The Orca Security 2020 State of Public Cloud Security Report

Public Cloud Estates Rife with Neglected Workloads, Authentication Issues, and Lateral Movement Risk

orca security

Executive Summary

Public cloud security is a shared responsibility. While cloud providers such as Amazon, Microsoft, and Google must keep their public cloud platforms secure, customers are responsible for securing the workloads, data, and processes they run inside the cloud.

This presents a tremendous challenge for several reasons. Today, any person with a corporate credit card can activate sophisticated IaaS assets across AWS, Azure, and GCP. Meanwhile, DevOps teams work at breakneck speeds, scaling usage up and down frequently—possibly thousands of times per hour—and all within a CI/CD pipeline that builds the infrastructure. Security isn't always in the loop on cloud deployments and even when it is, visibility is limited.

For most organizations, cloud workload security is dependent upon the installation and maintenance of security agents across all assets. This rarely happens, as this report shows.

Key findings include:

80.7% of organizations have at least one neglected internet-facing workload — meaning it's running an unsupported operating system or has remained unpatched for 180 days or more.

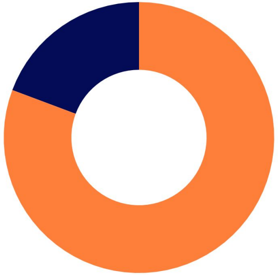
Authentication issues are also commonplace, with **5.3%** of organizations having at least one workload accessible using either a weak or leaked password; **23.5%** of organizations aren't using multi-factor authentication to protect one of their cloud account's root, super admin users; and **19.3%** of organizations have at least one internet-facing asset accessible by way of non-corporate credentials.

Almost half the organizations (**43.9%**) have internet-facing workloads containing secrets and credentials, posing a risk of lateral movement.

Executive Summary

The security of internal workloads is much worse than frontline workloads, with **77.2%** of organizations having **10% or more** of their internal workloads in a neglected security state—meaning the OS is unsupported or unpatched.

The above data describes the sequencing of how most breaches happen. Attackers find the vulnerable frontline service—the weak link—and use it as a foothold from which to move laterally across the organization.



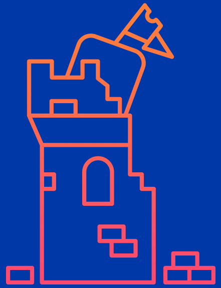
80.7%

of organizations have at least one neglected, internet-facing workload

Orca Security analyzed data from more than two million scans of 300,000 public cloud assets running on AWS, Azure, and GCP. Scanned accounts represent Orca's customer base across numerous industries, including financial services, professional services, travel, cloud computing, online marketplaces, entertainment, and real estate, with locations in North America, Europe, and Asia-Pacific. The breadth and depth of data in this report are possible because Orca SideScanning™ sees 100% of the workloads inside each customer's public cloud estate. The cloud scans ran from November 6, 2019, to June 4, 2020.

2M **Scans** of

300k **Public Cloud Assets**



Weak Link: Neglected Workloads

Weak Link: Neglected Workloads

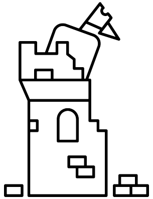
The world of cybersecurity isn't fair. Security teams need to secure everything, but attackers need only find one weak link.

Our study found that **80.7%** of organizations have at least one neglected, internet-facing workload—meaning it's running an unsupported operating system or has remained unpatched for 180 days or more.

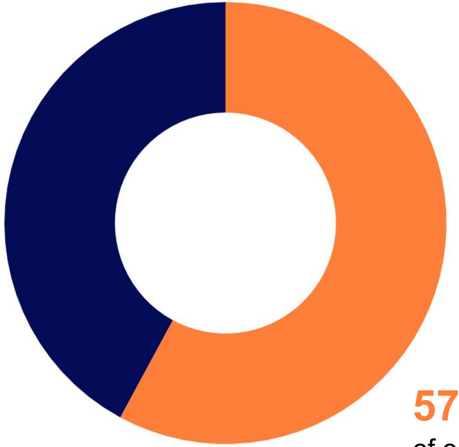
57.9% of organizations have at least one neglected internet-facing workload that falls into the unsupported OS category; that has reached "end-of-life" and will no longer be supported by manufacturer security updates.

These are the weak links attackers are looking for and are way most large breaches happen. Attackers find the vulnerable frontline workload—the weak link—and use it as a foothold from which to move laterally within the network and attack the organization.

The Equifax mega-breach of 2017 is a case in point. In that breach, the culprit was an unpatched web server. While it's easy to single out Equifax, but it's far from alone. Despite increased awareness of these dangers, we found **49.1%** of organizations have at least one unpatched web server within their cloud estate.

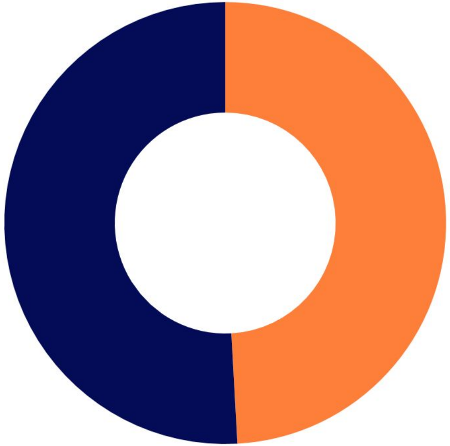


Weak Link: Neglected Workloads



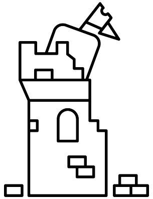
57.9%

of organizations have at least one internet-facing workload running an unsupported OS



49.1%

of organizations have at least one unpatched web server

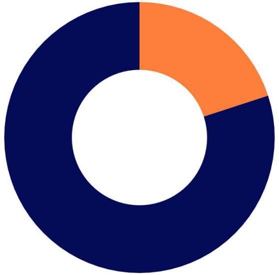


Weak Link: Authentication Issues

Weak Link: Authentication Issues

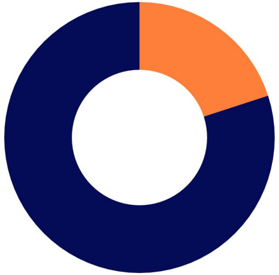
Weak security authentication is another way attackers breach cloud environments. We found that **23.5%** of organizations have at least one cloud account that doesn't use multi-factor authentication for the cloud provider root account (super admin).

Another type of weak authentication is the use of non-corporate credentials. **19.3%** of organizations have at least one internet-facing workload accessible via non-corporate credentials.



23.5%

of organizations have at least one cloud account that doesn't use multi-factor authentication for the cloud provider root account

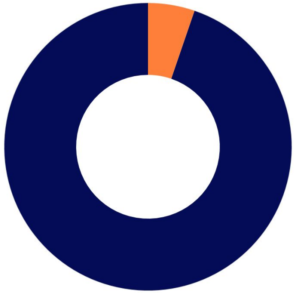


19.3%

of organizations have at least one internet-facing workload accessible via non-corporate credentials

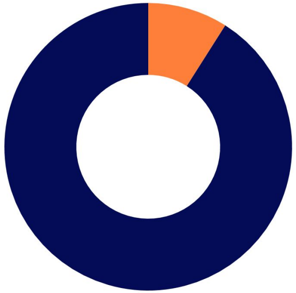
Weak Link: Authentication Issues

Equally concerning are the use of weak or leaked passwords, as well as internet-facing, open RDP ports.



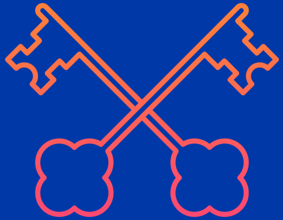
5.3%

of organizations have at least one workload using an easy-to-guess or leaked password—meaning it's a simple derivative of existing credentials or the password exists within Orca Security's database of breached passwords



8.8%

have at least one internet-facing asset with Microsoft Windows OS and RDP port (3389) publicly exposed. Remote desktop protocol (RDP) is used to connect remotely to Windows assets. The protocol has critical vulnerabilities and is highly targeted by attackers. It's not secure to keep the RDP protocol exposed to anyone on the internet



Finding the Keys to the Kingdom

Finding the Keys to the Kingdom

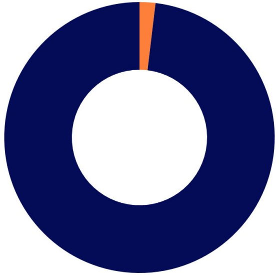
Only a small number of neglected, internet-facing workloads (**1.9%**) contain customer information.

However, almost half of organizations host internet-facing workloads (**43.9%**) containing secrets and credentials—including clear-text passwords, API keys, and hashed passwords.

For example, **5.6%** of internet-facing assets contain SSH keys that could be used to access adjacent systems. Hackers use these credentials and secrets to move laterally across the network in search of crown jewel data or to wreak havoc on their target.

The Matrix.org breach is a case in point. Here, a hacker exploited a known vulnerability in the Jenkins open source automation server to hijack accounts and access its production infrastructure.

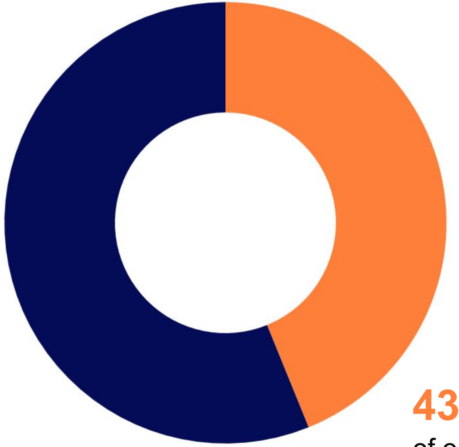
Then, during the data breach cleanup, Matrix failed to replace a Cloudflare API key. This allowed the hacker to change its DNS records and redirect Matrix.org users to a GitHub page showing some of the data the hacker was able to access.



1.9%

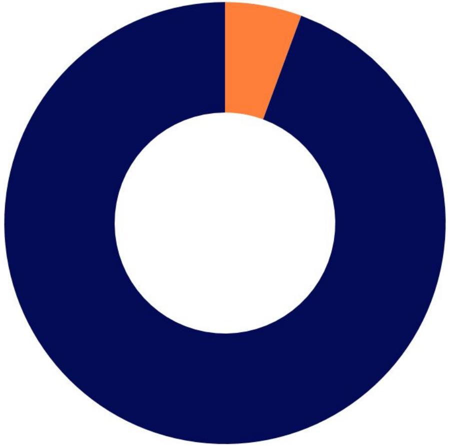
of neglected, internet-facing workloads contain sensitive data

Finding the Keys to the Kingdom



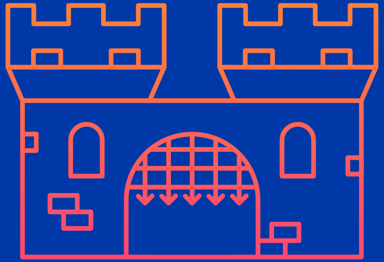
43.9%

of organizations have internet-facing workloads that contain secrets and credentials



5.6%

of internet-facing assets contain SSH keys that could be used to access adjacent systems

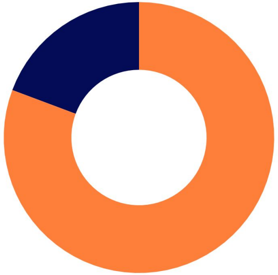


Past the Gates

Past the Gates

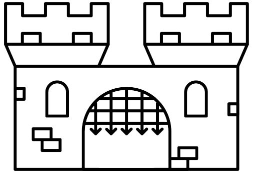
Once past the front gates via an OS vulnerability or a weak authentication issue in a frontline workload, attackers take advantage that the security posture of internal machines is much worse than internet-facing servers.

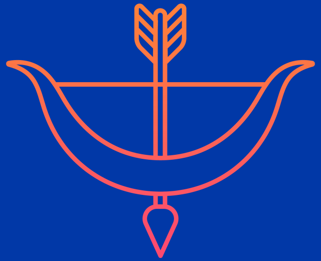
We found that **77.2%** of organizations have **more than 10%** of their internal workloads in a neglected security state. This means they had been running an unpatched or unsupported operating system, thereby were at risk to potentially hundreds of known vulnerabilities.



77.2%

of public cloud estates have more than 10% of their internal workloads in a neglected security state



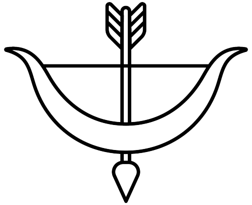


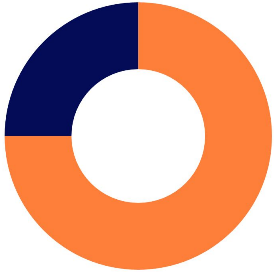
Shooting Yourself in the Foot

Shooting Yourself in the Foot

Mistakes happen. And when they do, hackers are ready to pounce. We found that **5.3%** of organizations have at least one publicly writable storage bucket, and **75.4%** had a storage bucket mistakenly open to the internet.

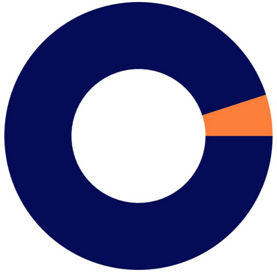
Easy-to-prevent cloud misconfigurations can have dire consequences. The Cultura Colectiva breach is a case in point. Here, the Mexican media company had 540 million Facebook records on an open S3 bucket that anyone could download from the internet.





75.4%

of organizations had a public storage bucket open to the internet



5.3%

of organizations have at least one publicly writable storage bucket

4 Key Recommendations

1 Security is only as good as its coverage. Make sure you cover 100% of your cloud assets, as attackers will always sneak through the weakest links.

2 Get your basics straight before progressing to more advanced capabilities. Breaches mostly stem from simple things such as an unpatched, neglected service or a stolen root account password with no MFA. Invest in IT hygiene and monitor it on a daily basis.

3 Look for lateral movement risk. Assume that internet-facing workloads will be breached, and make sure this doesn’t lead to uncontained damage via less secure internal servers.

4 Mistakes will happen. This is human nature. Embrace it while implementing tools that will enable you to react quickly.

About Orca Security

Orca Security is the cloud security innovation leader, providing instant-on, workload-level security and visibility into AWS, Azure, and GCP—without the gaps in coverage and operational costs of agents.

Delivered as SaaS, Orca Security's patent-pending SideScanning™ technology reads your cloud configuration and workloads' runtime block storage out-of-band, detecting vulnerabilities, malware, misconfigurations, lateral movement risk, weak and leaked passwords, and unsecured PII.

Orca Security deploys in minutes—not months—because no opcode runs within your cloud environment. With Orca, there are no overlooked assets, no DevOps headaches, and no performance hits on live environments.

And unlike legacy tools that operate in silos, Orca treats your cloud as an interconnected web of assets, prioritizing risk based on environmental context. This does away with thousands of meaningless security alerts to provide just the critical few that matter—along with their precise path to remediation.

Connect your first cloud account in minutes and see for yourself. Visit https://orca.security