Orca Security 是 Databricks 的明智之选

行业
企业技术

冠军
Caleb Sima：
信息安全副总裁

云环境
AWS、Azure、
Google Cloud

“Orca Security 提供了与机器上安装的代理类似而且更多的功能，但却不会影响运行。它非常出色。这正是我想要的。”

Caleb Sima
信息安全副总裁
Databricks

云安全挑战

- 无需部署代理就可以看到正在运行的所有内容
- 准确评估漏洞和风险，优先处理它们，以修复问题
- 支持多云资产
- 避免与软件工程的摩擦

云安全结果

- 通过准确、可操作和上下文中的风险优先警报获得可见性
- 能够解决所有主要的安全问题；现在监测较小的问题
- 单一的带外工具提供所有云系统中的漏洞识别、资产库存，并监控和检测正在发生的事情
- 该技术完全由安全团队控制

Databicks 管理风险，以帮助客户成功

Databricks 是一家领先的数据分析和机器学习公司。今天，全球有 5000 多个组织 — 包括一系列《财富》500 强公司 — 依赖 Databricks 来进行大规模数据工程、协作数据科学、全生命周期机器学习和业务分析。该公司有数百个全球合作伙伴，其中包括 Microsoft、Amazon、Informatica 和 Cap Gemini 等知名公司。

Databricks 作为一家企业技术公司，属于客户和合作伙伴供应链的一部分，非常重视监控和管理自己的风险，以赢得和保留他们的信任。它投资于高质量的安全产品和供应商，以提供这种保证。

Databricks 使用 AWS、Azure 和 GCP 运行多云环境。在所有三个平台上运行，使云运营商原生工具难以全面地实现统一的安全性。因此，选择合适的工具来维护安全环境至关重要。

安全企业家称 Orca “既简单又出色”

Caleb Sima 是该公司的信息安全副总裁。在他的大部分职业生涯中，他是一个连续企业家，创立、开发和出售了几家网络安全公司。几年前，Sima 将他的职业生涯从创始人和企业家转变为公司内部的捍卫者。这让他对部署捍卫和保护数据库应用程序和云环境的最佳技术类型有了独特的视角。

“作为企业家的我说：‘就是它了！’这是如此明显和简单，但非常出色。这是一个明智之选。”

Caleb Sima
信息安全副总裁
Databricks

“当我加入 Databricks 时，我有机会从零开始构建我的安全团队。我们共同评估并选择了安全技术栈的工具，”他说。一个重要的标准是不影响 Databricks 软件工程团队的工作。“我们是一家快速发展的公司，我不想做任何事情来减慢我们工程师的进度。我们的技术栈变化如此迅速，安装资源代理非常具有挑战性和复杂性。”

“我听说了 Orca 之后，真的很想看看它的演示。我很感兴趣的是通过基本上使用磁盘快照并分析它们，以解决活动和漏洞，来了解它如何运行。”

代理产生复杂性；复杂性增加了风险

Sima 知道他不想在机器上使用需要安装代理的产品，特别是在关键的基础架构和主机方面。

> “Orca 以一种可操作性非常好的方式对警报进行风险优先排序，在提供的信息和给予的安全级别方面都是如此。这是一流的、纯粹的魔法。”
>
> **Caleb Sima**
> 信息安全副总裁
> Databricks

“无论对于安全还是工程，想让基于代理的解决方案正常工作，都会浪费大量精力，”他说。“每个使用代理的供应商都说它们是轻量级的。问题不在于 CPU 功率，而在于增加更多的风险。您加载到系统中的东西越多，添加的复杂性就越多，出现问题的风险就越大。”

Orca 的价值显而易见

Databricks 注册了 POC，并很快让 Orca 上线运行。它只需要设置一些云帐户权限。几个小时内，Orca 就开始在其数据面板上显示结果。Sima 及其安全同事无法相信他们看到的。“我记得在浏览警报时，我感到很惊讶，”Sima 说，“起初，我们以为看到的是错误警报。然后我们自己检查了一下，才发现每一个警报都准确无误。”

Databricks 面临着许多挑战，希望通过 Orca 这样的解决方案来解决。最初的动机是获取所有正在运行中的内容的可见性，而无需在机器上安装代理。他们还寻找一个有助于云监控、检测和响应的工具。它想识别其所有云环境中的风险。“Orca 以某种方式实现了这些需求之间的平衡，满足了我们所有标准。“所有云环境都可以互相通信，并且与 Orca 通信，让我们对整体风险有了更高层次的了解。”

“我们最大的痛点是云工作负载、实例和机器的可见性，”Sima 报告说。“POC 向我们表明，我们不仅可以看到正在发生的事情，而且 Orca 还可以告诉我们可能发生的事情。也就是说，“这就是可能发生的横向移动，以及攻击者可能访问的资源类型。如此洞察力令人难以置信，所以我们立即看到了价值。”

Sima 非常赞赏 Orca 在发现结果上的准确性和深度。“你可以检测出这台机器上有大量恰好包含密钥的 SSH 登录失败，这些密钥可以访问这些机器，其中还包含可以访问这些基础架构的 AWS 凭证。显然，此机器受到了攻击，而且它也权限过大，这都是事实。您可以做到这一点，并以相当可理解的方式将其传达给组织中的任何人，” 这非常有用。”Sima 说。

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。与云提供商即时、只读和无冲突地集成后，它能检测漏洞、恶意软件、错误配置、侧向移动风险、身份验证风险和不安全的高风险数据，然后根据潜在问题、可访问性和爆发范围对风险进行优先级排序，且无需部署任何代理。

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。