SOPHOS
Cybersecurity delivered.

为什么 ZTNA 重要：安全网络的未来

ZTNA 保护远程访问安全，抵御勒索软件

Sophos 白皮书。2022 年 2 月

在网络安全方面，一切归结于风险和信任。您信任刚刚登录网络的用户吗，或者尝试访问企业应用程序的人？电子邮件看起来来自您的企业合作伙伴，但包含看起来异常的请求，可能指示企业电子邮件攻破攻击。信任但检验在上世纪 80 年代成为一句流行的口号，但现在重心已经转向“不信任一切，检验一切”。

零信任模型要求必须对网络上的每个人进行身份验证以获得访问权，但这不是全部。任何访问网络资源（如服务器、应用程序或数据）要求还必须验证用于访问资源的设备或应用程序的合规性，然后每次提出新请求时重新验证身份和验证。

从网络安全角度，信任是赢得的，而不是给予的。每次用户、设备和应用程序尝试在网络上操作时，必须再次运行身份验证过程。

什么是 ZTNA？

零信任网络访问 (ZTNA) 基于零信任原则，即“不信任一切，检验一切”。这样可以像自己的网络微分区上的自己的屏障一样有效对待每个用户、设备和应用程序，不断评估和验证身份与运行状况，获得企业应用程序和数据的访问权，从而明显改善安全性。用户只能访问其政策明确允许定义的应用程序和数据，减少横向移动以及相关风险。

勒索软件受害者明显更加熟悉 ZTNA 方法，很可能是在防御后续攻击的渴望驱使之下。我们将在本文稍后部分深入研究，了解 Sophos 用户如何查看和使用 ZTNA 技术。

ZTNA 是安全访问服务边缘 (SASE) 安全框架的一个基础部分，介绍网络和云安全如何汇聚到一个云平台中。SASE 最早在 2019 年由 Gartner 推出，大体上是利用云原生架构合并传统广域网 (WAN) 管理和安全功能。除了 ZTNA，SASE 架构还包含云访问安全代理、防火墙即服务、入侵防御系统和安全访问网关。

云管理提供巨大的优势，能够即可上线并运行，减少管理基础设施，部署和注册，支持在任何地方访问。云管理的一个重要优势是能够即可登录并开始，无需添加额外管理服务器或基础设施。云管理还支持在任何设备从任何位置即时安全访问，支持您需要的工作方式。方便世界各地的新用户注册。

但实施 ZTNA 是为远程用户改进安全，在疫情推动下远程用户网络重大安全升级，以及保护企业网络防范恶意软件和勒索软件攻击的关键部分。

消解 VPN 威胁

就像疫情给人类带来的恐怖一样，改进远程访问一直是一个意外而显著的优势：部署 ZTNA 作为有漏洞的 VPN 的替代。疫情迫使数以百万的员工离开企业网络的友好边界，转为在家办公，产生数以百万的存在漏洞的新端点，往往位于企业 IT 人员的控制之外。

这些端点对攻击者来说充满诱惑力，因为很大一部分可能还没有企业级端点防护。此外，数以百万的新远程用户给企业 VPN 带来巨大负担，后者可能还没有经受过如此重压力的挑战。

ZTNA 以零信任原则为基础，代替存在问题的 VPN（将远程用户连接到企业网络的传统方法）。从技术上来说，VPN 对于现在大部分远程办公人员有三个重大缺陷。

首先，VPN 设计无法缩放，以满足随着大型企业远程员工数量大幅增加带来的需求。其次，VPN 客户端软件往往老旧、疏忽和复杂，成为攻击者的潜在目标。VPN 还往往存在安全漏洞，因为设计采用传统用户名/密码的安全方法。最后，使用 VPN 访问网络的用户在连接后事实上进入了网络，非常类似外围防火墙内的工作站。根据内部网络控制，这可能存在问题。

我们来研究每个问题，看看 ZTNA 如何解决这些问题。

VPN 不能很好地缩放。限制包括 VPN 最大带宽（通常限制为 1Gbps），可被漏洞攻击的暴露端口，潜在中间人攻击，以及过高权限访问。此外，VPN 设计为 VPN 用户从远程用户处理的特定数据量，无法动态缩放。如果数据量过高，例如，一些用户在其他用户掉线前无法访问 VPN。

其次，美国国家安全局多年来在多次网络咨询中提到 VPN 漏洞，2019 年，加拿大网络安全中心发布指南，指出 3 个常用 VPN 产品存在多个发现恶意行为隐患的迹象。这些包括凭据重置以及存在漏洞的专有 SSL 和 TLS VPN 协议。

最后，VPN 在用户断开网络时不提供过滤。基本上用户具有的所有权限就像在企业防火墙背后的工作站一样。

可以通过两种方式，减少远程访问工具为攻击者提供在网络中移动能力的威胁：首先，要求每次进入网络时，仅对网络的一个特定微分区验证用户、设备和软件身份。即使攻击者成功获得访问权，移动仍然受到限制。其次，大幅限制网络上任何人的权限。如果攻击者因为权限受限而看不到网络，则无法在网络中移动。

根据 The Forrester NewWave：2021 年第 3 季度的 Zero Trust Network Access，“利用 ZTNA，用户可以利用零信任原则访问本地应用程序，同时运行双向视频会议流量直接进入互联网，从而改善安全状态和员工体验”，报道称。“最终 ZTNA 减少员工 VPN 的需求，让基础设施和安全团队采纳云联网和安全方法。”

ZTNA 的奥秘

从企业治理角度出发，管理网络上的用户和他们的操作是重要企业顾虑。采取决定公司如何运营的策略和程序，以及带来经济可行性的可靠道德业务做法，是企业治理职能的目的。坏人可能在网络上游荡，威胁或盗取保密数据，安装勒索软件和其他恶意软件程序，或者在隐秘模式下等待更好的攻击机会。这不仅违反合规性法规，给公司带来高额经济损失，而且大幅降低公司的市值。

部署普遍的和 ZTNA 特定的零信任网络模型不仅可以识别网络上的入侵者、恶意和好意应用程序以及不属于的用户，而且大幅减小企业网络的攻击面，从而改善公司的整体风险状况。

当用户访问配备 ZTNA 的企业网络时，设备访问自己微分区外围上的网络资源，始终进行身份验证和检查。利用零信任，用户不再处于具有通常所有暗含信任和访问权的“企业网络”上。他们只能访问他们及其设备身份验证过的网络部分。传统 VPN 连接则并不如此。

在传统网络中，企业防火墙将攻击者隔离在外，接受用户凭据后只有很少防御，攻击者可以自由移动，查找提升凭据，允许其访问更安全的网络部分，寻找可以盗窃、复制、破坏或加密勒索的数据。

实施零信任基础设施不仅让凭据盗窃的价值降低，而且企业防火墙成为数据和应用程序的众多防御中的第一道防御。即使在家办公员工的计算机被攻破，在攻击者访问更大的企业网络时用户凭据也不足。

ZTNA 访问仅提供有限网络部分的访问权。这假定他们具有为批准应用程序或数据验证自身、设备和软件身份的凭据。

克服勒索软件

根据 Sophos 的 2021 勒索软件现状报告，37% 的受访者在去年遭遇勒索软件攻击，其中 54% 表示网络罪犯成功加密其数据。从数据丢失角度来说，好消息是 96% 的受访者表示至少找回部分数据。但是，坏消息是支付赎金很少找回全部数据：支付赎金后，平均仅恢复 65% 的加密数据。

报告提到，2020 年中型企业支付的平均赎金为 170,404 美元。但是，这只是整体补救费用的一部分。弥补最近勒索软件攻击造成影响的平均成本（包括停工、人力时间、设备成本、网络成本、失去机会、支付赎金和其他成本）为 185 万美元，超过 2020 年报道的 761,106 美元的两倍。

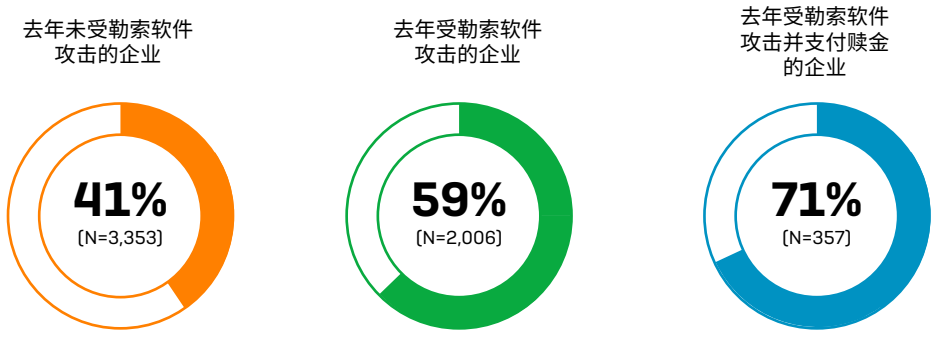
在 Vanson Bourne 开展并由 Sophos 签署的最近一项对全球 5,400 名 IT 专业人员的调查中，20% 的受访者表示已经采取零信任方法，41% 表示已经开始实施零信任，预计在 2022 年初完成。另外 20% 表示预计在 2023 年初完成。

ZTNA 解决方案消除勒索软件和其他网络渗透攻击的一个常见攻击渠道。由于 ZTNA 用户不再“位于网络上”，而是企业网络的微分区上，可能通过 VPN 进入的威胁在 ZTNA 下将无处立足。

勒索软件攻击推动 ZTNA 采用

调查显示，相比去年没有遇到过勒索软件攻击的企业，去年受到勒索软件攻击的企业 IT 专业人员对 ZTNA 方法“非常熟悉”的数量几乎多 50% (59% vs 39%)。在受到攻击并支付赎金的企业中达到 71%。

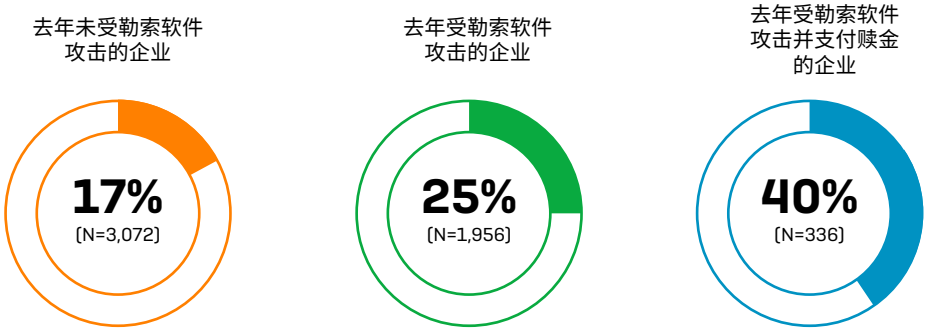
认为自己“非常熟悉”零信任网络访问 (ZTNA) 方法的受访者比例



进一步证明这一观点的是，只有 10% 的勒索软件受害者不熟悉或几乎不熟悉 ZTNA，而没有成为过受害者的企业则为 21%。

调查还显示，勒索软件受害者在零信任采纳中更加主动。去年遇到勒索软件攻击的企业中，四分之一 (25%) 已经完全采用零信任方法，而受到攻击并支付赎金的企业上升到 40%。相比之下，没有遇到过攻击的企业只有六分之一 (17%) 已经完全迁移到该方法。

已经采用零信任方法的企业受访者比例



此外，勒索软件受害者对采纳 ZTNA 具有不同的动机。

- 受访者被问及采纳零信任方法的动机，包括多个共同点和一些明显差异。“改善整体网络安全状态”是受害者和非受害者最共同的动机
- 勒索软件受害者第二个最共同的动机是渴望“简化网络安全操作”(43%)，可能反映复杂安全导致了以前的攻击。
- 勒索软件受害者明显更有可能说出，“从 CAPEX 转向 OPEX 模型”是采纳零信任方法背后的主要因素之一 (27% vs. 16%，在受到勒索软件攻击并支付赎金的受害者中上升到 34%)
- 勒索软件受害者还受到“支持转移以增加云的使用”的激励 (42%)。在最近没有遇到过攻击的企业中降至 30%

展望

可能很难向高管和股东解释零信任环境的优势，要证明攻击失败或者从而发生是有难度的，因为攻击者在投放恶意软件之前已经被阻止。也就是说，可以证明零信任显著降低风险，而降低风险可以为企业带来经济效益。

例如，降低企业风险可以降低网络保险保费，带来更好的条款，有可能提高公司价值。网络保险公司和承销商认可，更低的风险带来的索赔更少，保险赔付更低更少。因此，网络保险行业目前正在重新评估，修改其条款以编写此类保单，为主动降低风险的公司提供更好的条款。

在 2021 年 5 月 Joseph Biden 总统签署的关于改善美国网络安全的总统行政命令中，联邦政府“必须采纳安全最佳做法 [和] 向零信任架构推进…”。一国总统采纳零信任模型凸显了该方法被视为降低风险的阳光大道的认可。

Gartner 认同零信任是未来的网络安全路径。“无论是正在进行中的大型企业，还是刚刚开始的企业，保护数据都是一项头等大事”，公司表示。据 Gartner 称，82% 的公司计划让员工远程办公一段时间。“随着公司开始将远程办公人员加入长期计划，安全性已经成为一项优先要务。但是，许多公司刚刚开始意识到，他们的传统安全方法不适合云原生远程办公人员”，Gartner 称。

Forrester 也表示认可，提到零信任保护资源而不是物理网络的安全。“按照最简单的形式，零信任模型将焦点从各种身份验证和访问控制，转向对敏感数据存储、应用程序和网络的跟踪控制”，Forrester 表示。“这些控制利用身份，根据定义的角色启用/禁用用户和代理访问权。”

如果未来是零信任，首先将是控制网络上的人，他们可以访问的内容以及访问方式。这就是 ZTNA 的本质，所以对于网络安全的未来至关重要。

了解更多
www.sophos.cn/ztna

中国（大陆地区）销售咨询
电子邮件: salescn@sophos.com

22-02-06 ZHCN (MP)