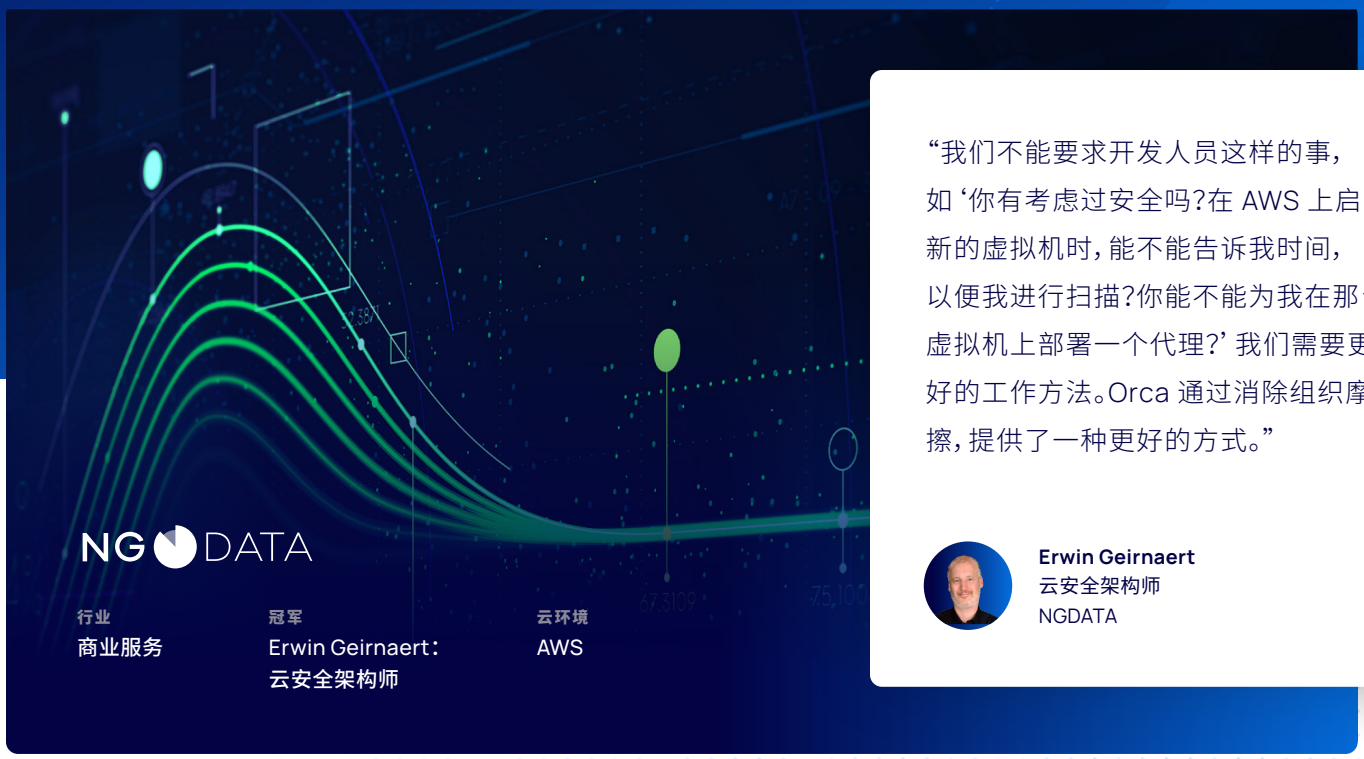
Orca Security 仅为 NGDATA 提供一种工具，但可以同时满足安全、DevOps 和合规性需求



“我们不能要求开发人员这样的事，如‘你有考虑过安全吗?在 AWS 上启动新的虚拟机时，能不能告诉我时间，以便我进行扫描?你能不能为我在那台虚拟机上部署一个代理?’我们需要更好的工作方法。Orca 通过消除组织摩擦，提供了一种更好的方式。”

Erwin Geirnaert
云安全架构师
NGDATA

云安全挑战

- 需要 AWS 资产的全球实时视图，以了解经常变化的资产，最好不使用代理
- 确保客户资产和公司知识产权得到保护
- 需要可以与开发人员的工作方式集成的工具

云安全结果

- 实时获取所有 NGDATA 资产的完整视图
- 与 Jira 集成，以实现漏洞修复流程的自动化
- 消除了与开发人员之间存在的组织摩擦，以转到 DevSecOps 方式

NGDATA 通过数据洞察帮助企业推动更具个性化的客户体验

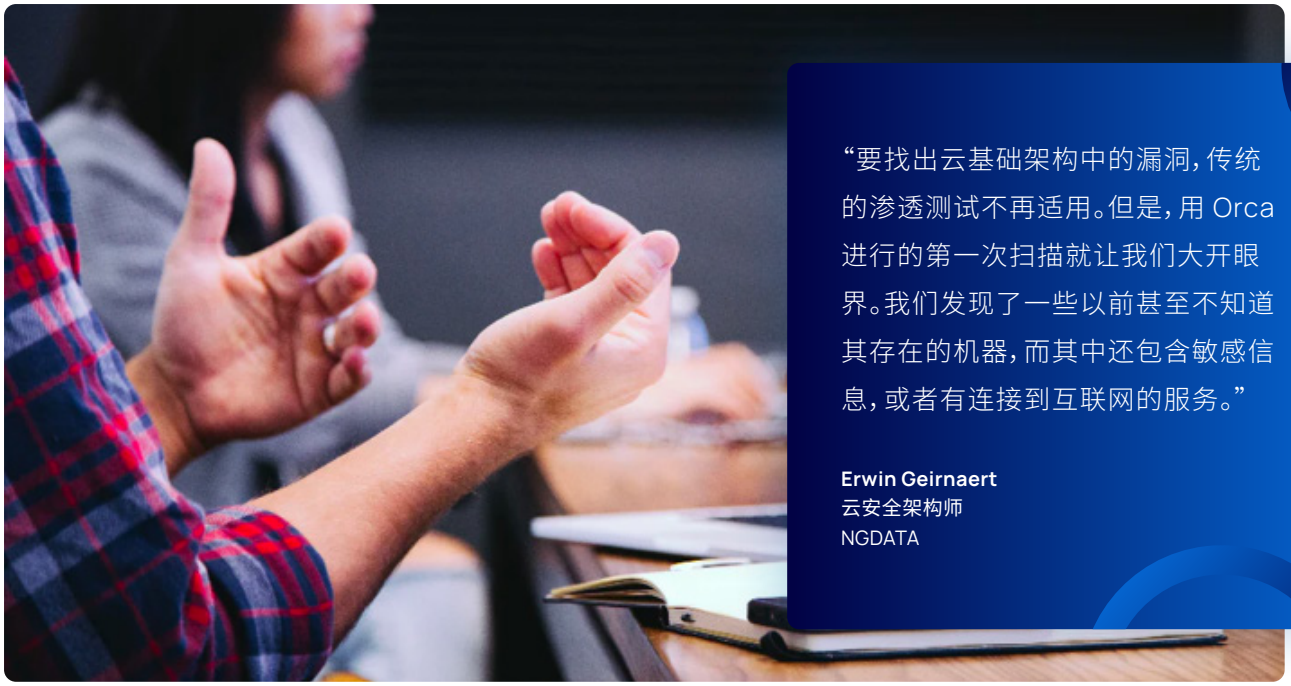
NGDATA 帮助金融服务、电信、公用事业和酒店等数据驱动行业内的企业提升互连的客户体验。它们的人工智能驱动型 CDP 和数字转换服务通过 Customer DNA 将人们置于每项业务的中心，Customer DNA 不断从行为中学习，从而为全球各企业提供卓越的体验。NGDATA 总部位于比利时的根特，并在美国、欧洲和亚太地区设有办事处。

该软件平台可以本地安装或部署在私有云中，而所有产品开发工作均在云端完成。NGDATA 已与 Shift Left Security 的云安全架构师 Erwin Geirnaert 签署了合同，维持其云环境的秩序，识别并系统性消除漏洞，并实施可以维持良好安全态势的程序。

Orca Security 弥补了传统安全扫描的短板

Geirnaert 的第一项任务是经典的渗透测试，以尽快识别当前环境的状况。扫描的作用微乎其微，因为它只是不断变化的云资产的快照。但即使使用经过认证的扫描器，如果它不清楚要扫描什么，还是会存在差距。“这根本不适用于云原生方式。”Geirnaert 表示。

他然后尝试从拉取到 Sumo Logic 数据面板的 Amazon 日志中获取有关要扫描的 IP 地址范围的信息。这一尝试得到了一些令人不安的结果。



“要找出云基础架构中的漏洞，传统的渗透测试不再适用。但是，用 Orca 进行的第一次扫描就让我们大开眼界。我们发现了一些以前甚至不知道其存在的机器，而其中还包含敏感信息，或者有连接到互联网的服务。”

Erwin Geirnaert
云安全架构师
NGDATA

Geirnaert 说明了 Orca 如何使 DevSecOps 动态成为可能。“开发人员可以访问 AWS 控制台，因此他可以使用只读策略将 Orca 连接到 AWS。他不需要部署、应用或安装任何东西，他只需要配置 AWS，然后信赖 Orca 平台执行扫描。附加只读策略并使其运行大约需要 5 分钟。他立刻就看到了 Orca 正在进行的深度扫描结果。”

“借助完整的合规性视图，开发人员可以问自己：‘我是不是遗漏了 Amazon 中的某些安全设置，这可能影响我的安全态势?’ 他可以立即看到自己需要配置和启用的设置、需要使用的功能或进行的操作。Orca 还会更新合规性。即使没有发现漏洞，仅此一项就为我们提供了大量的信息，所以我们不需要求助于安全公司告诉我们该怎么做。Orca 会告诉我们需要做什么以及怎么做。”Geirnaert 表示。

> “Orca 允许我们为不同的用户授予不同角色的访问权限。首席信息安全官对合规性很感兴趣。安全工程师查看漏洞和警报。开发人员可以从数据面板中了解某些问题的原因。”
>
> **Erwin Geirnaert**
> 云安全架构师
> NGDATA

这要求他们找到一款这样的工具：可以连接到 AWS API，并获得所有 NGDATA 资产的实时视图。这样的工具应该可以揭示关键漏洞，以及任何 PII 或知识产权是否存在风险。在这次寻找过程中，Geirnaert 找到了 Orca Security。

“用 Orca 进行的第一次扫描就让我们大开眼界。我们发现了一些以前甚至不知道其存在的机器，而其中还包含敏感信息，或者有连接到互联网的服务。”凭借 Orca 返回的洞察，他设置了对所有 IP 地址和虚拟机的每日扫描，即使它们未连接到互联网。“我们需要充分了解我们必须采取哪些措施才能确保客户资产以及 NGDATA 自有知识产权得到保障。”

Orca 是 DevOps 的变革性工具

NGDATA 的开发人员遍布全球。Geirnaert 说：“我们不能要求开发人员：‘你考虑过安全吗?你在 AWS 上启动新的虚拟机时，能不能告诉我，我好进行扫描?你能不能为我在那台虚拟机上部署一个代理?’ 我们需要更好的工作方法。Orca 通过消除所有这些组织摩擦，提供了一种更好的方式。”

“我坚信 DevOps 方式，然后转到云原生和无服务器架构，因为这将有助于提高安全性，而无需将开发人员培训成安全方面的能手。我们需要使用与他们的工作方式集成的工具来支持他们。”

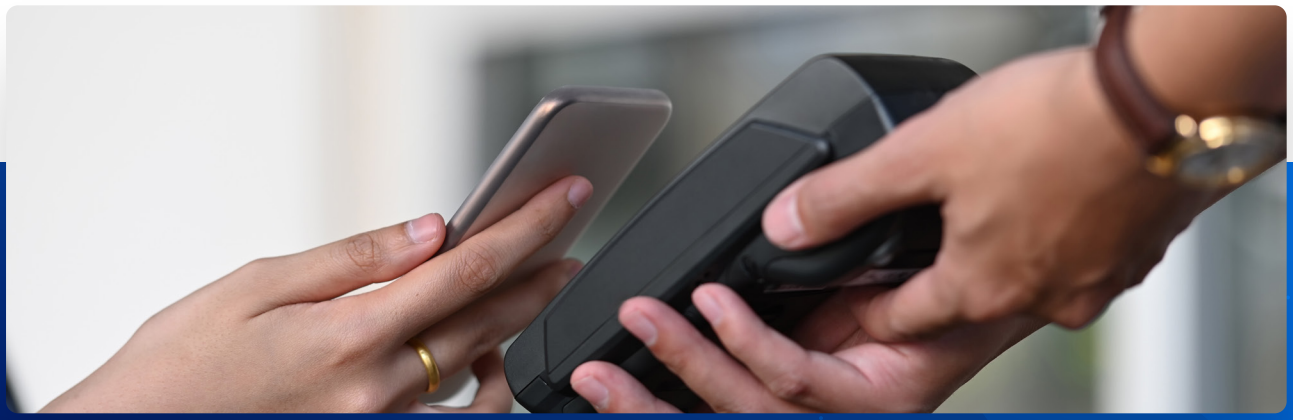
促进法规和安全框架的合规性

Geirnaert 刚开始就职于 NGDATA 时，就根据 AWS 互联网安全中心合规框架编制了一份最佳做法清单。以前，他将含有 100 项的清单用作项目管理工具，来分配任务。现在，他不再需要这份清单了。

“在我们启动 Orca 时，它可以动态检查合规性要求。在使用 Orca 前，我们自己在 Sumo Logic 中编写了此类检查。在查看 AWS CloudTrail 日志中的事件时，我们会捕获它们并在数据面板中展示。现在，我们可以在单个 Orca 数据面板中立即自动查看所有内容。”

GDPR 合规变得更加容易，因为 Orca 在服务器和文件中查找 PII。Orca 有助于查找隐藏的 PII，并显示 PII 可能存在的位置。作为安全人员，Geirnaet 没有访问生产环境的权限，而 Orca 为他提供了通常没有的可见性。如果涉及 PII，这有助于指导修补或缓解问题。

Orca 也简化了审计流程。“我们可以轻松过滤，以显示 PII 存储的位置。由于都记录在案，我们可以轻松向审计人员展示他们要求的证据。”Geirnaert 表示。



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