CYBERARK®

# Building a Business Case for Cloud Infrastructure Entitlements Management (CIEM)

The cloud offers significant opportunity for modern businesses — speed, agility and scalability being just a few. But it also comes with challenges when it comes to security, and sometimes those challenges can't be solved with homegrown solutions or built-in security features from cloud service providers. The most notable are the exploding number of cloud permissions and the ease of privilege escalation in cloud environments. Addressing these challenges is especially complex in hybrid and multi-cloud environments at enterprise scale.

While you may be very familiar with these security challenges, you may have to take a step back to sell your leadership on why they should invest in cloud infrastructure entitlements management (CIEM).

## EXPLAIN THE RISKS

As you're positioning challenges to your leadership, you'll want to make sure you explain difficulties without getting lost in the technical weeds. Leaders are looking at company operations as a whole, and the risks should be outlined as such.

When communicating the risks of cloud permissions, stick to statistics and always tie back to the dollar amount when you can. Your executive stakeholders may not need to know what a shadow admin is, but if you tell them that a simple permissions misconfiguration could lead to major financial losses, they're likely to listen.

Below are some examples of the risk of a cloud breach from IBM's Cost of a Data Breach report.

| $4.80M | $4.55M | $3.61M | 18.8% |
|---|---|---|---|
| Primarily **Public** Cloud Approach | Primarily **Private** Cloud Approach | **Hybrid** Cloud Approach | Higher cost of cloud migration projects for those organizations that experience a breach.* |

*Source IBM, "Cost of a Data Breach Report 2021," July 2021, www.ibm.com/security/data-breach.

## ADDRESS OBJECTIONS

When presenting a new technology solution to leadership, it always helps to come prepared to address any possible objections. Below are some example questions you may get as you present your business case, along with sample answers.

*"There are IAM security features in our existing cloud platforms. Can't we just use those?"*

Cloud providers do have built-in IAM controls. Unfortunately, this is part of the difficulty, as siloed controls across on-prem and cloud environments create operational challenges and obscure visibility. Additionally, according to a recent survey, 67% of respondents are using multiple public clouds and at least one private cloud.[1] In fact, the average number of clouds used by respondents was 2.6 public clouds and 2.7 private clouds.

These hybrid, multi-cloud environments make it harder to centralize your cloud security operations, and you can run the risk of creating "security islands," resulting in a piecemeal security strategy.

Finally, cloud providers operate under a shared responsibility model. While providers are responsible for the security of the cloud itself, customers are responsible for secure configuration within their clouds. If there's a misconfiguration somewhere exposing your data to the public, that's your responsibility to secure it — not the cloud provider's.

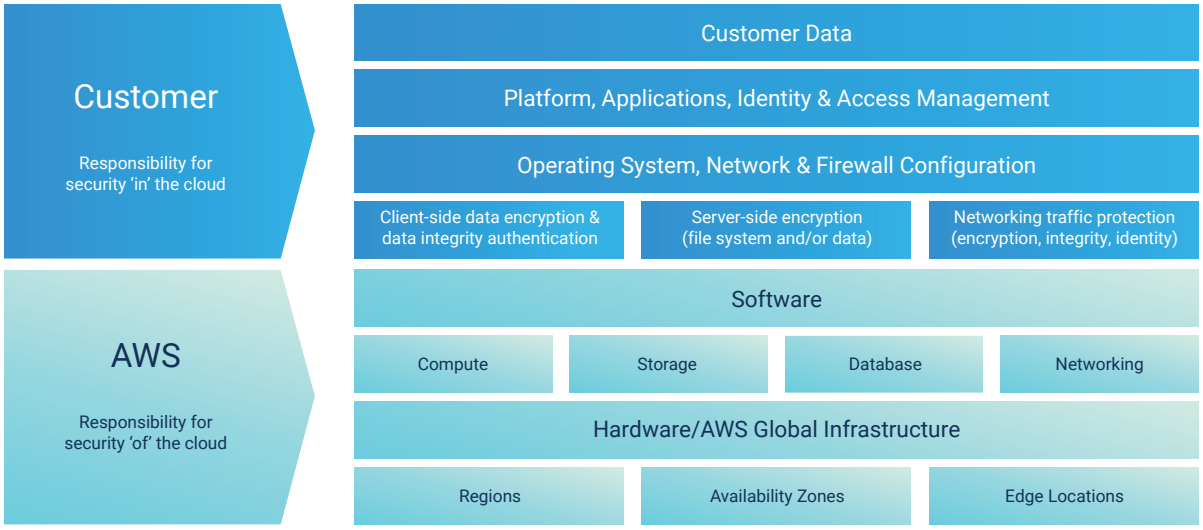


*Figure 1: AWS shared responsibility model - indicative of shared responsibility models for Azure, GCP*

*"What if we break something by removing access privileges?"*

In the name of making sure everything is connected and working seamlessly, organizations tend to over-permission users and applications in the cloud by default. These excessive permissions are ripe for an attacker to compromise a role with the right access. But you don't want to slow production down with onerous security policies or potentially break something while remediating access. The goal of cloud security is flexibility — creating environments in which accounts have just the right amount of privileges they need for only the time period required.

Thankfully, leading CIEM solutions operate by the principle of least privilege — with granular policy remediation options to remove only unused permissions, meaning valid entitlements for ongoing operations are preserved while permissions that pose risk are stripped away. By right sizing your cloud permissions, you can reduce risk and minimize the attack surface while still ensuring that cloud workloads are running smoothly.

—

[1]Flexera, "2021 State of the Cloud Report," March 2021, https://info.flexera.com/CM-REPORT-State-of-the-Cloud.

*Implementing security solutions can require a lot of staffing resources and time.*

One of the benefits of using cloud infrastructure is its speed and agility. The last thing organizations want is to slow their processes down with a long, resource-intense implementation of a security tool, especially if they need those resources focused on business-critical areas of their cloud migration projects.

Fortunately, leading CIEM solutions do not require the time and resources you may think. A CIEM solution that leverages serverless architecture means that you don't need to bring in any virtual machines to host the solution. That keeps your resources free for other tasks, improving your operational efficiency, as well as accelerating your time to value. Artificial intelligence (AI) can be used to spot and remediate excessive permissions more rapidly than a human could, freeing up your people's time for more higher-value work. AI can even create policy corrections and make proactive risk reduction recommendations to speed along the remediation process even more.

CIEM solutions can also integrate with your existing Identity Security tools, such as IDaaS and privileged access management solutions, to drive further efficiencies. Finally, CIEM solutions don't typically require long implementations and tons of IT resources – some can be ready to start scanning in a little as five minutes.

## DEFINE THE BENEFITS

Now that you've proven the need and have addressed some of the main objections up front, it's time to make the case for your solution. Just like with the risks, come armed with clear benefits that tie to overall business goals.

- **Continuous, cloud-agnostic visibility and control.** Using a single CIEM platform means you gain insights regarding permissions across your environments. Instead of creating security islands, you have a one-stop shop to manage your cloud security. Centralization also limits the operational drag of training staff across multiple platforms, increasing overall efficiency.
- **Efficiently implement least privilege.** A centralized CIEM solution means you can implement **least privilege** across cloud accounts from a single location, leveraging programmatic remediation of excessive permissions. This drastically improves efficiency compared to manually managing permissions in disparate view panes for each cloud environment. Analyzing thousands of permissions and right-sizing them becomes easier when you're managing from a single tool.
- **Proactively measure risk.** Cloud environments are dynamic and ephemeral by nature, spinning up new accounts and granting new permissions all the time. With a centralized tool, you can keep pace with the introduction of new identities and cloud services, monitoring your cloud environments for any newly introduced risky permissions.

Don't just tell — but also show your executives the value of a security solution whenever possible. For instance, with the **complimentary assessment of CyberArk™ Cloud Entitlements Manager**, you can find and remediate risky permissions in under an hour and take those findings back to your leadership.

---

**About CyberArk**

CyberArk is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security offering for any identity – human or machine – across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets.

CYBERARK®