Orca Security 2020 State of Public Cloud Security Report

Follow the exploitation path below to discover how most large breaches happen

Neglected Workloads

and authentication issues are the weak links attackers are looking for

80%

80% of organizations have a frontline workload with an unpatched or unsupported operating OS

Authentication Issues are Commonplace

Weak or Leaked Passwords

5% of organizations have one or more workloads accessible via weak or leaked passwords

No MFA on Super Admin Accounts

23% of organizations aren't using MFA to protect one of their cloud account's root, super admin users

Non-Corporate Credentials

19% of organizations have at least one internet-facing asset accessible via non-corporate credentials

Finding the Keys to the Kingdom

Almost half of organizations (**44%**) have internet-facing workloads containing secrets and credentials, posing a risk of lateral movement

44%

Past the Gates: Lateral Movement Risk

The security of internal workloads is much worse than frontline services which increase the risk of lateral movement once a frontline service is breached

77%

77% of organizations have **10%** or more of their internal workloads in a neglected security state — meaning the OS is unsupported or unpatched

Download the Full Report

Follow Us

orca.security