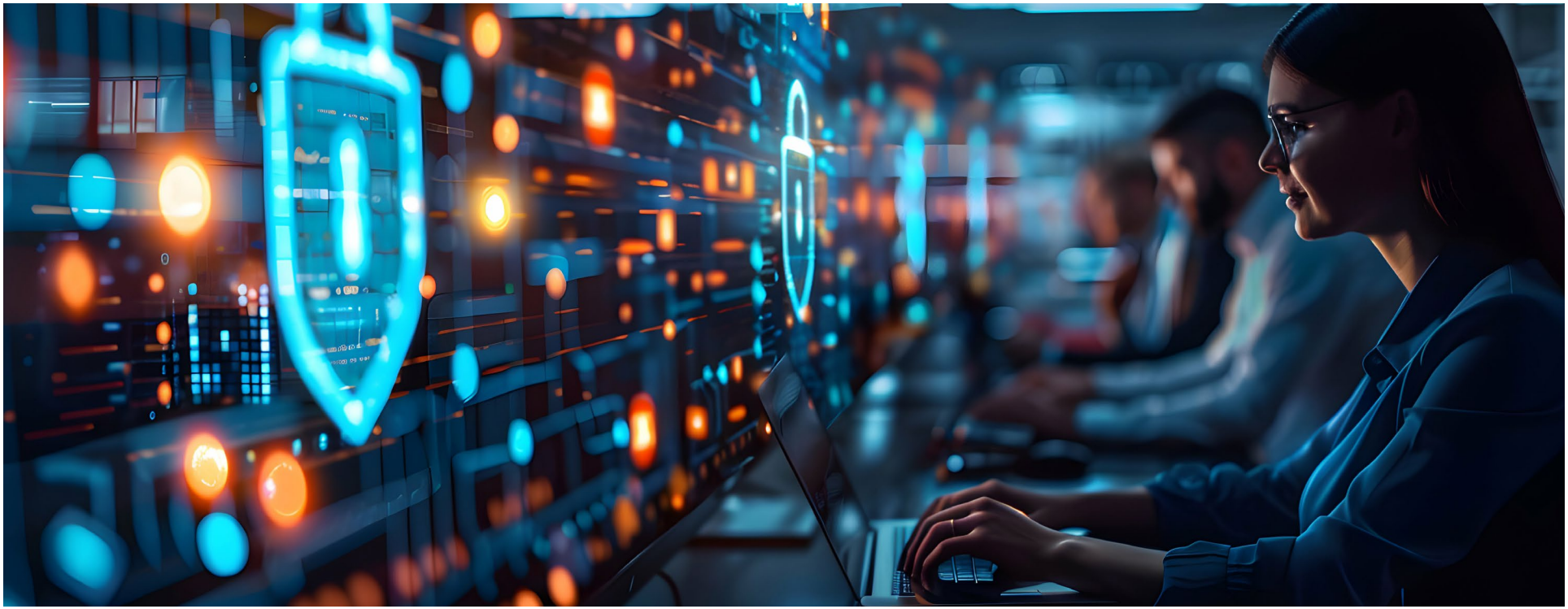
一致性与协作如何推动行业领先的网络安全发展

确保从客户端边缘到数据中心应用实现固若金汤的安全性



目录

安全始于边缘

从根本上讲，安全效力的衡量标准可以简单理解为安全功能在预防、检测和应对威胁方面的表现。

在典型环境中，安全始于客户端边缘的最终用户。这里的边缘是指员工使用设备并访问企业资源的位置。如果这一层的安全防护薄弱，所产生的影响便会层层递进，使数据中心最敏感的 IP 面临风险。

因此，“安全始于边缘”的理念不容小觑。

例如，一名员工打开了一封看似无害但实则含有恶意附件的电子邮件。如果终端设备缺乏足够的安全控制措施，就可能会导致安全漏洞，不仅危及用户设备的安全，还可能对整个网络构成潜在威胁。一时的判断失误可能会对业务造成持久的影响。

因此，现代组织必须采取整体式安全方法，确保从客户端边缘到数据中心应用的每一个组件都能得到主动强化，从而抵御威胁。减轻威胁的最佳方法是在威胁开始之前就加以阻止。

瞻博网络可以大幅减少漏洞，同时简化网络和安全管理。

了解具体做法 →

主要安全趋势

面对日益复杂的网络威胁，企业需要能够利用最新安全技术提供全面保护，同时又不影响网络性能的解决方案。

01 AI 增强型网络安全

当今的数字世界充斥着各种高级威胁，演变速度之快令传统安全措施应接不暇。人工智能 (AI) 将大量数据转化为具指导作用的洞察，可在异常行为和潜在风险对网络造成影响之前，快速、准确地主动加以识别。

02 安全接入服务边缘 (SASE)

随着企业采用云并在移动终端上远程办公，传统的网络边界已经非常模糊。SASE 是一种能够将网络连接和安全功能整合到单一云交付服务中的网络架构。

03 零信任安全性

在当今这个互联互通的数字时代，传统的安全边界已经消融。零信任会假定存在漏洞并验证每个访问请求，无论其来自何处，从而确保只有经过授权的用户和设备才能进入您的网络。

03 挫折无处不在

延迟带来的挫败感无所不在

网络架构的飞速发展开启了员工队伍分散、云托管应用以及各种设备之间高度连接的时代。

这种新格局会导致攻击面增大，需要采取更加弹性、智能和可调整的安全措施。

那么，为什么如今走进几乎任何一个网络团队时，都会感受到空气中弥漫着一种挥之不去的挫折感呢？

原来，这些额外的安全措施导致网络基础架构饱受延迟问题的困扰。您所依靠的网络俨然成为了用户不便的来源。此外，故障排除既耗时又需要人工操作，团队需要在孤立的系统和零散的数据中不停摸索，才能找出问题症结并有效加以解决。

更糟糕的是，网络团队与安全团队相互指责和推卸责任的风气盛行，让彼此间产生了嫌隙并阻碍了协作。

这些现实情况使得提供用户所需的快速、无缝体验变得极具挑战性。网络的安全性和复杂性越高，性能就越容易受到影响，从而导致用户和运维人员饱受挫折并产生怀疑。

73%

的组织表示，与两年前相比，他们的网络环境已经开始变得复杂，甚至非常复杂[1]

Enterprise Strategy Group

04 通过协作消除困惑

通过协作消除困惑的好处令人难以抗拒

从过往经验来看，网络和安全团队往往各自为政，而不是团结协作。

网络团队关注的重点始终是保持最佳连接和性能，而安全团队的重点则是保护这些连接、应用以及在其中穿梭的敏感数据。

这一现实情况很容易导致混乱、相互指责，并且最终产生漏洞。当发生安全事件时，很可能会快速发展成双方互相指责，网络团队认为安全团队做得不够，安全团队则认为是网络团队留下了安全漏洞……并且周而复始。

这种各自为政的局面会对安全态势造成极大的损害。

通过制定网络团队与安全团队通力合作的前瞻性威胁检测和快速事件响应程序，您可以帮助确保在出现网络或安全相关问题时能够进行实时沟通和协作，并做出明智的决策。

促进网络团队与安全团队协作所带来的运维效益不可估量。采用统一的方法，不仅能提高安全效率，还能简化运维，并有助于确保网络以最佳水平持续运行。两个团队能够更加有效且高效地展开协作，而不是重复执行流程，也不会因沟通不畅而导致网络中断或安全疏漏。这是一种双赢的局面。

64%

的受访者表示，他们的组织将在未来 24 个月内积极推动网络团队与安全团队的统一协作[2]

Enterprise Strategy Group

05 通过一致性消除混乱

遏制网络犯罪的策略途径

确保在网络层和应用层实施一致的安全策略至关重要。

如果没有统一的安全策略，组织就需要努力应对网络犯罪分子急于利用的安全漏洞。

假设有一项策略强制规定每台设备必须具备某些安全功能，比如加密和健全的身份验证协议。如果贯彻执行这一策略，便可构建一个强大的框架，不仅能在各个层面保护数据，还能向网络团队和安全团队阐明期望。

当大家意见一致时，出现误解和不一致的可能性就会降低，从而营造一个更加安全的环境。

这就需要一款安全策略引擎，用于横跨网络供应商的整个产品组合增强网络安全性。换句话说，从客户端边缘到数据中心，所有平台和所有位置均适用之前的配置和安全标准。

当大家意见一致时，出现**误解和不一致的可能性就会降低，**从而营造一个更加安全的环境。

06 The NOW Way

The NOW Way 网络安全防护

集成式零信任安全性原则和先进的 AI 功能可确保卓越的网络性能，同时不影响安全性。

通过人工智能原生安全，瞻博网络将体验至上的方法融入网络和安全领域。这意味着利用负责将数据从一个点移动到另一个点（路由、交换、接入点）的网络基础架构，可以同时保护数据，而不会造成延迟或其他性能问题。

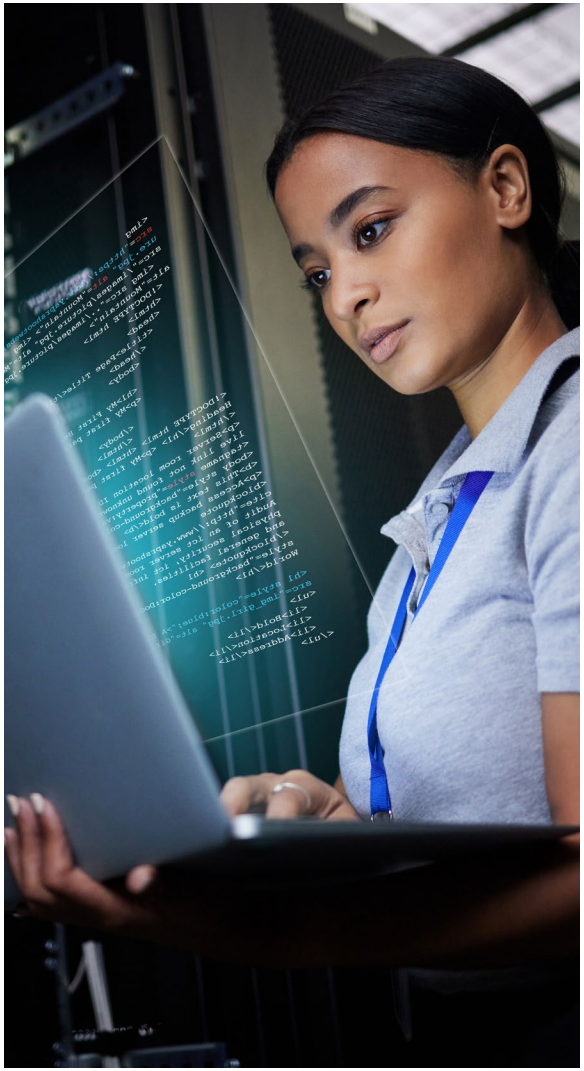
有人提到生产力了，是吗？

网络安全团队都在充分利用网络 AI 和自动化来提高运维效率。Enterprise Strategy Group 的数据显示，62% 的组织观察到威胁检测的速度有所提升，52% 的组织发现威胁检测的准确性也有所提高[3]。这会让网络安全团队的工作变得更加轻松，同时还能提高整体生产力。

瞻博网络人工智能原生安全是一套集网络、安全和 AIOps 于一体的集成式套件，所有功能均可通过 Mist AI 控制台进行访问，更有助于提高生产力。此外，这款套件可以提供出色的可见性和高级 AI 洞察，有助于更快速、更主动地识别威胁并作出响应。

一致性与简单性的完美结合

通过将人工智能驱动型网络和安全遥测技术集成到 Mist 用户界面，瞻博网络 Secure AI-Native Edge 与 Secure Data Center 解决方案珠联璧合，可提供统一、自动化的安全和网络管理。从 WAN 边缘到远程用户、从云计算到数据中心，在网络和安全方面采用一致的策略，可以提供无与伦比的运维效率和保护。



47%

的受访者表示，他们已经或将要部署可同时供网络和安全团队使用的技术[4]

Enterprise Strategy Group

07 Secure AI-Native Edge

从互相指责到击掌相庆，瞻博网络 Secure AI-Native Edge 具有神奇魔力

业界首款也是唯一一款将 AIOps、网络和安全功能集成到单一通用云和用户界面的安全边缘解决方案。

瞻博网络 Secure AI-Native Edge 提供一整套安全接入服务边缘（SASE）架构，可增强网络安全的交付方式，在移动性不断增强的今天，无论您的员工身在何处，都能获得强大保护。这款解决方案提供统一的可见性、运维敏捷性和强大的威胁防护，可帮助您的运维团队更快做出安全决策，而不会影响网络性能。

更强大的协作，更高的生产力

唯一一款将网络和安全性集成到通用运维门户的 Secure AI-Native Edge 解决方案，可提供业界领先的 AIOps。这款解决方案可以改善协作并提高网络可见性，从而更高效地进行故障排除，加快安全事件响应速度。

全栈式、全方位保护

Secure AI-Native Edge 为 Web、SaaS 和本地应用提供全方位的安全性。这款解决方案能够确保用户无论身在何处、无论使用哪种设备，都能够获得一致且安全的访问体验，有效防范各种数字威胁。

借助人工智能驱动型 SD-WAN 增强连接

Secure AI-Native Edge 与瞻博网络的人工智能驱动型 SD-WAN 相结合，可提供最贴合需求的全套 SASE 方法。这一集成有助于简化 WAN 运维、改善云应用的性能，随时随地确保更安全、更完善的连接。

易于管理和部署

Secure AI-Native Edge 通过统一的策略管理简化不同平台和地点的安全协议，借此简化 IT 运维，在确保一致性的同时，还能降低复杂性。更快速的安全决策意味着网络可以实现其设计目标——快速运行。

“可见性是我们安全优先理念的重要组成部分。如果我们看不到系统和网络中的情况，自然也就无法施加控制和保护。”

Seth Tabor, Syntrio 首席技术官

08 Secure Data Center

借助瞻博网络 Secure Data Center 在所有位置实施安全保护

如今，数据中心正迅速成为应用和工作负载分布在多个私有云和公共云环境之间的“数据中心”，不仅增加了复杂性，而且形成了更大的攻击面。

瞻博网络的 Secure Data Center 是数据中心安全领域的一次重大飞跃，弥补了传统安全方法与现代数字环境需求之间的差距。Secure Data Center 是瞻博网络人工智能原生安全中的重要组成部分，可提供统一的管理体验、单一策略框架和业内最具成效的威胁防御。

自动实施零信任

在混合环境中扩展零信任安全性，执行授权访问和微分段。创建更加有效的安全策略，在应用迁移到新的云环境时，这些策略可随时随地跟踪应用，而无需手动进行重新配置。

出色的可扩展性

该架构消除了与机箱尺寸和外形规格相关的传统限制，使您能够不受限制地扩展安全服务和性能。这种开放式的扩展能力可确保数据中心根据企业需求不断演进，省去了不断购置新硬件的麻烦。

充分利用现有硬件

通过利用现有投资，您可以重新利用转发设备，充分利用可扩展的高性能架构，无需大量的额外支出。

瞻博网络的 Secure Data Center 解决方案可为现代组织提供强大、可扩展的解决方案，帮助他们保护数据中心安全，抵御新出现的威胁，同时确保可扩展性、可靠性和高性能。

“瞻博网络为我们提供了同类最佳的防火墙，我们可以按照自己的方式对网络进行微分段，获得了极大的灵活性。”

Seth Tabor, Syntrio 首席技术官

09 第三方测试

稍加验证，长远保障

瞻博网络大力倡导通过第三方测试来独立验证我们解决方案的效力。

过去五年中，凭借来自权威测试组织（如 CyberRatings.org）的行业领先效力测试结果，您可以信心满满地购买和部署瞻博网络的产品，因为事实证明，我们的解决方案无论采用哪种配置，均能始终如一地提供 99% 以上的效力。

瞻博网络对这一领域的不变承诺意味着，在安全基础架构上的投资将转化为切实的效益，使系统能够主动出击，而不是被动响应。您将迅速获得信心，确信现有的安全工具在重压之下也能发挥关键作用，助力企业专注于业务发展，而不是解决漏洞。

真实的客户案例凸显了瞻博网络人工智能原生安全解决方案的变革潜力，是瞻博网络值得信赖的又一有力证明。

99.7%

的安全效力，尽在瞻博网络 vSRX 虚拟防火墙。[5]

CyberRatings.org

10 总结

没有企业能像瞻博网络一样提供如此全面的安全效力

在当今充满网络威胁的环境中，从客户端边缘到数据中心应用实现安全效力是一项势在必行的任务。

通过制定一致的策略并促进网络团队与安全团队协作，您不仅能够巩固自身安全态势，还能在统一战线中提升运维效率。

瞻博网络展现了对这一使命的承诺，通过严格的测试证明了安全效力是可以实现的。在一次又一次的测试中拔得头筹并持续保持低误报率，足以令您的团队倍感安心。

企业面临的威胁不断演变，他们必须优先考虑一套包含合适工具、有效沟通和协作文化的综合战略。通过瞻博网络，客户可以仰赖我们的 AI-Native Security 解决方案，在网络的各个位置（从客户端边缘到数据中心再到云端）提供有效的安全保障。

过去五年里，瞻博网络**在第三方效力测试中一直名列第一**，在所有用例中的有效性均超过 99%。

11 案例研究

AmeriTrust

瞻博网络的威胁感知网络提高了弹性，改善了客户体验。

挑战：保护客户和数据安全

AmeriTrust 是一家专业的商业保险承保和管理服务公司，该公司希望简化运维，并将安全性放在首位。众所周知，不同行业和州级安全法规各不相同，纽约州和加利福尼亚州亦是如此，该公司既要确保尽其所能防范网络攻击，同时又要遵守数据隐私权。

成果：更完善、更安全的用户体验

AmeriTrust 借助瞻博网络 Session Smart 路由器建立了一套应用感知型网络交换矩阵，通过零信任访问控制和分段提供更完善、更安全的用户体验，从而将企业 WAN 水平提升到了新的高度。此外，瞻博网络新一代防火墙 (NGFW) 还在网络边缘提供可见性、控制和防御。这些防火墙将行为和实时威胁检测相结合，为 AmeriTrust 的用户、应用和设备提供强大保护。

“混合工作模式让我们得以在全国范围内广纳贤才，所以我们必须利用威胁感知型网络来为远程工作环境保驾护航。”

Brent Riley, AmeriTrust IT 高级副总裁

安全等级提升行动指南

虽然本书中只是粗略浅谈到安全效力，但我们希望能够引起您的重视。如果不出意外，在与组织中其他志同道合的人接触时，这将是一个不错的开场话题。与此同时，您也可以从以下四件简单的事情入手，扩展您的安全效力知识。

01

迎接人工智能原生安全

有了这种态度，现在就可以消除孤岛、提高生产力并降低风险，同时满足用户对卓越体验的需求。

02

考虑成本效益

将网络和安全可见性整合到由 AI 驱动的单一平台中，帮助消除冗余工具、简化工作流程，并降低整体复杂性。

03

了解 Secure Data Center

查看该信息图表，更好地了解真正的零信任数据中心所包含的十大要素，例如“化无形为有形”和“全面实现自动化”等。

04

查阅第三方测试报告

查看来自知名测试机构的行业领先效力结果，例如 CyberRatings.org 刚刚发布的 2024 年云网络防火墙和企业防火墙报告。

后续举措

与专家联系

瞻博网络将一路为您提供指导，确保从客户端边缘到数据中心应用实现固若金汤的安全性，准备好开启您的安全之旅了吗？安排预约，免费进行咨询。

联系我们 →

进行深入探究

瞻博网络人工智能原生安全是一套集网络、安全和 AIOps 于一体的集成式套件，通过通用云统一进行管理，该套件本身及其如何帮助提高生产力，都是非常值得探索的方面。

访问网站 →

查看客户案例

了解瞻博网络人工智能原生安全如何帮助客户化挑战为机遇，在各行各业和各种场景中取得丰硕成果。

费城 →

Syntrio →

Scripps →

给我们一次机会

立即试用瞻博网络人工智能原生网络平台，现在体验既方便又实惠。一系列精彩的视频、诱人的演示和限时优惠，静待您来体验。

开始体验 →

关于作者

Jeff Aaron

瞻博网络
产品营销全球副总裁

LinkedIn

Jeff 负责瞻博网络人工智能原生网络产品组合的整体全球推广。他在高科技领域拥有超过24年的营销经验，曾就职于各大软件、网络和电信公司。Jeff 拥有杜克大学学士学位，主修计算机科学和经济学。

为什么选择瞻博网络

瞻博网络认为，拥有连接能力并不等于获得出色的连接体验。瞻博网络的人工智能原生网络平台从零开始构建，利用 AI 为边缘、数据中心和云端用户提供卓越、高度安全且可持续的体验。如需了解其他信息，请访问 juniper.net，或者在 X（原 Twitter）、LinkedIn 和 Facebook 上关注瞻博网络。

更多信息

如需了解瞻博网络人工智能原生安全的更多信息，请联系瞻博网络代表或合作伙伴，或者访问 juniper.net/cn/zh/security.html。

注释和参考文献

01 现代网络的人工智能原生需求，Enterprise Strategy Group，2024 年 1 月。https://www.juniper.net/cn/zh/forms/2024/ai-native-networking-platform-requirements-for-modern-networks.html

02 从网络角度综观网络与安全融合，Enterprise Strategy Group，2024 年 1 月。https://research.esg-global.com/reportaction/515201726/Marketing?SearchTerms=network%20security%20collaborate%29

03 完整调查结果：AIOps 在网络基础架构运维中的作用，Enterprise Strategy Group，2024 年 4 月。https://research.esg-global.com/reportaction/515201780/Marketing?SearchTerms=The%20role%20of%20AIOps

04 从网络角度综观网络与安全融合，Enterprise Strategy Group，2024 年 1 月。https://research.esg-global.com/reportaction/515201726/Marketing?SearchTerms=network%20security%20collaborate%29

05 2024 年云网络防火墙报告，CyberRatings.org，2024 年 4 月。https://www.juniper.net/cn/zh/forms/2024/2024-cyberratings-cloud-network-firewall-report.html

Juniper.net

Juniper Networks Inc.
1133 Innovation Way
Sunnyvale, CA 94089

7400200-001-ZH 2024 年 10 月