Orca Security 帮助 BeyondTrust 保障数千名客户使用的云服务的安全

BeyondTrust

行业	冠军	云环境
IT 安全	Morey Haber：CTO 兼 CIO	AWS, Azure

“今天，Orca Security 管理着我们所有基于云的特权访问管理 (PAM) 解决方案。”

Morey Haber
首席技术官兼首席信息官
BeyondTrust

云安全挑战

- 使用基于代理的安全工具变得过于复杂且难以管理；而且它也没有提供足够的可见性
- 代理无法在公司定制的设备映像上加载
- 需要报告以帮助确保符合 ISO、SOC、CIS 和 PCI 的要求

云安全结果

- 两个月内全面投产；通过 Azure Sentinel 安全中心完全集成 - 包括与 ServiceNow、Jira 的工单处理和各种其他集成
- 能够保护和监控出售给客户的云解决方案，而不会给生产环境增加风险
- 将开发和 QA 时间减少了 1.5 FTE，同时提供更广泛的可见性和更具可操作性的评估结果
- Orca 报告可呈现与密码、防火墙配置、漏洞等相关的合规性证据

BeyondTrust 为超过 70% 的财富 500 强企业提供基于云的特权访问管理

BeyondTrust 是特权访问管理领域的全球领导者，使组织能够保护和管理其整个特权领域。超过 20,000 名客户——包括超过 70% 的财富 500 强企业——使用 BeyondTrust 的三种核心解决方案来保护自己的环境并获得需要的控制权，以降低风险、实现合规性和提高运营绩效。

Morey Haber 在 BeyondTrust 身兼数职。作为 CTO，他负责监督产品战略。他还是公司的 CISO，负责管理客户使用的 4,000 多个云部署方案的内部和云端安全。他还负责督导所有治理、风险和合规性方面工作。

Haber 在 IT 领域的 20 年全部投身于网络安全工作。他撰写了多本关于攻击媒介和漏洞管理策略的书籍，并且是 BeyondTrust 收购的一家公司的安全工程总监。他了解如何才能检测出那些让公司面临风险的技术缺陷。

Orca 采取新的云安全方法

看过 Orca Security 的演示之后，Haber 表现出浓厚的兴趣。“我彻底服了。在我专注于漏洞管理策略和产品的这些年里，这是一种拥有巨大潜力的全新方法。”

Haber 和他的云团队对 Orca 平台进行了试验。“我们安装几天后，它就开始发挥效用了。与竞争对手通过安装代理为我们提供的结果相比，它能获得更好的结果和更高的可见性。在使用 Orca 前，代理只为我们提供了实例运行时的可见性，没有向我们展示环境中其余部分的情况，”Haber 说。“它给我们留下了非常深刻的印象。Orca 现已全面运行，管理着我们如今销售的所有云解决方案。”

Orca 为 BeyondTrust 的客户工作负载保驾护航

BeyondTrust 展示了一个独特的 Orca Security 应用场景。大多数 Orca 客户用它来评估自己的云工作负载，而作为安全供应商，BeyondTrust 用它来监控运行客户正在使用的云解决方案的工作负载。如今，该公司支持 4,000 多个云部署，随着 BeyondTrust 继续快速增长，他们还计划部署更多解决方案。

> “20 多年来，我一直在使用各种漏洞评估解决方案。我甚至写了一本关于如何制定漏洞管理策略的书。但我从未见过像 Orca Security 平台这样的产品。这是一款不可多得的产品。”
>
> **Morey Haber**
> 首席技术官兼首席信息安全官
> BeyondTrust

Haber 引用了他现在如何使用 Orca 的一个例子。“BeyondTrust 的特权远程访问允许第三方访问客户的环境，比如检查 HVAC 系统、确保打印机正常工作，或处理任何可能的需求等。我们的解决方案可对目标系统执行凭据注入，因此第三方完全不会知道或看到密码。一旦他们登录，产品屏幕将录制并记录他们所做的一切，从而为远程访问实现真正的零信任架构。”

“Orca 有助于确保没有任何内容处于开放状态或出现配置错误，没有任何实例缺少补丁，并且我们客户的云环境中不存在漏洞，”Haber 说。“这是 Orca 凸显其重要价值的另一个例子。我们为自己的一种产品安装了新的防火墙。Orca 很快就识别出默认设置中存在的配置错误，所以我们能立即纠正它。否则，我们又怎么能看到呢？由于问题发生在外部，因此代理没办法提供帮助，但 Orca 发现了它。对我来说，其价值无法衡量。”

“Orca 有助于确保没有任何内容处于开放状态或出现配置错误，没有任何实例缺少补丁，并且我们客户的云环境中不存在漏洞，”

Morey Haber
首席技术官兼首席信息安全官
BeyondTrust

基于代理的解决方案存在的问题

BeyondTrust 使用行业内竞争对手的一种解决方案，对其内部资源和笔记本电脑进行传统的漏洞管理。在找到 Orca 之前，该公司尝试将其基于代理的技术用于基于云的解决方案，但遇到了许多问题。“根据基础设施和我们对该工具的了解，我们决定在自己的产品中使用他们的代理。我们的想法是为每台虚拟机都部署一个代理，"Haber 说。

“这需要多个虚拟机为一个客户端组成一个实例，再加上所有的后端管道。相关的成本尚且合理，但 DevOps 链 — 认证、构建、连接、运行、更新的过程以及其他所有事情 — 需要大约六个月的时间来实施。在我们飞速发展的过程中，我们新增了数以百计的客户，要保证所有这些代理正常运转是一件痛苦的事情。很快我们便发现，管理起来也变得非常困难。”

Haber 解释说，对于云环境，如果他需要将一个代理包整合到某个产品中，就必须从早期开发直到质保和生产阶段都要将代理包括在内。“我们必须设置环境让代理融入各个阶段，以确保它正常工作，获取数据输出，同时保证它不会崩溃。当您开始拥有数以千计的代理时，总会有一个或更多的代理发生崩溃，或者无法得到更新。然后我们必须排查故障，然后更新客户的生产环境。这是更改控制和合规性的噩梦，最好能完全避免。”

Orca 让 BeyondTrust 避免了这些问题。“有了 Orca，我便无需再操心代理需要的时间和投入。我再也不需要支付代理使用 CPU 的运行时间费用，而且将运营团队成员引入生产环境也不会导致更改控制方面的风险。”在节约成本方面，Haber 说：“每个客户端的代理成本约为每年 20 至 30 美元。当扩展到成百上千个客户端时，使用代理的成本就变得相当可观。使用 Orca，我们不必考虑任何这些因素。我估计我们为每个客户端节省了大约 2% 的运行时成本，并将我们的 DevOps 和 QA 时间减少了 1.5 FTE。”

代理不适合 BeyondTrust 的另一个关键原因，是它的产品之一使用了定制、安全强化的自定义内核。代理根本不能加载到该系统上。Orca 的 SideScanningTM 技术就没有此类问题。

“对于任何正在考虑跨地区扩展的公司，Orca 提供了简化的方法。该方法需要更少的设置时间，提供更快的价值实现，而且运行风险要低得多。”

Morey Haber
首席技术官兼首席信息安全官
BeyondTrust

Orca 合规性模块和集成是非常有用的工具

多项监管或行业合规性方面的要求对 BeyondTrust 至关重要。为了赢得客户的信任和业务，BeyondTrust 始终保持 SOC 和 ISO 合规性 — 两者在其 AWS 和 Azure 平台上都获得了全面认证。另外，尽管 BeyondTrust 不需要 PCI 合规性来达到其目的，但客户可能会许可其技术并在 PCI 区域中使用。因此，获得 PCI 认证就显得尤为重要。Orca 具有内置的合规性模块，可帮助 Haber 记录合规性要求（例如，有关密码、防火墙配置、PII 暴露风险等）。

Orca 与 Azure Sentinel 安全中心和 ServiceNow 的集成使该解决方案对 BeyondTrust 具有更高的价值。它利用诸如 SIEM 这样的安全中心，因此 Orca 的检测结果可以直接进入 Azure Sentinel 安全中心。如果需要调查或修复，Orca Security 可以在 ServiceNow 中发出工单。

Azure Sentinel 安全中心仪表板受到持续监控，因此可以快速解决问题。“我们在不到一周的时间内就完成了这些集成，并且它能完美运行，”Haber 说。“从 Orca 检测到异常情况起，我通过一个仪表板图表就能得知鉴别此问题所需的时间。对于任何关键问题，我们的平均解决时间已经缩短了一半，”他说。“一旦工单关闭，Orca 不再发现问题，我们的整个循环便结束，这对我们的治理团队和必须确保我们满足 SLA 的人员来说具有重要意义，”Haber 说。

对安全工程的影响

通过与 ServiceNow 的集成，Orca 可以生成包含特定细节的工单，以供安全工程人员进行处理。这比使用基于代理的工具节省了大量时间。“我们在全球多个地区进行了部署 — 北美、欧洲和南美，”Haber 回忆道。“在各个地区，如果考虑到使用基于代理的技术时需要部署多少组件，与便捷的 Orca 连接相比，您就会理解为什么工程和运营团队对 Orca 的满意度要高得多。”

至于 Orca 的部署速度和准确性，Haber 说，“它是一种获取复杂数据，以指导我们行动的有效方法。它在漏洞管理、合规性以及安全配置方面为我们提供帮助。仅仅使用了几个月后，Orca 就成为了我们颇具价值的解决方案。”

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。

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。