radware

Protecting Cloud Workloads from 2021’s Top Cloud Threat

WHITE PAPER

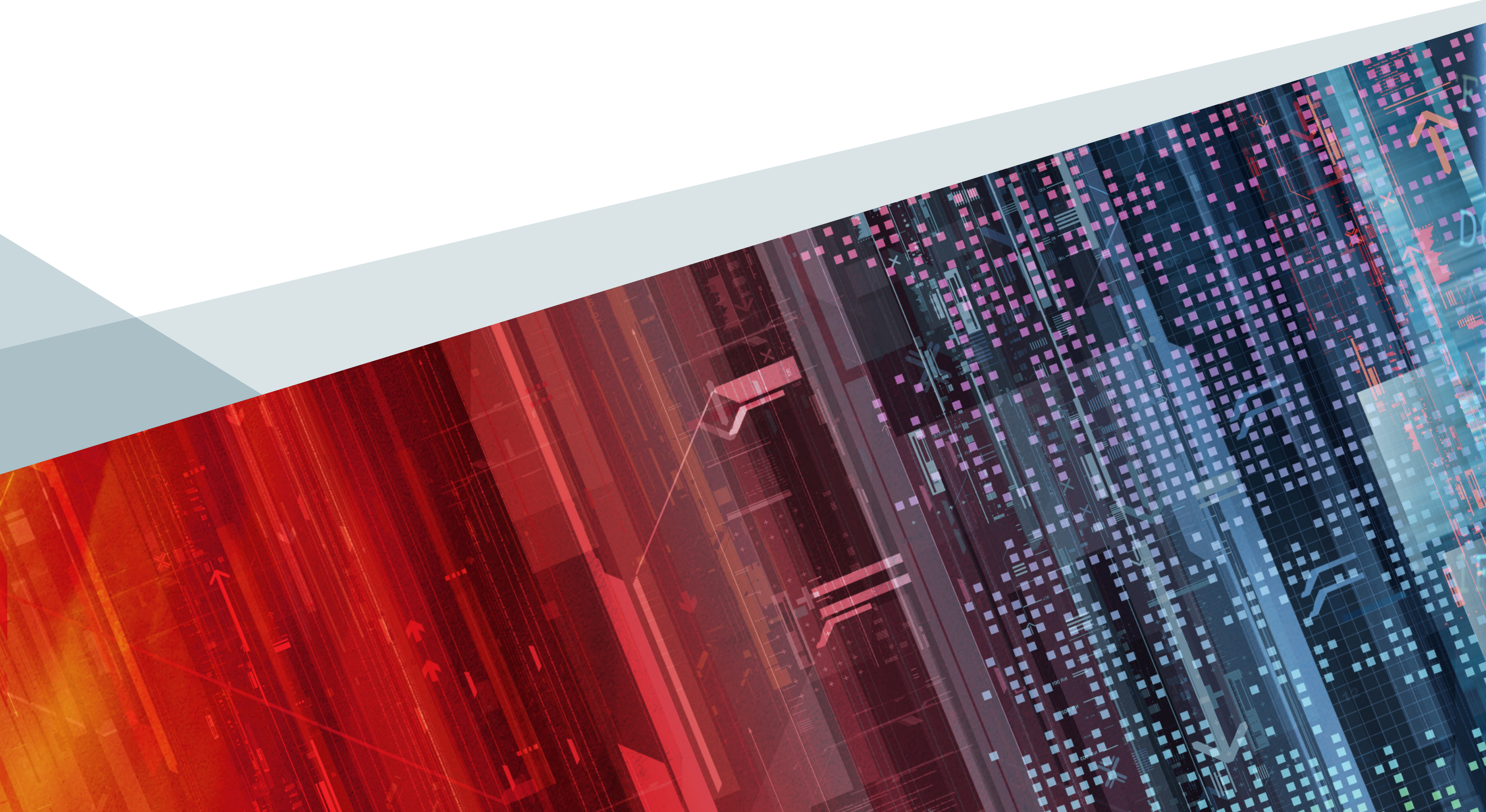


TABLE OF CONTENTS

- The Old Insider Is the New Outsider 3
- Your Permissions Equal Your Attack Surface 4
- Removing the “Mis” from Misconfigurations 4
- Traditional Protections Provide Piecemeal Solutions 5
- A New Approach for Protection 5
- Radware’s Cloud Native Protector 6
- Comprehensive Protection 6
- Agentless, Cloud-based Deployment 6
- Smart Hardening 7
- Detection of Anomalous Activity 8
- Customer Benefits 9
- Summary: Take Responsibility 9

Migrating workloads to public cloud environments exposes organizations to a slate of new cloud-native attack vectors that do not exist in the world of premise-based data centers. In this new environment, workload security is defined by which users have access to your cloud environment and what permissions they have. As a result, protecting against excessive permissions — and quickly responding when those permissions are abused — becomes the first priority for security administrators.

Radware provides an agentless, cloud-native solution for comprehensive protection of assets hosted on Amazon Web Services (AWS) and Microsoft Azure. It extends Radware's stack of security solutions to protect the overall security posture as well as individual cloud workloads. Radware's solution helps organizations fortify their cloud security posture, reduce their attack surfaces and protect their cloud environments against cloud-native attack vectors.

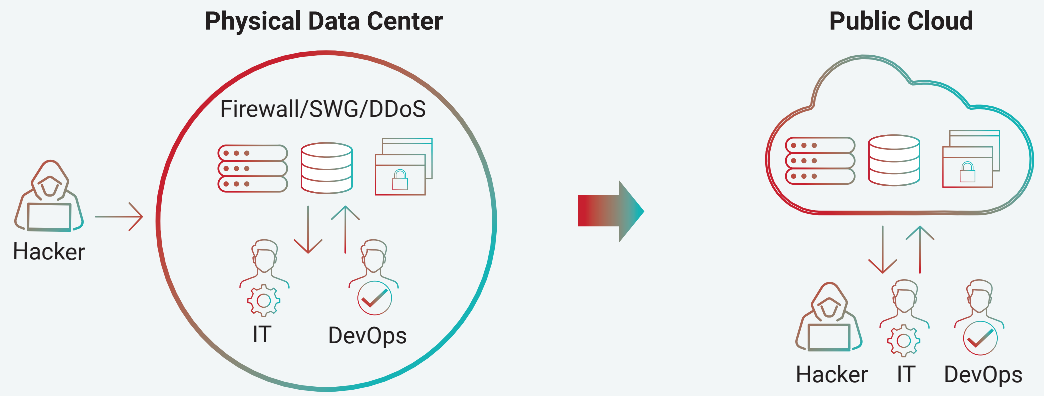
This white paper provides an overview of the security challenges brought about by migrating computing workloads to public cloud environments and describes how Radware addresses those challenges and assists organizations in protecting themselves.

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 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. IT administrators and hackers now 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. Workload security, therefore, is defined by the people who can access those workloads and the permissions they have.



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

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

Figure 1: The "old" world compared to the new cloud world

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), service violations (i.e., completely taking over cloud resources) and resource exploitation (such as cryptomining).

Such excessive permissions are frequently mischaracterized as "misconfigurations," but they are actually the result of permission misuses or abuses by people who shouldn't have them. Protecting against those excessive permissions becomes the No. 1 priority for protecting publicly hosted cloud workloads.

Removing the "Mis" from Misconfigurations

To prevent attacks, enterprises must harden configurations to address promiscuous permissions 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 the approach of "least privilege" enables enterprises to meet those goals. The process requires applying behavioral analytic methods over time, including regular reviews of permissions and a continuous analysis of the usual behavior of each entity just 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 with the assistance of an outside security partner with deep expertise and a system that utilizes automated algorithms that measure activity across the network to detect anomalies and calculate if malicious intent is probable. Often attackers will perform keychain attacks over several days or months.

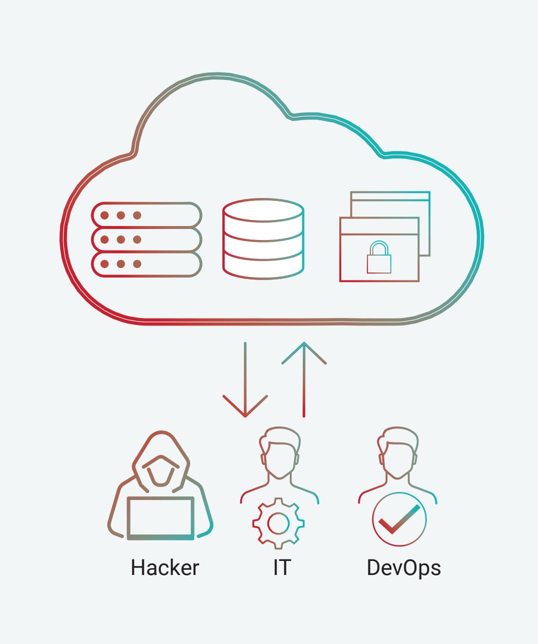


Figure 2: In the cloud, IT administrators and hackers have equal access.

Traditional Protections Provide Piecemeal Solutions

The problem is that existing solutions provide incomplete protection against the threat of excessive permissions.

- The **built-in mechanisms of public clouds** usually provide basic 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 of their networks.
- **Compliance and governance tools** usually use static lists of best practices to analyze permissions usage. However, they will not detect (and alert to) excessive permissions and are usually blind to activity within 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 nonserver 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

Modern protection of publicly hosted cloud environments requires a new approach.

- **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 alerting against such permissions becomes paramount. This cannot be done just by measuring against static lists of best practices, but it must be based on analyzing the gap between the permissions a user has defined and the permissions that user actually uses.
- **Harden security posture:** The best way of stopping a data breach is preventing it before it ever occurs. 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 of a list 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 allow administrators to respond faster to security incidents and mitigate attacks within seconds of detection.

Radware's Cloud Native Protector

Radware is extending its line of cloud-based security services to provide an agentless, cloud-native solution for comprehensive protection of workloads hosted on AWS and Azure. Radware's solution provides overall cloud security posture management (CSPM), together with cloud infrastructure entitlement management (CIEM) capabilities, cloud threat detection and response, and cross-cloud visibility.

Radware's solutions address the core problem of cloud-native, excessive permissions by analyzing the gap between granted and used permissions and providing smart configuration hardening recommendations.

Radware's Cloud Native Protector contains a number of unique features.

Comprehensive Protection

Radware's Cloud Native Protector provides comprehensive protection for cloud environments by securing the overall cloud account security posture and protecting individual workloads within the account.

Unlike other solution categories that focus on either management of the control plane (such as most compliance and governance tools) or protection of individual assets and resources (agent-based solutions), Radware's solution covers both the data plane and control plane, enabling protection of individual assets while taking into consideration the overall context of the account. In addition, Cloud Native Protector offers security for cloud-native services, such as Amazon Simple Storage Service (S3).

This approach protects AWS accounts across the five dimensions that comprise public cloud activity: users, machines, databases, storage and AWS services.

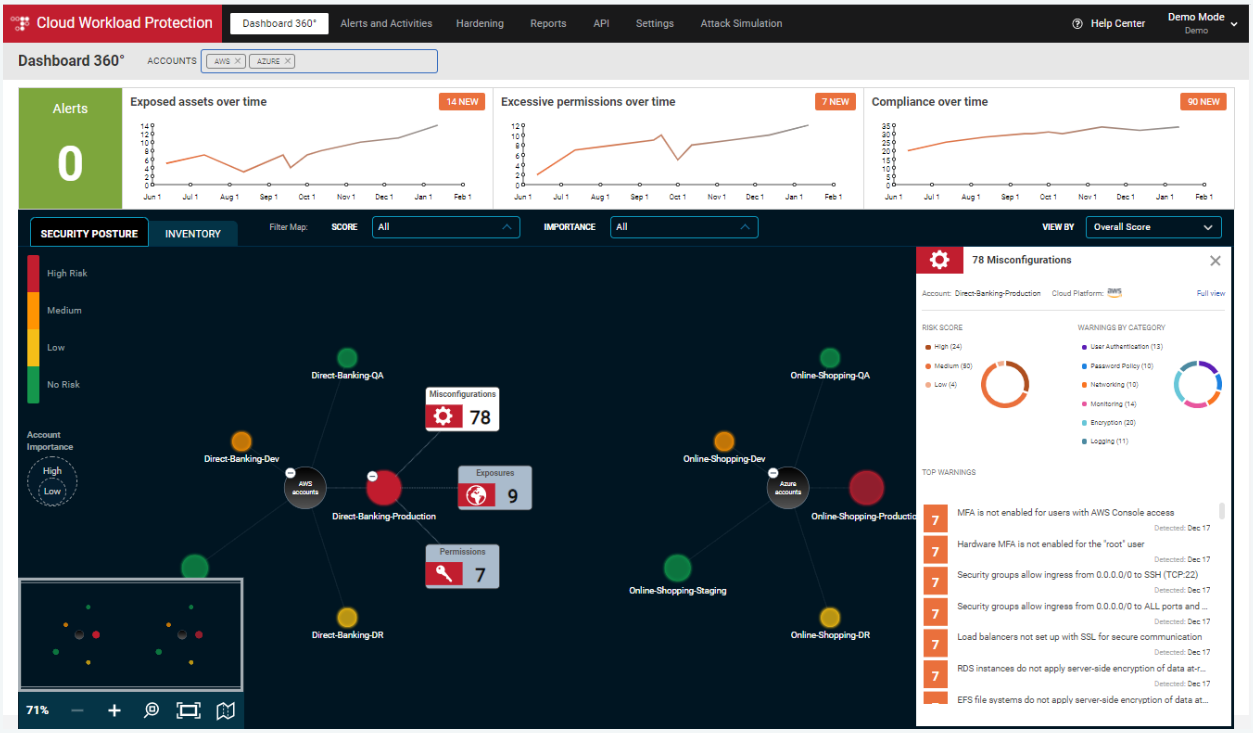
Moreover, Radware is the only security vendor to provide full-stack protection of applications hosted on public clouds, covering both the application surface with its WAF, bot management, API protection and DDoS protection solutions, as well as the cloud infrastructure, with its Cloud Native Protector offering.

Agentless, Cloud-based Deployment

Radware's solution is agentless, so it can be deployed easily and effortlessly.

Cloud Native Protector works through direct integration with cloud-based environments, collecting logs, policy configurations and alerts to build a full picture of cloud account activity and potential vulnerabilities. Compared to agent-based solutions, the agentless approach has a number of key benefits to it.

- **Management:** Installing software agents on a large number of servers incurs high management overhead. This is particularly true for large and dynamic environments in which servers are spun up and spun down on a regular basis.
- **Security coverage:** Since agent installation is required for protection of each specific server, if administrators forget or neglect to install an agent on any one of those servers, those assets will not be protected at all.
- **Protection of nonserver assets:** While agent-based solutions can provide granular insight into specific resources, they usually lack insight into the overall cloud security posture and context. In addition, they usually cannot protect cloud-native services or serverless functions for which there is no server on which an agent can be installed.



Account: Direct-Banking-Production Cloud Platform: aws

RISK SCORE

- High (24)
- Medium (50)
- Low (4)

WARNINGS BY CATEGORY

- User Authentication (13)
- Password Policy (10)
- Networking (10)
- Monitoring (14)
- Encryption (20)
- Logging (11)

TOP WARNINGS

7 MFA is not enabled for users with AWS Console access
Detected: Dec 17

7 Hardware MFA is not enabled for the "root" user
Detected: Dec 17

7 Security groups allow ingress from 0.0.0.0/0 to SSH (TCP:22)
Detected: Dec 17

7 Security groups allow ingress from 0.0.0.0/0 to ALL ports and ...
Detected: Dec 17

7 Load balancers not set up with SSL for secure communication
Detected: Dec 17

7 RDS instances do not apply server-side encryption of data at-r...
Detected: Dec 17

EFS file systems do not apply server-side encryption of data at...

Figure 3: User-friendly, agentless solution

Smart Hardening

Radware addresses the problem of excessive permissions by detecting who has relevant permissions, what is the scope of the permissions and what anomalies occur in permission usage.

Most compliance and governance solutions measure configurations against a static list of best practices. This is useful for discovering if two-factor authentication (2FA) is enabled, all user passwords meet strong password rules, etc. However, it will not alert you, for example, to a database administrator having system-level permissions that are never used — and probably shouldn't have been issued in the first place.

Radware takes a different approach by analyzing the gap between granted permissions and permissions that are actually used. Radware builds a baseline of user activity in the cloud accounts and looks for patterns and vulnerabilities which, if exploited, could lead to data theft or account compromise. Radware's approach provides a number of key customer benefits.

- **Reduces attack surface:** Radware helps detect unused and unnecessary permissions and applies the principle of least privilege to eliminate them.
- **Hardens security posture:** Radware provides smart hardening recommendations to help revoke excessive permissions that might be exploited by malicious actors and fortifies the organization's cloud security posture.
- **Detects anomalous activity:** Once a baseline of user behavior is established, Radware uses advanced machine learning algorithms to detect anomalous user activity that deviates from established behaviors. This helps with detecting potentially malicious activity within the cloud account.

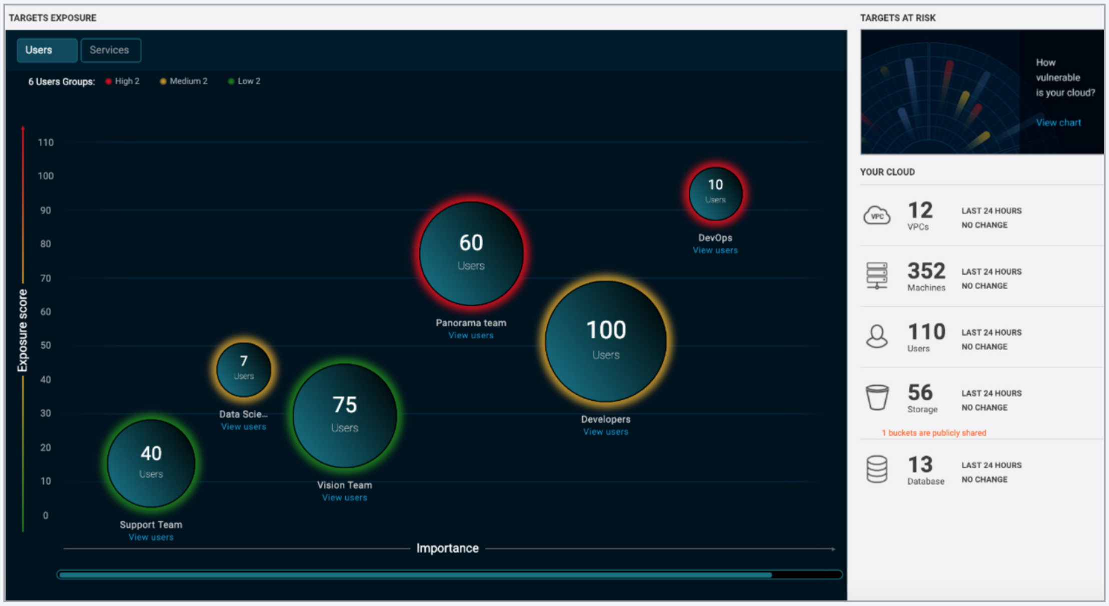

TARGETS EXPOSURE
Users
Services
6 Users Groups: ● High 2 ● Medium 2 ● Low 2
Exposure score
110
100
90
80
70
60
50
40
30
20
10
0
10 Users DevOps View users
60 Users Panorama team View users
100 Users Developers View users
7 Users Data Scie... View users
75 Users Vision Team View users
40 Users Support Team View users
Importance
TARGETS AT RISK
How vulnerable is your cloud?
View chart
YOUR CLOUD
12 VPCs LAST 24 HOURS NO CHANGE
352 Machines LAST 24 HOURS NO CHANGE
110 Users LAST 24 HOURS NO CHANGE
56 Storage LAST 24 HOURS NO CHANGE
1 buckets are publicly shared
13 Database LAST 24 HOURS NO CHANGE

Figure 4: Detecting excessive permissions for user groups

Detection of Anomalous Activity

Radware uses advanced machine learning algorithms to detect anomalous user activity that might be indicative of malicious account activity, such as data theft attempts or account compromises. Examples of such anomalous activities include the invocation of API calls that the user has never done previously, changing resource access permissions to be public or changing system settings.

The challenge, however, is that each such activity can be legitimate or illegitimate, and it is usually difficult to tell without proper context. This is why Radware correlates individual activities and places them in linear storylines that show step-by-step attack progression. This helps uncover attacks underway by monitoring lateral movements and communications across all asset types, including users, servers, accounts and services.

Based on this information, security administrators can work to quickly block potential attacks by using a combination of manual and automated response mechanisms.

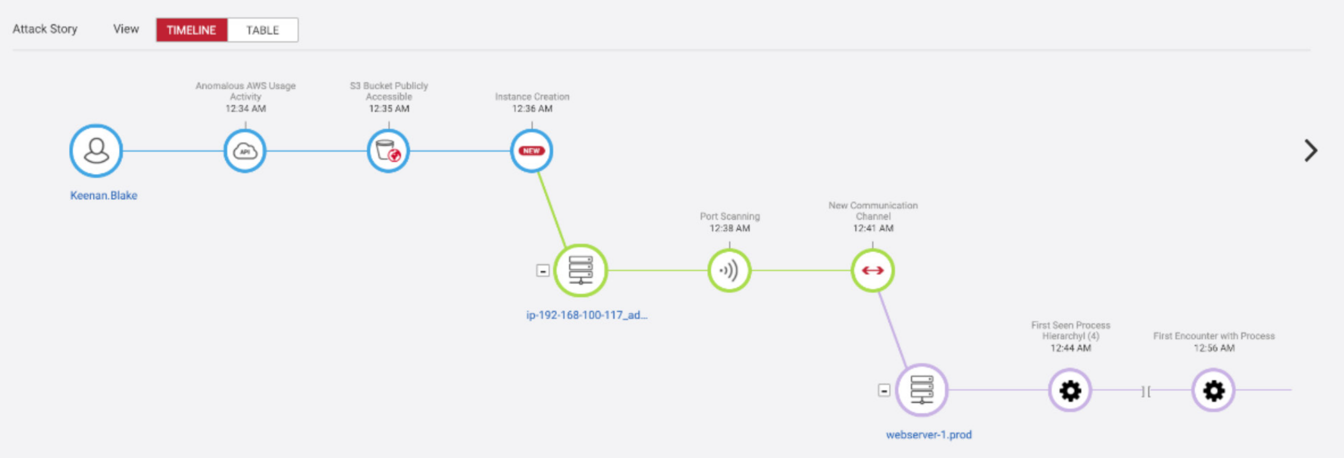

Attack Story
View
TIMELINE
TABLE
Keenan.Blake
Anomalous AWS Usage Activity 12:34 AM
S3 Bucket Publicly Accessible 12:35 AM
Instance Creation 12:36 AM
NEW
ip-192-168-100-117_ad...
Port Scanning 12:38 AM
New Communication Channel 12:41 AM
webserver-1.prod
First Seen Process Hierarchyl (4) 12:44 AM
First Encounter with Process 12:56 AM

Figure 5: Contextual, step-by-step attack progression

Customer Benefits

Customers of Radware's Cloud Native Protector enjoy the following benefits:

- Prevention of data breaches that occur through accidental exposure of cloud infrastructure
- Protection of cloud accounts against takeovers and account misuses, such as cryptomining
- Visibility into cloud assets and an understanding of what assets exist and where the customer might be exposed
- Avoidance of excessive permissions thereby limiting the potential for exposure through user account compromises
- Detection of hacking attacks by identifying suspicious behaviors and blocking them before data is lost
- One-click compliance reporting, with built-in reports for key industry standards such as PCI DSS, HIPAA, and others

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.

Radware helps organizations secure their cloud environments by providing a comprehensive, cloud-based solution to harden cloud configurations, reduce their attack surfaces, fortify their security posture and immediately respond to attacks once they are discovered.

Contact us to learn more about how Radware's Cloud Native Protector can help you secure your cloud environment.

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 www.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.