FORCEPOINT 下一代防火墙 (NGFW)

通过您的企业网络连接和保护员工及其数据

FORCEPOINT

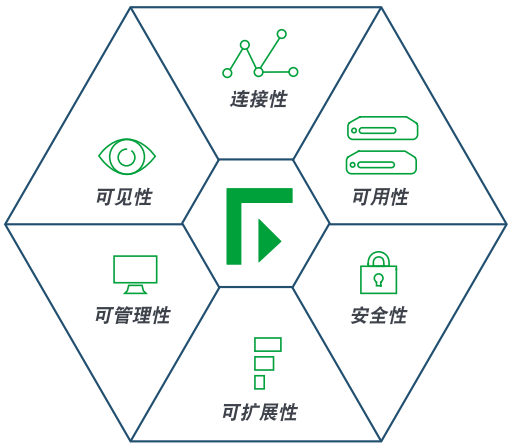
Protecting the human point.

Forcepoint NGFW

最安全、最高效的企业防火墙 —
集中管理、始终开启、从不间断

Forcepoint 下一代防火墙 (NGFW) 通过企业网络连接和保护员工及其所用的数据，集最高的有效性、可用性和安全性于一身。Forcepoint 网络安全解决方案得到全球数千客户的信赖，可帮助企业、政府机构和其他组织经济高效地解决关键问题。

用户可以无缝集中管理 Forcepoint 网络安全解决方案，不受部署形式所限，无论是物理、虚拟还是云部署，皆能轻松应对。管理员能在数分钟内部署、监控和更新数千个防火墙、VPN 和 IPS，所有工作都在一个控制台上完成 — 网络运营支出降低多达 50%。防火墙和网络高级集群消除了停机时间，管理员可以快速将业务流程映射到强大、准确的控制程序中，以拦截高级攻击、防止数据被盗并妥善管理加密流量，且所有这一切不会对性能造成任何影响。



防火墙与 IPS 强强联合

- Forcepoint NGFW 不仅在 NSS Labs 的 2017 NGFW 测试中获得了安全性最高分，还内置了顶级入侵防御系统 (IPS)，无需额外许可证或单独的工具即可实施强大的反入侵策略。

阻止入侵与盗窃

- 在 Gartner 2017 年《企业网络防火墙魔力象限报告》中，Forcepoint 被列为具最佳执行能力的企业级防火墙。它提供广泛的高级访问控制和深层检测功能，可拦截会导致关键数据或知识产权泄露和被盗的高级威胁。
- 作为检测高级逃逸技术 (AET) 的先驱，Forcepoint NGFW 常常可以先于现代攻击，扰乱攻击者致使其无法入侵恶意代码、发现异常并阻止好事者利用网络中的漏洞。

NSS Labs
NGIPS
推荐 2016 年

NSS LABS
RECOMMENDED

NSS Labs
NGFW
推荐 2017 年
最高分

“我们看到了将路由器和高级防火墙功能相结合，从而加强各站点安全性并提高吞吐量的机会。我们需要一个具备集中管理功能的解决方案，以便每次添加新的移动站点时只需轻松复制即可，从而减轻 IT 员工的管理负担。”

— Christophe Hazeman，IT 部主管，Carglass

减轻 TCO 负担的运营效率

Forcepoint NGFW 专用于降低复杂性和缩短网络平稳安全运行所需的时间 — 并保持其长久运行。分析师表示，IT 总体拥有成本 (TCO) 的 80% 发生在初次购买之后。[1] 负担过重的网络运营团队不得不持续布设新的防火墙、监控网络活动、更新策略、升级软件和应对事故。

Forcepoint NGFW 围绕统一的软件核心而构建，可为所有类型的部署提供一致的功能、加速的运转和集中式管理。Forcepoint NGFW 安全管理中心 (SMC) 可以从单一虚拟管理平台配置、监控和更新多达 2000 个 Forcepoint NGFW 设备，且不受部署形式所限，物理、虚拟和云部署皆能应对。

防火墙部署速度加快 **70%**[2]

IT 人员耗时缩短 **53%**[2]

事件响应速度加快 **73%**[2]

零接触部署

无需现场技术人员即可将 Forcepoint NGFW 部署到远程办公室和分支机构，节省了时间和金钱。设备可以从 Forcepoint 的安装云中自动下载初始配置，无需人工设置。

智能策略，一键更新

Forcepoint 的智能策略采用您所熟悉的术语（例如用户、应用程序、位置等）来表述业务流程。简易分组取代了硬编码值，因而策略可以在整个网络动态再利用。管理员只需一个点击，即可快速更新策略并将其发布到全球所有相关的防火墙。

事件响应速度加快

Forcepoint SMC 可以轻松展示和分析整个网络中的动态。网络管理员能够交互式地深入探究相应数据，快速调查模式和异常情况，并将见解转化为即时的行动。

Forcepoint NGFW 专用于降低拥有成本

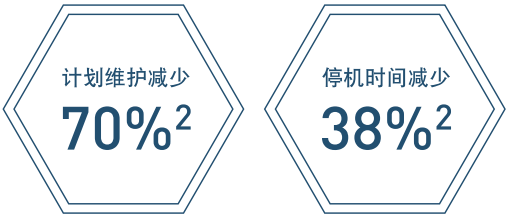
- 硬件
- 订阅和许可
- 支持

FORCEPOINT 如何帮助降低无形成本：

- 统一的解决方案 — 物理、虚拟、云
- 内置 IPS、VPN、NGFW、代理
- 零接触部署
- 每个级别都具备高可用性
- 采用低成本宽带的 SD-WAN 控制
- 集中管理，一键部署
- 软件可升级
- 设备可重复使用
- 按应用程序和版本控制访问权限

消除网络停机时间的高可用性

Forcepoint NGFW 经特殊设计，会始终保持开启，即使发生故障也不例外。每个层级（防火墙、网络和管理）都具备弹性设计，机器脱机或缆线被切断时能够妥善应对。Forcepoint NGFW 消除了停机时间，提高了业务连续性，可保持业务平稳运行。



持续运行的高级防火墙集群

以小组方式（而不仅仅是成对）部署 Forcepoint NGFW 称为集群，这样可在单个设备中存在服务中断时保持网络正常运行。您甚至可以将不同型号混在一起，以延长当前设备的使用寿命。

零停机更新和软件升级

有了 Forcepoint NGFW 之后，您可以在不脱机的情况下更新防火墙安全策略、在不影响连接性的情况下立即响应安全事件，并无缝升级设备软件 — 无需让问题留至维修时段或丢弃任何数据包。

多 ISP 安全 SD-WAN 集群

Forcepoint 是将不同网络链路集群在一起的先驱之一。多链路 VPN 技术可以轻松地同时混合商用宽带链路和专用租用线路，以消除单点故障、降低网络成本、增加容量并提高服务质量。

弹性管理

通过 Forcepoint NGFW 安全管理中心 (SMC)，您可以同时使用多台服务器以继续管理网络并调查事件，即使主服务器脱机也不受影响。

“我们的网络强大，吞吐量极高，因此对于新防火墙解决方案来说，性能是首要考量因素。Forcepoint NGFW 是理想之选，因为它集成了最先进的安全功能且表现稳健。”
— 网络架构师，Cegedim

在 NSS Labs 的 2017 年下一代防火墙测试中，Forcepoint NGFW 在安全性方面位列第一。

无与伦比的安全性可以在不牺牲性能的情况下，防止数据被盗

在 NSS Labs 的 2017 年下一代防火墙测试中，Forcepoint NGFW 在安全性方面位列第一。其内置了多种安全功能（包括 VPN、IPS、NGFW 和安全代理），因此您无需同时应付分散在多个位置的不同产品、分配许可或处理管理事务。您甚至可以将安全设备重新用于其他目的，从而延长基础架构的使用寿命。

通过 Forcepoint 安全管理中心 (SMC)，您可以将不同类型的安全技术应用于每种连接，例如：按应用程序、组织、位置或各种其他因素，所有这些都不会影响到网络性能。

控制加密流量 — 保护隐私

借助 Forcepoint NGFW，您可以轻松将传入和传出流量快速转换到加密传输。使用加速解密检查 HTTPS 和其他基于 SSL/TLS 的协议，以拒绝或允许 HTTPS 内的特定 HTTP 命令或 URL 段 — 即使在虚拟部署或云部署中也是如此。Forcepoint NGFW 的 SSH 安全代理具备高级控制功能，适用于任务关键型应用程序。此外，智能策略可确保遵守新出台的隐私法律和内部惯例，防止用户与银行、保险公司或其他敏感站点通信时暴露个人身份信息 (PII)。

网络攻击事件减少 **86%**[2]

网络攻击事件减少 **69%**[2]

沙盒和高级恶意软件检测

Forcepoint NGFW 将多种扫描技术应用于网络流量中的文件，包括信誉审查、内置反恶意软件扫描和使用 Forcepoint 高级恶意软件检测服务。这个基于云的强大系统使用业界领先的沙盒和其他分析技术来检查文件的行为，并可靠地发现和阻止恶意代码。组织可以根据自己的运营需求，灵活选择基于云或内部部署版本。

强有力地防止入侵

Forcepoint 是防御高级逃逸技术 (AET) 的先驱。我们的流量完整协定规范化可扰乱攻击者致使其无法入侵恶意代码、发现异常并阻止好事者利用网络中的漏洞。

保护任务关键型应用程序

Forcepoint NGFW 能够提供基于代理的保护，并全面检查通过加密 HTTPS 连接通信的任务关键型应用程序的流量。这项技术源自 Sidewinder 防火墙，依赖于众多全球最敏感的网络。它进一步扩展了我们独一无二的代理功能，使得管理员能够控制 HTTPS 流量、允许或者阻止特定 URL 或特定类型的 HTTPS 请求。

强化安全性 — 集成的 URL 过滤

Forcepoint NGFW 提供快速灵活的方式来强制实施 Web 访问策略，以确保合规性并阻止访问网络钓鱼站点及恶意或不良内容。Forcepoint ThreatSeeker Intelligence 云服务提供覆盖广泛、不断更新、可直接在访问策略中使用的 URL 分类，从而动态控制允许哪些用户访问哪些站点。

业务转型 — 将企业应用程序迁移到云端

Forcepoint NGFW 能够保护在 AWS 和 Azure 云中运行的工作负载。Forcepoint NGFW 可直接从云市场部署，然后通过现有的 SMC 系统管理。这有助于组织保护云中的应用程序和其他工作负载，同时如同在内部数据中心、办公室、门店和分支机构以及其他云环境中一样，享受业界领先的安全性和连接性。

将应用程序列入白名单和黑名单，实现端点精细控制

终端环境代理 (Endpoint Context Agent) 可以将主机和最终用户设备上运行的客户端应用程序列入白名单和黑名单。例如，其允许管理员指定可以或不能访问互联网的浏览器及其版本。这带来了更精细的控制能力，用户可以根据组织的业务需求和安全状况自定义。

Forcepoint — 创造直接的企业价值

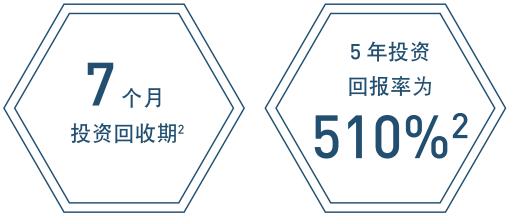
Forcepoint 带来新的企业安全管理方法：抑恶扬善。Forcepoint NGFW 下一代防火墙屡获殊荣，可以拦截恶意攻击、阻止数据和知识产权被盗，同时改善基础架构并提高运营效率。

提高业务生产力 — Forcepoint 网络安全解决方案专为需要始终保持连接的企业而设计，可让致力于创新的分布式员工团队安全访问所需的数据。

减轻 TCO 负担 — Forcepoint NGFW 独一无二的高可用性架构、多功能平台和自动化集中管理降低了运营成本，延长了使用寿命，并且减少了对于培训或专业知识的需求。

降低 IT 风险 — Forcepoint NGFW 可将威胁、入侵和盗窃风险扼杀在摇篮，阻止其转变为金融灾难。

简化合规性 — Forcepoint NGFW 将业务流程映射到了控制程序中，因此您可以快速响应事件并纠正问题，这一点在与审计员合作时尤为重要。



参考文献

[1] Gartner

[2] Forcepoint NGFW Business Value Snapshot, IDC Research, March 2017.

“Forcepoint 能够满足我们法律客户方方面面的需求，包括安全性、合规性和成本。其具有弹性、安全，并且可以在一定范围内灵活扩展。它带来的安全性其他防火墙无法企及。”

— 高级安全顾问，Netprotocol

关于 FORCEPOINT

Forcepoint 致力于实现网络安全转型，将重点放到最重要的事情上，即了解人们在与关键数据和知识产权（无论其位于何处）交互时的意图。我们的系统绝不牺牲任何功能，让公司能够在保护知识产权和简化合规性的同时，赋予员工畅通无阻地访问机密数据的能力。Forcepoint 总部位于德克萨斯州奥斯丁，为全球 20,000 多家组织提供支持。有关 Forcepoint 的更多信息，请访问 www.Forcepoint.com.cn，并在 Twitter 上通过 @ForcepointSec 关注我们。

联系信息

www.forcepoint.com.cn/contact

[BROCHURE_NGFW_OVERVIEW_ZHCN] 400013.101017