Paidy 转而使用 Orca Security 以实现多云可见性，节省了两个 FTE 和每年 50 万美元的云安全管理费用

位置
东京

行业
金融服务

云环境
AWS、Azure、GCP

“我们有 12 个 AWS 账户。我们之前不知道其中都有些什么内容，于是把它们都连上了 Orca。不到 30 分钟，我们就对所有账户的运行情况有了很清楚的了解。我们无法通过任何其他方式如此迅速地做到这一点。”

Jeremy Turner
Paidy
高级云安全工程师

云安全挑战

- 数百名开发人员将微服务推送至多云中的数十个账户，使得跟踪和保护该公司在云中的所有资产很困难
- 自行构建解决方案至少需要两个 FTE 工作一年，以及每年 50 万美元的维护费用
- 寻求主动保护 PII，并符合日本法规，如《跨境隐私规则体系》和《个人信息保护法》

云安全结果

- 三十分钟后即开始获得对其云资产的可见性；将 12 个 AWS 账户连到 Orca Security，识别出“重大缺陷”
- 每年节省 50 万美元的繁琐云安全工作开支
- 可以向审计人员证明其有能力识别和保护 PII
- 更快速的商家入驻驱动收入增长

Paidy - 日本云端金融机构

Paidy 是金融科技领军企业，为日本大众市场和企业提供无卡支付和其他金融服务。其解决方案处于革新性在线和移动支付、P2P 转账、个人金融和商家结算等服务的前沿。Paidy 支持客户仅使用其电子邮件地址和手机号码即可结账。无需信用卡或预先注册。为防止欺诈，每笔交易都使用 PIN 通过 SMS 进行身份验证。客户可以现在购物，然后在下月支付一份合并账单。

Paidy 的整个平台在云中运行，主要跨多个 AWS 账户，但也跨 Azure 和 GCP。它具有多个测试和开发环境。平台处理金融交易，其中安全是最大的问题。CISO Felix Beatty 负责优化 Paidy 的总体安全态势。

“我们本质上是个云端金融机构，”Beatty 表示，“由于我们的发展十分迅速，不到一年就积累了 300 多万个客户，因此我们有一些可以改进的业务领域，其中之一就是云安全。现在，我们的大多数服务都在云端运行，因此我们需要云安全解决方案，可以立即显示重大问题，以便我们能够快速解决它们。”

“代理可能或可能不适用于该 Linux 内核，Windows 版本也是如此。关键是有太多的变量发挥作用。跟代理打了那么多年的交道，之后看到 Orca 的安装和使用那么轻松，我就知道它的无代理方式既是一项重大创新，也是游戏规则的改变者。”

Jeremy Turner
Paidy
高级云安全工程师

Paidy 的大规模云环境导致很难做到完全可见

了解 Paidy 平台上的所有内容是他面临的最大挑战之一。“我们的云环境庞大而复杂，很难管理所有这些动态资产，”Beatty 表示，“我们有数百名开发人员尝试将微服务以尽可能快的速度地推送至云端，启动和关闭实例，创建备份，创建 S3 存储桶，并快速移动，快到在任何给定的瞬间都难以了解我们拥有什么内容。我们需要知道：‘我们所有云资产的当前安全态势如何?’”

高级云安全工程师 Jeremy Turner 是他的左右手，负责保障云环境的安全。在加入 Paidy 之前，两人就是一个团队，并了解如何应对其安全挑战。

安全代理很好 - 前提是它们有效（通常无效）

“我一直都在从事这方面的工作，”Turner 表示，“我了解到，任何处理安全和漏洞的产品通常都需要安装某种代理。如果你在信息安全领域工作过一段时间，你就知道代理会中断，它们需要更新，并且可能成为其他安全漏洞的载体。”

Turner 承认，代理很好，前提是它们有效。“代理通常无效。需要考虑的依赖性和其他内容太多了。代理可能或可能不适用于该 Linux 内核，Windows 版本也是如此。关键是有太多的变量发挥作用。跟代理打了那么多年的交道，之后看到 Orca 的安装和使用那么轻松，我就知道它的无代理方式既是一项重大创新，也是游戏规则的改变者。”Turner 表示。

传统漏洞扫描器和 AWS 工具不适合

Paidy 安全团队拥有使用各种针对云环境进行了改造的传统工具的经验。Turner 称："我在企业环境或测试中使用过 Trend Micro、Qualys 和 Tenable。Tenable 和 Qualys 似乎都是将传统企业产品勉强转移到了云端。但那样做的效果并不理想，因为仍然需要使用代理。我们还是得对付那些并非为无服务器或容器而开发的技术。"

Paidy 还排除了使用网络扫描器的可能性。Turner 表示："我用过未经身份验证的扫描器，知道它们的可见性有限，而且可能导致停机。经过身份验证的扫描器可能会为你提供更多的漏洞数据，但仍然需要进行大量的配置工作以及更高的权限。这会导致企业暴露在风险中，因为你本质上还有一个共享账户和密码。"

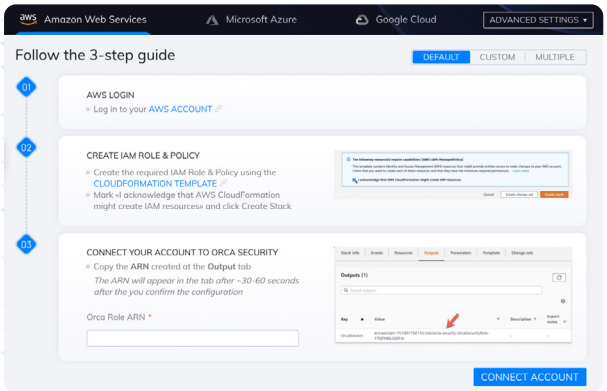
Amazon 等云提供商确实提供安全扫描工具。"Amazon 的漏洞扫描器 AWS Inspector 需要配置代理。通常情况下将它烘焙到 Amazon AMI 中，但它仅适用于特定的 AMI，"他继续说道，"AWS GuardDuty 满足了漏洞扫描和合规性检查的需求，但报告是最大的问题，使用数据也很难。它只会弹出一个漏洞清单，然后由我们决定如何处理它们。"

Beatty 补充道："由于我们有多个 AWS 账户，而且是多云环境，所以很难获得单一视图，来查看正在发生的一切。多云可见性是我们的头号难题。其次，我们没有

"Tenable 和 Qualys 似乎都将传统企业产品不严格地迁移到了云端。但那样做的效果并不理想，因为仍然需要使用代理。我们还是得对付那些并非为无服务器或容器而开发的技术。"

Jeremy Turner
Paidy
高级云安全工程师

时间和资源去协调工具的使用，例如，AWS 服务或类似工具。我们希望使用一项无需任何代理的服务，我们不需要定期更新它，它就可以正常运行。”对 Paidy 而言，Orca Security 可以满足所有这些需求，而且更多。



Orca SideScanning™ 提供完全可见性，解燃眉之急

Orca Security 平台与其他安全工具大不相同。它作为 SaaS 提供，从侧面读取带外云块存储，因此得名 SideScanning™。它不在客户的云环境中运行代码，而是为其云环境构建只读模型，然后对模型进行扫描，以评估潜在的安全问题。

拥有完全的可见性是 Turner 最感兴趣的功能。“可见性是每个组织都面临的问题。Orca 几乎可以立即为我们提供针对威胁形势的广泛而深入的可见性，”Turner 表示，“当我们获取这些数据并展示给同事们时，他们觉得不可思议。一个事例是，Orca 揭示了某个系统的一个‘重大缺陷’，这个缺陷在测试环境中存在了约两三年的时间。

该系统运行的是完全过时的操作系统。Orca 识别出这个问题后，我们就为工程师创建了工单，要求其立即解决。我们很幸运在系统进入用户验收测试 (UAT) 和生产之前捕获了这个漏洞。”

Beatty 同意可见性的重要性：“如果问题就摆在你面前，就没有理由忽视它们。在 Orca 的数据面板显示‘重大缺陷’时，就再清楚不过了。”

Orca 还帮助 Paidy 解决了账户扩张的问题。“我们运行 12 个 AWS 账户，”Turner 表示，“我们根本不知道里面存储着什么，所以就把它们连到了 Orca 中。不到 30 分钟，我们就了解了所有账户内运行的内容。我们无法通过任何其他方式如此迅速地做到这一点。”

资产管理是 Orca Security 为 Paidy 提供的另一项功能。Orca 提供每项资产的位置、元数据和漏洞清单的编目。“我可以选择一个实例，查看谁登录了它，有多少次失败的登录尝试，或者上面安装了什么软件包，这种感觉太酷了。我很高兴能够实现这一点，每个实例无需依赖代理。”Turner 表示。

Orca Security 识别并保护 PII，减轻了 Paidy 的合规性工作

随着 Paidy 使用 Orca Security 平台的经验越来越丰富，其团队找到了更多使用它生成的数据的方式。“作为一家金融科技公司，我们非常关注恶意数据组合，Orca 在这方面提供了帮助，”Turner 表示，“例如，客户必须提供手机号码，才能使用我们的服务。但是，如果我们处理家庭住址或电子邮件地址，以及可能的银行账户信

息和购买记录，那么我们就会涉及 PII 问题和日本数据隐私法规。”

Turner 解释 Orca 如何帮助保护 PII：“一个功能让我们了解 Orca 是否能察觉到 PII 的问题。这就像是个信标，告诉我们：‘这台服务器含有并不属于 paidy.com 的电子邮件地址。这是怎么回事？’然后，我们就可以进行调查。现在，工具不会说‘这是个恶意的数据组合’，但它会告诉我们去哪里寻找。我们遇到过这样的情况，其中数据科学团队创建了一个数据库互连器，产生了这样的恶意数据组合。Orca 帮助我们及时”发现了这一问题并加以解决。”

Paidy 必须遵守大量数据隐私法。日本的《跨境隐私规则体系》与欧盟的 GDPR 类似，而且该国的《个人信息保护法》于 2004 年颁布。Orca 有助于向审计人员证明，Paidy 完全有能力识别和加密个人信息。Paidy 大可以放心，因为它知道 Orca 有能力扫描到易受攻击的 PII。

Turner 利用 Orca Security 与 Jira 的集成，来创建工单。反过来，这些操作会触发工作流程，以便人们和流程能够采取适当的行动；例如，加密敏感数据或修复 Orca 找到的其他问题。

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。

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

© 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。