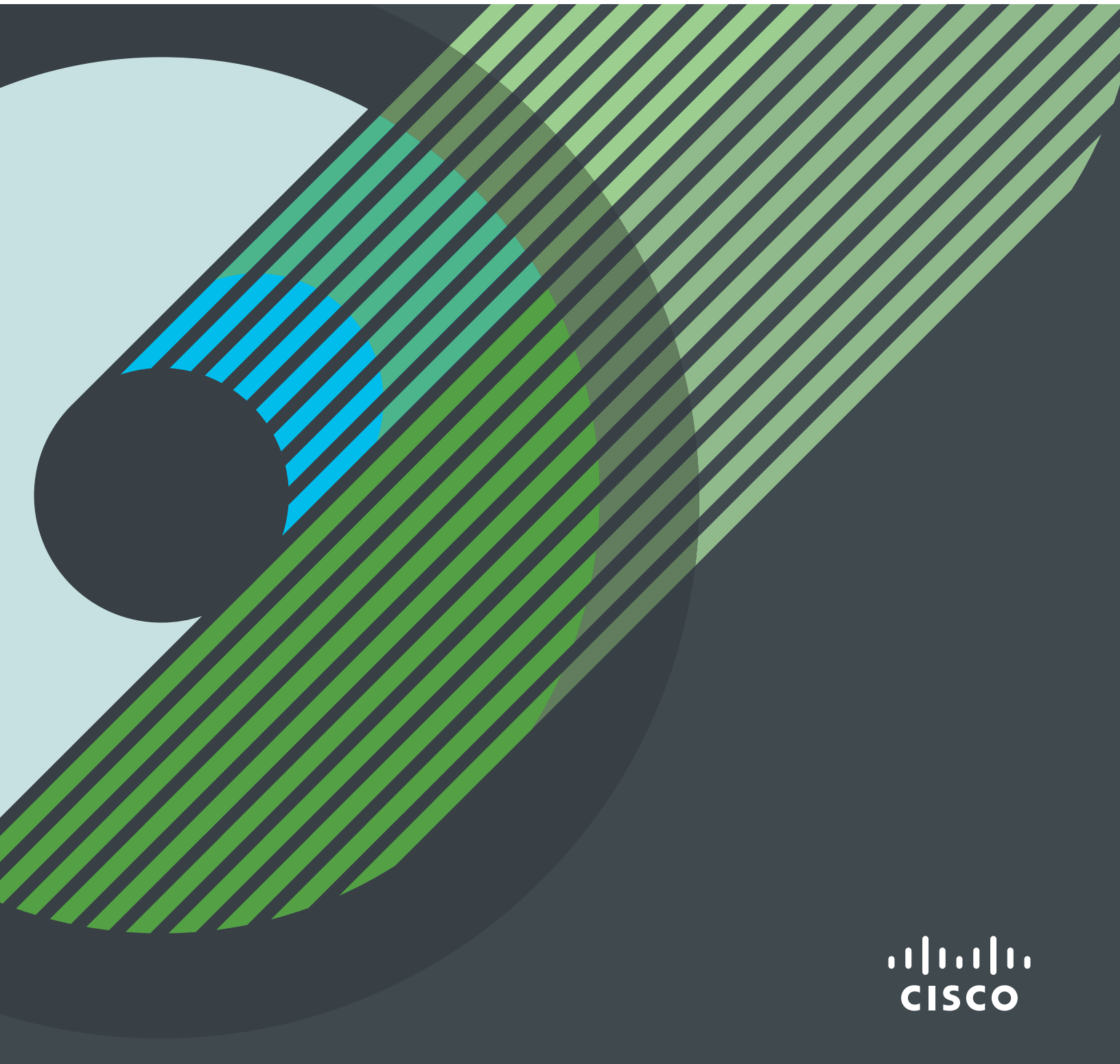
# 零信任

## 让安全超越边界



# 零信任

## 让安全超越边界




**AUTHORS**

J. Wolfgang Goerlich
Wendy Nather
Thu Pham

0.0

# 为什么选择零信任？

我们之前的安全方法是，划分属于企业以及不属于企业的信息资产（服务器、台式机、网络、应用程序和登录名），通常通过边界防火墙以及部署在终端的安全软件来保护。但是当我们看到屡屡登上新闻头条的那些案例就能发现，这些防护措施还远远不够。多年来，大家一直在为推进去边界化而努力，为了解决“去边界化”问题，早在2003年就开始举办了杰里科论坛(Jericho Forum)。随着云计算作为一种数据存储和处理平台而被人们日益接受，这种思路才真正得到企业的关注。Forrester Research 的首席分析师 John Kindervag 在2009年左右就率先提出了“零信任”这一术语，并基于该术语设计了一个特殊的安全框架。谷歌公司不仅针对这一原则的内部落实做了详细描述，还赋予它一个特有的名称 - BeyondCorp。当下，这一原则的可行性已经扩展到越来越多的企业组织，企业在考虑如何落实这套方案时，也掌握了可供参考的具体应用实例。

企业在面对消除边界这一理念时，通常比较犹豫，尤其是如果他们最近刚刚对边界进行了加固。

**所以，我们不要认为零信任原则是在消除边界，而是要借助这一原则来强化企业的内部安全，这样一来，网络边界就再也不是阻挡恶意攻击的唯一屏障了。**

# 传统方法

用于保护企业信息资源的传统方法一般会做以下几点假设:

1.访问企业信息资源的终端设备，其所有权、配给权和管理权均归企业所有。

2.所有用户、设备和应用程序的位置均是固定且可预测的，通常由企业网络防火墙提供防护。

3.初始访问只需一种验证方法。

4.同一类别的企业管理系统从本质上可以相互信任。

这些年来我们逐渐意识到，由于移动技术、BYOD（自携设备）、云计算的不断发展以及合作伙伴间协作关系的日益密切，这些假设已经不再适用。在 IT 日趋消费化的大背景下，用户不仅追求个性化更强的网络环境，又希望在使用个人设备时免受企业的管制。而攻击者在成功突破一个防御点（例如防火墙或用户登录名）之后便能利用网络固有的信任弱点，通过在网络、应用环境中横向移动来锁定敏感数据目标。在受信任区域内发起攻击的内部威胁则可以获得更高的权限。**我们再也不应认为“内部”实体都是可信任的，不能以为只要对这些实体实施直接管理就能降低安全风险，或者只需要一道验证就足以抵挡威胁。**

# 走向零信任安全

Forrester 将“从来不信任,始终在校验”规定为“零信任”的指导原则。换句话说，假设您网络中的每个部分都存在潜在威胁（就像直接访问互联网一样），您就必须对访问请求进行相应地处理。针对那些想方设法绕过防火墙（例如，通过遭泄漏的用户凭据或易被攻击的面向 Web 的应用程序）或在企业内部“受信任”网络中发起的威胁，我们应当通过可防止威胁横向移动的额外安全控制措施对其加以阻止，从而将恶意攻击所产生的影响降到最低。

网络边界，与其将它视为网络“边缘”的一种访问控制方法，倒不如把它看作能够实施访问控制决策的任何位置。这道边界仍然可以是防火墙或交换机，但也可能是其他层面：在登录第三方 SaaS 应用程序时，使用个人 ID 与使用公司 ID 之间的区别不仅决定了哪些安全决策适用，还决定了这些决策由谁来制定。应用程序试着访问数据库的地方，是边界；用户为执行敏感操作而提高权限时，也是边界。每次出现访问事件时，零信任安全模型都会提醒您是否确认原有的信任假设。

# 零信任安全方法

## 搭建零信任模型，要遵循以下几项基本原则：

- **以可见性指导策略。**为技术管理人员提供尽可能丰富的情报和可见性，以便在制定策略时有理有据。
- **信任不是一次性的，也不是恒久不变的。**这就需要我们不断地对用户、设备和应用程序的状态进行反复评估，并对信任度做出相应的调整。通过遏制新发现的威胁和漏洞，随时做好准备，以应对那些使网络风险级别升高的安全事件。
- **所有权不等于控制权。**从 BYOD 和 IoT（物联网）设备到 SaaS 和公有云，验证并将信任扩展到所有权或管理权并不掌握在企业手中的设备、应用和网络。
- **边界为您做出访问控制决策提供了广阔空间。**选择最适合企业网络环境的层面和流程点，包括网络层、应用层、身份验证点、以及交易处理工作流程。
- **访问决策的制定以每一次重新建立起的信任为基础。**组内成员资格、层内应用服务、或连接到某个网络位置的设备，本身都不足以对活动进行授权。
- **有效遏制。**将最低权限和分段与各种响应能力结合起来，以及时监控威胁活动，并限制威胁活动的蔓延。

## 除了要质疑所有信任假设之外，您在执行该模型时最好还应具备以下特征：

- **透明化。**安全措施应尽可能在无形中为技术使用者提供保障。
- **以零接触支撑零信任。**通过合理化、自动化、编排、集成来尽可能降低管理压力。

## 业绩成果

采用零信任模型后，您在处理每一次访问请求时都要对用户、设备、容器、网络和应用程序的安全状态进行验证，从而帮助您获得更全面更深入的可见性。

您可通过细分资源以及仅批准必要权限和流量的方式来缩小企业的受攻击面。如果您同时采用更多身份验证因素、加密措施并对已知和受信任设备进行标记，就能有效增大恶意攻击者收集所需资料（用户凭据、网络访问权限和横向移动能力）的难度。

最后，无论用户身处何处，正在使用哪种终端设备，将应用程序部署在本地还是云，他们都可以获得完全一致且效果更好的安全体验。

[1] 有些专家也将其称为“半透明化”：应当具备足够的可见性，以便用户在必要时能够因知晓安全措施的存在而感到安心。

# 零信任安全三大支柱

安全不应当是一刀切的主张，即使在相同的企业环境下亦是如此。举个例子，如果用户不使用过多的应用，连续身份验证机制能够一直保持非常理想的效果：但是如果多种因素身份验证过于频繁，用户势必感到厌烦（而且会试着规避相关控制手段）。

再看软件，频繁的身份验证对软件来说并不构成问题，因此彼此通信的工作负载足以为这类交互提供支持。物联网设备（例如医疗设备或制造设备）可能会因安全性和可用性问题而影响它们的联网方式。在此，我们希望借助零信任安全的三大支柱来简单说清楚其中的差异：

**01**

### 面向企业员工的零信任安全

指那些使用个人设备或企业管理设备访问工作应用程序的员工、承包商、合作伙伴和供应商。这项支柱能够确保只有授权用户和安全设备才能访问应用程序，而无需考虑位置因素。

**02**

### 面向工作负载的零信任安全

指那些在云、数据中心中以及可实现彼此交互的其他虚拟环境中运行的应用程序。这项支柱重点在于确保 API、微服务或容器在访问应用程序中的数据库时的访问安全。

**03**

### 面向办公场所的零信任安全

这项支柱重点在于确保连接企业网络的任何设备（包括 IoT）的访问安全，例如用户终端、物理和虚拟服务器、打印机、摄像机、暖通系统、终端机、输液泵、工业控制系统……

在以下章节中，我们将按照目标风险、实施方案和建议成熟度对每个支柱进行细分。

| | 目标人群或对象 | 信任验证时刻 | 目标地点 |
|---|---|---|---|
| 企业员工 | 人员及其设备 | 访问应用程序 | 任何地点 |
| 工作负载 | 应用程序、服务、微服务 | 与其他系统通信 | 本地网络、混合云、公有云 |
| 工作场所 | IT终端及服务器、物联网（IoT）设备、工业控制系统（ICS） | 访问网络 | 本地网络、混合云、公有云 |

# 1.0
# 面向企业员工的
# 零信任

## 目标风险

面向企业员工的零信任
安全方案可为企业化解以下几大风险:

- 重要的账户凭据（即用户名和密码）在很多时候都是通过网络钓鱼攻击或被攻击的第三方遭到窃取，然后被远程恶意攻击者(包括僵尸网络)重新使用。威瑞森（Verizon）**2019年数据泄露调查报告**指出，近三分之一的数据泄密事件都存在账户凭据被盗的情况，这就表明密码是一种可突破传统边界防御机制、并在不被发现的情况下顺利访问应用程序的一种有效手段。

- 如果恶意攻击者能够突破防火墙，或在企业内网中发起攻击，那么这种攻击会逐渐扩散并破坏关键系统，从而窃取敏感数据。**而我们需要做的则是直面现实：局外人只要伪装地足够完美，便很难将其与局内人区分开来。**外部攻击者可通过相同的方法混进合法用户的工作中，因此您必须对每个用户的操作权限加以限制。

- 恶意攻击者还会利用适用于同类资产的不同策略或执行方式之间的差异，这是另外一个重大风险。如果在采用不同类型身份验证的两个不同的系统中允许使用相同的机密数据，那么恶意攻击者肯定会选择更容易窃取的数据-要么是由于它信任可被您利用的其他信息，要么是由于某种身份验证方法存在固有缺陷。如果某个应用程序或系统处于不同控件的保护下（具体取决于用户是否位于“边界内”），那么恶意攻击者则会把比较薄弱的一组控件作为攻击目标。

- 基于云的外部应用和移动用户则要面临企业边界保护机制之外的攻击。

- 如果用户使用无法管理及未修复设备访问关键系统和数据，极有可能会将企业置于危险的境地。这些薄弱点会导致勒索软件攻击、其他类型的恶意软件攻击、以及未经授权的访问。

## 概述

要落实面向企业员工的零信任安全方案，离不开合法终端设备以及使用它们的合法用户。而这些设备和它们所访问资源之间的端到端加密手段，则会让原有的防护如虎添翼。

最后，仅允许按用户的角色所需为其分配最低访问权限（也称为“最小权限”）。只要按照正确数量的身份因素进行用户验证，并且使用已注册且经过安全漏洞检查的终端设备，那么用户就能通过一个集中的代理精确访问他们已被授权访问的那些资源。

## 员工零信任安全成熟度模型

### 第1阶段 构建用户信任

务必采用正确的机制和流程，以确保只有授权用户才有权限访问企业资源。虽然实现这一目标的途径有很多种，但比较常见的还是多因素身份验证（MFA）技术。

### 第2阶段 设备及活动可见性

务必采用正确的机制和流程，以确保只有授权用户才有权限访问企业资源。虽然实现这一目标的途径有很多种，但比较常见的还是多因素身份验证（MFA）技术。

### 第3阶段 可信任设备

无论是否归企业所有，无论托管还是未托管，企业组织都可以将自己已注册并希望与特定用户相关联的设备标记为受信任设备。

### 第4阶段 适应性策略

根据资源的敏感性和已知的安全状态实现访问要求，以便根据风险等级作出适当的管理。策略可以包括：仅授权企业管理设备，要求特定版本的补丁软件、加密手段或基于用户行为的递升式认证等。

### 第5阶段 面向企业员工的零信任安全

至此，所有应用程序和系统在前面列出的阶段中都已提及；对风险事件的监测和响应也一刻没有停止；且所有用户都能拥有一致的单点登录体验。

## 2.0
面向工作负载的
# 零信任

### 目标风险

面向工作负载的零信任
安全方案可为企业化解以下几大风险:

- 如果恶意攻击者利用了应用程序的漏洞，就能通过横向移动来攻击各种关键系统。
- 恶意攻击者窃取并外泄敏感数据。
- 内部应用和外部云应用间迥然不同的防控方式成为网络安防人员的盲点。
- **54%的 Web 应用程序漏洞容易被恶意攻击者利用，**这意味着如果服务器和应用程序未经过修复，就会暴露在已知漏洞中，恶意攻击者正是利用这些漏洞入侵您的系统。

### 概述

企业的系统在功能上不断丰富，并根据具体的业务需求增加连接和依赖项。为了促进企业系统这种良性的增长，系统设计人员和开发人员有时会倾向于采用最宽松、最灵活的安全配置。由此产生的过度信任会被恶意攻击者利用，然后再通过横向移动顺利访问企业的敏感资源。解决这个问题的最佳答案即网络分段。比如由表示层、应用层和数据层组成的通用三层 Web 应用程序。

我们可将这几层划分为不同的网络，并通过特定的访问控制来限制层与层之间的通信方式。应用层上的服务由于要与同一层上的其他服务进行通信，因此会被信任，这样一来便不利于解决在层内横向移动的风险。应用程序越来越复杂，数量越来越多，过度信任问题也会随之增加。而且，久而久之，企业很可能会搞不清哪些才是关键性工作负载，其他哪些资源需要与之通信，因此要准确锁定它们，更是难上加难。

这些问题理论上有两种解决方法。我们可以假设网络是不受信任的，并将信任决策向上移至应用堆栈。这种方法的优点在于我们可以将控制措施植入应用程序。而缺点就是必须在实施零信任安全方案后才能进行应用程序的开发。开发人员不会一直记录应用程序应当如何与其自身的工作负载进行通信，更别说如何与外部资源通信了；鉴于这一点，网络和安全运营团队如果想知道如何在最小权限和应用可用性之间掌握好平衡就更加困难。

另外一种方法就是通过仅根据应用程序的需要来限制通信，以此降低网络内部的信任。这种方法非常适合现有的应用程序（包括旧版本），并且有助于将现有生态系统引至零信任模型之中。这种方法的缺点就在于我们需要依靠网络安全机制，而且即使这道安全防线被突破，应用程序服务也不会发现安全机制被削弱这一危险的情况。

这两种方法并非相互排斥，在需要通过冗余控件来满足高安全等级要求的环境中，二者可能会更好地彼此平衡。

为了将现有环境向零信任模型引导，我们的网络必须要在网络通信点完成信任评估和访问控制决策。考虑到我们的应用程序服务通常分布在云服务商、数据中心和其他异构虚拟化环境中，因此要做到这一点这绝非易事。我们需要定义一个应用程序生态系统，使其仅容纳应用程序的依赖项，包括服务、流程和网络通信。然后，我们就能通过白名单或默认拒绝模式来进行访问控制，而且能够在不考虑网络或环境的情况下，都只对应用程序所需的资源进行授权。在明确信任等级时，我们的依据并非网络的位置，而是应用程序的具体要求。

实现这种微分段需要三种技术

- **深入、广泛的网络通信洞察。**以分布式网络传感器代替传统的中央监控系统（SPAN / TAP 或 NetFlow），从而使大规模深入可见性成为可能。

- **精确、实时的应用程序建模。**大数据分析技术大大减少了人工记录应用程序的工作量，从而帮助用户及时了解流量模式及依赖关系。

- **应用控制策略到跨不同环境中多台设备的能力。**一个统一的高级策略引擎，同时管理在多个多云环境中的访问控制设备，由此简化了应用程序的可见和分析步骤。

## 可见性、分析、策略，三者结合，由此降低了应用程序生态系统中存在的过度信任。

但是，如果出现信任滥用的情况，会造成怎样的结果？ 举个例子，假设企业面临管理人员和其他特权用户带来的风险，而这部分用户往往在较大范围内都享有较高的访问权限。任何会威胁到开发人员或管理员身份凭据的外来入侵者都可能获得访问权限，而安全操作人员对此可能毫不知情。即使为安全操作团队配备负责检查单个工作负载和连接情况的专人，也无法彻底解决这个问题。为了面相工作负载实现零信任安全，思科通过无人监管的机器学习技术和行为分析技术来监控恶意活动的迹象。一旦发现恶意行为，网络就会立即隔离相关服务器并阻止通信，以此来撤销信任。

变化的速度一旦超出了人们的能力范围，人们必然会选择通过自动化技术来解决问题。而这就网络分段技术当下的发展状态。如果从零信任的角度进行思考，系统设计和开发人员也能找到解决问题的新思路。面向工作负载的零信任安全凭借更优质的洞察、更快速的分析以及对应用通信更深入的了解，围绕预期行为重新定义了什么是边界。从最初的威胁到横向移动再到数据泄露，恶意活动在整个过程中都清晰可见，因此可防可控。

## 工作负载零信任安全成熟度模型

### 第1阶段 构建工作负载信任

查明具有关键任务工作负载的应用程序生态系统和环境。这个阶段主要明确零信任方案的范围。

### 第2阶段 工作负载可见性

深入洞察应用环境中的设备、流程、数据包、网络流以及工作负载的通信情况。这项工作仅限于应用程序生态系统，此外可见性对于深入洞察工作负载（例如未下载补丁程序的软件以及配置状态）也至关重要。

### 第3阶段 映射应用程序依赖项

在分析网络通信和数据流的基础上完成应用建模，对应用层进行分类，并找出应用程序依赖项。这些工作需要一段时间才能完成，目的就是要捕获那些不常见的活动，例如月度工作或季度会计流程。应用程序映射的结果越准确，得到的策略就越正确。

### 第4阶段 策略及微分段

在对源自企业员工及办公场所相关支柱的身份及上下文信息加以适当考虑的前提下，制定相应的策略以尽可能降低应用程序生态系统中的信任，执行策略模拟及验证，并面向所有环境完成一致的策略部署。微分段技术以流量白名单（也称为默认拒绝）为核心，旨在根据工作负载的具体需求对访问边界进行相应的移动。

### 第5阶段 面向工作负载的零信任安全

在零信任安全方面已经比较成熟的企业会对企业的各种环境进行持续改进和实时监控。俗话说，唯一不变的就是改变 – 应用程序、企业组织、恶意攻击都会发生改变 – 因此，随着生态系统的日益演变，零信任安全需要策略也随之演变。

## 3.0

面向办公场所的

# 零信任

## 目标风险

面向办公场所的零信任
安全方案可为企业化解以下几大风险:

- 恶意攻击者利用终端、服务器或设施设备的漏洞在网络中站稳脚跟，并通过横向移动来破坏关键系统。
- 攻击者通过对网络业务基础架构的攻击来破坏正常运行。
- IoT 或者工控网络（OT）存在的漏洞。
- **据调研公司 Quocirca 称**，有百分之六十的企业都经历过因网络打印机产生的安全事件。
- 据卡巴斯基（Kaspersky）称，**2017至2018年间，新的 IoT 恶意软件变种数量已增长了三倍。**

## 概述

现代办公场所通常以园区网、数据中心、广域网、分支网络和云网络为支撑。信任被扩展到任何用户、设备和应用程序，再通过有线或无线方式连接其他用户、设备、应用程序以及办公场所的其他部分。办公场所中会布置一些最终用户设备、IT 服务器和打印机、工业控制系统（ICS）以及 IoT 设备。无论哪一类设备在企业网络上进行身份验证和通信，面向办公场所的零信任安全方案都将及时强制实施信任。

但是，员工使用的设备和安装在办公场所中的设备，二者之间的确存在明显的差异。我们可以对面向终端用户应用的访问决策强制实施信任，但这种思路并不适用于打印机、生产控制设备、暖通设备、标记阅读器等设备。为了覆盖所有与业务相关联的系统，我们需要将堆栈的底层移至网络。

我们在设备管理、设备修复以及非法设备防御方面的能力已经不足以应对网络中数量激增的设备。而近年来网络设备的爆炸式增长，也让物联网得到了广泛关注。物联网通常建立在消费级平台上，缺乏企业级安全控制措施，并且可能无法修复。而这就会带来一种结果：我们拥有了更多类似的设备，这些设备平均每台的漏洞数量相对更高，而且要维护物联网的安全也相对更加困难。在物联网成为人们关注焦点的同时，我们也不能忽视打印机、视频会议、安防摄像头、VoIP 电话等一系列传统的商业设备，因为这些设备仍然为犯罪分子入侵企业网络提供了可行途径。此外，我们需要考虑的还有医疗设备和 OT。出于操作、功能和技术方面的许多因素，这些设备通常部署在安全团队无法修复或保护的平台上。从广义上讲，面向办公场所的零信任安全策略必须能够跨越所有设备实现身份验证、授权、分段和信任监控。

零信任假定网络本身是不安全的。当用户、设备和应用程序连接网络时，我们需要对网络进行保护，反之亦然。在零信任网络中，任何有漏洞的设备均要被屏蔽或分段，以降低它们被犯罪分子发现和利用的可能性。此外，在零信任网络中，还要防止其它设备免受被攻击和遭利用设备的影响。这两套保护措施密切相关，而且都需要我们掌握使用网络的所有已知实体以及设备的安全状态。

当设备试着连接网络时，就需要做出访问控制决策。网络工程师们往往会通过某些固定属性（例如，网络交换机所在位置或 IP 地址的组合）来完成此任务。在这个模型中，我们在对设备进行信任时，并不了解它们是否存在漏洞或已遭恶意利用。传统的信任模式所依据的属性也通常很有欺骗性。企业在向零信任过渡的过程中，信任决策必须根据许多因素来做出，比如身份和行为，而且需要根据设备行为和任何不断变化的因素进行定期验证，尤其是要通过限制原始网络访问权限或完全切断其访问路径来应对新查明的威胁和漏洞。

网络访问控制（NAC）构成了实现零信任安全的基础。在这个模型下，设备必须先对网络进行身份验证，才能被信任，然后连接网络并进行通信。通过 802.1X 和基于证书的身份验证搭建起的软件定义访问控制框架就是一种理想的方案。而 Windows 设备则能利用活动目录和 Windows 管理规范（WMI）对网络进行身份验证。如果这些方法不可用，我们也可以选择 MAC 旁路认证（MAB）。虽然 MAB 具有一定的欺骗性； 但是，对于不支持新方法的老旧设备，或我们无法通过配置让设备支持这些新方法，那么它可能就是唯一的选择。

零信任网络的下一个层次便是基于组的分段网络。我们会对各种网络连接进行验证。在做出访问决策时，网络会根据设备隶属的一种或多种角色，以及它们隶属的一个或多个组别，对设备的身份进行标识。设备所隶属的角色与 IP 地址或物理位置无关。在大部分结构比较复杂的企业中，这些角色通常包括多个子网和多栋建筑。然后，我们就能根据哪些实体组能与哪些网络资源（包括互联网）进行通信来定义网络分段策略。我们可以根据设备的行为判断设备的受信任程度，并在出现风险因素时再进一步限制对设备的访问。此外，我们还能通过持续的通信监控以及持续的策略改进，不断降低网络中的假设信任，同时强化网络内部的安全。

伴随员工自有设备的剧增，企业网络中的设备数量也相应地增多。从物联网到打印机，从 OT 到医疗设备，支撑企业正常运营的设备比以往任何时候都要更多。正因为如此，由设备所创造的攻击面也比以往任何时候更大。面向办公场所的零信任策略能帮助安全操作人员和网络工程师更好地了解所有主机设备和通信数据，对网络通信实施更严格的限制，并根据信任度执行相应的自适应策略。 然后，我们就能够有效降低这些设备遭恶意活动利用的风险，并针对任何可疑流量做出更及时的响应。

## 办公场所零信任安全成熟度模型

### 第1阶段 构建办公场所信任

搞清楚部署在办公场所中的系统、这些系统的用户及相关应用程序，包括 IoT 和 OT，并确定其在企业组织中的功能及其在网络上的操作。明确零信任安全方案的适用范围。

### 第2阶段 网络可见性

深入洞察办公场所网络环境中用户、设备和应用程序的通信以及网络流量。了解并记录适用范围内的网络功能及要求。

### 第3阶段 网络访问控制

面向适用范围内的用户、设备及应用程序配置并实施网络身份认证和授权。防止任何未经身份认证（并因此不受信任）的实体连接到网络。

### 第4阶段 分段策略

定义基于组的网络策略，确保这些策略仅允许业务运营所必需的网络连接和通信。

### 第5阶段 面向办公场所的零信任安全

企业向零信任安全过渡的最后一个阶段即持续改进。及时根据设备、功能及企业需求的变化，不断调整适用的范围、设备和策略。

## 4.0

# 总结

采用零信任安全解决方案，您的基础设施无需经过整体改造。因为最成功的解决方案应当在混合环境的顶层为其提供支撑，而不是完全取代现有的投资。

跨各种执行点共享与用户、设备和应用程序相关联的身份、漏洞和威胁的动态情景信息，才是协调安全策略的最佳途径。尽管要与整个环境的不同部分协同，必然需要使用不同类型的策略创建和执行方法。

# 思科零信任方法

思科零信任提供了一种综合全面的安全方法，旨在确保面向企业应用程序和网络环境的所有访问，无论来自哪一位用户、哪一台设备、哪一个位置，都安全可靠，从而为企业员工、工作负载和办公场所提供全方位保护。

- **为企业员工提供保护。**思科通过基于 Duo 的零信任员工安全策略，思科就能确保只有合法的用户和安全的设备才能访问应用程序，而无需考虑它们的具体位置。而 AMP（恶意软件防护）则可以持续的对终端设备进行威胁检测和防御，保证信任关系的实时性和持续性。

- **为工作负载提供保护。**思科基于 Tetration，与 ACI 数据中心架构以及 Firepower 结合，提供零信任工作负载安全策略，就能确保企业应用程序内部以及在整个多云环境和数据中心内，所有连接都是安全可信的。而 Stealthwatch/Firepower 在用户数据中心的威胁分析能力，则可以保证实时发现恶意违规流量，从而也保证了信任关系的持续性。

- **为办公场所提供保护。**思科基于 SD-Access 网络架构，与 ISE 深度结合，提供零信任办公场所安全策略，能确保整个网络上所有的用户和设备（包括物联网）连接都是安全可信的。Stealthwatch/Firepower 的威胁分析能力，也可以保证实时发现恶意违规流量，从而保证了信任关系的持续性。

这套完整的零信任安全模型能帮助用户减轻、发现并应对整个网络中的不同风险。

了解有关**思科零信任**的更多信息。