网络空间安全丛书

零信任安全架构设计与实现

[美] 杰森 • 加比斯(Jason Garbis)
杰瑞 • W. 查普曼(Jerry W. Chapman) 著

吕丽 徐坦 栾浩 译

清華大學出版社

北 京

北京市版权局著作权合同登记号　图字：01-2023-0678
Zero Trust Security: An Enterprise Guide
by Jason Garbis and Jerry W. Chapman
Copyright © 2021 by Jason Garbis and Jerry W. Chapman
This edition has been translated and published under licence from Apress Media, LLC, part of Springer Nature.

本书中文简体字版由Apress出版公司授权清华大学出版社出版。未经出版者书面许可，不得以任何方式复制或抄袭本书内容。

本书封面贴有清华大学出版社防伪标签，无标签者不得销售。
版权所有，侵权必究。举报：010-62782989，beiqinquan@tup.tsinghua.edu.cn。

图书在版编目(CIP)数据

零信任安全架构设计与实现 / (美) 杰森 • 加比斯 (Jason Garbis)，(美) 杰瑞 • W. 查普曼 (Jerry W. Chapman) 著；吕丽，徐坦，栾浩译. —北京：清华大学出版社，2023.4
(网络空间安全丛书)
书名原文：Zero Trust Security: An Enterprise Guide
ISBN 978-7-302-63150-7

Ⅰ. ①零… Ⅱ. ①杰…②杰…③吕…④徐…⑤栾… Ⅲ. ①计算机网络—网络安全 Ⅳ. ①TP393.08

中国国家版本馆 CIP 数据核字(2023)第 053386 号

责任编辑：王　军
装帧设计：孔祥峰
责任校对：成凤进
责任印制：朱雨萌

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-83470000　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：三河市春园印刷有限公司
经　　销：全国新华书店
开　　本：148mm×210mm　　**印　　张**：8.625　　**字　　数**：291 千字
版　　次：2023 年 6 月第 1 版　　**印　　次**：2023 年 6 月第 1 次印刷
定　　价：79.80 元

产品编号：093778-01

译 者 序

我国的“十四五”规划和2035年远景目标纲要提出：“加快推动数字产业化”“推进产业数字化转型”，为打造数字经济新优势指明了方向。在数字经济正成为经济发展的核心驱动力的同时，云计算、大数据、物联网、5G等新兴技术的普及对企业运营模式产生了潜移默化的影响，内部员工、业务合作伙伴甚至供应商对企业资源的访问需求日益增多，企业传统的基于“边界”的IT架构已无法满足业务需求，“去边界化”转变已是大势所趋，而以“边界”为防护核心的传统网络防护架构逐渐失效，在日益频繁的网络攻防对抗中暴露出弊端。

2019年底一场突如其来的疫情，迫使企业快速转入远程办公模式，无形中加速了“去边界化”的转变进程。根据中国互联网信息中心发布的第50次《中国互联网发展状况统计报告》，截至2022年6月，中国远程办公用户达4.6亿，占全国网民人数的43.8%。疫情对社会生产生活方式的转变仍会继续，云办公将成为数字经济时代的新常态，企业迫切需要重新定义网络安全，以应对新常态下产生的新风险。

John Kindervag在2010年创造性地提出“零信任(Zero Trust)”一词，用于描述一种安全模型。按照NIST在《零信任架构标准》中的定义：“零信任提供了一系列概念和思想，在假定网络环境已被攻陷的前提下，当执行信息系统和服务中的每次访问请求时，降低决策准确度的不确定性”。零信任代表了新一代的网络安全防护理念，推翻了传统的默认“信任”——默认不信任企业网络内外的任何人、设备和系统，基于身份认证和授权重新构建访问控制的信任基础，从而确保身份可信、设备可信、应用可信和链路可信。用一句通俗的话概括，就是“持续验证，永不信任”。然而，零信任是一种安全理念，而不是单一的技术或产品，这就意味着不存在统一的零信任解决方案；组织需要根据自身传统IT架构、安全运营及安全风险的差异，系统地规划零信任实施策略和方案。

有鉴于此，清华大学出版社引进并主持翻译了《零信任安全架构设计与实现》一书。本书从零信任的历史和发展讲起，系统、详尽地介绍零信任的基础

概念和基本原则；通过理论和实践描述零信任架构；深入探讨 IT 和安全技术，以及与零信任的关系；跨越应用程序、数据、身份、运营策略的界限，探索零信任安全的各个方面。通过讨论成功实现零信任的战略和战术方法，分享关于在组织的环境中最合理地实现零信任的想法和建议，引导企业思考如何应用零信任提高组织的安全性和效率。

本书第一作者 Jason Garbis 持有 CISSP 认证，拥有美国康奈尔大学的计算机科学学士学位和美国东北大学的 MBA 硕士学位，在安全和技术公司拥有 30 多年的产品管理、工程和咨询经验，担任云安全联盟 SDP 零信任工作组的联合主席，研究并发布项目提案。本书的另一位作者 Jerry W. Chapman 是一名经认证的 Forrester 零信任战略师，拥有 DeVry 大学计算机信息系统学士学位，具有超过 25 年的设计和实施身份和访问管理战略的行业经验，活跃于身份定义安全联盟的技术工作组，是 IDSA 组织的创始技术架构设计师。两位作者开展了大量的零信任研究，完成这本极具价值的专业书籍，深入浅出地讲解零信任相关知识和实施策略，本书可作为组织及其安全专家实施零信任的权威参考材料。

本书翻译工作历时 10 个月全部完成。译者团队力求忠于原著，尽可能传达作者的原意。参与本书翻译和校对工作的专家们辛勤付出，保证了书稿内容表达的一致性和文字的流畅。栾浩、吕丽、徐坦、姚凯和王向宇在组稿、校对和通稿等工作中投入大量时间和精力，保证了全书在技术上符合零信任安全工作实务要求，以及内容表达的准确性和连贯性。

同时，还要感谢本书的审校单位上海珪梵科技有限公司(简称“上海珪梵”)。上海珪梵是一家集数字化软件技术与数字安全于一体的专业服务机构，专注于数字化软件技术与数字安全领域的研究与实践，并提供数字科技建设、数字安全规划与建设、软件研发技术、网络安全技术、数据与数据安全治理、软件项目造价、数据安全审计、信息系统审计、数字安全与数据安全人才培养和评价等服务。上海珪梵是数据安全人才培养运营中心单位。在本书译校过程中，上海珪梵投入了多名专家助力本书的译校工作。

在此，一并感谢北京金联融科技有限公司在本书译校工作中给予的大力支持。

最后，感谢清华大学出版社和王军等编辑的严格把关，悉心指导，正是有了他们的辛勤努力和付出，才有了本书中文译本的出版发行。

译 者 介 绍

栾浩，获得美国天普大学 IT 审计与网络安全专业理学硕士学位，持有 CISSP、CISA、CISP 和 CISP-A 等认证。负责金融科技研发、数据安全、云计算安全和信息科技审计以及内部风险控制等工作。担任中国计算机行业协会数据安全产业专家委员会专家、(ISC)²上海分会理事。栾浩先生担任本书翻译工作的总技术负责人，并承担全书的校对、通稿和定稿工作。

吕丽，获得吉林大学文秘专业文学学士学位，持有 CISSP、CISA、CISM 和 CISP-PTE 等认证。负责信息科技风险管理、网络安全技术架构评估和规划、数据安全治理、信息安全管理体系制度管理、信息科技外包风险管理、安全合规与审计等工作。吕丽女士承担全书翻译和定稿工作。

徐坦，获得河北科技大学理工学院网络工程专业工学学士学位，持有 CISP、CISP-A 等认证。现任安全技术经理职务，负责数据安全技术、渗透测试、安全工具研发、代码审计、安全教育培训、IT 审计和企业安全攻防等工作。徐坦先生承担本书全书的校对和通稿工作，并担任本书项目经理。

姚凯，获得中欧国际工商学院工商管理硕士学位，持有 CISSP、CCSP、CEH 和 CISA 等认证。负责 IT 战略规划、策略程序制定、IT 架构设计及应用部署、系统取证和应急响应、数据安全、灾难恢复演练及复盘等工作。姚凯先生承担本书全书的校对工作。

王向宇，获得安徽科技学院网络工程专业工学学士学位，持有 CISP、CISP-A、软件工程造价师和软件研发安全师等认证。现任高级安全经理职务，负责安全事件处置与应急、数据安全治理、安全监测平台研发与运营、云平台安全和软件研发安全等工作。王向宇先生承担本书全书的校对工作。

李浩轩，获得河北科技大学理工学院网络工程专业工学学士学位，持有CISP、CISP-A 等认证。现任安全技术经理职务，负责 IT 审计、网络安全、平台研发、安全教培和企业安全攻防等工作。李浩轩先生承担本书全书的校对工作。

贺秋雨，获得北京交通大学教育技术专业理学硕士学位，持有 CISSP 和 CCSP 等认证。负责数据安全、云计算安全和信息安全治理等工作。担任中国计算机学会计算机安全专业委员会委员。贺秋雨先生承担本书部分章节的校对工作。

马修湖，获得华南理工大学计算机学院计算机应用专业工学硕士学位，现为南昌大学软件学院网络空间安全系副教授，负责数据安全实验室建设运营、安全工具研发、数据安全人才培养、数据安全方案建设咨询等工作。马修湖先生承担本书全书的校对和通读工作。

高崇明，获得解放军信息工程大学工学硕士学位，高级工程师。获得CISP-PTE、CISP 和商用密码应用安全性评估等认证。负责信息安全评估、商用密码应用、电子认证技术、数字证书应用、等级保护、密码应用安全性评估等工作。高崇明先生承担本书部分章节的审校工作。

余莉莎，获得南昌大学工商管理硕士学位，持有 CISP 和 CISP-A 认证。负责数据安全评估、咨询与审计、数字安全人才培养体系等工作。余莉莎女士承担本书部分章节的通读工作。

王泓娟，获得江西财经大学会计专业本科学历，持有 CISP-A 认证。负责数据安全评估、咨询与审计、数字安全人才培养体系等工作。王泓娟女士承担本书部分章节的通读工作。

作 者 介 绍

Jason Garbis 担任 Appgate 公司产品部门的高级副总裁；Appgate 是一家提供零信任安全访问解决方案的专业供应商。Jason Garbis 拥有 30 多年在安全和技术公司的产品管理、工程和咨询经验，在 Appgate 公司负责安全产品战略和产品管理。Jason Garbis 也是云安全联盟 SDP 零信任工作组的联合主席，领导研究并发布项目提案。Jason Garbis 持有 CISSP 认证，并获得 Cornell 大学的计算机科学专业学士学位和 Northeastern 大学的 MBA 硕士学位。

Jerry W. Chapman 担任 Optiv Security 公司的身份管理工程师。Jerry W. Chapman 凭借超过 25 年的行业经验，通过满足安全需求和业务目标的方式，成功帮助众多企业客户设计并实施 IAM 战略。Jerry W. Chapman 的工作职责涵盖企业架构设计、解决方案工程和软件架构研发等领域。作为 IAM 行业专家，Jerry W. Chapman 在 Optiv Cyber Security 实践领域作为思想领袖提供指导和支持，重点关注作为企业安全架构核心组件的身份和数据两个方面。Jerry W. Chapman 是 Optiv 零信任战略的关键发言人，经常在会议和行业活动中发表演讲。Jerry W. Chapman 活跃于 IDSA 技术工作组，是 IDSA 组织的创始技术架构设计师。Jerry W. Chapman 是一名经认证的 Forrester 零信任战略师，获得 DeVry 大学计算机信息系统专业学士学位，目前正在 Southern New Hampshire 大学攻读应用数学学位。

技术编辑介绍

Christopher Steffen 作为知名的信息安全执行官、研究员和演讲家，拥有超过 20 年的行业经验，专注于 IT 管理/领导力、云计算安全和法律法规监管合规等工作。

Christopher Steffen 曾担任多个职位和高管角色，从 Boy Scouts 营地主管到 Colorado 议会发言人的新闻秘书。Christopher Steffen 的技术生涯开始于信贷报告公司的金融服务垂直系统管理部门，直至建立网络运营组，并负责信息安全保障和技术合规工作实务，最终，Christopher Steffen 以首席技术架构师的身份离开该公司。Christopher Steffen 曾担任制造公司的信息总监和多家技术公司的首席宣传官，专注于云安全和云应用程序的转型实践，还担任过金融服务公司的首席信息官，负责管理与技术相关的企业职能。

Christopher Steffen 目前是 EMA(Enterprise Managements Associates)的首席信息安全、风险和合规管理研究专家。EMA 是一家领先的行业分析公司，提供全面的 IT 和数据管理技术分析建议。

Christopher Steffen 持有多项技术认证，包括 CISSP 和 CISA，并凭借虚拟化、云计算和数据中心管理(Cloud and Data Center Management，CDM)五次获得微软最具价值专家奖(MPV)。Christopher Steffen 以优异成绩获取了 Denver Metropolitan 州立学院的文学学士学位。

致　　谢

零信任安全(Zero Trust Security)涵盖多个领域，探索和学习相关技术、非技术以及架构概念并将其组合在一起往往是极具挑战的。幸运的是，众多的安全专家愿意花费大量时间，通过深入交谈、相互引导和回答彼此问题的方式，在涉及零信任安全的多个领域提供了大量的反馈和指导意见。有些安全专家通过阅读和讨论规划摘要或正在开展的工作提供帮助，有些安全专家则通过视频会议展开头脑风暴(这是 2020 年新出现的交流方式)，而另一些信息安全专家则通过定期的专业交流提供支持。

感谢 Chase Cunningham 博士对行业的深远影响，感谢 Gregory J. Touhill 撰写的前言。感谢两位专家在军事和信息安全领域为美国国家和政府所作出的贡献。还要感谢 Evan Gilman、Doug Barth、Mario Santana、Adam Rose、George Boitano、Bridget Bratt、Leo Taddeo、Rob Black、Deryck Motielall 和 Kurt Glazemakers 等专家。此外，我要向来自云安全联盟以及 SDP 零信任工作组的专家致敬，包括 Shamun Mahmud、Junaid Islam、Juanita Koilpillai、Bob Flores、Michael Roza、Nya Alison Murray、John Yeoh 和 Jim Reavis。我还要向身份定义安全联盟(IDSA)团队，特别是将身份管理置于安全工作核心地位的技术工作组致敬。还要感谢那些无法一一列举，但多次参与交流和给予支持的伙伴们，感谢 Apress 公司的编辑 Rita Fernando 和 Susan McDermott 在整个项目中的支持、鼓励和帮助。当然，还要感谢作为技术审核员、意见提供方的好友 Chris Steffen。

最后，要感谢阅读本书的诸位安全专家，作为信息安全行业的专家或领导者，每天都在为更好保护所供职的组织而辛勤工作。希望本书能够帮助安全专家们更轻松地开展工作。

前　言

零信任的出现不是为了配合销售一种新的安全控制措施或解决方案，而是源于期待解决企业现实问题的真实想法。零信任更专注于安全的本质和现状。

——Chase Cunningham 博士，又称“零信任博士(Dr. Zero Trust)”

本人已经期待本书二十多年，非常荣幸能为本书的出版发行写作前言。

早在 Jericho 论坛于 2004 年发表以“去边界化(De-perimeterization)”为特征的新安全战略宣言之前，国内安全界的许多专家已经认识到，边界安全模型(Perimeter Security Model)不再是 Internet 连接系统和企业的可行安全战略。将所有事物连接到 Internet 的期望很难得到充分满足，不断上涨的安全工具成本及其复杂性，以及技术变革的快速，在破坏已经形成的边界安全模型。如果将组织的深度防御(Defense-in-depth)安全防线比作一道堤坝，当堤坝上存在太多缺口时，无论再投入多少资金都将毫无意义。Jericho 论坛宣言指明了不同的方向，给予安全行业新的希望。

然而，可悲的是，就像死星上的莫夫塔金(Grand Moff Tarkin)一样，许多安全从业人士和专家对现状感到满意，而且对于采用新方法确保现代企业安全的想法嗤之以鼻。甚至，曾有安全评论家表示，Jericho 论坛宣言是“方向错误”，并以极尽嘲讽的方式预测：Jericho 论坛的工作很可能“将以未实现的想法和徒劳的努力而告终”。希望这位安全评论家在阅读本书时能怀有一丝愧疚和遗憾。

事实上，Jericho 论坛的工作成果并未浪费，但的确也未立即产生成效。在提出“去边界化”概念 5 年多之后，当时的西方研究分析人士 John Kindervag 在 2010 年创造性地提出“零信任(Zero Trust)”一词，用于描述这一新的安全模型：组织不应自动(默认)地信任其边界之外或之内的任何事物，与之相反，将所有事物连接到系统并授予对数据的访问权限之前，应验证所有访问要素。

对于军队而言，零信任并不是一场安全模型的革命。军人在整个职业生涯中一直在践行物理安全。例如，所有人都需要在门口接受安全人员的检查，在

进入基地之前出示合法的身份证件。一般而言，军队会划分 A、B 和 C 级资源周围的保护区。航线区域是 A 级优先资源的所在地，并由武装警卫严格控制进出。基于角色的访问受到严格控制，并授权武装警卫对“越过红线”的攻击方使用致命武力。作为中尉，在进入办公室之前，应经过四级安全检查。安全已经在军队的文化、流程和预期中根深蒂固。

遗憾的是，在逐步建立国防部信息网络且同时采用“零信任”物理安全模型保护最具价值的基础设施(Facility)和武器系统的过程中，由于缺乏实施“零信任”的技术手段，以至于很难保护连接到 Internet 的数字资产。可用的商业化安全工具极其复杂且价格昂贵。例如，应与知名的供应商签订合同，创建“技术学院”并培训已掌握高级技能的员工正确使用供应商所提供的复杂网络产品。随着组织持续努力将所有业务职能转变为数字生态系统，安全成本亦随之飙升，但边界的安全防线仍很难控制陆续出现的缺漏。当 Gregory J. Touhill 从联邦政府退休，担任美国政府首席信息安全官时，业界已经可以得出结论，零信任安全战略(Zero Trust Security Strategy)是保护数字生态系统的唯一希望。

COVID-19 的流行促使企业从传统的办公环境转向居家办公模式(Work-From-Home Model)，从而加速了企业期待已久的、向零信任安全战略的转变。大规模移动、云计算、软件即服务(SaaS)以及无可替代的自携设备(Bring Your Own Device，BYOD)打破了安全边界的幻视感，世界各地的组织都开始由传统企业环境转向今天更加现代化的数字生态。随着数字化技术的逐步实现，传统的网络安全边界已经消亡；再也没有“外部(Outside)”或“内部(Inside)”之分。

遗憾的是，许多安全专家和组织，包括那些曾经嘲笑 Jericho 论坛的反对方，都已经加入了零信任的行列。一些安全专家虽然号称支持“零信任”，但实际上并不清楚零信任的真正含义，也不清楚践行零信任的方法。某些组织的传统网络设备和方法已证明是极其复杂且脆弱的，但其市场营销团队竟然“奇迹般地”宣布组织脆弱的防护能力就是“零信任”实践。尽管 Forrester 的 Chase Cunningham 博士和 Gartner 的 Neil MacDonald 开展了大量的零信任研究，但直到本书出版之前，仍缺少一本真正实用的零信任权威指南。

幸运的是，本书作者 Jason Garbis 和 Jerry W. Chapman 拥有丰富的经验，是零信任、企业网络运营、网络安全和商业运营领域公认的专家。本书鼓励安全专家们多多阅读 Jason 和 Jerry 的传记，Jason 和 Jerry 的资历令人印象深刻且毫无修饰。

Jason 和 Jerry 展示了一本极具价值的专业书籍，深入浅出地讲解了零信任相关知识，本书应作为各地学生和安全专家的权威参考素材。

本书内容翔实，结构合理紧凑。无论安全专家是否熟悉零信任相关概念，都能从前四章获益，前四章阐述了零信任旅程的整体战略。其中，第 1 章深刻地讨论并回答了“为什么需要零信任？”这一疑问。而那些刚刚开始零信任旅程的安全专家则会发现第 2 章更具价值，因为第 2 章提供了完整的技术发展编年史，阐述了行业如何发展至当今的零信任，并清晰地定义了零信任的概念和范围。需要了解如何将零信任整合到自身运营架构中的组织，需要深入学习第 3 章中列出的实用建议和生动形象的描述。许多组织在开展重要投资或重大战略变革之前，更愿意尝试和体验“飞行测试(Flight Test)”的经历。本书第 4 章详细讨论了 Google 等组织如何将零信任纳入其运营活动的案例。

本书的第 II 部分，从第 5 章开始讨论关于身份的概念，充分阐述了零信任的基础组成部分。本书认为身份是成功实施零信任的核心组件，很高兴看到 Jason 和 Jerry 从本书的这一章开始的相关讨论。接下来的三章论述了零信任对网络基础架构(Network Infrastructure)、网络访问控制措施(Network Access Control)以及入侵检测和防御系统的影响。如果安全专家们觉得这三章很有启发性，那么第 9 章关于零信任世界中虚拟私有网络(Virtual Private Network，VPN)的讨论可能改变安全专家对当今环境，以及对未来随处工作(Work-from-anywhere)的看法。

第 10 章对于下一代防火墙(Next-Generation Firewall，NGFW)的讨论具有同样的挑战，讨论了下一代防火墙功能的历史和演变，并预测了下一代防火墙在零信任世界中的未来场景。第 11 章讨论了零信任模型中的安全信息与事件管理(Security Information and Event Management，SIEM)以及安全编排和自动化响应(Security Orchestration, Automation and Response，SOAR)，对专注于识别、管理和控制风险的安全专家们而言，第 10 章是必读的内容。阅读过第 5 章与身份相关讨论内容的安全专家，应不会对第 12 章关于特权访问管理的讨论感到失望。致力于降低内部威胁风险的组织也需要密切关注这部分内容！

接下来的四章对许多组织正在努力解决的技术问题开展了实践分析和指导。第 13 章是关于数据保护的讨论。第 14 章对于云计算资源的讨论就如何在基于云的环境中合理运用零信任提出了实用建议。由于许多组织都采用软件即服务(Software as a Service，SaaS)、安全 Web 网关和云访问安全代理等技术，

第 15 章讨论了如何将云计算相关技术集成到零信任战略中，并就如何“合理实施”提供了切实可行的建议。最后，很高兴看到 Jason 和 Jerry 在第 16 章纳入物联网设备和相关事项的讨论。大多数网络安全人员专注于 IT 设备，却忽视了与组织运营技术、工业控制系统和“物联网(Internet of Things，IoT)”设备相关的风险。无论处于哪一类组织角色，都需要关注本章内容，并认识到运用零信任技术保护关键系统的重要性。

本书的最后三章，对于所有致力于在组织内部合理实施零信任的组织而言都至关重要。第 17 章对于如何创建和实现有效的零信任策略模型展开了必要的讨论。第 18 章讨论了组织在实施零信任时，最可能需要解决的用例(Use Case)。第 19 章是对前一章的必要补充，讨论了组织应如何着手实施零信任，以获得成功的最大可能性。相信秉承“大处着眼，小处入手，快速推进”这一理念的安全专家们不会对 Jason 和 Jerry 的实践建议感到失望。最后，第 20 章完整地总结了本书的零信任旅程，并提醒机构、企业和组织，安全的目标是保障组织能够实现其业务使命。零信任不应仅是一句时髦的术语，而是能够成功实施的安全解决方案，在需要的场景中顺利实施。本书将帮助组织快速且精准地实现零信任目标。国家背景的参与方和网络犯罪案例已经证明基于边界(Perimeter-based)的安全模型不再有效。迅速且有意识地转向零信任安全模型的时机已成熟。值得庆幸的是，由于 Jason 和 Jerry 富有成效的工作，现在业界有了如何实现目标的实用指南。

自孙子兵法开始，军事将领们实施了一系列基于边界的安全模型用于保护资产(Asset)。但是，从前的军事将领并未接触过 Internet、移动设备、云计算和现代技术。Jericho 论坛的判断是正确的；边界已经正在成为过去。现在就是全面接受和实施零信任的时代。

——Gregory J. Touhill，CISSP，CISM，美国空军退役准将

目　录

第 I 部分　概述

第 1 章　介绍……3

第 2 章　零信任概念……7

2.1　历史与演变……7

2.1.1　Forrester 的 ZTX 模型……9

2.1.2　Gartner 的零信任方法……11

2.2　零信任展望……12

2.2.1　核心原则……12

2.2.2　扩展原则……14

2.2.3　定义……15

2.3　零信任平台需求……16

2.4　本章小结……17

第 3 章　零信任架构……19

3.1　具有代表性的企业架构……20

3.1.1　身份和访问管理……21

3.1.2　网络基础架构(防火墙、DNS 和负载均衡器)……22

3.1.3　跳板类设备……23

3.1.4　特权访问管理……23

3.1.5　网络访问控制……23

3.1.6　入侵检测和入侵防御……24

3.1.7　虚拟私有网络……25

3.1.8　下一代防火墙……25

3.1.9　安全信息与事件管理……25

3.1.10 Web 服务器与 Web 应用程序防火墙……26
3.1.11 基础架构即服务……27
3.1.12 软件即服务和云访问安全代理……27
3.2 零信任架构……28
3.2.1 NIST 零信任模型……28
3.2.2 概念性零信任架构……29
3.3 零信任部署模型……36
3.3.1 基于资源的部署模型……37
3.3.2 基于飞地的部署模型……39
3.3.3 云路由部署模型……41
3.3.4 微分段部署模型……44
3.4 本章小结……46

第 4 章 零信任实践……47
4.1 Google 的 BeyondCorp……47
4.2 PagerDuty 的零信任网络……52
4.3 软件定义边界和零信任……53
4.3.1 交互 TLS 通信……54
4.3.2 单包授权……55
4.4 SDP 案例研究……56
4.5 零信任与企业……59
4.6 本章小结……59

第 II 部分 零信任和企业架构组件

第 5 章 身份和访问管理……63
5.1 回顾 IAM……63
5.1.1 身份存储(目录)……64
5.1.2 身份生命周期……66
5.1.3 身份治理……68
5.1.4 访问管理……69

5.1.5　身份验证……69
5.1.6　授权……73
5.2　零信任与 IAM……75
5.2.1　身份验证、授权和零信任集成……76
5.2.2　增强传统系统的身份验证……77
5.2.3　零信任作为改进 IAM 的催化剂……79
5.3　本章小结……80

第 6 章　网络基础架构……81
6.1　网络防火墙……82
6.2　域名系统……83
6.2.1　公共 DNS 服务器……84
6.2.2　私有 DNS 服务器……84
6.2.3　持续监测 DNS 的安全态势……85
6.3　广域网……86
6.4　负载均衡器、应用程序交付控制器和 API 网关……88
6.5　Web 应用程序防火墙……89
6.6　本章小结……89

第 7 章　网络访问控制……91
7.1　网络访问控制简介……91
7.2　零信任与网络访问控制……94
7.2.1　非托管访客网络访问……94
7.2.2　托管访客网络访问……95
7.2.3　关于托管与非托管访客网络的辩论……96
7.2.4　员工自携设备(BYOD)……97
7.2.5　设备态势检查……98
7.2.6　设备探查和访问控制……99
7.3　本章小结……100

第 8 章　入侵检测和防御系统……101
8.1　IDPS 的类型……102

8.1.1 基于主机的系统……103
8.1.2 基于网络的系统……103
8.2 网络流量分析与加密……104
8.3 零信任与 IDPS……106
8.4 本章小结……109

第 9 章 虚拟私有网络……111
9.1 企业 VPN 和安全……113
9.2 零信任与虚拟私有网络……115
9.3 本章小结……117

第 10 章 下一代防火墙……119
10.1 历史与演变……119
10.2 零信任与 NGFW……120
10.2.1 网络流量加密：影响……120
10.2.2 网络架构……122
10.3 本章小结……124

第 11 章 安全运营……127
11.1 安全信息与事件管理……128
11.2 安全编排和自动化响应……129
11.3 安全运营中心的零信任……130
11.3.1 丰富的日志数据……130
11.3.2 编排和自动化(触发器和事件)……130
11.4 本章小结……135

第 12 章 特权访问管理……137
12.1 口令保险库……137
12.2 秘密管理……138
12.3 特权会话管理……139
12.4 零信任与 PAM……140
12.5 本章小结……143

第 13 章　数据保护……145
13.1　数据类型和数据分类分级……145
13.2　数据生命周期……147
13.2.1　数据创建……147
13.2.2　数据使用……148
13.2.3　数据销毁……149
13.3　数据安全……150
13.4　零信任与数据……151
13.5　本章小结……153

第 14 章　基础架构即服务和平台即服务……155
14.1　定义……156
14.2　零信任和云服务……157
14.3　服务网格……161
14.4　本章小结……163

第 15 章　软件即服务……165
15.1　SaaS 与云安全……166
15.1.1　原生 SaaS 控制措施……166
15.1.2　安全 Web 网关……167
15.1.3　云访问安全代理……168
15.2　零信任和 SaaS……168
15.3　本章小结……170

第 16 章　物联网设备和“物”……173
16.1　物联网设备网络和安全挑战……175
16.2　零信任和物联网设备……177
16.3　本章小结……183

第 III 部分　整合

第 17 章　零信任策略模型……187
17.1　策略组件……188

17.1.1 主体准则……188
17.1.2 活动……189
17.1.3 目标……191
17.1.4 条件……194
17.1.5 主体准则与条件……196
17.1.6 示例策略……197
17.2 适用的策略……200
17.2.1 属性……200
17.2.2 策略场景……202
17.2.3 策略有效性评价和执行流程……206
17.3 本章小结……209

第 18 章 零信任场景……211
18.1 VPN 替换/VPN 替代……211
18.1.1 考虑因素……213
18.1.2 建议……215
18.2 第三方访问……216
18.2.1 考虑因素……217
18.2.2 建议……218
18.3 云迁移……219
18.3.1 迁移类别……219
18.3.2 考虑因素……220
18.3.3 建议……222
18.4 服务到服务访问……222
18.4.1 考虑因素……224
18.4.2 建议……225
18.5 研发运维一体化……225
18.5.1 DevOps 阶段……227
18.5.2 考虑因素……228
18.5.3 建议……228
18.6 并购和购置……229

18.6.1　考虑因素……229
18.6.2　建议……230
18.6.3　资产剥离……230
18.7　完全零信任网络/网络转型……231
18.7.1　考虑因素……233
18.7.2　建议……233
18.8　本章小结……234

第 19 章　零信任成功之旅……235
19.1　零信任：战略方法(自上而下)……236
19.1.1　治理委员会……237
19.1.2　架构审查委员会……237
19.1.3　变更管理委员会……237
19.1.4　价值驱动因素……238
19.2　零信任：战术方法(自下而上)……240
19.3　零信任部署示例……241
19.3.1　场景 1：战术性零信任项目……241
19.3.2　情景 2：战略性零信任项目提案……244
19.4　常见障碍……246
19.4.1　身份管理不成熟……247
19.4.2　政治阻力……247
19.4.3　法律法规要求的约束……248
19.4.4　资源的探查和可见性……248
19.4.5　分析瘫痪……248
19.5　本章小结……249

第 20 章　结论……251

第 21 章　后记……253
21.1　严谨且详尽的方案……253
21.2　零信任的公司文化和政治考量……253
21.3　梦想远大，从小做起……254

21.4 获取预算资金……254
21.5 数字化转型契机……254

—— 以下资源可扫描封底二维码下载 ——

附录 延伸阅读：注释清单……259

第 I 部分

概　　述

零信任(Zero Trust)是一种安全理念和原则，代表了企业 IT 和安全处理方式的重大转变。实施零信任的成果可能帮助安全团队和企业获得巨大收益，但零信任的范围涉及多个领域，而且可能都是决定性的。本书的第 I 部分讲述了零信任的历史和基础知识，阐述零信任的概念，并在理论和实践中描述零信任架构。本书旨在帮助安全专家们更好地理解零信任，开始思考如何合理运用零信任组件，以帮助提高组织的安全性、韧性(Resiliency)和效率。

第1章

介　绍

真正的企业安全很难实现，原因在于IT和应用程序基础架构的复杂性、用户访问的范围和时效性以及信息安全固有的对抗性。由于大多数企业网络过于开放的特性，且并未实施网络级别和应用程序级别的最小特权(Least Privilege)原则，因此组织自身极易受到攻击。对于内部网络和面向公共 Internet 的远程访问服务(如 VPN)而言都是如此，面向公共 Internet 的远程访问服务是允许 Internet 上的敌对方公开访问的。考虑到当今的网络安全威胁态势，组织永远不会选择设计这样的系统。然而，大量已存在的传统安全和网络系统却延续着这种模式。

本书的主题“零信任安全”改变了传统安全的风险态势，带来了一种全新的安全方法，零信任强制执行网络和应用程序的最小特权原则。未经授权的用户和系统将很难访问企业资源，而授权用户也仅拥有所需的最小权限。实施零信任可帮助企业更加安全，且更具有韧性。零信任还通过自动实施动态和以身份为中心的访问策略，显著提高效率和有效性。

注意，零信任中的“零(Zero)”可能引起歧义，并不是字面上的“零”信任，而是关于“零”固有的或隐含的信任。零信任是指谨慎地建立信任基础，提升信任，最终在预设的时间内允许合理级别的访问。有时，也称零信任为“赢得信任(Earned Trust)”“适应性信任(Adaptive Trust)”或“零隐式信任(Zero Implicit Trust)”，上述措辞可能更适合这一趋势，但“零信任”一词更有吸引力，而且一直在延续使用。请诸位安全专家不要仅按字面意义理解“零”的表述！

目前，零信任是信息安全行业中非常重要且引人注目的新趋势，虽然零信

任已成为营销热词，但组织更应该相信零信任背后有着实质的内容和价值。零信任是一种理念、一种方法和一套指导原则。这也意味着有多少家企业，就有多少种对零信任的理解和解释。然而，每套零信任架构都将遵循一些基本和通用的原则。本书将基于零信任旅程中与不同规模和成熟度的企业合作的经验，为零信任提供指导和建议。记住，本书引入“旅程(Journey)”一词；目的是强调这样一个事实：零信任不是指已经完成的项目，而是正在实施和不断发展的项目提案。这就是为什么通过本书分享关于如何在组织的环境中更好地实现零信任的想法和建议。

本书确信零信任是一种实现企业安全的更好、更有效方法。在某些方面，零信任与网络安全密切相关，而网络领域是零信任的核心元素，因此，本书将跨越应用程序(Application)、数据(Data)、身份(Identity)、运营(Operation)和策略(Policy)的界限，探索零信任安全的诸多领域。

作为组织的安全负责人，有责任推动、影响和督促组织采用零信任架构，提升组织的灵活性，并帮助提高安全负责人的专业水准。本书共分为三部分。第Ⅰ部分介绍零信任原则，建立用于定义零信任并帮助与安全基础架构保持一致的框架和词汇表。这也是本书介绍完整的零信任内容所需要的基础知识。

第Ⅱ部分深入探讨 IT 和安全技术，以及与零信任的关系。通过本部分的阐述，安全专家们能够掌握组织如何启动零信任项目，以及裁剪当前的 IT 和安全基础架构的方法，并将裁剪后的 IT 和安全基础架构集成到更先进的架构中。该部分还将探讨不同技术如何整合身份上下文(Identity Context)并从中获益，从而帮助组织的安全控制措施更加有效。

第III部分整合所有内容，在本书第Ⅰ部分的基础上丰富了基础概念并深入讨论相关技术。该部分探讨零信任策略模型(Zero Trust Policy Model)的部署方式，检查特定的零信任场景(用例)，最后讨论零信任之所以能够成功的战略和战术方法。

此外，值得注意的是，本书并未评价供应商或供应商产品的有效性。行业发展和创新的步伐发展迅速，关于供应商和产品的评论都会很快过时。相反，本书专注于探索架构性原理，组织和安全专家们可以从中提取需求，这些原理也可用于评价供应商、平台、解决方案提供商和方法的有效性。

在本书的结尾时，组织的安全负责人应清楚地认识到，零信任并没有绝对唯一的正确方法。在设计零信任项目提案时，安全负责人需要考虑现有的基础架构、优先事项、员工技能、预算和时间轴。这可能导致零信任看起来很复杂，但零信任涉及广泛内容，在实践中有助于简化企业的安全和架构。作为顶层安全和访问模型，零信任规范了相关事项，并为组织提供了一种用于定义和实施跨分布式异构基础架构访问策略的集中方式。

最终，本书的目标是帮助安全专家们充分理解零信任的定义，并掌握如何成功地引导组织踏上零信任旅程的知识。如果能实现这一点，我们为本书所做出的诸多努力就值得了。

现在，开始零信任旅程吧！

第 2 章

零信任概念

本章将介绍作为概念、哲学和框架的零信任。除了简要阐述零信任的历史和演变外，还将介绍零信任的指导原则。每套零信任项目提案(Initiative)都有相同的核心和扩展原则，在开始零信任旅程前，掌握零信任指导原则非常重要。本章的目标是基于指导原则提供零信任的定义，并列出一系列基础平台需求。

2.1 历史与演变

安全边界一直以“城堡和护城河”的传统方式部署在企业网络的周边。然而，随着技术的发展，远程工作团队和远程工作负载变得越来越普及。安全边界必然随之改变，从公司边界扩展到包括远程用户所连接的设备和网络，以及所连接的资源。这种改变可以有效地帮助安全和网络团队顺应业务需求，并调整组织安全运营和访问的模式，然而，所取得的效果参差不一。[1]

2010 年，Forrester 分析师 John Kindervag 在颇具影响力的 *No More Chevy Centers: Introducing the Zero Trust Model of Information Security* 白皮书中引入“零信任(Zero Trust)”一词。白皮书纳入了业界近期讨论的内容，特别是 Jericho 论坛提出的设想。Forrester 文档描述了从硬边界(Hard Perimeter)向需要观察和理解网络中的元素才能获得一定程度的信任和访问的方法的转变。随着时间的推移，Forrester 将这一概念演变为大众所知的零信任扩展(Zero Trust eXtended，ZTX)框架，ZTX 框架包括数据、工作负载和身份，是零信任的核心组件。

几乎在同一时间，Google 启动内部的 BeyondCorp 项目提案。BeyondCorp

1 本书试图以含蓄的方式表达这种观点。然而，不可否认的事实是，目前安全行业普遍使用的企业网络安全和数据安全的相关控制措施，无法有效地保护组织免受数据丢失和系统破坏的危害。诚然，组织面对的是主动寻求机会的成熟攻击方，但组织也应相信，这种普遍的保护不力的现状主要是由传统信息安全工具和方法的缺陷导致的，而本书将证明零信任更加有效。

项目提案采用多种零信任模型中的一个版本，使用其基本零信任元素有效地消除企业网络边界。从 2014 年开始，Google 通过一系列文档记录了其突破性的内部实施旅程，对业界产生巨大影响。同样在 2014 年，云安全联盟引入软件定义边界(Software Defined Perimeter，SDP)架构，为支持零信任原则的安全系统提供具体规范。第 4 章将通过零信任的视角探讨 BeyondCorp 项目提案和 SDP 架构。

2017 年，行业分析公司 Gartner 修订并更新其持续自适应风险与信任评估(Continuous Adaptive Risk and Trust Assessment，CARTA)概念，CARTA 与零信任有许多共同原则。CARTA 不仅提供身份和数据元素，还包括与身份和访问环境的设备相关的风险和处理方式。

随着美国国家标准与技术研究所(National Institute of Standards and Technology，NIST)于 2020 年发布的与美国国家网络安全卓越中心(US National Cybersecurity Center of Excellence)项目相关的零信任架构(Zero Trust Architecture)的出版，向全行业进一步强调零信任的重要程度。

随着供应商、标准化组织对零信任规范和实施的审查及完善，零信任正在蓬勃发展，并将零信任视为信息安全方法的根本转变。最终，业界一致认为，为了防止恶意攻击方通过组织边界访问私有资源、泄露数据或中断运营，实施零信任带来的变化和改进是组织的必要组件。

撰写本书的安全专家在信息安全行业工作多年，且花费了大量时间与业内安全专业人士讨论零信任。安全专家们在讨论中经常遇到的问题之一是“零信任有哪些新特性？与组织已经实施的安全计划有何不同？”确切地说，零信任的某些元素，例如应在零信任环境中使用的最小特权(Least Privileged)访问和基于角色的访问控制(Role-based Access Control，RBAC)，是当前网络和安全基础架构中普遍使用的实施原则，但需要注意：仅包含上述元素并不能完整描述零信任实施的全景图。

在部署零信任之前，组织所使用的基础安全元素通常仅能实现用户、网络和应用程序的粗粒度隔离。例如在大多数组织中，已经实施了研发环境与生产环境隔离技术。然而，零信任扩展了隔离范围，实现了所有身份和资源之间的更有效隔离。零信任支持由自动化平台驱动的细粒度、身份和上下文感知的访问控制措施。尽管零信任最初是一种专注于在未经身份验证和未授权之前不信任任何网络身份的方法，但零信任的适用范围正在逐步扩展，且能跨组织环境提供更多安全功能。

在介绍本书所理解的关键零信任原则之前，先讲述一下 Forrester 和 Gartner 的零信任模型。

2.1.1　Forrester 的 ZTX 模型

Forrester 于 2010 年发布了最初版本的零信任模型，在接下来的几年中，Forrester 修订 2010 版零信任模型并最终发布了零信任扩展(Zero Trust eXtended，ZTX)模型。ZTX 模型提供丰富的内容和以数据为中心的完整模型，如图 2-1 所示。ZTX 模型反映了 Forrester 的观点，即将本地环境(On-prem)和云计算环境所面临的“数据大爆炸(Data Explosion)场景”视为保护核心。同时，针对数据管道的周边元素，如工作负载、网络、设备和人员，也都予以保护。后续章节将依次讨论上述周边元素。

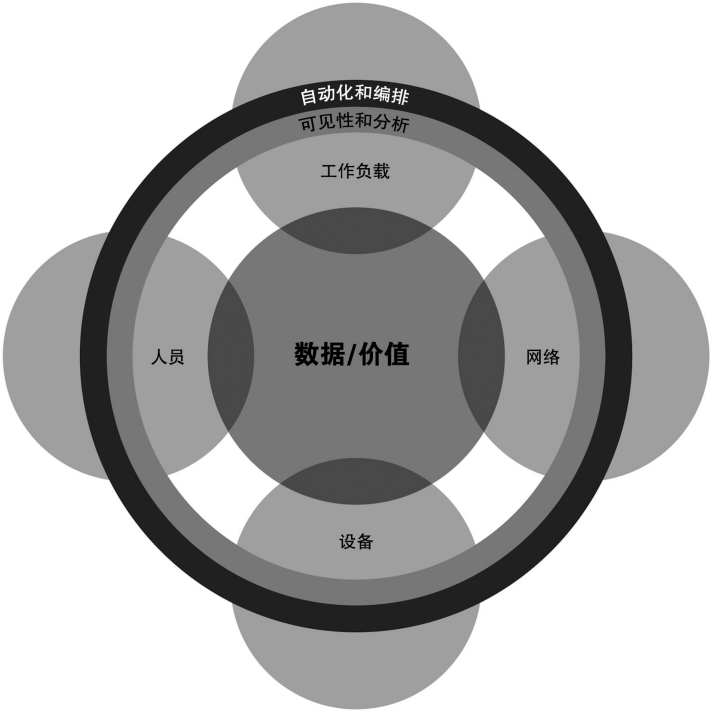

图 2-1　Forrester 零信任扩展模型

(来源：零信任扩展生态系统：数据，Forrester 研究公司，2020 年 8 月 11 日)

1. 数据

数据(Forrester 将数据标记为“价值”以凸显其重要程度[1])是 ZTX 模型的核心，数据支持零信任模型的核心需求包括数据分类分级和保护(Data Classification and Protection)。本书将数据视为零信任系统应保护的资源元素。此外，数据防丢失(Data Loss Prevention，DLP)也应作为零信任架构的一部分，并与策略模型绑定在一起，以便在可能的情况下实施基于上下文的访问策略。

2. 网络

ZTX 模型的网络支柱主要集中在网络分段(Network Segmentation)，即从用户和服务器的角度，基于以身份为中心的属性提供更强大的安全性。安全专家应意识到，企业已经拥有构成传统网络安全基础架构的多种现有组件，例如，下一代防火墙(Next-Generation Firewall，NGFW)、Web 应用程序防火墙(Web Application Firewall，WAF)、网络访问控制(Network Access Control，NAC)解决方案和入侵防御系统(Intrusion Protection System，IPS)。传统的网络安全基础架构组件通常都可在零信任系统中发挥效用。本书将在第 3 章的具有代表性的企业架构中介绍传统安全组件，并在本书的第 II 部分探讨传统安全组件与零信任的关系。

3. 人员

ZTX 模型的人员(People)支柱应包括身份和访问管理(Identity and Access Management，IAM)的多个元素。基于角色的和基于属性的访问控制(Role-and Attribute-Based Access Control，RBAC 和 ABAC)是 IAM 常见的模型，零信任将在整个企业基础架构中的更多领域，更有效地运用 RBAC 和 ABAC 模型。多因素身份验证(Multi-Factor Authentication，MFA)是另一项必要条件，也是支撑零信任的关键技术。最后，实施单点登录(Single Sign On，SSO)——OAuth 和 SAML 等现代开放标准也是核心元素。正如本书始终所支持的理念：组织应将身份作为零信任环境的核心。

1 事实上，Forrester 的声明是：“Forrester 认为只有‘数据’才是真正的‘价值’。只有对组织业务具有价值的，才是组织应该集中防御的最关键资产，组织应以全部成本捍卫这一价值。”

4. 工作负载

基于 Forrester 的定义，工作负载(Workload)由构成面向客户和后端业务系统中，驱动业务逻辑功能的组件组成，包括容器、应用程序、基础架构和进程(Process)等。零信任需要元数据驱动(Metadata-driven)的工作负载访问控制措施，本书将在第 17 章进一步探讨工作负载。

5. 设备

设备(Device)安全模型应包括设备的身份、资产清单、隔离、安全和控制措施。第 3 章将描述运行在设备中的用户代理，以及用户代理如何成为零信任环境的核心(Core)。本书将在第 4 章讨论设备在 Google 的 BeyondCorp 实施过程中的关键作用。

6. 可见性和分析

ZTX 模型的可见性和分析(Visibility and Analytics)是跨企业支持基于上下文信息安全决策所使用和展示的数据。本书认为这至关重要，在跨越多个不同来源的数据整合场景中尤其如此。目前没有单一平台具有能够横跨大范围的必要能力，但这是一个不断发展的领域。本书将在第 11 章中进一步讨论可见性和分析的内容。

7. 自动化和编排

ZTX 模型中的自动化和编排(Automation and Orchestration)实现手动流程的自动化，并将自动化流程与安全策略和响应活动联系起来。本书认为，自动化和编排对于零信任平台的成功至关重要——零信任具有内在的动态性和适应性，实现这一目标的唯一方法是跨企业环境使用的自动化和编排技术。本书接下来将对此深入讨论，因为自动化(Automation)是零信任的关键原则之一。

2.1.2　Gartner 的零信任方法

Gartner 基于 CARTA 模型实现零信任，即持续自适应风险与信任评估(Continuous Adaptive Risk and Trust Assessment，CARTA)模型。CARTA 模型的前提是从预测(Predict)、防御(Prevent)、检测(Detect)和响应(Respond)的角度提

供与用户、设备、应用程序、数据和工作负载相关的持续风险评估。

CARTA 模型通过不同的安全平面(Security Plane)实现安全态势(Security Posture)，并监测和调整安全态势的基本流程。Gartner 认为，上述原则应在企业中全局实施，并覆盖企业的全部安全、策略和监管合规要求。

Gartner 倾向于更狭义地看待零信任，使用零信任网络访问(Zero Trust Network Access，ZTNA)表示用户到服务器的安全性，使用零信任网络分段(Zero Trust Network Segmentation，ZTNS)表示微分段/服务器到服务器的安全性。零信任的全局安全框架是围绕 CARTA 模型建立的，其原则与本书介绍的原则非常一致。这并不影响战略性项目提案(Initiative)被称作“零信任”“CARTA 模型”或“赢得信任”。[1]Gartner 的 CARTA 模型观点与本书中探讨的原则和目标是一致的。

2.2　零信任展望

零信任是用于保护网络、应用程序和数据资源的全局模型，重点是提供以身份为中心的策略模型以控制访问行为。所有企业都已经在其环境中使用了一套 IT 和安全工具，但零信任要求以身份为核心，全面审查和运营这些工具，并能在整个环境中实施基于属性和上下文感知(Attribute-and Context-Sensitive)的策略。这一点应在接下来探讨零信任的基本原则(核心原则和扩展原则)时变得更加清晰。

2.2.1　核心原则

在整个行业中，有三项核心零信任原则是公认的基础和必要原则。核心零信任原则最初定义在 Forrester 发表的“No More Chewy Center”论文中，本书相信这些原则在每个零信任实现中都是正确的。除了核心原则外，本书还将 NIST 零信任架构文档中描述的原则纳入其中。本书将从当前的行业角度重新解释 NIST 零信任原则。

1 事实上，本书也了解到部分刻意在内部避免使用“零信任”一词企业的想法。这些企业认为零信任是一种误导，最终用户可能将“零信任”负面解读为 “组织不信任员工”。

1. 应确保安全地访问所有资源(与物理位置无关)

这是一份强硬且严谨的声明，覆盖了多个维度。首先，要求所有资源都包含在零信任解决方案的范围内。要求组织采取零信任的全局方法，消除存在于安全工具和团队之间的竖井和屏障。

其次，这一原则要求所有身份(人员和机器)对所有资源(数据、应用程序和服务器)执行零信任安全访问，而不考虑身份的位置，也不考虑需要访问的资源的物理位置或采用何种技术。这一原则可以有效地帮助公司摒弃传统的企业边界，并采用另一种更安全的方式取而代之。这一原则还意味着，不仅在网络流量通过不受信任的网络区域时应对其使用加密技术[1]，而且所有访问都应遵守强制策略模型(Enforced Policy Model)——这是第二个原则的主题。

2. 应采用最小特权战略，严格执行访问控制措施

对资源使用最小特权访问的概念并不新鲜，但是，在零信任出现之前很难大范围实施。对于跨越物理位置和资源类型应同时执行最小特权管理，并且在网络和应用程序层通过使用身份上下文实施安全功能。

从历史上看，安全解决方案一直难以弥合网络级和应用程序级之间的安全脱节问题。传统安全环境中，用户(及其设备)获得对网络、应用程序的访问仅依赖于通过身份验证的访问控制措施。虽然只有公司财务用户拥有财务服务器的账户和口令，但公司的所有人员都可以访问财务服务器的登录页面。类似于账户和口令的单一访问控制措施不再能够维持有效的安全水平。组织存在很多已知且严重的漏洞，特别是那些不需要执行身份验证工作程序就可以远程利用的漏洞。本书将清晰地说明这一问题——向系统发送网络数据包的能力是一种特权，应按照特权的属性执行差异管理。如果企业没有授予用户访问特定服务的权限(例如，缺少 SSH 访问服务器的安全凭证，或者未通过 VPN 的身份验证)，那么用户一定就不应具备在网络层连接到特定服务的能力。

3. 应检查并记录全部流量

由于网络是分布式组件相互连接和通信的手段，安全专家在安全和 IT 基础

1 第 3 章将介绍隐式网络信任区(Implicit Network Trust Zone)的概念，隐式网络信任区是某些零信任部署模型的副产品。加密的应用程序协议将降低此类区域的风险。

架构方面特别关注网络。因此，零信任的决定性核心原则是组织应检查并记录全部流量。零信任系统非常适用于组合一组分散的网络执行点的场景——本书将在第 3 章讨论。值得注意的是，零信任系统应检查和记录尽可能完整的网络流量元数据，但由于处理和存储成本的原因，在检查网络流量内容时应更加谨慎(第 8 章将进一步讨论)。

安全专家可通过零信任系统完善单一的网络流量信息——例如，添加身份和设备上下文信息，并将其输入下一代防火墙、网络持续监控工具和 SIEM，以增强检测、告警和响应的决策能力，以及支持事故响应和其他告警机制的能力。

2.2.2　扩展原则

除了讨论零信任核心原则外，还有三个扩展原则，同样在企业级零信任环境中具有相当的重要性和必要性。

1. 应确保所有组件都支持事件和数据交换的 API

零信任可提供全局性的安全策略和实施模型，涵盖多个 IT 生态系统领域，并与第一个核心原则关联。因此，零信任应能与生态系统的多个(理想情况下可能是全部)组件集成。安全专家们都很清楚，零信任组件与传统安全领域中孤立的安全产品、基础架构和业务系统的集成能力至关重要。正如本书将在后续讨论中所提到的那样，身份与安全工具的集成可实现全局的安全上下文，零信任可通过身份上下文提供更安全的环境。身份与安全工具的集成将用于启动和响应事件，以及交换数据和日志信息，并启用下一个原则。实施这一原则的必然结果是：每个集成到零信任平台的安全和 IT 组件都会提升其价值、有效性和覆盖范围。相反，每个独立(未集成)的组件都会增加冲突，降低零信任系统的有效性，并可能降低安全性。

2. 应在上下文和事件的驱动下，执行跨环境和系统的自动化运营

自动化(Automation)是零信任环境的关键成功元素，即使是对于规模较小的运营场景也是必要的元素之一。零信任基于一组动态访问控制规则，规则基于身份、设备、网络和系统上下文差异而变化。正如将在第 3 章所要讨论的那样，零信任模型都需要集中的策略决策点(Policy Decision Point，PDP)，通过逻辑控

制通道与一组分布式策略执行点(Policy Enforcement Point，PEP)关联。逻辑控制通道(Logical Control Channel)用于通过集成/API 自动更改执行策略，对于零信任系统的运行至关重要。

在零信任系统中，对访问的自动变更可采用多种形式，包括通过身份管理系统、访问管理系统或网络访问控制系统授予用户访问权限。其他自动化活动包括临时或永久取消对特定资源的访问，例如，由纳入生命周期管理的事件或上下文的变化所驱动的自动化活动。

注意，虽然自动化操作是运营环境的基础活动，但这并不排除在启动自动化响应之前利用手动干预或在工作流中包含显式手动步骤的能力。也就是说，自动化并不意味着“全自动(Automatic)”。例如，访问请求流程需要管理员审批，以满足安全和合规准则。审批工作流要求参与人员阅读相关信息，并做出决策，然后将决策提交至系统。这应是审批流程中唯一的手动步骤。因此，工作流的其余部分(包括所有访问变更的设置)应是自动化的。

3. 应交付战术和战略价值

最终，围绕零信任的核心项目提案均应与业务价值挂钩。零信任项目可以(而且通常确实)对基础架构、团队、运营和最终用户体验产生重大影响。虽然零信任的成果往往是积极的，但在技术、文化和政治方面，变革往往难以实现。与零信任项目相关的变更可能涉及多个领域，组织环境中的多个组件将集成到零信任环境中，这些组件将作为组织零信任项目的执行点或策略驱动器。

组织应将零信任视为时间和资金的投资。了解组织的业务驱动因素和优先事项将有助于在企业环境中验证并执行零信任战略愿景。在旅程的初始阶段，应实现增量部署和战术胜利。这将极大简化组织的零信任旅程，并在内部提供动力和支持。也就是说，在零信任架构的战略框架内提供早期战术胜利，将有助于组织实现其全部战略价值。每个成功的新项目都会为零信任项目提案进一步开辟前进道路并提供支持。

2.2.3　定义

本书通过对零信任原则、架构和工作示例概念的介绍，帮助安全专家们理解零信任的概念。组织通过零信任检视并说明安全项目提案和组件的有效性。

本书提出以下简明定义：

零信任系统是一套安全集成平台，综合使用来自身份、安全、IT 基础架构以及风险和分析工具的上下文信息，在企业内部统一并动态地实施安全策略。零信任将安全从无效的、以边界为中心(Perimeter-centric)的模型转变为以资源和身份为中心(Resource and Identity-centric)的模型。因此，组织可以不断调整访问控制措施以适应不断变化的环境，从而提高安全水平、降低风险、帮助运营简化和恢复运营，并提高业务灵活度。

除了上述定义的原则，核心定义还提供一组接下来即将讨论的初始零信任需求。

2.3　零信任平台需求

本节提供了一组基于前面讨论的零信任原则的平台需求基线集合。本节的目标不是简单阐述原则，而是试图从平台的角度强调相关内容。其中部分原则(特别是 API 和集成)应表示为与特定 IT 和安全功能相关的需求，并从全局和多个维度定义若干需求：

(1) 应加密数据平面(Data Plane)的所有通信。例外情况都应审慎对待(例如，DNS)。

(2) 系统应能够对所有类型的资源实施访问控制措施。访问控制机制(Access Control Mechanism)应由以身份为中心的上下文策略驱动。

(3) 数据资源保护应基于身份和上下文的策略控制访问。

(4) 系统和策略模型应支持在所有位置保护全部用户。策略模型和控制对于远程和本地用户应保持一致。

(5) 设备应能够在授权访问目标资源之前以及之后定期检查其安全状态和配置。

(6) 应能区分 BYOD 和公司管理的设备，并相应地控制访问级别。

(7) 对网络资源的访问应由策略明确授权。用户或设备本身都不应具有过多的网络访问权限。

(8) 访问控制措施应能区分同一网络资源中的不同服务。例如，授予 HTTPS 的访问权限应与 SSH 的访问权限分开。

(9) 应基于业务策略强制访问包含在具有不同分类分级的应用程序或容器中的特定数据元素。

(10) 应记录网络流量元数据，并使用身份上下文填充元数据内容。

(11) 网络流量应能检查安全和数据丢失的态势。

(12) 迁移至云平台的工作负载应包括与本地解决方案相同的访问控制策略。

(13) 自动化应包括以身份为中心的详细信息，提供高效且有效的事故响应。

(14) 分析工具应包括日志，以便有效且动态地实施策略。

2.4　本章小结

本章重点介绍了零信任的历史，从 2010 年 Forrester 提出“零信任”一词开始，后续经过不同组织(包括 Google、NIST、CSA 和其他组织)的持续演变。基于这一历史背景，本书解释和提炼了三个核心零信任原则，并增加了三个扩展原则。综上所述，这些零信任原则应作为零信任项目提案的基础。

下一章将介绍具有代表性的企业架构模型。将要介绍的模型并非包罗万象，但将提供类似的工作基础，从中可引入零信任部署模型，并说明模型如何适用于企业。本书的第 II 部分将深入探讨零信任对 IT 和安全技术的影响。