解决方案简介

Fortinet 动态云安全解决方案

要点概述

尽管公有云使用率日益增长（无论是总量还是服务多样化方面），但这并非单向趋势。为了满足不断演进的业务需求，各组织正在云和本地环境之间来回迁移应用和工作负载。这一趋势已在最新一次调查中为 74% 的受访者所肯定。[1] 为了在此动态环境中最大限度地减少可利用漏洞，安全团队必须密切跟踪网络流量、应用传输及云平台活动和配置。Fortinet 动态云安全能够满足这一需求，提供原生集成网络、应用和安全解决方案，以支持并助推数字化创新。

满足动态云网络需求

借助 Fortinet Security Fabric 安全架构全面覆盖、合度结合与动态协同的特性，Fortinet 动态云安全解决方案可通过跨任何云或非云基础设施的统一安全管理，并提供一致的安全防护和策略实施。

- **在私有云中**，Fortinet 网络安全解决方案可与基础设施自动化系统无缝集成，以针对动态多变的虚拟机及其他工作负载实施安全策略。
- **在公有云中**，Fortinet 网络、应用及平台安全解决方案能够与云网络服务相集成。云负载平衡和平台应用编程接口 (API) 提供了针对整个攻击面的全面安全保护。
- **在软件即服务 (SaaS) 云中**，Fortinet 通过连接到云 API 提供可视性和控制力，以规避 SaaS 配置错误带来的风险。

跨主要云环境提供一致保护

不断演变的威胁态势需要高级威胁防护能够深入至加密流量，并发现零日威胁。配合原生云提供商安全工具的基本功能，Fortinet 提供了一系列广泛的安全功能，其中包括：

FortiGate VM 下一代防火墙 (NGFW) 助力保护网络安全

- **网络微分段**，可保护云到互联网（南北）流量和横向云到云或内部（东西）流量，确保可预测的应用性能。Fortinet 虚拟 NGFW 通过 Fortinet Security Fabric 进行集中管理，能够跨混合多云环境一致地应用安全策略。部署至公有云的 FortiGate VM 解决方案可与私有数据中心配置的任何 FortiGate NGFW 安全通信，并共享一致的策略。

Fortinet 动态云安全与单点产品安全方案有很大不相同，可帮助组织随时随地确保一致的安全保护，支持在任何位置运行任何应用。

支持的主要公有云

- AWS
- Azure
- Google Cloud
- Oracle Cloud
- 阿里云
- IBM

支持的私有云技术厂商

- VMware
- Microsoft
- Xen
- KVM
- Cisco
- OpenStack

- **高级威胁防御，**利用 FortiGate VM 应用控制和入侵防御系统 (IPS) 等功能，帮助组织有效阻止应用层威胁感染和危害基于云的基础设施。FortiGate VM 高级威胁防御功能可有效拦截已知攻击。
- **安全 SD-WAN**，将智能 WAN 路径选择和安全功能整合至单个基于云的解决方案中。Fortinet Secure SD-WAN 能够帮助组织简化云连接，同时维护安全并降低成本，无论是用其将分支机构连接至云端还是用于云与数据中心之间的互连。

Fortinet 动态云安全使用模式

Fortinet 动态云安全包括 FortiCWP、FortiWeb 和 FortiGate VM。它们以多种形式提供，例如虚拟机、SaaS 和 Docker 容器，能够全面满足客户需求和用例要求。此外，各种解决方案均支持作为自带许可 (BYOL) 选项使用，可通过常规云供应链购买，通常分为永久许可或按需购买的即付即用 (PAYG) 许可。

使用 FortiWeb Web 应用防火墙 (WAF) 确保 Web 应用安全

FortiWeb 采用支持机器学习 (ML) 多层防护方案，可保护 Web 应用和面向外部的 API 免遭已知威胁（例如 OWASP 十大威胁）和零日威胁。借助机器学习，FortiWeb 能够识别异常行为并区分恶意和无害异常状况。较之大多数 WAF 所需的手动应用学习，这可以提高准确度并节省大量时间。此外，高级 Bot 防御功能还可支持搜索引擎等无害 Bot 连接，同时阻止恶意 Bot 活动。最后，为了满足各种客户的使用要求，FortiWeb 的可部署的形式包括 SaaS、Docker 容器或虚拟机。

通过 FortiCWP 执行云平台安全管理

在多云基础设施中实施一致且高效的风险管理，确保数据安全。

深入洞察可帮助安全管理员和 DevOps 团队高效评估其云配置安全状态、检测因云资源配置错误而产生的潜在威胁、发现违反策略的行为并生成合规报告。

灵活的部署选项有助于降低总拥有成本

Fortinet 动态云安全解决方案可满足广泛的资源和性能要求。其中不仅包括小型虚拟机，可最大限度地发挥横向扩展架构的优势，而且还包含大型虚拟机，能够利用不同云平台上的高容量网络加速技术，并为无法使用横向扩展架构的有状态应用提供大规模网络处理支持。

原生集成能够优化混合多云生态系统的安全性

云与本地环境之间以及云特定工具与专用安全工具之间的不兼容性会导致出现安全漏洞。为了最大限度地减少这些漏洞，Fortinet Security Fabric 通过云特定集成来提供架构一致性。原生集成有助于免去安全人员了解每个云环境的特定对象类型和命名规范的麻烦，取而代之的是单个直观的配置界面。Fortinet 提供了以下三种集成：

- **Fabric Connector** 将云特定安全对象和服务名称转换为一致格式，以便在整个 Fortinet Security Fabric 中定义安全策略。
- **Fabric API** 可跨云端和本地部署的 Fortinet 产品实现安全操作编程标准化。
- 针对通过 Fortinet 产品检测到的安全事件**而配置的自动化响应**能够直接在不同云平台上触发补救措施，无需安全操作员掌握深厚的云专业知识即可轻松利用无服务器功能。

Fortinet 与云服务提供商密切协作开发了其所有连接器和 API，并根据各个云环境变化进行定期更新。

图 1：Fortinet 动态云安全释放业务敏捷性

可管理性与自动化

针对组织面临的快速演进的威胁态势和相关应对技能的持续短缺， Fortinet 动态云安全提供了可靠的安全管理和自动化功能，可跨云环境一致地实施。这些功能有助于获得覆盖整个多云基础设施的适当级别的可视性，这对于定义有意义的策略并最终有效控制基础设施而言至关重要。

Fortinet 动态云安全管理和自动化解决方案可通过一站式管理帮助安全管理员和操作员简化日常运营。其中还包括 API，可帮助 DevOps 和 DevSecOps 团队自动执行所有常规作业的安全操作，而无需进行云特定的自定义。除了提高运营效率外，这些工具还能够降低培训和人员成本，因为同一安全技能适用于所有云环境。最终，Fortinet 动态云安全解决方案能够帮助组织以最低的开销维护更高的网络级、应用级和云平台级安全状态。

值得投资的安全解决方案

数字创新需要与动态云基础设施相匹配的安全性。Fortinet 动态云安全解决方案为希望快速、长期交付价值的组织提供以下优势：

- 可从最小的构建模块单元扩展至最大的高容量网络虚拟设备 (NVA)
- 轻松适应各种用例并满足业务特定和应用特定安全需求
- 利用最新机器学习和人工智能 (AI) 的安全技术可为动态云基础设施提供不断优化的 Web 应用保护，从而防御快速演变的威胁
- 真正协同的安全结构方案，将网络、应用和云平台安全性集成至单个框架中，可提高业务网络安全性，并减少人为错误发生几率

Fortinet Security Fabric 组件经过了可信第三方组织的反复验证，已被全球超过 425,000 家客户所采用. 这一骄人的成绩和 Fortinet 在云安全领域的持续投入让组织的安全负责人可放心利用 Fortinet 动态云安全解决方案将任何应用部署至任何云。

1 “The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments,” IHS Markit, Q2 2019. IHS Markit，2019 年第二季度。

2 “Powering WAN Edge Transformation: Integrated Security and SD-WAN,” Fortinet, Q4 2019.