tufin The Security Policy Company.

Tufin 云安全指南

直面企业云安全挑战

执行摘要

借助新的云技术和流程，现代企业对客户需求和竞争压力的响应能力超过以往任何时候。然而，IT部门使用的传统安全工具和流程是为慢速、低动态情境设计的，导致许多企业为了敏捷性而放弃安全性。要保护企业，IT领导者需要更深入地了解云安全挑战的根源，以及如何通过增加可见性、自动化和控制来解决这些挑战。通过采用云原生和DevOps实践，IT安全可以帮助企业恢复敏捷性和安全性之间的平衡。

企业云迁移及安全问题跟踪

毫无疑问，随着企业向云端迁移，结构性转变在所难免。事实上，根据2021年Flexera（富莱睿）发布的《云计算现状报告》，2020年，超过50%的企业将工作负荷转移到云端。

不过，根据451 Research的调研，46%的企业之声（VoE）报告受访者表示，安全性和合规性是他们在采用云原生技术时最担心的问题。目前，许多安全、网络和云运营团队都需要在一个多云混合世界中平衡安全性和敏捷性。

专业人士担忧的安全问题并非空穴来风，据Gartner（高德纳）预测，到2025年，至少99%的云安全问题源自配置错误。

这份白皮书将帮助企业更好地理解云安全挑战的根源，以及如何通过增加可见性和更有效的安全控制来有效地解决这些挑战。以下是白皮书的具体内容。

为什么企业难以实现云安全

在ESG Research进行的一项调查中，结果报告《网络安全运营转型：采纳自动化、云计算和DevOps》全方位透视了当今企业中不断涌现的云安全挑战。过半的安全专业人士表示，当前网络安全运营比两年前更具挑战性。

为什么？归结起来有以下几个因素：

- 更多联网设备
- 不断增加的云采用
- 更加频繁和严重的网络攻击
- 更多漏洞

该报告以及其他最新的行业研究表明，混合云计算和敏捷开发都处于增长期，同时企业中容器和微服务的使用也在增加，这无疑令形势变得更加复杂。。在公共云环境中工作与传统网络显著不同。习惯于本地预置环境的IT团队往往不熟悉云最佳实践，对云安全控制的误解可能会导致最终用户出错，从而增加业务风险。例如，对于云资源的访问，团队可能会意外配置得过于宽泛，从而为直接攻击或来自破坏服务的横向移动创造机会。传统和云计算环境之间的差异导致混合IT程序的操作具有挑战性，并增加了随之而来的安全问题。

此外，随着我们将更深入地探讨，敏捷开发要求DevOps和IT团队找到方法，尽早并经常地在开发管道中进行安全检查。如果操作得当，代码发布将变得更快、更安全，但挑战也会出现。

如何成功克服企业所面临的障碍呢？正如ESG报告所指出的，“CISO必须通过整合网络安全操作来解决这些额外的挑战，以实现云工作负荷的可见性、安全策略的管理以及安全流程的自动化。”

听起来足够简单，对吧？

“公司不知道自己不知道什么”

问题在于：大多数公司对其云基础设施中正在发生的事情缺乏足够的可见性。另一份来自企业管理协会（EMA）的研究报告发现了一些令人不安的统计数据，表明人们对可见性的构成有很深的误解。

例如，98%的使用人工安全检查流程的公司认为，他们对应用程序如何在其基础设施中通信具有中等到较高的可见性。另有97%的公司表示，对于所请求的变更可能会对正在运行的应用程序产生何种负面影响，他们拥有较高或中等的可见性。到目前为止还不错……

然而，58%的使用人工安全检测策略的公司承认，他们无法维护标准化的安全策略，这是导致安全或操作事故的一个重要或非常重要的因素。其中，34%的公司表示，安全设备配置错误是导致中断的主要原因。我们在应用程序测试中也发现了类似情形。

结论呢？公司不知道自己不知道什么他们可能认为在进行手动检查时，他们有足够的可见性，但这可能是因为他们没有认识到完整的基础设施可见性。近一半的受访者承认，在将业务关键型应用程序迁移到云端时，他们发现自己并没有完全理解应用通信流，而这表明他们的可见性还不够。

直面企业云安全挑战

如果您现在是一名企业运营人员，很可能我们在上面绘制的图片对您来说很熟悉。但是您可能会思考，如何才能获得云环境的可见性以确保安全？

简单来说，企业必须将安全集成到整个设施中（包括本地预置、私有云、公共云和微服务）以及开发团队的日常流程中，用于实现渠道的持续集成和部署（CI/CD）。此外，有效覆盖企业整体设施的唯一方法是聚焦于安全策略。

正如EMA报告所指出的，“安全不应限制而应促进业务……在继续向前发展的进程中，许多公司似乎忘记了安全策略并没有绑定，必须由业务流程驱动。”

让我们来探讨一下这意味着什么。

采用敏捷性驱动：企业云现状

企业正日益进行云迁移。以下是促成这一举动的动机，及其对业务优先级的影响。

速度需求和混合云现实

数字化转型和业务敏捷性是当今企业保持相关性和竞争力的必要条件，也是所有前瞻性企业的优先执行事项。焦点在于推动云采用和新的开发实践。

虽然遗留应用程序依然至关重要且继续存在，但大型企业正日益转向公共云基础设施，以满足现代商业世界对敏捷性的要求。由于旧有基础设施中有大量投资，不能简单粗暴地淘汰和替换。由此产生的混合和多云环境成为新型计算模式的固有组成部分。最终，您将面对难以管理的复杂和碎片化环境。在制定包含安全性的战略决策时，必须考虑如何管理混合环境。

优化DevOps

DevOps通常是一个职位名称，但更准确地说，它是一种企业内开发方式。DevOps包含自动化软件开发、测试和部署流程的实践，最终赋权企业在保证可靠性和质量的情况下更快地发布软件。

DevOps需要团队考虑迭代和持续改进（相对于“一步到位”的版本），因此，DevOps的成功离不开自动化。自动化是使开发和运营团队之间的工作流比以往任何时候都更高效的支柱。这些敏捷团队能够加速开发和迭代新的应用程序和服务，以推动主要的业务价值，从而使DevOps在当今企业中越来越受欢迎。

这带来的挑战是，DevOps团队通常希望行动速度超过处理传统流程的IT或安全团队。例如，开发人员不能等上几个星期才准备好基础设施并更新防火墙规则，但这是大多数公司目前的现实。这常常使NetOps、SecOps和DevOps在部署时产生分歧，必须协调以平衡速度/敏捷性和安全性的目标。所有团队都必须学会紧密合作，并构建能够快速发布安全代码的流程。

“模式2”IT

DevOps和现代软件架构（微服务）的结合使企业能够获得传统IT范式（Gartner称之为“模式1 IT”）无法获得的敏捷性。模式2 IT取代一体化架构和瀑布式开发模型。Gartner对“模式2 IT”的描述如下：“模式2是一种探索和尝试，旨在解决新问题并优化不确定领域。此类举措通常从假设开始，然后在涉及短迭代的过程中测试和调整，并可能采用最小可行产品（MVP）方法。”

虽然很难完全摆脱模式1，但企业越来越多地采用双模式实践。Mode 2 IT与DevOps一样支持敏捷性，但安全地过渡到云才是企业长期成功的关键。

企业云安全的五大障碍

当然，任何事都是知易行难。根据我们的经验，企业要安全地实现云迁移，需要解决五大障碍。采用正确的方式可以克服这些障碍，但要建立全面的安全策略，关键是要充分理解这些障碍。

可见性

采用有机云会使获取并保持可见性变得具有挑战性，因为企业中到处都是这样的实例，来来去去并没有得到任何处理。在部署过程中，经常忽略或延迟使用传统的安全实践。此外，遗留实践往往需要人工干预，更糟的是，缺乏对云及云原生安全控制的支持。因此，IT人员无法可靠地度量风险。

合规性

本地很难实现合规性，而云端又增加了一层复杂性。现有工具和实践很难在不全面降速的情况下对云施加控制。例如，HIPAA合规企业必须随时了解PHI数据的存储、移动或访问位置。幸运的是，有一些在传统环境中执行合规性的知名最佳实践可供参考。但是，在云端实施类似的保护需要使用不同的策略，例如，可以非常有效地满足HIPAA要求的云原生控制。不过，必须理解云如何工作才能正确地实施这些控制措施。

自动化

在企业内部，安全团队一直担心自动化等同于“失控”，因此自动化可能是云安全的障碍之一。实际上，自动化能够在安全问题进入生产环节之前，对其进行主动检测和纠正。安全策略变更的自动化为安全规则的一致应用及衡量合规性提供了途径。如果操作得当，自动化可以将安全专业人员从常规任务中解放出来，使他们能够专注于更高价值（通常也更有意义）的挑战。

部署与安全优先级之间的冲突

DevOps团队通常希望尽可能快地行动，而安全团队则专注于确保没有任何未经审查的输出，以确保其符合安全策略。每个团队都会各自努力履行职责，并满足提供业务价值的目标。然而，其旧流程会让每个部门几乎处于孤立状态，而不是相互协作，而不是尽早且经常地针对不安全的代码进行协作。这些双重需求也增加了DevSecOps的构建，以确保企业能够平衡安全与发展的需求。

混合IT

混合或“双模”IT（如前所述）是当今许多企业的现实配置，但它会增加复杂性，尤其是在需要不同安全实践的情况下。虽然企业中现有的安全工具和实践对于模式1（可预测、易于理解的遗留IT基础设施和应用程序）而言可能已经足够，但它们并不适用于模式2项目。对于双模式IT程序，关键是理解并接受“在模式1项目中运行良好的安全实践很少会延续到模式2中”的事实。

例如，在传统网络中，我们会为实体机和虚拟机分配IP地址。在这些机器上运行的工作负荷往往会持续很长时间（数月甚至数年），因此不会经常更换IP地址。从安全性的角度来看，这些标记是跟踪正在发生的事情的一种简单方式。

相比之下，云原生的工作负荷是高度动态的，可比传统应用部署更大的规模。云原生工作负荷由一组服务构建，其中每个服务都会单独部署。作为安全参数，一组静态IP对于这样高度动态的环境而言过于僵化。

这只是传统安全实践在云基础设施领域不符合标准的示例之一。

此外，即使已经准备好接受云优先方法的企业，也经常发现自己背负着本地应用和资源造成的可能会持续数年甚至数十年的负担。企业将拥有需要访问本地资源的云原生应用程序，这意味着他们需要采用跨混合基础设施的安全策略。

未来的道路

如果您阅读到这里，则表明您已经认识到了云挑战，那么未来的道路是怎样的？

从较高的层次上讲，我们认为，无论您是在本地部署应用程序，还是在私有云和/或微服务中部署应用程序，安全性必须集成到整个IT环境中才能达到最佳成功标准。安全不能是事后想法或附加物，而是需要与日常流程和行动紧密结合。

要实现这一目标，每个企业都应该采取四个关键步骤。

赋权安全倡导者

生活的方方面面都是如此。如果没有人专门负责指定的任务，该任务就无法完成。我们建议指派一名内部倡导者，以便将这一原则应用于安全性。该职位的目标应该是促进整个企业中从NetOps和SecOps到DevOps和DevSecOps的协作。安全倡导者的任务是帮助其团队解决和避免安全问题，从而使整个企业获得成功。

安全倡导者可以是您的CISO（首席信息安全官）、安全从业者，甚至是DevOps团队中对安全有深刻理解的成员。您指派给该职位的人员应该对主动式安全充满热情，并从深层次理解为什么安全对您企业的成功非常重要。

此人应该是您企业安全的代言人。您可以让他们定期就相关的安全话题展开自由讨论，以确保公司里的每个人都知道他们可以向谁询问与安全有关的问题或担忧。

警告：安全倡导者不应独自承担企业中所有的安全事宜。成功取决于所有团队成员都承担起安全职责，所以安全倡导者的工作更多是教育和树立安全的价值，并促进跨部门协作，以便每个人都能采用最佳安全实践。

当涉及到DevOps和安全性时，您会希望确保双向交流。如果没有对DevOps实践的深入理解或不了解他们使用的工具，那么安全卫士就不能合理倡导具体的安全措施。安全卫士不只是向DevOps传授最佳安全实践，他们还要合作开发一种与DevOps实践无缝协作的安全方式。

采用护栏：聚焦安全策略

传统的安全策略往往相当宽泛，但在应用程序和服务激增的云环境中，必须非常具体和明确。为此，云应用遗留安全模型的挑战在于，安全策略可能很快变得过度复杂和难用。

相反，我们建议使用我们所说的“护栏”，即一组可广泛应用于多个应用程序和资源的策略规则。例如，安全团队可以定义限制公共访问数据存储的护栏，或者限制开发/测试环境的访问和生产资源的护栏。您的安全团队所定义的护栏，将用于保护在云端部署的数据和应用程序。首先，建立护栏，以自动强制哪些服务之间可以通信，这也称为“分段”策略。要实现更好的控制，您可以定义将护栏扩展到极为精细级别的微分段规则。

我们还建议您的护栏以应用程序而非基础设施为中心。这将使您能够查看业务应用程序，并在适当的情境中查看安全策略错误或风险，从而使业务负责人能够快速地从安全性的角度查看和理解正在发生的事情。

护栏的实施越简单，就越有可能适当地应用于整个环境。通过一致的护栏实现对安全策略的高度关注，将使您的团队可以继续专注于他们的增值工作，而不会因错综复杂安全策略偏离正轨。

考虑新工具

实现成功的企业云安全需要采取哪些步骤？部分答案是采用正确的技术。

到目前为止，企业已经测试各种实现云安全的技术方法，其中一些不合格，具体包括:

- 自定义的内部工具和脚本（难以维护和实施）
- 专注于安全操作的技术解决方案（效率低下且难以扩展）
- 防火墙（当网络边界消失时不符合标准）
- 仅限云端的安全工具（不能保护混合环境并导致额外的安全孤岛）

为了避免在云安全方面出现错误，我们建议您寻找既能在云端成功实施又适用于混合环境的解决方案。具体来说，您应该在适用于整个企业的强大云安全解决方案中寻找5个关键属性。

- **云原生**：这似乎看起来很简单，但您希望选择在云端构建并服务于云的工具。您应该首先使用现有云平台中内置的安全工具，包括安全组、IAaM策略和基于角色的访问控制。除了这些基本的控制措施，还要寻找能够为您的独特业务提供可见性和洞察力的云原生安全工具。
- **聚焦应用**：由于存在海量信息，在基础设施层级上管理云安全非常困难。相反，我们建议选择着眼于应用程序层级的解决方案。该理念可以让您在具体情境中查看策略错误或风险，并与那些参与应用部署的人员进行有意义的对话。这使得在复杂的企业中正确实施安全工作变得更加容易。
- **多云和混合**：当前，大多数企业都有一个多云环境，这意味着工作负荷分布在各种云实例和提供者之间。他们通常也有一些遗留的本地基础设施，正如我们所讨论的，不可能立即淘汰掉这些基础设施。因此，请确保您选择的安全工具能够在整个混合和多云基础设施中正常运行。
- **集成到CI/C渠道**：正如我们在本白皮书中所讨论的，持续开发和集成是当今企业成功的关键。要确保您不会减缓这些发展进程，请寻找能够轻松集成到交付渠道中的安全工具。
- **易于部署**：如果特定工具需要长时间部署、广泛的微调以及管理重要的团队资源，很可能无法得到充分利用，而您会发现自身存在安全漏洞。

在评估云安全工具时，您应自问是否勾选了这5个选项，而它们是否达到了确保您基础设施各方面的最终安全目标。

衡量成功

一旦您指定安全倡导者、设置护栏并选择新的安全工具，您将希望开发一个衡量成功并随着时间的推移改进的程序。以下是我们建议您注意的一些关键指标：

指标	前	后
安全检查所需时间		
事故数量		
DevOps渠道中的安全检查数量		
安全异常的数量		

我们建议您跟踪这些KPI（关键绩效指标），以证实您的方式是否有效。从合规性角度来看，这是很有用的，可帮助您获得持续的安全预算来支持您的项目。

结论：不要怕“云”

您的企业无需担心过渡到云。尽管云可能会在安全方面带来更多复杂性，但在速度和敏捷性、时间和资金节省以及输出水平方面，具有无可争议的优势。

随着越来越多的大型企业实现云迁移，应立即重新考虑如何处理安全性问题，并找到一条体现敏捷性和速度原则的前进道路。我们认为安全必须按照从本地到云端再到微服务的流程，集成到整个产业设施以及应用程序开发和部署渠道中。实现这一目标的最佳方法是理解传统与云安全需求之间的差异，并通过稳健而易于执行的安全策略来执行最佳实践。

借助本指南，对于任何独特或复杂的安全访问和连接，您都可以在保持敏捷性和安全性的前提下体验云优势。

tufin The Security Policy Company.