tufin

应对企业云安全挑战实用指南

Tufin云安全白皮书

执行摘要

执行摘要

在新的云技术和流程的支持下，现代企业对客户需求和竞争压力的反应比以往任何时候都更迅速。但是，IT使用的传统安全工具和流程是为较慢、较不动态的环境而设计的。这导致许多公司为了敏捷性牺牲安全性。为了保护企业，IT负责人需要更深入地了解云安全挑战的根源，以及如何通过提高可视性、自动化和控制来应对这些挑战。通过采用云原生和DevOps实践，IT安全可帮助企业建立敏捷性和安全性之间的平衡。

企业迁移到云；对安全问题的担忧随之而来

毫无疑问，随着企业迁移到云，结构性转变正在发生。77%的企业已在云中至少拥有一个应用或部分计算基础架构。到2020年， 83%的企业工作负载将在云中。

66%的IT专业人士表示，采用企业云计算策略时，安全性是他们最关注的问题。这并不是因为云自身不太安全。恰恰相反，公共云基础架构工作负荷的事件比传统数据中心的同类事件少60% — 很大程度上是因为它们在分担责任模式下运营，并且提供商受到多种合规和法律要求约束。

但安全专业人员的担忧是合理的。有预测表明，从现在到2022年，至少95%的云安全故障是因客户 (即公共云基础架构买方) 过失导致的。

本白皮书将帮助企业更好地了解云安全挑战的根源，以及如何通过增加可视性和更有效的安全控制来应对这些挑战。让我们深入了解一下。

为什么企业陷入云安全困境

我们最近与ESG Research进行了一项调查，发布了报告《网络安全运营变革：引入自动化、云计算和DevOps》，提供全方位的视角，了解当今企业面临的云安全挑战。 超过一半的安全专家表示，如今的网络安全运营比两年前更具挑战性。

为何？有以下几个原因：

- 更多连接的设备
- 更多使用云
- 更频繁严重的网络攻击
- 更多漏洞

该报告以及其它最近的行业研究表明，混合云计算和敏捷开发都在增加，企业也开始使用容器和Kubernetes，使情况进一步复杂化。习惯于本地环境的IT团队通常不熟悉新云平台的最佳实践和不同的安全控制，从而可能导致错误配置，增加业务风险。例如，团队可能不慎将访问云资源的范围配置得过于广泛，从而为直接攻击或从入侵服务漫游带来可趁之机。传统环境与云原生环境之间的差异使混合IT运营具有挑战性，增加了安全问题。

此外，敏捷开发需要DevOps和IT团队尽早地将安全检查内置于开发流程。若能顺利完成，代码发布就能更快更安全。但这不易完成。

成功克服企业所面临的障碍需要什么？正如ESG报告指出的那样：“CISO必须整合网络安全运营来应对这些挑战，获取对云工作负载的可视性，管理安全策略并自动化安全流程。”

听起来很简单，对吧？

“公司对不擅长的领域认知不足”

症结在于：许多机构并不充分了解其云基础架构。企业管理协会(EMA) 发布的另一份研究报告表明企业对可视性存在严重的认知不足。

例如，98%使用人工安全性检查流程的机构认为他们对应用在基础架构中的通信具有中等至高度的可见性。97%的机构表示，他们对请求的更改会对运行的应用可能产生的负面影响具有中等至高度的了解。这看起来还算不错…

但是，其中58%的机构承认，他们无法保持标准化安全策略是发生安全或运营事件的重要因素。其中34%的机构表示，安全设备配置错误是造成连接中断的主要原因。我们在应用测试中也看到了类似现象。

这说明了什么？公司对不擅长的领域认知不足。他们可能认为进行人工检查时有足够的可见性，但这很可能是因为他们并不清楚完全的基础架构可视性是怎样的。几乎有一半的受访公司甚至承认，将业务关键型应用迁移到云时，他们才发现并不完全理解应用通信流程，表明其可视性不足。

应对企业云安全挑战

如今的企业现状与上面所述大致相同。那么如何获得对云环境的可视性，以确保安全性呢？

简而言之，机构须将安全性集成至整个网络（包括本地、私有云、公共云和微服务）中，并内置到开发团队的持续集成和部署（CI/CD）的日常流程中。 有效保护网络的方法是注重安全策略。

正如EMA报告所说：“安全性不应限制业务，而应为业务服务。许多机构似乎忘记了安全策略不受限于，但须由业务流程来驱动。”

让我们探讨一下这意味着什么。

敏捷性驱动方案：企业云现状

企业正在逐渐迁移到云。以下阐明了这一趋势的原因和对企业优先事项的影响。

对速度的需求和混合基础架构现状

数字化转型和业务敏捷性对企业保持竞争力十分必要，是所有前瞻性企业的优先事项。从而推动了对云的使用和新开发实践。

尽管传统应用仍十分重要和普遍，大型机构正逐渐转向公共云基础架构，以满足现代商业世界的敏捷性需求。由于对传统基础架构的大量投资，所以并不能直接淘汰和替换原有架构，由此产生了混合和多云环境，公司拥有了难以管理的复杂分散的环境。在制定策略时—包括安全性策略，公司须考虑如何管理混合环境。

DevOps的兴起

DevOps通常被认为是职位名称，但更准确地说，它是机构内的文化运动。DevOps包含自动化软件开发、测试和部署流程的实践，使企业在不牺牲可靠性或质量的情况下更快地发布软件。

由于DevOps要求团队考虑迭代和不断改进（而不是一次性开发），因此必须使用自动化。自动化是使开发和运营团队的工作流比以往任何时候都更有效率的基础。这些敏捷团队能够快速开发并迭代可带来业务价值的新应用和服务，从而使DevOps在当今的企业中越来越受欢迎。

随之而来的挑战是，DevOps团队期望的速度比IT或安全团队使用传统流程的速度更快。例如，开发人员无法等待数周的时间配置基础结构并更新防火墙规则，但这却是大多数公司的现状。这使得NetOps、SecOps和DevOps在配置时出现矛盾，必须进行协调以平衡速度/敏捷性和安全性的目标。所有团队须紧密合作建立能够快速发布安全代码的流程。

“模式 2” IT

DevOps与现代软件架构（微服务）的结合使机构能够获得传统IT模式（Gartner称之为“模式1 IT”）无法实现的敏捷性。模式2 IT取代了整体架构和瀑布式开发模型。Gartner如此描述模式2 IT：“模式2是探索性的，尝试解决新问题并对不确定性区域进行优化。作出假设，在短迭代的流程中测试和调整，可能采用最小化可行产品（MVP）方法。”

由于很难完全弃用模式1，企业逐渐采用双模式IT实践。与DevOps一样，模式2 IT可实现敏捷性。但是安全过渡到云是企业取得长期成功的关键。

企业云安全的五大障碍

当然，这说起来容易做起来难。根据我们的经验，企业安全地迁移到云有五个主要障碍。可采用正确的方法来克服这些障碍。全面了解障碍以制定安全策略是关键所在。

可视性

采用有机云可使获得和保持可视性具有挑战性。因为事件在企业内不时涌现。传统安全实践通常在部署周期中规避或行动得太晚。此外，传统实践往往需要人工干预，甚至缺乏对云和云原生安全控制的支持。因此，IT无法可靠地衡量风险。

合规性

在本地已不易满足合规性要求，云又增加了复杂性。现有的工具和实践很难在不影响效率的情况下控制云。例如，需要遵守HIPAA合规性要求的企业必须始终了解所有PHI数据的存储、移动或访问位置。有一些众所周知的最佳实践可用于在传统环境中促进合规性。在云中实施类似的保护需要不同策略，例如，使用有效满足HIPAA要求的云原生控制。企业必须了解云的工作原理以正确实施这些控制。

自动化

企业安全团队担心自动化是“失去控制”的代名词，因此自动化可能被视为云安全的障碍。实际上，自动化可对安全问题进行早期检测和纠正。安全策略变更自动化提供了一致的安全规则和衡量的合规性。若能正确使用，自动化可使安全专业人员从繁琐的任务中解放出来，使他们可以专注于更高价值（通常更有趣）的工作挑战。

开发与安全的优先级冲突

DevOps团队通常希望开发进程越快越好，而安全团队则专注于全面审查，确保遵守策略。每个团队都努力地履行各自的职责，并实现业务价值目标。但是，它们的常用流程往往只适合独立工作，而不是协作。

混合IT

混合或“双模式” IT（如前所述）是许多企业的现状，但这增加了复杂性，尤其是需要不同的安全实践。尽管企业现有的安全工具和实践对于模式1（可预测、易于理解的传统IT基础架构和应用）可能已足够，但它们不适用于模式2。使用双模式IT，关键是要理解并接受对模式1有效的安全实践很少能适用于模式2。

例如，在传统网络中，我们将IP地址分配给物理机和虚拟机。在其上运行的工作负载往往会停留很长时间（数月甚至数年），不会经常交换IP地址，因此很容易使用这些标记从安全角度追踪情况。

相比之下，云原生工作负载是高度动态的，并且可能比传统应用更大规模部署。此外，云原生工作负载是由一组服务构建的，每个服务都是单独部署的。作为安全性参数，静态IP集合对于这种复杂多变的环境而言过于呆板。

这只是传统安全实践无法适用云基础架构的一个例子。

此外，即使是采用云就绪的企业，也经常发现受本地应用和资源的负累，并且这种情况可能会持续数年甚至数十年。机构将拥有需要访问本地资源的云原生应用，这意味着需要采用适用混合基础架构的安全策略。

未来之路

到此，我们了解了使用云将面临的挑战，那么未来之路是怎样的？

我们认为，无论是在本地、私有云、公共云和/或微服务中部署应用，都必须将安全性集成到整个IT环境中，以确保获得最佳实践。安全性不应是开发后或附加的工作，需要内置于日常流程中。

为实现这一目标，企业应采取以下四个关键步骤。

任命安全代言人

若无人专门负责一项特定的任务，那任务将无法完成。将此原则应用于安全性，我们建议指定企业内部安全代言人。其目标是在整个机构（从NetOps、SecOps到DevOps）促进协作。安全代言人的宗旨是帮助团队解决和避免安全问题，以使企业盈利。

安全代言人可以是企业的CISO、安全从业人员，或者是对安全性有深刻了解的DevOps团队成员。应积极推行安全性，并深刻理解安全性对业务成功的重要性。

安全代言人是公司的安全代表，定期进行安全主题的培训，确保公司员工了解应向谁寻求安全问题的帮助。

请注意：安全代言人不应成为机构安全的唯一负责人。成功取决于让所有团队成员承担安全责任。安全代言人的工作更多是对安全价值进行培训，并促进跨部门协作，以便所有员工都采用安全最佳实践。

需要确保DevOps和安全性的双向交流。若不深入了解DevOps及其工具，安全人员就无法推行适用的安全措施。安全人员不仅要培训DevOps人员有关安全最佳实践的知识，还应与DevOps合作完成与DevOps实践无缝配合的安全部署。

使用Guardrails: 专注策略

传统的安全策略往往范围很广。但是在云中，随着应用和服务的激增，必须具体化。因此，将传统安全模型应用于云的挑战在于安全策略很快变得过于复杂且难以使用。

我们建议使用“guardrails”，一套可以广泛应用于多个应用和资源的策略规则。例如，安全团队可定义限制公共访问数据存储的guardrails，或者限制访问开发/测试环境的guardrails。安全团队定义guardrails，保护部署在云中的数据和应用。构建自动执行服务通信权限的guardrails很重要，也称为“分段策略”。为了获得更好的控制，可定义“微细分”规则，将guardrails扩展到更细微的级别。

我们还建议guardrails以应用为中心（而不是基础架构）。这使企业能够查看业务应用和安全策略错误或风险，从安全角度快速了解正在发生的情况。

实施的guardrails越简单，就越有可能在整个环境中正确实施。安全策略通过一致的guardrails实现，使团队专注于高价值工作，而不会因复杂的安全策略而降低效率。

采用新工具

要实现企业云安全，需要采取哪些措施？其中之一是是采用适用的技术。

迄今为止，机构已经测试了多种用于云安全的技术方法，其中一些方法还不够完善，包括:

- 内部工具和脚本（难以维护和实施）
- 专注于安全运营的技术解决方案（缺乏效率且难以扩展）
- 防火墙（当网络边界消失时无法防御）
- 仅适用云的安全工具（无法保护混合环境并导致更多的安全孤岛）

我们建议企业选择既适合云又适用混合环境的解决方案。更具体地说，企业的云安全解决方案应有五个关键属性。

- **云原生：**选择与企业云和Kubernetes平台无缝集成的工具。与传统安全工具不同，云原生解决方案支持诸如安全组、IAM策略、公共云提供商的负载平衡器之类的控制，并支持Kubernetes的网络和安全功能。除了这些基本控制之外，使用可为企业提供业务所需的可视性和洞察的云原生安全工具。
- **以应用为中心：**由于存在大量信息，因此很难在基础架构级别管理云安全性。我们建议选择以应用为中心的解决方案。企业可查看策略错误或风险，并与部署应用的人员交流。这使得在复杂的机构内确保安全性容易得多。
- **多云和混合：**如今，大多数企业都拥有多云环境，这意味着工作负载分布在各个云实例和提供商。企业通常还拥有传统本地基础架构，不可能立即弃用。因此，请选择能够在混合和多云基础架构中使用的安全工具。
- **内置于交付流程：**正如我们在本文中所讨论的，持续开发和持续集成对于当今企业成功至关重要。为确保企业不会减慢这些流程的速度，请选择可以轻松集成到交付流程的安全工具。
- **易于部署：**若工具需要长期部署和微调以及大量的团队资源来管理，则很可能缺乏效率，容易出现安全漏洞。

在评估云安全工具时，请检查是否满足了这五个属性，以及它们是否达到全方位保护基础架构的最终目的。

评估成果

任命安全代言人，采用guardrails并选择新安全工具后，企业需要评估成果并不时改进。以下是我们建议注意的一些关键指标:

指标	之前	之后
用于安全检查的时间		
事件的数量		
DevOps流程中的 安全检查次数		
安全例外的数量		

我们建议企业追踪这些KPI，因为它们可证明所采用措施的有效性。可帮助企业确保合规和持续的安全预算以支持程序。

结论：无需畏惧云

企业不必担心过渡到云。尽管云可能会在安全方面带来更多的复杂性，但在速度和敏捷性，节省的时间和金钱以及提高效率方面的作用是显而易见的。

随着越来越多的大型机构迁移到云，是时候重新考虑如何确保安全性和敏捷性的途径了。我们认为，安全性必须集成到整个环境（从本地、云到微服务）以及应用开发和部署流程。实现此目标的最佳方法是了解传统安全要求与云安全要求之间的差异，并通过可靠且易于执行的安全策略实施最佳实践。

企业可使用此白皮书作为指南，获得使用云的益处，同时在整个环境中实现有效性和安全性，无论其差异性或复杂性。

Tufin®是企业网络安全策略编排的引领者。福布斯全球2000强企业排名前50位的公司中，超过一半是Tufin的客户。Tufin帮助简化了全球一些最大型复杂网络的管理。这些网络包括数千个防火墙和网络设备以及新兴的混合云基础架构。企业选择屡获殊荣的Tufin Orchestration Suite™，在不断变化的业务需求下提高敏捷性，同时保持稳定的网络安全状态。该套件减少了攻击面，满足了对安全和可靠的应用连接的更大可视性的需求。其网络安全自动化功能使企业能够通过风险分析和持续的策略合规性，在几分钟内实施更改。Tufin为多个行业和地区的2000多家客户提供服务。Tufin的产品和技术在美国和其他国家受到专利保护。更多信息请访问www.tufin.com。

关注Tufin Twitter: @TufinTech Read

关注Tufin 博客: Suite Talk

关注Tufin 微信公众号：@Tufin_Official