Akamai

白皮书

保护混合云和多云环境中的工作负载

保护混合云和多云环境中的工作负载

为寻求创新、竞争优势和效率，企业已转向基于 DevOps 的云基础架构模式。这让他们以前所未见的方式提高了企业 IT 的速度和敏捷性。许多企业延用了公有云基础架构，并采用新的部署方法，如容器和无服务器技术。通过采用这种新模式，最新云计算技术显著加速了变革的步调。通过这些做法，工作负载、应用程序乃至环境都能实现自动化、自动扩展和迁移等。这带来了强有力的竞争优势。

与此同时，企业还在延用一些传统的服务和系统，如传统数据中心基础架构。企业可能正在逐步淘汰这些系统，也可能在对其进行现代化改造，但这些系统本身仍然存在，因为它们承载着关键业务应用程序和工作流。

此外，传统安全技术跟不上变化的步调，带来了如何在这类新型混合云和多云环境中保护云工作负载的问题。除了速度方面的考虑因素之外，在绝大多数流量都发生在云或数据中心内部（即“东西向”），而非来自外部（即“南北向”）时，基于边界的安全防护机制将不再有效。这种转变也迫使 IT 高管重新思考其安全行动方案。

传统安全技术在混合环境和多云环境中往往不是那么有效

事实上，传统网络安全模式在构建时并未考虑到基础架构即服务 (IaaS)。公有云需要根据自身的独特挑战制定新策略。

企业安全机制必须发展进步，这样才能支持全新的业务环境。为了满足业务需求和敏捷工作方法的要求，各企业已经做出了巨大的改变。虽然企业做出了大量投资，但安全投资相对较为落后。

事实上，将资金投入到开发时并未考虑云技术的解决方案绝非明智之举。这类解决方案无助于检测和防范当前或未来的入侵。如何才能保证关键数据安全无忧，同时使用公有云服务并享受速度和敏捷性方面的优势？

现代混合云数据中心

现代数据中心的组成方式、工作负载粒度的增加以及开发速度都在快速变迁。典型的现代混合数据中心包含在本地环境和公有云/IaaS 环境中运行的工作负载，与多家供应商合作，并在本地或云环境中利用平台即服务 (PaaS)。在公有云中运行的工作负载数量不断增加。与此同时，企业本地数据中心在近期还不会淘汰。例如，近期一次面向技术高管的调查显示，在现代 IT 环境中，约 59% 的受访者“在云环境中运行部分工作负载，但仍以本地环境为主”，34% 的受访者“在云环境中运行大部分工作负载，但仍有部分使用本地环境”。只有 7% 受访者选择了“全面使用云环境”，但这一数字预计会大幅度增加。[1]

我们可以看到，企业在越来越多地使用 DevOps 实践并提高其敏捷性。原生云服务和无服务器技术的实施比以往更加轻松。通过在云端结合使用容器、虚拟机和无服务器工作负载，您可以提高成本效益，并从战略视角实现转型。

安全机制需要适应这种混合云模式。企业需要在 DevOps 流程的每个阶段应对安全问题，从测试、构建、规划、监控、运行，直到部署和发布新功能。迁移到云端不能成为成功的绊脚石。

分布式工作负载未得到充分保护，制约了新型云技术的使用

当今的许多企业必须保护分布在多个不同环境中的工作负载，包括本地环境、主机托管环境以及多个公有云/IaaS 平台。传统的本地网络安全模式很难保证这些工作负载的安全。

与此同时，您还要尝试部署新的云端工具和技术来确保新型云技术的安全性，导致问题更加错综复杂。企业尝试在不同环境中实施不同的安全控制措施，并在监测能力不足的情况下部署这些控制措施，这造成了风险，进一步提高了复杂性。

换句话说，云技术的初衷是让企业更加动态、敏捷、迅速，并加强企业创新力，但现在却给许多企业带来了风险。由于缺乏适当的云安全工具，企业在采用这种新技术时受到限制，无法避免盲点和更多挑战。

自适应工作负载保护应运而生。

过渡到 IaaS 推动了对自适应工作负载保护的需求

要保护生命周期较短的细粒度工作负载，理想方法是在启用工作负载时立即动态地应用保护措施。在涉及到公有云基础架构时，相较于传统网络安全模式，以工作负载为中心的解决方案在执行安全策略方面要简单得多。

云工作负载保护平台支持不受平台限制、以工作负载为中心的安全解决方案

策略与工作负载相关，与底层基础架构无关，因此这种模式适用于整个混合云数据中心环境内的所有工作负载。通过这种模式，您就可以采用一致、不受平台限制的安全控制方法。

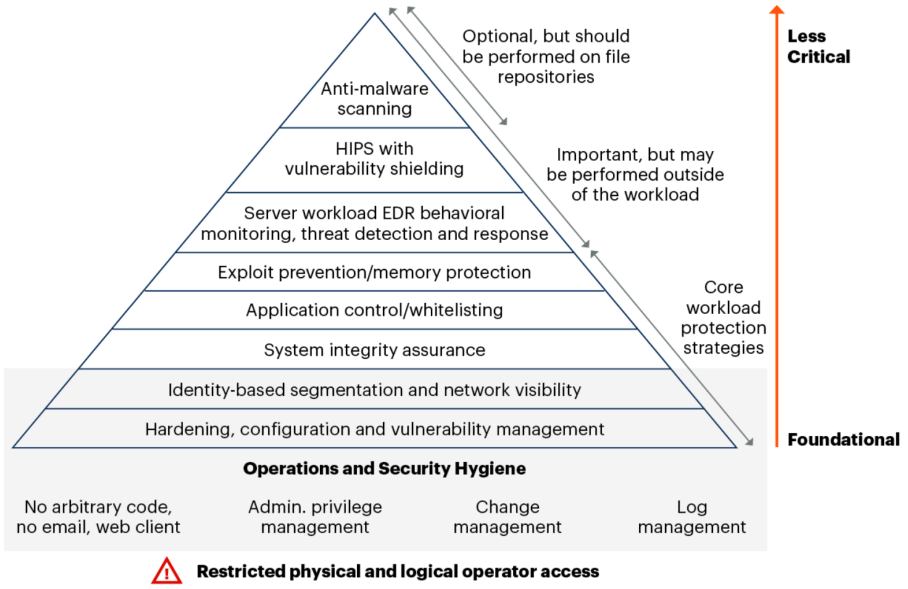
虽然有原生云安全工具，但自适应云工作负载保护平台 (CWPP) 也有自己的优势，它能在进程、用户和完全限定域名层面上提供更全面、更精细的控制。它们还能跨多家云提供商和本地环境运行，为虚拟机、容器和无服务器工作负载提供更强大、更全面的保护。

可行的核心工作负载保护策略：对照 Gartner 云工作负载保护准则设计控制措施

Gartner 的行业专家撰写了一套云工作负载保护准则，这是采用范围最广的准则之一。Gartner 认为，在保护云工作负载时，有一个清晰的控制层级。

在下图所示的金字塔图中，Gartner 按照从必不可少到可有可无的顺序展示了所认定的核心策略，以及重要但非必须实施的策略。在理想情况下，应该在每个工作负载中包含这些步骤，确保云端的每一项操作都内置安全机制。

基于风险的工作负载保护控制措施层级[2]



Source: Gartner
716192_C

Gartner

Gartner 的云工作负载保护准则为企业提供了清晰的安全控制层次结构

下文详细解析了我们的解决方案所满足的核心策略，旨在帮您了解如何以最佳方式将这些策略整合到混合或多云数据中心保护计划之中：

- **安全强化、配置和漏洞管理**

  Gartner 认为，必不可少的工作负载保护策略是从降低风险的目的出发，合理配置系统和设置。漏洞管理工具在手动清除攻击媒介的基础上更进一步，实现了这一过程的自动化。这样，您就能发现并解决可能给攻击者创造机会的软件问题。

- **基于身份的分段和网络监测能力**

  Gartner 强调，网络分段和监测能力是云保护的核心策略。大多数企业的本地环境使用的都是下一代防火墙，但许多企业在迁移到云端时采用了安全性略低的解决方案。

  安全团队知道下一代防火墙不足以满足云保护需求，但不知道如何在动态混合数据中心环境内获得对异构环境的见解，也不知道如何对这样的环境实施控制。所以我们花些时间来介绍合理的做法。

  首先是实现监测能力。通过快速监测能力，所有利益相关者均可立即自动达成一致共识，因此能更快地实现价值。

  原生云工具可能会提供快照映射或文本日志，但这些内容通常比较难懂、不够完整或不够充分。理想的解决方案应能自动发现网络中的所有应用程序、流量和依赖关系。这样，即便企业采用混合分布式环境，您也能一目了然地了解整个 IT 生态系统。

  您的解决方案还应该包括强大的情境功能，能帮您有效了解数据中心的真实状况。对于希望大规模管理安全操作和查询的企业而言，每个流程都需要具备这样的情境功能，还需要能深入探究个别进程和服务器通信。这样就能实现由数据驱动的决策，为策略创建提供支持。

  在实现监测能力、获得情境信息之后，需要根据公司的最佳实践创建合适的分段规则。例如，您可能希望将生产环境和开发环境分离开来，或者隔离客户数据以证明合规性。您还可以制定更精细的微分段策略，通过适合具体业务情境的方式提供深度安全和控制措施。

- **应用程序控制/允许列表**
  如果您的安全团队能制定策略，并确信这些策略能在整个 IT 生态环境内运行，您上云之旅的每个阶段都会更轻松、更安全。

  仅依靠端口/IP 无法获得全面保护云工作负载所需的监测能力。对强大的微分段解决方案而言，核心部分就是严格管控应用程序组件之间的流量。理想技术应具备精细的监测能力和控制能力，可细化到应用程序进程、用户和完全限定域名，并使用哈希值、校验和、完整路径、解析度和身份存储验证等细节。

  一些可增强应用控制的附加功能包括：

  - 可限制云端横向移动的微分段，甚至能限制应用程序集群内部的横向移动
  - 采用单一管理平台设计，安全性更出色
  - 创建允许列表和拒绝列表模型的功能，这两种模型都能防止未经授权的应用程序或流量，并确保重要连接畅通无阻

- **漏洞防御/内存保护**
  在 Gartner 的 CWPP 指南中，最后一项核心服务器保护策略就是漏洞防御。您应该关注可提供漏洞检测和响应功能的微分段安全工具。这样，就可以取代多余的工具，降低数据中心复杂性。

  此外，如前所述，监测能力和映射是不可或缺的。在获得整个网络的完整映射后，即可轻松发现未修补的漏洞或不寻常的恶意通信。在贵企业建立合法流量基线后，就能轻松发现未经许可的流量。

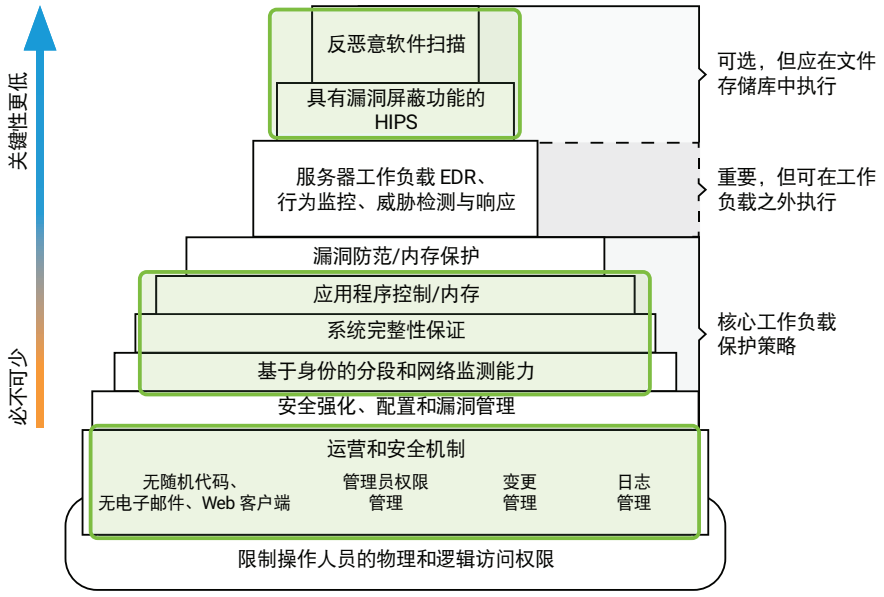
其他重要保护战略

上述核心服务器策略是云安全的基础。与此同时，Gartner 还确定了另外几种可加强混合云或多云环境安全性的策略，包括服务器工作负载端点检测和响应 (EDR)、行为监控，以及威胁检测与响应 (TDR)。

EDR、行为监控和 TDR 是漏洞检测和事件响应的重要组成部分。为了涵盖安全性的这些方面，您应该注意寻找包含信誉分析的解决方案。这能让您确定有关攻击的更多信息，并获得高级欺骗功能，诱使攻击者泄露其攻击方法。这样，您就可以在将来加强策略和安全程序。

您可能需要监测数据来确定既往事件的信息。理想的供应商应能将您的数据保存数月，让用户可以关注特定应用程序、流程和时间段。安全团队还可利用这些数据开展取证调查，并改进事件响应方案。

Akamai Guardicore Segmentation：根据 CWPP 层级保护混合云工作负载



突出显示的部分指出了我们的解决方案在哪些方面满足了 CWPP 的要求

Akamai Guardicore Segmentation 消除了原生云安全工具的固有缺陷，满足了 CWPP 中列举的许多基本原则。此外，该解决方案还通过智能方式支持跨混合和多云数据中心的监测能力、策略创建与执行。

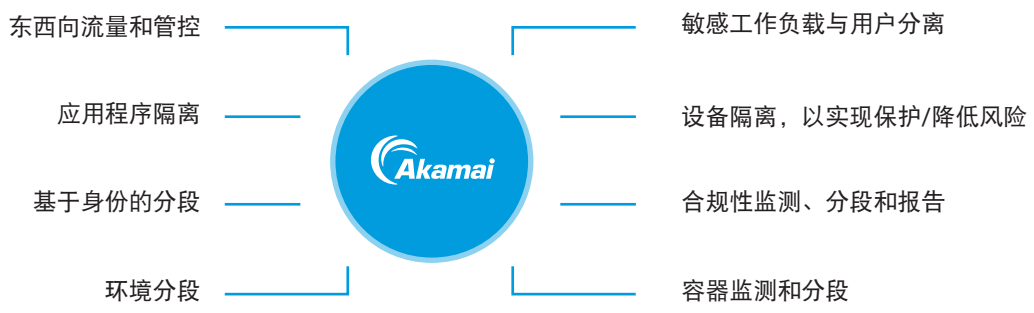
我们的解决方案提供了深度监测能力，让您可以在一个管理平台中纵观整个数据中心的情况。有了这种把控全局的能力，您就可以全面了解混合数据中心内应用程序的依赖关系，以及任何策略对网络的影响。这对云迁移有着巨大的影响，相较于原生可视化工具，能帮助客户显著加快云迁移速度。

这种深度监测能力让您能够：

- 创建云环境中的网络待办事项清单
- 在任何基础架构和应用程序依赖关系中快速检测应用程序—这是保证迁移成功的一项关键能力
- 提前了解基础架构和运营成本
- 获得有关如何制定最佳策略的洞察，从而从迁移规划阶段开始降低风险
- 利用最短、最简单、最安全的途径实现云的业务目标

Akamai Guardicore Segmentation 可执行基于情境的深层次监测，从而帮助您迅速、全面地了解环境

我们的全面监测能力还能提供每一次通信、每一个流程的情境信息，支持您减少错误、降低整体复杂性。您可以对信息进行分组和过滤，确保任何利益相关者都能读懂映射，轻松获得所需的确切信息。这种由情境驱动的视图可减少对第三方供应商和策略创建者的需求，让您能够迅速了解环境，并进而创建、优化或修改适用策略。



Akamai Guardicore Segmentation 应用场景示例

我们的解决方案提供的其他重要功能包括：

- 进程和服务级策略，可在处理动态协议（如 FTP 或 Spark 等）时提供更简单、更可靠的安全性
- 基于身份的微分段策略，根据创建连接的用户实施连接
- 基于完全限定域名的策略，允许您访问具有动态 IP 地址的自动扩展式资源
- 将现有公有云标记用作标签，简化混合云或多云数据中心的可视化
- 根据观察到的流量自动构建策略，在您开启微分段之旅时快速为您提供专家指导

我们的解决方案不受平台和基础架构限制，可管理整个基础架构的监测和执行工作

降低复杂性是确保混合数据中心安全性的终极目标。根据这样的需求，Akamai Guardicore Segmentation 不受平台和基础架构限制，能为您提供与工作负载相关的所有应用程序和策略的整体视图，而无论工作负载位于何处。每条规则都会应用于所有工作负载，从 vCenter 和公有云（AWS、Azure、GCP）到裸机服务器和容器。

降低复杂性不仅能加强安全态势，还能降低 IT 和安全部门的工作量。使用云端安全组时，对于每一家供应商的技术，您都要具备原生云专家。相较之下，如果有一种安全解决方案能管理整个基础架构的监测和执行，您只需有单独一项技术的认证专业人员即可满足需求。

未来无忧的云工作负载保护平台

敏捷方法论和 DevOps 的基本理念之一就是快速失败，并轻松过渡到“下一件大事”。遗憾的是，在不同云提供商之间迁移工作负载可能会造成您的工作效率大幅度降低，这也颇有几分讽刺意味。此外，这也很难在保持原有安全措施不变的前提下实现。

您需要获得开放的选择。如果您想迁移到多云基础架构，甚至是将工作负载迁移到新的云提供商，迁移工作不该对安全性产生负面影响，安全性也不该妨碍迁移工作。

Akamai Guardicore Segmentation 让您能够保持灵活性，并根据业务发展的步调进行迁移，同时保持安全策略不变。它不会妨碍 DevOps 流程或敏捷性，也不需要在每个阶段重新进行配置。与此不同，它提供了值得信赖的云工作负载保护平台的基础，确保混合或多云数据中心安全无忧。

Akamai Guardicore Segmentation 支持您安全地迁移到云端，也能在不同云环境之间安全地进行迁移，而且提供了带有情境的出色监测能力。利用我们的解决方案，您可以在进程和用户层面上实施策略，并随时随地跟踪工作负载。

现在，您可以将安全性作为 DevOps 流程每个阶段的一项功能，实现敏捷性并为业务提供有力支持。贵公司将能够采用前沿云功能，同时保持以安全性为核心。

进一步了解如何使用业界卓越的微分段解决方案保护云环境。立即访问 akamai.com/guardicore。

1 2022。Foundry（前身为 IDG）云计算研究。

2 Market Guide for Cloud Workload Protection Platforms；作者：Gartner 分析师 Neil MacDonald 和 Tom Crow；2020 年 4 月 14 日发布