RAPID7

July ‘24

Cloud Attack Paths Unveiled: Lessons Learned from the SOC

David Coleman

Senior Manager, Solution Engineering
APAC

RAPID7

Best-in-Class Technology

Security Services

Research and Community

Global Ecosystem

11,000+ Customers

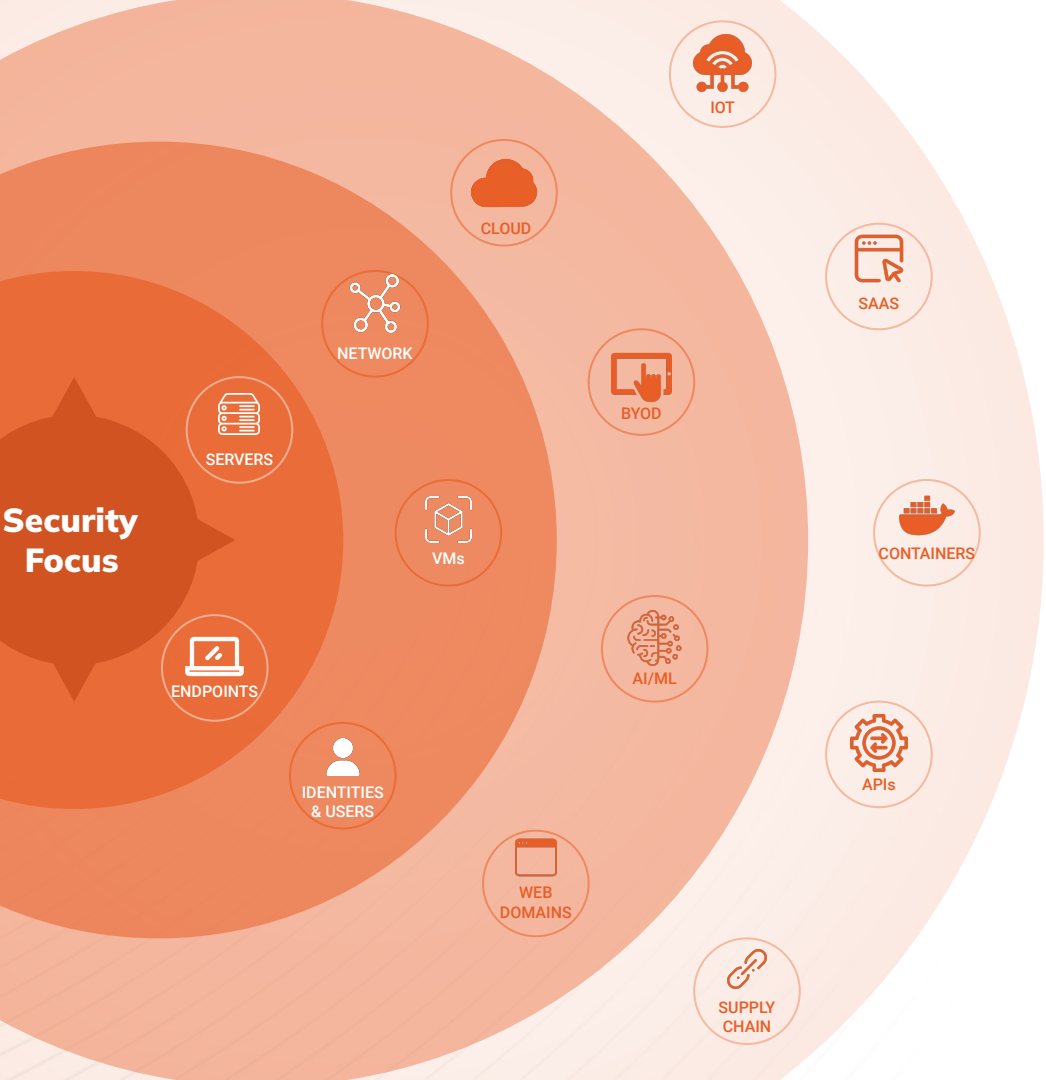
43% of Fortune 500
NASDAQ: RPD

Global Footprint

144 Countries
21 Offices

Leader of Innovation

56 Patents
Open Source Communities



It's rare that an organisation knows if they are monitoring 100% of their attack surface

You can't secure what you can't see

You don't have visibility if you don't have confidence in your data

You cant trust your data if your data sources are in conflict

Rapid7's Chief Security Officer Jaya Baloo pointed out that roughly 45% of data breaches are due to cloud issues, caused by misconfigurations and vulnerabilities, making cloud security a critical focus

https://www.rapid7.com/blog/post/2024/06/25/takeaways-from-the-take-command-summit-understanding-modern-cyber-attacks/

Threat Actor Playground

Initial Access

Discovery

Credential Access

Execution

Persistence

Impact

Scenario 1

Real-World Scenario: Ransomware

Incident Timeline

All times are in Universal Coordinated Time (UTC)

Cloud Account | T1078.004

Earliest evidence of compromise on May 23rd, 2024. The **root** user performed enumeration from the IP address 195.35.36[.]157

Cloud Services | T1021:007

On June 1st, 2024 at 08:51:45, KMS key created by threat actor. A KMS key was created by the **ses-smtp-user-prod** account

Data Destruction | T1074

On June 1st, 2024 at 11:29:13, earliest evidence of storage bucket, database, and instance deletion and termination by source IP address 18.210.12[.]218.

Create Account | T1136.003

On June 1st, 2024 at 8:27:10, the threat actor created **ses-smtp-user-prod** with default admin policy, access key, and no password reset on login

Transfer Data to Cloud Account | T1537

On June 1st, 2024 at 08:53:02, the threat actor initiated copying and modifying databases and database snapshots

Real-World Scenario: Remediation actions

- **Ensure all threat actor-leveraged Access Keys are deleted:** Immediately disable or delete compromised root user access keys to prevent further unauthorized access. This can be accomplished through either AWS Management Console, AWS CLI, or AWS API.
- **Ensure all user accounts that the threat actor created are remediated:** Temporarily deactivate any unauthorized users to prevent further access. This can be done by removing permissions or disabling access keys.
- **Ensure that any modifications made to RDS instances or the creation of resources, such as buckets, are reverted:** If the organization has backups or snapshots, restore the RDS instance from the most recent known good snapshot. Ensure that the restored instance is placed in a secure environment with restricted access.
- **Rotate all Access Keys:** Rotate all access keys associated with IAM users and roles to ensure that no other keys have been compromised. This involves creating new keys and disabling or deleting the old ones. Rotate the keys regularly.

Real-World Scenario: Corrective Actions

- **Implement Multi-Factor Authentication (MFA)** for all accounts with access to the cloud services and applications: Implement MFA on all accounts for all ingress points into the environment. For externally facing systems, MFA helps to mitigate the risk of brute- force, password spraying, phishing, and accessing the environment unauthenticated via VPN. Applications, such as G-Suite, AWS, password managers, and all business applications, should contain MFA as well.
- **Enable a trail in CloudTrail to store data in a S3 bucket:** This enhances monitoring and auditing capabilities, ensures that all API activities are logged and retained for an extended period, and facilitates better forensic analysis and compliance with data retention policies.
- **Enable CloudTrail for data events:** This enhances monitoring and auditing capabilities by logging detailed resource operations (data events) in addition to management events. This also helps in tracking specific actions on resources, such as S3 object-level operations, which are crucial for forensic analysis.
- **Search for plain text access keys that could lead to the root account compromise** (GWS, Confluence, GitHub, etc.): This helps in preventing future incidents by ensuring that no sensitive credentials are inadvertently exposed in plain text across various platforms.
- **Enable bucket versioning with MFA delete:** This enhances data protection and recovery capabilities by enabling versioning on S3 buckets and requiring MFA for delete operations. This helps to prevent accidental or malicious deletion of objects and ensures that previous versions of objects are retained for recovery. Additionally, it limits the ability to change bucket versioning settings, as MFA is required for such changes.

Scenario 2

Real-World Scenario 2: Resource Hijacking

Initial Access T1078

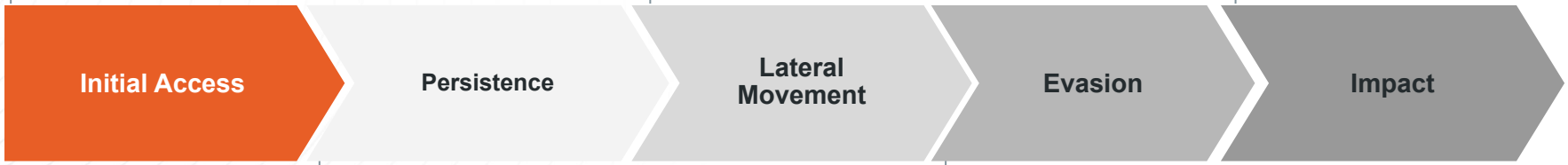
Earliest evidence of compromise March 29th, 2024. Exposed IAM Access keys in Public S3
Request via AWS CLI to ‘Start Instance’ & ‘RequestServiceQuotaIncrease’

Lateral Movement T1021

Two new IAM Resource created & assigned additional permissions and roles for SES & SQS (AttachUserPolicy)
SES commands issued to verify new domain, DKIM and email address

Impact

Sending an abnormally large amount of emails in mass phishing campaign.
Customer contacted by AWS re SES email bounce rate issue and rate increase



Resource Development T1098 & T1583

Via CLI New IAM Resource created, assigned additional permissions & New microservice deployed.
Increase Sending Quote initiated & Sending Rate, and SNS quota

Evasion T1070

Delete profile elements, policies and access keys for a previously created user, executed from external IP not owned by customer

Real-World Scenario: Remediation actions

- **Remove all non-Company ZZZ or stale IAM resources**
  - Delete any unused and non-Company ZZZ IAM users and roles.
  - For any IAM user resources that are for service account use, remove console access by removing the login profile.
  - Delete any attacker created access keys and generate new access keys.

- **Change Passwords for IAM Users that require Console Login and generate new access keys**
  - Change the affected account passwords as soon as possible to prevent a threat actor from leveraging the credentials to access services.
  - Instruct users to not just change one character of a password, such as changing Example1! to Example2! and to follow the NIST guidelines for the ‘memorized secret’ password policy1. A threat actor who has captured past credentials could be more successful in guessing credentials changed by only one character.

Real-World Scenario: Corrective Actions

- **Limit access to AWS resources to Organization accounts**
- **Enable a trail in CloudTrail to store data in a S3 bucket**
- **Enable CloudTrail for data events**
- **Enable AWS Guard Duty**
- **Configure an Identity Provider and Single Sign On (SSO) for human users and MFA**
- **Only allow access to AWS resources from approved IP addresses and approved AWS accounts**

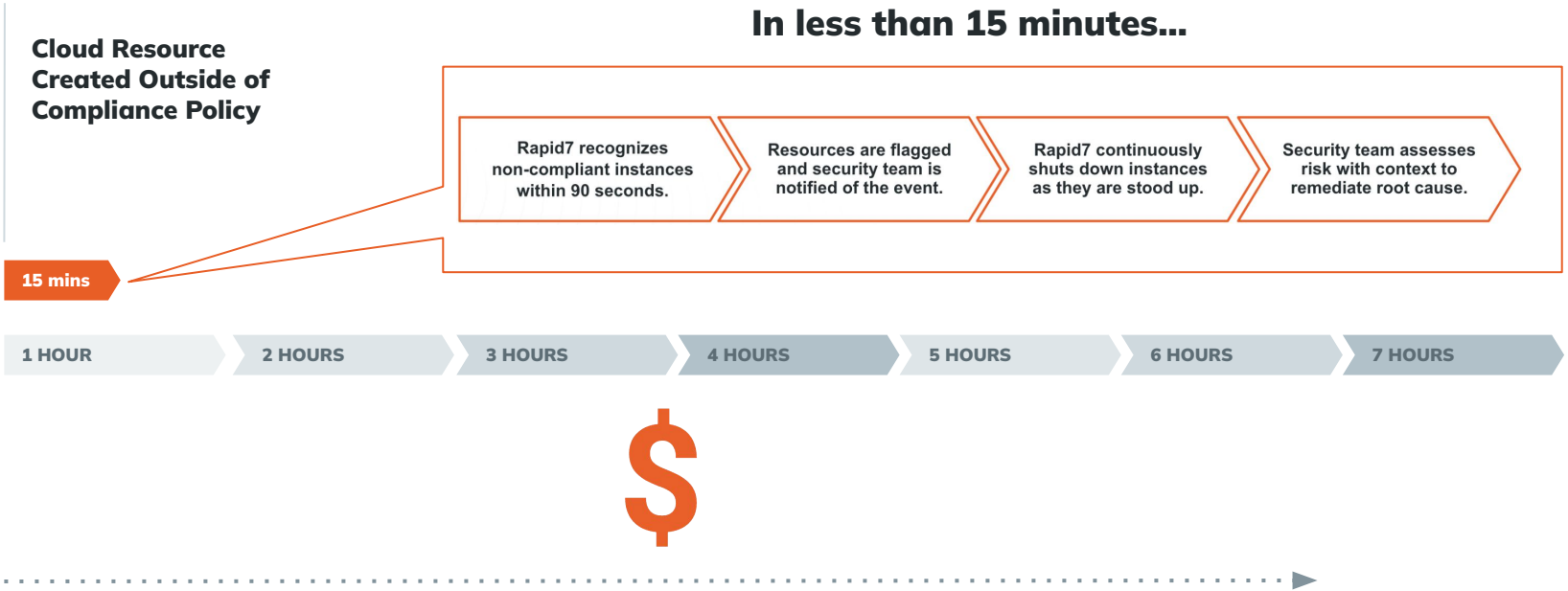
Scenario 3

Real-World Scenario: Cryptomining

Options?

Real-World Scenario: Cryptomining

Remediation is automated to prevent catastrophic scenarios.



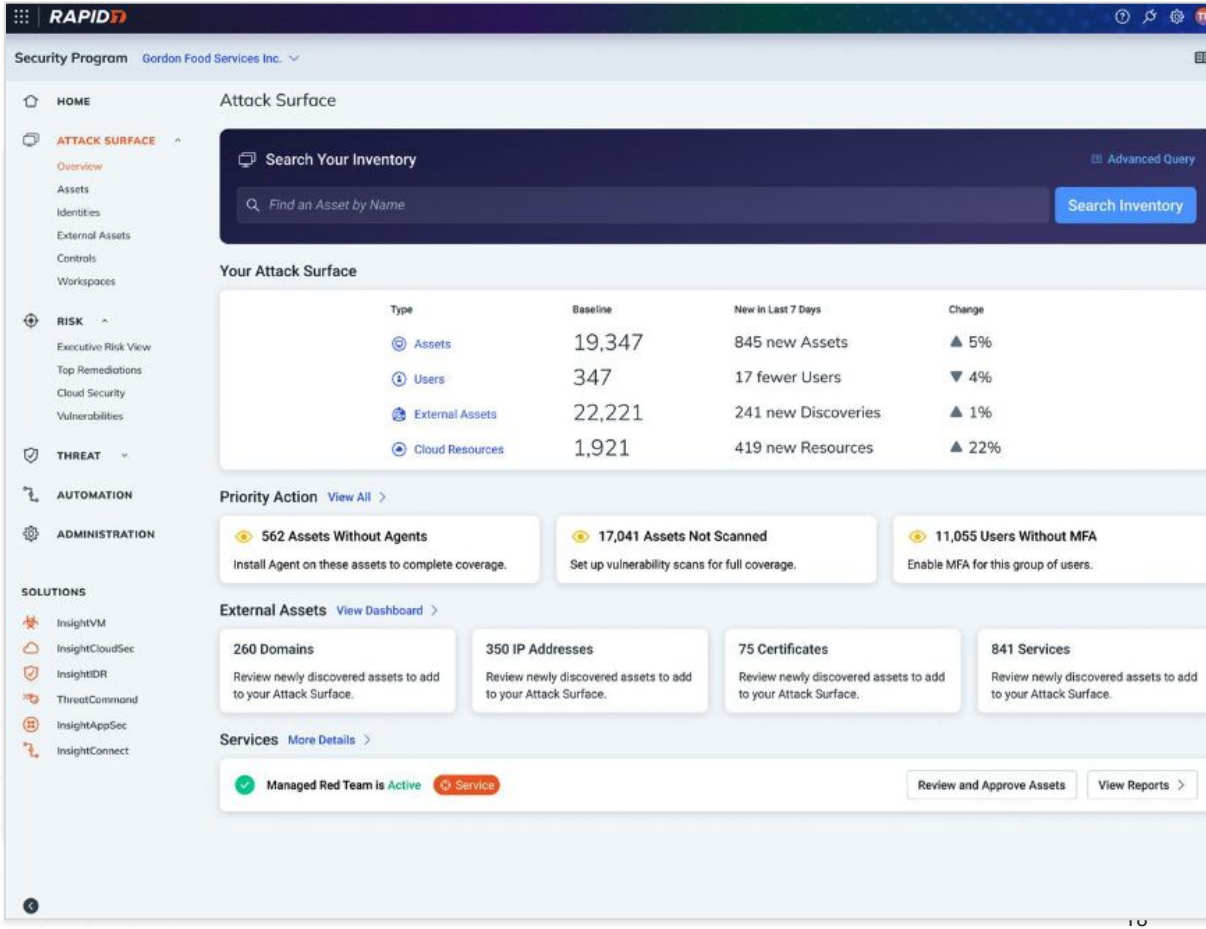
Attack Surface Management

WHY

Comprehensive inventory of attack surface across applications, cloud, and devices

WHAT

- Visualize relationships between applications, services, and the underlying infrastructure. Alert on best practices deviations
- Organize inventory by app/business to make it easier to communicate risk and build accountability
- Aligned view across Security and Ops teams to drive effective collaboration and risk reduction
- Search on multiple attributes and gain actionable insights on remediation functions
- External Attack Surface lets you view what an outside actor would



Attack Path Analysis

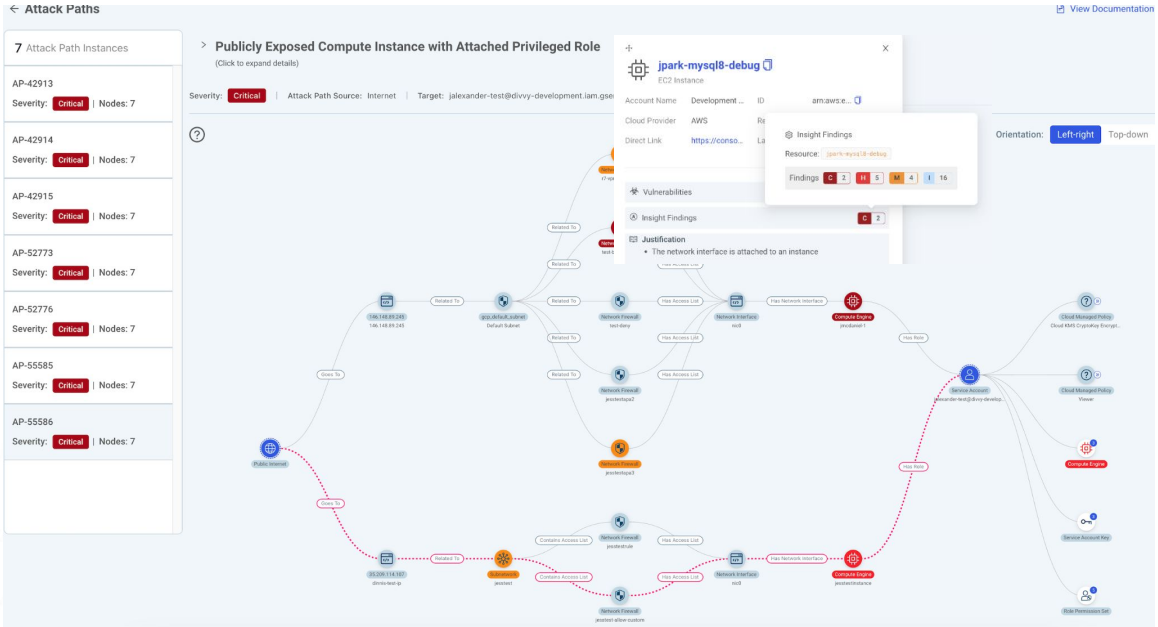
WHY

Security teams need a way to visualize risk context and potential blast radius to focus remediation on exploitable resources and resources that an attacker could reach by lateral movement

WHAT

Security graph visualizations for related resources and attack paths

- Map relationships between compromised resources and the rest of your environment in real-time
- Prioritize remediation efforts by identifying toxic combinations that lead to real business impact
- Communicate risk and potential impact of an exploit to non-technical stakeholders
- Visualize multiple paths to a compromised resource



RAPID7

Context-driven cloud security can help get ahead.

Relevant insights, not aggregated noise.

Cloud Detection and Response

Detect and Respond to Threat Actors in the Cloud

Detection

Detect cloud malicious activity and suspicious events and aggregate alerts from your various cloud security controls in one place with the ability to automatically forward to SIEM/XDR

Environmental Context

Surface key indicators that matter most from the noise such as Public Access, Application, Production flags, and Resource Owners

Risk Context

Analyze and surface asset and user risk profiles to accelerate prioritization and investigation of alerts

Response

Automatically respond to threats in the cloud with bot automation to perform response actions like disabling user access or turning off instances.

Our Research Shows Maturing Your Security Program Has Real Perks

76%

Enable Strategic Business Goals

76% more likely to recognize the link between security and business

7x

Contain Attacks Faster to Limit Damage

7x more likely to contain an identified attack in minutes

4.3x

Mitigate Risk Effectively

4.3x more likely to say they can mitigate risk in a timely fashion

10.8x

Retain Top Security Talent

10.8x more likely to report low security team attrition

7x

Maintain Good Security Hygiene in the Cloud

7x more likely to monitor and manage cloud hardening well

56%

Adopting the Cloud at a More Rapid Pace

56% more workloads in the cloud

Source: Rapid7 original research conducted in partnership with ESG.

Thank you!