Rapyd 利用 Orca Security 的深度云可见性，为其全球支付系统保驾护航

Rapyd

行业	冠军	云环境
金融服务	Nir Rothenbergm，首席信息安全官	AWS

“Orca 在帮助我们使用 DevOps 方面发挥了巨大的作用。现在，我的系统管理员可以向 DevOps 显示和解释我们发现的问题。我们现在协作得更紧密，对他们的帮助更大了。这是向 DevSecOps 迈出的一大步，DevOps 和我的安全团队之间的组织摩擦不复存在。”

Nir Rothenberg
首席信息安全官
Rapyd

云安全挑战

- 获取完整的上下文可见性，以推动优先补丁的管理
- 向审计人员展示良好的治理和监管合规
- 简化安全工作

云安全结果

- 立即获得对其云基础架构的充分可见性
- 将 Orca 与 Jira 集成，以实现 CI/CD 流水线的自动化，从而执行与安全相关的任务
- 与 DevOps 创建了协作环境，以转向 DevSecOps

Rapyd 打破了环球支付的的障碍

Rapyd 正在解决全球支付行业中存在的碎片化问题。它构建的技术可以消除跨境商务的后端复杂性，也可以提供关于当地的支付专业知识。

全球电商公司、技术公司、市场和金融机构使用 Rapyd 的金融科技即服务平台，以简单的方式将本地化的金融技术和支付功能无缝嵌入到其应用程序中。Rapyd 全球支付网络支持企业访问全球最大的当地支付网络，提供 900 多种当地首选支付方式。这些包括 100 多个国家/地区的银行转账、电子钱包和现金。

Orca 解决了补丁管理的痼疾

如今，每种全球数字支付系统都必须毫不松懈地关注安全问题。这就是管理 IT 和安全运营的 Rapyd 首席信息安全官 Nir Rothenberg 感兴趣的方面。虽然他的公司已实施良好的安全措施，但如何向审计人员证明这一点颇具挑战性。

“我们的业务是支付，所以我们必须符合 PCI DSS 的规定，而且我们确实做到了，”Rothenberg 表示，“审计人员每年都希望看到我们已经实施良好的补丁修复流程。我们不懈地修补，但出于多种原因，从未 100% 做到。在我们发现 Orca 之前，记录一切相关内容以证明我们在这方面的掌控是一大痛点。”

Rapyd 完全在云端运行，一切都存储在 AWS 上。Rothenberg 想要一款智能工具，来全面了解那些真正需要补丁的服务器。他希望有一个确定了优先级的清单，并且有清楚的上下文。很多工具都可以扫描并列出需要补丁的内容，但没有上下文，清单就会很长，而且很多内容都毫无意义。

“原生 AWS 工具缺乏智能。AWS Inspector 扫描可以为我们提供结果，但并不总是适合我们的上下文，”Rothenberg 表示，“我们会得到一个包括 1,000 个补丁的清单，每一个都被认为很重要。但我们并未部署某些补丁，因为它们与我们的分布不匹配，或者它们适用于修补无关紧要的离线服务器。如果我将这样的报告展示给审计人员，他们就会认为我们不关心业务的安全。假设有个服务器存在严重的漏洞。有个补丁适用于 Ubuntu 18.4，但我们的是 Ubuntu 18.9。在这种情况下，我们就无法修补。不仅如此，而且这台服务器并不面向互联网，因此这个问题并不重要。Orca 会告诉我们，‘关键的补丁，中等的风险’。我可以向审计人员展示这些，以证明我们的操作是合理的。”

Rothenberg 评估了包括 GuardDuty、Inspector 和 Detective 在内的多种 AWS 工具，以及基于代理的传统安全工具和网络扫描器。他发现要让这些工具发挥作用需要大量的开销，远远超过了 Orca 所提供的现成服务的成本。“对于基于代理的工具，我们必须创建服务器、部署代理、编写并运行脚本、了解我们的环境、配置数据面板，以显示我们想要看到的内容。我们必须教它什么是风险、什么不是风险，我们还要进行大量的分析工作。我们总是在调整它，因为风险是动态的，随时会发生变化。使用 Orca，所有这些步骤都可以自动实现。”

Orca 识别不符合互联网安全中心控制 (CIS Controls) 和 PII 风险的问题

Rothenberg 负责监督 Rapyd 对互联网安全控制中心的遵守情况。为此，他还尝试了原生 AWS 工具，并发现这些工具功能不足。“我们必须自己搞清楚它们的扫描结果意味着什么。但使用 Orca 时，扫描结果都经过了整理并标明重点。我们可以立即查看 CIS 违规情况，并优先进行处理。我们已经将 Orca 与 Jira 进行了集成，如果要将工作分配给 DevOps，单击一下按钮即可。”

Rothenberg 表示创建工单对于内部任务的跟踪至关重要。“随时了解任务和相关风险，我们就可以确定发送到 DevOps 的问题的优先级，以免他们不堪重负。如果我们接受审计，我们可以向他们展示：‘这就是我们的流水线，我们的工作计划。’一切内容都在 Jira 中，一切都有审计跟踪。”

CISO 还通过 Orca 在未得到适当保护的文件中识别 PII 面临风险的情形。“作为一家支付公司，我们对 PII 暴露非常敏感。如果服务器中含有 PII 或暴露了加密密钥，Orca 就会立即捕捉到，并向我们提供基于该机器和特定资产的风险。我们能够快速修复问题。”

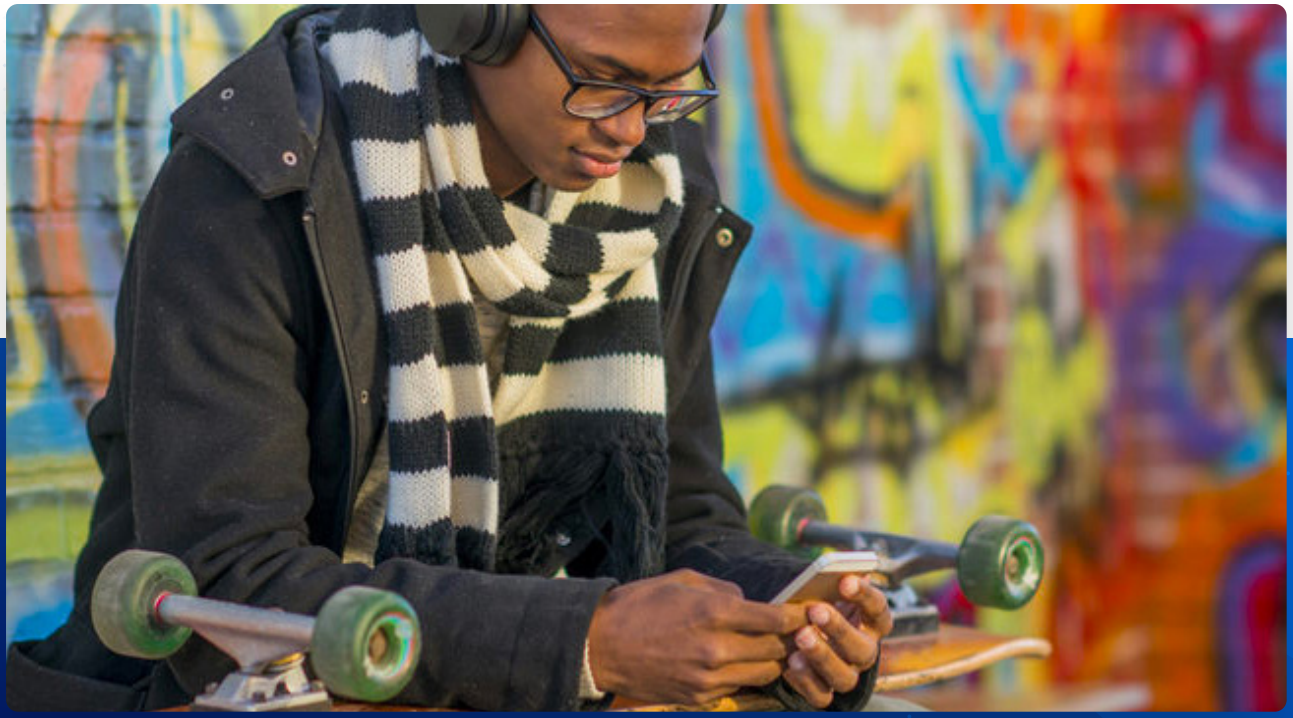
前几年，Rapyd 在 Excel 电子表格中跟踪漏洞。Orca 消除了这一流程。“现在一切都已自动化，且配有 CI/CD 流水线。下次我们接受审计时，我可以展示 Orca 和 Jira 报告，以显示我们正在跟踪的风险以及为了修复它们所做的努力，”Rothenberg 表示，“通过我们现在监控资产的方式，证明修补与合规变得轻而易举。”

> “Orca 的扫描会返回一份有意义、实用的报告，并且所有内容都有相应的上下文。除了发现结果，它还提供外围考虑，指导我们的修补管理流程。”
>
> **Nir Rothenberg**
> Rapyd
> 首席信息安全官

简化促成更高的安全性

Orca 简化了 Rothenberg 的安全团队的日常工作。“将 Orca 连接到我们的环境后，它立刻就发现了大量有意义的信息。没有 Orca，我们的可见性绝不会达到这种程度。”

“Orca 在帮助我们使用 DevOps 方面发挥了巨大的作用，”Rothenberg 表示，“我的系统管理员现在可以与 DevOps 团队面对面沟通。他可以解释我们发现了什么，并展示给他们看。这有助于提高我们的专业性，帮助我们更好地查看环境，更好地了解环境。现在，我们与 DevOps 的协作更加密切，对他们也更加有帮助。这是向 DevSecOps 迈出的实质性一步。现在，我们是一台运转良好的机器。安全团队和 DevOps 之间的组织摩擦已消失。”



关于 Orca Security

Orca Security 利用其独特的、专利申请中的 SideScanning™ 技术为 AWS、Azure 和 GCP 提供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。