

简译版

实施零信任访问的六个步骤

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	Six steps for implementing zero trust access		
原文作者	Noa Shafir	原文发布日期	2019 年 10 月 18 日
作者简介	Noa Shafir 是 Odo Security 首席产品官。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2019/10/18/implementing-zero-trust-access/		
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		
免责声明	<ul style="list-style-type: none"> 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。 		

实施零信任访问的六个步骤

Noa Shafir

2019 年 10 月 18 日

现代企业不再受固定边界的限制。事实上,在一个用户可以在任何地方使用自己的设备、公司的敏感数据存储多个云服务中的世界里,基于边界的安全模型正在瓦解。

企业不能再依赖“允许‘好人’进来,阻止‘坏人’进来”的二元安全模型。他们面临的挑战是:如何让用户获得所需的访问权限,同时降低设置和维护成本,而且又不损害安全性。

为了应对这一挑战,精明的企业正在放弃传统的“信任但验证”的网络访问方法,转而采用“零信任访问”方法:该方法基于“从不信任,反复验证”的原则。

根据 Forrester Research 公司的研究,零信任架构消除了定义的公司边界内建立可信网络的想法。相反,该公司建议围绕敏感数据资产建立微控制边界。

接下来,我们将介绍实施零信任访问架构的六个步骤。

使用多因子身份鉴别 (MFA)

MFA 是网络安全智能方法的基本组成部分。如果该方法得以正确使用,能够体现零信任的指导原则:“从不信任,反复验证”。

MFA 要求采用两个或多个身份验证因子:知识因子(只有用户知道的内容,例如口令、PIN 码或模式)、拥有因子(只有用户拥有的东西,例如 ATM 卡、智能卡或手机),以及内在因子(生物特征,如指纹、视网膜扫描或人脸扫描)。必须验证每个因子以进行身份鉴别。

验证所有端点设备

攻击者经常利用受感染的机器来破坏公司网络。如果不验证用户的设备,可能会导致灾难。

通过设备验证,企业能够确定试图访问其内部资源的端点是否满足其安全要求。最佳解决方案包括以下功能:跟踪和执行所有设备的状态,轻松管理端点设备的入网和离线。

实施最低权限原则 (PoLP)

每个零信任架构都应该采用 PoLP。PoLP 基于“每个用户只应被授予允许其完成特定任务所需的最低权限”的概念。例如，不应允许应用程序开发人员访问财务记录。

为了实现最大的有效性，PoLP 应该扩展到“即时”访问，即将用户的权限限制到特定的时间段。

监控和审计所有内容

除了身份鉴别和分配权限外，监控和审计网络上的所有用户活动也非常重要。这有助于企业实时识别任何可疑活动。对于有权访问各种敏感数据的管理员账户来说，深度的可见性尤其重要。

采用基于属性的控制措施

这些控制措施将各种属性组合在一起，根据相应策略向用户授予访问权限。这些策略可以组合任意数量的用户属性、资源属性、对象属性等。

这些控制措施可以在整个安全堆栈中运行—从本地到云、到 API、到数据和网络基础设施。它们使网络和安全管理员能够自动执行访问策略，从而实时阻止可疑事件。

涉及整个最终用户社区

实施零信任访问，应倡导全员参与，从所有用户和部门获取信息，以平滑无障碍进行安全策略和安全流程的设置和切换。

实施零信任访问提供了几个重要的安全优势。首先，零信任访问能够连续、主动地管理访问策略，因此能够改进访问控制。其次，零信任访问通过使未经授权的资源无法访问甚至不可见来防止横向攻击，从而减少了企业的攻击面。最后，零信任访问架构通过监控用户活动提高了可见性，这对于事件响应、审计和取证分析至关重要。

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,安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十五亿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>