GlobalDots

In Collaboration with

radware

GlobalDots radware

Least Privilege, Zero Sweat:

Protecting Cloud Workloads from 2021's Security Threats

A Security Admin's Quick Guide

Table of Contents

Introduction

Whether your company is "Cloud-Native" or is migrating workloads to public cloud environments - cloud workloads expose organizations to a slate of new, cloud-native attack vectors, foreign to the world of on-premise data centers. In this new environment, workload security is defined by permissions: which users and roles can access what. As a result, implementing a "Least-Privilege" security approach, protecting against excessive permissions — and promptly mitigating permission abuse — becomes top priority for security administrators.

This quick guide outlines:

The security challenges brought about by having or migrating computing workloads to public cloud environments.

How security professionals should address those challenges.

The capabilities required to help protect cloud workloads from new cloud-native threats.

The Old Insider Is the New Outsider

Traditionally, computing workloads resided within the organization's data centers, where they were protected against insider threats. Application protection was focused primarily on perimeter protection via mechanisms such as network firewalls, intrusion prevention/detection systems (IPS/IDS), web application firewall (WAF) and distributed denial-of-service (DDoS) protection, secure web gateways (SWGs), etc.

However, moving workloads to the cloud has led to organizations (and IT administrators) losing direct physical control over their workloads and relinquishing many aspects of security through the "shared responsibility model".

As a result, the insider of the old premise-based world is suddenly an outsider in the new world of publicly hosted cloud infrastructure. Employees such as IT administrators, developers and security teams are just like hackers now and have identical access to publicly hosted workloads, using standard connection methods, protocols and public APIs. As a result, the whole world becomes an insider threat. Cloud workload security, therefore, is defined by the people and machines who can access those workloads and the permissions they have.

'Old' world
Physical Data Center

- Network resources are hosted on-site
- Workloads are protected against insider threats
- Perimeter defenses guard against external threats

2021 cloud world
Public Cloud

- Workloads are hosted on the public cloud
- Organizations lose direct control over resources
- All access is "remote"

Your Permissions Equal Your Attack Surface

Primary reasons for migrating to the cloud include decreasing time to market and streamlining business processes. As a result, cloud environments make it very easy to spin up new resources and grant wide-ranging permissions, but they also make it very difficult to keep track of which users have permissions and who uses them.

All too frequently, there is a gap between granted permissions and used permissions. In other words, many users have too many permissions that they never use. Such permissions are frequently exploited by hackers who take advantage of them for malicious purposes. As a result, cloud workloads are vulnerable to data breaches (i.e., theft of data from cloud accounts), denial of service violations (i.e., completely taking over cloud resources) and resource exploitation (such as cryptomining).

In an ideal world, each developer or DevOps engineer would get the minimal amount of permissions to allow them to perform their job. There is a fine line between the neverending task of reducing the attack surface of excessive permissions and allowing the business to be agile and move fast without the hurdles of security.

Continuous, Smart (Mis)Configuration Hardening

To prevent attacks, enterprises must harden cloud workload configurations to address permission abuse, by applying continuous hardening checks to limit attack surfaces. The goals are to avoid public exposure of data from the cloud and reduce overly permissive access to resources by making sure communication between entities within a cloud, as well as access to assets and APIs, is only allowed for valid reasons.

Only smart configuration hardening that applies a “least privilege” approach enables enterprises to meet these standards. The larger and more distributed the development organization gets, the more complex and broad this issue becomes. This is especially true for hyper growth startups that keep recruiting more and more developers at a rapid pace. The process requires applying behavioral analytics methods over time, including regular reviews of entitlements and permissions, and a continuous analysis of each entity’s regular behavior to ensure users only have access to what they need, nothing more. By reducing attack surfaces, enterprises make it harder for hackers to move laterally in the cloud.

The process is complex and is often best managed by a combination of technology tools and people. The assistance of an outside security partner with deep expertise and a system that utilizes automated anomaly detection algorithms is therefore highly advised. Often attackers will perform keychain attacks over several days or months, which are harder to detect using traditional security solutions.

Secured Shouldn't Mean Slow

The premise of an organization based on cloud native infrastructure is enhanced agility & scalability hassle or huge capital expenditures, spinning up cloud instances in a click of a mouse or a CLI command. However, "with great power comes great responsibility": exposing the company's assets to the public cloud introduces new security challenges and attack surface.

Traditional security solutions will help by scanning the cloud environment, finding holes and providing a long list of hardening recommendations which the IT, developers and DevOps teams will then have to implement in order to reduce their exposure. Security teams find themselves in a constant struggle with the developers due to the lack of prioritization and focus on which hardening recommendations are nice-to-have, and which can actually prevent forthcoming attacks.

Staying on top of the cloud means that you move fast by consuming more cloud native functions, but you must also include smart security solutions that help you as a security professional to become an enabler of the business rather than the bad guy that keeps saying "no" to requests, or keep chasing down developers to close security holes that detract them from their core mission.

An ideal cloud native security solution should have an intelligent, AI-based learning component that can detect abnormal behaviors, correlate sporadic suspicious events into a coherent attack story and provide prioritized, actionable recommendations to harden the cloud environment and permissions in the most time efficient manner. Automated remediation can save a lot of time and effort if done correctly with minimal false positives and prevent attackers from moving laterally up the attack kill chain.

This balance between security, technology and automation allows developers and DevOps personnel to focus on enabling accelerated business growth with minimum security headcount.

Traditional Protections Leave You Exposed

Existing solutions provide incomplete protection against the threat of excessive permissions and entitlements. Here's why:

The built-in mechanisms of public clouds usually provide basic network protection and are mostly focused on security over the computing environment, leaving individual workloads vulnerable. Moreover, since many companies run multiple cloud and hybrid cloud environments, the built-in protections offered by cloud vendors will not protect assets outside their networks.

Compliance and governance tools usually use static lists of best practices to analyze permission usage. However, they will not detect (or flag) excessive permissions and are usually blind to activity within cloud workloads themselves.

Agent-based solutions require deploying (and managing) agents on cloud-based servers and will protect only servers on which they are installed. However, they are blind to overall cloud user activity and account context, and usually cannot protect non server resources, such as services, containers, serverless functions, etc.

Cloud access security broker (CASB) tools focus on protecting software-as-a-service (SaaS) applications, but they do not protect infrastructure-as-a-service (IaaS) or platform-as-a-service (PaaS) environments.

A New Approach for Protection

Protecting publicly hosted cloud environments facing new threats emerging daily requires a whole new approach.

Apply a Zero Trust approach and assume your credentials are compromised — Hackers acquire stolen credentials in a plethora of ways, and even the largest companies are not immune to credential theft, phishing, accidental exposure or other threats. Therefore, defenses cannot rely solely on the protection of passwords and credentials.

Detect excessive permissions — Since excessive permissions are so frequently exploited for malicious purposes, identifying and flagging such permissions becomes paramount. This cannot be done just by measuring against static lists of best practices, but rather must be based on an ongoing permission-usage gap analysis.

Harden security posture — The best way of stopping a data breach is preventing it. Therefore, hardening your cloud security posture and eliminating excessive permissions and misconfigurations guarantee that, even if a user's credentials become compromised, attackers will not be able to do much with those permissions.

Look for anomalous activities — A data breach is the result of not one mistake but rather of a series of errors. Most data breaches follow a typical progression, which can be detected and stopped in time if IT administrators know what they're looking for. Monitoring for suspicious activity (such as anomalous usage of permissions) in a cloud account will help identify malicious activity in time and stop it before user data is exposed.

Automate responses — Time is money, and even more so when it comes to preventing exposure of sensitive user data. Automated response mechanisms, such as AWS Lambda allow administrators to respond faster to security incidents and mitigate attacks within seconds of detection.

Cloud-Native Challenges Require Cloud-Native Solutions

Here at GlobalDots we've been working with a variety of customers and vendors in different stages of their cloud migration journey - some customers were "born in the cloud", while some still have hybrid environments as we help them adopt more cloud-native capabilities. The security challenges outlined above, of excessive permissions and entitlements, have risen from using cloud-native workloads, containers and services, thus requiring a new approach and a cloud-native security solution.

When you research and test a new security solution to help keeping your sensitive cloud workload assets safe from data breaches, please consider the following core components:

Quick Detection of Excessive Permissions & Misconfigurations — the ability to identify excessive permissions and entitlements, as well as misconfigurations that may increase your attack surface.

Comprehensive Protection — a solution that covers both data and control planes, enabling protection of individual assets while taking into consideration the overall context of the account. This approach protects cloud accounts across the 5 dimensions that comprise public cloud activity: users, machines, databases, storage, and cloud services.

AI-Based Anomaly Detection — a learning solution that can differentiate between normal and abnormal use of cloud workloads and resources. Attacks can go on for days, weeks, and even months. Only an intelligent system can correlate between sporadic events and draw an attack timeline as it progresses.

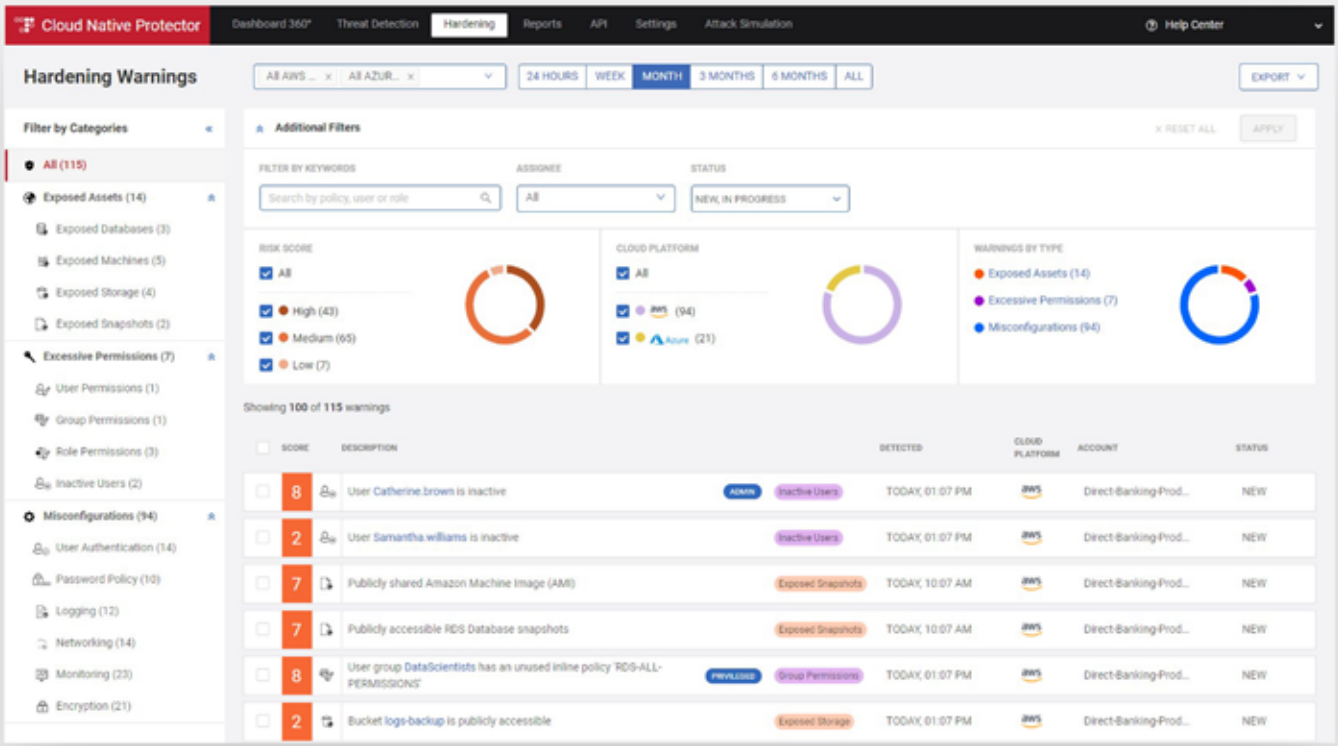
Compliance Support — the solution should be able to provide standard and custom compliance reports based on common security standards such as PCI-DSS, SOC2, ISO 27001, GDPR etc. This capability is helpful in M&A or pre-IPO scenarios which have become more frequent in recent years.

Actionable Recommendations — once excessive permissions or entitlements were detected, the solution should provide actionable hardening recommendations, prioritizing the most important gaps first, how to implement them in a detailed manner.

Future-Proof Cross-Platform Solution — companies move much faster than before, migrating from one platform to another. Whether you have a hybrid environment or are using one cloud provider today, you need a cross-platform solution in case your teams decide to use multi-cloud for multiple workloads and services, or to migrate from one platform to another in a year or two.

Easy-to-Deploy & DevOps-Friendly — the biggest barrier to evaluate and adopt a new security solutions is often the pain and efforts of deployment, and the amounts of false-positive alerts it generates. The ideal solution should be relatively quiet, only alert on real attack attempts, and easy to deploy (agentless).

Actionable Recommendations — once excessive permissions or entitlements are detected, the solution should provide actionable, detailed hardening recommendations, prioritizing the most important gaps first.



Radware's Cloud Native Protector includes smart hardening of configurations and permissions, AI-based anomaly detection of malicious activity, and provides compliance reports.

Customer Benefits

Adopting a least-privilege approach easily closes the gaps of excessive permissions and entitlements. Using the appropriate technology to implement it opens up a world of opportunities:

Prevent data breaches that occur through accidental exposure of cloud infrastructure

Protect cloud accounts against takeovers and account abuse, such as cryptomining

Visibility into cloud assets and their exposure potential

Avoid excessive permissions, thereby limit exposure potential via user account compromises

Detect hacking attacks by identifying & blocking suspicious behaviors before data is lost

Easily access compliance reporting for key industry standards such as PCI DSS, HIPAA and others

A consistent security policy makes it considerably easier to detect anomalies. Having it enforced automatically also enables greater visibility and efficiency at scale - meaning the same-sized IT and Security teams can handle much larger workforces operating a much more complex ecosystem.

Summary — Take Responsibility

It is tempting for enterprises to assume that cloud providers are completely responsible for network and application security to ensure the privacy of data. In practice, cloud providers provide tools that enterprises can use to secure hosted assets. While cloud providers must be vigilant in how they protect their data centers, responsibility for securing access to apps, services, data repositories and databases falls on the enterprises.

Network and application security can be a competitive advantage for companies to build trust with their customers and business partners. Now is a critical time for enterprises to understand their role in protecting public cloud workloads as they transition more applications and data away from on-premise networks.

The responsibility to protect the public cloud is a relatively new task for most enterprises. Since everything in the cloud is external and accessible, if not properly protected with the right level of permissions, enterprises must quickly incorporate smart configuration hardening into their network security strategies to address this growing threat.

GlobalDots works with cutting-edge security players to help organizations secure their cloud environments by providing a comprehensive, cloud-based solution to harden cloud configurations, reduce attack surfaces, augment security postures, and immediately respond to attacks once they are discovered.

About GlobalDots

GlobalDots is a 17-year world leader in connecting businesses with the latest cloud & web technologies. We consult, resell, implement, and customize full-stack solutions, including cost & performance optimization, security, connectivity, and managed services. Fusing an insatiable hunger for innovation with a diligent team of hands-on experts, we help our customers thrive & grow in a quickly-changing world.

Contact us to learn how to better secure your cloud environment.

Gilad Kfir
Cloud Specialist
gilad@globaldots.com

Steven Puddephatt
Solutions Architect
steven@globaldots.com

Mickael Franco
Tech Partnership Manager
mickael@globaldots.com