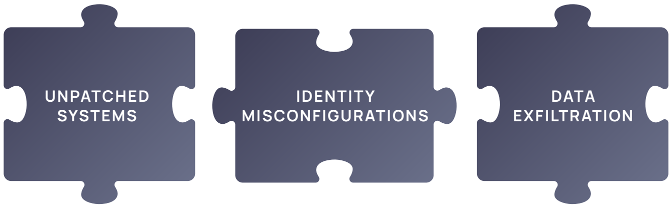
orca security

How to CISO in the Cloud: Risks and Attack Paths Explained

Cloud usage creates unique security challenges, making proper guardrails a must to prevent your organization from being targeted. This infographic outlines prominent cloud risks and how they can piece together to form 3 types of dangerous attack paths.

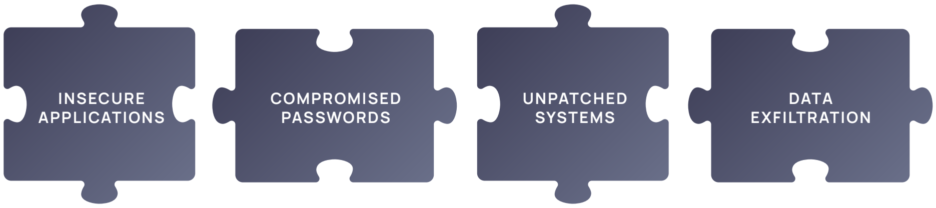
Attack Path #1: System Exploitation

Using credentials on an exploited system, the adversary accesses systems deeper within the cloud estate



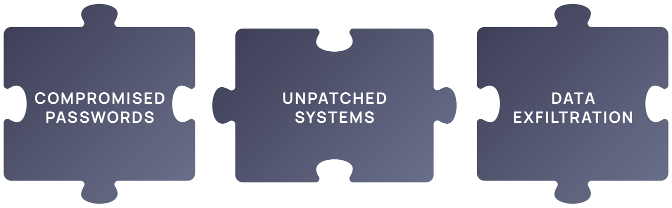
Attack Path #2: Ransomware

An adversary gets malware to run on a machine by any number of methods, followed by stealing data and leaving behind an encrypted copy that costs money to decrypt



Attack Path #3: Account Takeover

A legitimate user's login credentials are exposed to an adversary, who then uses credentials to login to the user's account to conduct nefarious activity



How to Protect Against The Most Common Cloud Risks and Attacks

Now that you're aware of the risks your organization faces and how they can piece together to form dangerous attack paths, ask yourself:

- Have any of these attacks affected my own company? If so, what steps were taken to remediate?
- Considering a full-picture view of my company (industry, past cybersecurity incidents, etc.), which of these risks is most important for me to tackle and why?
- Where should my team start in order to tackle the risk(s) I've identified as being the most important?

To get the full list of the most prominent cloud risks and potential attack paths that could leave your organization vulnerable, get your copy of "How to CISO in the Cloud Part I: The State of Your Cloud Security Usage and Risks." Or, if you're ready to get started now on a plan to address these risks in your own organization, get your copy of Part II here.