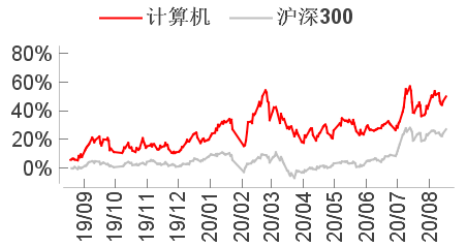
网络安全系列报告之三：零信任安全——将成为数字时代主流的安全架构

东方证券 ORIENT SECURITIES

行业评级	看好 中性 看淡 (维持)
国家/地区	中国
行业	计算机行业
报告发布日期	2020 年 08 月 17 日

行业表现



资料来源：WIND、东方证券研究所

证券分析师 浦俊懿
021-63325888*6106
pujunyi@orientsec.com.cn
执业证书编号：S0860514050004

证券分析师 游涓洋
010-66210783
youjuanyang@orientsec.com.cn
执业证书编号：S0860515080001

联系人 陈超
021-63325888*3144
chenchao3@orientsec.com.cn

联系人 徐宝龙
021-63325888*7900
xubaolong@orientsec.com.cn

核心观点

- **数字时代下旧式边界安全防护逐渐失效，零信任架构将成主流趋势。**传统的安全防护是以边界为核心的，一定程度上默认内网是安全的。而云大物移智等新兴技术的应用使得 IT 基础架构发生根本性变化，可扩展的混合 IT 环境已成为主流的系统运行环境，平台、业务、用户、终端呈现多样化趋势，传统的物理网络安全边界消失，并带来了更多的安全风险，旧式的边界安全防护效果有限。面对日益复杂的网络安全态势，零信任以身份为中心实现动态访问控制，被认为是数字时代下提升信息化系统和网络整体安全性的有效方式，逐渐得到关注并应用，呈现出蓬勃发展的态势
- **零信任架构适应多种业务环境及应用场景。**零信任架构的应用需要对 IT 基础设施与应用系统深度融合、全面覆盖，根据 NIST 下属的 NCCoE（国家网络安全卓越中心）发布的《实现零信任架构》（草案）项目说明书中，建议零信任安全应用的八大应用场景，囊括各类业务访问、数据交换以及服务网格场景。在数据中心、远程办公等实际场景均有较好的解决方案。
- **零信任安全需求正快速普及。**2019 年底，Cybersecurity Insiders 联合 Zscaler 发布的《2019 零信任安全市场普及行业报告》指出， 78%的 IT 安全团队希望在未来应用零信任架构，19%的受访者正积极实施零信任，而 15%的受访者已经实施了零信任，零信任安全正迅速流行起来。Gartner 的《零信任访问指南》也认为到 2022 年，在向生态合作伙伴开放的新数字业务应用程序中，80%将通过零信任进行网络访问，到 2023 年，60%的企业将采用零信任替代大部分远程访问虚拟专用网（VPN）。
- **我国零信任政策及标准正逐步落地，国内厂商积极布局零信任。**当前美国国防部已明确将零信任实施列为最高优先事项，同时海外零信任产业已走向规模化落地，营收超过 1.9 亿美元的厂商已超过 10 家。自 2019 年开始，我国也加快了零信任相关政策及标准的落地，各个安全厂商亦陆续推出零信任相关产品或解决方案，在零信任快速普及的背景下有望迎来快速发展。

投资建议与投资标的

- 当前海外零信任产业已进入规模化发展阶段，国内厂商已陆续推出自身的零信任产品或解决方案。在零信任安全逐渐普及的背景下，我们认为两类厂商最为受益：

  1）综合实力强劲并已有相应产品或解决方案推出的网络安全公司，建议关注奇安信-U(688561，未评级)、深信服(300454，增持)、启明星辰(002439，未评级)、安恒信息(688023，未评级)、绿盟科技(300369，未评级)、南洋股份(002212，买入)；

  2）在 SDP、IAM、MSG 或是某一应用场景具备突出优势的厂商，建议关注美亚柏科(300188，买入)、山石网科(688030，未评级)、格尔软件(603232，买入)。

风险提示

- 网络安全政策落地不及预期；零信任安全发展不及预期。

东方证券股份有限公司经相关主管机关核准具备证券投资咨询业务资格，据此开展发布证券研究报告业务。
东方证券股份有限公司及其关联机构在法律许可的范围内正在或将要与本研究报告所分析的企业发展业务关系。因此，投资者应当考虑到本公司可能存在对报告的客观性产生影响的利益冲突，不应视本证券研究报告为作出投资决策的唯一因素。
有关分析师的申明，见本报告最后部分。其他重要信息披露见分析师申明之后部分，或请与您的投资代表联系。并请阅读本证券研究报告最后一页的免责申明。

目 录

有关分析师的申明，见本报告最后部分。其他重要信息披露见分析师申明之后部分，或请与您的投资代表联系。并请阅读本证券研究报告最后一页的免责申明。

图表目录

有关分析师的申明，见本报告最后部分。其他重要信息披露见分析师申明之后部分，或请与您的投资代表联系。并请阅读本证券研究报告最后一页的免责申明。

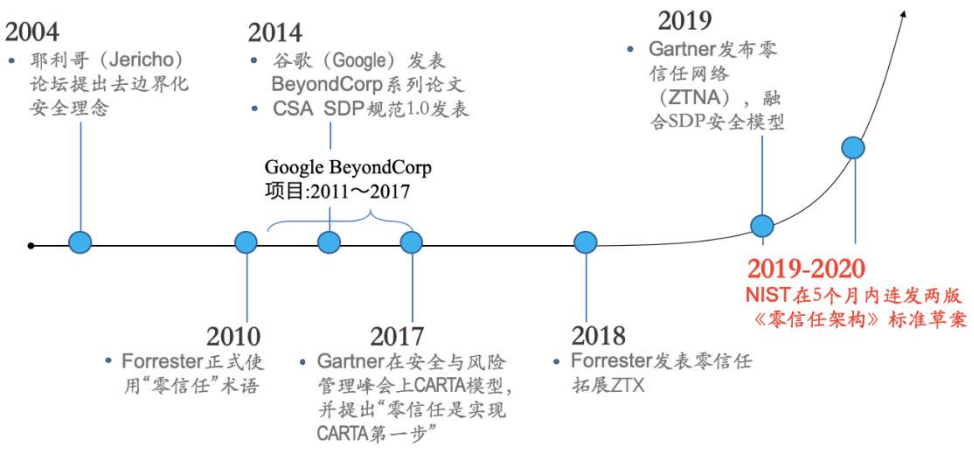
有关分析师的申明，见本报告最后部分。其他重要信息披露见分析师申明之后部分，或请与您的投资代表联系。并请阅读本证券研究报告最后一页的免责申明。

一、零信任将成为数字时代主流的网络安全架构

1.1 零信任是面向数字时代的新型安全防护理念

零信任是一种以资源保护为核心的网络安全范式。《零信任网络：在不可信网络中构建安全系统》一书对零信任安全进行了简要归纳和概况：1）网络无时无刻不处于危险的环境中；2）网络中自始至终都存在外部或内部威胁；3）网络位置不足以决定网络的可信程度；4）所有的设备、用户和网络流量都应当经过认证和授权；5）安全策略必须是动态的，并基于尽可能多的数据源计算而来。**因此零信任安全的核心思想是默认情况下企业内部和外部的所有人、事、物都是不可信的，需要基于认证和授权重构访问控制的信任基础。**零信任的雏形最早源于 2004 年耶利哥论坛提出的去边界化的安全理念，2010 年 Forrester 正式提出了“零信任”（Zero Trust，ZT）的术语。经过近十年的探索，零信任的理论及实践不断完善，逐渐从概念发展成为主流的网络安全技术架构。

图 1：零信任概念演进历程图

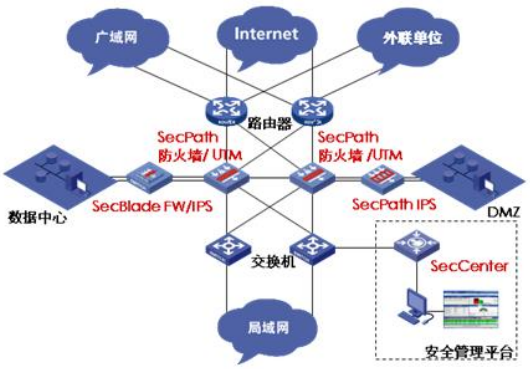


数据来源：中国信通院，东方证券研究所

数字时代下，旧式边界安全防护逐渐失效。传统的安全防护是以边界为核心的，基于边界构建的网络安全解决方案相当于为企业构建了一条护城河，通过防护墙、VPN、UTM 及入侵防御检测等安全产品的组合将安全攻击阻挡在边界之外。**这种建设方式一定程度上默认内网是安全的，而目前我国多数政企仍然是围绕边界来构建安全防护体系，对于内网安全常常是缺失的，在日益频繁的网络攻防对抗中也暴露出弊端。**而云大物移智等新兴技术的应用使得 IT 基础架构发生根本性变化，可扩展的混合 IT 环境已成为主流的系统运行环境，平台、业务、用户、终端呈现多样化趋势，传统的物理网络安全边界消失，并带来了更多的安全风险，旧式的边界安全防护效果有限。**面对日益复杂的网络安全态势，零信任构建的新型网络安全架构被认为是数字时代下提升信息化系统和网络整体安全性的有效方式，逐渐得到关注并应用，呈现出蓬勃发展的态势。**

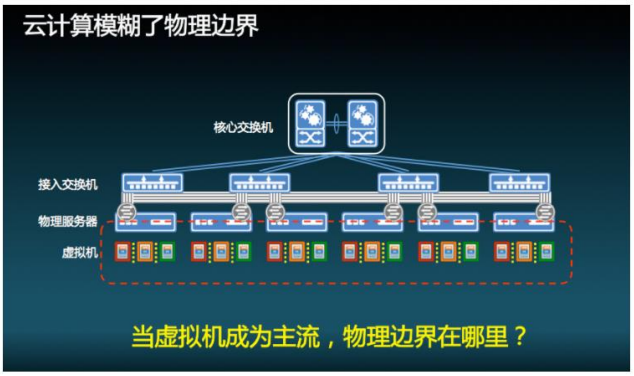
有关分析师的申明，见本报告最后部分。其他重要信息披露见分析师申明之后部分，或请与您的投资代表联系。并请阅读本证券研究报告最后一页的免责申明。

图 2：传统边界安全防护架构



数据来源：H3C，东方证券研究所

图 3：云计算等新兴技术带来传统安全边界消失



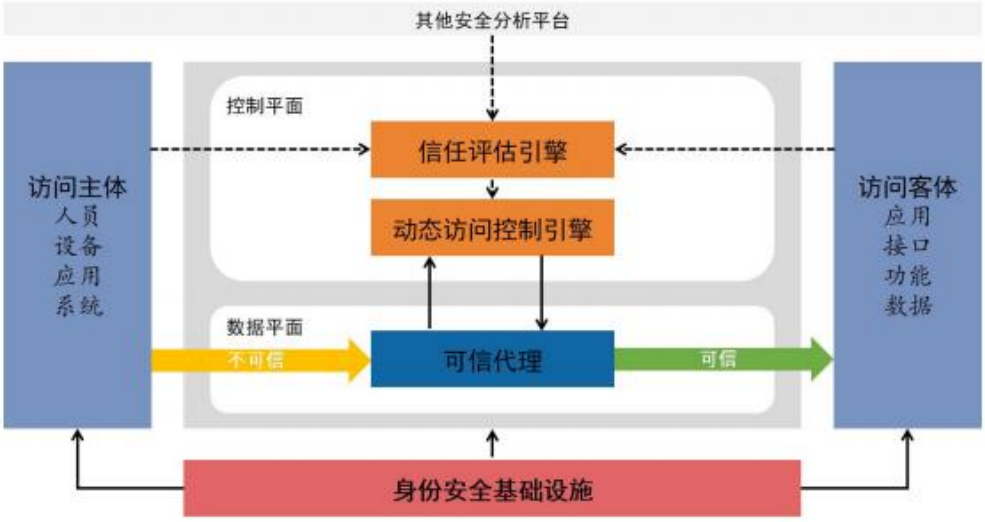
数据来源：TechTarget，东方证券研究所

1.2 “SIM”为零信任架构的三大关键技术

零信任的本质是以身份为中心进行动态访问控制。零信任对访问主体与访问客体之间的数据访问和认证验证进行处理，其将一般的访问行为分解为作用于网络通信控制的控制平面及作用于应用程序通信的数据平面。访问主体通过控制平面发起访问请求，经由信任评估引擎、访问控制引擎实施身份认证及授权，获得许可后系统动态 数据平面，访问代理接受来自主体的数据，从而建立一次可信的安全访问链接。过程中，信任评估引擎将持续进行信任评估工作，访问控制引擎对评估数据进行零信任策略决策运算，来判断访问控制策略是否需要作出改变，若需要作出改变时，将及时通过访问代理中断此前连接，从而有效实现对资源的保护。综上，可将零信任架构原则归纳为以下五个：

- **将身份作为访问控制的基础：**零信任架构对网络、设备、应用、用户等所有对象赋予数字身份，基于身份来构建访问控制体系；
- **最小权限原则：**零信任架构中强调资源按需分配使用，授予的是执行任务所需的最小特权，并限制资源的可见性；
- **实时计算访问控制策略：**零信任的授权决策根据访问主体的身份、权限等信息进行实时计算，形成访问控制策略，一旦授权决策依据发生变化，将重新进行计算，必要时将即时变更授权决策；
- **资源受控安全访问：**零信任架构对所有业务场景及资源的每一个访问请求都进行强制身份识别和授权判定，符合安全策略才予以放行，实现会话级别的细粒度访问控制，同时所有的访问连接均须加密；
- **基于多源数据进行信任等级持续评估：**零信任架构中访问主体的信任等级是根据实时多源数据（如身份、权限、访问日志等）计算得出，人工智能技术提高了信任评估策略的计算效率，实现零信任架构在安全性、可靠性、可用性及成本方面的综合平衡。

图 4：零信任架构总体框架图



数据来源：奇安信，NIST，东方证券研究所

“SIM”，即 SDP（软件定义边界）、IAM（身份与访问管理）、MSG（微隔离）是实现零信任架构的三大关键技术。NIST（美国国家标准委员会）在 2019 年发布的《零信任架构 ZTA》白皮书中，总结出实现零信任架构的三大核心技术“SIM”，分别是“S”，即 SDP（软件定义边界）；“I”，即 IAM（身份与访问管理）；“M”，即 MSG（微隔离）。

图 5：实现零信任架构的三大关键技术“SIM”

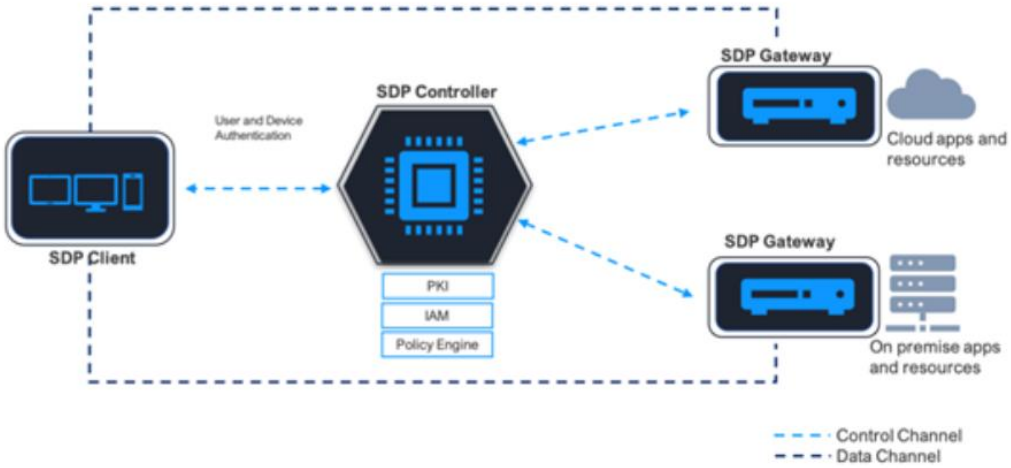
数据来源：云深互联，东方证券研究所

1） SDP（软件定义边界）

SDP 技术是通过软件的方式，在“移动+云”的背景下构建起虚拟 ，利用基于身份的访问控制及完备的权限认证机制提供有效的隐身保护。SDP 是由云安全联盟（CSA）开发的一个安全框架，

其体系结构主要包括 SDP 客户端、SDP 控制器及 SDP 网关这三个组件，其中客户端主要负责验证用户身份，将访问请求转发给网关，控制器负责身份认证及配置策略，管控全过程，网关主要保护业务系统，防护各类网络攻击，只允许来自合法客户端的流量通过。SDP 可将所有应用程序隐藏，访问者不知应用的具体位置，同时所有访问流量均通过加密方式传输，并在访问端与被访问端之间点对点传输，其具备的持续认证、细粒度的上下文访问控制、信令分离等防御理念可有效解决企业业务拓展中的安全问题，成为了零信任理念的最佳践行之一。

图 6：SDP 的组成架构



数据来源：Quadrant Knowledge Solutions，东方证券研究所

2）IAM（身份与访问管理）

全面身份化是零信任架构的基石，零信任所需的 IAM 技术通过围绕身份、权限、环境等信息进行有效管控与治理，从而保证正确的身份在正确的访问环境下，基于正当理由访问正确的资源。随着数字化转型的不断深入，业务的云化、终端的激增均使得企业 IT 环境变得更加复杂，传统静态且封闭的身份与访问管理机制已不能适应这种变化，因此零信任中的 IAM 将更加敏捷、灵活且智能，需要适应各种新兴的业务场景，能够采用动态的策略实现自主完善，可以不断调整以满足实际的安全需求。

图 7：零信任身份与访问管理

数据来源：云深互联，东方证券研究所

3）MSG（微隔离）

微隔离通过细粒度的策略控制，可以灵活地实现业务系统内外部主机与主机的隔离，让东西向流量可视可控，从而更加有效地防御黑客或病毒持续性大面积的渗透和破坏。当前微隔离方案主要有三种技术路线，分别是云原生微隔离、API 对接微隔离以及主机代理微隔离，其中主机代理微隔离更加适应新兴技术不断更迭及应用带来的多变的用户业务环境。

表 1：微隔离三大技术路线

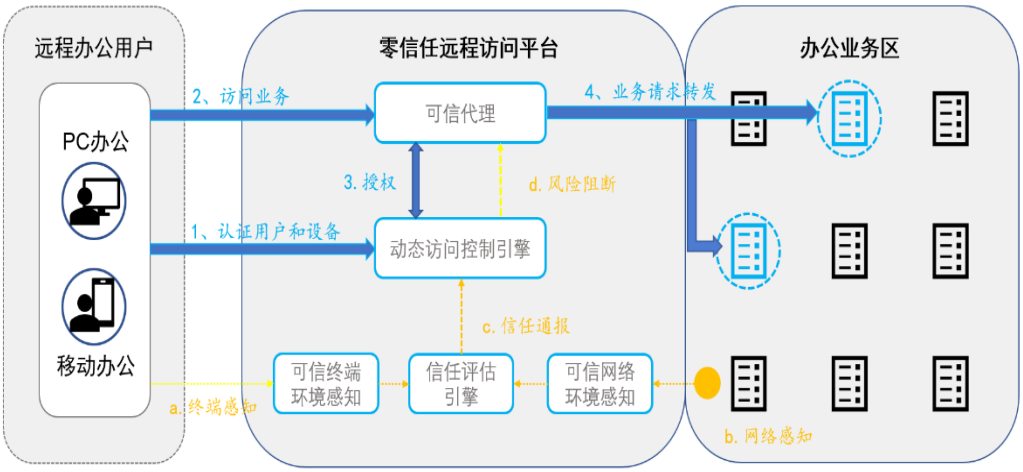
技术路线	支持架构	优点	缺点
云原生微隔离	仅支持虚拟化	平台原生技术，购买增值模块后在云平台可进行配置	混合云架构，或者非云PC环境，无法适用；用户一旦更换云服务商，很难简单快速迁移微隔离策略
API对接微隔离	仅支持虚拟化	与防火墙隔离逻辑一样，容易从防火墙隔离进行配置的迁移	非常依赖虚拟主机的对外接口，因此产生瓶颈：出现售后问题溯源困难；无法适用于PC或混合云场景；经过API接口调用性能损耗相对较大
主机代理微隔离	**支持PC、传统服务器、任意虚拟化平台**	**无需依赖底层架构，是唯一支持PC、混合云环境的微隔离方案，且主机迁移时安全策略能随之迁移**	**在初次实施时需通过批量工具进行部署**
备注：三种方案技术可组合形成混合方案，其优缺点取决于组合的技术			

数据来源：深信服，东方证券研究所

1.3 零信任安全应用场景丰富

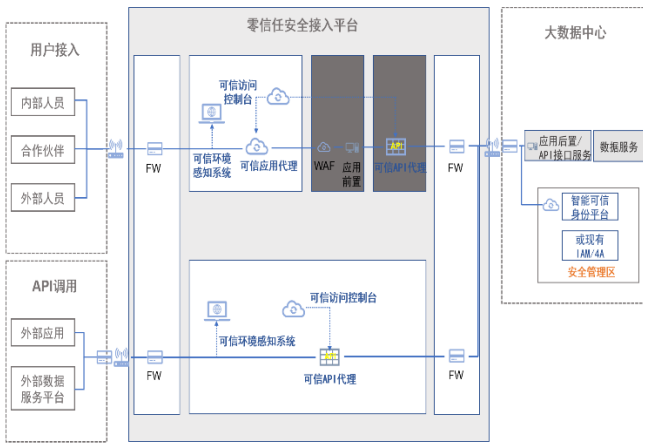
今年在疫情及新基建的双重刺激下，远程办公、云计算得到快速发展，政府大数据快速推进，对于零信任安全建设的必要性亦大大增强。而基于零信任的安全架构可以很好地兼容云计算、大数据、物联网等各类新兴应用场景，支持远程办公、多云环境、多分支机构、跨企业协同等复杂网络架构。如适用于远程办公的零信任安全架构，不再区分内外网，在人员、设备及业务之间构建虚拟的、基于身份的逻辑边界，实现一体化的动态访问控制体系，不仅可以减少攻击暴露面，增强对企业应用和数据的保护，还可通过现有工具的集成大幅降低零信任潜在建设成本。在大数据中心的应用场景中，东西向流量大幅增加，传统以南北向业务模型为基础研发的安全产品已不适用，零信任架构可通过微隔离技术实现有效防护。

图 8：基于零信任架构的远程办公安全参考架构



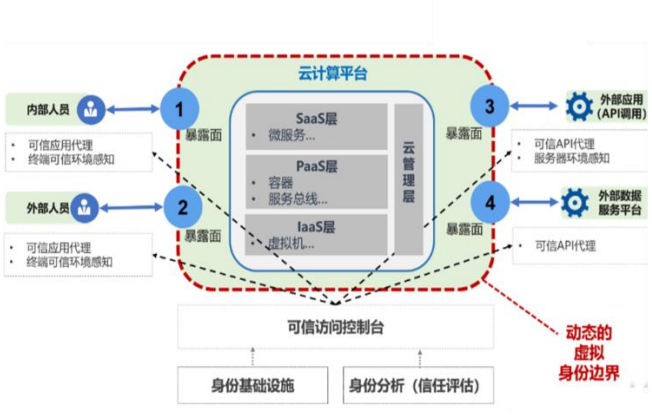
数据来源：中国信通院，东方证券研究所

图 9：数据中心安全接入区案例示意图



数据来源：中国信通院，东方证券研究所

图 10：基于零信任架构的云计算平台安全参考架构

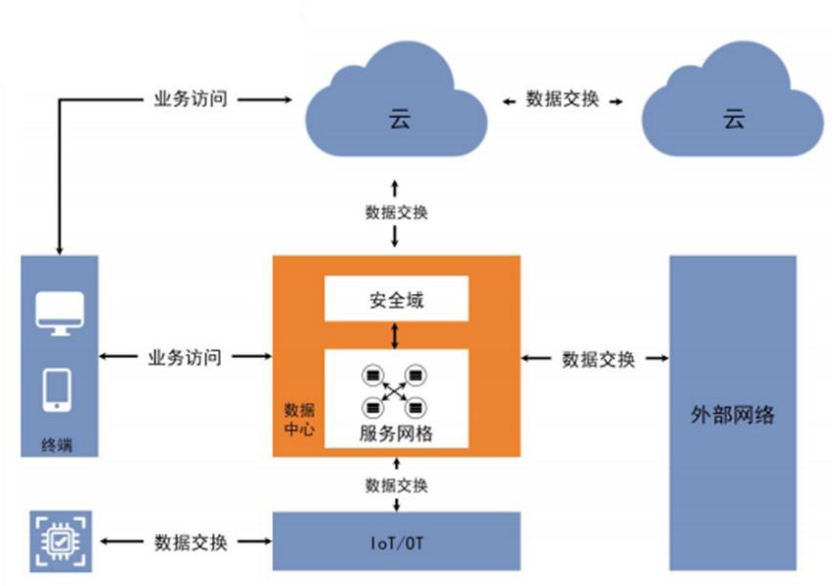


数据来源：中国信通院，东方证券研究所

有关分析师的申明，见本报告最后部分。其他重要信息披露见分析师申明之后部分，或请与您的投资代表联系。并请阅读本证券研究报告最后一页的免责申明。

零信任架构具备多种灵活的实现部署方式，适应多场景。现代 IT 环境下，业务场景呈现多样化趋势，根据访问主客体、流量模型以及业务架构可将这些场景归纳为三大类：业务访问、数据交换以及服务网格场景。其中业务访问场景是指用户访问业务应用的场景，是零信任架构的主要应用场景，包含移动办公、PC 办公等各类子场景，成功的零信任解决方案能够满足不同访问主体（如内部员工、临时员工以及外部人员等）、不同设备对各种应用协议的业务访问需求，在保持整体相同架构情况下具有高度适应性。大数据时代下数据交换场景变得更加频繁，相应的零信任解决方案需要有效应对接口多样化、运行环境多样化等挑战。服务网格场景，即数据中心内部服务器间的多方交互场景，是对业务架构嵌入最深的场景，由于节点数量较多，对零信任架构中的动态访问控制引擎及信任评估引擎要求更高。

图 11：零信任架构适应各类功能场景



数据来源：《零信任架构及解决方案》，东方证券研究所

二、零信任已从概念走向落地，迎来强劲风口

2.1 中美双双加码零信任安全

2019 年起美国相关组织陆续发布了多项零信任相关的报告或标准。2019 年 4 月，ACT-IAC（美国技术委员会—行业咨询委员会）发布了《零信任网络安全当前趋势》，对当前零信任的技术成熟度及可用性进行评估，随后 DIB（国防创新委员会）、NIST（美国国家标准委员会）均发表了零信任相关的报告或标准，其中《零信任架构》标准正式版也于今年 8 月 11 日发布，此外，Forrester 在《 2019 年度预测：转型走向务实》中明确指出零信任将在美国某些特定的领域成为标准的、阶段性的网络安全架构。

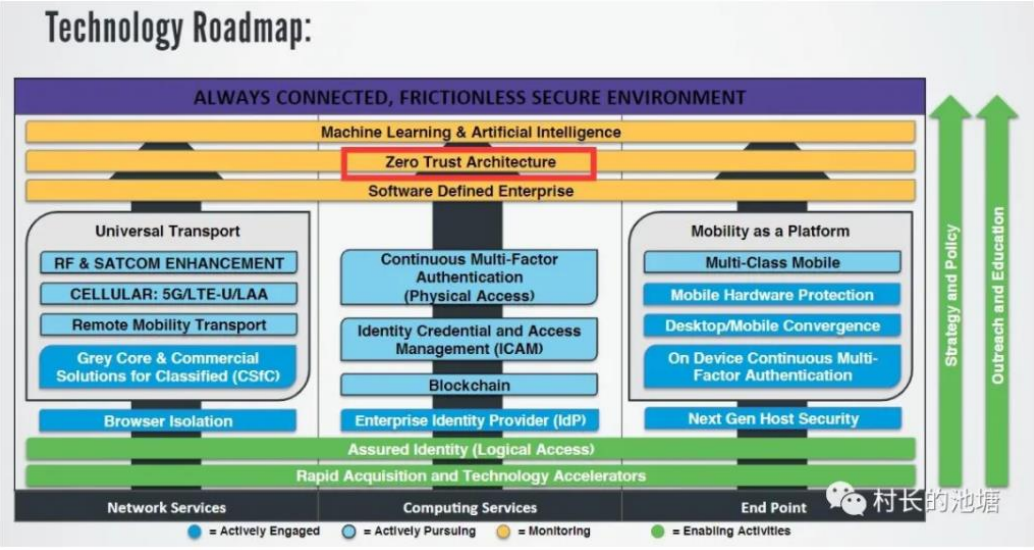
表 2：美国各组织发布的零信任相关报告

报告	时间	相关机构	内容
《零信任网络安全当前趋势》	2019.4	ACT-IAC	评估零信任技术和服务的技术成熟度和可用性
《零信任安全之路》	2019.7	DIB	指导国防部网络实施零信任架构
《零信任架构（ZTA）建议》	2019.10	DIB	建议国防部将零信任实施列为最高优先事项并在整个国防部内迅速采取行动
《实现零信任架构（草案）》	2020.3	NIST	为配合零信任标准的推进工作征求公开评论，瞄准的是零信任架构的落地实践，希望实现安全性与用户体验的兼得
《零信任架构》标准正式版	2020.8	NIST	给予零信任架构（ZTA）的抽象定义，并给出了零信任可以改善企业整体信息技术安全态势的普遍部署模型及应用案例

数据来源：互联网，东方证券研究所

值得注意的是，美国国防部已明确将零信任实施列为最高优先事项。无论是 DIB（国防创新委员会）提出的《零信任架构（ZTA）建议》还是 2019 年美国的《国防部数字现代化战略》中，均将零信任实施列为最高优先事项，侧面反映出美国政府及军队对于零信任架构的深刻认知和重视。

图 12：基于零信任架构的远程办公安全参考架构



数据来源：《美国数字现代化战略规划 2019》，东方证券研究所

我国零信任亦紧锣密鼓地展开，标准及应用案例逐渐落地。2019 年 9 月，工信部发布的《关于促进网络安全产业发展的指导意见（征求意见稿）》中将“零信任安全”列入需要“着力突破的网络安全关键技术”。2019 年 7 月腾讯牵头提交的《零信任安全技术—参考框架》行业标准通过评审，

成为我国首个立项的零信任安全技术行业标准。此外，奇安信发起的零信任首个国家标准《信息安全技术零信任 参考体系架构》已成功立项。同时，自 2019 年起国内部分机构也开始将零信任作为新建 IT 基础设施的安全架构，能源、银行、通信等行业也针对新型业务场景开展零信任技术的研究及试点工作。

表 3：我国零信任相关政策及标准

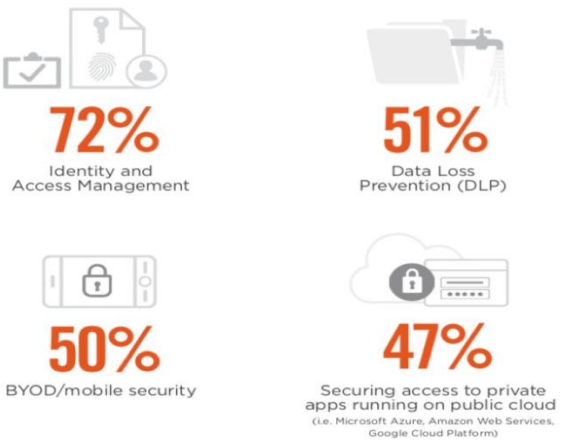
报告	时间	相关机构	意义
《关于促进网络安全产业发展的指导意见（征求意见稿）》	2019.9	工信部	将“零信任安全”列入“着力突破的网络安全关键技术”
《零信任安全技术-参考框架》	2019.7	腾讯牵头	国内首个立项的零信任安全技术行业标准。
《信息安全技术零信任 参考体系架构》	2020.5	奇安信牵头	国内首个立项的零信任国家标准

数据来源：互联网，东方证券研究所

2.2 零信任安全正在普及应用

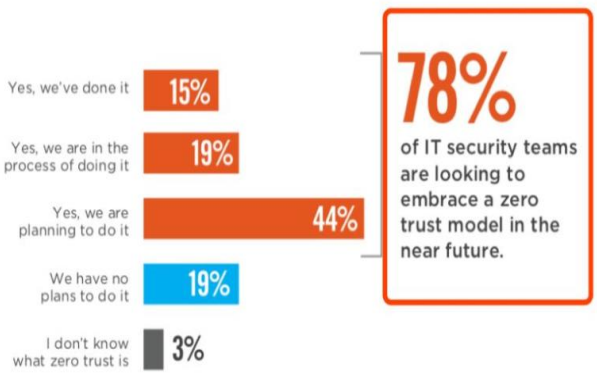
零信任架构成为企业 IT 安全建设的必然选择。2019 年底，Cybersecurity Insiders 联合 Zscaler 发布的《2019 零信任安全市场普及行业报告》指出，62%的受访者表示目前最大的应用程序安全挑战是确保对分布在数据中心和云环境中的私有应用程序的访问安全，对此企业所采用的安全措施主要是身份和访问管理（72%）、数据丢失预防（51%）、BYOD/移动安全（50%）等，这些措施均与零信任相关。报告指出，78%的 IT 安全团队希望在未来应用零信任架构，19%的受访者正积极实施零信任，而 15%的受访者已经实施了零信任，零信任安全正迅速流行起来。

图 13：面对当前安全访问挑战所需的安全措施



数据来源：《2019 零信任安全市场普及行业报告》，东方证券研究所

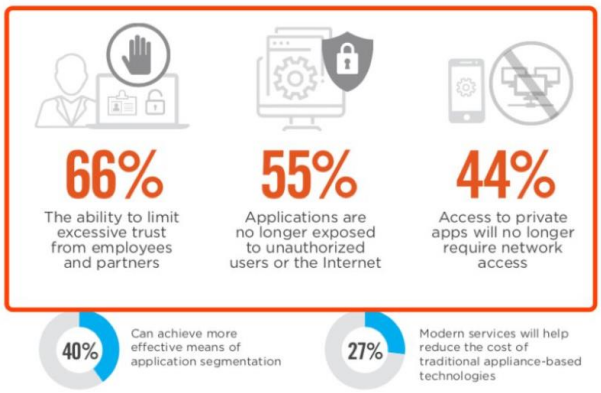
图 14：采纳零信任安全模型的组织比例



数据来源：《2019 零信任安全市场普及行业报告》，东方证券研究所

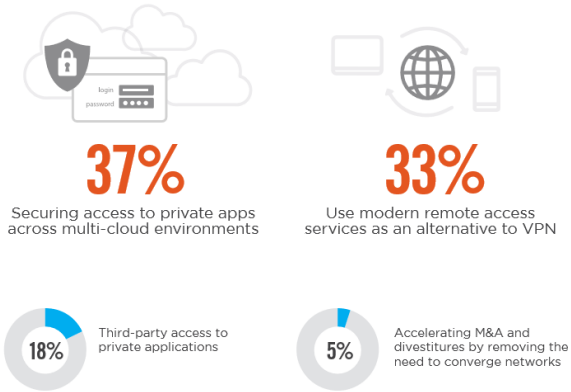
此外，受访者表示零信任被看重的优点在于零信任安全访问能够提供最低权限的访问来保护私有应用程序（66%）、应用程序不再暴露给未经授权的用户或互联网（55%）以及访问私有应用程序不再需要网络访问（44%）。而通过落地的零信任应用领域看，主要集中在安全访问运行在混合和公共云环境中的私有应用程序（37%）、使用现代远程访问服务取代 VPN（33%），以及控制对私有应用程序的第三方访问（18%）。

图 15：受访者看重的零信任优点



数据来源：《2019 零信任安全市场普及行业报告》，东方证券研究所

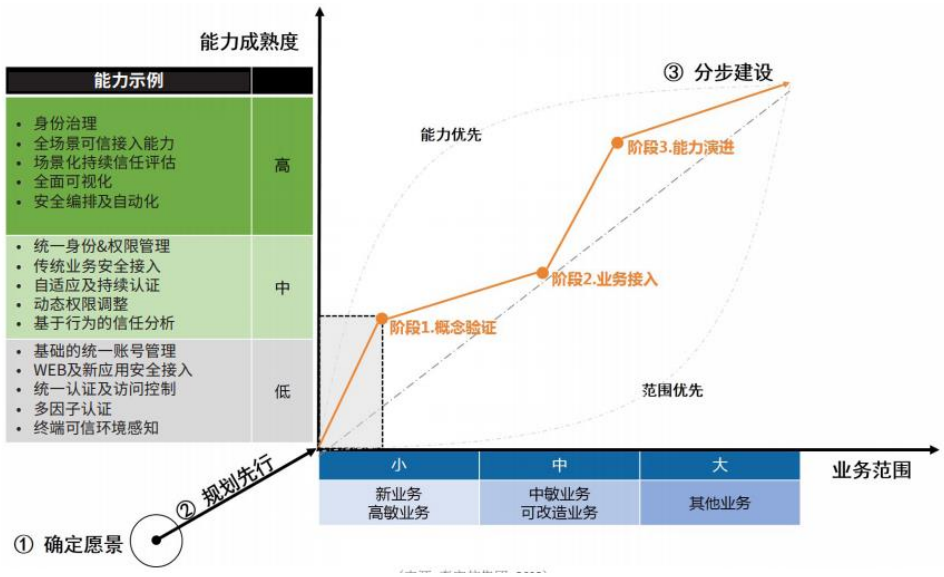
图 16：零信任主要的应用领域



数据来源：《2019 零信任安全市场普及行业报告》，东方证券研究所

零信任作为全新的安全理念，需要基于业务需求、安全运营现状、技术发展趋势等对零信任能力进行持续完善和演进。零信任的迁移并不是一蹴而就，需要结合企业现状、同一目标和愿景进行妥善规划和分布建设。**Gartner 的《零信任访问指南》认为到 2022 年，在向生态合作伙伴开放的新数字业务应用程序中，80%将通过零信任进行网络访问，到 2023 年，60%的企业将采用零信任替代大部分远程访问虚拟专用网（VPN）。**

图 17：零信任迁移方法



数据来源：奇安信，东方证券研究所

2.3 海外零信任产业已初具规模，国内即将步入建设高峰

海外零信任起步较早，目前已初具规模。Google、Microsoft 等巨头率先在企业内部实践零信任并推出了完整的解决方案；OKTA、Centrify、Ping Identity 等为代表的身份安全厂商推出“以身份为中心”的零信任方案；Cisco、Symantec、VMware、F5 等公司推出了偏重于网络实施方式的零信任方案；此外 Vidder、Cryptzone、Zscaler、Illumio 等创业公司亦表现。 根据 Forrester 在 2020 年二季度对于零信任产业的统计数据，按照零信任解决方案收入规模，市场的供应商可分为三类，其中零信任相关营收超过 1.9 亿美元的厂商已超过 10 家，海外零信任已经进入规模化产业发展阶段。

表 4：海外零信任解决方案市场供应商分析

公司规模等级	公司列表（字母排序）	营收标准
大型	Akamai、Cisco、Fortinet、Google、 Illumio、Microsoft、Okta、Palo Alto Networks、Proofpoint、Unisys	收入超过 1.9 亿美元
中型	AlgoSec、Armis、Centrify、Check Point Software Technologies、FireMon、 Forcepoint、Forescout、Gigamon、 GitLab、Ionic Security、MobileIron、 Tufin、Venafi	收入在 0.35~1.9 亿美元
小型	A10 Networks、AppGate、 Awingu Axis Security、BlackBerry、 ClearedIn、 、Edgewise、Guardicore、HyperQube、 IDENProtect、Infocyte、ShieldX Networks、ThreatLocker、 Zentera Systems	收入小于 0.35 亿美元

数据来源：Forrester，中国信通院，东方证券研究所

国内安全厂商积极布局零信任。尽管 Forrester Wave 的零信任扩展的生态系统平台提供商矩阵中未见国内安全厂商身影，但奇安信、深信服、启明星辰、绿盟科技等厂商始终关注国际网络安全技术发展趋势，均推出了相应的零信任整体解决方案。此外，山石网科、云深互联等厂商亦积极推动 SDP、微隔离等零信任技术方案的落地应用。在零信任快速普及的背景均有望迎来良好的发展机遇。

图 18：零信任扩展的生态系统平台提供商（2019Q4）

数据来源：Forrester Wave，东方证券研究所

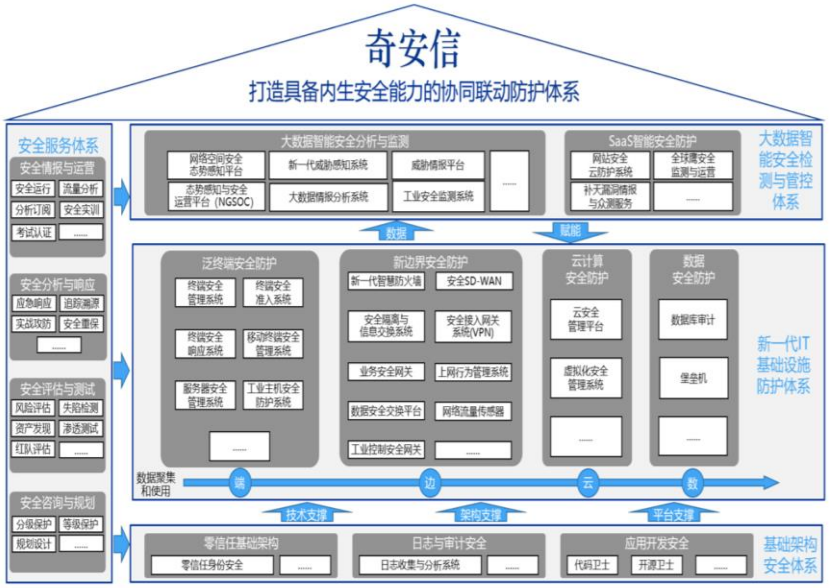
三、投资建议

数字时代下，云大物移等新兴技术的融合与发展使得传统边界安全防护理念逐渐失效，而零信任安全建立以身份为中心进行动态访问控制，必将成为数字时代下主流的网络安全架构。当前海外零信任产业已进入规模化发展阶段，国内厂商已陆续推出自身的零信任产品或解决方案。在零信任安全逐渐普及的背景下，我们认为两类厂商最为受益：一是综合实力强劲并已有相应产品或解决方案推出的网络安全公司，建议关注奇安信-U(688561，未评级)、深信服(300454，增持)、启明星辰(002439，未评级)、安恒信息(688023，未评级)、绿盟科技(300369，未评级)、南洋股份(002212，买入)；二是在 SDP、IAM、MSG 或是某一应用场景具备突出优势的厂商，建议关注美亚柏科(300188，买入)、山石网科(688030，未评级)、格尔软件(603232，买入)。

3.1 奇安信：网络信息安全龙头，专注于新型安全领域

奇安信业务布局完整，公司处于快速成长期，现已成为国内网络安全龙头。公司针对云计算、大数据、物联网、移动互联网、工业互联网和 5G 等新技术下产生的新业态、新业务和新场景，为政府与企业等机构客户提供全面、有效的网络安全解决方案。公司主营业务可分为安全产品、安全服务、硬件及其他三大部分，现已打造出具备内生安全能力的协同联动防护体系。2019 年，公司实现营收 31.54 亿元，同比增长 74%。2017-2019 年公司保持高速增长态势，三年里复合增速达到 56.62%。

图 19：奇安信协同联动防护体系



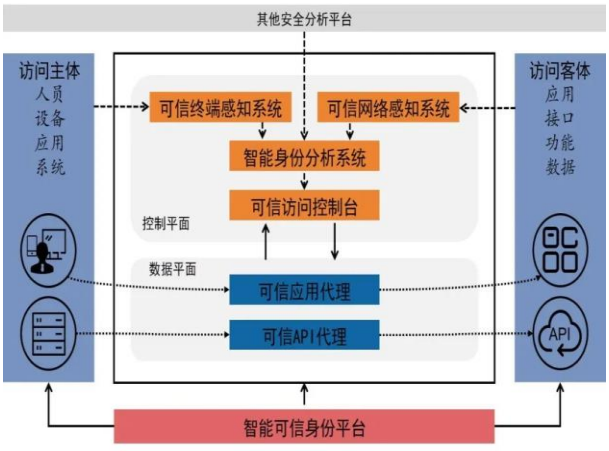
数据来源：奇安信招股书，东方证券研究所

在零信任架构下，奇安信推出一系列安全解决方案。公司零信任安全解决方案主要包括 TrustAccess 动态可信访问控制平台、TrustID 智能可信身份平台、ID 智能手机令牌及各种终端 Agent 组成。公司的零信任安全解决方案将产品组件进行拆分和扩展，将其映射到零信任参考架构上。同时，公司零信任安全解决方案和丰富的安全产品和平台之间可以实现联动，比如移动安全解决方案、数据安全解决方案以及云安全管理平台等。

图 20：奇安信零信任安全解决方案

数据来源：奇安信，东方证券研究所

图 21：奇安信零信任安全解决方案与参考架构的关系



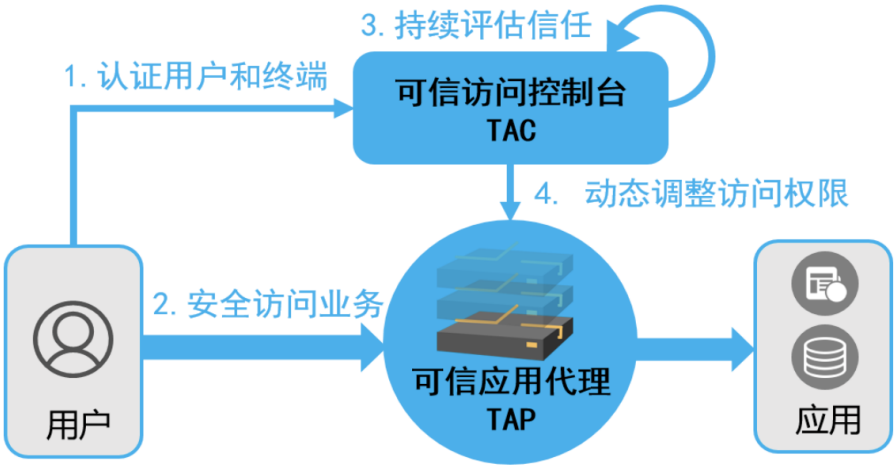
数据来源：奇安信，东方证券研究所

为保障数字化业务开展，奇安信推出零信任远程访问解决方案。远程访问常态化打破了传统的物理边界，因此需要全新的适用于新型 IT 环境的安全体系来应对日益严峻的网络威胁形势。根据 Gartner《2020 年度九大安全与风险趋势》报告表明，零信任网络访问（ZTNA）技术现在已开始

有关分析师的申明，见本报告最后部分。其他重要信息披露见分析师申明之后部分，或请与您的投资代表联系。并请阅读本证券研究报告最后一页的免责申明。

取代 VPN。奇安信推出的零信任远程访问解决方案聚焦远程访问场景，重点解决了边界易被攻破、全面网络开放、使用不稳定、扩容不平滑、管理不便捷等典型问题，全面增强了自身攻击防御能力。

图 22：奇安信零信任远程访问解决方案架构



数据来源：奇安信，东方证券研究所

3.2 美亚柏科：国内电子数据取证行业龙头，大数据智能化、网络安全专家

公司自成立以来深耕电子数据取证及大数据智能化业务，现已成为国内电子数据取证行业龙头和网络空间安全及大数据智能化等领域专家。公司以电子取证和大数据信息化为基本盘，为国内各级司法机关和行政执法部门提供政务信息化服务。公司目前已发展成“四大产品”和“四大服务”体系，其中电子取证业务以及大数据智能化平台是公司主要收入来源，2019 年收入占比分别为 40.4%和 37.1%。

图 23：美亚柏科“四大产品”及“四大服务”

数据来源：美亚柏科，东方证券研究所

作为“新基建”最大的服务对象，智慧城市正在步入发展“快车道”。“新基建”的核心是科技，主要包括信息基础设施、融合基础设施、创新基础设施，建设的目的在于为发展数字经济提供基础。数字化基础设施与智慧城市的建设是相辅相成的，因为建设智慧城市本身就是发展数字经济。当前，公司正基于自身大数据技术优势和多年的行业积累，加快智慧城市的业务布局，并已参与多地智慧城市规划和建设。

表 5：重大会议上提及“新基建”情况

时间	会议	会议相关内容
2018 年 12 月	中央经济工作会议	加大制造业技术改造和设备更新，加快 5G 商用，加强人工智能、工业互联网、物联网等新兴基础设施建设
2019 年 7 月	中央政治局会议	加快推进信息网络等新型基础设施建设
2020 年 3 月	中央政治局常委会会议	加快 5G 网络、数据中心等新型技术设施建设进度

数据来源：公开资料，东方证券研究所

公司重视“零信任体系”搭建，并将其拓展至智慧城市的建设中。面对复杂的接入环境、多样化的接入方式和数量庞大的智能接入终端可能带来的未知安全威胁，传统网络安全模型逐渐失效，“零信任安全”日益成为新时代下网络安全问题的新理念、新架构。公司成立认证管理、权限管理、审批管理、审计管理、安全策略控制、环境感知等基于“零信任体系”的六大产品中心，构筑安全可信合规的纵深防御体系。公司把“零信任体系”拓展至“城市网络安全大脑”建设中，使其实现态势感知、预警、分析、反制等能力，为智慧城市的网络安全构筑了一道有力的屏障。

图 24：美亚柏科城市大脑逻辑架构

数据来源：美亚柏科，东方证券研究所

3.3 深信服：领先的信息安全企业，从零信任到精益信任

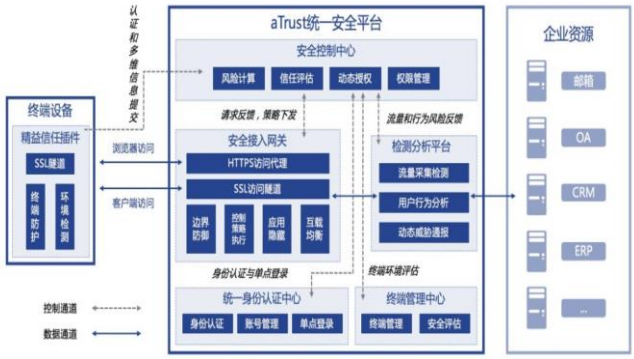
深信服专注于软件和信息技术服务行业，为政府部门、事业单位等企业级用户提供信息安全、云计算、企业级无线相关的产品和解决方案。公司信息安全业务种类丰富，包括上网行为管理、下一代防火墙、VPN、应用交付等多款产品，市占率常年保持行业领先。在云计算业务方面，公司已完成企业级云、专属云、桌面云三朵云的业务布局。企业级无线业务主要由子公司信锐网科经营，产品包括无线控制器、无线接入点等。2019 年公司实现 45.90 亿元，同比增长 42.35%。根据 IDC 数据，公司 2019 年国内虚拟专用网产品的市占率 24.8%，排名第一；在安全内容管理产品的市占率 22.4%，排名第一。

图 25：深信服主营业务

数据来源：深信服招股书，东方证券研究所

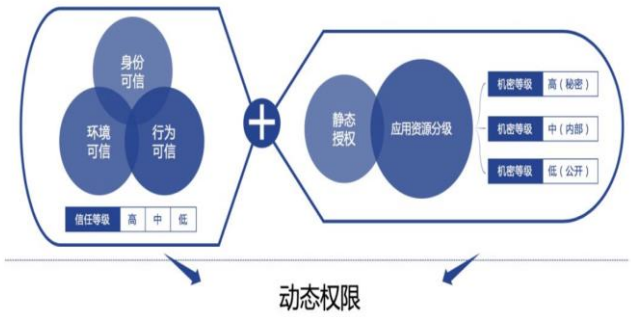
基于零信任的基础上，深信服推出精益信任 aTrust 安全架构。零信任解决了破碎边界的问题，但安全不能被任意一个安全产品独立解决，而是需要一定的联动和协作。2019 年，深信服推出精益信任 aTrust 安全架构。精益信任 aTrust 安全架构主张零信任需要和其他安全的设备进行联动，形成互补的安全体系，构建统一的安全。aTrust 基于信任和风险的闭环，整合终端、边界、外网的已有安全设备，进行统一联动，形成自主调优、快速处置的统一安全架构，最终实现内外网“精确而足够”的信任。aTrust 安全架构主要由全面身份化、多源信任评估、动态访问控制、统一安全、可成长等五点组成。此外，公司还推出了零信任“VPN”，实现可信访问、智能权限等方面的全面升级。

图 26：深信服精益信任解决方案架构



数据来源：深信服，东方证券研究所

图 27：深信服精益信任动态访问控制



数据来源：深信服，东方证券研究所

3.4 启明星辰：老牌网络安全龙头，零信任管控平台为多种应用场景提供安全保障

启明星辰是网络安全市场龙头企业，具有完善的专业安全产品线。公司完善的专业安全产品线横跨网关、检测、数据安全与平台、安全服务与工具等技术领域，共有百余个产品型号。其中，入侵监测与防御(IDS/IPS)、统一威胁管理(UTM)、 安全管理平台(SOC)、数据安全、数据库安全审计与防护、堡垒机、网闸等 9 项产品市场占有率常年保持第一。2019 年度，公司实现营业收 入 30.89 亿元，同比增长 22.51%，其中安全产品业务收入 22.21 亿，同比增长 19.79%，安全运营与服务业务收入 8.48 亿，同比增长 31.67%。

图 28：启明星辰全流程安全产品布局

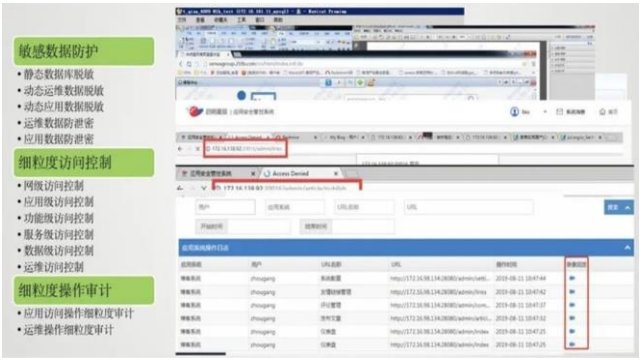
数据来源：启明星辰，东方证券研究所

启明星辰推出零信任管控平台，为多种应用场景保驾护航。启明星辰零信任管控平台能接收外部生态系统的数据并进行精细化处理，通过访问控制服务，向策略执行组件提供策略信息和策略决策服务；通过环境感知系统输送的环境信息和用户行为分析系统输送的审计分析信息，分析出高风险操作行为；同时反哺权限管理模块，进一步动态调整用户权限。零信任管控平台为应用代理、API 代理、运维代理或其他代理组件提供策略执行依据，通过多种应用场景提供全方位的安全保障。

图 29：启明星辰零信任体系架构

数据来源：启明星辰，东方证券研究所

图 30：零信任管控平台典型应用场景



数据来源：启明星辰，东方证券研究所

3.5 安恒信息：网络安全后起之秀，新兴安全业务发展迅速

安恒信息构建了以“新场景”及“新服务”为方向的专业安全平台产品和服务体系，平台类产品和网络安全服务业务增长迅速。公司一直以来聚焦于网络信息安全领域，主营业务为网络信息安全产品的研发、生产及销售，并为客户提供专业的网络信息安全服务。公司的产品及服务涉及应用安全、云安全、大数据安全、物联网安全、智慧城市安全和工业互联网安全等新兴领域，构建了以“新场景”和“新服务”为方向的产品体系。2019 年，公司实现营收 9.44 亿元，同比增长 50.66%，其中网络安全平台产品以及网络安全服务业务增速分别为 91.15%与 62.03%。

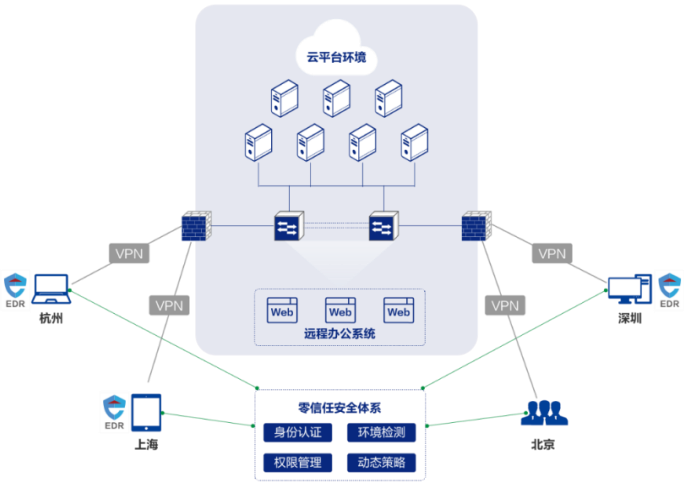
图 31：安恒信息产品体系全线概览图

数据来源：安恒信息招股书，东方证券研究所

云上业务天然存在安全风险和信任危机的隐患，公司利用零信任安全体系架构为云上业务提供动态保护。在远程办公模式下，员工可能存在使用不安全终端或处于不可信环境下办公的情况，也会存在员工身份鉴别不准确、账号权限控制不足、远程网络链路不安全等问题，这些都增加了云内核心业务系统遭受恶意攻击的风险。在这种情况下，对员工身份的认证管理、账号权限的最小

化控制和建立安全的传输通道尤为关键。在云平台产品中，公司通过建立健全零信任安全体系架构，辅以 VPN 和主机安全（EDR）等专有安全措施，对远程接入终端进行检测、病毒查杀和加固，同时将远程连接进行加密，保证数据在传输过程中不被第三方窃取。

图 32：安恒信息依托零信任体系确保云上业务的接入访问可信



数据来源：安恒信息，东方证券研究所

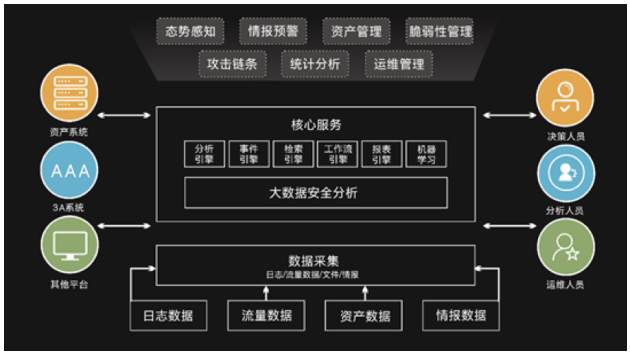
3.6 绿盟科技：领先的网络安全解决方案供应商，产品逐步向零信任安全架构迁移

绿盟科技是国内领先的企业级网络安全解决方案供应商，具有完善的安全产品线，并持续推进 P2SO 战略。公司业务线分为安全产品和安全服务两大类，安全产品分别是检测防御、安全评估、安全监管、安全实验室和安全平台五大类产品；安全服务包括客户服务、安全运营、安全服务和云安全服务。2015 年，公司正式提出“P2SO”战略，向安全解决方案和安全运营模式全面转型。近年来，公司在工控安全、云安全等领域都取得不错进展，核心产品市占率也保持中国区第一或领先位置。2019 年，公司实现营收 16.71 亿元，同比增长 24.24%。

图 33：绿盟科技安全产品线

数据来源：绿盟科技，东方证券研究所

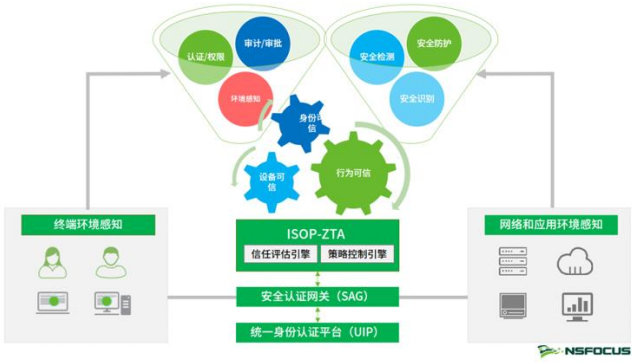
图 34：绿盟科技安全运营架构



数据来源：绿盟科技官网，东方证券研究所

绿盟科技借助已经部署的安全产品，将安全防护与零信任结合，面向未来构建安全架构。零信任架构需要多种安全产品和技术来构建，公司在原有的网络安全基础上，增加零信任安全组件，实现零信任网络访问控制，构建以用户可信和设备可信为基础，持续评估访问行为可信，自适应访问控制的架构体系。

图 35：绿盟科技零信任安全解决方案



数据来源：绿盟科技，东方证券研究所

图 36：绿盟科技零信任网络访问控制

数据来源：绿盟科技，东方证券研究所

绿盟科技推出零信任远程办公解决方案。随着上半年新冠疫情的爆发，远程办公已成为企业的首选办公方式。但中大型企业 VPN 在远程办公过程中也暴露出难以连接 VPN、VPN 不稳定等问题，同时也出现了内部人员利用 VPN 登入公司内网跳板机，报复性破坏客户数据的事件。相比传统远程办公方式，零信任远程办公方案有更加突出的安全性、更低的网络质量要求等优势。据 Gartner 预测，到 2023 年，全球将有 60%的企业淘汰大部分 VPN，转向使用零信任访问网络。

表 6：零信任与 VPN 在通用办公场景的对比

	基于 VPN 实现的远程办公	零信任理念的远程办公方案
鉴权设计	一次访问鉴权成功，不再校验，建立隧道后即维持	对每次访问请求进行校验，包括设备、用户、权限等
会话加密	支持 CBC，DES，AES 等算法加密但易被破解，SSLVPN 支持 SSL 加密	支持国密、SSL 加密，加密复杂度较高
认证方式	静态密码/OTP 认证	支持多因子认证
授权控制	多基于 IP、端口进行授权控制。攻击者突破 VPN 后容易内部横向移动	支持功能级、API 级、数据级授权，可实现最小化授权，防止内部横向移动
行为风险评估	不支持评估用户行为风险	支持联动行为分析平台，评估行为风险，实现动态访问控制；支持联动环境感知产品，实现用户身份及其访问终端设备的双重可信。

数据来源：绿盟科技，东方证券研究所

3.7 南洋股份：国内防火墙龙头企业，持续推动零信任安全理念的落地实践

公司全资子公司天融信是国内防火墙龙头企业，安全服务快速增长。天融信是国内网络安全领域的领先厂商，主要提供安全及大数据产品（包括安全网关、安全检测、数据安全、云安全等）以

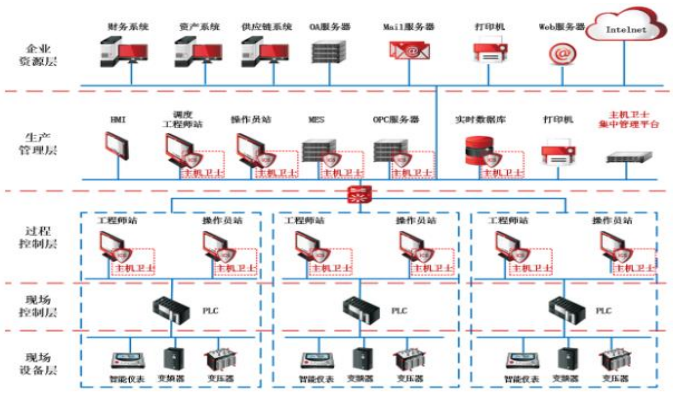
及安全服务（包括安全云服务、安全咨询与评估服务、安全运维服务等）两类产品。2019 年，公司网络安全业务快速增长，其中安全产品营收 20.78 亿元，同比增长 33.81%；安全服务营收 3.37 亿元，同比增长 90.35%。公司防火墙市占率达到 23.97%，排名第一，VPN 与入侵防御硬件市占率分别为 6.55%和 8.77%，分列市场第三和第四。

图 37：天融信以下一代防火墙为基础的安全防御体系

数据来源：天融信，东方证券研究所

天融信积极推动零信任理念与业务系统结合，推出工控主机卫视系统。公司结合零信任技术架构、安全理念，积极探索新技术方向并推出下一代可信网络安全架构（NGTNA），同时为客户提供终端环境持续检测、访问行为基线判断、身份安全集中管理、业务风险动态评估、安全策略即时下发等能力。公司推出工控主机卫士系统，采用零信任安全机制，对工控上位机及服务器实现全方位安全防护，保障用户业务连续稳定运行。

图 38：天融信工控主机卫士系统



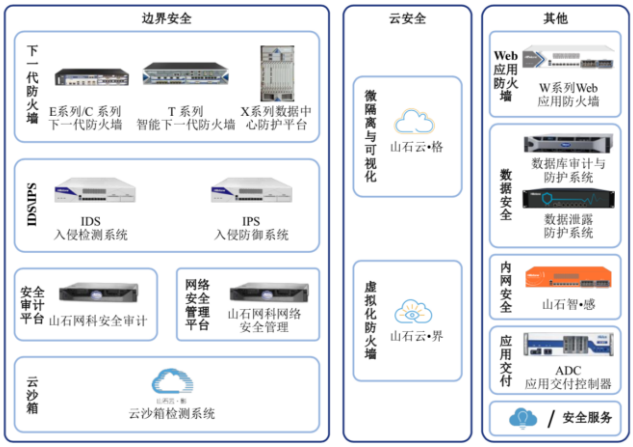
数据来源：天融信，东方证券研究所

3.8 山石网科：边界安全领域领导厂商

山石网科是我国网络安全行业的技术创新领导厂商，自成立以来一直专注前沿技术的创新。公司提供包括边界安全、云安全、数据安全、内网安全在内的网络安全产品及服务，致力于为用户提供全方位、更智能、零打扰的网络安全解决方案。公司产品主要分为三大类，分别为边界安全、

云安全和其它类别的产品。2019 年，公司实现营收 6.75 亿元，同比增长 20.0%，近年保持稳定增长，2016-2019 年的复合增长率为 27.4%。

图 39：山石网科主要产品及服务矩阵



数据来源：山石网科，东方证券研究所

山石云·格采用山石网科自主研发的“云安全微隔离技术”，真正实现零信任安全模型。在 Gartner 发布的《2020 年云工作负载安全防护平台市场指南》中，山石云·格（CloudHive）成功入选指南中“基于身份的隔离、可视和控制能力”分类，山石网科也成为中国首家获得指南推荐的微隔离与可视化云安全产品全球供应商。山石云·格采用山石网科自主研发的“云安全微隔离技术”，利用 NFV 和 SDN 的优势，将微隔离、可视化能力深入到虚拟化环境中，拥有深度微隔离、多维可视化、智慧运营、合规性检查以及全面安全防护等功能。

图 40：山石云·格主要功能

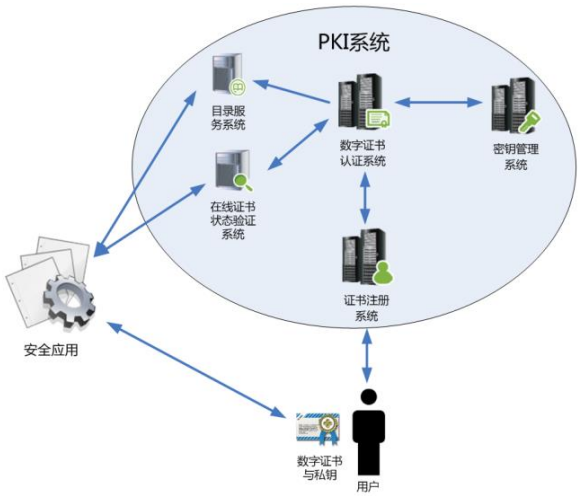
- **深度微隔离：**采用分布式高可靠架构、NFV组件设计，真正实现零信任安全模型。
- **多维可视化：**可基于业务、时间、终端、应用、流量、交换关系、安全威胁等多种维度对云内网络及业务运行情况深度可视。
- **智慧运营：**业务性能实时监测预警，服务链自梳理，助力管理员提高网络安全运维效率。
- **合规性检查：**遵循网络安全法、满足等保监管要求，灵活划分安全区域、分级分域防护。

数据来源：山石网科，东方证券研究所

3.9 格尔软件：国内 PKI 领先企业

格尔软件是国内 PKI 领域的领先厂商，具有完备的以 PKI 为核心的信息安全产品和服务体系。公司主要产品包括 PKI 基础设施产品、 PKI 安全应用产品和通用安全产品。公司与客户建立了长期稳定的合作关系并拥有各类经营资质或许可。IDC 数据显示，2018 年公司在身份和数字信任软件市场份额排名第三，达到 11.3%。

图 41：格尔软件 PKI 系统架构



数据来源：格尔软件，东方证券研究所

募投项目将有助于公司扩大业务规模，实现产业链延伸，打开未来成长空间。公司于 2019 年底发布非公开发行股票预案，募集资金将用于“下一代数字信任产品研发与产业化项目”、“智联网安全技术研发与产业化项目”以及“补充流动资金项目”三个项目。其中“下一代数字信任产品研发与产业化项目”是面向云计算、大数据及互联网+等新场景，研发以密码技术为基石，PKI/CA 基础设施为支撑，以身份为中心的下一代数字信任产品，将形成统一密码服务平台、云 PKI/CA 基础设施系统、零信任安全体系产品以及面向联盟链的区块链技术平台等新产品，“智联网安全技术研发与产业化项目”包括面向“智联网”的基础共性技术研究及产品开发、视频监控领域产品和解决方案、车联网领域产品和解决方案等内容，助力公司实现在视频监控、车联网等应用场景下各种产品的部署应用。我们认为若募投项目得到顺利实施，公司将进一步完善自身的产品线，同时把握在视频监控、车联网等领域的先发优势，提升公司的核心竞争力，有望实现高速增长

表 7：公司非公开发行预案募投项目一览

项目名称	建设内容	产品功能
下一代数字信任产品研发与产业化项目	统一密码服务平台	平台采用多租户架构，云原生技术及容器技术，可实现统一的密码设备资源管理、弹性调度，以及密钥管理、密码计算能力的服务化，为上层业务应用提供安全高效的密码服务支撑
	云 PKI/CA 基础设施系统	该系统采用云原生架构和容器化设计理念，可为大规模 PC 及移动用户、IT 设备、应用提供证书管理服务，为身份认证、数据安全传输及访问控制提供基础信任服务

	零信任安全体系产品	**零信任安全体系产品包括云身份服务系统、零信任网关、安全策略管理中心。和传统安全产品的区别在于采用云服务架构设计，通过实现先认证后访问、持续信任评估、动态访问控制等功能，帮助企业在新 IT 环境下构建零信任安全体系**
	面向联盟链的区块链技术平台	拟研发自主可控的面向联盟链的区块链技术平台，以打造区块链密码支撑环境、区块链应用开发和实施体系。应用领域方面，公司将重点专注于：智能制造（航空、汽车等）、智能交通（港口、铁路等）、智能账本（供应链金融、资产交易等）、智能文档（电子存证、电子合同等）
智联网安全技术研发与产业化项目	基础共性技术研究及产品研发	研究面向“智联网”的密码应用技术、网络安全技术、数据保护技术和适应设备管理技术，形成面向智能设备的密码基础设施产品、设备身份认证产品及智能数据加解密产品以及设备信息管理平台产品
	视频监控领域产品和解决方案	根据视频监控系统中前端摄像机、后端平台及使用人员的特点，研发适合视频监控系统的公钥基础设施产品（PKI）、面向摄像机及监控使用人员的视频身份认证产品、视频监控安全网关产品和视频数据加解密产品，并结合公司原有及新研发的各种安全产品，形成视频监控系统安全整体解决方案并进行推广应用
	车联网领域产品和解决方案	针对智能网联汽车及车联网的特点，在兼容国际主流标准的前提下，研究同时支持交通部、工信部、公安部相关安全标准的智能驾驶 PKI 体系，研发智能网联汽车的车端应用中间件和适用于 V2X 的云端应用中间件，实现对智能驾驶过程中，人、车、路、云的身份标识，为包括智能网联汽车、智能道路设施、智能交通在内的各种设备及应用提供可靠密码服务
补充流动资金	—	有助于增强公司资金实力，为保持与强化公司在技术研发与专业人才方面的行业领先地位提供有力保障；缓解公司日常经营的资金压力，支撑业务持续发展

数据来源：公司公告，东方证券研究所

风险提示

1、 网络安全政策落地不及预期

政策是驱动信息安全快速发展的重要力量，若相关政策落地不及预期，导致行业需求出现波动，对行业内相关公司的经营造成不利影响。

2、 零信任安全发展不及预期

若零信任安全架构发展不及预期，会影响相应需求，从而对网络安全整体行业的发展带来负面影响。

分析师申明

每位负责撰写本研究报告全部或部分内容的研究分析师在此作以下声明：

分析师在本报告中对所提及的证券或发行人发表的任何建议和观点均准确地反映了其个人对该证券或发行人的看法和判断；分析师薪酬的任何组成部分无论是在过去、现在及将来，均与其在本研究报告中所表述的具体建议或观点无任何直接或间接的关系。

投资评级和相关定义

报告发布日后的 12 个月内的公司的涨跌幅相对同期的上证指数/深证成指的涨跌幅为基准；

公司投资评级的量化标准

买入：相对强于市场基准指数收益率 15%以上；

增持：相对强于市场基准指数收益率 5%～15%；

中性：相对于市场基准指数收益率在-5%～+5%之间波动；

减持：相对弱于市场基准指数收益率在-5%以下。

未评级 —— 由于在报告发出之时该股票不在本公司研究覆盖范围内，分析师基于当时对该股票的研究状况，未给予投资评级相关信息。

暂停评级 —— 根据监管制度及本公司相关规定，研究报告发布之时该投资对象可能与本公司存在潜在的利益冲突情形；亦或是研究报告发布当时该股票的价值和价格分析存在重大不确定性，缺乏足够的研究依据支持分析师给出明确投资评级；分析师在上述情况下暂停对该股票给予投资评级等信息，投资者需要注意在此报告发布之前曾给予该股票的投资评级、盈利预测及目标价格等信息不再有效。

行业投资评级的量化标准：

看好：相对强于市场基准指数收益率 5%以上；

中性：相对于市场基准指数收益率在-5%～+5%之间波动；

看淡：相对于市场基准指数收益率在-5%以下。

未评级：由于在报告发出之时该行业不在本公司研究覆盖范围内，分析师基于当时对该行业的研究状况，未给予投资评级等相关信息。

暂停评级：由于研究报告发布当时该行业的投资价值分析存在重大不确定性，缺乏足够的研究依据支持分析师给出明确行业投资评级；分析师在上述情况下暂停对该行业给予投资评级信息，投资者需要注意在此报告发布之前曾给予该行业的投资评级信息不再有效。

东方证券 ORIENT SECURITIES

免责声明

本证券研究报告（以下简称“本报告”）由东方证券股份有限公司（以下简称“本公司”）制作及发布。

本报告仅供本公司的客户使用。本公司不会因接收人收到本报告而视其为本公司的当然客户。本报告的全体接收人应当采取必要措施防止本报告被转发给他人。

本报告是基于本公司认为可靠的且目前已公开的信息撰写，本公司力求但不保证该信息的准确性和完整性，客户也不应该认为该信息是准确和完整的。同时，本公司不保证文中观点或陈述不会发生任何变更，在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的证券研究报告。本公司会适时更新我们的研究，但可能会因某些规定而无法做到。除了一些定期出版的证券研究报告之外，绝大多数证券研究报告是在分析师认为适当的时候不定期地发布。

在任何情况下，本报告中的信息或所表述的意见并不构成对任何人的投资建议，也没有考虑到个别客户特殊的投资目标、财务状况或需求。客户应考虑本报告中的任何意见或建议是否符合其特定状况，若有必要应寻求专家意见。本报告所载的资料、工具、意见及推测只提供给客户作参考之用，并非作为或被视为出售或购买证券或其他投资标的的邀请或向人作出邀请。

本报告中提及的投资价格和价值以及这些投资带来的收入可能会波动。过去的表现并不代表未来的表现，未来的回报也无法保证，投资者可能会损失本金。外汇汇率波动有可能对某些投资的价值或价格或来自这一投资的收入产生不良影响。那些涉及期货、期权及其它衍生工具的交易，因其包括重大的市场风险，因此并不适合所有投资者。

在任何情况下，本公司不对任何人因使用本报告中的任何内容所引致的任何损失负任何责任，投资者自主作出投资决策并自行承担投资风险，任何形式的分享证券投资收益或者分担证券投资损失的书面或口头承诺均为无效。

本报告主要以电子版形式分发，间或也会辅以印刷品形式分发，所有报告版权均归本公司所有。未经本公司事先书面协议授权，任何机构或个人不得以任何形式复制、转发或公开传播本报告的全部或部分内容。不得将报告内容作为诉讼、仲裁、传媒所引用之证明或依据，不得用于营利或用于未经允许的其它用途。

经本公司事先书面协议授权刊载或转发的，被授权机构承担相关刊载或者转发责任。不得对本报告进行任何有悖原意的引用、删节和修改。

提示客户及公众投资者慎重使用未经授权刊载或者转发的本公司证券研究报告，慎重使用公众媒体刊载的证券研究报告。

东方证券研究所

地址： 上海市中山南路 318 号东方国际金融广场 26 楼

电话： 021-63325888

传真： 021-63326786

网址： www.dfzq.com.cn