部署零信任策略的五个阶段

简译版

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	The 5 Phases of Zero-Trust Adoption		
原文作者	史蒂夫·莱利（Steve Riley）	**原文发布日期**	2021 年 10 月 11 日
作者简介	史蒂夫·莱利是 Netskope 的首席技术官。		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/endpoint/the-5-phases-of-zero-trust-adoption		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
摘要	零信任策略的主要目标是从“信任，然后验证”转变为“验证，然后信任”。每家公司的零信任之旅都不会完全相同，但零信任的部署通常可以分为五个阶段：（1）不允许匿名访问任何内容；（2）维护显式信任模型；（3）实施隔离以遏制影响范围；（4）持续进行数据保护；（5）通过实时分析和可见性进行优化。		
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。		

部署零信任策略的五个阶段

史蒂夫·莱利

2021 年 10 月 11 日

如今，零信任无处不在。有效的零信任策略旨在通过跨用户、设备、网络、应用程序和数据的显式、持续自适应信任取代隐性信任，以提高整个企业的安全性。

零信任策略的主要目标是从“信任，然后验证”转变为“验证，然后信任”。要实现这一点，应不断评估情境。零信任的第二个目标是假设企业环境可以随时被破坏，然后基于此向后设计。该策略通过消除隐性信任，并根据身份、自适应访问和综合分析持续评估用户和设备的安全性，以降低企业风险并提高敏捷性。

每家公司的零信任之旅都不会完全相同，但零信任策略的部署通常可以分为下述五个阶段。

阶段 1：不允许匿名访问任何内容

首先，企业应对用户角色和访问级别进行分类，清点所有应用程序和数据资产；然后进行身份和访问管理（包括角色和角色成员），识别私有应用程序，清点已批准的“软件即服务” （SaaS）应用程序和网站类别。此外，企业应通过多因子身份鉴别（MFA）和单点登录（SSO），减少横向移动的可能性，保护应用程序不被指纹识别、端口扫描或漏洞探测。

该阶段的具体任务包括：确定身份的真实来源以及他们可能与哪些身份有关联，确定何时需要强身份验证，确定哪些用户有权访问哪些应用程序和服务。企业应构建和维护将用户（包括员工和第三方）映射到应用程序的数据库；及时删除由于角色变更、离职、合同终止等而不再需要的陈旧权限（包括员工和第三方的权限），以限制对应用程序的访问。此外，企业还应通过策略实施点引导所有访问，并删除直接连接。

阶段 2：维护显式信任模型

对应用程序和身份架构有了更好的了解之后，企业就可以进入自适应访问控制阶段了。在该阶段，企业应评估来自应用程序、用户和数据的信号，并实施能够调用身份验证或为用户发出告警的自适应策略。

该阶段的任务是 :确定如何识别设备是内部托管的 ,并为访问策略添加情境信息(阻止、只读或根据各种条件允许特定活动 ）。在高风险的情况下（例如远程访问私有应用程序），可以增加强身份验证的使用；而在低风险低的情况下（例如托管设备访问本地应用程序），可以减少强身份验证的使用。企业应评估用户风险并根据应用程序类别对用户进行分类 ,同时不断调整其策略以符合不断变化的业务需求。此外 ,企业还应为应用程序活动中的授权建立信任基线。

阶段 3：实施隔离以遏制影响范围

用户应尽量减少对风险 Web 资源的直接访问，尤其是当他们同时与托管应用程序交互时。在这方面，按需隔离（即在高风险情况下自动进行的隔离）能够限制受感染用户和危险网站的影响范围。

该阶段的任务是 : 在访问有风险的网站时，自动进行远程浏览器隔离。如果发现行为异常的 SaaS 应用程序 ,应评估是否将远程浏览器隔离作为 CASB 反向代理的替代方案。此外，企业还应监控实时威胁和用户仪表板，以进行 C&C 和异常检测。

阶段 4：持续进行数据保护

接下来 ,企业应了解敏感数据的存储位置和传播范围 ,通过批准和未批准的应用程序和网站来监控和控制敏感信息的移动。

企业必须区分来自托管和非托管设备的数据访问 ,并添加自适应策略的信息 ,以根据情境来确定能够访问的内容（例如，完全访问、敏感或机密）。企业可以通过云安全态势管理来持续评估公有云服务配置，以保护企业数据并满足合规性。此外，企业应评估所有应用程序的内联数据丢失保护（DLP）规则和策略的使用；定义静态数据 DLP 规则和策略（尤其是云存储对象的文件共享权限以及支持数据共享和移动的应用程序-应用程序集成）。除了部署和执行最低权限模型外，企业还应不断进行调查并消除过度信任。

阶段 5：通过实时分析和可见性进行优化

最后一个阶段是实时丰富和完善零信任策略。企业应根据用户趋势、访问异常、应用程序更改以及数据敏感级别的变化，评估现有策略的有效性和适用性。

企业应保持对用户应用程序和服务以及相关风险的可见性。他们还可以获得更高级别的

可见性，以深入了解云和 Web 活动，持续调整/监控数据和威胁策略。此外，企业应确定安全和风险管理计划的关键利益相关者（CISO/CIO、法务部门、CFO、SecOps 人员等），并帮助这些利益相关者实现数据可见性。企业还可以创建可共享的仪表板，以了解不同部门的情况。

2020 年和 2021 年的疫情加速了企业的数字化转型。与此同时，现代数字企业越来越依赖通过互联网交付的应用程序和数据，但这些应用程序和数据在设计时并没有考虑到安全性。很明显，企业需要一种新的安全方法，通过简单、有效的风险管理控制来实现快速、轻松的用户体验。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com