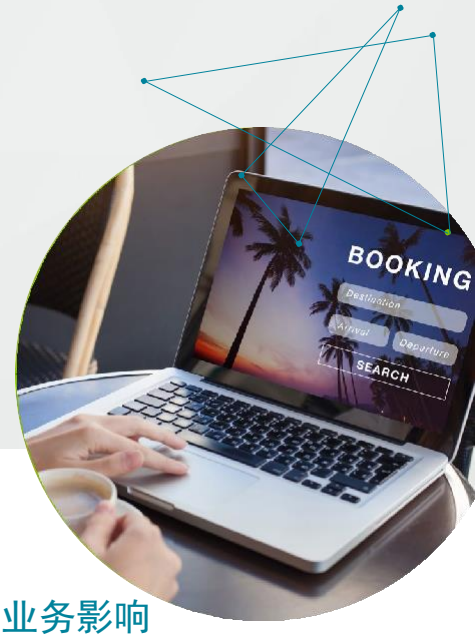
tufin 安全策略公司

案例研究

财富500强旅游公司的自动策略管理和审计报告



这家电子商务旅游公司在15个以上的国家或地区拥有25,000名员工，旗下拥有一些全球最值得信赖的在线旅游品牌。他们纷纷找到以为消费者和合作伙伴提供最终用户体验而闻名的Tufin，希望Tufin能帮助他们加快新服务启动的安全交付，同时有效管理跨异构IT环境中的安全策略。

挑战

为了在竞争激烈的全球在线旅游行业中取得成功，这家《财富》500强公司必须及时推出新的服务，迅速实施访问变更，并成功通过季度安全审核。对于跨混合、多供应商环境的安全策略，他们没有进行集中关注和管理。由于在网络操作、变更跟踪和创建审核跟踪上花费了大量时间，手工流程往往容易出错。

为了在动态市场中取得成功，在线旅游公司的网络和安全团队希望快速检测、分析和解决安全和运营网络的访问问题。他们必须登录各种网络安全管理控制台以找出阻塞流量或配置错误的规则，这可能需要耗费几个小时。由于缺乏对异构环境的整体认识，公司不得不快速关联来自多个网络资源的洞见，以作出有效响应。满足或超过定义的SLA以及安全性和合规性要求，对他们的团队来说至关重要。

这家在线旅游公司需要一个集中化解决方案，以增强其分散化网络（包含完全不同的平台和技术）的可见性。他们还需要加快服务交付，并快速解决部署在本地、公共和私有云上的50多个多供应商防火墙（如Palo Alto Networks、Check Point、Juniper和Cisco）中的任何问题。

为何选择Tufin

借助Tufin Orchestration Suite（TOS套件），他们开始在多供应商、异构环境中自动化并跟踪访问变更。他们可以快速排除访问问题以更快获得解决方案，并应用分段策略以增强安全性。他们成功降低了防火墙出现事件的次数和SLA时间，现在可以满足合规性需求。

凭借Tufin的支持，团队可以从他们分散化网络控制面板和警报的端到端可见性中获益，从而帮助他们检测和解决网络安全和运维问题。

业务影响

- 跨多个供应商的自动化合规性报告
- 显著降低防火墙变更所需资源数量
- 利用集成化安全工具提升效率和一致性

关键成功指标

- 将SLA从5天缩短至几分钟或几小时
- 一周内清除数千条规则，以降低CPU消耗
- 减少防火墙事件
- 通过联合可见性和统一流程，在安全、网络、SOC和NOC团队之间实现更广泛的协作

结果

随着安全状况的可见性增强，安全和网络团队可以确定工作的优先次序，以便将注意力转向价值更高的任务。他们现在可以立即发现网络安全和操作问题，例如规则中可能表明攻击或网络中断的异常峰值，从而快速进行检测和补救。然后，这些数据可以通过关联IPS/EDS数据来帮助验证真伪。通过将Tufin与他们的SIEM解决方案集成在一起，他们还会收到有关过度宽松规则和未使用规则的实时警报。SIEM集成确保利用最新的策略信息来强化背景因素并加速事件解决，其中他们可以看到任何事件的完整路径、哪些设备可能受到影响以及哪些策略可以促进流量。这些警报不仅帮助他们有效缓解风险，还确保他们的分段策略足够准确，从而使日常运维满足“零信任”目标。

通过自动化简化服务交付

在采用Tufin之前，该公司的网络团队必须手动访问个体管理控制台（如Panorama、FortiManager等），以完成规则变更、激活对应用的新访问或停用服务器等任务。这是一个费力且容易出错的过程。团队平均要花5天时间来完成一次防火墙变更，同时还要平均每天处理10-20个防火墙规则变更。这些变更相当冗长，或者需要一个独特的技能集，其中每个变更可能包含多达500行防火墙规则，最终会促成创立专门负责防火墙变更的团队。跨多个管理控制台实现手动变更，会导致成本中断、风险访问和合规性等问题。

通过Tufin的变更自动化，他们的网络团队能够在几分钟或几小时内自动化策略管理和实现访问变更，并显著减少防火墙的错误配置。将网络变更次数从5天减少至几分钟或几小时，降低了案例升级的次数。

> *“借助Tufin，我们只需要添加数据源、目的地、端口和服务，Tufin就会找到最佳路径、实施变更并验证更改是否按计划部署。尤其是在新冠疫情期间，当我们需要彻夜实施访问变更以启用远程工作人员时，Tufin为我们节省了大量时间。现在，我们的防火墙变更部署几乎“零事件”，所有操作都已实现自动化，并且对我们的生产环境“零影响”。Tufin的解决方案使我们的开发人员能够比以往更快地立即测试和部署他们的应用”*
>
> —公司的安全工程师

安全工程师补充道，“我们还将Tufin SecureChange与我们的ITSM票务系统ServiceNow集成在一起，票务在SecureChange中触发一个工作流，并将实现通知发送回ServiceNow，便于简单的集中化跟踪。Tufin设计师可以跨多供应商防火墙运营并突出规则和接口。通过与大多数网络安全设备集成，Tufin可以帮助我们实现精确的拓扑结构，使我们能够自动快速实施同样符合我们策略的变革。”

持续合规

审核一直是在线旅游公司的一个关键问题，尤其是在防火墙方面。审核人员试图删除过度宽松、未使用和不合规的规则。手动执行时，防火墙规则中的每一行都必须接受审查以及合规性检查。旅游公司开始依赖通过SecureChange提供的可定制工作流，并将其部署到访问更改和修改/部署对象组等众多用例中。

使用Tufin，该公司的安全团队自动进行防火墙规则审核。利用在Tufin中创建的合规模板，只需点击一下，就可以在任何区域的任何防火墙上运行。例如，自动快速删除未使用的规则和隐藏的规则，并将结果发送给审核人员。部署Tufin后不再需要手动流程，数千条规则一周内即可清除。

> *“有许多隐藏规则和冗余规则，很难直接从防火墙中删除。如果你说你必须删除一条规则，所有人都会跳出来问，‘你要破坏什么？’这就是Tufin帮我们做到的。”*

有了Tufin报告工具包，每个变更都会被记录下来，而团队可以轻松地为审核做好准备。每季度公司会对防火墙进行一次PCI-DSS审核，以确保没有任何防火墙规则违反PCI-DSS安全策略；特别阻止生产环境和非生产环境之间的任何流量。这就是Tufin报告功能在监控和证明合规方面非常有用的地方。

维护未来安全

凭借Tufin提供的增强可视性和自动化，这家在线旅游巨头强化了自身的安装状况，提高了运维效率，并提升了其在市场上的地位。未来他们计划使用Tufin漏洞管理应用（VMA）来优先考虑漏洞补救工作，并自动应用缓解控制。他们进一步计划部署Tufin IPAM安全策略应用（ISPA），自动同步他们的分段矩阵与其IPAM的网络地址。

有一点毋庸置疑：他们可以满怀信心地选择这些技术，并且确信他们的集中化安全策略将继续降低风险并提升整体安全性。

Tufin (NYSE: TUFN) 简化了世界上一些由数千个防火墙、网络设备和新兴混合云基础架构组成的最大、最复杂网络的管理。企业选择公司的Tufin Orchestration Suite™ 来提高应对不断变化的业务需求时的敏捷性，同时保持稳健的安全状态。
该套件缩小了攻击范围，并满足了提高安全可靠应用连接可见性的需求。自成立以来，Tufin的网络安全自动化系统已拥有超过2000家客户，它不仅使企业能够在几分钟而不是几天内实现变更，还可以改善其安全状态和业务敏捷性。

tufin
安全策略公司

DP20211006