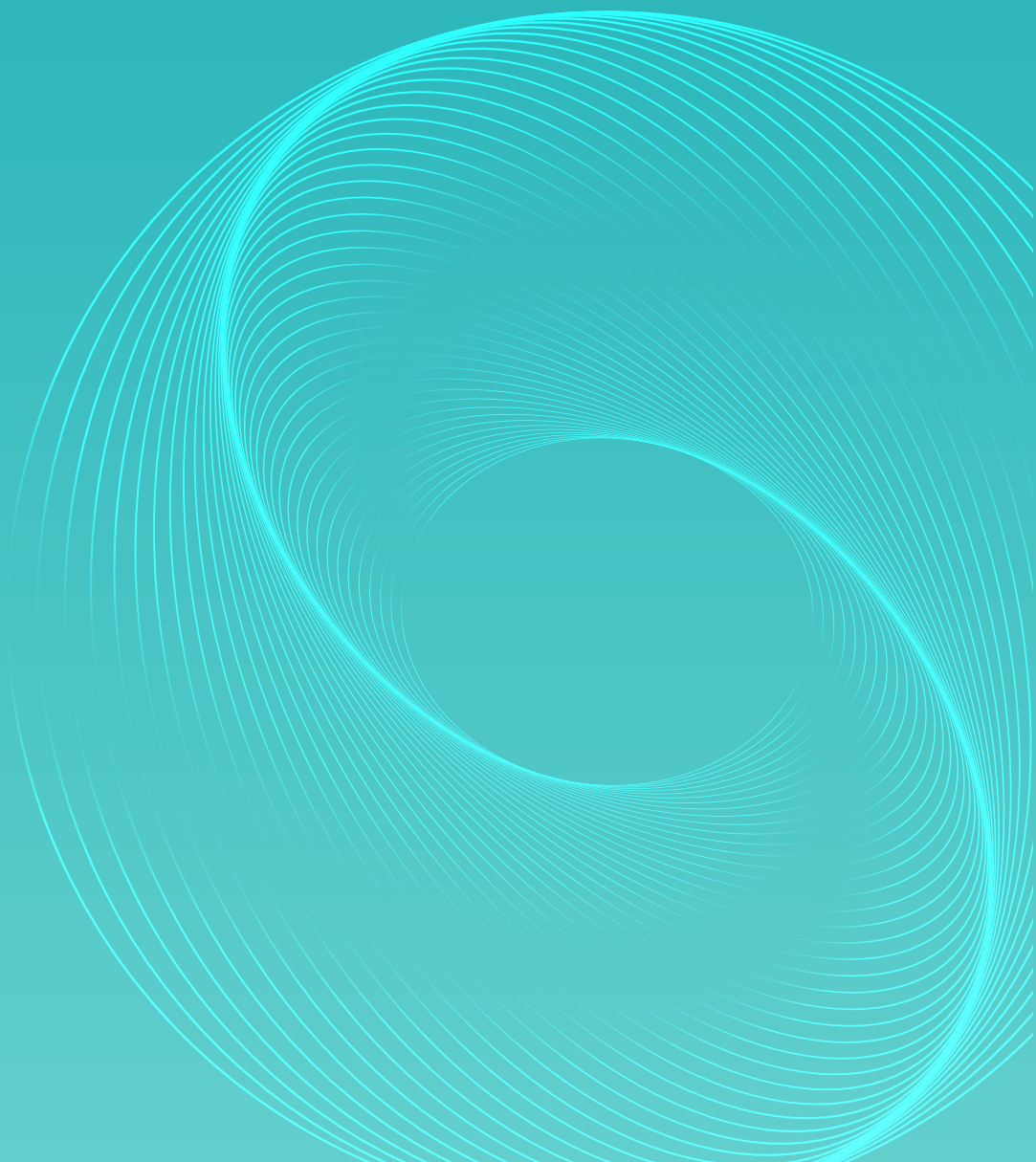
网宿科技 | 网宿安全

网宿安全 · 2023版

零信任安全白皮书



目录 CONTENTS

第一章 严峻的网络威胁态势

1.1. 传统边界模型面对挑战

随着云、大数据、移动互联网、5G、IoT等技术的快速发展，日趋开放和复杂的网络边界已经成为互联网安全的重要挑战。传统的网络边界注重建设多重防护设施，难以应对有组织的、武器化的、以数据及业务为攻击目标的高级持续攻击，仅仅依靠传统边界防护难以应对从身份、权限、系统漏洞等多维度的攻击向量，现有的传统基于内网边界防御的框架已无法因应当下全方位网络异构多样化的挑战。整个新冠疫情时期宣告着远程办公时代的全面到来，无论大型还是小型企业，迅速因应变革工作环境，整个世界都转向线上活动，大量员工远程办公、外包协作、三方合作伙伴、供应链协同，这一切导致线上的网络和业务、数据交互快速增长，其迁移速度和规模十分惊人，多样化的人员、设备、分支、地域间的互联与业务数据访问带来更多的网络边界敞口和安全控制风险。工业OT领域的风险也不可忽视，工业控制系统由于设计之初没有考虑到海量异构设备以及外部网络的接入，随着物联网开放性日益增加、远程监控和远程操作加快普及，网络攻击者更容易利用系统性漏洞和运营薄弱环节发动入侵攻击，一旦成功即可造成多达数十亿台设备的集体沦陷，导致生产业务中断、数据被加密和窃取。从云化到Shadow IT(影子IT设施) 到ICS（工业控制系统），均在工业4.0时代快速就位并准备好迅速扩张，这种转变背后潜在着巨大的网络风险，因为随之而来的就是网络暴露面大大增加。

概括而言，传统网络安全类似物理安全的做法，通过堆叠安全设备构筑组织内网边界，数据和业务均放置在企业内部IDC，假设坏人在外部、内部只有好人，护城河式防御针对的是入向威胁。随着移动业务快速扩展，物联网、车联网、智慧城市的持续发展，资产防护的安全边界越来越不清晰，传统的边界防护架构越来越显得力不从心，传统的边界安全主要存在的问题如下：

1、旧有VPN访问模式，不可避免漏洞频发，由于其服务暴露在互联网，采取偏静态化的控制机制，黑客易于渗透，通过劫持边界内的设备并横向移动攻击企业应用、关键基础设施和敏感数据；
2、随着使用自带设备（BYOD）越来越普遍，设备不受企业管控，成为企业安全建设中效率成本与强安全管控的矛盾点，不安全的设备在内网接入和接入内部敏感业务系统，引入不可控风险；
3、远程办公兴起和普及，2020年开始的疫情大大推动了这一进程，用户接入位置不限于企业内网，企业迫切需要随时随地快捷流畅、安全可靠的远程访问模式；
4、随着数字化转型发展，外包人员、合作伙伴、供应链上下游均需要接入不同类型的业务应用，连接人员身份、设备多样化，而配套的安全控制机制十分薄弱；
5、企业的业务资源除了部署在传统数据中心，也在不断向外部云资源扩展，包括PaaS、IaaS和SaaS的广泛应用。传统边界安全网络设备无法很好地保护企业的云上应用资源，对于云迁移的企业，需要统一保护处于企业内部、公有云上的私有应用和SaaS应用。

传统上，大多数网络和安全架构都是由企业主导设计的，数据中心作为访问需求的目标焦点，支持相对静态的用户。但数字化转型推动了对新数字功能场景的多样化需求，现在有更多的用户、设备、应用、服务需要连接交互，并且数据同时分布在企业内部外部。原来的基于一系列企业IDC边界外围安全设备的网络安全设计，已经不再满足现代数字业务的动态、泛化地域和其混合办公、协作模式的诉求。旧边界必须转变为一组以用户

和应用为中心的融合功能，并在企业需要的时间和地点进行实施支持，即动态创建的基于策略的边界控制。

1.2. 数据安全与隐私合规

近年来，中国网络安全立法进程加快，合规监管深入行业内部。网络安全不再局限于个人和企业的自身防护，开始成为涉及各行业产业链乃至国家安全的重要问题。

2022年，中国颁布多部与网络安全相关的政策法规，进一步推进国家网络、数据安全体系和能力建设，强化网络安全、数据安全和个人信息保护，从多个维度完善了安全合规要求与标准，筑牢国家数字安全屏障，为网络安全技术与产业发展提供指引。随着《网络安全法》、《数据安全法》、《个人信息保护法》等一系列基础性法律法规落地，中国已建立起一套基本的网络安全法律合规框架。

据全国信息安全标准化技术委员会发布的《2022年网络安全国家标准需求清单》，清单共包含34项标准，其中制定标准20项，修订标准14项。涉及重要数据处理、关键信息基础设施安全评测、网络安全保险、网络安全服务能力等方面，针对三部关键上位法的体系化标准、规范支持实施已经全面展开。

2022年2月，新修订的《网络安全审查办法》实施，将原来的“数据处理者”变更为“网络平台运营者”，连同关键信息基础设施运营者作为网络安全审查的规制对象，要求网络平台运营者开展数据处理活动，影响或者可能影响国家安全的应进行网络安全审查。其中，明确规定掌握超过100万用户个人信息的网络平台运营者赴国外上市必须申报网络安全审查。

针对数据出境专项问题，2022年7月，国家网信办公布《数据出境安全评估办法》，并于2022年9月1日起施行。《办法》规定了数据出境安全评估的范围、条件和程序，为数据出境安全评估工作提供具体指引，明确了数据处理者向境外提供在中国境内运营中收集和产生的重要数据和个人信息的安全评估适用。《办法》规定，数据处理者向境外提供重要数据，关键信息基础设施运营者和处理100万人以上个人信息的数据处理者向境外提供个人信息、自上年1月1日起累计向境外提供10万人个人信息或者1万人敏感个人信息的数据处理者向境外提供个人信息，以及国家网信部门规定的其他情形，均需申报数据出境安全评估。此外，《数据出境安全评估办法》还要求数据处理者在申报数据出境安全评估前，应当开展数据出境风险自评估，其中重点评估的事项包括出境数据的规模、范围、种类、敏感程度等。

云上数据安全方面，全国信安标委发布《信息技术 安全技术 公有云中个人信息保护实践指南》7月15日发布，自2023年2月1日实施。同期，《信息安全技术关键信息基础设施安全保护要求》国家标准获批发布，《保护要求》规定了关键信息基础设施运营者在识别分析、安全防护、检测评估、监测预警、主动防御、事件处置等方面的安全要求，将于2023年5月1日实施。

同时，各地也纷纷针对数据安全提出法规和政策指引，强化《中华人民共和国数据安全法》、《中华人民共和个人信息保护法》等上位法的要求，强化属地监管和安全要求：

（1）浙江省发布《浙江省公共数据条例》强调个人信息安全的保护，将于3月1日执行，《条例》共五十一条内容，明确提出打造公共数据平台，建立公共数据共享机制，构建公共数据有序开放制度。这是国内首部以公共数据为主题的地方性法规，也是保障浙江省数字化改革的基础性法规。

（2）广东省发布《广东省公共数据安全管理办法（征求意见稿）》，强调公共数据的安全性，《征求意见稿》共六章三十二条，进一步加强了数字政府公共数据安全管理，规范公共数据处理活动，促进数据资源有序开发利用，保护个人、组织的合法权益。
（3）深圳发布《公共数据安全要求》领域标准，将数据安全与网络安全等级保护要求有效结合，为《深圳经济特区数据条例》的落地提供坚实指导。
（4）《四川省数据条例》，《条例》共有八章七十条，包括总则、数据资源、数据流通、数据应用、数据安全、区域合作、法律责任和附则，自2023年1月1日起实施。
（5）《厦门经济特区数据条例》发布，《条例》为了规范数据处理活动，保障数据安全，保护自然人、法人和非法人组织的合法权益，培育数据要素市场，促进数据有序流动和开发利用。

新兴行业市场的网络安全风险，尤其互联网、云平台、数字化高度依赖和集中的各行业，也已经快速推进网络与数据安全的行业标准的体系化，以规范化的标准强化行业内的安全经营和风险控制。

2022年12月，工信部发布《工业和信息化领域数据安全管理办法（试行）》，《管理办法》作为工业和信息化领域数据安全管理顶层制度文件，共八章四十二条，重点解决工业和信息化领域数据安全“谁来管、管什么、怎么管”的问题。

2022年2月25日，工信部印发《车联网网络安全和数据安全标准体系建设指南》，聚焦车联网终端与设施网络安全、网联通信安全、数据安全、应用服务安全、安全保障与支撑等重点领域。

图1 车联网网络安全和数据安全标准体系框架图

2022年4月8日，工业和信息化部等五部门联合发布了《关于进一步加强新能源汽车企业安全体系建设的指导意见》，该《意见》强调，加强网络安全防护，企业要依法落实关键信息基础设施安全保护、网络安全等级保护、车联网卡实名登记、汽车产品安全漏洞管理等要求。对车辆网络安全状态进行监测，采取有效措施防范网络攻击、入侵等危害网络安全的行为。

2022年8月29日，国家卫生健康委、国家中医药局、国家疾控局联合发布《医疗卫生机构网络安全管理办法》。办法共六章三十四条，涉及网络安全管理、数据安全管理、监督管理、管理保障等内容。

2022年10月，民航局印发《关于民航大数据建设发展的指导意见》，《指导意见》阐明民航大数据建设的6大主要任务和14个方面具体工作任务，要求加强法规体系建设、构建数据标准体系、提升数据管理水平、加强数据质量管理、推进数据要素流通、加强民航数据网络建设、强化安全管理责任、提升安全保障能力等。

1.3. 网络攻击愈演愈烈

随着各行业数字化的快速进展，疫情期大大促进了远程办公业务、云化服务的广泛应用，同时也使得组织的安全敞口变大，在缺少体系化防御措施的情况下，在各个行业网络攻击的态势更趋向严重。据SonicWall在2023年发布的网络威胁报告，在整个2022年度，恶意软件、网络入侵、加密劫持和物联网恶意软件出现明显增长，其中，入侵尝试高达6.3万亿次，恶意软件攻击达55亿次，而针对物联网的恶意软件攻击出现87%上升幅度，达1.12亿次。另外，位于业界No.1关注热度的勒索软件攻击，虽因为俄乌战争等因素出现下降（业界分析勒索软件攻击中一些政府支持的团体因为制裁措施被迫收缩），但是仍然高达4.93亿次攻击，且针对关键的医疗健康、金融、教育领域分别出现8%、41%和275%的上升。

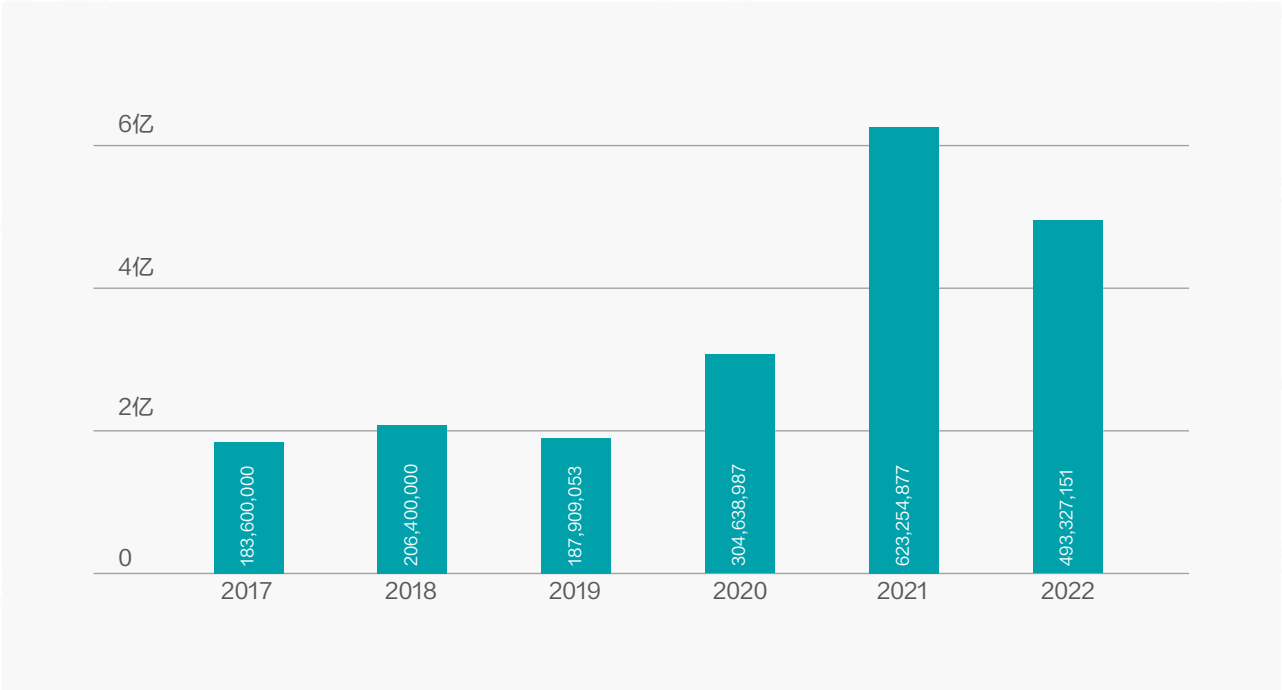


图 2 全球勒索软件攻击数量趋势

网络威胁实施者利用不断变化的局面，抓住机会采用各种手段和方法，成功渗透进世界各地的组织和企业中，攻击者瞄准政府、金融、能源、医疗等承载重要社会职能、拥有大量数据资源的行业信息系统作为实施攻击的“高价值”目标，一旦得手往往造成重大损失，勒索软件攻击是对组织形成最大威胁的攻击，窃取敏感数据且阻断运营，如下仅列举部分近年来造成恶劣影响的勒索软件网络攻击和数据窃取事件。

- 2022年12月，蔚来汽车公司收到外部邮件，发件人表示拥有大量蔚来内部数据，并以泄露数据勒索225万美元（当前约1570.5万元人民币）等额比特币。经初步调查，被窃取数据为2021年8月之前的部分用户基本信息和车辆销售信息。

- 2022年6月，澳大利亚交易巨头ACY证券暴露了60GB的用户数据，总部位于澳大利亚悉尼的贸易公司ACY Securities (acy.com) 在网上公开了大量用户和企业的个人和财务数据供公众访问。

- 2022年6月，富士康证实其墨西哥一家工厂在5月底遭遇了勒索攻击，黑客窃取了100GB的未加密文件，并删除了20TB至30TB的备份内容，并索取1804比特币（约合人民币2.3亿元）赎金。该事件极大程度上干扰了富士康的生产节奏，其影响波及富士康整体上下游产业链。

- 2022年4月，哥斯达黎加多个政府机构遭到Conti组织的勒索网络攻击，政府程序、签名和邮票系统被破坏，财政部的数字服务无法使用，这影响了整个“生产部门”，总统罗德里戈·查韦斯（Rodrigo Chaves）宣布全国进入紧急状态。

- 2022年2月底，全球最大的轮胎制造商之一普利司通遭受LockBit勒索攻击，普利司通公司承认其一家子公司在2月份遭遇勒索软件攻击，导致其在北美和中美地区的计算机网络和生产中断了约一周时间，攻击者威胁从普利司通公司系统中删除信息，并将这些信息予以公布，该组织提供给被勒索的公司一个在发布数据之前付款窗口，并添加了一个倒计时器，以此产生戏剧性效果。

- 2021年11月，丹麦风力涡轮机巨头维斯塔斯（Vestas WindSystems）于19日前后遭到网络攻击。此次事件中公司数据被挟持和加密，并且遭到勒索高额赎金，事件导致了尚未明确的数据泄露，部分受到攻击的设备正在恢复中，攻击事件发生后，维斯塔斯的股价跌至两周低点。

- 2021年5月，美最大成品油管道运营商科洛尼尔遭DarkSide组织勒索软件攻击，导致美国东部沿海主要城市输送油气的管道系统被迫下线，成品油供应中断，美国于当地时间5月9日宣布进入国家紧急状态。科洛尼尔支付约500万美元（约合人民币3200万元）的加密货币勒索赎金，获得暗面组织提供的勒索软件解密工具，但由于该工具恢复数据速度缓慢，科洛尼尔已采用备份数据进行系统恢复。

各组织在网络基础设施和业务被攻陷，多与网络暴露、身份和访问控制的漏洞及内部泄漏等相关，当下，应用、用户、业务和数据大量迁移到传统内网边界之外，传统的固化边界安全的有效性降低，企业无法依靠基于固化边界的安全工具来保护其内部敏感业务和数据，边界内部，外部引入设备数量、类型也在快速增长，移动终端、远程办公、企业业务在内网和公有云同时部署，这样的趋势已经破坏了企业使用的传统固化边界安全模型。急需要一种新型的安全模式提供高强度、一致化和兼具灵活度的访问边界安全构建。

第二章 零信任安全框架和标准

2.1. 零信任安全理念框架

零信任网络访问ZTNA（Zero trust network access）在身份安全、设备安全、传输安全和数据安全上保障企业资源的安全接入，首先在网络边界模糊的趋势下给业务资源提供隐身衣，使网络黑客看不到目标而难以针对性发动攻击，在访问准入控制上，充分校验接入者身份合法、设备符合安全基线，并动态评估接入者行为风险来控制访问权限。从安全原则上讲，零信任首次颠覆了传统网络安全里面的重要前提：“缺省信任”。而从技术本质，零信任是在一个不可信的开放网络环境下，以身份为中心，通过动态的访问控制技术，围绕核心保护对象，遵循最小权限原则，构筑端到端的逻辑身份边界的安全体系。

零信任概念自2010年由知名咨询机构Forrester提出，直到2017年，谷歌对其内部网络进行基于零信任安全的改造成功后，验证了零信任安全模型在大型复杂网络环境中的实际落地可行性，各界开始关注零信任理念和实践，出现越来越多的零信任产品、平台及标准规范，2020年Covid-19疫情爆发带来远程办公需求激增，将零信任热度推向了一个新高度。

零信任安全访问模型，将传统的基于边界“城堡与护城河式”的安全管理方式，转变为按需在单个资源与客户之间构建信任的安全管理方式。在零信任模式下，用户将基于经不断重新验证的内外部因素建立可信连接，遵行零信任关键理念原则：

（1）不自动信任网络的安全性(内网≠可信)；
（2）对任何接入系统的人和设备都进行验证；
（3）每次访问都要进行身份验证和行为审计；
（4）细粒度访问控制策略Need-To-Know(最小权限原则)；

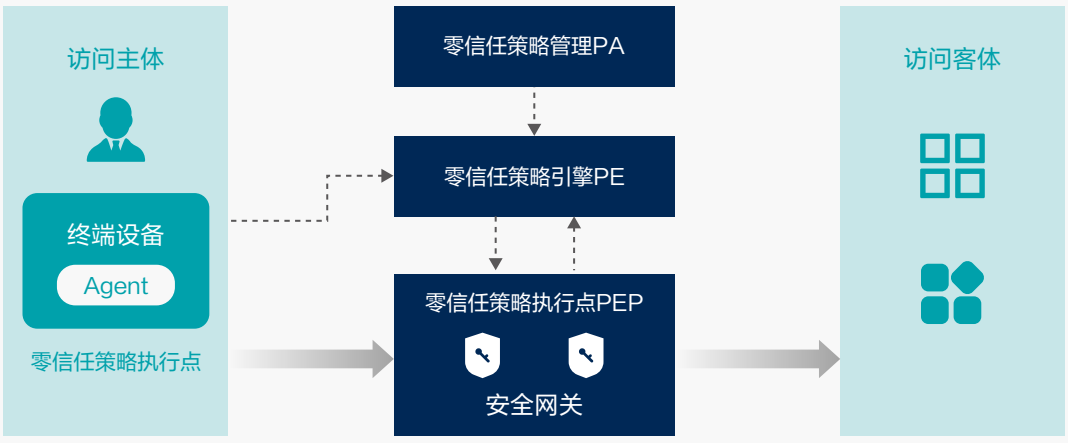


图 3 零信任访问控制策略引擎

对当前愈演愈烈的网络攻击，部署零信任已然成为企业和组织IT安全架构转型中重要一环，在实施过程中，它是对网络生态系统的边界模糊的有效应对，它认为组织架构内每个组件都有弱点，每一层设施均需要保护。而得益于近期计算能力的提升，零信任架构已经在广泛的行业中得到应用。零信任不仅仅是一种技术修复，它是一套相互交织、洞悉敌对活动及相关业务风险、并致力于消减风险的方案集合。

（1）零信任是IT安全架构和行为模式的转变，它假设安全风险无处不在，通过各种方法加大攻击活动渗透到组织网络的难度。

（2）零信任核心理念是实践最小权限原则，在整个网络中建立强有力的验证措施，以确保只有具有权限的访问者才能以适当的方式接入相应应用和数据。

（3）零信任构建软件定义的安全边界，当今云大物移网络架构演变迅速，传统边界防御机制趋于失效，零信任模型提供了一种解决方案，它要求对所有连接网络的用户、设备、应用进行认证和授权，在访问过程中进行持续验证。

（4）零信任核心是了解关键数据位于何处，以及谁有权访问这些数据，它在整个网络中建立强有力的验证措施，以确保只有具有权限的个人才能以适当的方式访问这些数据。

（5）零信任使用基于持续风险评估的实时访问决策替换简单的、静态的实体验证，在网络连接活动的整个周期内持续监测评估和干预处置。

（6）零信任方法相关的原则（包括实施MFA以及最少特权原则）有助于降低组织面对主要攻击类型的脆弱性，如实施MFA大大增加攻击者接管帐户的难度，仅仅盗取静态凭证无法攻破网络。

（7）零信任体系有效阻止黑客入侵后在内网扩散。攻击者可能控制某些脆弱的单点，当其通过已攻击的终端向网络内部更重要系统渗透时，零信任的安全机制可以及时检测到威胁，从而帮助企业将风险控制在最小限度，阻止发生进一步全局渗透攻击的严重后果。

建立零信任安全防护机制，可有效地弥补传统边界防护模式网络暴露面大和解决隐式信任问题。传统网络安全架构最大的缺陷就是过于信任，而零信任架构意味着每个试图访问网络资源的人和设备都要进行验证，其访问控制不仅能应用于用户，也适用于服务器设备与各类应用，以防止不必要的特权，并且将业务资源从互联网暴露面上进行隐藏，从而降低恶意软件的渗透风险。针对办公场所环境，零信任假定网络本身是不安全的，当用户、设备和应用程序连接网络时，需要对网络进行保护，任何有漏洞的设备均要被屏蔽或分段，以降低它们被网络犯罪分子发现和利用的可能性。实现这一目标，需要掌握使用网络的所有已知实体以及设备的安全状态，当设备试图连接网络时就需要在对请求做出访问控制决策。传统的信任模式所依据的属性通常很有欺骗性，并不实时了解它们是否存在漏洞或已遭恶意利用。企业在向零信任过渡的过程中，信任决策必须根据许多因素来做出，比如身份和行为，而且需要根据设备状态、行为和任何不断变化的环境因素进行持续验证，支持通过限制原始网络访问权限或完全切断其访问路径来应对新查明的威胁和漏洞。

2.2. 零信任安全核心价值

在企业的整体业务、安全需求大框架下，企业越来越多地追求零信任战略转型，零信任网络模型用持续评估取代隐式信任，以风险/信任级别的计算和判断在访问边缘上执行控制策略，零信任体系结构将原来静态授予的显式信任调整为围绕交互上下文的动态授权，同时对企业IT复杂性提供可管理统一平台，实现真正以零信任原则敏捷地支持数字业务转型工作的需要。

采用零信任模型后，在动态边界处理每一次访问请求时都对用户、设备、容器、网络和应用的安全状态进行验证，从而获得更全面更深入的可见性。通过细分资源粒度、数据敏感度以及仅批准必要权限和流量的方式最小化控制访问权限，收缩企业的网络攻击面。无论用户身处何处，正在使用哪种终端设备，将应用程序部署在本地还是云，他们都可以获得完全一致且效果更好的访问体验和安全防护能力。

从安全防御角度，今天各类网络攻击技术快速进化演变，新的恶意软件变种和攻击策略层出不穷，经过精心设计的攻击模式致力于避免被安全软件检测到。普通安全检测设施即使只是很小的延迟检测，也可能为潜在的网络入侵、窃取数据、勒索攻击加密文件提供足够的时间。当企业组织以事后审计方式检测到恶意的攻击行为时，往往攻击行动已经实现其全部或部分破坏目标，虽然仍有机会能够遏制住攻击进一步的扩散，但是此时想阻止全部攻击往往可能已经太迟了。对于企业组织而言，预防和检测、实时阻止显得尤为重要，零信任通过提供在网络层面的暴露面收敛、身份MFA强校验、凭证密码加固、恶意访问威胁检测和设备环境安全感知、行为异常识别等能力，能够在恶意攻击的探测、远程连接阶段就进行安全防护和及时干预。

根据IBM的2022年度数据泄露成本报告，与没有部署零信任的企业相比，部署零信任的企业可将攻击的平均损失降低95万美元。对于没有实施零信任框架的企业而言，数据泄露的平均成本为510万美元，而拥有零信任框架的企业则为415万美元。随着企业的零信任计划日趋成熟，数据泄露成本可大幅降低20.5%。企业零信任框架越成熟，就越能更好地保护可被攻击者利用的潜在破坏性的威胁面，从而降低安全事件的发生可能性和平均成本。根据该报告，早期采用零信任的企业平均数据泄露成本为496万美元，而零信任实施成熟期的企业可将数据泄露成本进一步降至345万美元，平均数据泄露成本降低多达151万美元。部署零信任可为企业平均节省28.7%-42.3%的安全事故成本。零信任已经成为全球企业、政府和网络安全产业公认的应对已知和未知威胁、对抗不确定性的最有效的“下一代安全防御”。

除了降低数据泄露经济成本外，零信任还将给企业带来业务敏捷性和竞争力的显著收益。成功的零信任方案可以为企业带来的巨大的战略性价值：

1、提高组织敏捷性，提供面向业务需求的安全能力
2、更安全的云迁移
3、更好地支持数字化转型战略
4、更准确地盘点基础设施资产
5、改进安全运营中心的监控和警报
6、安全地进行远程办公，改善终端用户体验
7、统一化、简化安全策略的创建和管理
8、对抗攻击和失误，防止数据丢失或泄露

第三章 零信任典型应用场景

3.1. 安全办公业务访问

主要场景是内部员工远程接入企业的分散在内外部平台的各类业务应用，需要有安全可靠、流畅的访问通道和访问策略控制平台。

- 远程办公：人员差旅、业务外拓、居家办公等情况下访问企业OA、邮件等业务系统
- 混合接入：企业业务系统分布在总部IDC、公有云、多地托管数据中心
- 云服务：接入企业部署在云平台的各类业务系统和SaaS化服务

业务痛点：

- BYOD设备风险，居家和移动办公需要远程接入，BYOD设备大量使用，此类非企业强管控设备为企业网络和业务引入未知风险
- 传统VPN风险，VPN服务暴露在公网容易受到黑客的扫描和渗透攻击，传统VPN设备层出不穷的漏洞也带来极大安全风险
- 恶意行为，内部人员、三方蓄意对信息系统进行目的性破坏、盗窃/损毁机密信息数据
- 传统VPN网络依赖互联网线路，设备长连接，传输不稳定、易掉线、访问体验差
- 用户体验差，多数据中心、多域接入时需要频繁切换用多套VPN，且管理复杂度高

解决方案：

接入方式： 零信任安全接入，针对用户使用各类型PC和移动设备，提供统一的用户资源应用访问门户

访问方式： 提供用户就近接入高速云节点，快速安全接入企业云上、本地业务资源

安全机制：

- 通过网络隐身及分布式云防护能力抵御网络攻击隐患，先认证再连接，不对外暴露企业业务资源，规避嗅探和入侵
- 持续验证动态授权，MFA多因子验证保护账号安全，最小化权限访问控制，异常行为识别控制，检测和抑制外部攻击和内部恶意行为
- 统一虚拟应用，可集成内部自建应用系统和SaaS类应用系统，访问便捷并提供统一的策略管理
- 提供安全DLP能力，针对访问关键业务和敏感数据，限定访问过程，通过多种方式进行隔离保护，防止数据泄露
- 提供流量可见性，过滤威胁流量，保护企业的IDC业务资产安全，对云上应用访问过程进行审计管控
- 基于全球的云加速传输网络，提供用户就近接入访问业务，保障访问速度和稳定性

3.2. 三方人员安全接入

主要场景是各类外包团队、三方运维人员和上下游合作方的网络接入和业务访问，三方接入存在人员流动性和脆弱安全管理状态，需要通过强化访问控制来保护企业的业务平台和数据安全。

- 三方外包：驻场、远程的外包研发，工程等类人员访问内部业务系统
- 运维访问：供应厂商或者外部的运维、维修人员访问服务资源后台
- 上下游访问：供应链上下游访问企业的供应链、商户平台等业务系统
- 合作伙伴：业务合作伙伴访问企业的生态合作业务平台

业务痛点：

- 对外开放服务业务多，各类系统暴露于公网上，易遭受外部网络攻击入侵
- 账号混用滥用现象常见，账号安全性差，易被不法利用
- 外方恶意人员蓄意对信息系统进行目的性破坏，盗窃/损毁机密信息数据、篡改数据
- 流动人员广泛使用BYOD设备，安全性无法保障

解决方案：

接入方式： 零信任平台统一接入，通过界安全网关访问业务系统

访问方式： 提供各类协议的应用资源访问，用户安全接入业务资源和管理后台，就近高速网络接入访问体验

安全机制：

- 通过网络隐身抵御互联网攻击隐患，业务收入零信任防护平台后方，不对互联网络暴露企业网络和资产
- 安全设备保障，策略化环境基线检测，设备授信可控绑定，使用MFA强化验证身份，保障用户合规接入业务资源和后台服务
- 持续验证设备和用户的安全基线，动态评估控制授权，识别用户异常行为并实时管控处置，多角色权限细化管理和自动化评估限制接入
- 深度检测访问连接的网络流量，识别威胁攻击并即时防御处置
- 提供DLP手段进行数据安全保护，针对访问关键业务和运维中访问关键系统和使用敏感数据的场景，限定在隔离环境中防止数据泄露

3.3. 数据防泄露保护

保护组织数据的安全，不仅需要在企业边缘构建防护体系来阻止入侵和窃取，同时也需要提供足够的内部泄露防御手段和追溯机制，防止敏感数据从各种管道脱离企业控制范围。

- 研发：研发人员访问内部业务系统，本地设备存留大量文档
- 设计：设计活动产生的各类电子图纸数据，本地存放，并且常常利用协作平台
- 数据采录：加盟营业厅、业务外拓等情况下采集客户敏感数据，上传管理平台

业务痛点：

- 本地设备存放大量企业关键数据，一旦设备被入侵，数据泄露损失严重
- 采录系统暴露于公网上，易遭受外部网络攻击入侵，本地存放易泄露，同时也存在恶意盗取存储数据的可能
- 研发设计工作访问协作平台，此类数据类管理平台敏感性高，是企业的核心知识财产，存在恶意大量盗取文档的风险

解决方案：

接入方式： 零信任统一安全接入，安全DLP组件能力提供数据泄露防护

访问方式： 信任安全客户端软件在本地设备上开启安全隔离的访问环境，提供用户安全接入业务资源和管理后台，安全空间数据隔离和网络访问受控，阻断外发流转通道

安全机制：

- 隐藏业务系统，通过网络隐身抵御互联网渗透、数据勒索攻击和窃取的隐患
- 隔离互联网威胁访问资源，防范钓鱼入侵和数据窃取
- 识别保存、流转的数据，并在分级分类标签化后跟踪保护
- 设备本地隔离关键数据，数据加密并控制外发
- 持续验证接入人员和设备安全状态，动态授权访问业务，识别和阻止超量访问、下载等异常用户数据访问行为
- 提供水印、防拷贝等数据DLP安全防护手段

3.4. 物联网安全连接

物联网设备在各种企业经营业务中迅速发展，各类物联平台承载连接大量终端设施，其控制连接和数据传输关系着企业运营能力与安全合规，而IoT终端设备种类繁多异构化严重，需要有端到端安全保护和平台化安全访问保护。

- 生产制造：工业物联网设备、联网机车、AGV小车、智能仓储
- 能源电力：充电桩、巡检无人机、风力和太阳能发电站点
- 汽车行业：车联网平台、车机监控
- 其他：安防、环保、物流等场景下无人机和IoT设备联网平台

业务痛点：

- 现象：物联网失陷导致生产停顿，物联设备失控导致内部业务平台被渗透入侵破坏，大量物联设备被劫持成为僵尸网络一部分
- 原因：IoT设备系统、软硬件多经过裁剪，原始自带的安全防护功能较弱，物联设备业务体系异构化、通讯协议繁杂，接入管控困难，物联网关、平台暴露在互联网中易遭扫描和攻击

解决方案：

接入方式： 物联网胖终端上可植入SDK提供零信任安全接入保护，瘦终端则在安全网关侧提供统一访问控制

访问方式： 信任安全客户端软件在本地设备上开启安全隔离的访问环境，提供用户安全接入业务资源和管理后台，安全空间数据隔离和网络访问受控，阻断外发流转通道

安全机制：

- 网络隐身防止扫描业务平台，抵御互联网攻击隐患，不对外暴露物联网关和平台
- TLS隧道加密流量传输，保障互联网设备上行传输数据安全和指令传输安全
- 提供物联设备边缘安全代理，IoT设备唯一身份绑定，设备安全状态监测
- 提供安全可视化能力，实时监测和识别异常流量和行为，动态调整访问权限，隔离可疑被劫持设备以阻断风险扩散

3.5. 一机两用安全办公

政务、金融等行业，内部政务和关键业务网络要求与互联网采用严格的隔离措施，严禁将任何设备直接连接双网，但是仍然存在大量跨网连接访问的情况，导致互联网威胁引入内部网络中，带来巨大的安全隐患。2022年正式发布了政务外网使用零信任沙箱管控机制支撑一机两用安全规范，安全沙箱限制访问连接政务外网，保护内部业务和数据的安全。

- 双网隔离：人员办公接入内部网络，同时自动强制隔断互联网连接
- 移动办公：业务人员从互联网远程访问内部业务系统，进行OA、邮件办公等
- 外部业务：行业员工进行外部拓业、执法，连接内部业务平台，采录上传敏感信息

业务痛点：

- 设备同时连接互联网，一旦设备被入侵，跳板连入内部网络可能造成入侵
- 黑客借由暴露在互联网的业务入口实施攻击，面临着开放环境带来的安全挑战
- 内部系统涉及到大量公共数据、政府机密等敏感信息，发生数据泄露会造成很大的影响

解决方案：

接入方式： 零信任安全平台统一接入，安全沙箱提供数据防护和双网隔离

访问方式： 在本地设备上开启安全隔离的访问环境，提供用户安全接入内部关键业务资源，限制互联网连接，内部业务数据隔离和保护在安全沙箱，阻断外发流转通道

安全机制：
- 隐藏业务系统，通过网络隐身抵御互联网渗透风险
- 安全沙箱提供强隔离环境，不允许访问互联网，仅可连接内部业务网络和数据
- 设备本地隔离保护业务数据，加密存储并限制外发

第四章 网宿零信任安全实践

4.1. 网宿零信任平台能力

网宿安达SecureLink产品自2019年全面推向市场，是国内首个基于全球高速网络服务能力建设的零信任安全防护平台，以云原生平台提供统一云化服务。

网宿零信任平台遵循CSA标准零信任SDP架构，系统组件包括安全客户端、安全网关和零信任控制台，采用控制面与数据面分离的架构，利用SPA隐身技术收敛网络暴露面，隐藏客户内部网络业务和资源数据，控制中心提供账户管理、认证、授权和审计能力，安全终端提供环境感知能力、接入统一门户和数据泄露防护，安全网关承载所有业务访问流量，识别处置各类威胁攻击，阻断敏感数据流出，通过安全策略引擎综合评估用户身份状态、用户异常行为、设备安全基线、环境风险因子，进而动态控制用户业务访问权限，以强大的动态评估计算引擎和细粒度访问控制策略提供访问接入安全可控的保障能力，保护内部业务和数据访问安全。

动态访问控制引擎

零信任系统中作为中控的安全访问控制引擎，是整个零信任安全控制的大脑中枢，平台通过在用户侧客户端的环境感知能力检测设备安全状态、测算健康值，结合用户认证、访问操作、时空环境状态来分析异常行为和检测攻击入侵，进行用户可信度评级评分，在控制中心的策略引擎进行运算决策，动态管制用户访问权限。

平台提供五类评估策略模型，包括规则、统计、关联、基线和情报模型，从简单的规则式模型到使用智能算法的基线模型，有效支撑在信任评估运算中纳入用户账户、行为、网络、端点设备和接入环境的风险，从而在访问过程中及时识别异常行为、不合规设备或者攻击入侵的风险，动态调整访问权限，阻断或者提升认证强度，保护业务和数据安全。

系统同时支持对用户、设备以评分和评级两种信任评估方式来进行控制，对于细颗粒管控提供有效支撑，平台具备500条模型内置库，开箱即用，并提供专家模式可供用户自行建设更多企业需要的模型，其开放式建模能力可对接任意三方安全设备日志信息，从而进行多维信息综合评估，进而在策略运行评估引擎决策计算，将处置动作指令下发到安全网关和安全终端，执行访问控制动作，如放行、阻断、二次认证、账号封禁等。

全球高速接入网络

网宿全球智能高速线路为用户提供随时随地的就近接入服务，其广泛分布的POP节点覆盖全球160+大中城市，打通各区域运营商线路，提供全面覆盖多地域的高质量网络连接，对于组织分布在全球各地的用户来说，可就近接入该网络从而获得优质的业务访问服务。

平台具备智能选路能力，自动化探测网宿全球POP点路由，实时监测网络变化状况，通过AI算法计算最快访问路径，线路出现拥塞、故障时智能切换。通过路由优化、协议优化、路径优化、数据优化等多种广域网优化技术提高网络速度。平台网络服务可用性达99.95%，网络稳定性比传统VPN方案提升400%。

基于平台底层网络加速的支持，将零信任安全接入与高速网络服务能力高度融合，无论SaaS服务和私有化部署零信任情况下，都能为客户提供加速网络接入，目前此支持能力为全球独家。

强大的网络管控运营，调控保障用户的访问体验，解决时延和丢包问题，为企业提供基于业务、用户级的QOS控制，通过流量特征识别技术DPI，准确识别用户应用类型，基于流量控制策略，保障企业关键人员和关键业务高效支撑。用户级接入网络质量监测，及时发现和处置网络线路故障，保障最后一公里接入质量问题。

网络威胁安全防御

平台为从用户终端到网关层提供全面的网络威胁防护能力，其中，网络流量安全检测、防御能力集成到边缘节点上，安全前移，向用户提供防火墙、IPS入侵防护、安全Web网关安全能力，抵御各类复杂的网络攻击。

同时，在用户设备侧提供安全防护，对设备进行杀毒保护和漏洞扫描、修复。客户端可切换防御模式和采集模式两种，一方面作为独立终端安全防御设备为终端设备提供安全防护能力，可根据终端设备防护需求，采用全面防御或策略防御等多种模式；另一方面作为终端高精度采集探针，采集终端高价值设备信息、安全信息，并输入到零信任安全评估引擎中，实现企业整体零信任安全防御。

网宿云平台支撑国内30%互联网流量，积累大量威胁情报，日常有效威胁库达3000万条规模，可帮助企业屏蔽各类恶意域名和IP，如钓鱼、挂马网站、僵尸网络等，并针对500余万流行病毒、5000余种漏洞利用攻击和1000余种间谍软件防护，是零信任安全网关过滤各类攻击和风险站点的坚实基础。

平台内置网络应用识别库，支持互联网访问安全防护和控制，结合网宿边缘计算和网络能力优势，为互联网访问场景提供安全防护。

数据防泄露保护

网宿零信任平台是业内首家集RBI、SWG和端点安全、和沙箱安全工作空间于一体的SasS化服务平台，在用户侧终端设备、安全边缘网关节点均提供DLP数据防泄露能力，保护企业数据的安全。

安全工作空间在用户侧设备虚拟隔离的安全网络访问和办公环境，满足一机两用的政务、金融等行业合规要求。RBI远程浏览器隔离则提供轻量化Web资源安全访问通道，隔离威胁风险和网络渗透，支持指定URL

目标以RBI方式保护访问过程，提供数据不落地、复制禁止、定制水印等手段保护业务应用数据的安全。

安全网关作为零信任访问的策略执行点和流量检测、转发承载点，以TLS协议加密传输数据流量，具备防篡改、抗重放安全防护能力。提供应用/URL级细粒度访问控制，执行RBAC和ABAC相结合的权限控制模型来确保最小权限原则，防止攻击流量横向移动，深度流量解析识别敏感文件和数据，阻断通过网络外发通道泄露敏感数据。

智能算法机器学习

平台内置UEBA高级用户行为分析模块，基于智能模型评估用户访问信任度，多维度对企业网络风险进行分析定级，其特点包括：

1、威胁模型：对用户行为进行实时的可信建模，多种模型包括基线模型、规则模型，统计模型、关联模型、情报模型和黑名单模型，智能算法识别历史偏离和群己偏离
2、全时空分析：模型不针对孤立的独立事件，而是采用全时空分析方法连接起过去（历史基线）、现在（正在发生的事件）、未来（预测的趋势），同时，也连接个体、群组的行为模式，综合研判人员接入安全风险
3、三方联动：支持与三方安全设备联动，使用三方安全设备的相关安全信息做为输入，更全局地支持用户行为和环境风险的深层次分析
4、评分评级：支持对用户异常行为进行分类并针对性设置扣分值，通过一定加权计算评估用户的信任分值，访问控制引擎依据信任分值对用户进行动态访问控制

云原生弹性平台

基于云原生的平台化能力，根据用户业务发展需要自动化弹性缩扩容，安全能力按需生成和推送，平台具备自诊断和自愈健壮性，自动化运营平台支持高效服务工作流。

平台高可用，集群化部署安全网关保障高可用性，POP节点、网络链路均采用多级冗余式保护。

提供可视化分析、审计能力，全网服务威胁捕捉、情报汇聚，阻断入侵流量，洞察追溯安全事件，平台提供统一的用户入口体验，高速的网络接入能力保障业务敏捷性。

可视化智能集中运维平台，管控全局网络资源，监测接入用户、设备和服务业务的安全状态，实现安全智能化分析和可视化运营，直观展示和监测全网拓扑、路由、实时带宽、网络健康情况，同时提供运营监控大屏、安全分析统计报表等。

4.2. 零信任安全建设框架

4.2.1. 远程办公访问

网宿安达SecureLink通过对网络空间中用户、设备、网络、应用、数据的安全连接保障和访问控制，建立可视化、自动化、智能化的零信任安全防护体系，其身份可信、终端可信、行为可信的核心控制特性能力，以及传输加密、边缘防护、网络隐身的平台安全能力，为企业搭建统一安全访问体系，支持用户使用任意终端在任意位置、网络环境中安全、高效、可靠、便捷地访问企业资源和进行日常办工。

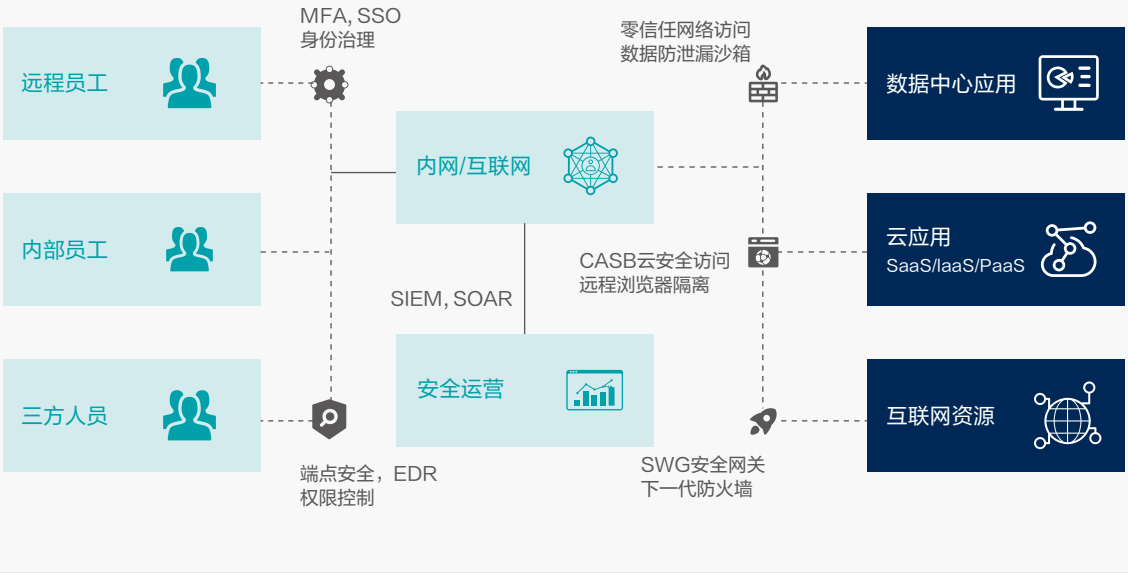


图 4 多方接入的安全控制

1、网络隐身，保护数据中心的应用和云上服务，减少应用暴露面，限制网络横向移动，抵御扫描攻击入侵

2、访问认证MFA，有效抵御暴力破解攻击，提供访问安全度和便利性。高强度的身份认证，包括基于用户、设备、应用、数据、用户行为进行可适应的安全策略控制，触发双步认证，确保合法用户访问

3、身份生命周期控制，识别僵尸账号并自动化封禁，对账号支持设置有效期，基于RBAC管理严格限制可及资源和网络，精准匹配业务需求，收敛业务连接时间和范围

4、应用资源发布，支持各类CS/BS应用发布并保护访问，同时支持RDP/SSH访问，有效支撑各类远程访问办公和安全运维场景

5、多层访问通道，提供无端方式，用户可直接由通用浏览器访问非敏感业务，提供通过RBI访问受保护Web服务，通过安全客户端保障端侧可感知、可控制的安全性，通过安全工作空间提供安全隔离的业务、数据访问环境

6、终端安全AllinOne，提供杀毒、EDR统一客户端，具备准入控制、杀毒防护、漏洞保护、外设控制和零信任接入能力，用户桌面无须安全各类客户端，减轻运维管理复杂度，提升用户体验

7、提供智能信任评估引擎，实时检测用户和设备的状态、网络连接信息、访问业务上下文、访问时空环境等多维数据，根据风险识别动态调整用户的访问权限

8、实施UEBA高级行为分析，使用UEBA智能模型机制来检测用户、设备的异常活动，自动化响应其威胁，告警和阻断，保障应用业务的安全，探测内部威胁、数据泄露、失陷设备和被盗凭证，追踪用户行为并进行信任评估，全方位防护业务访问安全

9、全球网络就近接入，分布式安全网关实现就近接入和就近回源访问，全球范围多运营商底层加速网络互通，解决时延和丢包问题，保障用户的业务访问体验

平台通过系统化机制保护用户安全访问内部业务和数据，通过基于用户身份的认证、鉴权机制，确保合法用户才能接入内网。针对用户登录或敏感数据访问、敏感操作等场景，支持多因子认证（MFA）方式增强用户身份鉴定能力，提供短信、TOTP等主流二次认证方式。用户使用终端设备连接过程中，按照安全基线要求实时监测终端设备的健康状态，判断终端是否授信准入，并联动三方安全端系统保护用户设备安全性，防止失陷设备成为攻击跳板。平台对用户行为进行持续评估，一旦检测到的异常行为、越权行为、威胁风险、终端不合规等异常即调整信任评分，根据检测结果动态调整用户的访问权限。

在用户使用和运营管理上，提供易用的体验和便捷运维。用户访问直接使用统一门户接入发布的权限范围内业务资源，提供自助诊断工具解决网络、准入等问题，支持SSO单点登录，用户便捷访问全量支持的应用，运维管理员通过可视化分析和监测全局掌握业务访问趋势和风险状态，统一的安全策略管理和细化的访问日志审计、多维度分析报表和监测大屏提供为安全运营提供有力支撑。

4.2.2. 网络攻击防护

平台具备体系化多层防护机制，首先利用网络隐身技术构建一张隐形的网络，只对认证授权的可信任用户可见，对其他人完全不可见，并且对该用户访问应用的行为进行严格控制和记录。这种模式很好地解决资产和应用暴露在公网的问题，同时也可以增强现有内网办公的安全性。由于网络资产被隐藏，攻击者无法嗅探、扫描到企业内部的服务，无法利用内部服务的漏洞，有效保护企业内部网络、业务的脆弱性，遏制漏洞利用。

实行最小授权原则，只授予员工所需的最小权限，细粒度的访问控制，保证用户只能看到和访问被授权的应用或资源。一旦发生入侵，降低在内部网络进一步横向传播的可能性。此外，实施MFA实际上改变了威胁态势，迫使威胁实施者寻找新的网络入侵方式，仅仅利用被盗的登录密码凭证无法攻破防线，MFA降低了多种不同的攻击类型的风险，包括勒索软件、数据盗窃、BEC和服务器访问攻击等。

在用户侧，提供强化的端点安全保障能力，客户端集成EDR能力，具备设备授信、合规检测、病毒查杀、漏洞修复等能力，确保设备安全合规。流量访问承载的安全网关，对所有网络访问流量进行深层解析和威胁识别，对网络攻击行为进行识别和拦截，同时也阻断外向恶意软件通信，防止网络入侵和敏感数据泄露。

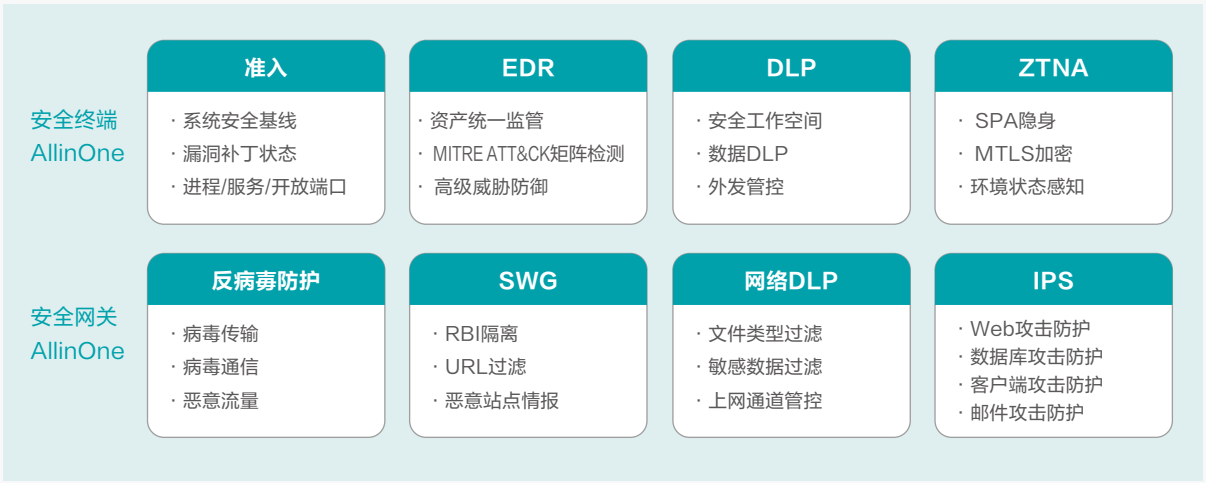


图 5 零信任统一化安全防护能力

安全联动增进体系化防护能力，平台对接现有网络中部署的防火墙、WAF、杀毒、主机IDS等安全设施，增强全局的威胁检测和风险汇聚能力，利用现有安全设备的信息输出提升整体零信任安全控制能力。

ATT&CK安全防御框架

网宿零信任平台支持按照ATT&CK安全防御框架对企业进行防护，由单载荷、单环节的层面提升到多个战术环节、多种攻击技术的层面，由被动防守的视角转变为以攻击者的视角去理解威胁，使防御体系的构建更具有主动性。具有足够纵深的主动防御能力，能够在多个环节逐步抵消威胁，同时由感知客户端、流量网关提供全面的信息采集与分析能力，以便发现常规防御手段无法发现的威胁并有效防护。

图 6 基于零信任的攻击防御框架

1、侦察阶段：采用SPA（单包授权）技术对企业网络进行隐身，黑客无法通过扫描等方式收集企业网络信息。
2、初始访问阶段：通过IAM的MFA等功能对访问账号进行管控；利用终端安全的合规检测功能对接入终端进行管控，对用户访问权限进行实时管控。
3、执行及持久化、权限提升阶段：通过终端EDR的病毒扫描、漏洞修复以及终端异常行为检测能力避免终端设备失陷。
4、发现及横向移动阶段：利用NDR识别并拦截异常网络行为；利用SWG识别并拦截异常Web访问行为；安全网关对用户权限进行管控避免横向移动；通过RBI确保内部核心系统只允许远程浏览器隔离访问。
5、命令与控制阶段：通过EDR的终端异常行为检测、NDR的异常网络行为检测结合威胁情报识别黑客的控制行为及C2服务器。
6、收集及数据泄露阶段：通过SWG模块对Web应用的敏感信息进行防护以免被恶意收集；通过安全工作空间在用户终端构建数据隔离区，避免敏感数据泄露。

安全网关流量过滤

零信任网关提供URL过滤和保护，Web应用程序控制访问通道控制，进行恶意代码检测和过滤，阻止存在风险或或未经授权的用户访问行为，支持通过RBI（远程浏览器隔离）实现对应用的隔离防护，避免恶意入侵攻击行为。

(1)平台承载网络流量安全分析，对勒索软件、木马、蠕虫等入侵攻击以及敏感文件、敏感信息进行识别和处置。
(2)支持基于WAF规则检测，包括SQL注入、XSS、文件上传、命令执行、敏感文件下载、敏感目录访问、XXE、文件包含、跨目录、后门文件、扫描器、敏感信息泄露等Web类流量检测。
(3)支持内网渗透、端口攻击、病索病毒、间谍软件、网络钓鱼、挖矿、恶意脚本等非Web类流量检测。
(4)支持检测防暴力破解、端口扫描，防止攻击者进入敏感业务系统。
(5)安全网关具备平台级的安全防护能力（DDoS、WAF等），为企业应用消除来自互联网中的攻击风险。
(6)流量全程加密保障通信安全，支持开启SSL/TLS加密能力，支持IPsec加密、国密算法加密，保障数据传输的安全。

抵御高级可持续威胁

基于长期持续跟踪各种网络威胁行为作业手法、漏洞利用工具和高级木马，形成自有威胁检测引擎和主动防御内核，建立多重机制拦截格式文档攻击和横向移动，如扇区监控、内核服务和驱动监控、文件监控、注册表监控等，从而有效拦截各式文档攻击和横向移动。

面对APT攻击，采用“未知可疑程序捕获+管理端静态分析+文件关联分析+威胁清除追溯”的防护策略，对新增的未知文件进行初步分析，针对发现的可疑程序会上报管理中心，管理中心进行静态深度分析，此外通过提取文件向量信息进行分析，分析判定文件是否为高危险文件。一旦判断该文件为高级威胁载荷，可以通过文件关联分析排查出与该文件有关的其他攻击载荷，进而针对相关威胁载荷进行统一清除。

勒索病毒防护，基于终端上文件多维信息监测和关联分析的精准检测勒索病毒的鉴定方法，监测文件加密动作、加密文件数量、文件访问和改写频率、文件后缀名形态变化和勒索URL采集等，通过对监测的多维信息进行关联分析，判断用户是否被勒索病毒攻击，同时为每项监测信息设置报警策略，当勒索病毒攻击时，自动触发用户报警，并将文件自动备份到安全隔离区中。即使在终端待机状态，同样支持实时防御勒索病毒。一般而言，勒索者软件都是工作在计算机系统空闲时间，安全客户端监测系统CPU利用率、内存占用率、磁盘的IO读写频率判断计算机是否处于空闲状态，通过文件多维信息监测和关联分析鉴定方法，判断当前终端进程行为是否异常，同时从对所有进程的实时监控发现有哪些进程在防御系统激活状态CPU占用率忽然激增，通过以上方法可定位勒索软件，并通过防御驱动拦截疑似勒索软件的恶意程序，并将已经加密的文件备份并进行防御处置。

全网威胁识别处置，基于“可疑程序（病毒）触发关键威胁规则”的敏感数据，从海量全部的终端行为中，计算并获得其所有前后的进程启动、文件改动、注册表等行为，计算并获得可疑程序（病毒）从感染开始到结束的全部行为链和攻击行为矩阵，按攻击事件行为矩阵和单一事件攻击链两种维度进行威胁事件的全方位溯源分析和处置。

4.2.3. 数据防泄露

围绕数据安全保护，网宿零信任提供RBI和数据DLP组件进行业务数据的保护，通过远程浏览器隔离RBI对Web应用上敏感信息进行防护，RBI支持管控文件下载、复制、粘贴等行为，确保敏感数据不落地。针对Web类应用，提供禁拷贝、水印防护手段。此外并在外发通道上进行管控，识别敏感的文件和数据，阻断数据泄露的外发。

在控制中心零信任动态访问策略的统一控制机制下，为用户侧提供安全工作空间，支持不同安全等级空间并行，以支持不同业务场景、多角色接入情况下企业的需要。安全空间落地数据加密，空间访问和空间内数据受控于企业，其中数据仅在策略允许和审核符合要求才可流转，提供进程水印，网络隔离策略防止外发，阻止截屏，防止数据泄露。

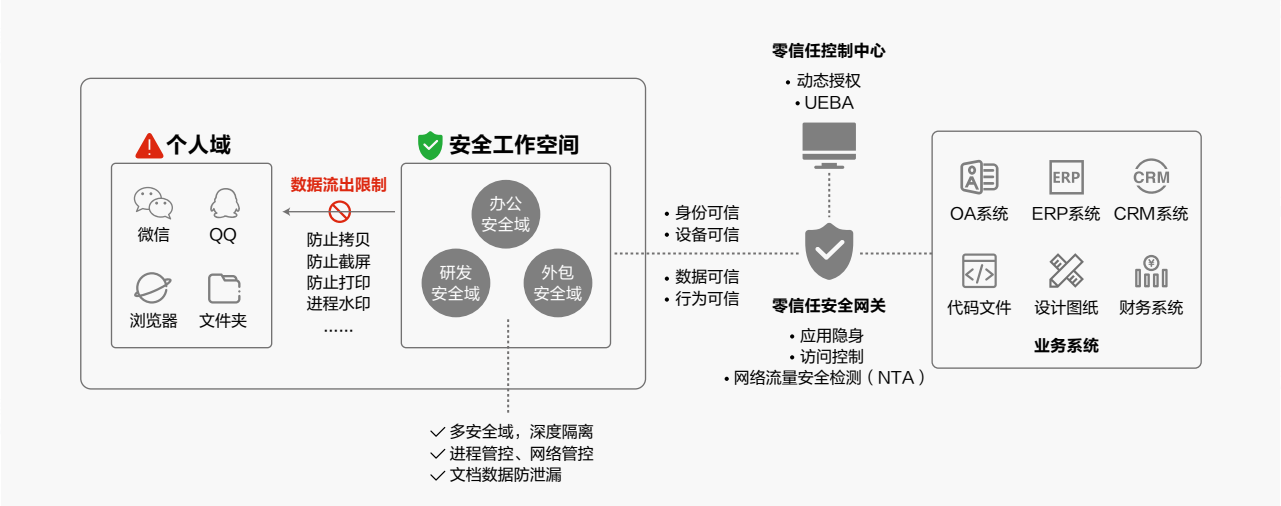


图 7 零信任安全工作空间

安全工作空间采用终端虚拟安全沙箱技术，在终端设备建构安全工作空间，业务人员访问行为和关键数据工作在安全工作空间内进行，空间中数据强加密，数据仅能安全空间内访问和使用，所有访问需要由企业合法认证授权，使用者无法自行外发数据和连接风险网络，从而避免敏感数据的泄露，为办公、设计、研发、运维等各类人员提供安全办公环境，安全地访问内部业务和数据，广泛应用在各类场景下：

1、数据采集：在终端设备建构安全工作空间，用户对数据采集工作（采集场景典型如电信、银行、电力、政务等营业柜台，采集内容客户照片、证件、资料等）在安全工作空间内进行，数据无法被私自发送出安全空间。

2、数据传输：终端设备上采集和处理的数据，通过安全工作空间与网关建立的高性能加密隧道传输到企业后台服务器，确保数据传输的安全。

3、数据存储：数据通过各类系统在用户侧访问都限制在安全工作空间内隔离使用，并且加密存储，未经授权无法访问，即使设备丢失或硬盘拷贝也无法获取使用。

4、数据使用：数据编辑、浏览均限制在安全工作空间，并以水印、截屏阻止来预防外发，数据在组织内部流转支持通过审核流程进行管控。

5、删除销毁：企业可以通过安全工作空间提供的远程锁定、擦除功能及账户禁用，随时销毁、禁止接入原来存放在用户侧的数据，保障企业数据安全可控。

6、数据备份：通过云备份保障企业数据资产安全，防止设备丢失、网络攻击软件勒索等事件发生。

在数据安全风险激增的环境下，安全工作空间受到国内各行业普遍欢迎，尤其在互联网、金融、政务等涉及大量敏感关键数据的行业。安全工作空间是对传统云桌面的一种有效可行替换方案，相对而言，安全工作空间显著减少对带宽的强依赖、充分利用现有端点设备存储和算力、更兼容本地外设，并提供细粒度的业务访问、数据控制，是一种轻量化、低成本、控制增强的安全办公新方式。

4.3. 零信任典型客户案例

4.3.1. 案例一：某股份银行零信任安全办公项目

某股份制商业银行在全国有众多分行和营业机构，公司雇佣了很多外包团队，其工程师主要来帮助研发和维护IT系统，并且存在大量的合作伙伴驻场服务，之前采用VDI解决方案保证数据不落地、不泄漏和安全研发的需求，但是VDI成本较高，无法满足业务和人员快速扩张的情况。

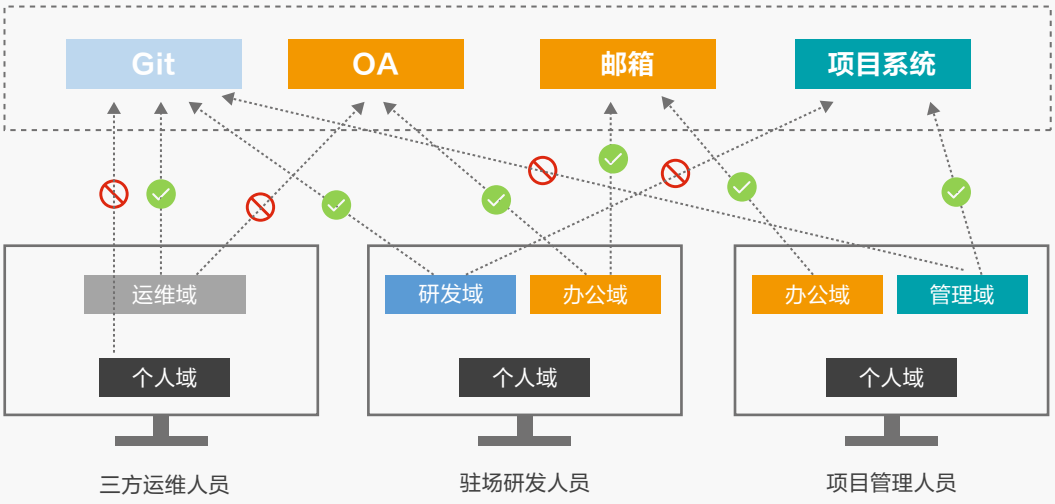


图 8 分域控制安全工作空间

业务诉求：

1. VDI方案办公场所受限，第三方人员无法驻场办公的情况下，还需要搭配VPN服务，带宽是额外运营成本，并且VPN漏洞频出，VPN被攻破事件频出，客户忧虑VPN的安全性
2. VDI对带宽需求、服务器资源要求高，成本投入高，无法满足大规模弹性扩容
3. 用户希望严格权限控制，但又要求灵活便捷管理，希望能够对内部异常用户行为快速识别和自动化处理

方案与效益：

1. 权限管控：根据不同权限组开放不同的业务权限，后台对外方人员权限进行灵活动态的管理，大大降低了策略配置工作量
2. 应用隐身：内网无需对外映射端口，所有业务系统从互联网上彻底实现了“隐身”，直接避免了VPN存在的可能漏洞
3. 数据安全：SecureLink安全工作空间为外包人员创建对应的安全域，仅允许访问相关的代码文件，同时安全域设置禁用剪贴板、禁止截屏、禁止打印，禁止文件流出，保障终端数据的安全性，可有效管控人员造成的数据泄露，相比VDI方案，成本降低30%以上
4. 远程接入：外包人员无需驻场开发，减少了办公场所成本，实现了更灵活的人员配置、部署，安全工作空间底层基于零信任加密隧道进行传输，无需额外购买VPN，集成的零信任平台提供统一化的安全控制策略

4.3.2. 案例二：某市政务外网零信任接入项目

某市大数据中心运营管理电子政务外网，为各委办局、事业单位等提供政务外网的安全接入服务。各单位公务员在日常办公、应急突发、远程执法、视频会议等场景下频繁接入种类政务外网应用。其中60%的用户为提升办公效率，日常使用一个终端，可以访问政务外网，也可以访问互联网。

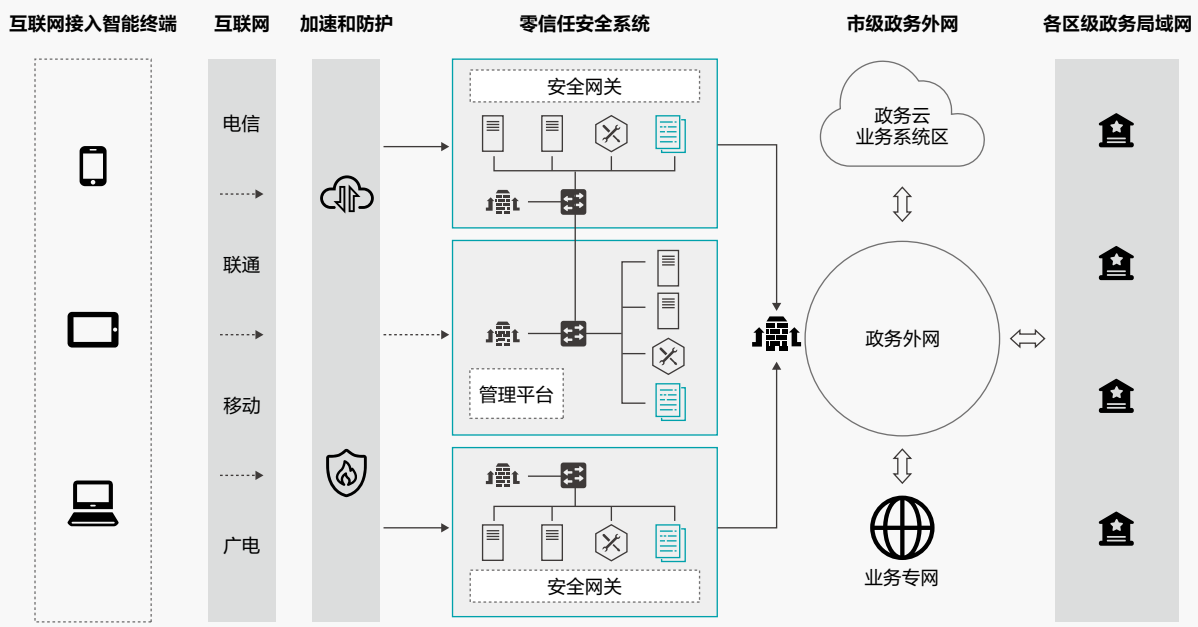


图 9 政务外网互联网零信任接入框架

业务诉求：

1. 政务外网终端存在“跨网访问”现象，极易成为网络攻击的跳板，将互联网威胁引入政务外网中，如果终端染毒或者黑客渗透攻击，将带来一系列安全隐患
2. 政务系统涉及大量个人隐私、政府机密等敏感信息，数据泄露影响大，数据的安全性尤为重要
3. 为满足国家电子政务外网标准《政务外网终端一机两用安全管控技术指南》需要确保政务终端入网的零信任安全沙箱确保安全性，在接入政务外网时，不得同时访问互联网
4. 大数据中心需要完成信息化创新任务，保持政府信息化建设高水平体系建设

方案与效益：

1. 零信任网关将内部核心业务“隐藏”起来，OA、邮箱等应用服务器IP及端口不对外暴露，只对授权用户开放访问
2. 项目建设合规匹配度高，满足等保及国产化政策要求，符合密评测评诉求，具备边界防护、入侵防范、访问控制等安全能力，配套体系化安全运营规范
3. 零信任安全接入总体建设，实现多场景终端快速接入、应对突发扩容需求，同时保障访问效果
4. 提供安全工作空间，具备限定业务访问、数据防泄漏、双网隔离的能力，安全可管可控，符合政务外网接入规范
5. 系统架构具备开放性与可扩展性，支持与第三方安全管理平台、网管平台与云管平台互通，支撑全局风险汇聚透视和高效安全运营

4.3.3. 案例三：某机械制造集团零信任远程访问项目

某机械制造集团在国内外拥有多个分支机构和项目部、营销公司，日常办公员工需访问国内、云上网应用系统，如OA、CRM、ERP等。

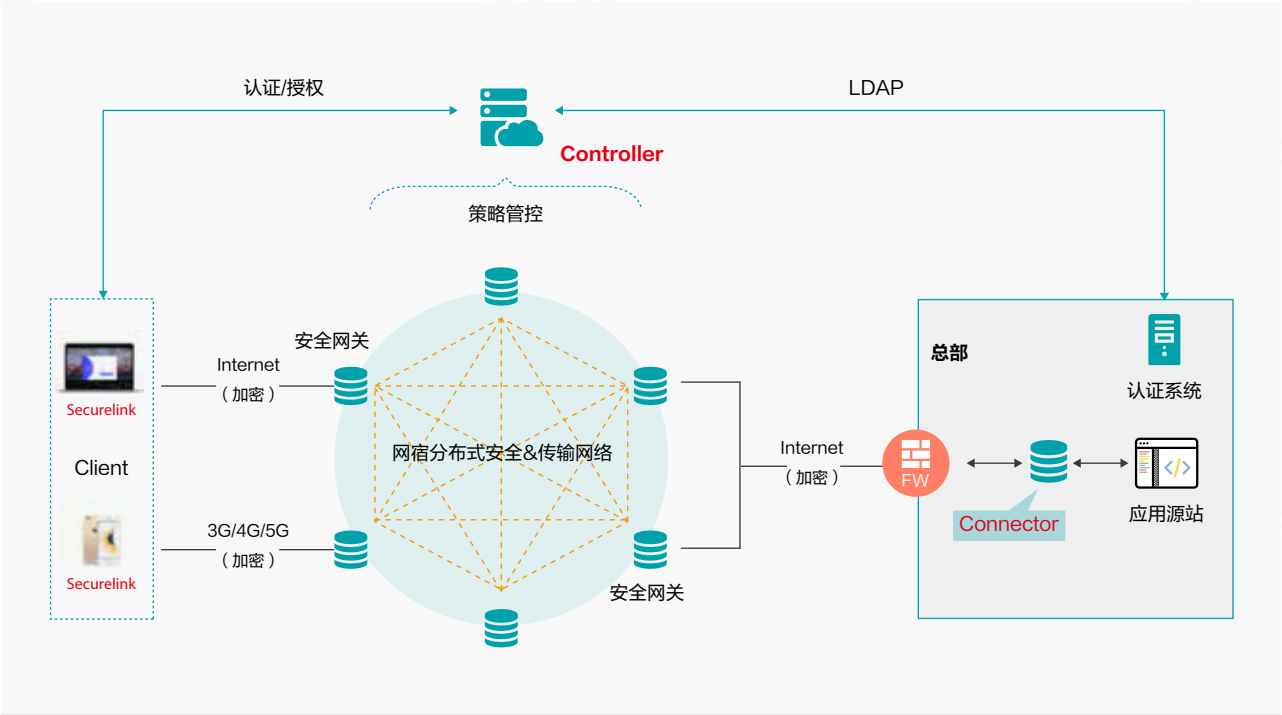


图 10 零信任全球安全远程访问

业务诉求：

1. 访问质量不稳定：基于公网默认路由访问，跨境互联质量差，VPN连接不稳定，影响员工办公效率
2. 运维管理困难：终端用户较多，难以统一管理，且现有传统VPN方案提供报表内容比较简单，无法满足客户需求
3. VPN安全性低：业内大量VPN漏洞被爆出，VPN被攻破事件频出，客户忧虑VPN的安全性

方案与效益：

1. 高质量访问：基于全球优化的加速网络，国内及海外员工访问零掉线，访问速度大大提升，在产品上线后实现零投诉
2. 应用隐身：内网无需对外映射端口，所有业务系统从互联网上彻底实现了“隐身”，直接避免了VPN存在的漏洞问题，应对攻防挑战，防止VPN等传统远程连接方式被攻陷
3. 远程接入：业务系统不在外网暴露，通过安全网关使得业务系统完全隐身，而总部/分公司/海外项目部员工可通过SecureLink零信任就近接入，远程安全访问内部系统
4. 统一管理：提供统一的可视化管理平台，支持以报表形式查看或导出业务趋势、安全监测分析数据。

小结

针对各行业居高不下的数据安全风险，网宿安达SecureLink产品为用户提供一种新的访问安全控制机制，将网络连接能力与数据安全防护能力以云原生形态融合以提供统一云化服务，是国内首家集RBI、SWG和端点安全工作空间于一体的零信任数据安全产品。SecureLink从端点、身份、网络、业务多层面检测和保护企业数据安全，提供高安全度数据保险箱抵御勒索软件攻击，识别和拦截APT攻击；并通过多级沙箱、隔离RBI有效保护企业核心数据的安全，收缩网络资产的暴露面，在各网关节点进行流量安全分析并拦截敏感数据离开企业；灵活的安全策略支撑企业内控安全基线要求，提供具备AI机器学习、异常行为识别的高阶分析控制能力，保障用户从任意位置高效安全地接入企业的资产业务和数据，适用于各类复杂的分布式网络环境和异构化业务数据访问场景。

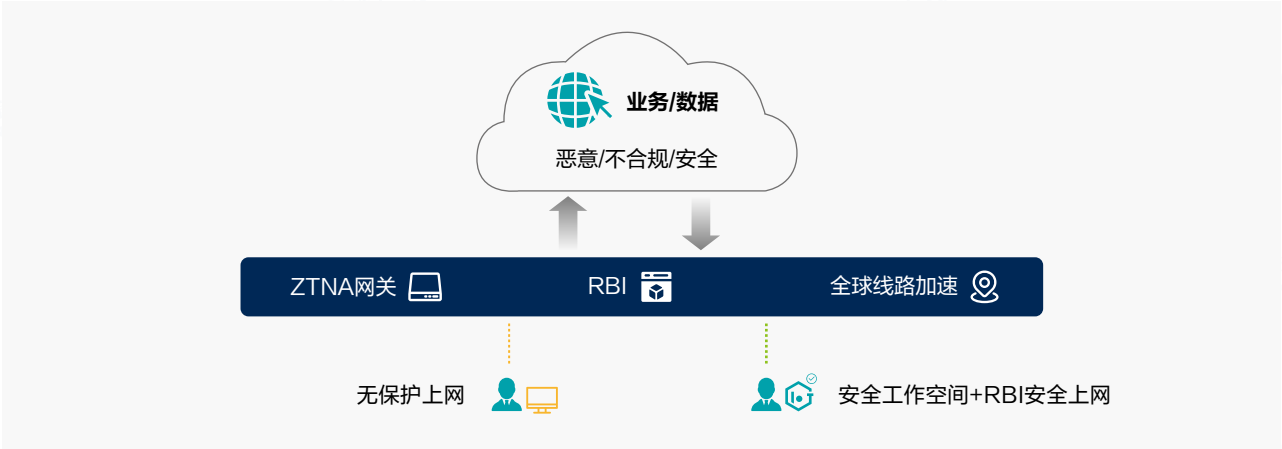


图 11 零信任统一安全访问

（1）安全工作空间，提供安全办公安全环境，检测阻断不合规网络连接，提供高速RBI工具，将互联网风险内容与用户设备、办公网络隔离开，有效防止外部恶意攻击渗透。

（2）动态信任评估引擎，用户访问业务过程中会话级动态授权，基于主体安全状态、异常行为、网络攻击、威胁情报和三方安全信息输入，以智能模型为基础、高速计算引擎实现真正的零信任动态授权。

（3）网络隐身，平台服务端口面向互联网络全隐藏，业务全隐身，只有验证用户和设备身份的合法性后，才针对合法用户合规终端临时开放网络端口和业务访问权限,有效收敛网络暴露攻击面。

（4）流量深度解析，实时分析、检测访问网络流量中的威胁攻击，进行告警和阻断。

（5）云边缘安全能力，提供分布式边缘防护，包括DDoS防护能力、WAF安全能力等。

（6）全球加速网络，解决企业远程访问速度瓶颈和稳定性问题，任意全球位置高速接入，提供最佳用户连接体验。

（7）一站式管理平台，对用户操作行为全面追踪审计，通过平台实现全网业务态势实时感知，支持威胁探测和告警，满足企业运维及安全需求，提高管理效率。

凭借全球部署分布的安全网络的天然优势，网宿零信任平台建立起一张虚拟安全网络，为企业打造安全、高效的零信任安全办公环境，提升网络业务访问环境安全性。当前，几乎所有行业都处于各类网络攻击风险和合规压力之下，网宿零信任平台支持用户对既有IT网络安全架构进行范式更新，因应云化、大数据、物联网、移动化的网络演化趋势，针对各类网络威胁构建多层立体防御体系。此外，网宿安达SecureLink是网宿SASE整体方案的重要组件，SASE平台将网络业务与安全技术深度融合，为用户提供一套高度集成、可扩展的SaaS化云交付安全连接服务，对于设定SASE长期转型目标的企业，SecureLink可为用户开启最佳平滑演进之路。

版权信息

CHINA INTERNET SECURITY REPORT