零信任商业价值综述

候选发布版

CSA GCR cloud security alliance® GREATER CHINA REGION

CSA cloud security alliance®

联盟简介

云安全联盟(Cloud Security Alliance,CSA)是中立、权威的全球性非营利产业组织,于2009年正式成立,致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识,推动数字安全产业全面发展。

云安全联盟大中华区(Cloud Security Alliance Greater China Region, CSA GCR)作为CSA全球四大区之一,2016年在香港独立注册,于2021年在中国登记注册,是网络安全领域首家在中国境内注册备案的国际NGO,旨在立足中国,连接全球,推动大中华区数字安全技术标准与产业的发展及国际合作。

我们的工作

联盟会刊下载地址
了解联盟更多信息

加入我们

CSA大中华区官网
(https://c-csa.cn)

点击会员

加入联盟

填写相关申请信息

成为CSA会员

JOIN US

致谢

《零信任商业价值综述（Communicating the Business Value of Zero Trust）》由CSA工作组专家编写，CSA大中华区秘书处组织翻译并审校。

中文版翻译专家组（排名不分先后）：

组长：陈本峰

翻译组：

陈珊　　余晓光　　赵锐

研究协调员：

郑元杰

感谢以下单位的支持与贡献：

华为技术有限公司　　苏州云至深技术有限公司

CSA零信任工作组

零信任研究和指南的业务范围包括云、私有部署以及移动终端等环境，同时也适用于物联网(IoT)和运营技术(OT)。CSA零信任(ZT)工作组的目标是:

- 共同开发和推广零信任(ZT)最佳实践，使其作为一种现代的、必要的、适用云计算的信息安全方法(InfoSec)。
- 为行业提供指导，传达不同零信任方法的优势和劣势，从而让组织可以根据他们的具体情况做出适当的决策。
- 提供成熟的零信任实现方法，同时保持产品和供应商中立。

- 提供零信任相关的权威技术建议，同时保持产品和供应商中立。

英文版本编写专家

主要作者：

Jason Garbis　　Alex Sharpe

贡献者：

Elier Cruz	Josh Woodruff	Saif Azwar	Rohini Sulatycki
Jonathan Flack	Christopher Steffen	Joseph Roblee	Megha Kalsi
Nelson Spessard Jr	Erik Johnson	Andrea Knoblauch	Lars Ruddigkeit
Dr. Ron Martin	Heverin Joy Williams	Rajesh Murthy	Don O’Neil
Akin Isinkaye			

审校者：

Michael Roza　　Osama Salah

CSA分析师：

Erik Johnson

在此感谢以上专家。如译文有不妥当之处，敬请读者联系CSA GCR秘书处给予改正！ 联系邮箱research@c-csa.cn； 国际云安全联盟CSA公众号。

序言

零信任是基于复杂多变的网络安全环境诞生的一种新的网络安全策略，它的出现同时也改变了企业的运营流程并促使了对安全合规的重视。CSA 针对零信任提出了七个原则，这七个原则是让零信任比别的安全策略更为高效的核心，并且任何零信任框架的建设都必须基于这些原则。

零信任的核心意味着企业对于任何访问的信任都是从零开始的，为了帮助人们理解零信任，CSA 概括了三种方法，分别是以始为终、泄露总会发生、风险控制。在了解了这三种方法之后，企业可以更容易地理解零信任并接受它带来的商业价值。

本白皮书以商业价值为核心，提出了提高运营效率、减少成本、提高运营韧性、降低风险、提高合规性、降低合规成本等好处。文中包括了 14 种商业价值，针对各类企业的方方面面，并且它们都有着固定的格式，以供安全专家参考并向企业各部门传达。

零信任现已被许多企业初步采用，其安全高效的特性被许多企业所青睐着，它的出现意味着企业将从上而下地实施着更好的安全措施。然而，这需要安全专家清晰地传达零信任的商业价值，并为此计划，才能让企业在当下的网络安全环境中取得先机。

李雨航 Yale Li

CSA大中华区主席兼研究院院长

目录

致谢 4

序言 6

摘要 9

面向人群 9

目标 9

1. 什么是零信任？ 10

2. 对零信任的理解误区 12

3. 商业价值综述纲领 13

4. 商业价值 14

4.1 商业价值的含义？ 14

4.1.2 商业价值与风险 15

4.2 信息安全的商业价值 16

4.3 为零信任投资做商业案例 18

5. 零信任的商业价值 19

章节格式 20

5.1 商业价值：成本节约与优化 21

5.2 商业价值：运营韧性 22

5.3 商业价值：业务敏捷 23

5.4 商业价值：促进合规 24

5.5 商业价值：维护声誉和品牌价值 25

5.6 商业价值：减少 IT 风险 26

5.7 商业价值：安全地采用新技术 27

5.8 商业价值：加速业务单位整合（并购） 27

5.9 商业价值：更好地利用现有投资 28
5.10 商业价值：提高可视性和分析性 29
5.11 商业价值：改进用户体验 30
5.12 商业价值：支持战略性业务计划 31
5.13 商业价值：重塑业务流程 32
5.14 商业价值：更好地满足潜在客户的安全需求 33
6. 传达商业价值 34
了解你的受众 35
了解你组织结构 35
建立一个团队并形成联盟 35
沟通策略 35
为过程制定计划 36
7. 结论 36
附录 – 有用参考资料 38

摘要

零信任是一个大规模的产业趋势，被全世界许多组织采用以及宣传；它带来了更好的安全性能同时减少支出，并提高商业效率以及灵活性。然而，“零信任”作为一个行业专有名词存在被错误理解或者难以理解。业务领导与非安全专业人才，例如关键决策人、预算持有人、以及监事等，他们在各个组织零信任发展的道路上影响着第一步的成败。这是因为，采用零信任作为一种组织战略，从根本上讲，需要在整个企业中进行支撑与改变，以及投入大量的时间、精力和金钱。所以，安全人员需要传达零信任的理念给非技术以及非专业人员，从下到上直到董事会的成员。我们相信，信息安全产业仍未赋能从业人员可以简洁直接地传达零信任战略的商业价值。这篇 CSA 国际云安全联盟的指南可以弥补这一空白。

面向人群

该文档主要面向人群是信息安全专家与从业者，他们希望向各个组织里的业务领导与重要参与者展示零信任带来的价值与商业影响。

该文档还面向的人群是各个组织里的非技术、非安全方面的从业者。这份白皮书包含部分技术概念，但是也能让非专业人群理解。

目标

该文档为信息安全专家提供信息与思路，以此来有效沟通与展示为什么他们的组织应该投资零信任安全战略。这些沟通是为了向内部参与者展示：例如非安全方面 IT 人员、企业规划人员、财务与预算团队、业务线经理、应用程序所有者、企业首席高管（CEO:首席执行官，COO:首席运营官，CFO:首席财务官）以及董事会成员。

这份白皮书使得安全专家能够向组织里的业务领导与重要参与者展示采用

零信任带来的价值与商业影响[1]。其次，说服组织主动投资零信任。

1. 什么是零信任？

零信任是一个基于若干核心原则的网络安全战略，以简单的、具有可观的积极影响方式作用于组织的架构、方式、运营。根据美国国家安全电信咨询委员会（NSTAC） 《零信任和可信身份管理报告》中的表述：“零信任是一个网络安全战略，假定没有任何用户和资产被隐式信任。它默认破坏已经发生或者即将发生，所以，企业范围内的用户不应该通过简单的认证就允许访问敏感信息。反而每个用户、设备、应用以及交易必须不间断地验证身份。”

根据美国国家标准与技术研究院（NIST）发布的《零信任建设》（SP 800-207）文档定义:

> “零信任（ZT）是一个术语，它是一个不断进化的网络安全范式的集合，从基于网络边界的静态防御，到专注于用户、资产，以及资源。零信任架构（ZTA）使用零信任理念来规划产业和企业的基础设施和流程。零信任假设没有任何隐式信任赋予物理或者网络位置（局域网或者互联网）的资产或者用户账户，或者基于资产拥有权（企业所有或者个人所有）来赋予信任。验证和授权（访问主体和设备）是独立的功能，作用在与企业资源的对话建立之前。”

NIST 文档还提出，零信任“不是单个架构而是一系列关于流程、系统设计和运营的指引原则，它可用作改进任意分类或者敏感等级的安全态势。”其中还包括了 7 个零信任的核心原则，列出以供参考：

1. 所有数据资源和计算服务应当作资源。
2. 所有通信在任意网络位置都应被保护。
3. 对每个企业资源访问权限是基于单次会话赋予的。

[1] Some international efforts use the term “consequences.” ISO 31000, Risk management — Guidelines is an example.

4. 资源访问是基于动态授权 – 包括客户身份，应用/服务，请求的资产的可观测状态 – 也可能包含其他行为或者环境参数。

5. 企业持续监视和衡量所有拥有资产以及相关资产的完整性和安全性。

6. 所有资源的验证和授权是动态并严格强制执行于访问被允许之前。

7. 企业尽可能多地收集关于资产、网络基础设施和通信的当前状态的信息，并利用它来改善其安全状况。

总体来说，零信任很大的程度不同于传统的、基于信任的“城堡护城河”物理网络边界安全架构，因为传统架构在云计算、远程办公、威胁加剧的时代下变得不再高效。

老练的攻击者越来越精于利用在现代高级的分布式企业网络中暴露出的技术或者人力薄弱点，时常严重地影响网络连接稳定性。成功的网络攻击基本上利用了各种方式的信任。这使得“信任”，无论是隐性的还是显性的，这个危险的薄弱点必须被排除。在零信任中，所有的网络数据包都是不可信的，同其他在系统中经过的数据包分别单独对待。信任等级实质上为零，所以被称之为零信任。值得注意的是，这个方法关注的是从数字系统中移除信任，而不是人群、关系或者文化。

零信任是一个全面的网络安全战略，包含云/多云，内部和外部伙伴/参与者用户（企业识别或者自带设备）端点，私有部署以及混合系统，包括 IT（信息技术），OT（运营技术）和 IoT（物联网）。零信任不是产品（尽管基于零信任的安全基础设施可以利用各种不同的产品来实施），也不需要组织剔除更换原有的安全基础设施。零信任驱动着新一代的信息安全的架构方法，使得资源与控制的对齐来保证最低权限的访问，保证每个网络数据包视作不可信，让系统强制在流程的每一层执行“默认拒绝”模型。

零信任方法是一个慎重和谨慎的战略，指引着组织对于基础技术的选择和部署，包括身份、设备、网络、应用和数据尽可能地安全。契合零信任的慎重决定反映了对于日渐增长的危险的认识，以及对更稳固和适应性强的安全态势的需求，利用基于风险的方法来授权访问。零信任的采用包括动态环境、严格

的访问控制、持续的验证、行为监视以及严格的安全规章强制执行。

通过慎重地采用零信任方法，组织志在通过以一个更警惕和怀疑的态度面对网络流量和人工与非人工活动来最小化数据泄露风险和非授权访问风险。

零信任现处在被企业大量应用的早期阶段，而且是美国联邦政府新的网络安全策略的必要部分。同样地，我们期望持续关注如何成功在组织中采用零信任的指引。

2. 对零信任的理解误区

零信任安全是一个战略，不是即买即用的，或者开发即可实施的。作为一个战略，它将影响你的思维、决策、优先级和对 IT 与安全工程的考虑。采用这个战略意味着您的组织架构将会升级和进化到零信任架构。应用得当的话，零信任指引着您对于技术架构的选择和部署，包括身份、设备、网络、应用、数据，以及交叉领域（例如可视化与分析、自动化与编排，还有治理）。

零信任不是防止数据泄露的一招制胜绝招。尽管大多数泄露仅包含数以千计的数据记录，但百万记录级别数据的泄露会使得代价成指数级上升。警惕性和严谨的治理是有效减少以下风险因素的重要方法：

- 网络钓鱼
- 商业电子邮箱泄漏
- 第三方软件漏洞
- 被盗窃或泄漏凭证
- 恶意内部人士
- 云端配置错误
- 社会工程
- 物理安全被攻陷

- 意外数据流失
- 设备丢失

以上这些是数据泄漏的主要来源，并是零信任实施时需要处理的。

零信任不仅仅是技术。市面上有大量的安全技术，在明确的环境中对威胁对症下药。相比技术，零信任更关注的是人和流程，它需要的是齐心协力，把这些要素结合起来，通过自动化策略达成更全面的安全。

零信任并不难，但它要求安全和技术团队与业务方（这个文档的重点）建立合作关系。这带来了组织内的文化转变，可能会一时难以适应，但当这个关系建立完成时，零信任会变得简单许多以及更加高效。

3. 商业价值综述纲领

商业价值纲领由 CSA 国际云安全联盟零信任工作组编撰，其中包括几个可以帮助理解和传达零信任商业价值的方法。

以始为终：这个方针鼓励人们在零信任过程的开始建立关于组织期望方向与明确的展望目标。与商业价值相关的期望结果包括减少合规成本、事故的经济影响、IT 和流程债务的复杂性、残余风险，以及总体拥有成本（TCO）。

泄露总会发生：承认这个事实使得机构不再要求 100%安全这种不现实的目标，转而考虑更有安全韧性这一更容易达成的目标。这个转变带来三个好处：

- 减少泄漏发生时的影响设备波及范围
- 减少黑客在企业里移动和侦察的能力
- 通过限制单次事故的破坏和损失而减少负面影响

风险控制：这是零信任中的关键元素。理解组织的风险偏好可以提供一个容许风险的阈值。零信任的目标帮助机构将内在风险减少至可接受范围，通过实施控制减少可能性、影响，或二者兼而有之。这可使组织变得更坚韧以及更灵活。

采用基于风险的优先级将帮助组织理解和识别他们需要解决的差距。组织可以做个稳妥的决策来选择出发点 – 通常从小问题出发是情理之中，通过快速达成短期目标来改善安全态势并建立零信任倡议的推动力。当选择一个较小且低风险的保护面作为试点时，获得和维护领导层的接纳会更容易，这样就可以利用其指标来突出安全范式的变化并展示商业价值。

传达零信任的商业价值将有效鼓励领导层来发布正确的指令，为成功的零信任过程树立根基。

4. 商业价值

4.1 商业价值的含义？

这一章节是为了向读者介绍普遍的核心商业概念和术语。提供了基础词汇和概念模型使得读者提出更有价值的问题，理解商业驱动因素，构筑一个具有商业意义的零信任应用案例。这一章节并不是全面的商业或者金融管理介绍，因为这方面在网上已经有许多可靠的相关资源了。

除了营利性企业之外，还有许多不同类型的组织，包括非营利性组织、政府机构，以及监管机构，它们并不是传统的企业。比如一个为了监管银行产业的联邦政府机构就不是一个“企业”，但它仍可以从零信任中获益。像这样的组织，它们的商业价值就应该是有助于实现其组织的任务目标。

企业运作在财务或者绩效指标上，已经发展出一套全面的标准来衡量这些指标。如果你的组织是一家公开贸易的公司，就需要公开报告财务状况。这些报告对你来说是必读的，因为它们将你与组织的指标和绩效联系起来，包括面临的战略挑战和机遇。

尽管并非所有以下的指标都适用于每个组织，这个列表涉及了几个你应该熟悉的指标。为了了解组织的具体情况，最明智的可能是在做了一些基础调查后，找财务部门一位友好的同事，问下他们哪些财务术语和指标是对你的组织最重要的。[2]

[2] There are also reputable web references for these terms, including Investopedia Financial Terms

- 营收：季度、年度、年度持续收入
- 净收入或者盈利
- 保证金
- 收入成本和毛利
- 售货成本（COGS）
- 现金流
- EBITDA（税息折旧及摊销前利润）
- 订单兑现和应收账款周转天数（DSO）
- 资产负债表状况
- 股价和表现，绝对价值以及与同行比较
- 遵守监管要求或自愿准则
- 审计和审计结果
- 商誉与品牌价值
- 员工生产力
- 经营效率

不同的角色有着不同的兴趣倾向。例如股东倾向于对健康的股价和/或可靠的股息感兴趣。另一方面，其他利益相关方对别的指标更为在乎，这根据他们的角色而定。

4.1.2 商业价值与风险

企业很大程度上在乎风险。风险控制（RM）原则提出四种风险处理方式：

接受、规避、缓解和转移[3]。近些年来的实践表明了无论接受还是规避风险都不充分。我们知道风险转移，常见于保险，并不防止事故，而且很多时候实际的成本太大。风险缓解仍然是最高效的投资。

缓解需要一系列的管控（技术、人员、流程）来减少风险直至可接受范围。通常来说，管控会花费金钱，消耗资源，并放慢事务的进度。由于零信任是企业的整体战略，因此一个平台和策略模型就可以为隐私、安全、合规性和第三方风险管理（TPRM）等其他领域奠定基础。零信任架构将在基础设施技术和层级之间执行多重控制。

内部威胁的风险对于组织来说是最难管理的，因为它涉及有效访问权限的合法用户（例如员工、前员工、承包商或者商业伙伴），他们拥有着有关组织安全条例、数据和计算机系统的内部信息。威胁可能涉及欺诈、盗窃资产、盗窃知识产权，甚至是破坏。其通常来自内部人员的事故涉及有效访问的滥用。零信任通过执行最小权限的原则，在授权对资产的访问之前，要求正确的身份证明（认证）和有效访问权（授权），以此来减少内部威胁的可能性。它还通过约束横向移动来限制其影响范围。

第三方风险管理，有时被称为供应商风险管理或者供应链管理，是评估和减轻供应商（例如供应商，商业伙伴和供应链成员）引入的风险的实践。这一过程通常从关系刚形成时就开始，并持续维持，包括至关系结束时。零信任战略通过提供更好的可见性和控制来减少任何第三方安全事件的影响，并赋予供应商最小的访问权限来降低这些风险。

4.2 信息安全的商业价值

简单来说，信息安全是指对公司的数字资产、系统和数据的保护和保障。通过实施有效的安全措施，企业可以最小化未授权访问、数据泄露和网络攻击的风险，使其正常运营，维持客户和合作伙伴的信任，避免因安全事件造成的潜在财务损失或者商誉减值。

随着商业和数字经济的普及，信息安全成为组织内部和董事会的首要关注

[3] The International Standards Organization (ISO) uses the terms Retain, Avoid, Optimize, Transfer to refer to these same principles in the ISO 31000:2018(en), Risk management — Guidelines

点。世界经济论坛（WEF）指出，超过 60%的国内生产总值（GDP）是数字化的[4]，同时美国国家经济研究局（NBER）认为企业估值主要由无形资产驱动，其中包括数据和知识产权（IP）[5]。这些资产逐渐成为攻击和破坏的目标，因此必须受到妥善保护。

信息安全基于三个主要概念：机密性（Confidentiality）、完整性（Integrity）和可用性（Availability），它们共同构成了 CIA 三要素。安全策略，实施和安全风险的描述都基于这三个参数：

- 机密性是指公司拥有的对业务至关重要的东西，或者不应被分享的信息，被安全和秘密地保护着，只有那些需要知道的人才拥有访问权。
- 完整性是对企业认为贵重物的保护。这些东西需确保在有关各方不知情的情况下不会被篡改或者改变。信息、数据或事物始终保持其准确性。
- 可用性是物件或者资产在业务需要时可以使用。

如果实施得当的话，信息安全应该也可以支持企业的使命。安全性通过保护企业认为贵重的资产来减少对整个企业的风险，以此来支撑企业。信息安全的成功实施有着额外好处，可以促进对国际和国内标准和法规的合规。遵从许多这些标准和法规（例如 HIPAA、GDPR、PCI DSS 和 ISO 27000）包括关于数据保护，正确的风险管理，限制对受保护数据和流程的访问，以及如何保护这些信息的定期培训。所有这些东西都是正确的信息安全计划的一部分。

从风险管理（RM）和合规性的角度来看，信息技术（IT）和运营技术（OT）系统代表了相当大的风险来源，必须通过实施技术或者流程控制来降低风险。这些控制可以是自定义，或者像遵从法规一样通过外力来强加给它们。组织通常必须通过合规性报告或者审核流程来证明他们的控制是如何按照预期执行的。

零信任通过确保现有控制按预期进行来提高安全性，并为组织提供进一步加强这些控制的持续改进规划。在没有固有信任的环境中，安全团队通过使用

[4] “Digitalization: a silver bullet”, World Economic Forum: https://www.weforum.org/agenda/2022/05/a-digital-silver-bullet-for-the-world/
[5] “Intangible Value”, Andrea L. Eisfeldt, Edward Kim & Dimitris Papanikolaou, November 2021, US National Bureau of Economic Research (NBER): https://www.nber.org/papers/w28056

风险框架来监视、识别、保护、检测、响应，并从感知到的和现有的威胁中修复。这有助于分清轻重缓急，因为任何组织都没有无限的资源和时间。零信任为你所有的网络安全、隐私和运营韧性（OR）的活动提供基础。

零信任不仅提高了控制效率。作为一种首要的战略和架构，零信任打破了组织内部的壁垒，将 IT、安全、应用、架构和商业整合在一个统一的构想下，以保障资产符合商业目标。

4.3 为零信任投资做商业案例

一般来说，商业案例的研究辅助组织的利益相关方做出关于项目提案的可行性决定，并且它的使用被认为是私营和公共组织的标准实践。商业案例通常是一个文档化、结构化的提案，准备它是为了帮助组织决策者对提案的投资或者项目做出选择决定。一个商业案例从商业过程表现、需求和/或问题、期望收益来描述投资或者项目的理由与解释。它确定了要满足的高级需求，并提供了对提案的替代解决方案的分析（包括拒绝或者推进每个选项的理由）、假设、约束、风险调整后的成本效益分析、初步收购策略。它还可能包括财务指标，例如投资回报率（ROI）、预计总拥有成本（TCO）或净现值（NPV）等。

信息安全投资和创收之间很少有足够的联系来使得计算 ROI 或者 NPV 的可行性。相反，信息安全投资通常被视为降低 TCO 的因素，或者作为推动商业价值的促成者。

不同的组织有不同级别的形式、过程和架构来进行决策，并且对商业案例的内容有着不同的期望。实践者应花时间去学习在组织内部技术、战略和 IT 投资决策是如何制定的，并遵循应当的流程和架构。

商业案例一个不变的方面是它必须体现商业价值，这是这份文档的主要关注点。接下来的章节提供了零信任倡议实现商业价值的 14 种不同方式。当你确定了适用的领域，你可以适当地量化它们，并结合到你的组织需求的商业案例结构中。

5. 零信任的商业价值

如前文所述，零信任是一个增强的安全和风险管理方式，它假定身份（真人、非真人/机器），设备（个人电脑、移动设备、物联网）或者工作负载（服务器、计算实例、容器或功能）在默认情况下是不可信的。所有的访问依赖于身份验证以及基于上下文信息的访问策略的评估与授权。

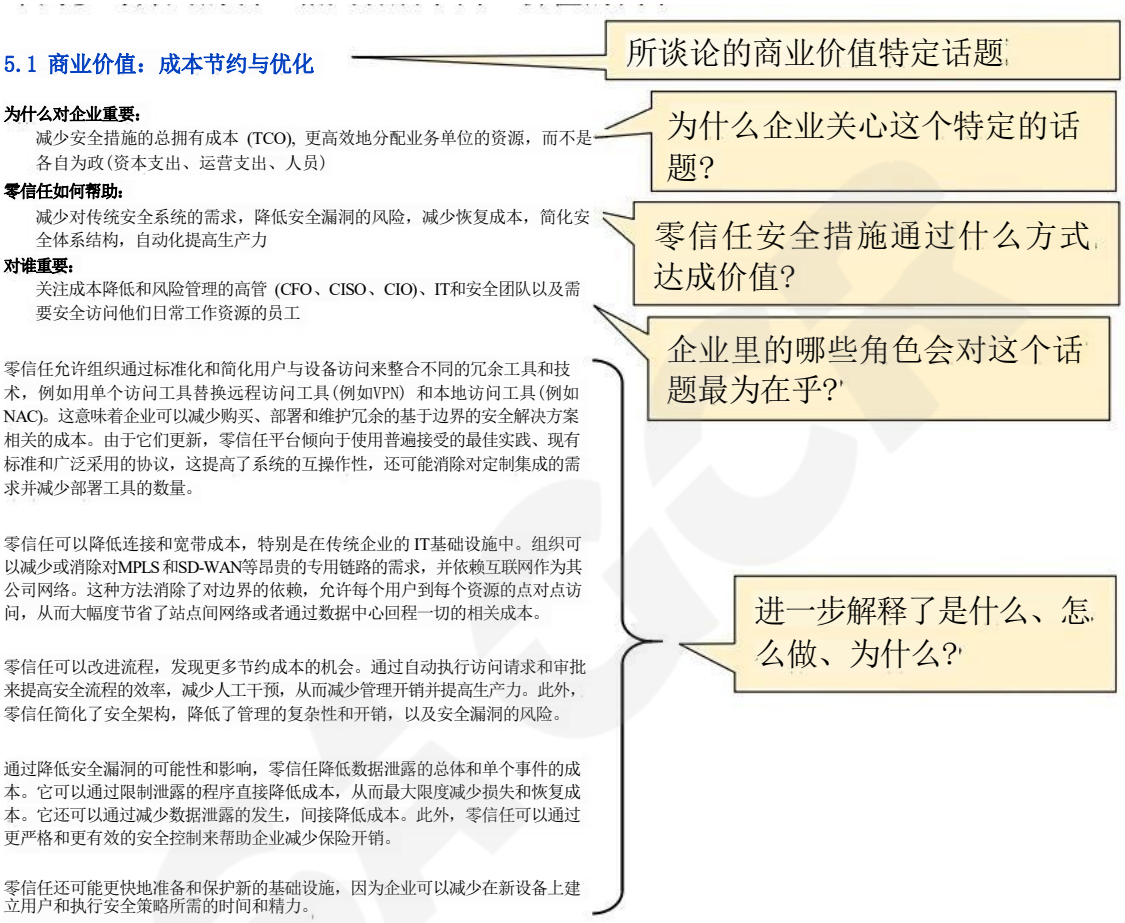
零信任需要持续投入时间、资源和预算，但作为回报，它带来了安全、技术和商业方面的好处。总的来说，零信任通过提供以下商业价值的收益：

- 通过集中和自动化安全策略，简化安全和IT基础设施管理，从而节约成本并提高运营效率。
- 更好地保护敏感数据和知识产权，以免遭受未经授权的访问，提高组织的网络韧性，降低数据泄露和财务损失的风险。
- 提高合规性，避免潜在处罚，保持良好的品牌声誉。
- 减少满足和报告合规性要求相关的时间、成本和工作量。
- 增强组织的灵活性和对商业环境变化的适应性，包括商业流程的重建。
- 增加利益相关者的信心，因为客户、合作伙伴和投资方可以信任组织对安全和数据保护的承诺。
- 通过简化基础设施、集中策略管理和自动化，降低IT和运营成本。
- 将IT和安全人员转变为业务推动者。
- 调整整个组织的业务和安全目标，减少离散的活动。

零信任不同于之前的安全方法，它们承诺了部分或全部这些好处。具体而言，零信任方法本质上是整体的，必须将传统的分离式系统与 IT 安全基础设施层级强制实施动态控制。

章节格式

为了更容易地传递这些总体目标，我们用一页的篇幅简洁地展示它们。以下是一个为参与并购的利益相关者展示商业价值的例子。



5.1 商业价值：成本节约与优化

为什么对企业重要：

减少安全措施的总拥有成本（TCO），更高效地分配业务单位的资源，而不是各自为政（资本支出、运营支出、人员）。

零信任如何帮助：

减少对传统安全系统的需求，降低安全漏洞的风险，减少恢复成本，简化安全体系结构，自动化提高生产力。

对谁重要：

关注成本降低和风险管理的高管（CFO、CISO、CIO）、IT 和安全团队以及需要安全访问他们日常工作资源的员工。

零信任允许组织通过标准化和简化用户与设备访问来整合不同的冗余工具和技术，例如用单个访问工具替换远程访问工具（例如 VPN）和本地访问工具（例如 NAC）。这意味着企业可以减少购买、部署和维护冗余的基于边界的安全解决方案相关的成本。由于它们更新，零信任平台倾向于使用普遍接受的最佳实践、现有标准和广泛采用的协议，这提高了系统的互操作性，还可能消除对定制集成的需求并减少部署工具的数量。

零信任可以降低连接和宽带成本，特别是在传统企业的 IT 基础设施中。组织可以减少或消除对 MPLS 和 SD-WAN 等昂贵的专用链路的需求，并依赖互联网作为其公司网络。这种方法消除了对边界的依赖，允许每个用户到每个资源的点对点访问，从而大幅度节省了站点间网络或者通过数据中心回程一切的相关成本。

零信任可以改进流程，发现更多节约成本的机会。通过自动执行访问请求和审批来提高安全流程的效率，减少人工干预，从而减少管理开销并提高生产力。此外，零信任简化了安全架构，降低了管理的复杂性和开销，以及安全漏洞的风险。

通过降低安全漏洞的可能性和影响，零信任降低数据泄露的总体和单个事

件的成本。它可以通过限制泄露的程序直接降低成本，从而最大限度减少损失和恢复成本。它还可以通过减少数据泄露的发生，间接降低成本。此外，零信任可以通过更严格和更有效的安全控制来帮助企业减少保险开销。

零信任还可能更快地准备和保护新的基础设施，因为企业可以减少在新设备上建立用户和执行安全策略所需的时间和精力。

5.2 商业价值：运营韧性

为什么对企业重要：

运营韧性是在任何危险造成的中断下依然可以开展业务包括关键业务和核心业务功能等运营的能力。企业运营通常完全依靠 IT 技术和系统，而脆弱或不可靠的 IT 基础架构将会对企业产生重大的破坏性影响。企业运营的基础架构系统的韧性必然是关键重点。

零信任如何帮助：

默认情况下，零信任架构中的系统和设备彼此隔离。只有通过验证和授权的身份才能通信，并且仅限于授权的协议。

零信任的细粒度隔离降低了攻击者执行侦察或横向移动的能力。攻击的影响范围越小，整个系统的韧性更强。零信任平台还通过快速适应和允许访问变化的环境（例如 DR 站点），从而改进业务连续性和灾难恢复的准备和执行工作。

对谁重要：

首席运营官（COO）、首席执行官（CEO）、首席财务官（CFO）、运营团队、业务领导

零信任策略应当基于一种由内而外的方法，企业应该深思熟虑地询问我们在对抗什么？我们在保护什么？可以根据资产的价值来确认策略的优先级，通常至少在一定程度上是根据他们交付的服务或他们支持的流程来决定的。这样可以更好地与业务保持一致，还可以增加业务的韧性。

采用零信任框架可以全面减少恶意行为者遍历网络的能力来降低风险，并通过高级隔离和授权来减少勒索软件的影响。正确实施零信任控制可以显著减少勒索软件或其他漏洞利用的影响范围。这在保护关键网络设施免受以网络为中心的攻击风险中尤为珍贵，这些风险通常来自受害用户和 VPN 连接。

从运营的角度来看，由于其主动性和有效的事故最小化，它降低了与业务运营相关的风险，并允许更精简的维护团队。并且，它还提供了强大的业务持续性和灾难恢复流程，实现运营韧性。

5.3 商业价值：业务敏捷

为什么对企业重要：

快速响应市场变化和商业机会的能力非常珍贵，并可对其成功产生巨大影响。能使业务更加灵活的技术或方法通常非常有吸引力。

零信任如何帮助：

通过简化和动态、实时的策略来增强安全性，同时提高生产力。

改进的预防措施和减少的安全维护开销，使企业随时准备并专注于抓住商业机会。即使只是为安全团队腾出时间以便更好地与业务协作，也是有价值的。

对谁重要：

首席执行官（CEO）、首席流程官（CPO）、首席信息安全官（CISO）、首席技术官（CTO）、首席信息官（CIO）、首席运营官（COO），风险、运营团队

零信任模型提供了适应不断变化的业务需求的灵活性。当员工在改变组织角色时，或者当新系统上线应用市场机遇时，访问策略可以自动调整。这使组织在不损害安全性的情况下能够快速适应不断变化的业务需求。

零信任模型确保职员可以在任何地方、任何设备上安全地访问公司资源。这通过提供对资源的安全访问来促进远程工作，允许职员在保持安全标准的同

时轻松访问完成工作所需的资源。通过对不同部门和团队提供资源的安全访问，允许员工更轻松地协助，并在不损害安全性的情况下共享资源，从而提高生产力。

零信任通过提供统一的控制平面和策略模型来简化企业安全架构的操作，从而提高系统管理和用户访问的效率。这使得组织能够在管理风险的同时快速行动以追求商业机会。此外，设备状况、恶意软件状态以及对安全策略的更改都会被持续监控和验证，允许组织能自信而敏捷地执行。

不仅如此，零信任通过提供可应用于任何环境的全面安全框架，加快了像云计算和移动设备等新技术的采用。通过增强组织的安全态势并最小化安全漏洞的风险，零信任可以在保持严格的安全协议的同时更快、更顺畅地部署新的应用和服务。

5.4 商业价值：促进合规

为什么对企业重要：

合规要求可能是政府或行业监管机构强加给企业的，也可能是企业为了通过获得各种认证来提高其级别而自愿采用的。在这两种情况下，组织都要求证明它符合合规标准。这些标准通常规定了各种技术和流程控制。合规报告是记录和证明这些控制是适当且有效的行为。未能满足合规要求可能会导致罚款，而且可能数额巨大。

零信任如何帮助：

零信任系统需要对动态和上下文感知策略进行积极评估。因为这些策略是动态的，因此减少执行策略所需的人工工作量。而且，由于它们可以绑定到业务流程，这些系统通常可以自动生成合规报告。零信任系统可以减少执行控制和报告合规要求（创建审计文档）的成本和工作量。它们还确保组织持续合规，而不仅仅是定期合规。

对谁重要：

董事会、合规团队/首席合规官、治理风险合规（GRC）团队、首席财务官

（CFO）、应用所有者

满足和报告合规需求通常是复杂、耗时和昂贵的。零信任会在很多种方式中减少这种开销。首先，由于零信任系统是基于上下文的自动化策略，这对于它们来说更容易实现并保持合规。这是因为策略，通常被描述成有意义的业务术语，会自动适应身份或关联设备的变化，来确保组织持续合规。

其次，零信任系统的控制集通常是自动文档化的。当范围内资产的策略清晰且一致时，所有流量都被加密，所有访问都被记录，证据收集的负担和时间减少，从而减少审计本身带来的组织负担。换而言之，零信任架构减少了开销和合规审计给组织带来的“麻烦”。

5.5 商业价值：维护声誉和品牌价值

为什么对企业重要：

当今世界，网络威胁和数据泄露变得越来越普遍，安全已成为各种规模的企业的关键忧虑。数据泄漏不但会导致财务损失，还会导致声誉受损，影响公司的品牌价值和股价。所以，企业需要采取措施来增加安全性，捍卫自己的品牌价值。

零信任如何帮助：

零信任架构将强化组织作为目标，加快威胁检测和响应，并减少成功攻击的影响。这些好处将通过减少网络攻击的频率和影响来保护其声誉和品牌价值。

对谁重要：

企业品牌和声誉的安全和保障涉及许多利益相关者，包括批准预算的高管、部署安全系统的 IT 领导、确保合规的法务人员以及监视安全协议的人力资源人员。零信任是公关消息传递和客户对数据保护期望的有用参考。

通过实施这些措施，企业可以保护其数据免受未授权访问、盗窃和其他网络威胁。企业还可以投资于能够实时监测和响应威胁的安全监控工具。这些工

具可以帮助企业快速识别和响应安全事故最小化泄漏造成的损失。

总之，提高安全性和捍卫品牌价值是企业的优先任务。通过实施强大的零信任网络安全架构，对员工开展最佳实践教育，投资安全监控工具，并制定危机管理计划，企业可以保护其数据和声誉免受网络威胁。

5.6 商业价值：减少 IT 风险

为什么对企业重要：

管理和处理 IT 风险来减少安全事故的影响对于各个行业的组织来说是至关重要的，这些事故可能会严重影响业务运营、收入产生和商业声誉。减少 IT 风险有助于保护敏感信息、保持生产力，确保不间断的服务交付，并满足合规性和监管要求。

零信任如何帮助：

组织需要一种动态和全面的方法来增强安全态势并减少相关风险。零信任架构假定不具有固有的信任，并促进动态的、基于风险的、强大的身份与访问控制，基于上下文和自适应的分段、持续监控和主动安全措施。因此，零信任促进了强大的安全态势，保护了关键资产，防范了复杂的网络威胁。

适用对象：

减少 IT 风险对于包括第三方在内的各类组织利益相关者至关重要。业务领导负责通过风险减少措施来确保组织安全和减少 IT 风险。负责评估、实施、管理和监控风险减少策略的 IT 和安全团队。处于前端的终端用户，以及他们的意识、行动和遵循与适应的意愿，可以显著影响零信任策略的采用过程。

采用零信任架构使组织通过实施严格的访问控制来降低网络安全事故的可能性，并确保用户和设备在访问资源前持续验证和授权，从而最小化未授权访问的风险。它还可以更好地了解和响应潜在异常活动，并创建和运行更具韧性的网络。此外，划分网络和限制横向移动可以最小化潜在事故的影响半径，确保任何安全泄漏都被遏制并减轻其影响。

这些降低风险的措施加强了组织的整体网络安全态势，提供更强的韧性以对抗数字领域中不断进化的威胁。

5.7 商业价值：安全地采用新技术

为什么对企业重要：

灵活性、减少成本、与时俱进

安全地采用新技术是在不断变化的环境和不断增长的收入中保持竞争力的关键。

零信任如何帮助：

由于其灵活性，良好构建的零信任架构应该能够无需大量重建和相关成本即可集成新技术。零信任本质上是关于使用更广泛的上下文信息来做出访问决策。

对谁重要：

工程师、财务、信息安全人员、产品所有者

采用基于零信任的架构将导致任何从新云、物联网到人工智能之类的新技术的采用更加安全，因为零信任专注于保护资源（包括基于云的资产、服务、工作流、网络账号、结构化与非结构化数据等），而不仅仅是网络段或 IP 地址。

例如，新的基于云的服务可以很容易地合并到企业的零信任策略模型和实施点中，并绑定到他们的身份验证系统中。这使企业可以在不牺牲安全性或生产力的情况下快速使用这项新技术。

5.8 商业价值：加速业务单位整合（并购）

为什么对企业重要：

短期：由特定人员从“随时随地”访问关键业务系统，将提高并购准备效

率，加速并购执行与整合，增加并购成功的可能性。

中期：由于标准化、重新架构和更改 IP 寻址方案，收购公司系统和网络的集成通常是昂贵、缓慢和痛苦的。这增加了成本和时间，降低并购活动的价值。

零信任如何帮助：

为用户和系统提供几乎即时的精确访问，实习协助和数据交换。

避免昂贵而缓慢的网络集成和 IP 地址重新映射。

为旧系统添加现代身份验证，在获得的系统上覆盖更强的安全层。

对谁重要：

财务部门、战略部门、主导收购的业务部门

企业兼并和收购(M&A)通常对企业具有战略重要性，涉及大量资金，并且通常具有很大的紧迫性。他们也经常失败——《哈佛商业评论》指出，70%到90%的收购都失败了，“整合”是主要的潜在挑战。

整合是一个多维度的问题，因为对数据和计算机系统的访问几乎是当今业务每一个方面的基础，而且访问系统可能以非常重要的方式帮助或阻碍被收购公司的整合。零信任可以通过两种方式加速访问。

首先，在短期内，零信任系统将使正确的人（或系统）能够精确访问正确数据和操作系统。这既应用于收购前的尽职调查，也应用于即时的收购后整合任务。关键人员的访问至关重要且时间敏感，企业必须在不损害安全性的情况下这样做。

其次，在收购完成后的中期，零信任系统可以快速部署一致和标准化的访问方法、身份、验证和策略实施。零信任平台通常允许不对被收购公司进行完整的网络改造的情况下实现目标。

5.9 商业价值：更好地利用现有投资

为什么对企业重要：

减少运营成本和现有投资间更好的集成，提供更好的可见性和对威胁的响应。

零信任如何帮助：

通过将控制简化到更少的平台，并最大程度地提高技术之间的集成，零信任可以创建一个简化的集成技术堆栈，具有更低的运营成本和更高的安全效率。

对谁重要：

首席信息安全官（CISO）、首席信息官（CIO）、采购、首席财务官（CFO）、安全运营

由于零信任结构利用了常用部署的安全基础设施的最佳实践，因此组织不必为了满足需求而购买新技术，只需要当前使用的现有技术能满足控制的需要。

例如，通常可以使用现有的身份和访问平台作为起点，并使用动态触发的多因素验证（MFA）和其他上下文分层，如设备运行状况和位置，来提供更粒度的访问控制。从那时开始，网络基础设施可能会减少，但是对于拥有传统内部工作负载的组织，可以根据要求继续利用当前的投资。

在大多数组织中，很可能已经有一些控制和活动非常适合零信任策略，并且应该扩展以覆盖企业内更广泛的范围。通过在整体零信任策略模型中增加现有平台的利用率，组织可以开始逐步淘汰一些重点产品，以支持整合，从而提高效率并降低运营成本。

5.10 商业价值：提高可视性和分析性

为什么对企业重要：

改进并增强数据收集，并将数据转换为信息和知识，使企业能够做出与风险和这些决策的成功或失败相关的明智的安全决策。

零信任如何帮助：

收集和报告身份和上下文增强数据提供了跨风险领域的可见性，以及特定变更对整个环境的总体影响。这种可视性还允许更好地识别资源需求，以及决策可能影响的过程。

对谁重要：

首席战略官（CSO）、首席信息官（CIO）、首席运营官（COO）、首席财务官（CFO）

IT、运营和安全团队经常被困扰于不完整、过时的资产库存和其使用信息。零信任，因为它以默认拒绝的方法运行，需要标识和/或身份验证才能使用。作为零信任体系结构的副产品，这导致了对基础设施和资产的更清晰、更准确的描述。

这增加了对系统的可视性和更准确的库存，允许更好、更准确的访问策略改进的安全事件响应。例如，在一个激活的安全事故中，准确识别所有受影响的环境和过程允许更及时、更完整的响应。更好的可视性转变成根据业务需要修复的系统的优先级，还可以识别和监控响应的完整性。在响应期间，安全和运营团队可以额外关注更脆弱的或业务关键的系统。

准确和最新的库存信息以及实际使用情况的可视性还有助于根据流程的变化对当前和计划的许可成本进行适当的调整。物理设备库存有助于维护成本，以及基础设施生命周期管理。

5.11 商业价值：改进用户体验

为什么对企业重要：

用户生产力是企业效率、盈利能力和竞争力的核心。消除挫折和障碍也是留住员工的良好策略。

IT 是提高企业用户生产力的关键工具，但它往往是人们认为或实际的分歧来源。

零信任如何帮助：

零信任可以消除各自为政和过时的访问系统，支持新技术的安全采用，减少网络延迟，避免与安全相关的停机时间。

对谁重要：

所有用户、首席财务官（CFO）、首席运营官（COO）、人力资源部（HR）、首席执行官（CEO）、首席信息官（CIO）、业务领导

零信任通过提高生产力、减少网络延迟、提高灵活性和提高员工满意度来改善用户体验。它使用户能够随时随地能够安全地访问资源，提高生产力，平衡工作与生活。通过更贴近用户和资源应用安全控制，可以加快访问流程，确保无缝和高效的用户体验。零信任的自适应特性使得组织能够快速响应不断变化的业务需求和威胁，提高灵活性和灵敏度。这反过来又有助于提高员工满意度和保留率。

零信任对细粒度访问控制的关注提高了“需知”策略决策的准确性。它确保用户保持充足的生产力，同时最小化未授权访问的风险，增强整体安全性。

尽管实施零信任通常需要对现有流程进行更改，但它提供了一个解决技术负债和现代化安全基础设施的机会。提高安全性，减少风险，增强用户体验的长期好处胜过了暂时的不便，这使得零信任成为寻求最佳化其组织的安全态势的一个有价值的框架。

5.12 商业价值：支持战略性业务计划

为什么对企业重要：

被定义为“战略性”的业务计划对于企业获得竞争优势、推动增长和盈利能力、适应变化、提供利益相关者的价值和使组织面向未来。

由于他们的战略性质，它们必须取得成功。

零信任如何帮助：

通过建立稳固的安全基础，零信任使组织能够接受创新，满足监管要求，安全地集成新资产，并促进信任的合伙关系。

对谁重要：

首席信息官（CIO）、首席财务官（CFO）、首席运营官（COO）、首席执行官（CEO）、董事会

通过为各个关键领域提供安全的基础，零信任在支持战略业务倡议方面发挥着至关重要的作用。首先，在数字化转型的背景下，零信任使组织能够自信地接受新技术，扩展其网络，并在不损害安全性的情况下促进远程工作和远程访问。它确保基于身份和授权对资源的访问，保护敏感数据并减轻泄漏风险。

此外，零信任通过提供一个框架来安全地整合（或分离）不同的网络、系统和用户群，从而支持对组织结构的战略性业务变革，例如合并、剥离或收购。它允许组织在集成过程中实施一致的访问控制、身份验证和敏感数据的保护。类似地，零信任通过将访问控制扩展到组织的边界之外以促进安全的合伙协作。安全身份联合和访问管理等机制使得组织能够与外部各方协作、共享资源并保护知识产权。

5.13 商业价值：重塑业务流程

为什么对企业重要：

业务流程是商业活动的核心，使用安全技术改造业务流程可以提高效率、更好的竞争优势、提高利润率、更有效地优化资源，以及增强客户体验。

零信任如何帮助：

零信任模型支持任何用户对任何资源的安全访问，扩展了新的和改进的业务流程的可能性，而不受传统IT和安全架构的位置或基于网络的限制。

对谁重要：

高管和业务领导、安全专家、员工、最终用户和客户、股东和投资人、监管机构和合规机构

大数据、云计算和无服务器计算的融合推动了新技术的采用，旨在提高运营效率和用户体验。因此，许多组织正在评估他们现有的业务流程，并拥抱数字化转型。在此过程中，识别和消除不必要的过程以及处理任何不再服务于目的的“无效代码”是至关重要的。这种主动的方法大量减少了总体攻击面，并改善了组织的安全态势。

在业务流程（重新）设计期间，组织应该认真评估每个工作流、访问控制机制和身份验证过程，以确保信任不是自动授予而是持续验证。采用最新权限访问策略和定期监控与分析流量及工作流行为，以检测异常。通过从零信任的角度评价业务流程，组织可以获得几个好处。首先，它们通过消除隐性信任假设、仔细检查对敏感信息的访问以及使用粒度授权策略加强访问控制显著改善其安全态势。这反过来又降低了未授权访问、数据泄露和内部威胁的风险。此外组织通过实施稳固的数据保护措施和可审计的访问控制来增强合规性。

零信任使组织能够减轻转换计划的风险。组织通常采用云服务，采用机器学习和移动性，并在过程中集成第三方系统和合作伙伴。这些新的数字功能扩大了攻击面并引入了潜在的缺陷。然而，通过实施零信任，组织确保对敏感资源和数据的访问不断得到验证和授权，无论位置或使用的设备。

零信任促进了一种更加敏捷和灵活的转换方法。传统的安全模型通常阻碍创新，妨碍新技术和新流程的采用。使用零信任，安全成为转换策略的一个组成部分，使组织能够接纳新技术，简化流程，并在保持稳固安全态势的同时向客户传达价值。

5.14 商业价值：更好地满足潜在客户的安全需求

为什么对企业重要：

为了与客户开展业务，许多组织越来越服从客户的需求。尤其是企业更频繁地对其供应商、合作伙伴和厂商强加更严格的网络安全要求，通常在第三方风险管理计划下。

零信任如何帮助：

采用零信任允许组织大量地改进其安全性，并且更容易和有效地证明他们已经这样做了。

这允许企业能够更快速、可靠地获得新客户，留住现有客户，并更容易、更便宜地获得资金和网络保险。

对谁重要：

首席财务官（CFO）、首席风险官（CRO）、首席执行官（CEO）

考虑到当今数字业务的高度互联性和恶意行为者的复杂性，许多企业开始对其厂商、供应商和合作伙伴实施更严格的安全要求。这些通常是在诸如厂商风险管理和第三方风险管理等计划下实施的。最重要的是这意味着需要来自第三方的更高级别的成熟度、文档和合规性。这些要求既适应于潜在的新供应商，也适用于现有的供应商。

从供应商的角度来看，满足这些增强的安全需求是必要的，而且考虑到它对业务总收入的直接影响，必须迅速成为业务优先事项。

零信任，因为它建立在现代安全最佳实践的基础上，将使这些组织改进其安全性、合规性和凭证，并增加业务收入。任何客户是其他企业的企业都可能已经或在不久后的将来面临这些更严格的安全要求。因此，这个实例通常是安全团队用来为其零信任项目争取支持的最佳候选案例。

6. 传达商业价值

在大多数组织中，零信任的固有和“显而易见”的安全优势有可能还不足以说服利益相关者做出改变、分配时间或投入预算。为了最好地传达我们在本文档中讨论的商业价值，我们建议采用以下方法。

了解你的受众

零信任可以转换为业务的大小方面以及其支持的IT基础设施和流程。这需要改变现状，而许多组织天生抵制改变。为了克服这个问题，重要的是要传达它将带来的业务价值，这是本白皮书的主要目标。有效的沟通需要了解你的听众，所以了解组织中关键利益相关者和决策者的角色，个性和动机是很重要的。这些知识允许你更好地调整你的方法、信息和内容，以最大限度地获得这些受众的理解和支持。

了解你组织结构

花时间了解你的组织是如何构建的。谁负责哪些方面，如何衡量他们的成功？这可以帮助你更容易地找到当前的需求、优先级和项目，你可以将零信任与其关联并挂钩。确定组织中谁负责（拥有）整体任务的哪些部分，以及这对他们和他们的团队来说意味着什么。

建立一个团队并形成联盟

我们将强调零信任不能仅仅是一个以安全为主导的倡议。为了获得进行变革和投资所需的资源，安全需要支持商业倡议。努力与关键业务和技术利益相关者建立联盟，并获得执行领导甚至董事会的支持。为了取得最大化的成功，零信任需要在整个组织的多个级别上得到理解和支持。

沟通策略

与你的安全团队合作，有意识地学习如何使用业务语言，以及如何为特定的相关受众定制信息。技术或安全演示不会让许多人铭记。因此要了解你的受众，并与IT和安全组织之外的友好支持者一起实践。

为过程制定计划

要承认零信任不是一蹴而就的。它将根据业务风险、预算、技术成熟度和改变容忍度分阶段实施。让每个人都为这段过程做好准备，并计划快速兑现一些价值，以建立势能和支持。

7. 结论

本文档为负责制定零信任项目业务的安全领导提供了重要的背景信息。它旨在帮助这些安全领导者通过将其与对其组织最重要的业务驱动因素和业务价值连接起来，来证明其实现零信任体系结构的合理性。通过使用本文档中描述的一个或多个业务价值，并将它们应用于（并适应）其组织的细节，安全领导将能够提出采用零信任的有力理由。

一个全面的零信任网络安全框架提供了几个关键的商业价值和优势。以下是采用基于最佳实践的零信任战略对所有组织都有价值的一些原因：

1. **减少风险：**帮助识别和评估组织信息资产的潜在风险，包括敏感数据、知识产权和关键系统。通过向IT/IOT项目组合实施安全控制和最佳实践，企业可以有效地减少具体的风险并最小化安全漏洞、数据泄露和其他网络威胁的可能性。

2. **监管合规：**许多行业和管辖区都有组织必须遵守的特定网络安全法规和合规要求。零信任框架有助于企业履行这些义务，并展示对数据保护和隐私的承诺。遵守相关法规可以避免法律和经济处罚，并提高组织在客户和合作伙伴中的名声和信誉。

3. **业务持续性：**网络安全事故可能会中断业务运营，造成财务损失，并损害组织的声誉。像零信任这样的战略方法可以帮助企业更好地了解威胁态势，并能够更好地建立稳固的事故响应计划、灾难恢复程序和业务持续性策略。这些措施确保在安全漏洞或系统故障的事件中，组织可以迅速响应最小化停机时间，并以最小的中断恢复正常操作。

4. **竞争优势：**在当今的数字环境中，客户和合作伙伴在选择与谁开展业务时优先考虑安全性。实施全面的零信任网络安全框架允许企业能够展示其保护敏感信息和维护数据完整性的承诺。这种承诺可以将他们与竞争区分开来，并赋予他们竞争优势，吸引重视数据隐私和安全的客户。

5. **信任和顾客信心：**强大的网络安全态势可以在顾客、客户和利益相关者之间建立信任和信心，允许组织展示客户信息安全。这种信任转换为长期的顾客关系、重复购买、积极的品牌声誉和增加的顾客忠诚度。

6. **节约成本：**虽然实施零信任网络安全框架需要初始投资，但它可以节省长期成本。积极主动的安全措施，如风险评估、安全控制、员工培训和漏洞管理，有助于尽早识别和解决安全漏洞，从而减少安全事故的潜在影响和相关成本。此外，专门的方法可以指导跨业务部门的有效资源分配，帮助企业充分利用其网络安全投资。

7. **简化、可扩展性和灵活性：**网络安全框架提供了一种管理网络安全风险的结构化方法。它们提供了指导方针、标准和最佳实践，可以根据组织的特定要求、规模和行业进行调整。组织范围的零信任战略可以促进这种可扩展性和灵活性，使企业能够适应新的安全措施以应对进化中的威胁，确保其网络安全实践保持有效和最新。并且，通过消除安全和运营的复杂性，组织可以获得更好的结果。

总之，零信任网络安全方法可以通过减少风险、促进监管合规、保持业务持续性、提供竞争优势、建立信任和顾客信心、简化运营、节约成本以及在管理网络安全风险、威胁和缺陷方面实现可扩展性和灵活性来提供商业价值。利用零信任功能可以帮助企业同步、放大当前和未来的技术投资，并将其与商业价值联系起来。零信任帮助组织打破孤岛，建立网络安全、财务、IT和业务领导的统一认知，推动核心业务部件（人员、流程和技术）的影响和彻底变革。

附录 – 有用参考资料

云安全联盟（CSA）在零信任推进中心（ZTAC）中维护着一个资源中心。值 得一提的是，ZTAC资源中心和CSA零信任生态圈社区 – 列举了许多零信任相关的演示报告的录制，其中包括了几个关系到商业价值，获得行政、计划和预算 等支持的成功案例录制。

本文中引用的云安全联盟CSA零信任研究的基础资源包括：

- 美国的国家安全电信咨询委员会（NSTAC）《零信任和可信身份管理报 告》
- 美国国家标准与技术研究院《零信任架构》（SP 800-207）
- 美国网络安全和基础设施安全局《零信任成熟度模型V2》

云安全联盟CSA也维护着相关术语参考：

- 整体云安全词汇表
- 云安全联盟软件定义边界词汇表

CSA GCR cloud security alliance GREATER CHINA REGION ®

Cloud Security Alliance Greater China Region

扫码获取更多报告

云安全联盟大中华区
官网：https://c-csa.cn 电话：0755-86548359
地址：上海市浦东新区东育路255弄5号3FB30（前滩国际经济组织集聚区）/
广东省深圳市南山区粤海街道北京航空航天大厦1号楼905