Fiverr 用 Orca Security 取代多个工具，以获得对 AWS 资产的即时和完整的可见性

fiverr.

行业
互联网

冠军
Shahar Maor：首席信息安全官 (CISO)

云环境
AWS

“几分钟内，我们就获得了 AWS 帐户的全面可见性。在使用 Orca 之前，我的可视性为零。现在我可以看到我需要看到的所有内容。而且，如今我们可以通过单一工具完成所有操作。”

Shahar Maor
首席信息安全官
Fiverr

云安全挑战

- 无法理解 AWS 正在发生的所有背景
- AWS 和开放源工具耗时且无效
- 数以千计的警报泛滥成灾，没人有时间查看

云安全结果

- 深度云检查识别恶意软件、错误配置、“机密”、易于攻破的密码和 PII
- 节省每周的工作时数，减少对 DevOps 的依赖，并且没有被忽略的资产
- 现在，警报会根据环境背景进行优先排序，推送到 Slack 加以解决

快速的全球扩张要求规模化的 AWS 云安全

Fiverr (NYSE: FVRR) 成立于 2010 年，总部位于特拉维夫，是一个提供自由职业者服务的庞大的全球在线市场。它的平台让自由职业者为全球各地的客户提供服务，同时帮助企业通过浏览目录或进行搜索找到所需的服务。

Fiverr 的平台为 550 万家企业提供服务，并促成了 5000 多万笔交易。由于有这么多的人访问平台，维护 AWS 基础架构的安全至关重要。

Fiverr 首席信息安全官 Shahar Maor 知道保护云环境是一件复杂的事情

“我是 Fiverr 雇佣的第一个全职安全专业人员，” 首席信息安全官 Shahar Maor 透露到。“虽然安全已经深深地植根于 Fiverr 的文化中。”

Maor 对 AWS 基础设施的初步分析指出了来自外部载体、黑客、恶意机器人和病毒可能的攻击。但他知道，在云环境中，不仅仅是表面上看到的那样。

“组织通常假设如果它们保护周边，就足够了，而云基础架构经常被忽略，”Maor 说。“您也许不会考虑到，平台本身的错误配置可能是一个问题。如果您有一个云原生基础架构，您就能更清楚地看到它，这是一种误解。保护云环境牵涉到很多的复杂性。”

Maor 担心平台用户密码易于攻破，以及存在恶意软件在 AWS 服务器上运行的可能性。“我第一次绘制高价值资产的风险图时，很明显我们有盲点。另外，我花了太多的时间来手动监视资产 (尤其是 AWS S3 存储桶)，以确保没有泄露任何内容。这是非常繁琐的。”

为所有 AWS 资产提供深度可见性所需的理想解决方案

考虑到特定要求，Maor 开始寻找 AWS 云安全解决方案。我们需要一种解决方案，既能提供 AWS 环境的完

> “组织通常假设如果它们能保护周边就足够了，而云基础架构经常被忽略。”
>
> **Shahar Maor**
> 首席信息安全官
> Fiverr

整可见性，又能扫描恶意软件、识别错误配置并保护 PII。

最优的云安全工具将是为已查明的风险提供全面的解决方案，以及 IT、DevOps 和工程领域的实用洞见和价值。AWS 安全解决方案的其他目标和要求包括：

- 无代理来管理
- 完全可见性；没有被忽视的资产
- 搜索和保护 PII
- 对服务器进行健康检查
- 识别易于攻破的密码
- 查找错误配置
- 寻找现有代码中的“机密”
- 监控公开的资产，如 S3 存储桶
- 简化监管合规性，特别是 对 PCI 。

> “我们需要一种解决方案，可以提供 AWS 环境的完整可见性，同时扫描恶意软件、识别错误配置并保护 PII。”
>
> **Shahar Maor**
> 首席信息安全官
> Fiverr

原生工具、传统扫描器和基于代理的方法都不能解决问题

Maor 知道 Fiverr 的云环境有着独特的需求，许多可用的云安全工具都无法满足。“像 Amazon Inspector 或 GuardDuty 这样的原生工具提供基本功能，但它们不会将逻辑与事件挂钩，也不了解正在发生的事情的完整背景。你仍然需要对日志进行分析，并花更多的时间来理解数据。它们比什么都没有强，开源工具也是这样，但它们都缺乏将发现结果传递给团队并采取相应行动的工作流程。”

Maor 补充说，扫描器和基于代理的工具功能非常有限。“一些商业工具扫描服务器以解决漏洞，但仅此而已。简而言之，这些工具创造了更多的工作，而且它们需要领域专业知识和更多工具才能有效工作。”

单一工具就能完成所有操作

Maor 将 Orca Security 视为减少隐藏在 Fiverr AWS 基础架构内的风险的一站式服务。“Orca 提供一个全面的解决方案，以减轻 Fiverr 的数据库中的风险。Orca 用来扫描 AWS 的独特方法对我们来说最适合，并且它赢得了我们 DevOps 团队的支持。另外，如今我们可以通过单一工具完成所有操作。”

Orca SideScanning™ 无需代理，对性能没有影响

在单个虚拟机上运行安全代理需要持续的管理。而 Orca 作为 SaaS 服务运行，对客户的 AWS、Azure 和/或 GCP 工作负载的运行时块存储具有只读访问权限。它从快照中重建数位和字节，以构建操作系统、应用程序和数据的虚拟只读视图，然后进行扫描，以查找漏洞和风险。

“Orca 非常轻量级，对网络没有任何影响，”Maor 说。“您可以获得可见性，而且对实例本身没有任何干扰。Orca 只是创建一个副本，进行阅读并分析结果，然后将其呈现在数据面板中供我们查阅。”

无噪音、有意义、高价值的警报

Orca Security 获得专利的 SideScanning™ 技术可自动检测客户环境中的每个资产。这为安全团队提供可对资源、漏洞、恶意软件和错误配置进行即时可见性。通过将此类信息与环境元数据相结合，Orca 在上下文中发送警报，以实现有效的优先级排序。

“Orca 实时发送有意义的、可操作的警报，以让我们关注威胁，而不是创建大量日志和数千个无人阅读或没有时间查看的警报。我们获得每一个关键发现的 Slack 警报。如果 Orca 发现新漏洞，我们会立即知晓。”

简化监管合规性

此外，Orca Security 简化了监管合规性。“PCI 需要我们扫描环境—因为它无服务器，这带来了独特的挑战。Orca 解决方案让我们扫描 EKS 和 ECS 容器，为 PCI 提供良好的解决方案。”

> “Orca Security 实时发送有意义的、可操作的警报，以引起我们对威胁的注意。如果 Orca 发现新漏洞，我们会立即知晓。”
>
> **Shahar Maor**
> **首席信息安全官**
> Fiverr

完全可见且省力

执行后不久，Orca 就出现了 Maor 团队能够解决的漏洞。“Orca Security 提供宝贵的洞察力和扩展 Fiverr 的安全态势的能力。而在使用 Orca 之前，我的可见性为零。现在，我可以看到我需要看到的所有内容。”

对 Maor 来说，这证明了 Orca Security 就是他所需要的。“我仍然同时部署了 Orca 和 CASB，但下一次重新开始时，我会删除 CASB，因为它没有提供任何洞见，”他说。“我将完全依赖 Orca 来端到端地监控 AWS 生产环境。”

节省每周工作时间，无需依赖 DevOps

现在，Maor 花在云安全工作上的时间只有过去的一半。“Orca 已经减少了云安全维护和管理工作每周的工作时数。此外，我无需依赖 DevOps 来提供支持。”

作为一个额外的奖励，Maor 能够依赖 Orca Security 的团队提供建议和专门知识。“Orca 团队带来了安全方面的广泛背景和实际知识，以及令人惊叹的敏捷性和灵活性。我们已经看到 Orca 大量的价值，并且我们很高兴将其作为我们主要的 AWS 安全平台来发展。”

关于 Orca Security

Orca Security 利用其独特、正在申请专利的 SideScanning™ 技术为 AWS、Azure 和 GCP 提供了云范围和工作负载深度的安全性以及合规性。与云提供商进行即时、只读和无影响的集成后，它能检测漏洞、恶意软件、错误配置、横向移动风险、身份验证风险和不安全的高风险数据，然后根据潜在问题、可访问性和影响范围确定风险的优先级，而且无需部署代理。

orca security

花几分钟连接您的第一个云帐户，
让您亲身体验：访问 orca.security