# 远程办公安全协议的未来

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 future of security protocols for remote work | | |
| **原文作者** | 阿尔莫格·阿皮里翁（Almog Apirion） | **原文发布日期** | 2022 年 1 月 14 日 |
| **作者简介** | 阿尔莫格·阿皮里翁是 Cyolo 公司的首席执行官。 | | |
| **原文发布单位** | Help Net Security | | |
| **原文出处** | https://www.helpnetsecurity.com/2022/01/14/security-protocols-work/ | | |
| **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** | 采用“零信任网络访问”（ZTNA）是提高所有办公环境（无论是远程、混合还是现场）安全性的最有效方法。在零信任访问模型中，没有什么设备、用户或身份是受信任的。相反，访问是基于强身份验证和持续授权的。此外，受监控访问和会话监控等功能能够提供额外的控制和验证层。 | | |
| **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。 | | |

# 远程办公安全协议的未来

阿尔莫格·阿皮里翁

2022 年 1 月 14 日

多年来，网络犯罪一直在迅速增长。新冠疫情的爆发迫使企业迅速转向“居家办公”（WFH），这进一步加剧了网络威胁。在这种情况下，企业开始关注创建可靠的安全协议并与网络安全供应商建立牢固的关系。

## 企业应重新考虑安全标准

WFH 和混合办公模式极大地扩展了攻击者的攻击途径，他们可以利用这些途径访问企业的资源和资产。各行业的企业都应加强其安全标准，这一需求既严峻又紧迫。

不幸的是，很多企业在更新安全协议方面进展缓慢，在实施更改方面就更慢了。不过，既然员工的办公方式和办公地点已经改变，企业的安全实践也必须随之改变。

## 仅采用 VPN 和 VDI 是不够的

如今，大多数企业都使用虚拟专用网（VPN）和虚拟桌面基础架构（VDI）来连接远程办公的员工。但是，多起严重的攻击事件表明，仅采用这些解决方案是不够的，会导致企业存在巨大的安全漏洞。

此外，企业需要注意，大多数 VPN 都被配置为提供“全有”或“全无”访问。虽说管理员可以限制某些用户访问敏感应用程序或资产，但这需要他们进行管理，对大多数管理员来说这根本不实际。这种控制不足和访问过多会导致灾难，尤其是当企业必须将 VPN 权限授予第三方供应商或承包商时。

美国总统拜登的网络安全行政令也指出了 VPN 和 VDI 的缺点，并建议联邦政府转向零信任策略。

## 安全解决方案必须减少人为错误

另一个不容忽视的事实是：“人”（包括最优秀的员工）都会犯错。未考虑人为错误的安全解决方案是不会取得成功的。

举例来说，有时候，开发人员和 IT 人员需要紧急解决生产问题（例如漏洞修复）。如果他们不在办公室，就要从任何可访问的网络（无论是酒店网络或星巴克公共 Wi-Fi）登录企业系统。不可避免地，有的人会忘记退出企业系统，攻击者会抓住这种机会轻松进入企业网络。

## 安全远程办公的未来是零信任

采用“零信任网络访问”（ZTNA）是提高所有办公环境（无论是远程、混合还是现场）安全性的最有效方法。

在零信任访问模型中，没有什么设备、用户或身份是受信任的。相反，访问是基于强身份验证和持续授权的。此外，受监控访问和会话监控等功能能够提供额外的控制和验证层。

那么，企业如何才能从当前的安全方法（很可能是城堡和护城河模型）转变为基于强身份验证和持续授权的零信任框架呢？虽然没有什么简单的方法能够迅速迁移到零信任模型，但是采用该模型也不像许多人担心的那样困难或耗时。如果企业选择能够在整个过程中为他们提供支持的供应商，就能少走很多弯路，并且能够更快地实现投资回报。

## 实施分段访问能够最大程度地减少安全漏洞

企业应识别最易受攻击的访问点并保护这些访问点，这一点至关重要。例如，与其向第三方供应商授予完整的 VPN 访问权限，不如向这些潜在风险用户授予对企业部分（微分段）网络的访问权限。在 WFH 模式下，这种策略能够把意外用户错误安全漏洞的风险降至最低。

## 零信任的未来是光明的

很多现实案例说明零信任方法有明显的优势。例如，Colonial Pipeline 通过采用零信任访问策略，防止了数百万美元的损失。即使攻击者进入了 Colonial Pipeline 的核心系统，零信任访问的身份鉴别和验证也能够防止他们造成持久的损害。在最近的案例中，零信任模型拒绝了未经授权的用户访问关键应用程序，从而防止了攻击者利用新发现的 Log4j 漏洞。

总体而言，越来越多的企业开始采用零信任访问策略，这有助于减少重大安全事件的发生。此外，将人工智能集成到这些新系统中可以帮助企业识别和弥补安全漏洞，而且无需人工干预。

# 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