CLOUD IN CRISIS: SOLVING THE MULTI-CLOUD SECURITY PROBLEM

data SOLUTIONS

TABLE OF CONTENTS

1 STATE OF THE CLOUD

Cloud adoption has ramped up during the pandemic. Businesses are migrating at a much faster pace, with 91%[1] of enterprises reporting their cloud usage has been higher than planned and 78% using a mix of public and private (or hybrid) cloud. Small wonder, then, that the cloud market is predicted to expand to $1 Trillion by 2024, with the IaaS market, in particular, set to see exponential growth.

Yet the key trend this year is the migration to multi-cloud – the use of more than one public cloud service provider, typically a combination of AWS, Microsoft Azure and Google Cloud – with 90%[2] of large businesses already embracing this strategy and 86% expected to follow suit within the next two years. Multicloud promises to allow organisations to use the best of what's on offer without the fear of lock-in to any one vendor.

[1] Flextera 2021 State of the Cloud report, March 2021, https://bit.ly/3sOUi7g

[2] HashiCorp State of Cloud Strategy survey, August 2021, https://bit.ly/3yIPK9q

Businesses recognise the benefits cloud can bring, with many now adopting a 'cloud first' strategy, but this enthusiasm is in stark contrast to confidence in security. 72% of organisations lack confidence in their cloud security posture, and 96% of security professionals are concerned about public cloud security even though 95% of cloud security breaches are deemed to be the fault of the enterprise. It takes a staggering 280 days to identify a breach, leading 81% to believe that traditional security solutions simply aren't suitable for the cloud.

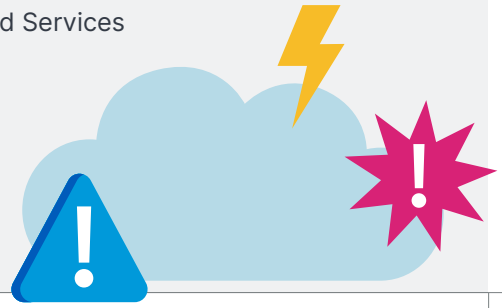
The rapid adoption and a distributed remote workforce we now have has magnified the threat surface of the enterprise. Since January 2020, there has been a 630%[3] rise in cyberattacks on cloud services, and while the top threats continue to be misconfiguration and unauthorised access and insecure interfaces, the fastest growing are ransomware and malware.

As cloud migration increases, security teams are struggling to get complete visibility into the cloud infrastructure, which can leave gaps and blind spots in the security posture, making it susceptible to attacks but there is also a perception problem over who's responsibility security is within the cloud.

CLOUD SECURITY ALLIANCE

TOP CLOUD THREATS

- Data Breach
- Misconfiguration and Inadequate Change Control
- Insufficient Identity, Credential, Access, and Key Management
- Insufficient Identity and Credential Management
- Account Hijacking
- Insider Threat
- Insecure Interfaces and Application Programming Interfaces
- Weak Control Plane
- Metastructure and Applistructure Failures
- Limited Cloud Usage Visibility
- Abuse and Nefarious Use of Cloud Services



[3] McAfee Cloud Adoption and Risk report, May 2020, https://bit.ly/3jhWcdo

2 THE DATA SECURITY DISCONNECT

Many enterprises believe that the cloud is secure by default and that cloud-native security tools will protect them against security breaches. This results in a disconnect which leaves data exposed.

It is highly important for businesses operating in the cloud to accept the fact that there is shared responsibility for security. Cloud service providers are responsible only for the security "of" the cloud; while security "in" the cloud is the responsibility of the business.

While all cloud service providers have their own native security capabilities that can be easily configured and deployed, these capabilities work well only for a business with minimal security aspirations. Native security capabilities are features and not tools. They do not have the depth of coverage that a third-party cloud security platform can offer, which is why the business needs to have its own cloud security solutions.

THE CLOUD PROVIDER IS RESPONSIBLE FOR...

- Protecting the cloud provider's physical premises, software, network, and hardware
- Service-level security, i.e. protection against attacks that would affect the entire cloud service
- Ensuring their systems are always updated and have the necessary patches in place
- Providing business continuity services and contingencies in case of an accident or system failure

THE CLOUD CUSTOMER IS RESPONSIBLE FOR...

- Ensuring systems are properly configured
- Security of traffic coming in and out of the server
- Maintenance and protection of all platforms and applications running on the cloud
- Patching their OS and applications
- Configuring their OS, databases, and applications
- Managing and handling all matters related to login, authentication and access permissions
- Protection of the data that enters and exits the cloud service
- Controlling what data is loaded to the cloud and ensuring an appropriate level of encryption
- Enforcing security best practices for the cloud

3 CLOUD SECURITY FAILS

Over the next four years, 99% of cloud security failures will be the customer's fault, according to analyst firm Gartner [4], and 75% of these failures will be a result of improper cloud management. Understanding where the repeat failings lie can help to guide cloud security policy and investment.

MISCONFIGURATION

The cloud has tens of thousands of configurations, and one or a combination of these, if misconfigured, can affect or contribute to the risk of a cloud resource.

Cases of misconfiguration will creep up as the business become more agile and takes advantage of cloud services or as the DevOps team start spinning up infrastructure using code. The same line of code that spins up a compute instance can also expose that same instance to the public internet, for example.

Today, most solutions only look at misconfigurations that affect a resource and do not report on risks from associated or connected cloud resources. It's estimated that 99%[5] of misconfigurations in the cloud go unnoticed with examples including unauthorised access due to the failure to implement restrictions and safeguards and security group misconfiguration that allows an attacker to access cloud-based servers and exfiltrate.

QUANTIFY RISK POSTURE

The business needs to be able to baseline its cloud environment by assessing its infrastructure, identifying threats, and correcting any risks and violations of compliance or best practice to understand its risk posture. And it needs to perform this discovery and inventory on a regular basis to control its cloud security and compliance.

[4] Gartner, 'Is the cloud secure?', October 2019, https://gtnr.it/3yqspDw

[5] McAfee, Cloud-Native: The Infrastructure-as-a-Service Adoption and Risk report, 2019, https://bit.ly/3zulTxa

PRIVILEGE CREEP

Failing to implement least privilege, whereby restrictions are put in place to assign the least access needed to perform certain tasks, is the number one cause of security breaches. During audits, we found almost 90% of cloud accounts had too many users assigned administrator privileges that were not needed.

Privilege creep is where your least privilege policy is slowly eroded and undermined as more identities are added. A typical cloud environment has multiple human and non-human identities with tens of thousands of associated entitlements. It quickly becomes impossible to manage and govern these identities and their entitlements manually and so access can become granted by default.

Once compromised, the attacker can then leverage entitlements attached to the identity to laterally move within the infrastructure and access services or exfiltrate data. For example, an IAM Access Key is compromised, resulting in the cloud infrastructure getting misused for Crypto Mining activities and the business paying cloud costs for the period until the breach gets detected.

Cryptojacking is a straightforward way for hackers to make money in the public cloud because all they have to do is find a way into a customer's cloud, spin up a lot of high-capacity CPU rich servers for mining, and keep making money until the hapless customer detects the breach (mostly after they get an alarming bill from the cloud provider).

FALSE POSITIVES

Approximately 75% of security teams spend the same amount of time or more investigating false positives as they do investigating genuine threats, and the sheer volume of alerts can be overwhelming. Up to 76.8%[6] of alerts are believed to be false positives, and 31.9% of analysts fail to attend to them due to alert fatigue.

As new cloud providers are brought onboard under multi-cloud, the business ends up with incompatible software, which is then run simply in log/monitor mode or is disabled, with 91%[7] of businesses hobbling their software in some way due to coping with alert volumes.

Failing to process data into actionable metrics results in missed threats that can then take their time looking for ways to exploit vulnerabilities, increasing the risk of very damaging lateral attacks that can move across business systems.

THREAT MANAGEMENT

In an ideal world, security teams would be able to detect and apply importance to alerts so that the most critical vulnerabilities could be dealt with and resolved first. In reality, they can't. There is a huge disconnect between the security alerts being generated and having the ability to grade and manage them effectively.

Key to threat management is being able to prioritise alerts. Without this, security management becomes a game of whack-a-mole as you cannot determine which incidents are the most pressing and require attention first.

Failing to quantify alerts leads to the security team operating at a high alert level, expending a great deal of effort triaging alerts that are false or perhaps are just minor true positives. This then prevents real-time detection and response.

Without a good grip on threats, risk and remediation, it becomes impossible to move towards a mature cloud operating model where auto-remediation can be considered.

[6] Cloud Security Alliance report, 2017, no longer available

[7] Fastly and the Enterprise Strategy Group, Reaching the tipping point of Web Application and API security 2021, https://bit.ly/3kxRirV

LACK OF OVERSIGHT AND CLOUD SPRAWL

As businesses have built out their cloud presence, moving to either hybrid or multi-cloud models, so complexity has increased. This makes it harder to maintain visibility of all the identities across the cloud infrastructure, for instance, and as more security systems are brought online, so more alerts are generated, particularly if these third-party solutions aren't integrated adequately.

Unless the business has cross-cloud visibility, it cannot create an accurate inventory across Compute, Network, Storage and IAM components, or gain contextual insights of the security posture, all resources, alerts, and the compliance status or gain real-time security and operational intelligence and check the configuration of various resources using Cloud Query Language (CQL).

COMPLIANCE CHALLENGES

Businesses and their cloud provider now share responsibility for security, and this, together with a lack of visibility, the ephemeral nature of resources, and a multi-cloud environment, make compliance in the cloud challenging, particularly for those in regulated industries and with contractual requirements.

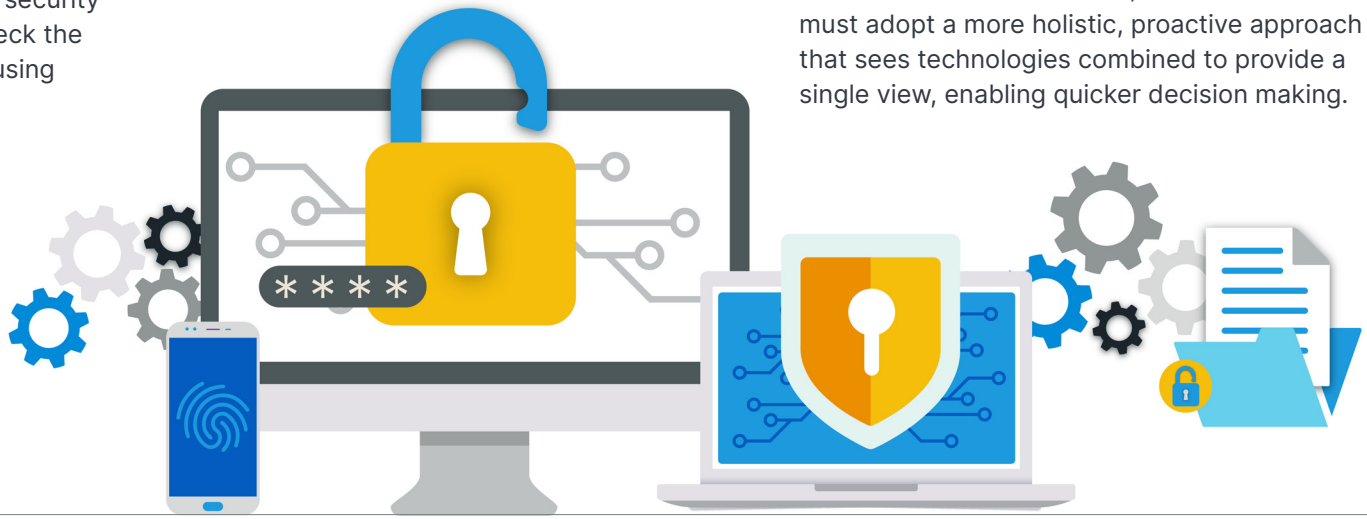
Cloud infrastructure should be continuously monitored for the risks of non-compliance with security requirements, standards, and regulations such as ISO 27001, CIS, NIST, GDPR, POPIA, Fedramp, HIPAA, HITRUST etc.

HIGH MTTD AND MTTR

The Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) to a potential security threat are the most important metrics for the security team when it comes to resolution. Both are now on the rise due to increasing threat volumes and the working from home trend.

The average time between discovery and notification has doubled in the past three years and now stands at 66 days[8]. Other reports suggest dwell time (the time between the start of a cyber intrusion and it being identified) stands at 30 days[9] for those self-detecting, although 12% of internal investigations have a dwell time in excess of 700 days.

To reduce MTTD and MTTR, the business must adopt a more holistic, proactive approach that sees technologies combined to provide a single view, enabling quicker decision making.



[8] BakerHostetler 2021 Data Security Incident Response Report, https://bit.ly/2UZV8Bu

[9] FireEye Mandiant M-Trends 2020 Report, February 2020, https://bit.ly/3teBHln

4 OVERVIEW OF TODAY'S SECURITY SOLUTIONS

The need to improve cloud confidence and create a cohesive approach to cloud security has seen a number of new archetypes emerge. Four cloud security pillars – CSPM, CIEM, CWPP, and CNAPP – are identified by Gartner and are now used as the basis to classify third party security solutions.

1. **CSPM** (Cloud Security Posture Management)

   CSPM provides cross-platform control of the cloud infrastructure. Previously known as Cloud Infrastructure Security Posture Assessment (CISPA), when capabilities were limited to reporting, CSPM security management automation tools address misconfiguration issues by analysing configurations and comparing these with other inputs to identify risks.

   CSPM solutions assess, detect, log, report, and automate issue remediation and are also capable of discovering all assets, detecting unused assets, enforcing a security baseline, and helping stay compliant with security standards and regulations.

   Today a good CSPM tool should facilitate security enforcement and operations, compliance assurance, investigation, and incident response.

> Through 2024, organisations implementing a CSPM offering and extending this into development will reduce cloud-related security incidents due to misconfiguration by 80%.
>
> — GARTNER, JANUARY 2019

2. **CIEM** (Cloud Infrastructure Entitlements Management)

Understanding the importance of access and entitlements, analyst firms Gartner and Forrester have highlighted the need to focus on Identity Governance in the cloud by reiterating the importance of Cloud Identity Governance (CIG) and CIEM. CIEM is newer than CSPM, and so fills the IAM gap.

Gartner defines CIEM as specialised identity-centric SaaS solutions focused on managing cloud access risk via administration-time controls for managing entitlements and data governance in hybrid and multi-cloud IaaS architectures, according to Forbes. CIEM Solutions leverage analytics and machine learning to detect anomalies around identities and entitlements.

Gaining complete control over all identities, access, and privileges can be challenging because of the number of enterprise infrastructure permissions. CIEM technologies discover all identities and users, their entitlements and enforce identity and access governance controls to reduce excessive entitlements and right-size privilege access across the multi-cloud.

3. **CNAPP** (Cloud-Native Application Protection Platform)

CNAPP is the latest addition to the Gartner cloud security fold and is a convergence of multiple disciplines such as CWPP, CSPM and some CIEM functionality that delivers a full stack multi-cloud overview.

CNAPP has come about in response to demand for 'cloud native' security that seeks to protect the apps rather than just the infrastructure. The reliance on Infrastructure as Code (IaC) (whereby the complexities of how to do things on each cloud platform were abstracted and code was run to build entire datacentres in the cloud), CNAPP became necessary in order to protect the code used to build this infrastructure from malicious intent.

CNAPP sees security workload and configuration scanning performed during development so that technologies are then protected during run time. Misconfigurations are not just identified but are used to identify security risks in associated or connected cloud resources.

CIEM AND CARTA

CIEM tools can be used in conjunction with Gartner's Continuous Adaptive Risk and Trust Assessment (CARTA) approach. This takes a "user and app" - centric approach to security that assumes:

a. More users requiring access to services will be situated outside of, rather than within, the enterprise network,

b. More unmanaged than managed devices will connect to services

c. Demand by internal users for apps delivered outside the enterprise network will be higher

This de-perimeterisation of the network assumes the perimeter is everywhere and so CARTA relies upon a zero-trust model, the implementation of least privilege, and ongoing monitoring to guard the network.

4. **CWPP** (Cloud Workload Protection Platforms)

CWPP solutions secure cloud workloads regardless of their type or location. CWPP is focused on the protection of workloads irrespective of type or location and scans for vulnerabilities and configuration issues, among other things, within the workload. (Workloads include VMs, containers, Kubernetes, and serverless workloads.)

CWPPs are designed to detect and prevent app attacks without needing to know the input source. They profile the application function and its behaviour and look for deviations from these and enforce a zero-trust policy.

A comprehensive CWPP should give you the ability to discover and manage any unmanaged workloads you discover. While CWPP capabilities vary across vendors, they typically include system hardening, vulnerability management, host-based segmentation, and system integrity monitoring. CNAPPs use CWPP to give them more visibility.

SUMMARY OF CLOUD SECURITY ARCHETYPES

	CSPM	CIEM	CNAPP	CWPP
SECURITY FOCUS	Misconfigurations, asset discovery, compliance, incident response	Identity and access management	Application protection	Secures cloud workloads
APPROACH	Cloud-native	Zero-trust, least privilege	Cloud-native, converged	Zero-trust
ADVANTAGES	Delivers control by creating a cloud footprint, monitoring for new additions and instances of misconfiguration, auditing against compliance policies, performing risk assessments and remediation	Fills the gaps left by CSPM. Applies identity control across the multi-cloud	Combines CWPP and CSPM. Looks to identify and correlate issues to determine risk.	Used by CNAPP to provide greater visibility across the data plane

RATIONALISING THESE APPROACHES

The four archetypes provide a much-needed cloud-centric approach to security, but they each focus on one particular area: no one strategy provides a complete security solution.

Over time, some of the archetypes have attempted to fill the gaps in security provisioning, which is why we see CIEM provide the IAM that CSPM lacks and CNAPP borrow from CWPP to gain more depth into application workloads. But they still largely operate independently.

To draw upon the security benefits of all four strategies, we need to simplify them and focus on what security teams need in order to quickly detect, investigate, triage, and resolve high-risk, high-impact vulnerabilities across the multi-cloud.

Core requirements to address security pain points are:

1. **A multi-cloud security baseline**

   The team needs to know its cloud footprint – resources, users, identities, roles and policies – across its cloud provider accounts, but it can be difficult to determine this information and create a unified view in a multi-cloud environment. Automating discovery and inventory enables all these assets to be detected and classified.

2. **Context-driven security**

   To deal with the huge number of false positives and prevent alert fatigue, the team needs to be able to prioritise threats, and for that to happen, they need contextual information. Today, most solutions only look at misconfigurations that affect a resource and do not report on risks from associated or connected cloud resources. This makes it difficult to establish true context indicators such as exploitability, exposure, blast radius and impact to help prioritise threats.

3. **Risk scoring based upon a standardised threat matrix**

   Using these context indicators based upon the CVSS framework from FIRST.org, the team can measure, assess and prioritise threats using the 0-10 framework and the risk appetite of the business to prioritise threats and determine how to remediate them.

4. **Real-time cross-platform threat detection**

   Centralising cloud management of security policies enables continuous monitoring of the security posture across potentially thousands of cloud accounts so that threats can be detected in real-time regardless of where they occur.

5. **Centralised visibility delivering actionable insights**

   The biggest challenge in the cloud is the lack of insight into identities that have access to cloud resources, the privileges they have, any over-provisioned identities, and determining who the privileged users are and what they can access. To gain real-time insights, the team needs a single pane of glass through which to view and govern these IAM events over multi-cloud environments, e.g., AWS, GCP and Azure.

6. **Enforcement of least privilege across the entire cloud estate**

   Gaining an understanding of the privileges that are being used by identities but also the privileges that are not used is incredibly important to prevent privilege creep and compromised credentials. To apply IAM governance across the multi-cloud, teams need to manage identities (human and non-human) right-size their entitlements and continue to monitor proactively.

5 UNIFIED MULTI-CLOUD SECURITY MANAGEMENT

A practical approach to multi-cloud security needs to unify the strategy outlined by the four archetypes while addressing the security pain points. This can be achieved by using cloud-native technology to provide a central view of the cloud estate. Below is an overview of how our solutions provide this capability.

4DATA CLOUD SECURITY POSTURE ASSESSMENT

WHAT IS IT?

Instant one-off assessment of the cloud that improves visibility by itemising cloud assets, searching for instances of misconfiguration or non-compliance with industry standards.

WHAT DOES IT DO?

Performs an inventory of all cloud assets across AWS, GCP and Azure. Reports on misconfigurations and policy compliance with over 500 cloud best practices and reports on any violations and how to remediate these. Checks compliance with numerous security standards and regulations, including ISO 27001, CIS Benchmarks, NIST, FedRamp, GDPR, HIPAA, HITRUST and PCI DSS.

HOW DOES IT WORK?

The assessment is fully automated, agentless and uses an API to discover cloud metadata, evaluate conformance with compliance, and produce security and compliance reports. It uses a service account with read-only permissions to scan cloud configurations, and once the assessment is complete, the cloud account is deleted.

NEXT STEPS

Running the assessment provides the business with complete visibility across the multi-cloud and recommendations on how to resolve any issues, but it can also illustrate the value of running assessments on a more continuous basis to provide a more real-time understanding of security posture.

WHO IS IT FOR?

SOC Teams, Compliance teams

C3M CLOUD CONTROL

WHAT IS IT?

A cloud security platform that offers enterprises complete cloud control through actionable and contextual cloud security intelligence across AWS, GCP, and Azure. The platform is based upon CSPM but also Cloud Security Orchestration, Automation, and Response (Cloud SOAR), unifying cloud security operations and management.

WHAT DOES IT DO?

C3M Cloud Control provides cloud security assessment, compliance and enforcement and includes:

- Risk Score – Delivers a risk score for each alert, providing much needed context to help prioritise triage alerts and prevent alert fatigue. Three types of assessment are performed based on the NIST CVSS (Common Vulnerability Scoring System) framework and our proprietary policy risk score framework:
  - CVSS 3.1 Framework – using Exploitability, Impact and Scope criteria
  - Risk Impact Factors – 4Data proprietary intelligence framework with points based on attributes and risk factors of a resource with enterprises able to modify and adjust
  - Alert Severity – based on the severity of a policy defined in Cloud Control

The resultant risk score is rated between 1 and 10 and has four levels of Minor, Moderate, Major and Severe.

- Incident Response – Offers real-time incident response using Identity and Access Management (IAM) log ingestion. Combining the incident response capabilities with Playbooks means that security policies can be set up to trigger actions in the event of a violation of these rules. These actions can include the creation of an incident ticket, a push to SIEM tools, or automated remediation.

- Playbooks – Brings Cloud SOAR to the platform, helping to streamline security operations via a flexible, customisable, and extensible serverless framework that can support multiple remediations or actions across AWS, GCP, and Azure. SOAR allows security teams to speed up the investigation process, driving down MTTD, and help them to automate response and remediation.

HOW DOES IT WORK?

Completely API-based and agentless, C3M Cloud Control continuously monitors multi-cloud environments to identify and remediate security issues automatically.

WHO IS IT FOR?

SOC Teams, Compliance teams and auditors, IAM administrators, External auditors

C3M ACCESS CONTROL

WHAT IS IT?

A cloud identity and entitlements governance module that integrates with the Cloud Control platform, and that addresses IAM (Identity and Access Management) issues by providing a unified view of identities (human and non-human) i.e., users, entities, groups, permissions, trust relationships and helps to manage these by ensuring they have the right entitlements.

WHAT DOES IT DO?

Assesses, detects and prevents instances of misconfiguration, preventing privilege creep and the exploit of credentials by enforcing the concept of least privilege.

HOW DOES IT WORK?

Uses IAM best practices and the CARTA approach to discover create an inventory of identities, service accounts, users, roles and policies across the multi-cloud. Can create and rollout custom IAM governance policies.

Continuously analyses identities and their behaviours. Can carry out investigations and root cause analysis of IAM events. Generates risk reports, audit activity reports for identities and executive summary reports that give oversight of the state of security cloud-wide.

NEXT STEPS

Access control can automate incident response and remediation when used with Playbooks so many users naturally migrate to the C3M Cloud Control platform.

WHO IS IT FOR?

Compliance teams and auditors, IAM administrators, External auditors

MATRIX OF 4DATA CLOUD SOLUTIONS

ATTRIBUTES / C3M SOLUTION	CLOUD SECURITY POSTURE ASSESSMENT (SERVICE)	ACCESS CONTROL (PRODUCT)	CLOUD CONTROL (PRODUCT)
PILLAR	CIEM	CIEM	CSPM SOAR
WHAT IT DELIVERS	Oversight of cloud security risk posture	Governance over identity and entitlement	Simplifies and provides context-based cloud security assessment and compliance
KEY FEATURES	• Inventory of cloud assets • Cloud best practice reports • Compliance reports	• IAM governance Inventory of identities • Profiles and risk scores users • Custom policies • Detects and flags activity • Behaviour analysis • RCA • Reporting	• Risk Scoring based on the NIST standard (CVSS Framework) - considered an industry first. • Real-time threat detection and response • Playbooks
USP	One-off assessment that gives a complete instant view of the state of your security in the cloud	Deals with the issue of misconfiguration which is the number one cause of cloud security failures. Can cope with high log volumes. Uses the CARTA approach.	A unified approach to multi-cloud security issues

PRODUCT ROADMAP:

- A new CNAPP module (i.e., Infrastructure as a Code)
- A new cloud VRM module (Vendor Risk Management)
- A new CWPP module (Cloud Workload Protection Platform)

BENEFITS FROM A UNIFIED APPROACH

- Centralises multi-cloud security management
- Provides visibility of all cloud assets, identities, and entities
- Mitigates the risk of misconfiguration and privilege creep and associated exploits
- Makes it easier to create security policies, put in place policy guard rails and ensure compliance with security standards
- Ensures risks are assessed using wider context parameters and against the NIST CVSS framework to focus alert response
- Automates incident response and remediation
- Ongoing assessment of the security posture of the business resulting in compliance and executive reports

6 CONCLUSION

The move to the multi-cloud is well and truly underway. But as companies build out their presence, there's the risk of cloud sprawl as more entities are added, increasing the risk of misconfiguration and privilege creep. The volume of alerts also ramps up, swamping security teams who have no way to qualify them and determine which are false alarms and which should be investigated, nor a way to prioritise them. As a result, many businesses are expanding cloud operations with limited visibility and are relying for defence on a mismatch of point security solutions.

To operate securely within a multi-cloud environment, the business needs to adapt its security stance to focus on securing a perimeter defined by the applications rather than the infrastructure and one which uses a zero-trust approach. This requires native-cloud solutions that are dynamic and flexible enough to operate within the cloud and deliver real-time intelligence.

Cloud security solutions are now available that fulfil this remit and have been grouped by Gartner into four archetypes, but these still operate largely independently. Combining these elements into a unified, multi-cloud security product provides the business with better visibility, awareness and control over its data across platforms. It enables teams to monitor the security and to assess and respond to alerts based upon the risk level. Set policies and assess compliance with industry standards and regulations in real-time. And can be used to automate incident response and remediation.

4Data's multi-cloud solution provides you with a range of options to tackle multi-cloud security:

- Cloud Security Posture Assessment helps you get an immediate picture of your security posture and diagnose areas for attention.
- Cloud Control, our flagship CSPM platform, featuring Risk Scoring, which qualifies and prioritises alerts using best practice frameworks. Also included is Playbooks, our SOAR module for handling investigations. Playbooks helps you reduce the pressure on your security and compliance resources, helping secure your multi-cloud environment.
- Access Control, our CIEM module, tackles identity and entitlement management and helps to implement and maintain least privilege.

7 ABOUT US

4DATA SOLUTIONS

4Data's cloud security solutions address the challenges of managing multi-cloud environments via centralised solutions. Our Cloud Security Posture Assessment offering allows you to instantly conduct an assessment of your cloud security posture and gain actionable insights into how best to improve.

C3M Cloud Control is a 100% API-based, agentless cloud security platform that offers enterprises complete cloud control through actionable and contextual cloud security intelligence across AWS, GCP, and Azure. The platform combines CSPM, Cloud SOAR via our Playbooks functionality, and CIEM, unifying cloud security operations.

C3M Risk Score uses the CVSS risk scoring framework to provide you with context-based intelligence that can be used to prioritise alert handling.

C3M Access Control is a comprehensive identity and entitlement governance module that integrates with the Cloud Control platform, and provides a deep visibility into cloud entities and entitlements and helps mitigate the risks associated with privilege escalation, compromised credentials and suspicious access activity.

4data SOLUTIONS

If you'd like to know more about our multi-cloud security solutions please go to:

4datasolutions.com, call us on **+44 (0)330 128 9180** or email **info@4datasolutions.com**.

BR-011-V 1.0 04 NOVEMBER 2021