SOPHOS

揭开零信任的神秘外衣

企业网络和单一安全外围即将退出历史舞台。越来越多的用户远程办公，在公共互联网上进行自己的工作。软件即服务 (SaaS) 应用程序、云平台和其他云服务的发展，使得网络作为主要措施保护资源安全的效果逐渐下降。随着网络之间界限的模糊化，我们再也无法依赖单一而封闭的企业网络，给予网络内的所有系统信任。

进入零信任 (zero trust) 时代；这是一种关于如何看待安全和如何实现安全的网络安全理念。零信任给予“不信任一切，检验一切”的原则，着眼于物理和数字方式保护资源，默认不信任任何内容。

任何一个供应商、产品或技术都无法带给您零信任。这需要观念的转变，以及大量改变资源安全保证定式的不同解决方案。

本白皮书探讨零信任概念，实施零信任模型的好处，并指导企业向零信任过渡需要采取的措施。

时代已经变了

信任在信息技术领域是一个危险的词语，尤其是绝对信任 – 即无条件或不容置疑时。

建立一个庞大而隔离的企业网络安全外围，并信任内部的所有内容，经过时间证明是一种存在缺陷的设计。这种不够健全且责任不清的网络中心是黑客梦想中的目标。一旦黑客进入网络，往往不被发现。在网络中传播，访问重要系统，以及其他许多操作简直易如反掌，因为只有外围具有安全控制和最强的检查机制。

无论您喜欢与否，外围的作用已经大幅削弱。

用户希望在不受信任的网络远程办公，如咖啡店的公共 Wi-Fi。他们希望在云端存储数据，这样可以在需要时随时访问。他们希望使用自己的个人设备访问企业数据和资源。我们的用户需要轻松访问，这样他们可以随时随地，按照想要的方式办公。

软件即服务 (SaaS) 应用程序、云平台及其他云服务的运用，将数据留在企业外围之外，公共云平台意味着许多过去在企业外围内运行的设备或服务现在在外围之外运行。我们的工作正在从我们所拥有、控制并信任的网络，向提供最经济处理方式的地方转移。

一切无处不在。旧的“企业网络”模型采用静态防御方法，无法支持企业在采用云功能的同时，保护他们的数据、用户和客户，因此需要改变固有观念。

进入零信任时代

零信任是一种解决企业工作方式中这些威胁和改变的全盘方法，这是与安全思维和执行方式有关的模型和理念。

不应自动信任任何人或任何事，无论是企业网络内外，甚至是企业网络本身。视网络位置的绝对信任以及如传统防火墙等静态防御措施，必须加以限制。

虽然最终需要信任某些内容，但在零信任时代，这种信任是临时的，根据多个数据来源（超过过去我们用过的数量）动态建立的，不断重新评估的。数据来源包括访问请求本身的相关信息、用户信息、系统信息、访问要求信息和威胁情报。此外，仅在需要时按连接授予数据和/或资源的访问权。

我们在每天使用互联网的过程中，对于不受信任的网络有着丰富的经验。面对公共互联网的计算机与传统外围内的计算机采用差异巨大的方式保护安全，需要额外审查和防御层以保护不受外部威胁影响。

零信任模型指导您将所有设备作为面对互联网的设备对待，不能仅仅设置一个外围，而是必须建立多个微外围（或微分段），对于所有内容以及内容之间的联系进行检查和控制。

采用零信任的核心好处

采用零信任模型带来许多好处，因此，为了让您的生活更轻松，我们选取了一些核心好处。

对整个 IT 资产的控制

从办公室内一直到您使用的云平台。不再缺乏对企业外围以外的控制，也不再出现远程用户的窘迫。

采用相同方式管理和保护所有用户的安全

再也不用查看企业外围内外的信息，您可以采用相同方式处理所有用户。这样简化 IT 安全，同时确保公平对待所有设备和用户。

即使您不拥有/完全控制使用的基础设置，也能保持安全

利用身份、位置、设备运行状况、MFA 和覆盖监测与分析，您仍可以在任何类型环境、平台或服务上实现强大的安全。

显著减少恶意软件或攻击者的活动

攻击者在进入网络后再也不能在整个网络内肆意妄为，只能访问受威胁用户可以访问的最少数量系统。不继续信任已验证身份的用户，在系统之间进行检查，进一步限制传播扩散。

零信任总结

零信任是一个宏观概念，人们对此开展了大量讨论。基本上我们可以将零信任的主要概念提炼为几句您应该牢记的口诀。

网络没有“内部”

假设您正从不受信任的位置，如咖啡店的公共 Wi-Fi，运转整个企业，您的所有设备直接连接所有网络中最危险的一种：公共互联网。想象这是您的现实情况，您无法采用依靠躲在传统企业外围背后的方法实现安全。

对于管理和内部系统来说始终存在企业“信任”的网络，但目的是通过应用程序代理和其他技术让普通用户远离这些网络，显著减少攻击面。

不信任一切，检验一切

假设您的网络内部和外部都有攻击者，他们一直在不断进行攻击。不应信任任何用户或设备，应该先验证身份，然后才可以考虑连接。想象您正受到各个方面的不断攻击，您必须为资源建立可靠的身份验证和授权机制，划分防御层次，不断监测和分析资产内发生的所有活动。

安全应该能够实时调整

用于实现零信任的安全政策应该是动态的，根据尽可能多的数据来源，尽可能多的不同技术带来的信息自动变化。如果用户使用时设备被攻破，类似“此用户”或“此设备”可以访问“此内容”的静态证策无法保护您。如果您的政策还考虑设备运行状况，如恶意行为标识，那么可以将其用于动态适应，无需管理员干预。

长期以来，Sophos 的网络安全策略和理念一直包含这一点。您可能知道 Synchronized Security 同步安全，我们的产品可以借助这个功能互相分享彼此的独有信息，这样可以实现动态自适应政策，充分利用这些信息使政策不再静态化和被人轻松绕过。

基本上这就是您可能正在执行的良好安全政策和最佳做法，如果您为 GDPR 做好了准备，那么您已经完成其中很多工作。

零信任原则

不信任一切。绝不。不信任一切，意味着只要存在风险，就必须寻找相关安全对策。

验证一切。不要假定通过检查就能带来信任。拥有凭据并不意味着您值得信任，仅仅说明您有凭据，而凭据可能被盗。

我们划分了四个需要记住的简单原则。

始终确定身份

您需要单一权威的身份来源，用于所有单点登录 (SSO) 的场合。应该采用多重形式身份验证 (MFA) 验证一切内容的身份。无论用户在哪里，尝试访问什么内容，验证他们的凭据，验证他们的第二（或第三）重形式，定期要求重新身份验证。

如果凭据被盗或者系统被劫持，MFA 和定期重新身份验证将快速阻止攻击者。

始终控制

在需要时应用控制和检查，采用并实施最低权限原则 – 用户应只能访问其工作需要的最低程度资源。例如，只能由德国员工使用人力资源系统，则只有德国员工可以具有访问权。任何其他人都不得具有访问权，即使具有该访问权的风险低。

始终分析

仅仅因为身份验证成功，或者授予该用户或设备访问权，不意味着可以信任。内部人员威胁和恶意行为者可以获取有效凭据。记录所有网络和系统活动，定期分析并检查，以检验身份验证后发生的情况。SIEM（安全信息与事件管理）、EDR（端点检测与响应）以及 MDR（托管式检测与响应）因这个需求而问世。

始终保护安全

采用“由内到外”的网络安全方法。您应重点关注重要数据，将方法由内到外推广，从数据生成到销毁，找出数据在网络中的流动路径中的漏洞点。

始终首先考虑风险，而不是合规性或法规。纯粹为了满足合规性检查或法规要求而应用安全措施是一种危险做法。合规性要求不知道您网络的具体情况，流动路线和工作负荷，系统和技术，不知道网络每个可能要素的相关风险。考虑风险并建模企业面临的威胁，将确保您了解哪些地方需要加强安全措施，哪些地方应该建立微分段。

向零信任过渡

那么，如何向零信任过渡，发挥其全部优点？

定义您的攻击面，确定资源

首先，您需要定义希望保护安全、控制和监测的表面。您的企业使用哪些资源、服务、应用程序和设备?透彻了解整个网络内使用的所有内容，有助于接下来采取新的零信任思路。

制定标准和需要权限的路线

研究完所有内容后，您需要制定标准路线 – 内容之间的哪些流程、行为和关系是标准的，预计的?这组用户将访问此应用程序，这个设备将连接那个网络，这个服务使用数据存储区等，以及哪些是需要权限的路线?这个管理员将希望连接此管理控制台，使用远程桌面协议 (RDP) 访问保存敏感数据的那个服务器，等等。需要权限的路线几乎肯定需要应用额外安全或控制。

设计零信任网络

现在您知道了网络范围有哪些内容，内容之间的关系，可以开始应用零信任理念。确定要应用的安全措施和访问权控制，应用位置，哪些技术能够最好地减轻哪些风险，等等。

创建零信任政策

接下来，您需要实施零信任政策，利用尽可能多的不同数据来源，取得任何连接或请求的相关信息。

监测并维护外围

最后，也许是最重要的，您需要对所有内容加入详细监测，这样可以维护新建立的外围。

这是管理员面对的最大变化之一。在您可以安装和配置防病毒功能，从不查看控制台的地方，采用零信任以后，您需要改变习惯。

您需要监测发生的事件，利用 EDR 等工具了解威胁如何进入环境的根本原因，发现前或潜在攻破后发生了哪些事件。

MDR 等服务在这里非常有用，支持网络安全专家协助您监测网络，代替您消除威胁。

零信任技术组合

保护网络上所有资源和资产的安全需要用到大量技术。任何一个供应商、产品或技术都无法解决所有问题。

零信任技术组合需要解决两个主要方面 – 零信任的管理，各种资源和资产的安全与控制。

管理分为三个子方面：

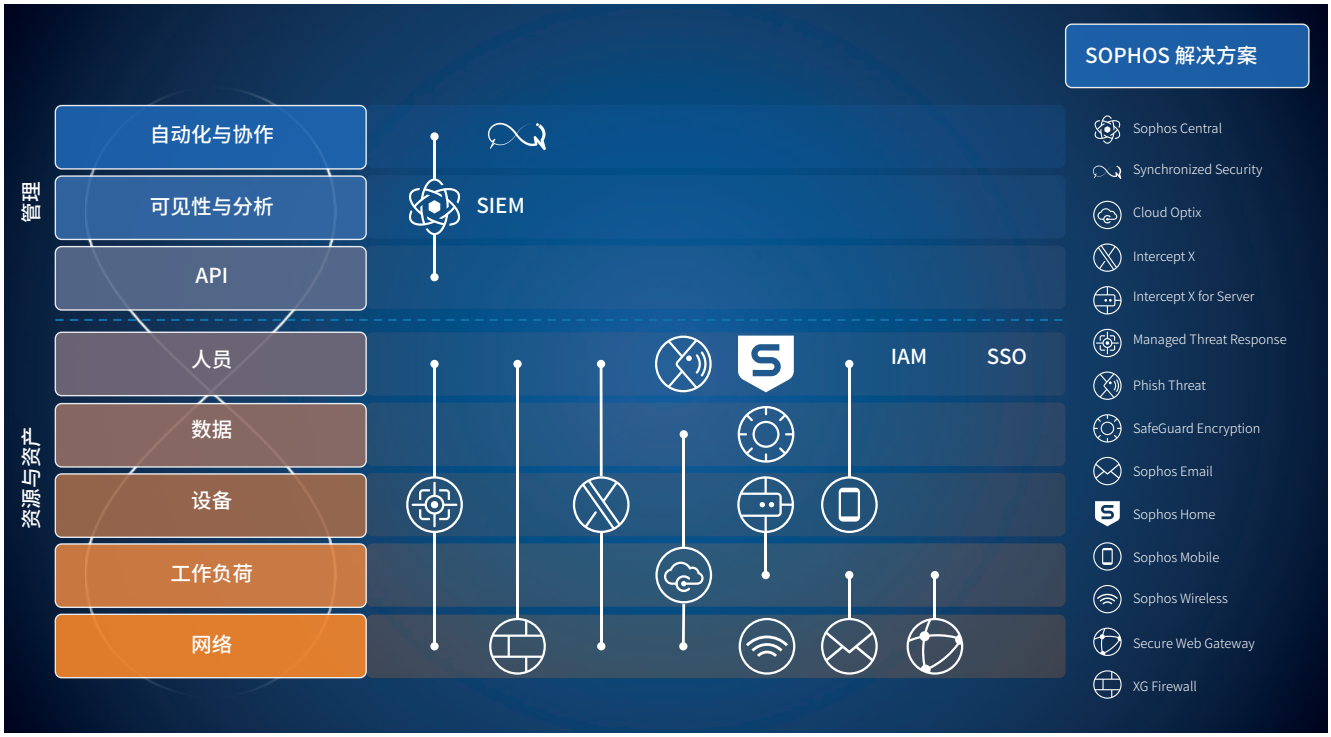
1. 自动化与协作 – 用于定义动态政策，协调所有不同技术，有序安排一切
2. 可见性与分析 – 用于维持对网络的监督，确保一切工作正常，发现是否或何时发生威胁和攻破
3. API – 用于整合各种技术，将数据从一个系统导入另一个系统

资源和资产分为五个子方面：

1. 人员 – 为您的企业工作或与您的企业合作的用户、管理员等
2. 数据 – 所有企业的生命线，可能是需要保护的最重要资产
3. 设备 – 用于开展业务的服务器、笔记本电脑、虚拟机等
4. 工作负荷 – 用于处理数据、执行计算、生成报告等的服务和应用程序
5. 网络 – 数据流动的通信渠道，Web、电子邮件、Wi-Fi、互联网等

Sophos 可以帮助做什么

由于一个供应商无法将您的企业改造为零信任模式，Sophos 提供了大量技术帮助您实现这一目标。



管理零信任

Sophos Central 是我们的云原生网络安全平台，支持您管理零信任环境，可以在一个控制台协同我们的所有技术，为您从一个位置提供对所有技术的监督，以及连接您使用的任何其他第三方技术的 API。

您还可以考虑 SIEM，聚合非 Sophos 和 Sophos 产品的日志，更加方便您全面了解发生的任何情况。我们的 API 能够轻松获取 Sophos Central 平台以及您使用的任何 SIEM 的信息。

Sophos Synchronized Security（通过 Sophos Central 控制）在这里也起到重要作用。启用 Synchronized Security 后，Sophos 解决方案彼此共享信息，自动响应事件。在零信任环境中，解决方案能够通过动态政策适应场景，自动执行复杂任务，如隔离计算机等。

资源和资产的安全与控制

我们许多产品可以同时帮助您保护多个资源和资产的安全，但这并不意味着您仅采用一种技术就可以不用理会了。例如，作为弹性零信任架构网络的一部分，保护人员安全需要大量不同技术。

Cloud Optix 提供必要的持续分析和可见性功能，检测、响应并避免令企业暴露的安全与合规性漏洞。在零信任环境中，Cloud Optix 有助于保护公共云内部、数据、设备、工作负荷和网络安全。

Intercept X 提供无人能及的端点防护，通过深度学习恶意软件检测、漏洞利用攻击阻止、行为检测和防勒索软件等独特组合功能，阻止最广泛的攻击。在零信任环境中，Intercept X 有助于保护所有资源和资产的安全。

Intercept X for Server 设计用于保护云、现场或混合服务器环境安全。在零信任环境中，Intercept X for Server 有助于保护您的设备和工作负荷安全。

Managed Threat Response (MTR) 是我们的专家主持的威胁响应解决方案，将机器学习技术与人工智能融合在一起，提供 24/7 全天候威胁追踪、检测和响应功能。在零信任环境中，MTR 有助于保护所有资源和资产的安全。

Phish Threat 是我们专门的防网络钓鱼解决方案，为您的员工提供安全意识培训，并附带大量报告，帮助您衡量企业的网络钓鱼威胁应对水平。在零信任环境中，Phish Threat 有助于保护人员安全。

SafeGuard Encryption 在内容创建后即进行加密，通过持续验证用户、应用程序和设备安全完整性，然后允许访问加密数据，主动保护您的数据，从而在零信任环境中帮助保护数据安全。

Secure Web Gateway 有助于实现高级 Web 防护，提供前所未有的 Web 安全、控制和信息。在零信任环境中，Secure Web Gateway 有助于保护网络和工作负荷安全。

Sophos Email 利用人工智能提供更智能的预测电子邮件安全。在零信任环境中，Sophos Email 有助于保护网络和工作负荷安全。

Sophos Home 设计用于保护家庭计算机，采用和多个企业级产品相同的技术。在零信任环境中，Sophos Home 有助于保护人员安全。

Sophos Mobile 是我们的安全统一端点管理 (UEM) 解决方案，帮助企业用更少时间和精力管理并保护传统和移动端点安全。在零信任环境中，Sophos Mobile 有助于保护您的设备、数据和人员安全。

Sophos Wireless 提供简单有效的管理和保护无线网络安全的方式。在零信任环境中，Sophos Wireless 有助于保护网络安全。

XG Firewall 提供综合下一代防火墙保护，暴露隐藏风险，阻止未知威胁，自动响应事件。在零信任环境中，XG Firewall 有助于保护所有资源和资产的安全。

采用这些技术有利于您向零信任模型过渡。但是，正如前文所说的，包括 Sophos 在内，任何一个供应商或技术，都无法让您过渡到零信任环境。要支持用户随时随地使用云服务，您还需要强身份访问管理 (IAM) 解决方案和单点登录 (SSO)，对所有系统和服务运用单个权威身份来源 – 这是零信任的关键。

您可以访问www.sophos.com，更多了解我们的产品和服务，并观看在线视频。

我们的网络安全远景

零信任和我们的网络安全远景 Synchronized Security 同步安全具有许多相同的目标，彼此互补。

Synchronized Security 是网络安全即系统。持续分析、调整并自动完成最复杂的 IT 任务，同时动态实时监测所有系统活动、用户行为、网络流量和合规性状态。所有技术彼此共享信息，互相提供处于单独一方盲点的信息和可见性。

技术应该互相沟通。只有通过这种沟通，才能实现我们需要的自适应动态政策，根据多个数据来源实现零信任网络。

结束语

正如前文提到的，零信任是一种很少人能够轻易接受的网络安全理念。但是，随着安全外围作用的不断削弱，将越来越需要采用零信任方法。网络罪犯在不断创新，防御技术必须努力跟上他们的脚步。零信任模型提供一种真正能够始终减小威胁，同时树立网络安全方案新标准的方式。

是时候采用不同思维方式了。是时候进化了。

中国（大陆地区）销售咨询
电子邮件：salescn@sophos.com

20-03-10 WP-ZHCN (DD)

SOPHOS