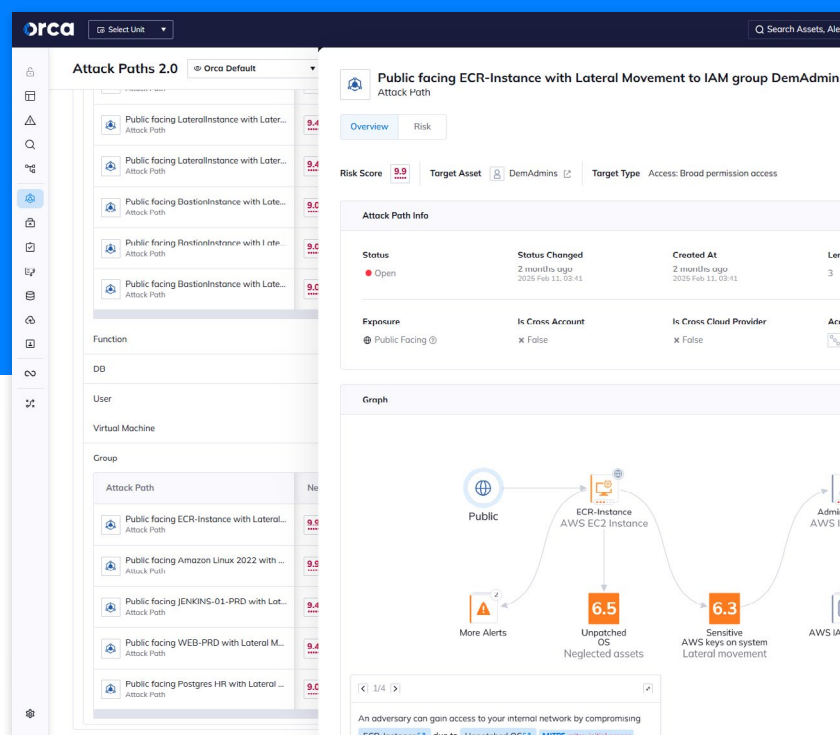# ATTACK PATH ANALYSIS

Attack paths represent the toxic risk combinations that attackers can exploit to endanger your high-value cloud assets. The Orca Cloud Security Platform surfaces and prioritizes all attack paths to ensure your teams can break critical risk chains, reduce alert fatigue, and maximize productivity—not to mention peace of mind.

Keep High-Value Assets Protected and Attackers at Bay

- ✔ Fully integrated with the Orca Cloud Security Platform
- ✔ Automatically surface and prioritize toxic risk combinations regardless of type
- ✔ Prevent critical risks, attacks, and severe security incidents
- ✔ Leverage flexible remediation options, including AI-driven and assisted
- ✔ Decrease mean time to remediate (MTTR)
- ✔ Accelerate threat investigation and incident response efforts

Stay ahead of attackers

When scanning your cloud estate, Orca not only looks at individual risks, but also looks at your environment just like an attacker does. Our patented SideScanning™ technology discovers relationships and connections between assets and looks for accessible keys, passwords, vulnerabilities, and more, that an actual attacker can use to move laterally. When Orca detects an issue, it displays prioritized alerts and enumerates all findings in detailed risk reports.

Surface toxic risk combinations

Leverage graph-based views of at-risk security relationships attackers can exploit to endanger high-value assets.

Prioritize your critical attack paths

Orca scores each attack path on probability and impact so that you can quickly discover and mitigate your most critical risks, limiting any potential damage of an ongoing attack.

Gain full contextual visibility for fast and focused remediation

Each attack path alert provides vital context, including important overview information, a graph visualization of the attack path, a concise explanation of it, and a timeline of events. Orca's graph-based view also offers contextual data like IAM policy, compute, storage, and more to show the relationships between cloud assets and risks.

## Fast and flexible remediation options

Orca offers multiple options to remediate each attack path fast and easily. You can remediate risks directly from the graph-based view or a prioritized list of alerts classified into three categories: those facilitating initial access, lateral movement, or direct compromise of a high-value asset.

Enhance Cloud Detection and Response (CDR)

Orca's Attack Path Analysis feature surfaces all attack paths associated with an active threat and the cloud assets that may be affected by it. Using Orca, security teams can accelerate their incident investigation and response and neutralize in-progress attacks more quickly, easily, and effectively.

About Orca Security

Trusted by hundreds of organizations, Orca is an enterprise-scalable platform designed to secure large multi-cloud estates efficiently and with low-overhead. With over 50 out-of-the-box third-party integrations, including Slack, OpsGenie, Jira, and ServiceNow, Orca seamlessly integrates with your existing workflows.
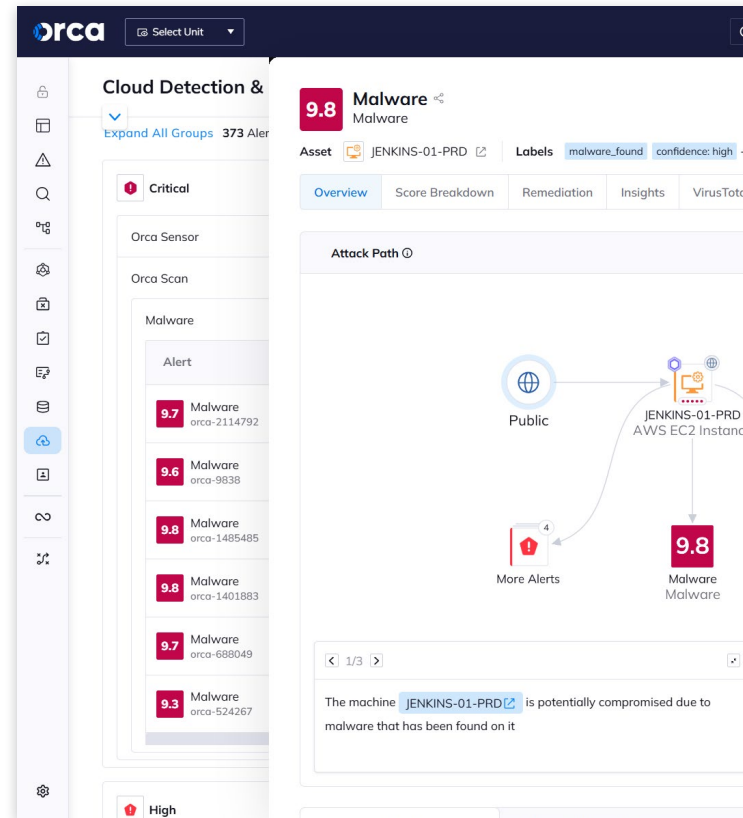
Ready to try it out?
Sign up for a demo. Visit orca.security/demo