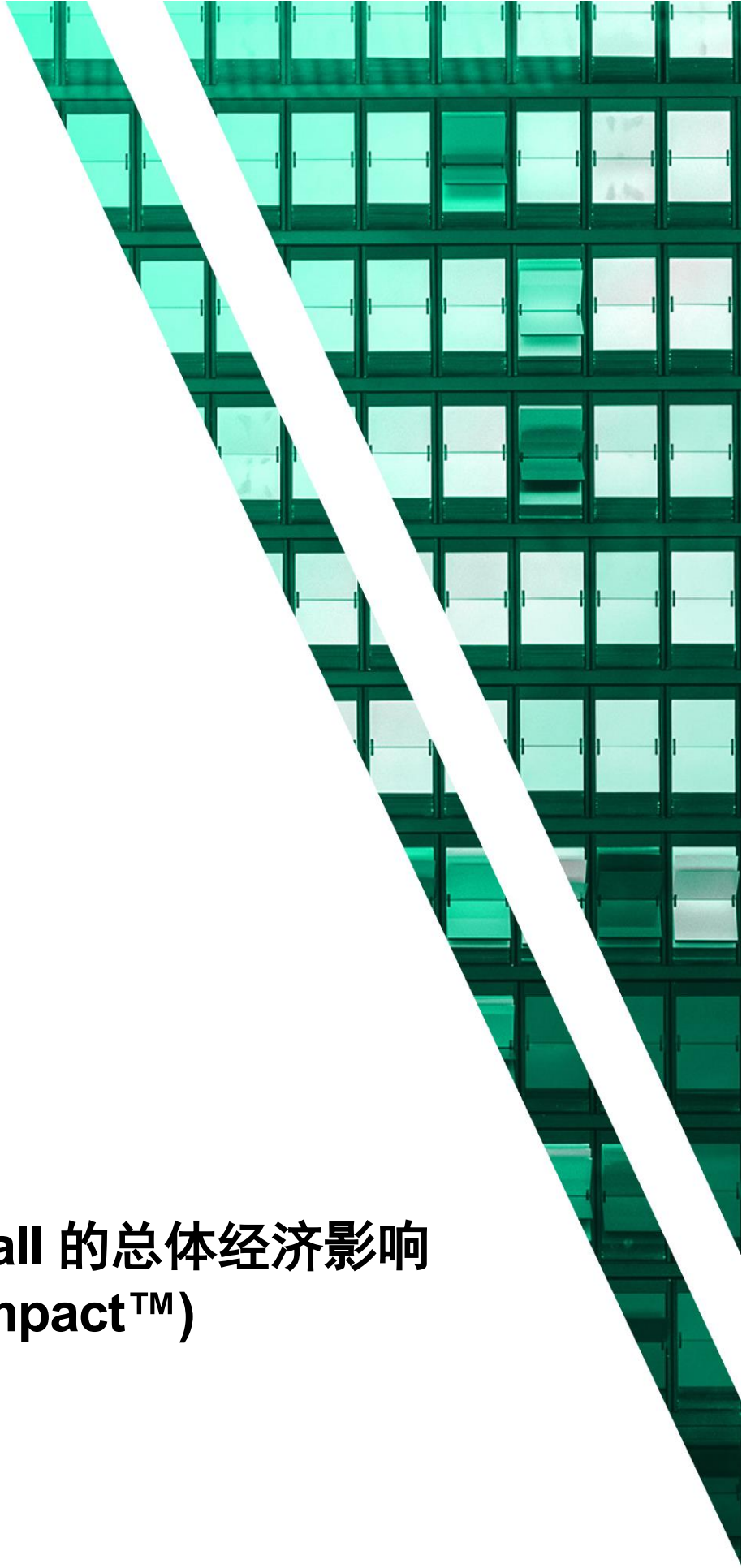
FORRESTER®



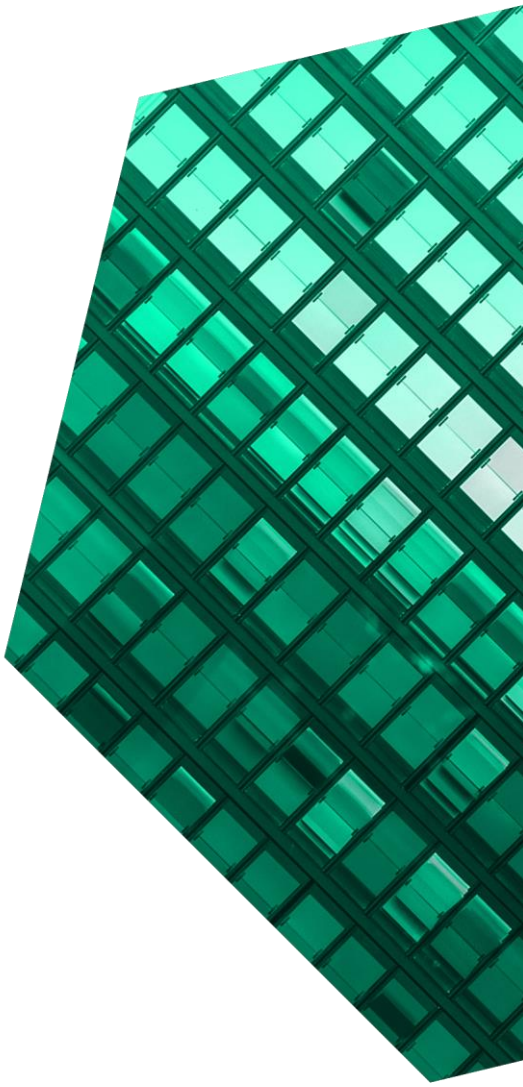
思科 Secure Firewall 的总体经济影响 (Total Economic Impact™)

Secure Firewall 带来的成本节约和业务收益

2022 年 3 月

目录

咨询团队： *Henry Huang*
Nick Mayberry



关于 FORRESTER CONSULTING

Forrester Consulting 提供独立客观的研究型咨询服务，帮助领导者带领企业迈向成功。如需了解详情，请访问 forrester.com/consulting。

内容提要

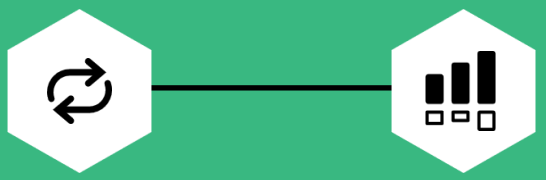
思科 Secure Firewall 和 Firewall Management Center 可提高企业对其网络安全的可视性和控制。受访企业在防火墙相关网络专业工作方面实现了 95% 的节约，并在安全相关专业工作方面实现了 83% 的节约。此外，他们还将重大安全漏洞风险降低了 80%，同时最大限度减少了网络和 VPN 中断，提高了终端用户的生产率。即使防火墙部署减少了 25%，安全态势仍得到改善。

思科 Secure Firewall 是下一代的 7 层网络安全解决方案，可保护企业免受外部和内部威胁，同时减轻防火墙和威胁管理对网络和安全团队的负担。企业可以通过 Firewall Management Center (FMC) 来管理思科 Secure Firewall；FMC 是集中式的防火墙管理和威胁防御中心，可以从更统一、更全面的视角，甚至通过应用层和加密流量中检测到的威胁来增强网络和安全团队对网络活动的可视性。此外，它还可增强对 Snort 3 入侵防御系统 (IPS) 的控制，并增强软件的 URL 过滤和恶意软件防御功能。

思科 Secure Firewall 许可包括使用思科的整合平台 SecureX；借助该平台，企业可将来自 Cisco Secure 产品组合和第三方安全工具的威胁数据整合到单个全局视图中，而该视图具有丰富的背景数据，可促进对威胁的快速调查和响应。

思科委托 Forrester Consulting 开展总体经济影响 (Total Economic Impact™, TEI) 研究，考察企业部署 Secure Firewall 可能实现的潜在投资回报率 (ROI)。[1] 本研究旨在为读者提供一种适当的框架，来评估 Secure Firewall 对所在企业的潜在财务影响。

关键统计数据



投资回报率 (ROI)
195%

净现值 (NPV)
1,229 万美元

为了更好地了解与这项投资相关的收益、成本和风险，Forrester 采访了八家企业中十名具备 Secure Firewall 使用经验的决策者。在本研究中，Forrester 汇总了受访者的体验，并将结果合成到一家复合型企业中。

这些受访者指出，在使用 Secure Firewall 之前，其企业缺乏充分管理和有效保护网络所需的可视性和可管理性。受访者还指出，由于缺少这种可视性和高效的图形用户界面 (GUI)，类似防火墙部署、策略创建、防火墙升级和策略更新等网络工作流都需要花费大量的时间。此外，还会在安全工作流方面花费额外的时间，如威胁调查和响应，以及远程访问管理。受访者还指出，在高需求时期，网络性能较差，以及管理多个供应商解决方案都会导致复杂性增加。

在投资购买 Secure Firewall 之后，受访者不仅减少了完成上述网络和安全工作流所需的时间，还提高了企业的整体安全性。与此同时，通过更快的策略更新、更强的网络流量检查和更好的整体网络性能，企业提高了员工的生产率，同时淘汰了原有解决方案，并在很大程度上消除了相关的管理时间成本。

总收益

1,860 万美元

重要发现

量化收益。 经风险调整后的现值 (PV) 量化收益包括：

- **网络运营工作流减少高达 95%。** 得益于思科 Secure Firewall 的最新功能和通过 Firewall Management Center 实现的便利管理，受访企业大幅减少了为以下工作流付出的时间：
  - 防火墙部署时间减少了 36%。
  - 防火墙更新时间减少了 90%。
  - 与传统的自适应安全设备 (ASA) 5500-X 防火墙相比，防火墙策略更新时间减少了 95%。
  - 相比基于防火墙威胁防御 (FTD) 策略的早期版本，防火墙策略更新时间减少了 80%。
  - 虚拟防火墙更新时间减少了 80%。
- **安全调查和响应工作流时间减少高达 83%。** 受访者还指出，将思科 Secure Firewall 和 Firewall Management Center 结合起来，可以更好地整理信息以进行使用和分析，从而大大节省安全专业人员的工作量。受访者表示，调查潜在威胁的时间减少了 49%，响应威胁的时间减少了 83%。将 SecureX 与 Secure Firewall 和 FMC 结合使用，可使企业节省高达 77% 的调查和响应剩余时间。

> **“我们拥有很强的安全意识，并希望利用各种产品来保护我们的公司。因此，我们选择了思科。他们提供安全产品，并一路发展壮大；对他们来说，安全并不只是可有可无的附属品。”**
> *高级网络工程师，制造业*

- **安全漏洞风险降低高达 80%。** 思科 Secure Firewall 和 Firewall Management Center 提供的综合可视性和控制功能降低了受访企业的潜在重大安全漏洞风险和相关成本。与传统的 ASA 5500-X 防火墙相比，这些解决方案将安全漏洞风险降低了 80%，与基于 FTD 的早期防火墙相比，则降低了 15%。SecureX 可使受访企业的安全漏洞剩余风险和成本最多减少 23%。

- **每年提高终端用户的生产率价值约 200 万美元。**部署思科 Secure Firewall 和 Firewall Management Center 在两个方面提高了受访企业的生产率。第一，它使网络专业人员修复中断策略更新错误的速度加快了 80%。第二，它降低了网络性能下降的严重程度，每年可为每个受影响的终端用户挽回近 9 小时的工作时间。
- **减少了淘汰原有工具的成本。**受访者还指出，思科 Secure Firewall 使他们能够淘汰之前实施的昂贵的原有安全解决方案。受访者指出，在独立的 IPS 方面，每年可以节省数十万美元，在避免更换现有安全解决方案的成本方面，每年可以节省数百万美元，此外，思科 Secure Firewall 可用更少的防火墙提供相同级别的保护，可额外节省 25% 的成本。

未量化收益。这项研究发现的未量化收益包括：

- **VPN 生产率和安全增强**。思科 Secure Firewall 还可通过负载均衡、本地认证和多证书认证等方式提高远程访问 VPN 的生产率和安全性。终端用户可以通过 VPN 建立更好的连接，而企业可以获得更好的访问控制。
- **改善居家办公时的业务运营。**在员工转向居家办公后，思科 Secure Firewall 的控制措施还能帮助在 VPN 使用量激增时保持业务的平稳运营。即使是在需求高峰期，网络专业人员也可以利用限速和冗余改进来改善员工体验并提高生产率。
- **轻松过渡到云端。**最后，受访者表示，思科 Secure Firewall 提供了一个统一的平台来保护站点内部、站点之间、组织之间甚至多个云平台之间的流量，从而使他们的云计划更容易实现。具体来说，思科通过云平台市场提供了标准化的策略和经过验证的方法来部署 Secure Firewall。

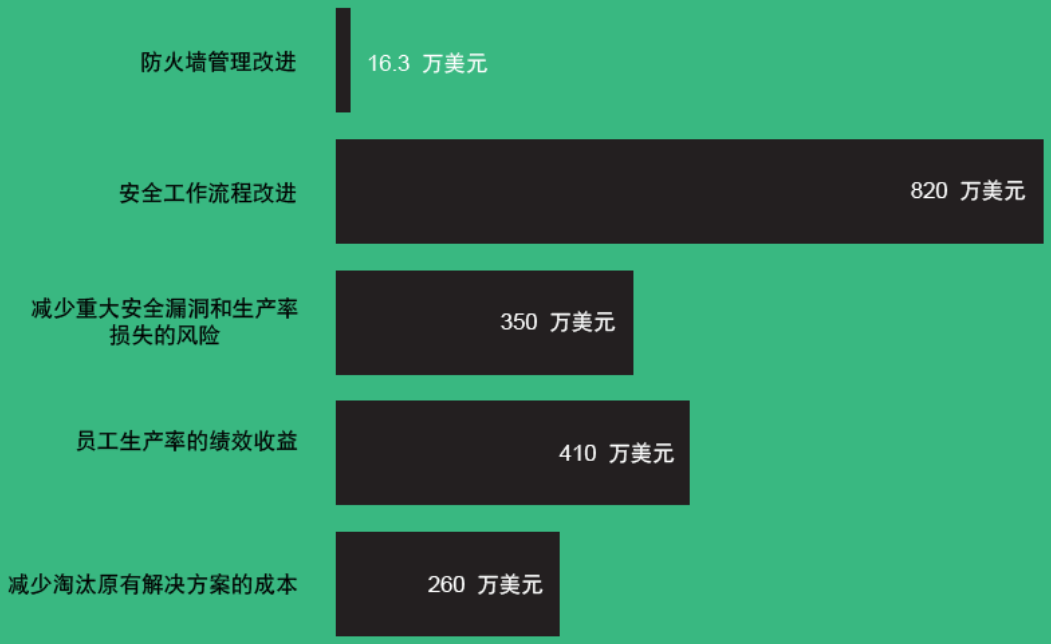
成本。经风险调整后的现值成本包括：

- **许可成本。**虽然许可成本是受访企业所付出的最高成本，但是，建立思科企业协议 (Cisco Enterprise Agreement) 可获得企业此前缺乏的额外功能和解决方案，从而节省数十万美元，并进一步增强企业的安全态势。Secure Firewall 内含 SecureX 许可授权。
- **实施、策略制定和培训的成本。**受访者指出，在实施和部署防火墙以及为它们创建策略方面存在内部成本。每个站点部署防火墙估计需要 6 个小时，而创建策略估计需要 30 个小时。SecureX 需要额外的 20 个小时来实施，并且每年需要 100 个小时来进行持续管理。有些受访者还指出，需要培训他们的网络和安全专业人员使用思科 Secure Firewall 和 Firewall Management Center。培训的内部成本达到每名受训员工 2 个小时，同时受访者指出可利用思科安全专家主讲的公开培训视频。

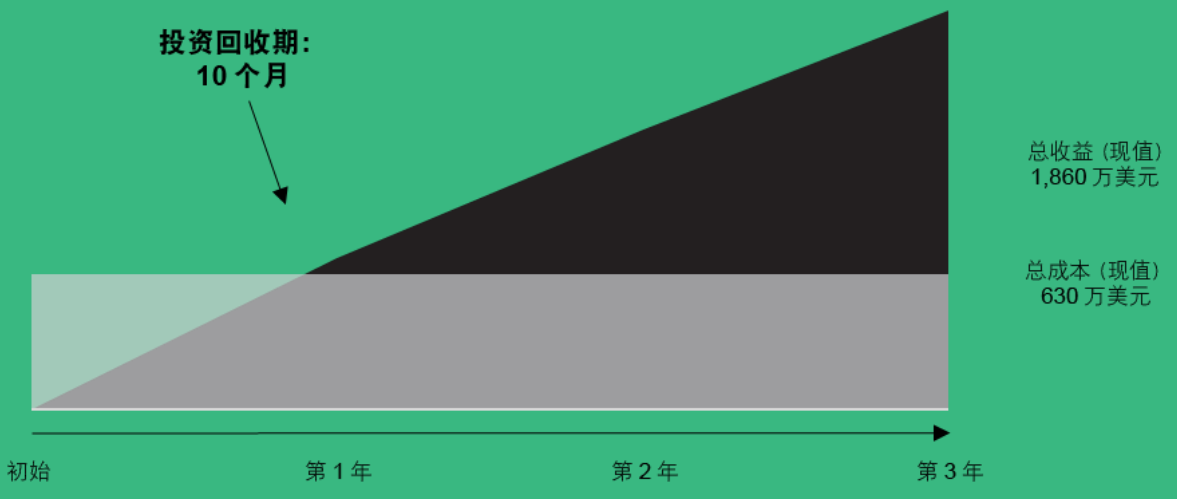
根据客户访谈结果和财务分析发现，该复合型企业在三年间获得了 1,859 万美元的收益，成本为 630 万美元，由此得出净现值 (NPV) 为 1,229 万美元，投资回报率为 195%。

投资回报率	收益现值	净现值	投资回收期
195%	1,859 万美元	1,229 万美元	10 个月

收益（三年期）



财务摘要



TEI 框架与方法

根据访谈中提供的信息，Forrester 为这些考虑投资购买思科 Secure Firewall 的企业构建了一种总体经济影响 (Total Economic Impact™) 框架。

该框架的目标是明确影响投资决策的成本、收益、灵活性以及风险因素。Forrester 采用了多步式方法评估 Secure Firewall 对企业的影响：

尽职调查
对思科利益相关方和 Forrester 分析师进行了访谈，以收集有关 Secure Firewall 的数据。

决策者访谈
采访了使用 Secure Firewall 的企业中的十名决策者，以获取与成本、收益及风险相关的数据。

复合型企业
根据受访企业的特征设计了一家复合型企业。

财务模型框架
使用 TEI 研究方法根据访谈情况构建了财务模型，并根据决策者的问题和顾虑，对该模型进行了风险调整。

案例研究
在对投资影响建模时，使用了 TEI 的四项基本要素：收益、成本、灵活性和风险。鉴于与 IT 投资相关的 ROI 分析日渐复杂，Forrester 的 TEI 研究方法能够全面考量购买决策所带来的总体经济影响。要进一步了解 TEI 研究方法，请参见“附录 A”。

披露声明

读者应注意以下事项：

本研究由思科委托 Forrester Consulting 开展。该研究并不用于竞争力分析。

对于其他企业可能获得的投资回报率，Forrester 未作出任何假设。Forrester 强烈建议读者根据研究中提供的框架，使用自己的估算数据来决定企业是否应投资 Secure Firewall 解决方案。

虽然思科进行了审查并且向 Forrester 提供了反馈，但 Forrester 保留对本研究及其结论进行编辑的权利，并且不接受与 Forrester 的结论相背或是会模糊本研究意义的更改。

思科提供了受访客户的名单，但未参与访谈。

思科 Secure Firewall 客户历程

投资 Secure Firewall 的推动因素

受访决策者			
受访者	**行业**	**地区**	**员工总数**
工程服务经理	IT 服务	北美	750
首席基础设施工程师	金融服务	北美	2,800
电信和电话服务助理经理	金融服务	北美	2,800
首席网络安全工程师	安全服务	北美	3,000
高级网络工程师	制造	全球	5,500
网络工程高级经理	科技	全球	40,000
高级安全工程师	科技	全球	40,000
安全运营团队负责人	教育	北美	46,000
资深基础设施架构师	工业	全球	205,000
高级网络工程师	科技	全球	275,000

主要挑战

在部署思科 Secure Firewall 和 Firewall Management Center 之前，受访企业主要使用传统的基于 ASA 5500-X 的防火墙设备来保护他们的环境。有些受访者在几年前从传统的基于 ASA 的防火墙转换到了早期基于 FTD 的防火墙，他们指出，在思科 Secure Firewall 和 Firewall Management Center 升级到最新版本的 FTD 之后，他们获得了额外的收益。

受访者表示其企业穷于应付这些共同的挑战，其中包括：

- **有限的可视性。** 受访者指出，他们之前的环境依赖于基于 ASA 5500-X 的防火墙，因此对整体安全性的可视性有限。其中一个原因就是缺乏整合。在以前的环境中，受访企业很难整合各种安全解决方案，建立统一的管理和一致的策略，同时也很难对真实环境有一致的认知。可视性有限的另一个原因是，以前的环境依赖于端口检查作为了解网络的主要视角。受访者指出，这使得他们无法更深入地了解数据，并且对应用程序和历史背景的可视性有限。

> **“我们以前缺乏诸如现代应用程序控制等功能。我们无法了解我们的用户如何使用网络，也不能对这种使用做出充分的响应。”**
> *安全运营团队负责人，教育行业*

- **实施和管理防火墙的高时间成本。** 受访者还指出，部署和管理原有防火墙非常耗时。这很大程度归因于无法同时向多台设备推送更新。来自教育行业的安全运营团队负责人估计，过去部署一个简单的防火墙规则需要 45 分钟到 1 个小时。此外，受访者指出，他们之前的环境缺乏可视性；这意味着，为确认安全态势，他们花费了过多的时间来关联不同系统之间的数据。

“易于管理和整合一直是思科的优势之一。此外，我们还受益于更丰富的数据，因为不同的系统更容易相互馈送。除此之外，我们还建立了针对某些威胁的自主响应机制。我们以前做不到这一点。”
首席网络安全工程师，安全服务领域

- **性能较差。** 受访者还指出，他们之前的系统性能较差。例如，来自教育行业的安全运营团队负责人表示，当对他们的网络和安全基础设施的需求飙升时，他们之前的解决方案会“崩溃，不断重启和丢包”。这甚至对工作效率产生了影响，因为“教授们无法利用网络播放视频或在课堂上进行演示。”
- **供应商管理。**最后，客户指出，在他们以前的环境中，多个供应商会带来供应商管理方面的问题。来自金融服务公司的首席基础设施工程师指出，“因为拥有多家供应商，每件事都必须重复做好几次，访问多个控制面板，在不同的系统中应用相同的更改或更新。”

复合型企业

根据访谈，Forrester 构建了一个 TEI 框架、一家复合型企业和一项说明财务影响的 ROI 分析。该复合型企业代表了 Forrester 采访的九名决策者所在的企业，在下一节将借该企业来进行总体财务分析。该复合型企业具有以下特征：

对该复合型企业的描述。 复合型企业是一家 B2B 科技企业，年收入达 50 亿美元，拥有 16,000 名员工。该企业为全球客户提供服务。该企业要求其数据中心具有高可用性，以确保客户可持续访问存储在数据中心的数据。这些数据中心还需要重视安全性，以保护敏感的客户数据免受恶意访问或攻击。除了数据中心之外，该企业正在推动以更分布的方法来运用多云技术。此外，该企业还使用 Secure Firewall 来保护其边缘站点/分支机构办公室。

部署特征。 该复合型企业已经投资购买了思科的下一代防火墙。其三分之二的防火墙系统由思科 Firepower 设备组成，另外三分之一由 ASA 5500-X 防火墙组成。如今，该企业正在将其所有 102 个家庭办公室、数据中心和主要办公地点的防火墙转换为最新版本的思科 Secure Firewall，更新 68 个 Firepower 设备，并替换 34 个基于 ASA 的设备。有些受访者选择在不更换硬件的情况下将现有的传统设备升级为 FTD 软件。此外，该企业还在其数据中心部署了思科 Secure Firewall 虚拟防火墙，以处理数据中心与分支机构办公室之间的东西流量，以及数据中心与多个公共云平台之间的流量。该企业利用 Secure Firewall 许可中内含的 SecureX，进一步加强其安全团队的威胁调查和响应工作。

重要假设

- **50 亿美元收入**
- **16,000 名员工**
- **替换 34 个基于 ASA 的防火墙**
- **将 68 个 Firepower 防火墙更新到最新的思科 Secure Firewall**

收益分析

应用于该复合型企业的量化收益数据

总收益

参考号	收益	第 1 年	第 2 年	第 3 年	总计	现值
Atr	防火墙管理改进	134,951 美元	25,556 美元	25,556 美元	186,064 美元	163,005 美元
Btr	安全工作流程改进	2,669,879 美元	3,685,484 美元	3,685,484 美元	10,040,848 美元	8,241,976 美元
Ctr	减少重大安全漏洞和生产率损失的风险	1,291,446 美元	1,393,402 美元	1,520,848 美元	4,205,696 美元	3,468,249 美元
Dtr	员工生产率的绩效收益	1,656,403 美元	1,656,403 美元	1,656,403 美元	4,969,210 美元	4,119,230 美元
Etr	减少淘汰原有解决方案的成本	1,985,115 美元	503,513 美元	503,513 美元	2,992,142 美元	2,599,074 美元
	总收益 (经风险调整)	7,737,795 美元	7,264,360 美元	7,391,805 美元	22,393,959 美元	18,591,534 美元

防火墙管理改进

证据和数据。 受访的决策者指出，在部署思科 Secure Firewall 后，无论是从原有防火墙进行转换，还是从早期 Firepower 威胁防御版本进行升级，都可以节省管理防火墙的时间和成本。以下事实在很大程度上印证了这些改进：Firewall Management Center 通过单一面板视图为网络专业人员提供集中式的防火墙管理，让他们能够将更改推送到许多设备。

“FMC 为我们提供了集中管理和升级防火墙的面板，而不是像以前那样在不同的防火墙之间不停转换。”

工程服务经理，IT 服务行业

受访企业介绍了与防火墙部署相关的时间和成本。受访者指出，对于传统的基于 ASA 的防火墙，其部署会花费大量的时间，需要编写特定于用例的防火墙规则，并手动将这些规则分发到现有的不同防火墙策略集合中。

“思科 Secure Firewall 让我们能够快速增加并部署新的防火墙。在增加防火墙的同时，我们不需要增加员工。”

网络工程高级经理，科技行业

在转换到思科 Secure Firewall 和 Firewall Management Center 后，受访者表示部署防火墙的时间节省了 30% 到 40%。时间的减少要得益于思科 Secure Firewall 的自动部署能力。例如，来自科技行业的网络工程高级经理表示：“我们已使用思科

Secure Firewall 实现了自动化部署。我们可自动地弹出方框、设置 IP、设置框架，及执行策略。”

“内置的自动化功能为我们节省了最多的时间。即使是在升级的时候。我不再需要像操作 ASA 防火墙那样坐在那里照看整个升级过程。我可以离开，如果防火墙在足够的时间里还没有重启，Firepower 会告诉我。”
网络工程高级经理，科技行业

自动化还帮助受访者管理和维护部署后的思科 Secure Firewall。思科 Secure Firewall 内置自动升级功能。受访者报告说，升级基于 ASA 的防火墙可能需要几个小时，从一个防火墙再到另一个防火墙，上传更新文件并重启系统。如果使用思科 Secure Firewall 和 Firewall Management Center，受访者表示只需点击界面升级防火墙，然后在 30 分钟后查看升级是否成功。

“从 ASA 转换到思科 Secure Firewall 后，我们的策略管理时间节省了 60% 到 70%。”
工程服务经理，IT 服务行业

受访者指出，思科 Secure Firewall 和 Firewall Management Center 可使用面向对象的系统，因此各项策略可以按类别和区域归类，而不需要使用冗长的访问控制列表 (ACL)。如今还可以自动部署和更新策略，无需手动更新每个设备。

“思科 Secure Firewall 会为你自动部署 90% 的策略。我们不再处理一次性配置。”
网络工程高级经理，科技行业

受访者指出，使用思科 Secure Firepower 从早期 FTD 升级到后期 FTD 后，可节省额外的时间。例如，来自金融服务行业的首席基础设施工程师指出，在早期的 FTD 中，策略部署需要 10 至 15 分钟，而在升级后的 FTD 中，部署时间降至约 3 分钟。

“思科 Secure Firewall 的策略管理直接且简单。Firewall Management Center 的 GUI 轻巧、简洁、直观。”
网络工程高级经理，科技行业

其中一名受访者并不使用 Firewall Management Center，而是使用云软件即服务 (SaaS) 的 Cisco Defense Orchestrator (CDO) 进行管理。关于 CDO，来自工业行业的资深基础设施架构师表示，“采用 CDO 非常简单便捷。因为我们的工程师已经熟悉 [Cisco Security Manager (CSM)]；他们已经可以操作命令行界面并构建各种宏。这比转换到其他供应商要容易得多，因为那需要学习新的上层概念，会变得很复杂。”

建模和假设。 对于该复合型企业，Forrester 做出如下建模：

- 34 个传统的 ASA 5500-X 防火墙被思科 Secure Firewall 替换。
- 该复合型企业可避免为所替换的每个传统防火墙部署和创建策略所需的 55 个小时工作时间。
- 以前每个季度升级每个防火墙需要 30 分钟，现在，该复合型企业可以节约大约 90% 的时间。
- 该复合型企业平均每天更新一次防火墙策略。通过转换到思科 Secure Firewall，该企业可将以往每次更新所需的 1 小时时间节约大约 95%。
- 网络安全运营 (NetSecOps) 专业人员的平均时薪为 65 美元。
- 68 个 FTD 防火墙升级至最新版本的思科 Secure Firewall。对于每天的策略更新，该复合型企业可节约在早期 FTD 防火墙所花费的 80% 的时间。
- 此外，该复合型企业还可节约更新虚拟防火墙策略所需的 80% 的时间。

风险。 防火墙管理的改进因以下因素而异：

- 现有防火墙的类型和数量。
- 由思科 Secure Firewall 替换的防火墙数量和部署速度。
- 是否决定在数据中心部署虚拟防火墙来处理东西流量和公共云流量。

结果。考虑到这些风险，Forrester 将此收益下调 10%，得出经风险调整后的三年期总现值 (按 10% 折现) 为 16.3 万美元。

防火墙管理改进

参考号	指标	数据来源	第 1 年	第 2 年	第 3 年
A1	替换原有防火墙的下一代防火墙数量	复合型企业；总数 102 的 1/3	34	0	0
A2	所节约的部署每个防火墙的时间	访谈	55.00	55.00	55.00
A3	所节约的更新每个 ASA 防火墙的时间	90%*17 小时/季度	61.2	61.2	61.2
A4	无需为 ASA 防火墙手动更新策略所节约的时间	95%*1 小时，每天一次*环境数量的 33%	114	114	114
A5	网络安全运营专业人员的时薪	复合型企业	65 美元	65 美元	65 美元
A6	小计：将原有的第 4 层防火墙部署并升级到下一代防火墙所节约的时间	((A1*A2)+(A3+A4))*A5	132,938 美元	11,388 美元	11,388 美元
A7	所更新的 FTD 防火墙数量	复合型企业；总数 102 的 2/3	68	68	68
A8	之前使用早期 FTD 防火墙部署策略所需的时间	访谈	0.25	0.25	0.25
A9	升级到后期 FTD 所减少的策略部署时间	访谈；从 15 分钟减少为 3 分钟	80%	80%	80%
A10	小计：在早期版本第 7 层防火墙上部署策略所减少的时间	365*A8*A9*A5*A7/102	3,163 美元	3,163 美元	3,163 美元
A11	虚拟防火墙总数	复合型企业	100	100	100
A12	每年更新虚拟防火墙策略所节约的时间	80%*266 小时/年	213	213	213
A13	小计：管理虚拟防火墙所节约的时间	A12*A5	13,845 美元	13,845 美元	13,845 美元
At	防火墙管理改进	A6+A10+A13	149,946 美元	28,396 美元	28,396 美元
	风险调整	↓10%			
Atr	防火墙管理改进 (经风险调整)		134,951 美元	25,556 美元	25,556 美元
	三年期总计：186,064 美元			**三年期现值：163,005 美元**	

安全工作流程改进

证据和数据。 部署思科 Secure Firewall 及利用 FMC 还帮助受访者简化了安全工作流程。决策者指出，基于 ASA 的设备需要多个独立的工具来进行跨防火墙跟踪和记录事件。结合 FMC，思科 Secure Firewall 的数据可整合到同一个位置，可以跟踪感染指标 (IOC) 和被拦截的入侵，或以一致的方式升级到某个安全信息和事件管理 (SIEM) 解决方案。得益于 FMC，受访者获得了在整个网络中以更相关的方式整体审查各种连接、事件和遥测的能力。

“过去，安全调查就像是只用一片图片来拼图。”
安全运营团队负责人，教育行业

通过 Firewall Management Center 进行整合，受访者表示可减少安全调查工作的时间成本。例如，来自安全服务行业的首席网络安全工程师指出，借助于 Secure Firewall 和 Firewall Management Center，调查时间从几个小时减少到 3 到 5 分钟。该受访者指出，之前必须通过多个系统来登录和协调数据，包括 SIEM 和电子邮件控制台。现在，他们可以登录到 FMC，并在该环境中查找特定的 IOC。

“Firewall Management Center 可作为单一的控制台来管理所有思科 Secure Firewall。它可简化管理，节约调查和整理事件以及对恶意活动做出应对决策的时间。”
工程服务经理，IT 服务行业

受访者还指出，他们的响应时间也减少了。例如，来自教育行业的安全运营团队负责人报告称，在投资购买思科 Secure Firewall 之前，他们每周都得向客户支持部门发送好几次工单。然后，支持部门会追踪用户并执行恶意软件检测，而这可能需要几个小时来进行扫描。接下来，受访者的团队将清理系统，甚至重新执行镜像。此过程可能需要一整天。使用思科 Secure Firewall 之后，受访者每月只需发送一次类似的工单，然后直接进入 FMC 解决问题，大约只需一个小时。

“我们原有的防火墙需要大量的日常管理来运行安全事件响应；这花费了大量的时间和金钱。使用 Firepower，我们可以节省大量的时间，同时大幅减少事件响应，因为大部分都被拦截了。”
安全运营团队负责人，教育行业

从早期版本的 FTD 升级到更新版本的受访者还体验到了与安全调查和响应工作流程相关的收益。来自金融服务行业的首席基础设施工程师报告称，早期版本的 FTD 仍允许通过 Firewall Management Center 来汇总安全警报视图，但升级之后，定义和触发功能都得到了改进。这位受访者还指出，与思科产品的进一步整合 (包括 AMP 和 Umbrella)，可因额外的相关性而获得更多收益。

“FMC 为我们提供了很大的可视性。现在，凭借这种可视性，我们会花更多的时间来寻求并确保一切正常运行，但我们在事件响应上所花的时间仍然比过去少。”
安全运营团队负责人，教育行业

如果充分利用 Secure Firewall 许可中内含的 SecureX，企业可通过可视性和定制功能进一步提高其安全团队的工作效率。例如，来自教育行业的安全运营团队负责人也指出，SecureX 允许个性化、可定制的仪表板，因此，他们的团队不仅可以获得额外的环境可视性，还可以向不同的用户显示其职责的最重要信息。

建模和假设。 对于该复合型企业，Forrester 做出如下建模：

- 每年的安全警报总数为 100,000 次。
- 其中 26% 需要安全分析师的注意。
- 在需要注意的警报中，70% 还需要调查。
- 思科 Secure Firewall 和 Firewall Management Center 用于调查警报的时间仅为 2.8 小时，可节约 49% 的时间。
- 在需要调查的警报中，10% 需要响应。
- 思科 Secure Firewall 和 Firewall Management Center 用于响应的时间仅为 6 小时，可节约 83% 的时间。
- SecureX 可为调查和响应工作流程节约额外的时间，第一年可节约 42%，第二年和第三年可节约 77%。

风险。 安全工作流程的改进因以下因素而异：

- 每年警报、需要注意的警报、需要调查的警报和需要响应的警报的数量。
- 网络安全运营专业人员的全额时薪。

结果。考虑到这些风险，Forrester 将此收益下调 15%，得出经风险调整后的三年期总现值超过 820 万美元。

安全工作流程改进					
参考号	**指标**	**数据来源**	**第 1 年**	**第 2 年**	**第 3 年**
B1	每年的警报总数	复合型企业	100,000	100,000	100,000
B2	需要分析师注意的警报	Forrester 研究；26%	26,000	26,000	26,000
B3	需要调查的警报比例	访谈	70%	70%	70%
B4	以前的平均调查时间	访谈	2.8	2.8	2.8
B5	使用 FMC 后减少的调查时间	访谈	49%	49%	49%
B6	需要响应的警报	访谈	260	260	260
B7	以前的平均响应时间	访谈	6	6	6
B8	使用 FMC 后减少的响应时间	访谈	83%	83%	83%
B9	使用 SecureX 后额外减少的调查和响应时间	访谈	42%	77%	77%
B10	安全专业人员的全额时薪	A5	65 美元	65 美元	65 美元
Bt	安全工作流程改进	((B2*B3*B4*B5)+(B6*B7*B8)+(B2*B3*B4*B5)+(B6*B7*B9))*B10	3,141,034 美元	4,335,864 美元	4,335,864 美元
	风险调整	↓15%			
Btr	安全工作流程改进 (经风险调整)		2,669,879 美元	3,685,484 美元	3,685,484 美元
	三年期总计：10,040,848 美元		**三年期现值：8,241,976 美元**		

减少重大安全漏洞和生产率损失的风险

证据和数据。 受访者还报告称，在部署思科 Secure Firewall 后，通过降低重大安全漏洞风险和相关生产率成本，他们获得了经济收益。

思科 Secure Firewall 和 Firewall Management Center 带来的增强的可视性，成为了受访企业改善安全态势的一种途径。例如，来自教育行业的安全运营团队负责人指出，“与传统的 ASA 防火墙相比，思科 Secure Firewall 为我们提供了更好的可视性。这一点尤其重要，因为用户正将越来越多的移动设备接入我们的网络，并通过网络访问打印等服务。升级到 Firepower 之后，我们可以获得更好的可视性，并能够过滤内部网络流量和南北流量。”

“我们看到，被拦截的威胁和 IOC 数量有了很大的改善。这是数量级的差异。以前，我们没有运行 Secure Firewall，所以我们的业务每天都面临风险。现在，我们获得了更大的可视性，从而风险也显著减小。我们现在感觉非常好。”

工程服务经理，IT 服务行业

改进的自动拦截功能也有助于降低潜在的安全漏洞风险。来自科技行业的网络工程高级经理指出，“Firepower 是[入侵保护系统 (IPS)]的行业领导者。我们能够增强我们的安全态势，并在问题萌芽时将其解决掉。对于每一个可能发生的事件，我们都能及早补救，从而节约资金。”该客户报告称，当从基于 ASA 的系统转换为思科 Secure Firewall 时，拦截性能提高了 80%。

“有了 Secure Firewall，我们立即消除了 80% 的威胁，且不需要任何额外的员工。”
网络工程高级经理，科技行业

重要的是，受访者还指出，通过将 FTD 防火墙更新到最新版本，可以改善拦截效率。来自科技公司的高级网络工程师表示，相比早期版本，升级到最新版本 FTD 的自动拦截效率提高了 10% 至 15%。

这位受访者还分享了一个关于自动拦截潜在影响的小故事：“我们曾经出现过一个可能会遭到社会工程攻击的漏洞，黑客能够从经过身份验证的用户那里窃取一个 24 小时访问令牌，而当黑客试图使用[令牌]时，思科 Secure Firewall 拯救了我们。我们能够检查安全态势，并确认攻击者是否在使用公司机器。Secure Firewall 自动拒绝了黑客的 VPN 访问。如果没有这个功能，黑客就会侵入我们的公司网络；我不确定那会对我们造成多大的损失。”

“思科 Secure Firewall 可提供一站式服务。它具有与其他工具整合的所有功能，可以提供相关数据，提高安全性。它拥有不同的风格；我们可以满足不同的吞吐量需求，并且支持垂直和水平扩展。它拥有解决当今安全风险所需的所有功能，且还在不断改进。”
高级网络工程师，互联网行业

该科技公司的高级网络工程师还指出，Secure Firewall 带来的一项安全收益是能够管理应用程序级别的访问：“我们看到，BitTorrent 在我们的客户网络上被广泛使用。通过利用 FTD 来拦截 BitTorrent，我们不仅防止了对其他客户的潜在威胁，而且还将线路占用率降低了约 400Mbps。”

受访者指出，除了应用层检测和拦截外，思科 Secure Firewall 使用基于 Snort 的自动威胁馈送，也帮助降低了企业遭受重大安全漏洞的风险。来自金融服务行业的首席基础设施工程师表示，“我们希望思科 Secure Firewall 能够提供更好的可视性和基于 Snort 的自动响应，以发现互联网上暴露出的服务器未打补丁等漏洞，并全面阻断恶意流量。”

通过利用 Secure Firewall 许可中内含的 SecureX，这些企业进一步降低了重大安全漏洞所带来的风险和成本。例如，来自金融服务企业的首席基础设施工程师指出，SecureX 使他们能够更清楚地识别安全问题和潜在威胁的根源。

“SecureX 可以为我们提供整个安全环境的单一视图。借助 FMC，我们可以看到我们所有的防火墙；借助 SecureX，我们可以看到 FMC，以及我们所有的整合思科安全解决方案。”

安全运营团队负责人，教育行业

建模和假设。 对于该复合型企业，Forrester 做出如下建模：

- 此前三年每年发生的重大安全漏洞数量。
- 重大安全漏洞的平均内部和外部合并成本为 968,480 美元。
- 外部攻击、内部事件和涉及合作伙伴和第三方的攻击/事件的比例为 79%。
- 思科 Secure Firewall 和 Firewall Management Center 可将采用传统 ASA 防火墙的企业的安全漏洞风险减少 80%。
- 思科 Secure Firewall 和 Firewall Management Center 可将以前采用基于 FTD 防火墙的企业的安全漏洞风险减少 15%。
- 该复合型企业 66% 的员工会受到每次安全漏洞威胁的影响；得益于思科 Secure Firewall 和 Firewall Management Center 降低了安全漏洞风险，因此挽回了 70% 的生产率。
- 普通员工的全额时薪为 40 美元。

风险。 重大安全漏洞风险的减少程度因以下因素而异：

- 目前每年出现的重大安全漏洞的数量。
- 重大安全漏洞的内部和外部总计成本。
- 外部攻击、内部事件和涉及合作伙伴和第三方的攻击/事件的比例。
- 现有防火墙的类型和数量。
- 受重大安全漏洞影响的员工数量、他们的全额时薪，以及当这些重大安全漏洞减少时他们恢复生产率的能力。

结果。考虑到这些风险，Forrester 将此收益下调 15%，得出经风险调整后的三年期总现值将近 350 万美元。

减少重大安全漏洞和生产率损失的风险					
参考号	**指标**	**数据来源**	**第 1 年**	**第 2 年**	**第 3 年**
C1	重大安全漏洞的平均数量	Forrester 研究	3	3	3
C2	每次重大安全漏洞的平均成本	Forrester 研究	968,480 美元	968,480 美元	968,480 美元
C3	外部攻击、内部事件和涉及合作伙伴和第三方的攻击/事件的比例	访谈	79%	79%	79%
C4	企业从 ASA 转换到 Firepower 的比例	复合型企业	33%	33%	33%
C5	使用 Firepower 后减少风险的比例	访谈	80%	80%	80%
C6	企业从早期 Firepower 转换到升级 Firepower 的比例	复合型企业	67%	67%	67%
C7	使用升级的 Firepower 后减少风险的比例	访谈	15%	15%	15%
C8	使用 SecureX 后额外减少风险的比例	访谈	14%	18%	23%
C9	小计：减少安全漏洞风险	(C1*C2*C3*(C4*C5+C6*C7))+(C1*C2*C3*C8)	1,162,951 美元	1,254,763 美元	1,369,528 美元
C10	受每次安全漏洞事件影响的用户数量	Forrester 研究	10,600	10,600	10,600
C11	普通员工的平均全额时薪	复合型企业	40 美元	40 美元	40 美元
C12	生产率提升	复合型企业	70%	70%	70%
C13	小计：通过减少安全漏洞风险提高的生产率	(C1*C10*C11*C12*C3*(C4*C5+C6*C7))+(C1*C10*C11*C12*C3*C8)	356,397 美元	384,534 美元	419,705 美元
Ct	减少重大安全漏洞和生产率损失的风险	C9+C13	1,519,348 美元	1,639,297 美元	1,789,232 美元
	风险调整	↓15%			
Ctr	减少重大安全漏洞和生产率损失的风险 (经风险调整)		1,291,446 美元	1,393,402 美元	1,520,848 美元
	三年期总计：4,205,696 美元			**三年期现值：3,468,249 美元**	

员工生产率的绩效收益

证据和数据。 借助思科 Secure Firewall，受访企业通常可通过两种方式提高员工生产率：1) 提供应用层的可视性和控制，从而提高网络性能；2) 减小策略更新带来的停机影响。

受访者指出，在实施思科 Secure Firewall 之后，得益于其在应用层控制网络访问的能力，企业网络性能下降的频率有所减小。客户报告称，在以前，当特定应用程序 (尤其是与视频媒体相关的应用程序) 产生很高的需求时，他们的网速经常会变慢，网络性能下降，乃至影响到员工生产率。来自教育行业的安全运营团队负责人表示，“网速每天都明显变慢，性能下降非常严重，每隔几周就影响到生产率。这主要发生在活动激增的时候，比如成千上万的用户观看某个视频的时候。”

由于思科 Secure Firewall 可让受访企业在包括应用层在内的多个层面设置网络安全策略，从而受访者对网络权限的控制更加细化。因此，这些企业可以更好地控制哪些应用程序及其何时可以访问他们的网络，防止高带宽应用程序导致的网络过载，改善网络性能，并提高员工的生产率。

“通过思科 Secure Firewall，我们可以更好地了解网络使用状况，并能够控制这种使用。我们目前有 4,000 多个不同的受控系统，所以如果我愿意，我可以看到[某个热门的视频社交应用程序]上周的使用情况。如果需要，我们可以制定规则禁止此类流量。”
安全运营团队负责人，教育行业

其他受访者指出，其公司通过减小策略更新中的人为错误所造成的负面影响来提高员工生产率。例如，来自 IT 服务公司的工程服务经理指出，由于使用 Firewall Management Center 可以更快地创建和更新策略，他们也能更快地收到更新是否成功的反馈。

在实施 Secure Firewall 之前，该公司需要花 15 分钟更新策略，另外还要花 15 分钟了解策略是否设置正确。如果没有设置正确，则还需再花 15 分钟来更新策略。有时，错误更新的策略会对员工生产率产生负面影响，特别是在生产环境中。

该工程服务经理指出，在使用思科 Secure Firewall 升级到最新版本的 FTD 后，策略更新和反馈的时间缩短到 3 分钟更新和 3 分钟反馈，并将更新、反馈和故障排除的总时间从 60 分钟缩短到 12 分钟，整体缩短了 80%。

建模和假设。 对于该复合型企业，Forrester 做出如下建模：

- 修复错误更新的策略需要整整一个小时 (发送错误更新需要 15 分钟，接收反馈需要 15 分钟，修复后更新和接收反馈需要 30 分钟)。
- 思科 Secure Firewall 和 Firewall Management Center 将修复错误策略的时间缩短了 80%。
- 假设该企业中平均有 2% 的员工会受到错误策略更新的影响。
- 在过去，网络性能会严重下降，大约每两周会影响员工 20 分钟的生产率。
- 使用传统的 ASA 防火墙保护时，约 33% 的员工会受到网络性能下降的影响。

风险。 员工生产率的绩效收益因以下因素而异：

- 受错误策略更新影响的员工比例。
- 网络性能下降的频率和时长会影响员工的生产率。
- 受网络性能下降影响的员工数量。

结果。考虑到这些风险，Forrester 将此收益下调 10%，得出经风险调整后的三年期总现值超过 410 万美元。

员工生产率的绩效收益

参考号	指标	数据来源	第 1 年	第 2 年	第 3 年
D1	之前使用早期 FTD 防火墙调整策略所需的时间	访谈	1	1	1
D2	使用更新的 FTD 调整策略所需的新时间	访谈	0.2	0.2	0.2
D3	受影响的平均员工数量	复合型企业	320	320	320
D4	普通员工的平均全额时薪	C10	40 美元	40 美元	40 美元
D5	生产率重获率	复合型企业	25%	25%	25%
D6	小计：更快的策略反馈带来的生产率提升	365*(D1-D2)*D3*D4*D5	934,400 美元	934,400 美元	934,400 美元
D7	因网络滥用而导致性能下降的频率	访谈	26	26	26
D8	性能下降的平均时长 (小时)	访谈	0.33	0.33	0.33
D9	受影响的员工数量 (仅限 ASA 迁移)	复合型企业	5,280	5,280	5,280
D10	普通员工的平均全额时薪	C11	40 美元	40 美元	40 美元
D11	生产率重获率	复合型企业	50%	50%	50%
D12	小计：终端用户员工的生产率提升	D7*D8*D9*D10*D11	906,048 美元	906,048 美元	906,048 美元
Dt	员工生产率的绩效收益	D6+D12	1,840,448 美元	1,840,448 美元	1,840,448 美元
	风险调整	↓10%			
Dtr	员工生产率的绩效收益 (经风险调整)		1,656,403 美元	1,656,403 美元	1,656,403 美元
	三年期总计：4,969,210 美元			**三年期现值：4,119,230 美元**	

降低和避免先前解决方案的成本

证据和数据。 通过将网络安全基础设施迁移到最新版本的思科 Secure Firewall，受访企业降低并节约了与原有网络基础设施相关的成本。毫不意外，受访者报告称，由于思科 Secure Firewall 替换了传统的 ASA 防火墙以及任何早期的 FTD 防火墙，从而避免了重新许可的成本。

除了替换物理防火墙和虚拟防火墙之外，由于思科 Secure Firewall 中包含 IPS，因此受访企业从 ASA 环境转换，还淘汰了之前部署的独立 IPS 解决方案，重要的是，受访者指出，当他们将防火墙从早期的 FTD 升级到思科 Secure Firewall 后，还可以节省额外的费用。由于这些最新的防火墙非常高效，受访者表示即便减少 20% 到 25% 的防火墙，也能达到同样的保护效果。

“对于传统的 ASA 防火墙，我们还需要在链接与防火墙之间部署 IPS。思科 Secure Firewall 内置有 IPS。我们不再需要管理两个不同的解决方案和两个不同的生态系统，并且，我们也不再依赖 IPS 工程师。”
网络工程高级经理，科技行业

建模和假设。对于该复合型企业，Forrester 做出如下建模：

- 通过用思科 Secure Firewall 替换传统的 ASA 防火墙，每年可减少 171,600 美元的独立 IPS 许可成本。
- 节约的独立 IPS 维护费用相当于 20% 的许可费。
- 将每周 2 名 FTE 各 30 分钟的 IPS 持续管理成本降低了 80%。
- 第一年节约了用类似类型的防火墙替换现有防火墙的成本，超过 130 万美元。
- 节约了每年 30 万美元的虚拟防火墙更换费用。
- 得益于思科 Secure Firewall 的高效，额外节约了 25% 的物理防火墙成本。

“从早期的 FTD 转换到思科 Secure Firewall 的最新 FTD 后，我们实现了更高的处理效率。思科 Secure Firewall 的效率比之前版本提高了 20% 到 25%，这意味着我们所需的防火墙数量减少了。”
高级网络工程师，互联网行业

“部署思科 Secure Firewall 之后，我们最终淘汰了那些价格昂贵、性能较差的 IPS 设备。”
首席基础设施工程师，金融服务行业

风险。 原有解决方案成本的降低因以下因素而异：

- 现有防火墙的类型和数量。
- 淘汰独立 IPS 解决方案的能力。

结果。考虑到这些风险，Forrester 将此收益下调 10%，得出经风险调整后的三年期总现值约为 260 万美元。

减少淘汰原有解决方案的成本

参考号	指标	数据来源	第 1 年	第 2 年	第 3 年
E1	减少的原有 IPS 成本	访谈	171,600 美元	171,600 美元	171,600 美元
E2	减少的维护费用成本	E1*20%	34,320 美元	34,320 美元	34,320 美元
E3	减少的原有 IPS 持续管理成本	访谈	53,539 美元	53,539 美元	53,539 美元
E4	节约的防火墙更换周期成本	复合型企业	1,616,980 美元	300,000 美元	300,000 美元
E5	节约的额外防火墙效率成本	复合型企业	329,245 美元	0 美元	0 美元
Et	减少淘汰原有解决方案的成本	E1+E2+E3+E4+E5	2,205,684 美元	559,459 美元	559,459 美元
	风险调整	↓10%			
Etr	减少淘汰原有解决方案的成本 (经风险调整)		1,985,115 美元	503,513 美元	503,513 美元
	三年期总计：2,992,142 美元			**三年期现值：2,599,074 美元**	

未量化收益

客户已获得但却无法量化的其他收益包括：

- **VPN 生产率和安全增强。**受访者还指出，思科 Secure Firewall 能够提高远程访问 VPN 的生产率和安全性。通过负载均衡，Secure Firewall 可在各组设备之间分布会话，确保性能、弹性和终端用户生产率。同样，通过 Secure Firewall 的本地认证，用户可在无法访问远程 AAA 服务器时保持生产率。在安全方面，思科 Secure Firewall 支持多证书认证，因此，除了验证终端用户身份之外，企业还可以验证远程设备是否由公司配发。
- **提高合规性。** 受访者还表示，思科 Secure Firewall 和 Firewall Management Center 为合规工作流程带来了无法量化的收益。来自金融服务公司的首席基础设施工程师表示，在部署 Secure Firewall 和 FMC 之前，合规报告较为困难。以前的解决方案缺乏简易的报告功能。然而，通过 Secure Firewall 和 FMC，其企业能够运行包含更多组件和更详细活动和视图的报告。受访者还提到，思科 Secure Firewall 支持传输层安全协议 (TLS) 1.3 加密标准。例如，来自互联网公司的高级网络工程师指出，由于行政管理负担，他们的团队目前还没有解密这些流量。在投资思科 Secure Firewall 之后，TLS 1.3 解密变得更加容易和高效。

“以前，我们无法获得针对很多不同配置组件的报告输出，但现在我们可以更容易地获得广泛和详细的报告。例如，我刚刚收到一份关于去年做出的每次访问权限控制变更的报告。它显示了所有页面视图的输出以及所做的变更。”
首席基础设施工程师，金融服务行业

- 改善**员工体验。**受访者还指出，他们公司的员工体验得到了改善。例如，来自互联网公司的高级网络工程师表示，“我们能够更好地控制我们网络上的应用程序访问权限，从而提高了员工的满意度。我们的本地 IT 团队过去很难追踪用户，所以难以要求他们停止使用特定的应用程序或阻止他们访问。有了 Secure Firewall 和 FMC，我们现在可以远程做到这一点。”

灵活性

灵活性的价值因客户而异。客户可能会先实施 Secure Firewall，日后再实现其他应用和业务机会——这样的情形不止有一种，包括：

- **额外的 Cisco Security 整合。** 除了 SecureX 的收益之外，受访者还指出，思科的安全产品生态系统带来了更高的灵活性，进一步增强了企业的安全态势。例如，来自 IT 服务公司的工程服务经理表示，“Cisco Security 具有深度整合的安全解决方案堆栈；这是其他供应商无法企及的优势。不仅仅是 Secure Firewall，还能将所有其他产品很好地整合在一起，让我们更好地建立防御。”
- **改善居家办公时的业务运营。**在员工转向居家办公后，思科 Secure Firewall 的控制措施还能帮助在 VPN 使用量激增时保持业务的平稳运营。来自互联网公司的高级网络工程师指出：“疫情期间，我们在全球范围的 VPN 并发连接量从平均 100,000 增加到近 350,000。为了保持我们网络的生存能力，我们使用思科 Secure Firewall 来设置限速，以促进业务的平稳运营。”
- **轻松过渡到云端。**最后，受访者表示，思科 Secure Firewall 让他们的云计划更容易实现。来自 IT 服务企业的工程服务经理表示，“我们需要一个单一的平台来连接现场、远程站点以及云端，但必须易于部署。其实，对于云平台，你只需要放一个 FTD 实例 ，将它安装在那里，然后连接到 Firewall Management Center。根本不需要花时间进行设置和部署。我们可以向这些实例推送标准化的策略。”

对具体项目进行评估时，灵活性也会被量化(详见附录 A)。

成本分析

应用于该复合型企业的量化成本数据

总成本							
参考号	成本	初始	第 1 年	第 2 年	第 3 年	总计	现值
Ftr	许可成本	6,000,690 美元	0 美元	0 美元	0 美元	6,000,690 美元	6,000,690 美元
Gtr	实施、策略制定和培训的成本	278,220 美元	7,924 美元	7,924 美元	7,924 美元	301,990 美元	297,924 美元
	总成本 (经风险调整)	6,278,910 美元	7,924 美元	7,924 美元	7,924 美元	6,302,680 美元	6,298,614 美元

许可成本

证据和数据。 客户分享了与其 Secure Firewall 投资相关的几项不同成本，包括：

- 物理防火墙的成本，取决于所需的吞吐量。
- 在数据中心或数据中心部署的虚拟防火墙，用于处理东西流量。
- 威胁防护、恶意软件防御和 URL 过滤许可证的成本。
- Firewall Management Center 许可证。

“对于思科 Secure Firewall 所整合的架构深度、工具集和功能，我们很难找到任何其他的同等选择。并且，除此之外，它的性价比也很有吸引力。”
首席基础设施工程师，金融服务行业

客户指出，他们无需额外成本便可部署思科 SecureX，因为它包含在 Secure Firewall 许可证中。

建模和假设。 对于拥有 100 个办公室和 4 个物理数据中心且需要冗余的复合型企业，Forrester 进行以下建模：

- 所有许可证按标价授权，期限为三年。
- 企业办公室防火墙的成本为 328,443 美元。企业办公室需要一个吞吐量达到 75Gbps 的大型企业级防火墙。
- 数据中心防火墙的成本为 978,067 美元。在每个数据中心，该复合型企业会部署两个物理防火墙的数据中心外围集群或高可用性服务包，以处理进出数据中心的南北流量。
- 100 个虚拟防火墙的成本为 2,628,561 美元。这些虚拟防火墙处理数据中心内的东西流量，以及数据中心与公共云平台之间的流量。
- 数据中心的物理和虚拟防火墙都有一个额外的威胁防护许可证，订阅费率期限为三年。这可提供额外的安全性，包含 Snort 3 以更好地检测和减轻感染和恶意流量的指标。

- 60 个分支机构防火墙的总成本为 1,848,160 美元。60 个办公室需要吞吐量达到 1.9Gbps 的 Secure Firewall。
- 39 个小型分支机构防火墙的总成本为 137,779 美元。其余 39 个办公室只需要吞吐量达到 650Mbps 的防火墙。
- 所有办公室防火墙都有额外的威胁防护、恶意软件防御和 URL 过滤许可证，订阅费率期限为三年。
- Firewall Management Center 也会获得适当规模的许可，以管理所有这些防火墙。Firewall Management Center 的成本为 79,680 美元。

风险。 思科 Secure Firewall 和 Firewall Management Center 的许可费因以下因素而异：

- 所需的虚拟防火墙数量。
- 所需的企业级防火墙数量。
- 数据中心的规模和数量以及对高可用性的需求。
- 分支机构办公室的规模和数量。

结果。由于 Forrester 直接与思科针对该复合型企业进行定价，因此我们没有对该成本进行风险调整，得出三年期总现值 (按 10% 折现) 为 600 万美元。

“通过思科企业安全协议，我们的总成本比逐项购买的成本更低。虽然 Firepower 占据成本的大部分，但是，我们可通过前所未有的产品获得额外的保护，从而节省了数十万美元。”

安全运营团队负责人，教育行业

许可成本

参考号	指标	数据来源	初始	第 1 年	第 2 年	第 3 年
F1	虚拟防火墙的成本	思科	2,628,561 美元			
F2	企业办公室防火墙的成本	思科	328,443 美元			
F3	数据中心物理防火墙的成本	思科	978,067 美元			
F4	小型分支机构办公室防火墙的成本	思科	137,779 美元			
F5	大型分支机构办公室防火墙的成本	思科	1,848,160 美元			
F6	Firewall Management Center 的成本	思科	79,680 美元			
Ft	许可成本	F1+F2+F3+F4+F5+F6	6,000,690 美元	0 美元	0 美元	0 美元
	风险调整	0%				
Ftr	许可成本 (经风险调整)		6,000,690 美元	0 美元	0 美元	0 美元
	三年期总计：6,000,690 美元			**三年期现值：6,000,690 美元**		

实施、策略制定和培训的成本

证据和数据。 受访者表示，在数据中心和办公室中部署和实现防火墙会产生内部时间和劳动力成本。其中第一项成本涉及在每个站点部署物理防火墙。第二项成本涉及跨各组防火墙创建和部署适当策略来实现这些防火墙。

“实现和部署非常迅速，也相对简单。真正的转换花费了 3 周时间，因为我们已经拥有设计，知道如何启动所有东西。”
安全运营团队负责人，教育行业

最后，受访决策者还指出了培训产生的相关时间成本。任何需要此类培训的员工都需要大约 2 小时的培训，以部署和管理思科 Secure Firewall。有些受访者指出，他们利用了思科安全专家主讲的公开培训视频。

建模和假设。 对于该复合型企业，Forrester 做出如下建模：

- 在 2 个数据中心和 100 个办公室中，平均每个需要 6 小时的实施时间。
- 平均每个防火墙创建策略需要 30 个小时。
- SecureX 需要 20 个小时来实施提前部署，并且每年需要 100 个小时来进行持续管理。
- 最初有 15 名员工需要培训；考虑到员工离职，每年需要再培训 3 名员工。

风险。 实施和创建策略的成本因以下因素而异：

- 要部署的思科 Secure Firewall 的数量。
- 最初需要培训的员工数量。
- 员工离职率。
- 网络安全运营专业人员的全额时薪。

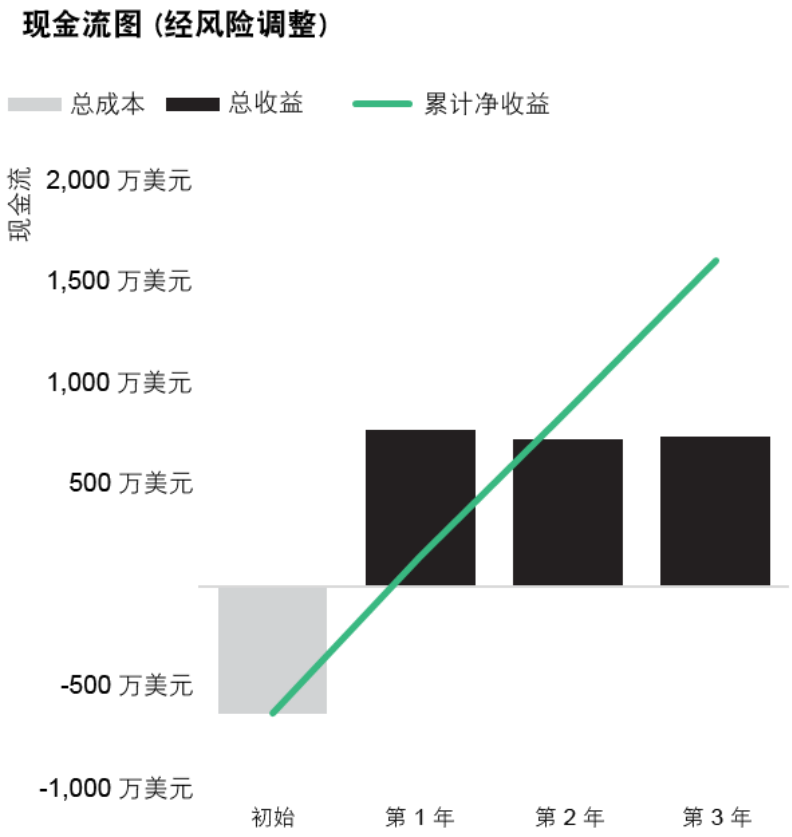
结果。考虑到这些风险，Forrester 将此成本上调 15%，得出经风险调整后的三年期总现值为 298,000 美元。

实施、策略制定和培训的成本

参考号	指标	数据来源	初始	第 1 年	第 2 年	第 3 年
G1	要部署的站点	复合型企业	102			
G2	在每个站点物理实现所需的平均时间	复合型企业	6			
G3	策略创建所需的时间	访谈	30			
G4	SecureX 实施和管理的时间	访谈	20	100	100	100
G5	需要培训的员工数量	访谈	15	3	3	3
G6	所需的培训时间 (小时)	访谈	2	2	2	2
G7	网络安全运营专业人员的平均全额时薪	A5	65 美元	65 美元	65 美元	65 美元
Gt	实施、策略制定和培训的成本	((G1*(G2+G3))+,G4+(G5*G6))*G7	241,930 美元	6,890 美元	6,890 美元	6,890 美元
	风险调整	↑15%				
Gtr	实施、策略制定和培训的成本 (经风险调整)		278,220 美元	7,924 美元	7,924 美元	7,924 美元
	三年期总计：301,990 美元			**三年期现值：297,924 美元**		

财务摘要

经风险调整后的三年期综合指标



"收益"与"成本"部分计算得出的财务成果，可用于确定该复合型企业所作投资的投资回报率、净现值和投资回收期。Forrester 在这项分析中假定年折现率为 10%。

这些经风险调整后的投资回报率、净现值和投资回收期，是通过对每个"收益"与"成本"部分中的未经调整结果应用风险调整系数后确定的。

现金流分析 (经风险调整后的估算值)

	初始	第 1 年	第 2 年	第 3 年	总计	现值
总成本	(6,278,910 美元)	(7,924 美元)	(7,924 美元)	(7,924 美元)	(6,302,680 美元)	(6,298,614 美元)
总收益	0 美元	7,737,795 美元	7,264,360 美元	7,391,805 美元	22,393,959 美元	18,591,534 美元
净收益	(6,278,910 美元)	7,729,871 美元	7,256,436 美元	7,383,881 美元	16,091,279 美元	12,292,920 美元
投资回报率						195%
投资回收期 (月)						10

附录 A：总体经济影响

总体经济影响 (Total Economic Impact，TEI) 是 Forrester Research 开发的一套研究方法，用于优化公司的技术决策流程，协助供应商向客户传达其产品及服务的价值定位。TEI 研究方法有助于公司向高级管理人员及其他关键业务利益相关方说明、论证并展现 IT 举措的实际价值。

总体经济影响方法

收益表示产品为企业带来的价值。TEI 研究方法在收益度量和成本度量上采用了相同的权重，这样便能全面考察技术对整个企业的影响。

成本是为了让产品实现所主张的价值或收益而必须支出的所有费用。TEI 中的成本类别涵盖现有环境中的任何增量成本，以便得出与解决方案相关的持续性成本。

灵活性表示在已经进行的初始投入基础之上，未来的一些额外投入所能获得的战略价值。具备获得该收益的能力可反映为一个可以估算的现值。

风险用于衡量收益和成本估值的不确定性，但须确定：1) 估值符合最初预计的可能性；2) 随时间推移来跟踪估值的可能性。TEI 风险因素基于“三角分布”。

初始投资栏包含“时间 0”或第 1 年初发生的成本，这些成本没有经过折现。所有其他现金流都会在年末按折现率折现。现值则根据每笔总成本和总收益的估算值进行计算。净现值在总结表中计算，是初始投资额与各年折现后的现金流之和。由于计算时可能会四舍五入，因此总收益、总成本和现金流量表中数值之和与现值计算结果可能有出入。

现值 (PV)

给定利率 (折现率) 下，成本和收益估算值的目前或当前价值 (折现后)。成本和收益的现值计入现金流的总净现值。

净现值 (NPV)

给定利率 (折现率) 下，未来净现金流的目前或当前价值 (折现后)。项目净现值为正数时通常表明应该进行相应投资，除非其他项目的净现值更高。

投资回报率 (ROI)

项目的预期回报率，以百分比表示。投资回报率的计算方法是净收益 (收益减去成本) 除以成本。

折现率

因考虑货币的时间价值而在现金流量分析中使用的利率。企业使用的折现率通常在 8% 到 16% 之间。

投资回收期

投资的盈亏平衡点。这是净收益 (收益减去成本) 等于初始投资或成本的时刻。

附录 B：尾注

[1] 总体经济影响 (Total Economic Impact, TEI) 是 Forrester Research 开发的一套研究方法，用于优化公司的技术决策流程，协助供应商向客户传达其产品及服务的价值定位。TEI 研究方法有助于公司向高级管理人员及其他关键业务利益相关方说明、论证并展现 IT 举措的实际价值。


FORRESTER®