保险业的创新者 Lemonade 通过 Orca Security 实现了从 0% 到 100% 的云端可视性

行业
保险

冠军
乔纳森·贾菲，首席信息安全官

云环境
AWS

“Orca 无容置疑是我们最重要的云安全产品。它能提供易消化的信息，不会使你应接不暇，其重要之处不可言喻。”

乔纳森·贾菲
首席信息安全官
Lemonade

云安全挑战

- 获得整个云资产的可见性
- 快速将重要问题划分为“易消化的小块”
- 对 DevOps 的影响最小

云安全结果

- 100% 云帐户覆盖，具有完全可见性和优先修复功能，且不对 DevOps 和生产环境造成影响
- 能够满足合规要求并向审计员示范管理
- Orca 数据面板能对紧急问题提出实用洞见
- 覆盖无缺口，非常省心

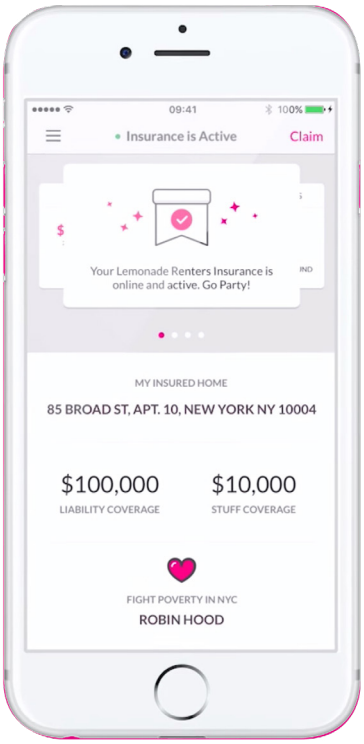
Lemonade 正在彻底改变保险市场

Lemonade 在美国和欧洲提供保险服务。它属于“保险技术”市场的一部分，让保险供应商利用先进技术提供传统公司无法企及的创新产品和服务。作为一家较为年轻的公司，Lemonade 拥有 cloudnative 技术栈使它可以 100% 在线运行。这使 Lemonade 成为保险市场上一个灵活的竞争对手。比如说，Lemonade 可以通过 AI 机器人以网络和移动应用程序的形式提供保单报价。同时，Lemonade 是一家 A 级、全面受规管的公司，并由保险业最受信任的保险公司再保险。

首席信息安全官以之前的 Orca 使用经验指引道路

Lemonade 的基础架构完全在 AWS 云中，因此要实时了解漏洞和安全风险是一项挑战。甚至是 Amazon 的原生工具也不能提供安全和开发维护专业人员所需的所有信息。

乔纳森·贾菲于 2020 年加入 Lemonade 作为其首席信息安全官。他立刻着手寻求整个云资产的可见性，来更好地为安全风险作评估。“当我加入的时候，我们没有一个合适的解决方案来检查漏洞，”他说。“我很希望在云漏洞问题上有比当时更好的可视性。”



Orca 打败了基于代理的竞争对手 Lacework 和 Palo Alto Prisma Cloud

“我们对 Orca Security、Palo Alto Prisma Cloud 和 Lacework 进行了评估，”贾菲说。“我的上一家公司使用 Lacework 已有一年多。我在那里的最后四个月里，我们还曾用 PoC 运行 Orca，因此很容易拿 Orca 来作比较。然后我们对 Prisma Cloud 进行了广泛的评估。”

Lemonade 的评估团队必须依靠 Prisma Cloud 和 Lacework 的产品演示，尽管当时贾菲已经对 Orca 和 Lacework 非常熟悉。“与 Orca 不同的是，其他的需要代理。DevOps 人员不是很愿意安装和维护代理。

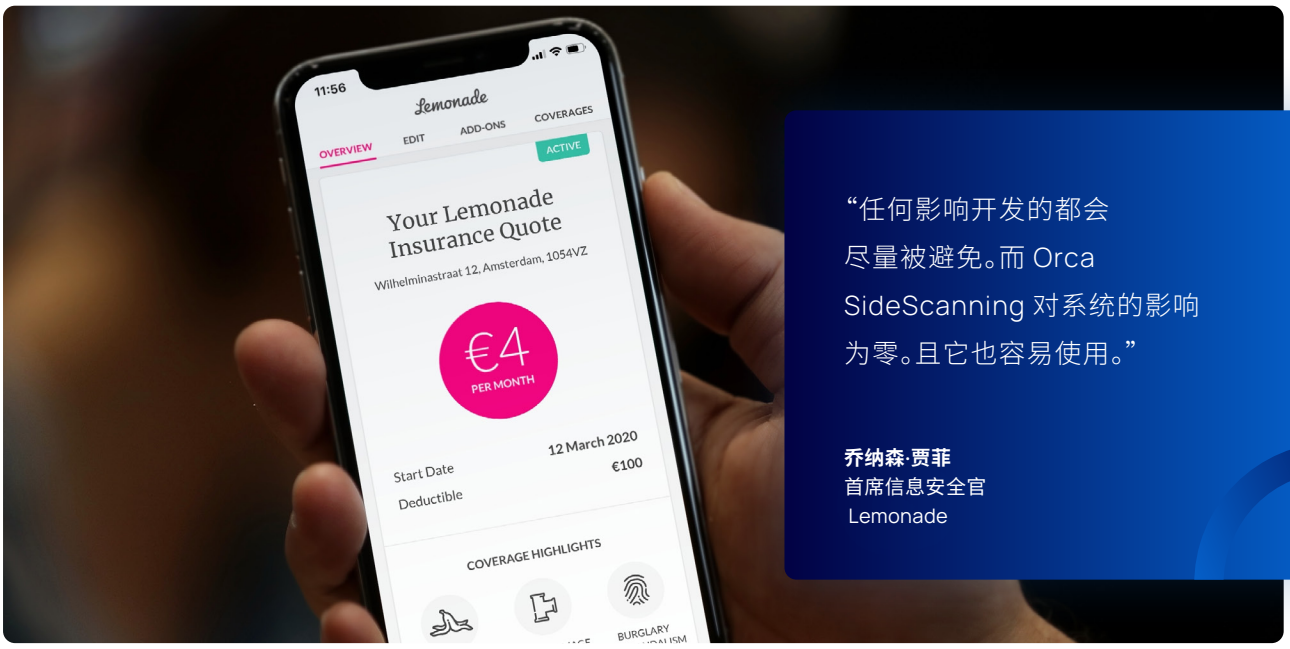
DevOps 人员还担心代理的性能可能会对我们的系统造成影响，尤其是在生产方面上。而且根据我以前使用 Laceworks 的经验，我知道它会有因代理丢失而减少可视度的烦恼。”Orca 在半小时内就在 POC 上完成了设置和全面部署。“启动和运行 Orca 轻而易举，”贾菲说。“我们马上就看到了结果。不到 24 小时，我们就可以看到所有 AWS 账户中的所有资源和环境。此外，我们还可以快速、轻松地看到 Orca 发现到的问题，还好幸运的是，这些都是容易处理的小问题。”

安全问题的 100% 覆盖率和优先处理

贾菲想在安全解决方案中寻求几个重要功能。“第一个是 100% 的覆盖率，这个是任何需要安装代理的工具都做不到的。我必须确保覆盖范围没有缺口。”

另一个必备功能是能够优先修复紧急的问题。“Lacework 提供了大量信息，但我们并没有从中找到用处；反而我们觉得它削弱了我们解决问题的能力。太多信息会淹没了有价值的东西。此外，它没有以一种可行的方式对信息进行优先排序。在使用 Lacework 时，我们的安全分析师在解析应该解决哪些问题上花了大部分时间。当他完成了上一步并选择问题来解决后，他又会遇到下一个问题：这是真的入侵还是又一个误报呢?- 这些都必须在他补救前得到解答。在使用 Orca 之前，我们会因为信息组织得太差而放弃去查看问题的解决办法。”

“Orca 则恰恰相反。利用统计提供的信息，我们可以按威胁类型、漏洞、帐户、受影响资源等进行分类显示。我们可以按类别查看前五项，例如被忽略的资源或漏洞等。



“任何影响开发的都会尽量被避免。而 Orca SideScanning 对系统的影响为零。且它也容易使用。”

乔纳森·贾菲
首席信息安全官
Lemonade

这就把一个个问题细分成了我们可以咀嚼的小问题，不像许多其他产品那样让所有问题一涌而来。我们可以迅速解决紧急问题，然后推迟或完全忽略那些不太重要的问题。”

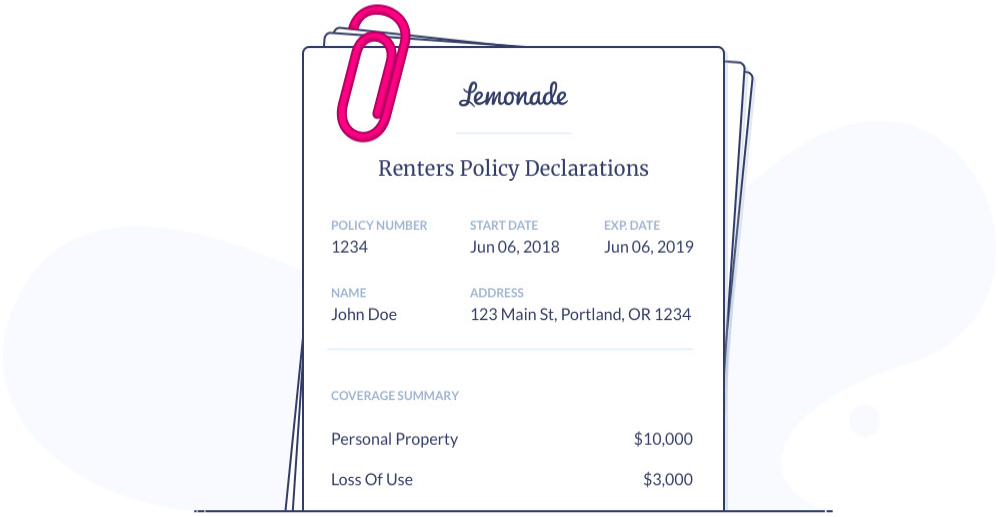
对于贾菲和他的团队来说，Orca 的数据看板提供了一种静心的效果，因为它不会提供过多的信息让人无从下手。他说，“Orca 的真正价值在于覆盖庞大数量的云安全、通知我们存在漏洞以及用精简的方式通知真正威胁。”

如果存在潜在的数据丢失问题或个人数据暴露于危险区域的话，Orca 也会提醒贾菲。Lemonade 团队可以在审计报告显示这些问题之前就早早地进行纠正。“Orca 在检测潜在的信用卡数据、电子邮件地址、身份证号码或其他国家身份证的暴露上表现非常出色，”贾菲说。“这些是我们可以迅速优先解决的问题。”

> “Orca 减轻了我们的头号痛点：与云相关的安全风险在哪里？在使用 Orca 之前，我们根本没有我需要的可见性。”
>
> **乔纳森·贾菲**
> 首席信息安全官
> Lemonade

供审计的管理证据

由于总部设立于纽约，因此 Lemonade 的业务受到纽约州金融服务部（NYDFS）的监管。此外，该公司还受各种欧盟法规的监管，并有自己的 SOC 2 审计。Orca 的报告帮助贾菲为各种监管和审计提供了管理证据。Orca 有助于减少我的审计工作；例如，我可以运行报告来显示我们一直采用最少权限控制，以及采用多重身份验证等。”

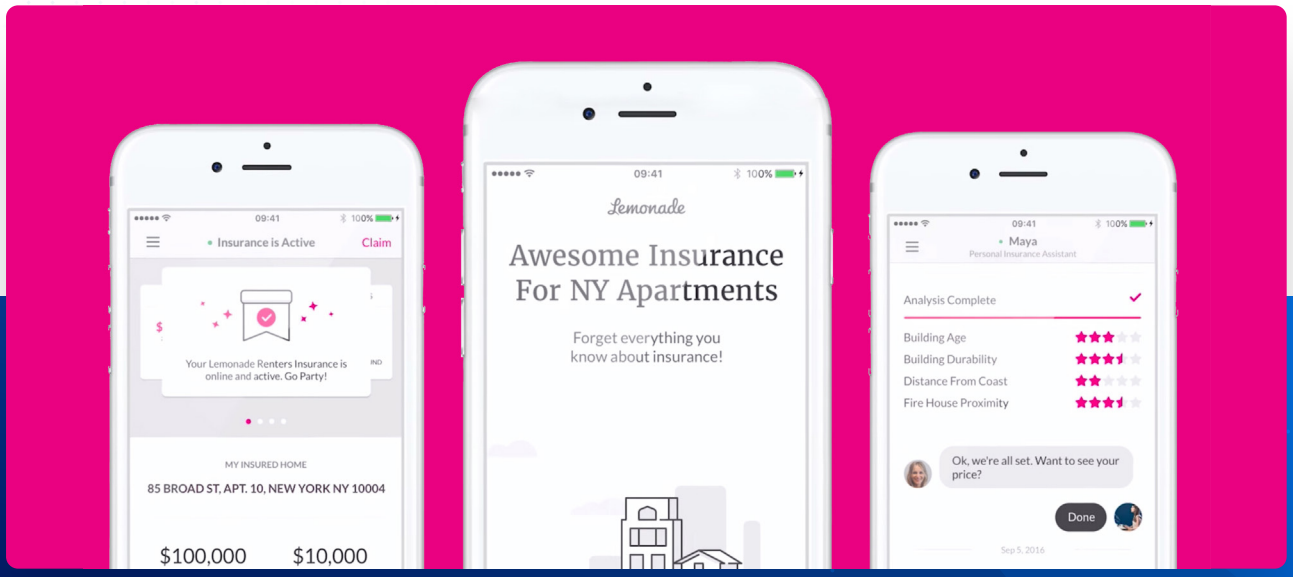


风险项目已大幅减少

Lemonade 已经大幅度地减少了其风险数量。“我们把这些减小成原来的六分之一，现在我们可以通过监控来控制它们，”贾菲说。“Orca 给我们指点该解决的问题，和无需担心的问题。”

贾菲最喜欢 Orca 的地方在于它列出优先问题的方式。“你可以按类别查看前五项，例如被忽略的资源或漏洞等。这就把一个个问题细分成了我们可以咀嚼的小问题，不像许多其他产品那样让所有问题一涌而来。”

他还很喜欢它的界面，说数据看板提供了一种静心的效果，因为它不会提供过多的信息让人无从着手。他说，“Orca 的真正价值在于覆盖庞大数量的云安全、通知我们存在漏洞以及用精简的方式通知真正的威胁。”



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，而且无需部署代理。

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。