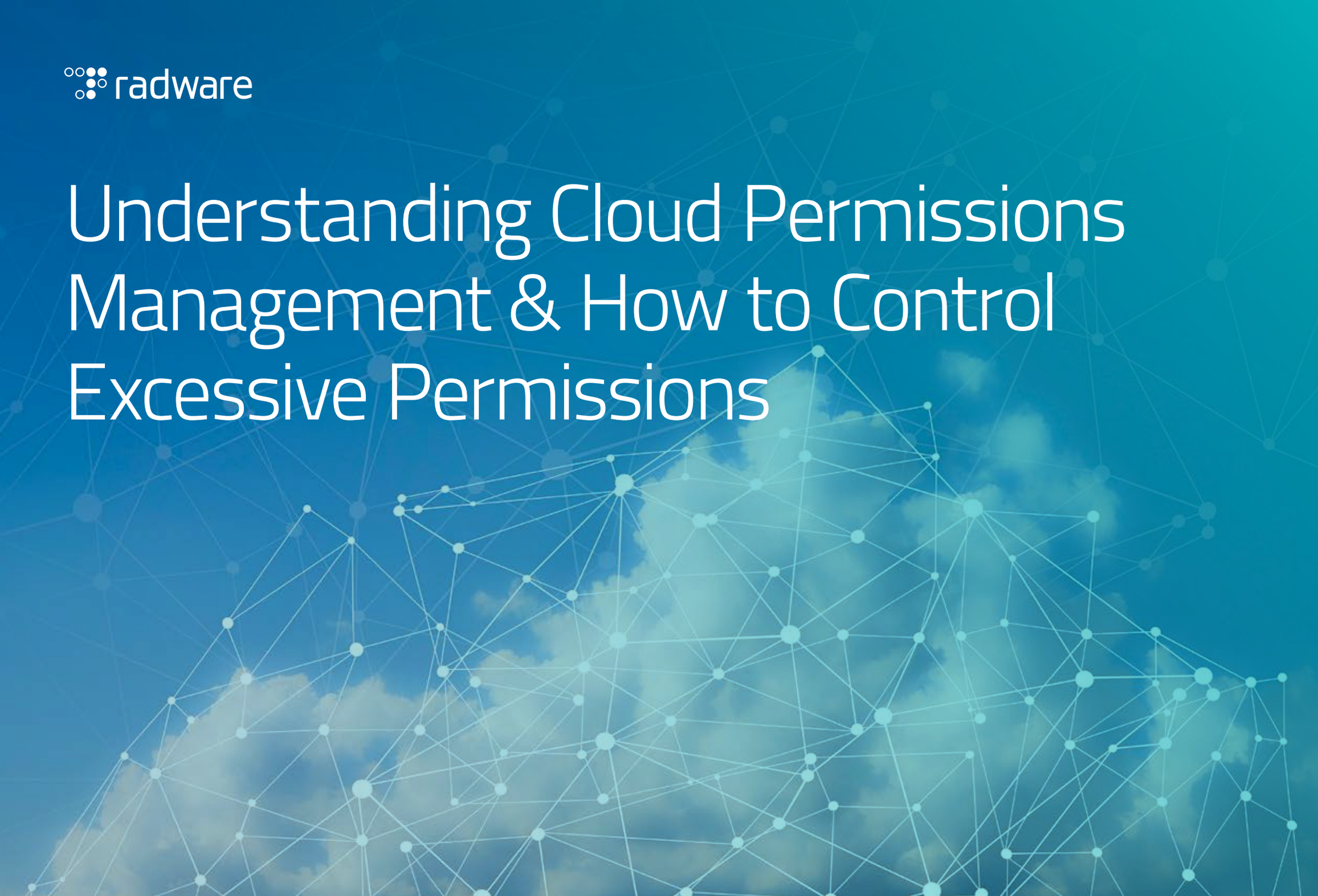
radware

Understanding Cloud Permissions Management & How to Control Excessive Permissions



Contents

Cloud Excessive Permissions: Balancing Agility vs. Security

Running in the cloud is all about agility and flexibility. The speed and convenience of using the cloud allows for rapidly spinning up new resources, expanding capacity dynamically, deploying new code, ultimately resulting in faster time to market.

However, this agility and flexibility comes at a cost to security: in the name of expediency, cloud administrators frequently grant extensive permissions to groups of users, to enable them to accomplish tasks seamlessly. In practice, most users use only a small portion of the permissions granted to them and have no business need for all of them. This represents a serious security gap, since if these user credentials were ever to fall into malicious hands, attackers would have extensive access to sensitive data and resources.

These concerns are also backed by industry-wide research. By 2023, 75% of cloud security failures will be attributable to inadequate management of identities, access, and privileges, according to Gartner's Managing Privileged Access in Cloud Infrastructure report.[1] This presents further complexity in managing and monitoring for malicious and unauthorized behavior in accessing infrastructure or applications.

Although authentication mechanisms, privilege, Role-based Access Control and Active Directory integration have extended themselves to ease the complexity of access via programmatic access, they have so far failed to curtail the challenge of excessive permissions. This phenomenon spirals with rapid application data flows which transcend the traditional boundaries of organizations and requires dedicated tools and procedures to mitigate.

[1] https://www.gartner.com/en/documents/3986121/managing-privileged-access-in-cloud-infrastructure

Your Permissions Equals Your Threat Surface

Excessive privileges define the dynamically changing attack surfaces quite different from the traditional IT security environments boasting a better frame of control.

However, organizations expand their cloud footprints without defining a comparable or improved set of controls through policies, configurations, governance, better visibility and observability. Added to these considerations, the added complexity of having to deal with multiple security tools, controls and applications operating in distributed environments combines to present a high level of complexity.

These attributes have a cascading affect on the applications, infrastructure and data flow in the cloud. Though the origin of these permissions may be due to several reasons, including the need to create quick permissions for a sandbox environment, creating one-time accounts with elevated permissions which lose their need after the completion of the activity results in accruing permissions that exceed the requirements of the organizations' workflows.

Consequently, this propagates a dangerous precedent whereby organizations exchange credentials with far more privileges than they should allow, raising the potential of inadvertently exposing the applications, configurations around build environments and their security defenses.

The challenge of being unable to monitor permissions at the right level and govern them further increases with the increased complexity of the workloads with the organization's accelerated shift to the cloud. Traditional identity and access management, and the associated permissions which are executed through policies and configurations, now find a far greater lineage in how they are used, whether credentials are used by third parties, access to sensitive data, access privileges beyond what is required, etc.

The average number of permissions being handled has exponentially increased which finds its footprint beyond the traditional IT boundaries. When you have so many permissions being issued, a percentage of these permissions have the potential to be misused, leading to large scale breaches. As some of the leading causes for data exposure are over-provisioning of permissions, unused and unchecked privileges, this can lead to massive security vulnerabilities.

The average number of permissions being handled has exponentially increased

Entitlement Management is Now a Core Requirement

According to Radware's C-Suite Perspectives: Accelerated Cloud Migration but Lagging Security, cloud acceleration has progressed more rapidly since the onset of the pandemic last year than in the entire previous decade.

Adoption comes in different forms: cloud native, hybrid workloads, distributed multi-cloud operations and others. However, the most rapidly evolving challenge lies in the way organizations maintain a stable security posture for the different cloud workloads. An effective approach to application workloads on the cloud is a function of focusing on defining and implementing access management through policies across all the systems.

Cloud environments bring several benefits, including automated scaling environments. Migrating applications to cloud environment raises the challenge of dealing with a mix of legacy identity solutions with cloud-native permissions management strategy for closed/local environments/datacenters.

There is often a gap between granted and used permissions. This gap is exploited by hackers to breach organizations.

The movement of workloads to the cloud has led organizations to lose control over their assets. According to Radware's The State of Web Application and API Protection Report, 30% say visibility is their #1 challenge in protecting applications. Not having the requisite visibility lift and shift of legacy applications causes force-fitting and creates gaps that make way for excess privileges and overarching permissions. Public cloud providers address the problem to a certain extent with their native tools, however, the evolving complexity of customer environments and distributed multi-cloud environments cannot be addressed by a single provider, leaving the enterprise accountable.

Too often there is a gap between granted permissions and used permissions, which is frequently exploited by hackers leveraging the unnecessary permissions breaching organizations.

This is a key ingredient of what Gartner calls Cloud Infrastructure Entitlement Management (CIEM). While the rapid cloud adoption has driven the ease of creating workloads, mapping resources while staging and de-staging environments has led to security blind spots. The focused segment of CIEM is an attempt to focus on the cloud-native security challenges of identities and the permissions associated with them.

The Role of ‘Roles’ in Permission Proliferation

One of the key challenges of managing permissions in the cloud is the fact that public cloud provides additional types of permissions that are not typically observed in traditional premise-based environments.

One of the permission types which has proven to be a point of particular concern is “role” permissions. Unlike the traditional “user” and “group” permissions, which are usually associated with actual physical users (or groups of users), “role” permissions are more flexible permissions which can be dynamically assigned to user, applications or services. Indeed, according to Radware’s own cloud network data, approximately 80% of excessive permissions observed in cloud environment are ‘role’ permissions.

Unlike user permissions, which are typically associated with a single person, role permissions are intended to be assumed ad-hoc by anyone (or anything) who needs it for that specific session. Cloud account role permissions allows delegating access to users and services to cloud resources for which they normally do not have access.

While this provides a great deal of flexibility, it also creates a security challenge of very flexible permissions which can be assumed by a wide range of people and services. The fluidity of these roles and the variety of use cases in which they may be used frequently leads to proliferation of access for which there is no business need.

Approximate number of excessive ‘role’ permissions observed in cloud environments

80%

Four Common Pitfalls to Watch For

There are a number of common pitfalls which organizations frequently fall into that lead to permission exposure and unnecessary access.

The key to mitigating these challenges is in providing visibility to those who can use these roles, helping security teams to reduce access only to entities that need it.

Cross-Account Access

Originally intended to ease the management of dealing with several authentications for different provisioned environments. This is a major risk for organizations' account takeover attacks. This is because cross-account access is rarely subject to monitoring and audit, once again highlighting the need for observability across such entitlements.

Set and Forget

Cloud workload protection should be able to continuously monitor cloud activity and track how different identities utilize the access permissions they have been granted.

Tactical and Unused Permissions

Excessive access permissions that have not been used for a long time should be revoked to reduce the attack surface.

Too Inclusive Entitlements

Enterprises need to analyze how access permissions are being used by cross-account roles, a special type of role that is typically seen in a cloud environment that includes many accounts. This is critical as users authenticate on one of the cloud accounts and then use the cross-account roles which exist in all the other accounts and grants them access to cloud services.

The Challenge of Enforcing Least-Privilege Access

Addressing these challenges creates an inherent tension between security and agility. As previously discussed, agility and flexibility are the main business benefits of adopting the public cloud, but in practice, the manner in which this flexibility is implemented frequently creates serious security gaps which can be exploited by hackers.

The solution is to implement Least Privilege Access (LPA), which guarantees that users have the permissions they need to effectively go about their business, without having excessive permissions which create those security gaps. **There are a number of key best practices to achieve this balance:**

Keep track of inactive users

Cloud environments are frequently very dynamic and rapidly changing environments, and this is also true of the people using them. Therefore, it is important to keep track of inactive users. You can remove them with no impact to your business activities.

Monitor "role" permissions

As explained earlier, "role" permissions are a point of particular concern because of their wide usage (and misusage). Therefore, it is important to monitor such permissions to ensure they maintain the limited permissions needed for the particular job they have to do without unnecessary expansion of their role.

Analyze the gap between defined & used permissions

Unnecessary permissions stem from gap between what users need in order to get their job done and what they have in terms of permissions. Put differently, it is the gap between defined and used permissions. The difference between these two is your organization's attack surface. This is why it is important to constantly monitor and analyze this gap to make sure that it is as small as possible, and consequently, that your attack surface is equally small.

Use automation

Keeping track of changes in public cloud environments is no simple task. As mentioned, these environments — and their users — tend to change all the time. This is why automation in this area is a key aspect of security. Trying to keep track of every user in the cloud environment, and of every access entitlement that they have, is simply not feasible. Therefore, using automated CIEM tools which take care of this aspect of security for you is highly recommended.

Conclusion

Digital transformation is all about faster time to market and the public cloud is an enabler for that. Running in the cloud is all about agility and flexibility, and from an IT perspective, it is where "the rubber meets the road" of digital transformation. The problem, however, is that in the name of expediency, IT managers frequently focus more on moving fast and fail to properly secure their cloud environments, leaving their workloads and customer data vulnerable to exposure and data breaches.

In particular, the issue of cloud entitlement management and excessive permissions is one that plagues many organizations. It is an area of focus where the agility of cloud environments clashes with security, putting the organizations and its users' data at risk.

Controlling excessive permissions is paramount to the security of the organization's public cloud environment, and ultimately its ability to manage risk as an organization

About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit radware.com.

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.