零信任安全理念

CSA GCR cloud security alliance GREATER CHINA REGION ®

CSA cloud security alliance ®

CSA 零信任工作组的官方网址是：

https://cloudsecurityalliance.org/research/working-groups/zero-trust/

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

《零信任安全理念（Zero Trust as a Security Philosophy）》由CSA工作组家编写，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：

王安宇　余晓光　袁初成　李安伦　鹿淑煜　何国锋

赵锐

审校组：

陈珊　张晨栋　杨涛

研究协调员：

夏营　郑元杰

感谢以下单位的支持与贡献：

华为技术有限公司

中国电信股份有限公司研究院

上海缔安科技股份有限公司

湖州市中心医院

苏州云至深技术有限公司

三未信安科技股份有限公司

OPPO广东移动通信有限公司

英文版本编写专家

主要作者：

Paul Simmonds

贡献者：

Hillary Baron　Marina Bregkou　Josh Buker　Daniele Catteddu　Sean Heide

Erik Johnson　Shamun Mahmud　John Yeoh

CSA分析师：

Frank Guanco　Stephen Lumpe

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秘书处给予雅正！ 联系邮箱research@c-csa.cn； 国际云安全联盟CSA公众号。

序言

零信任是一个总体的安全理念，规定对系统或数据的访问请求都应基于风险，从零开始建立信任。但是诸多企业对零信任都有着不同的定义，其主要原因之一是监管机构未曾对零信任制定统一的标准定义。因此，为了减少沟通成本，统一行业标准，提高生产效率，本文对于零信任理念的解读就尤为重要了。

零信任的核心即为“假定已被入侵”。与传统的安全理念相比，零信任更注重的是问题的解决而非问题的预防，通过控制架构的转变，企业可以更好地掌握企业安全框架，通过持续的风险监控保证更好的安全态势。

本白皮书以基于风险的零信任方法为核心，通过解析以往二元信任的不足，引出新的上下文敏感的安全态势，并指出持续风险监控的重要性，表明了零信任方法的重要特征。

除了满足零信任的重要特征，迈向零信任原则还应准确地评估风险。本文就风险评估概括了九条重要的“不信任”，任何的风险评估中都应当包含这九条。云计算也可以与零信任方法结合，它们有着一部分相同的安全优势，并且它们架构上的差异可以帮助零信任更全面地维持安全态势。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

目录

总结

如果实施得当，零信任策略或方法及其体系结构，具有巨大潜力为组织的 IT 提供更简单、更安全和灵活的业务环境。

本文从中立的角度阐述了零信任供应商和技术解决方案对组织的意义；为组织及其工作流程的战略和支撑架构提供制定建议；并使 IT 与业务目标和成果保持一致。

本文着眼于术语的起源，以及术语今天的含义，并进行主题概述，以便高管们能够理解零信任背后的目的和目标；而技术专家门可以看到他们的专业领域（或产品集）对整体方案的贡献。

原则上，可以通过以下方式将零信任视为与其他（历史）方法区分开来：

- 由内而外，而不是外部方法；零信任始于数据的价值和访问权限
- 在信任（和共享信息）之前进行验证
- 减少对物理边界的依赖
- 基于风险的数据和逻辑访问
- 信任决策基于身份

最终，对于大多数组织来说，零信任方法只是其工具箱中的另一个工具；补充现有的安全解决方案，如防火墙和 VPN。与任何其他控制一样，它可以与其他（例如补偿控制）一起使用或代替其他（保护性）控制。

零信任简介

有一个寓言可以追溯到大约 2500 年前，三个盲人在丛林中遇到了一头大象，抓住它的腿的人将其描述为一棵树，抓住尾巴的人将其描述为蛇，等等。

零信任类似于大象，根据您的专业领域、您的角色或您销售的产品，您将以完全不同的方式描述问题及其解决方案。

“零信任”已经演变成一个对立的术语，因为多年来，传统的安全模型和解决方案已经根深蒂固，从某种意义上说，IT、网络和安全专业人员的培训，已经失效多年。

Public Domain,
https://commons.wikimedia.org/w/index.php?curid=4581243

那么，什么是“零信任”？是一种策略吗？一套设计原则、架构或产品？

今天，“零信任”是一个总体的安全理念，规定对系统或数据的任何/所有访问请求都应基于风险，从零建立信任。

本文将论证上述所有内容。但更重要的话题是，这个理念是如何将当今业务需求与 IT 基础架构、网络、安全和云的风险应对方案对齐的。“零信任”也是用词不当，因为对于“问题表述”的回应，本质上取决于如何在 IT 生态系统建立信任的具体实施方案。

然而，需要注意的是，零信任的定义在不同的供应商和不同的安全专业人员之间都有不同变种。也许这主要是由于监管机构没有制定统一的标准定义。为了应对这个零信任的当前挑战，零信任理念的解读就尤为重要。

企业应该以零信任理念为目标解决什么问题?

对“零信任理念”是组织的一个独特的架构战略，由组织的战略目标驱动，并与其风险偏好保持一致，以提供满足该组织当前、中期和长期需求的灵活技术环境。该目标通过将零信任原则重构或整合到当前的业务实践和方法论中来实现。

零信任方案使组织能够更安全、更具韧性。如果实施得当，它的一些关键优势是：

- 它使组织变得更加安全和具有韧性。
- 聚焦于关键业务资产，并对其安全性采取基于风险的、量身定制的方法。
- 建立一个供应商中立的、技术无关的方案，减少了对供应商的依赖，并使企业主对信息的访问全权掌控。
- 技术和安全合作变得更加简单，尤其是与其他组织（合作伙伴、合资公司、外包合作关系等）的合作。
- 简化了 IT 和网络团队的运维模式，让 IT 和信息安全更好地与业务需求结合。
- 通过消除终端用户、IT 和安全团队之间的隔阂来提高用户体验。
- 减少资本支出（CapEx）和运营支出（OpEx）。
- 提供一个基于标准的方法来落地零信任和面向未来的投资，而不引入复杂的重构工作。

实施“零信任”的其他好处包括（但不限于）：

- 加强可视化程度和自动实时响应，赋能防御者能够有效应对威胁。
- 使得私有部署架构向云计算解决方案的过渡更加容易。
- 支持企业拥抱多云战略。
- 使企业能够拥抱 IIoT（工业物联网）并支持运营技术（OT）战略。

今天的零信任哲学

如果你严格地调研组织的 IT 基础架构、以及它们的资产和数据，大多数企业都认为边界无关紧要，只是作为一种可行的安全方案。最多会保留公司内网的一个企业 IT 流量吞吐区域，通过粗过滤器筛除流量中的“颗粒”，提供一个可控的、点对点吞吐量和服务质量。

许多组织和政府已经采用了“云优先”、“云智能”或混合云战略，而今天的初创企业不太可能拥有自己的基础设施，整个业务都依赖于外部服务，通过 OpEx（运营支出）方式进行外包。[1]

无论组织采取的技术战略是什么，它的资产（人员、系统、用户设备和数据）广泛而分散。一些资产由组织拥有和管理，但越来越多的资产被外包（例如 SAAS[2]和其他在云端或第三方的服务）。因此，组织的数据，尤其是关键数据，通常不存储在组织拥有或管理的基础设施上，这些数据通常通过互联网进行访问。

因此，美国政府国家安全局的“零信任”工作中有一个基本原则，即“假定已被入侵”！[3]

> “如果有人想要入侵，那他们就正在入侵”
>
> *- 前中央情报局和国家安全局主任迈克*

对于大多数组织来说，应对最常见的安全漏洞的架构级解决方案就是使用零信任能力。无论是公司内部网络的漏洞，还是服务供应商或第三方的漏洞，或者合资企业合作伙伴的漏洞，都可以从零信任架构的角度进行安全管理（入侵、检测、预防等）。

通过拥有对无形财产、关键数据和数据流动的细节可见性，然后设计或减轻风险，组织可

[1] Operational Expenditure; funded by day-to-day running cost, not requiring capital expenditure/investment
[2] SAAS is Software-as-a-Service
[3] NSA | Embracing a Zero Trust Security Model (U/OO/115131-21 | PP-21-0191 | February 2021 Ver. 1.0)

以更好的保护已识别的商业资产，无论这些资产在何处放置。

然而，将零信任哲学转化为可落地的架构需要一种基于风险的方法来验证交易链条中的所有实体[4]，并结合上下文（用户、设备、网络、行为参数等）和持续评估的角度，以确定当前交易是否合法，或者是否继续合法，这就是“授权”的概念。

组织正在从基于边界控制的架构转向联动式安全控制的架构，这是一种以数据为中心的控制和以用户/身份/行为和威胁为中心的控制的两者结合。零信任哲学的主要目标是将边界更接近“访问主体”和“企业资源”。 采用零信任哲学时面临的挑战是如何适应不断变化和快速演进的安全局势，以及维持组织的稳定安全态势。

“零信任”方法是假定问题已经存在（并解决问题），而合规要求通常更注重预防。这为机构和组织带来了巨大的好处，因为与其被锁定到一个单一供应商，技术负责人现在可以掌控整个框架。区别于一个仅仅满足合规要求的产品或服务，零信任实施可以归结为一个参数化架构以及一系列产生虚假安全感的风险假设。零信任赋能技术负责人可以选择最适合监测、管理和控制各地资源的最佳技术。

基于风险的零信任方法

实施任何零信任哲学都要求组织将基于风险的方法融合到信息安全措施中，包括（数据访问治理、身份和访问控制、威胁管理、IT/OT 融合等）许多支柱。这些措施涵盖了数据安全、网络安全、终端安全、服务器安全、OT 安全、IT 安全、物理安全、位置安全和个人安全等领域。

不幸的是，目前大多数技术和安全设计假设都基于二元信任的概念。“他们被信任因为他们在我们的内网中”，或者“他们是他们声称的人，因为他们最终提供了一个正确的密码”，或者“他们通过了安全审查”。风险，特别是在遵循零信任原则所要求的更细粒度的方法时，必须基于不断变化的因素：

- 了解所涉及的相关实体的上下文情况
- 了解实体所请求的目标的安全态势
- 持续分析与实体（用户、设备、身份等）相关的行为和风险

[4] Entities are: People, Devices, Organizations, Code and Agents - Definition: Jericho Forum

- 随着上下文情况的变化而持续评估

当零信任模型采取上下文敏感的安全态势后，它会变得更加强大。

上下文意味着能够理解用户、设备、组织、位置、交易的性质，以及它们与先前的交易如何相关，以及其它可能的因素。基于实体预定义的风险边界，持续分析与实体相关的行为，将增强安全上下文。

理想情况下，任何能够验证风险是否可控的系统，都应该能够对被判定是高风险的交易进行进一步认证，这种判定是基于现有的政策或额外的安全上下文。这种评估应该在尽可能接近被保护的资产的地方执行。

值得一提的是，风险是时间敏感的，随着时间会发生变化。例如：一个“暴力终止用户”的行为应该几乎瞬间阻止所有当前用户对于系统和数据的访问。持续风险评估应该成为任何基于零信任原则的方法的设计特征。

迈向零信任原则

在设计零信任的实际组件时，首先是了解风险。在了解以下每个领域内的整体风险和实体风险的同时，获得对资产和访问权限的全面了解。对于每一个领域，都要了解风险会是什么样的...

> - 淘汰（设计出来），或
> - 减轻（增加补充控制），或
> - 转移（另一方承担风险，例如；保险），或
> - 接受（风险仍然是经营成本）

因此，通过定义每个风险领域的信任级别，可以了解任何交易链的端到端风险。

应使用尽可能多的组件和/或架构策略以减轻风险。例如，对数据存储使用加密和/或对传输中的数据使用加密协议（密钥从未共享/公开）可以减轻许多风险。

然而，尤其是在实施补充控制时，为零信任体系结构设计的新策略、新工具和新架构可能会被使用。

在企业环境中讨论零信任时，任何风险评估都应包括以下内容。

1. 不信任任何网络，包括您自己的网络

首先，假设内网不比互联网更安全，通过任何网络传输的数据都应该使用适合于传输该数据的内生安全协议[5]进行保护。

一般来说，除非绝对必要，否则应避免使用封装技术（如：VPN）。例如，当一个老旧系统或者工具无法使用使用更现代的、基于风险的 MFA 的时候，一种临时的措施是采用 VPN 来保护。

2. 互联网上无信任

显而易见，如果您不信任自己的内网，那您也会认可通过互联网传输的数据会被监控、拦截、欺骗，并且通常不可信，还有互联网服务（如：DNS）也是如此。

然而，互联网通常被设计为提供非常强大的、基于标准的、具有多个入口和出口点的基础设施（例如，有线、4G、5G、专用和公共连接）。

请注意，在设计零信任体系架构时，应谨慎尝试在互联网上设置私有安全隧道。组织应确保所选择的任何解决方案都不会抵消许多弹性优势，或导致被锁定到单一供应商的解决方案。

3. 不信任您经营所在的国家/地区

从最近和过去的攻击中可以明显看出，国家级别的攻击者在任何国家/地区都有活动。 因此，所使用的基础设施，即使是“专属于您的”，例如专用 MPLS 链路、云服务或第三方托管服务，也应被假定为受到监控和可颠覆的。

请注意，大多数国家都有相当于美国政府的“国家安全信函”（NSL），禁止披露政府的数据请求。

考虑确保加密密钥仅在您的组织内或由个人持有； 如果发生对数据的合法请求或非法盗窃，则需从数据所有者处获得密钥。

[5] An inherently secure protocol is one where the data is protected and both/all parties are appropriately authenticated.

4. 不信任第三方硬件或代码

硬件可能在芯片级别[6]（具有“未记录的功能”的芯片）和电路板级别[7]（未记录的芯片/功能）受到破坏。

代码，无论是 BIOS 级别[8]、操作系统、应用程序还是微服务，都可能包含可利用的代码缺陷，或者本身就带有恶意的或被破坏的代码。

通常可以通过全面了解制造硬件和固件的整个供应链来减轻这种风险，并将成为更广泛的第三方风险管理 (TPRM) 流程的一部分，可能仅由军方和政府组织承担。

- 在可行的情况下，使用不在服务器上或不被服务器使用的密钥对传输中的数据和静态数据进行完全加密，以降低风险。
- 虽然代码审查可能是一个缓解因素，但对于许多商业软件来说，代码审查是被禁止的。因此，当使用商业软件（COTS）时，大多数组织选择接受风险[9]；或添加补充控制。
- 使用开源（包括开源库）的最佳实践应包括源代码控制、业务逻辑和代码评审（DAST/SAST/IAST）。同样，它们需要基于风险以及基于行业标准和框架，如 MITRE 和 OWASP Top 10。

5. 不信任 DevSecOps

代码开发无论是使用 DevOps 模型还是 DevSecOps 模型，仍然会引入缺陷和漏洞。当代码在内部开发时:

- 功能需求应该描述软件预期如何运行，业务需求开始于几个不同的地方。 设计人员、编码人员、测试人员和许多其他操作人员都遵循这些要求。环境分离或“职责分离”、验证和对合规性的持续监控应有助于降低风险。
- 软件开发必须在整个安全软件开发生命周期（SSDLC）中实施“设计安全”原则，无论采用何种软件工程模型（例如，瀑布式、敏捷式、螺旋式）。

[6] https://cwe.mitre.org/data/definitions/1242.html
[7] https://www.wired.com/story/plant-spy-chips-hardware-supermicro-cheap-proof-of-concept/
[8] https://searchcloudsecurity.techtarget.com/definition/BIOS-rootkit-attack
[9] Zero trust establishes the framework for minimizing risk from third parties by examining security gaps that occur during these interactions. It unifies and consolidates security policies in-house, minimizing vulnerabilities created by insufficient security practices of outside vendors

6.不信任系统管理员（“您的”或“他们的”）

系统管理员是一个高价值的特权用户，对任何组织都构成了巨大的内部威胁。组织在管理这些可能构成重大威胁的高风险用户时面临两难境地，无论是有意（恶意）还是无意（疏忽）。威胁参与者可以获得有效的管理员帐户，以便在组织中横向移动并访问和控制关键资源。在不了解行为、风险和安全上下文的情况下，很难确定何时使用有效凭据。

系统管理员通常有能力在系统上执行（或重置）任何操作，无论您如何审查您的系统管理员（假设您的组织也这样做了），实际上没有机会审查第三方雇佣的管理员（这些第三方是你的外包商/云提供商/合资伙伴等）。

对于高价值目标的系统，您应该假设系统管理员本身成为勒索、胁迫、勒索等的目标。

根据零信任原则，管理员应该像系统的所有其他用户一样受到持续验证和监控。应根据权限、访问策略、行为和动态风险，在“须知”（Need-to-Know）的原则上授予访问权限，并确定这些用户是人工用户还是服务帐户。例如，他们应该能够管理系统（备份、管理和配置系统），但不能访问实际数据。

- 如果系统不处理未加密的数据（这在存储服务器上可行，但在应用程序服务器或终端用户设备上不太可能），则可能可以实现完全降低风险。
- 可以通过特权访问管理 (PAM)，结合独立的变更控制系统和代码指纹，来实现部分降低风险。PAM 解决方案随着“即时”权限管理的发展而演进，使之已成为现实方案.。
- 可以通过将员工监控（在合法/道德的情况下）与更广泛的日志记录、监控和异常分析工具生态系统（如：SIEM、SOAR、NDR、EDR）集成，实现部分降低风险。
- 可以通过选择第三方提供商的相关安全认证或证明（如：CSA STAR、ISO27001、SOC2 等），其范围应涵盖您对供应商服务的使用，来部分降低风险。
- 当服务外包给第三方时，还可以通过利用供应商风险管理、数字风险管理和供应商风险管理等工具来实现部分降低风险。

7. 不信任服务器（安全的）位置或系统的物理安全

毫无例外，如果目标具有足够高的价值，几乎所有的安全服务器/系统位置都可能被攻破

（通过内部攻击、偷盗、暴力夺取或法院签发的搜查令）。

- 同样，如果系统不处理未加密数据，则可能实现完全降低风险。也可通过选择第三方提供商（具有 ISO27000 系列认证的）来提供部分降低风险，其范围需涵盖您的使用服务。
- 在提供基于零信任的安全服务时，物理安全性（无论是您在管理的区域位置，还是在第三方环境中管理的区域位置）常常被忽视。对服务器机房/数据中心和/或物理服务器的物理访问会严重破坏系统的安全性。
- 社会工程学（如：网络钓鱼）越来越受欢迎，人类的“安全链中最薄弱的环节”可能会破坏最佳技术防御。但是，也必须知道人类可以提供第一道、第二道和最后一道防线。 安全意识计划应该作为降低风险策略的一部分，以提供补充控制。

8. 不信任端点

鉴于“设备”涵盖所有系统、服务器等，“设备端点”由特定的人支持。通常情况下，它们以非零信任原则的方法游走在各种网络，成为边界之间的桥梁，这意味着在“外部”感染/破坏设备会将感染带到“内部”。

端点还有其他问题，从诱骗人类点击恶意代码的能力，到（现在）无处不在的家庭办公以及 BYOD 的兴起，但设备所有者通常不愿意在“他们的”设备上安装公司监控软件/应用程序。它们是人与数据的交互点，应当需要需要解密才允许交互。

端点的风险降低策略应当包括:

- “锁定”的企业级镜像。
- 代码执行限制，代码批准(通过签名代码和/或公司批准的应用商店)。
- 能够报告设备“健康”属性的端点软件/应用程序;如操作系统版本和补丁级别、防病毒版本、设备风险评分/态势等。
- 端点软件/应用程序能够报告设备的“状态”属性，如地理位置，设备模型，以及能力(如生物识别能力)。
- 用户意识培训。
- 访问关键系统的端点的异常监控。

- DNS 防火墙(或 DNS 防火墙服务)。
- 系统变更管理和补丁管理。
- 数据从端点聚合到一个集中的异常监控系统(假设它是一个企业拥有的设备)。

9. 不信任的身份认证生态

大多数(传统)身份认证解决方案都存在以下一个或多个问题:

- 它们只支持人(而不是设备、服务帐户和非人类身份等实体)。
- 它们认证机制是二进制的 (“用户 123 已经通过认证”)。
- 它们要求成为控制范围(只有当一切都在这个系统内时，你才能让它工作)。
- 它们包含非权威和/或陈旧(非维护)的属性。
- 验证必须直接或间接地只针对身份认证解决方案。

身份认证策略将可能是任何零信任架构的核心。如果身份认证策略配置正确，将实现基于上下文对交易进行风险识别，通过基于风险的有条件访问来判断交易的可行性。

这种身份认证系统的特征应包括:

- 控制点对其具有权威性的任何实体的可信(签名)属性。
- 融合来自传统网络边界之外的实体的可信属性的能力。
- 能够分析访问行为以及来自多个实体的遥测数据，如设备、访问的应用程序、权限、位置、时间等。
- 基于风险的实体和属性之间恒定等级评分机制。

无论是单独还是作为集成解决方案，赋权/授权引擎都将:

- 遵循交易访问授予权限的规则。
- 使用上下文属性及其风险分值。
- 从交易中所涉及的设备获取属性信息(例如，智能设备的 GPS)。
- 从内部和外部的其他系统获取设备、数据和情报(例如，地理定位服务或 IP 地址

聚合威胁情报数据)。

- 支持逐步身份认证，并将其扩展到传统系统和工具(例如 PowerShell)，因为这些系统和工具通常不在身份验证。
- 工具的覆盖范围内。
- 支持持续实时监控和分析交易中的行为、风险和偏差。
- 从提供持续监控和行为异常检测的系统中获取额外的输入。
- 利用(基于端口的)网络访问控制[10]来管控对某些受限网络的访问(可能用于高度敏感的访问)。
- 启用基于风险的有条件访问以改善用户体验，即仅当风险发生变化时，才触发逐步身份认证，这与行为、基准和其他信息(如使用的设备、地理位置等)相关。

随着时间的推移，授权解决方案可能会从中央控制转移到更靠近系统和应用程序的位置，或者成为系统和应用程序的一部分，以便更好地与正在处理的应用程序集成。这使得无论是在内部、在第三方还是在使用云服务时，授权实施都可以“对齐”一致。

云和零信任

零信任架构所需的风险分析与(第三方托管的)云实施所需的风险分析有很大的相似性和重叠性：无论是 SaaS、IaaS 还是 PaaS，系统、应用程序和数据都运行在一个控制最少、可见性受限的环境中。

这使组织能够在分析零信任架构风险时利用许多与分析云风险时相同的方法，例如:

- ENISA[11]致力于应对云风险[12]
- CSA 云控制矩阵(CCM)

虽然这些方法可能有助于发现风险，但降低已识别风险的许多解决方案可能会有所不同。

[10] 802.1X-2020 - Port-Based Network Access Control - https://ieeexplore.ieee.org/document/9018454
[11] ENISA is the European Union Agency for Cybersecurity
[12] https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

架构差异

云环境旨在让云服务提供商(CSP)能够完全控制其“责任共享模式”的组成部分(参见图 1 以及对网络和网络流量的可见性。

图1.云的共享责任模型

因此，大多数使用基于云的基础设施的组织将采用一种需要 CSP 信任的共享责任模型，依靠外部认证来确保风险得到适当降低，同时依赖工具和流程来获得模型中他们所负责的组件的可见性。

虽然 CSP 为他们管理的模型部分提供相关监控和日志记录，但涉及到与客户端相关的日志，组织可能希望将此类数据纳入他们自己的工具，以进一步降低使用云服务所涉及的风险。

云环境中的零信任工具

任何组织如果运行过程中混合了外部服务、内部部署、第三方、云等。那么应该确保采用的零信任理念，特别是用于支持其架构的工具和服务，将扩展到他们使用的任何第三方服务、云服务或云基础架构。

第三方环境中的数据

静态数据和处于传输过程中的数据都能通过运用零信任和云方案应对类似的风险，并且提供解决方案。然而，如果运用云服务（尤其是 SAAS 软件即服务）处理数据，控制层面解决方案的实施会变得更困难。

云计算或零信任不适用的场景

迁移到零信任架构将使企业不再依赖物理边界作为安全界限，那么系统和应用程序的部署位置就不再重要。但还有其他运营、安全性和设计限制方面的问题需要考虑。例如：

- 在保证隔离和冗余度，并且网络服务达标情况下，工业控制系统需要与其控制的设备共用同一个网络。
- 组织内通过资质审查的员工需要直接对安全风险较高或本身价值较高的系统和应用程序进行实时监控，并做好管理工作。

将云解决方案集成到基于零信任风险的体系架构中的关键是能够（实时地）掌握云解决方案所涉及相关信息，并需要进行信任的验证，即“信任但是仍然验证”。

通过云计算交付的零信任来降低风险

云服务不再仅限于托管需要以零信任保护的应用程序，还可以针对这些资源提供安全的零信任访问。这些云交付的零信任解决方案有着与基于云的应用程序托管的相同的优势——兼容性、拓展性、可见性、用户体验透明性等。减少外部攻击面、消除单点故障、分离控制和数据平面、防止未经授权的横向活动以及减少易受自动程序攻击的漏洞，这些都是基于云的零信任访问方法所提供的一些潜在风险缓解措施。

结论

大多数企业都认为他们的信息技术部门和安全团队会增加业务流程的繁琐程度。落后的边界防御安全模型导致了许多问题，因为需要复杂网关和接口来越过边界，就要对人员和设备采用隔离的身份认证。

现在这个时代，没有企业是一座孤岛。董事会、商界领袖和股东们要求数据和系统层面活动要彼此配合，并且无障碍连接，以此提供及时、高效的服务。

将零信任策略与业务风险、业务成熟度和业务战略情况相结合

零信任为正在开展数字化业务的企业提供了无限可能。

零信任让企业可以将信息技术更好地运用在企业发展战略上。无论是在内部网络中，通过公用互联网，还是作为外包服务的一部分，现代网络计算的主要功能是促进协作，这包括企业内部人员的协作，但更重要的是要促进与企业外部实体协作。

要实现零信任必须实现组织层面和文化层面的转变；它既不是技术问题、安全问题，也不是身份问题，而是在于业务蓝图与相关技术支持的战略调整。

管理目标和管理层面提供的支持将在克服文化障碍方面发挥重要作用，所以零信任会为企业工作和企业运作方式带来根本性改变。“永不信任”的概念易于理解，但在战略和运营层面上，为所有内部和外部利益相关者的实施、管理和维护带来了重大挑战。

因此，零信任的实施必须由业务部门主导并负责。他们需要明确定义关键系统，了解与这些系统交互的权利规则，还有他们要面对的风险。

零信任理念和架构不是专为保守性用户而构建的，而是希望能够以低成本、高效率、以及风险完全感知的方式达成企业业务需求目标。

附录 1：零信任战略的高阶方法论

在实施零信任战略时要牢记：零信任战略目标是将信息技术战略和安全战略调整到与整体业务战略一致。

批判性地思考“不设限制（或者最小化限制）”将会如何推动业务，这也是一个关键因素。这类似于谷歌/BeyondCorp 的模式：“世界上没有可以完全信赖的网络，无论是在我们公司的办公室里，还是在星巴克”。但是事实正好相反，每个人都能随时随地使用我们企业的网络，即使他们在星巴克。

这种思维转变可在以下场景应用（场景有待补充）：

- 广泛使用自带设备（BYOD）。
- 外部顾问、合资企业、合作伙伴等在合作办公时能使用他们自己的办公电脑连接到你的公司系统。
- 合作伙伴和外包服务商能够将他们自己的设备连接到你的公司网络上。
- 使用公共 5G 移动网络应用。
- 采用“多渠道连接”策略，利用多种低成本的公共连接到互联网。
- 广泛使用物联网和物联网设备[13]（大多在 5G 移动网络场景下）。
- 采用 ICS/工业 4.0 。
- 并购场景：加速价值落地进程，不必要整合企业之间的网络。
- 应用程序方面的变化：将应用程序从数据中心迁移到云或联合数据中心，而不影响用户体验。

一些企业可能会选择在采用 IPv6 战略的同时使用零信任战略；所以会允许所有人员、设备和组织能够直接连接到你的系统（无论是内部直连还是外部托管），所有人都使用相同的安全模型/访问模型。拥有多个站点的组织可以独立利用本地互联网连接或与企业 WAN 连接相结合，这有利于构建更牢固的全球网络，所以两种方法综合运用有望促成更强大的全球互联网战略。

[13] IIoT = Industrial Internet of Things, IoT = Internet of Things (generally more consumer focused)

关键系统

每个组织都有一组关键系统和相关的数据流,组织依靠这些系统和数据流来开展业务。识别这些系统以及业务本身,可以开发零信任架构(希望具有常见组件),从而可以建立一套“权限”规则,每个系统将根据这些规则授权访问。

权限/授权

权限[14]，即定义资源可以在可接受的风险水平下由何人以何种方式访问的规则（请记住,风险是双向的,而且始终不对称)，应由受信任的属性和其他补充信任来源驱动。因为这样有助于得出上下文，从而作出权限决定。

如果妥善实施，权限应延续到应用程序本身。例如，允许设备/人查看他们的银行账户是一个可接受的风险级别。但不允许转账。为此，可能需要某种级别的进一步认证。

基于上下文和风险的访问权限也可以为所有用户提供更流畅的系统和数据访问。

对于权限决定中使用的所有元素，关键的是考虑到用于作出决定的属性/数据的真正权威性来源。

上下文

上下文分为两种形式:断言的上下文和推断的上下文。

- 断言的上下文通常是两实体的数字签名结合——这里是我的断言：我是企业笔记本电脑，是由企业签名并由笔记本电脑断言(“设备”和“组织”的结合)；或者，我是 Acme Corp. 的全职员工约翰·杰(“人”和“组织”的结合)。
- 推断的上下文是可以收集的。通常通过观察——这台笔记本电脑的 IP 位于俄罗斯,或者上次这位用户试图访问此系统时的地理位置在公司总部,但 10 分钟后在保加利亚。
- 理解上下文以及拥有能够为权限系统/引擎提供属性的系统以作出基于上下文的

[14] See also: CSA Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 - Domain 12: Identity, Entitlement, and Access Management (cloudsecurityalliance.org/download/securityguidance-v4)

访问决定,这对成功至关重要。

治理和监督

任何组织内的零信任计划必须有适当的治理模式、监督委员会、指导委员会和执行层的支持。实施零信任模型可能会破坏每个网络、系统和工作方，因此必须建立适当的治理模式和监督机制，以确保企业全面理解和支持这些变化。

附录 2：构建您的零信任路线图

董事会和高级管理层对于钱和风险是容易理解的。对组织来，,具备能够将零信任之旅的技术和优势的语言翻译成商业语言的人员至关重要。

在制定零信任路线图时,关键步骤应如下：

1. 确保业务领导理解实施零信任理念的必要性和益处——大多数企业将任命一个由业务主导的指导委员会。
2. 理解当前环境可以是一个很好的起点。安全评估对于理解组织的“现状”至关重要。
3. 与业务部门合作，了解他们的短期、中期和长期战略路线图。这些路线图需要与组织的安全愿景、使命和文化相一致。
4. 与业务部门合作，确定业务的关键系统和资产，并与这些系统/资产的业务所有者合作，以了解风险和这些系统/资产的未来战略计划。
5. 映射和理解服务架构和数据流。
6. 映射和确定涉及的实体(人员、设备、组织、代码和代理)。
7. 挑战业务假设，宣传零信任可以实现的目标（记住:业务领导人也习惯于“边界”思维)。
8. 举行风险工作特别行动（IT、安全和业务联合)，为关键系统和资产定义可接受的风险阈值。

9. 对所有关键系统的要求列表作为结果发布，并提供高级技术战略概述。
10. 与零信任架构师合作,定义一系列技术解决方案来实现战略。
11. 与业务部门一起审核，并根据需要进行调整迭代。
12. 制定路线图，从目前的状态转变到明天想要的目标。
13. 实施合适的零信任成熟度模型，以在路线图的每个阶段验证您的成熟度。

基本原则

- 零信任不是一个“项目”，也不是一种产品，它是一个不断进化的旅程。
- 所有的假设都需要被挑战。4 个“W”和 1 个“H”：什么（What），为什么（Why），哪里（Where），何时（When）以及如何(How)，通常有用。问为什么需要这个以及它带来的好处。
- 保持非常简单。复杂性成本高昂，很少有效或可扩展，而且当然不利于无缝的商业环境。
- 记住人类通常是第一、中间和最后一道防线。零信任不仅仅关乎“技术”。
- 记住从小开始并采取渐进步骤。
- 记住您的零信任战略应该不断为业务所有者提供“回报价值”和“保障”。
- 做好基础工作，选择“快速获胜”？
- 尽可能在自然更新时间升级/增强系统。
- 最终目标应该始终是将剩余业务风险降低到可接受水平。
- 为老旧系统制定独立战略，不要让遗留问题驱动您的战略。

记住,不存在所谓的零信任解决方案。您的战略将是独一无二的，由多个解决方案组成，并且应该是 IT、网络和安全三者的持续进化结合，以更好地支持业务驱动的计算。

零信任理念的挑战

除非您的组织是从“白手起家”开始，或者您有业务授权的级别来“拆除和替换”几乎每

一个系统和网络组件，已经成立的组织向完全零信任架构转变的挑战不容低估。

常见错误

- 试图使用零信任组件加固(或更糟：复制)现有的基于边界的安全模型。
- 认为零信任是一个“网络”、“内网”或“安全”问题。
- 试图“煮沸整个大海”和验证所有内容——风险为本方法至关重要。
- 将 VPN 技术应用于任何其他过渡工具和老旧系统以外的用例。

信任

- 找到有效和高效的解决方案来与不在您直接控制下的实体建立信任[15]是一项挑战。
- 与此相反的是，陷入“控制中心”问题的陷阱——“我们只能在所有系统都在我们控制中的情况下作业。

身份识别

- 对于大多数组织来说，联邦认证承诺了很多，却带来复杂性和定制化解决方案的恶梦。相反，请看那些允许使用可信的（签名的）属性进行授权的解决方案。
- 了解你的组织真正具有权威性的实体的属性，并且了解你将从哪里（以及如何）使用这些属性。

老旧系统

- 老旧系统可能意味着问题一直存在! 这些问题通常是无法修复的，你需要一个变通办法来降低在零信任环境中运行老旧（可能是脆弱）系统的风险。
- 谨慎行事，为符合零信任的解决方案制定一个计划和共同商定的升级路径。
- 扁平网络的分割和微隔离是一条充满风险的道路，虽然隔离老旧系统可能是可行

[15] Botsman, Rachel. “Who Can You Trust? How Technology Brought Us Together – and Why It Could Drive Us Apart” Penguin
Books Limited, 2017, 5 October 2017 ISBN-10: 9780241296189 ISBN-13: 978-0241296189

的，但只有在绝对必要的情况下才这样做，并且要有一个解决老旧系统问题的计划。

云

- 云迁移既是机遇也是风险。
- 避免以零信任的名义，在云中“迁移复制”本地（外围和内部管理）的解决方案和架构。云需要与你的零信任架构对接的并适用于云的架构，最好是找到足够灵活的零信任解决方案，以全面集成云和内部解决方案，包括混合和多云的部署模式。

监控和观测

- TLSv1.3 和其他类型的加密协议不利于监控，在可能的情况下，监测终端、应用和数据，而不是监测网络或网络网关。
- 避免封装流量，特别 VPN，因为它限制了获取上下文的能力，造成无法了解风险情况。
- 用威胁建模的方法来满足监测要求。

隐私

- 在终端用户看来，目前很多零信任方法都会侵犯隐私，只有当用户同意时，才能获得监控的权限，或者只有在自带设备（BYOD）上安装公司应用/程序才能有访问权限。

互操作和供应商锁定

- 尽可能地利用标准，确保不仅与组织内的不同系统，而且与外部各方进行互操作。
- 严格评估供应商解决方案的互操作性水平，避免“控制权”陷阱。

附录 3：零信任架构和其他框架

- NIST SP 800-207 - 零信任架构

https://csrc.nist.gov/publications/detail/sp/800-207/final

- CISA - 零信任成熟度模型 (草案)

https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

- NCSC - 零信任架构设计原则

https://www.ncsc.gov.uk/collection/zero trust-architecture

- 云安全联盟-软件定义边界 SDP 标准规范最新版

https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-and-zero trust/

- 云安全联盟-SDP 架构指南

https://cloudsecurityalliance.org/artifacts/sdp-architecture-guide-v2/

- 云安全联盟 - 云控制矩阵 (CCM)

https://cloudsecurityalliance.org/research/cloud-controls-matrix/

- 在 21 世纪赢得信任 - CSA DC 分会

https://cloudsecurityalliance.org/artifacts/earning-trust-in-the-21st-century/

- ENISA - 云计算风险评估

https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment/@@download/fullReport

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