不到一天，Orca Security 就将 Zip 18% 的风险可见性提升到 100% 覆盖

行业
金融服务

冠军
Peter Robinson，
网络安全与企业 IT 总监

云环境
AWS、Azure

“只用了一下午的时间，我们就实现了全面可见性，摆脱了多年的苦恼。请相信一个有切身体会的人，这太了不起了。”

Peter Robinson
Zip 网络安全与企业 IT 总监

云安全挑战

- 该公司的快速扩张导致云资产的快速增长
- 基础架构的短暂性导致难以扫描漏洞
- 不同的环境由多个国家/地区的几个人运行

云安全结果

- 100% 覆盖云账户，具有完全可见性、资产清单和优先修复功能，不会对生产环境造成任何影响
- 对 DevOps 的依赖减少，同时获得其对优先修复的全力支持
- 节省大量成本，因为没有集成成本，无需 6 名 FTE 来查找风险并确定其优先级，并且 Orca 的即用即付许可模型仅应用于实际使用的资产

Zip 相信创新永无止境

Zip 是零售金融和支付行业的新一代领军企业。该公司为零售、家居、健康、汽车和旅游行业提供销售终端信贷和数字支付服务。成立于 2013 年，总部位于澳大利亚悉尼，发展迅速，现在的业务已遍布澳大利亚、新西兰、南非、英国和美国，并计划将进一步进军北美、欧洲和中东市场。

Zip 的计算平台是完全数字化的，且托管在云端。该平台利用其专有欺诈和信贷决策技术中的大数据，提供实时响应。反映公司成长的云资产也在迅速扩张。一年前只有 6 个 AWS 账户。而如今有 22 个 AWS 账户和 9 个 Azure 账户，未来还将有更多。

Peter Robinson 是网络安全和企业总监，负责该公司的网络风险和安全态势。“诞生在云端，这个环境对于保障我们的资产安全充满了挑战，因为传统的安全手段不适用于云端。”他表示。在他供职于 Zip 的两年里，大部分时间他都在寻求正确的工具组合，能够提供对面临的漏洞和风险的良好可见性及其解决方案。

> “在使用 Orca 之前，我们的漏洞评估大概覆盖了整个范围的 18%。Orca 在不到一天的时间里让我们实现了 100% 覆盖。”
>
> **Peter Robinson**
> Zip 网络安全与企业 IT 总监

一个下午将可见性从较低提高到 100%

Zip 的平台处于云技术的前沿。“我们已大量转到无服务器计算和基础架构即代码，” Peter Robinson 表示“我们的环境的短暂性，让我们无法在机器消失前部署代理。我们无法对它们进行传统意义上的网络扫描，而且在设备非运行期间，无法连接到这些机器以访问其安全态势。”

“我们还有一个问题，许多环境是由不同的组来运行的。我们有个团队，负责基础架构的不同部分及其他工作。几乎不可能安排他们部署任何用于进行风险评估的架构，” Peter Robinson 表示“Orca 立即为我们解决了这个问题。”

Peter Robinson 是从 LinkedIn 的文章中听说了 Orca Security。“一开始我们对 Orca 的宣称持怀疑态度，但还是尝试了。“在一个下午之内，我们实现了全面可见性，摆脱了多年的苦恼。请相信一个有切身体会的人，这太了不起了。”

Orca 远胜竞争对手

Robinson 花了两年的时间评估传统的漏洞扫描工具和其他专门适用于类似于容器环境的工具。“这些工具有几个通病。首先，部署代理和扫描器需要过多的资源。其次，它们需要凭证，才能实际进行身份验证，许可模型在我们看来毫无作用。再次，这些工具都无法自动确定优先级并跟踪修复。”

许可问题也是这些工具的一大短板。“如果与这些供应商合作，我就必须购买一份完整的、无限资产许可。许可一经使用，即使是在暂时性的资产上，我们也必须付费。一台服务器仅仅运行了 6 个小时，但却消耗了一份许可。如果借助这些工具，成本需要五倍以上。”Robinson 报告说，以这种方式获得许可每月将花费 25 万美元。

所有这些工具的主要问题是，它们都不会确定风险的优先级。例如，Robinson 表示，可能有 129 条规则出了问题，涉及 2,000 项资产，而该工具会列出 6 或 8 页的故障。“真是让人眼花缭乱，没有可行性。在过去的 7 天内，就连 SIEM 也返回了 55,000 个故障。根本无法评估。”

Orca 克服了所有这些缺点。部署是零接触的，仅需要创建一个角色，几分钟即可。无需安装代理。许可更易于管理，且基于实际使用的资产。

然而，Orca 真正出彩的特质在于其确定优先级的功能。“Orca 会告诉我今天有 28 个需要关注的问题。在拥有约 840 项计算资产、虚拟机和数千项其他资产的 25 个云账户中，真正的风险归结为今天要处理 28 个问题，”Robinson 表示，“我们完全可以做到。”

Robinson 的 Zip 团队规模很小，所以需要依赖于工具帮助自己实现目标。“借助 Orca，所有的自动化、优先级确定、关联性和对我们的生产环境零影响的部署太难能可贵了，简直太棒了。”他说。

Orca 提升 IT 安全性、DevOps 合作和生产效率

Robinson 表示，DevOps 团队行动迅速，致力于将产品推向市场。他无法要求他们停下构建 Zip 产品的工作，去部署代理和网络扫描器。Orca 负责了这部分工作。其实，DevOps 团队是在采用 Orca Security 平台方面为他提供最多支持的同事。

“最主要的是，DevOps 团队不需要做任何事情。他们只需要创建一个角色，然后就不必再做任何事。他们不需要更改部署、网络规则、安全组，不需要处理端点应用或代理部署，不需要获取凭证，什么都不需要做了。这改变了我的世界。”Robinson 表示。

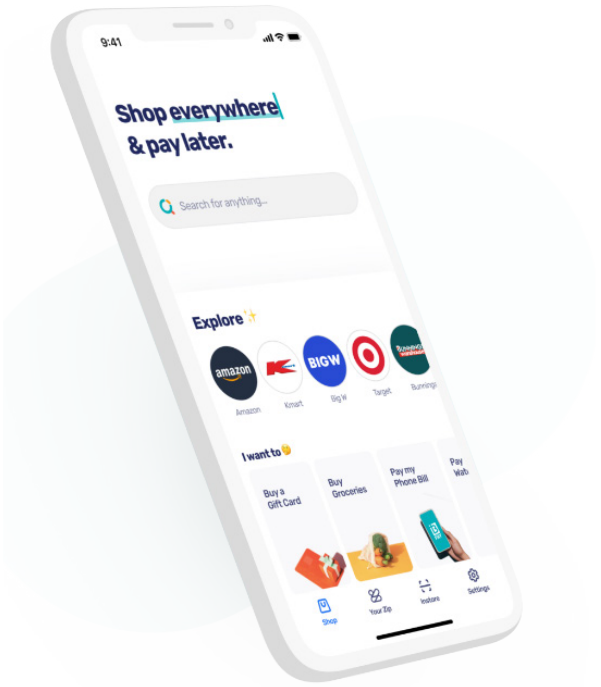
IT 安全和 DevOps 团队现在协作密切。“我可以要求他们处理 Orca 建议的优先修复。对于极其重要的问题有非常明确的说明，”Robinson 表示，“而这不仅仅是一项端点资产。例如，假设我们网络 ACL、负载均衡器和端点的安全组出现了故障。Orca 会提供一份地图。我们的员工会说：‘Orca 会显示如何绕过 CloudFlare 和内部负载均衡器，显示多路径路由。’我们都知道这种情况不应该发生，因为这意味着有人绕过了我们的 WAF。”Robinson 表示无法从其他来源获得此类信息。“Orca 提供对错误配置的深入洞察。团队可以直观地看到问题，知道需要改变它或巩固安全组，这样就只能通过负载均衡器了。负载均衡器仅接受来自 CloudFlare 的输入，您无法直接通过互联网访问负载均衡器。这种洞察特别有助于减少我们的工作量，”Robinson 表示。

“我们的 DevOps 团队专注于我们的产品，这正是他们的本职工作。我不能分散他们的精力，去到处部署端点代理、创建扫描器凭据。”

Peter Robinson
网络安全和企业 IT
总监
Zip

Orca 支持企业级功能，如基于角色的访问控制。“特别好的一点是，在有新人加入时，我们可以为他们分配账户。我可以通过设置，让位于美国的 Quadpay 团队只能看到 Quadpay 数据并处理 Quadpay 账户，而不能看到整个公司。他们只能看到需要看到的内容。”Robinson 表示。

如果 Zip 没有在整个公司部署 Orca，Robinson 估计他们需要在 6 个司法管辖区中的每个管辖区至少配备一名全职员工。“我们可能需要增加 6 个 FTE 一排查一长列未确定优先级的漏洞清单，找出需要处理的漏洞，创建修复工单，同时还要努力将代理部署到机器上，并同时进行所有其他工作。因此，这不仅仅是风险管理工作，还需要花费时间、成本和精力，”Robinson 表示，“Orca 是一石二鸟之计 - 至少从可见性的角度立即处理风险，而且成本降低效果立竿见影。”



Orca 适合 Zip 的风险管理流程

Robinson 有一套发现问题的方法，无论是渗透测试、外部漏洞扫描、内部扫描、观察、事件，还是其他方式，并通过风险管理流程推动问题进入 Jira。“我们在 Jira 中设有风险板，用于评估固有风险。然后我们将子工单或任务分配给负责的所有者，并评估所需的修复，”Robinson 表示，“Orca 与 Jira 的集成相得益彰，因此绝对适用于我们。”

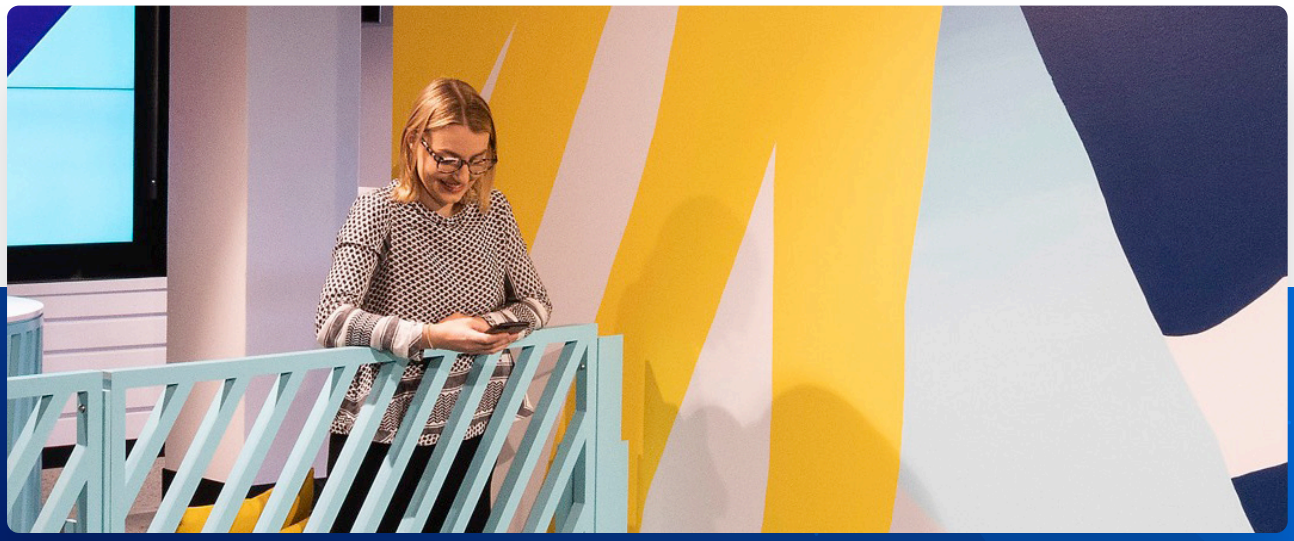
Orca 的一个特色是自动解决功能。如果发现问题并加以解决，Orca 会指出问题已修复。“以前，我的团队必须进行人工评估和测试，以验证是否已切实修复问题。而 Orca 只会告诉你：‘问题已解决，谢谢。’ 我们可以将剩余风险降为零，并关闭工单，”Robinson 表示，“真的大大节省了时间。”

Zip 近期收购了一家公司，并要求 Robinson 接手管理该公司的资产。“毫不夸张地说，我只花了几分钟，就将两个全新的 Amazon 账户完全部署在我的漏洞管理范围内了，100% 覆盖。”

Orca 赢得投资回报和商业案例

Zip 具有从外部扫描其资产的工具。“我们将域名丢给它，它就会发现并使用漏洞报告奖励技术，以评估我们的外部漏洞，”Robinson 表示，“但内部评估一直是我们面临的难题，直到采用了 Orca。我以前要费很大功夫才能获得所需的内部扫描。我们重新编制预算，试图为 Zip 产品开发所需的精力、劳动和减损确定开支。我编写了商业案例，将这些无形资产包括在内。我告诉高管们，让团队搁置常规工作去部署代理并进行设置需要耗费多长时间，一一排查找出重要的漏洞并手动进行所有关联需要耗费多长时间。这些工作所需的时间多到无法想象。此外，集成成本也高到不可思议。”

他表示，借助 Orca，由于覆盖范围高达 100%，因此风险大幅减少了。而且与任何其他产品相比，几乎节省了 100% 的时间。“部署需要 20 分钟，它在后端与 Jira 集成，”Robinson 表示，“从系统管理员、基础架构或 DevOps 的角度来看，这是一劳永逸的解决方案。Orca 的这一商业案例非常强有力。”



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，而无需部署代理。

只要几分钟就可以连接您的第一个云账户，
获得亲身体验：访问 orca.security

© 版权所有 Orca Security 2021。本材料中引用的所有商标、服务标志和商号名均为其各自所有者的财产。