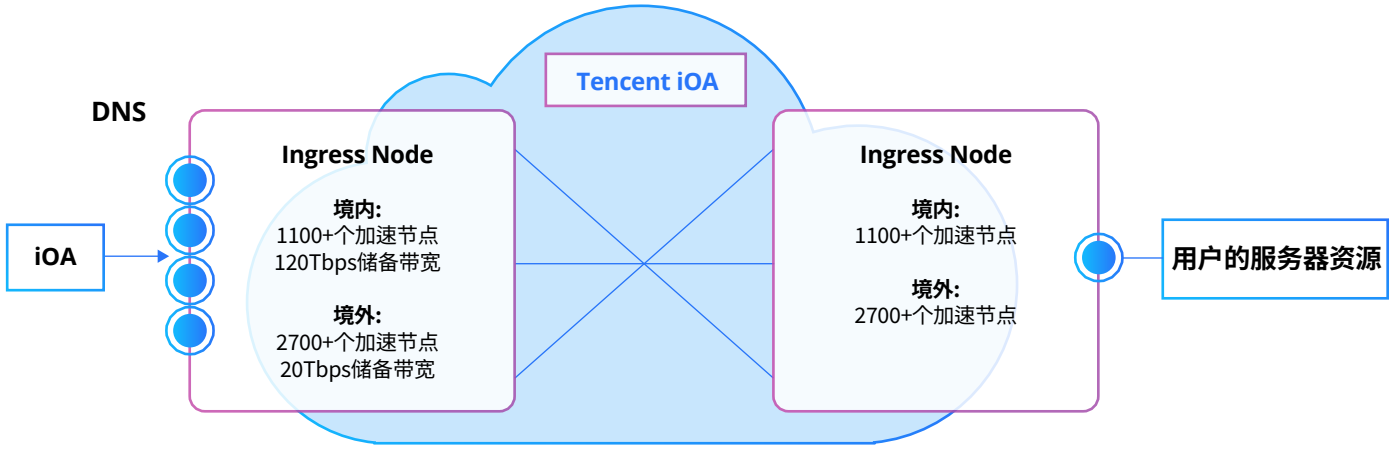
- 无代理版本使用部署在腾讯自身网络基础设施上的Web代理，流量由腾讯的骨干网承载，而腾讯以SaaS模式提供ZTAC
- 基于代理的版本使用类似于SDP的架构，但使用由腾讯开发和专有的一个不同的协议。在该情境下，由企业客户负责管理该平台并在其选择的网络基础架构上运行该平台。

WAN加速和链路优化

腾讯iOA

值得一提的是，腾讯还利用其搭建的基础网络设施为客户提供更全面的服务。iOA结合腾讯遍布全球的约1300个加速节点，为客户提供网络加速，并采用智能路由、协议优化、多路复用和抗抖动电路等技术，实现更快速稳定的业务访问，除网络加速外，还提供DDoS等防护服务。

图8：腾讯的智能办公访问（iOA）WAN服务

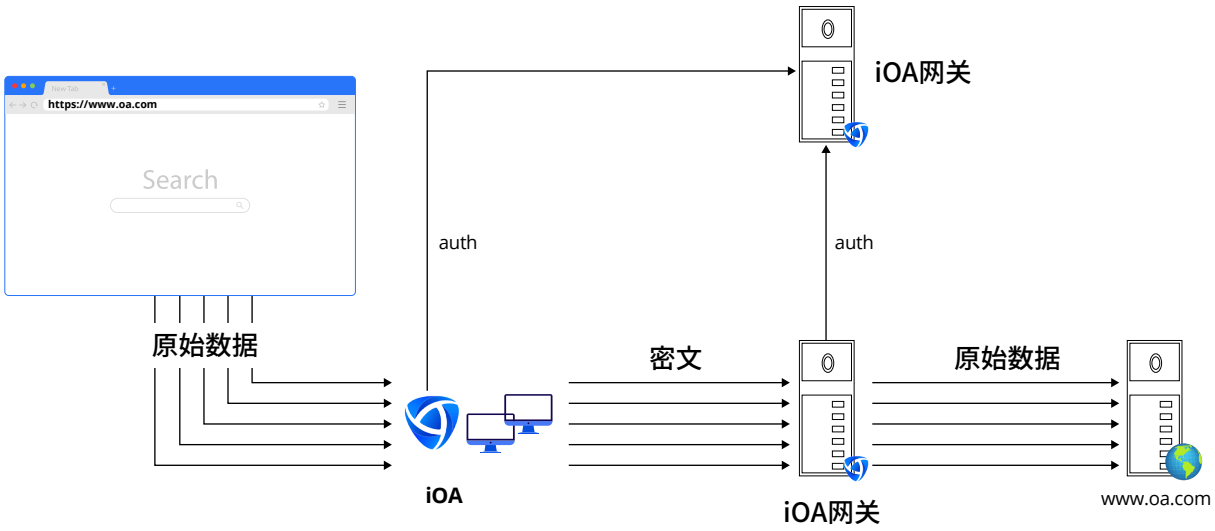


资料来源: Tencent

通过链路优化提高VPN性能

尽管将ZTA用于远程连接的益处十分显著，但腾讯意识到，许多客户已经对传统的VPN技术投入了大量资金。对于这些客户，其IOA服务提供了链路优化技术，可以根据需求为VPN客户端建立一个专用的安全通信通道，从而无需再采用传统隧道技术。这对于可用带宽以及延迟、抖动和丢包具有显著的积极影响。

图9：链路安全性和优化



资料来源: Tencent

附录

作者

Rik Turner
Rik Turner, 首席分析师, 网络安全
askananalyst@omdia.com

关于Omdia

Omdia是一家全球性科技研究机构，由Informa Tech研究部门（Ovum、Heavy Reading和Tractica）与收购的IHS Markit科技研究部门合并而成。

Omdia汇集了超过400名分析师的专业积累，覆盖全球150个市场，每年发布3000多份研究报告，服务于14000多家订阅客户，遍及数千家科技、传媒和电信企业。

我们拥有详尽的信息和深厚的专业技术积累，能够揭示出可操作的洞察，支持我们的客户在当今不断发展的技术环境中串点成线、统揽全局，进而推动自己的业务持续向前——把握今天、决胜未来。

*IHS Markit的大部分科技研究产品和解决方案已于2019年8月被Informa收购，现已成为Omdia的一部分。

Omdia的400多名分析师和咨询师遍布全球

美洲
阿根廷
巴西
加拿大
美国

亚太地区
澳大利亚
中国大陆
印度
日本
马来西亚
新加坡
韩国
台湾

欧洲、中东、非洲
丹麦
法国
德国
意大利
肯尼亚
荷兰
南非
西班牙
瑞典
阿联酋
英国

Contact Omdia

E insights@omdia.com
E consulting@omdia.com
W omdia.com

OmdiaHQ
Omdia

Contact Tencent

腾讯安全网址： https://s.tencent.com/index.html
腾讯安全零信任解决方案网址： https://cloud.tencent.com/solution/zero-trust
腾讯安全零信任ZTAC产品网址： https://cloud.tencent.com/product/ioa
邮箱： stevenyzhou@tencent.com