WELCOME TO

CLOUD ALPHABET SOUP - CNAPP

Alexei Balaganski
Lead Analyst & CTO | KuppingerCole

Mike Small
Senior Analyst | KuppingerCole

Audio Control

You are muted centrally. We are controlling these features. No need to mute or unmute yourself.

Polls

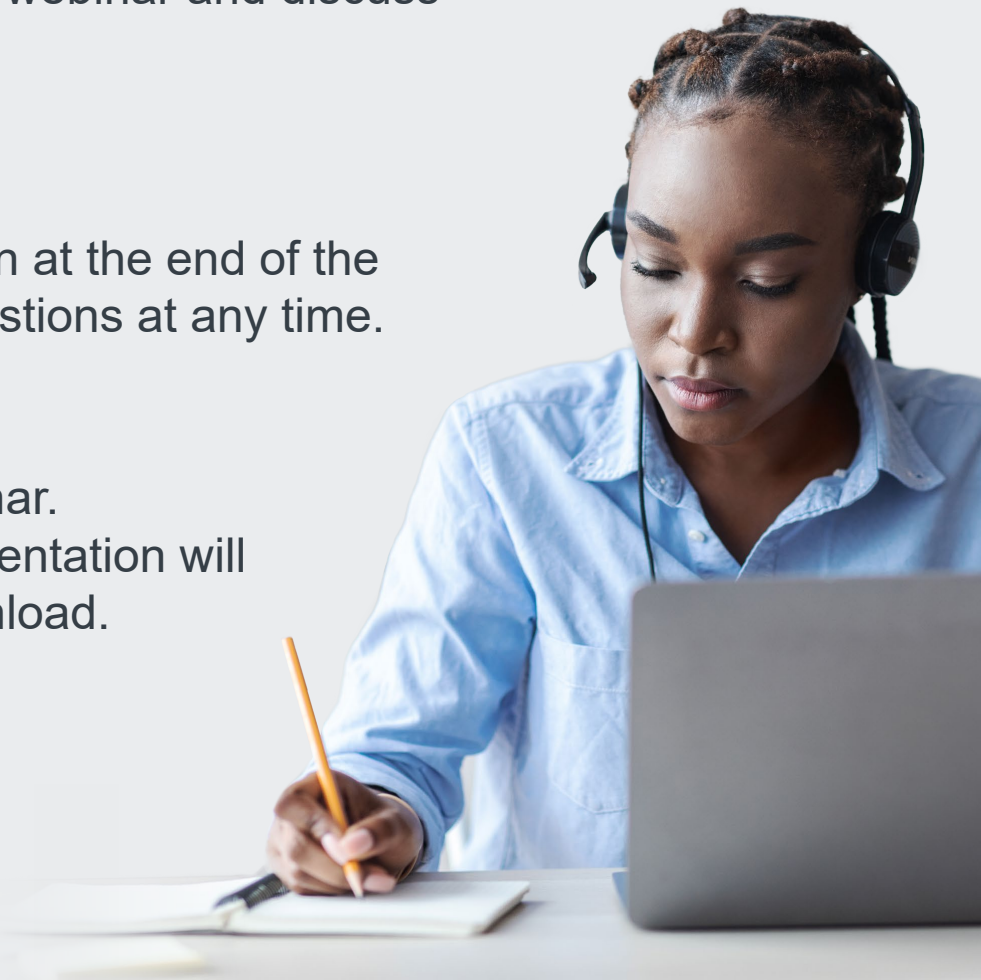
We will run polls during the webinar and discuss the results during Q&A.

Questions and Answers

There will be a Q&A session at the end of the webinar. You can enter questions at any time.

Recording and Slides

We are recording the webinar.
The recording and the presentation will be made available for download.



POLL #1

What is the biggest security challenge in your hybrid multi-cloud environment?

1. Understanding the real risks.
2. Complexity of the environment.
3. Managing the shared responsibilities for security.
4. Inconsistent tools and capabilities.
5. Lack of transparency of controls.

Digital Transformation

Using cloud services

Digital Transformation

Brings new risks that must be managed

IT as a Service

Agile

Enables rapid Business-Led Change
but creates volatile services, workloads and resources.

Flexible

DevOps approach is flexible to business needs and customer *feedback*
but creates new risks.

Responsive

Just in Time Resources - Servers, Storage and Services on demand
but create new management challenges.

Three Major Concerns

That must be managed

1

Compliance Failure

Didi Global fined $1.2 billion for data violations

2

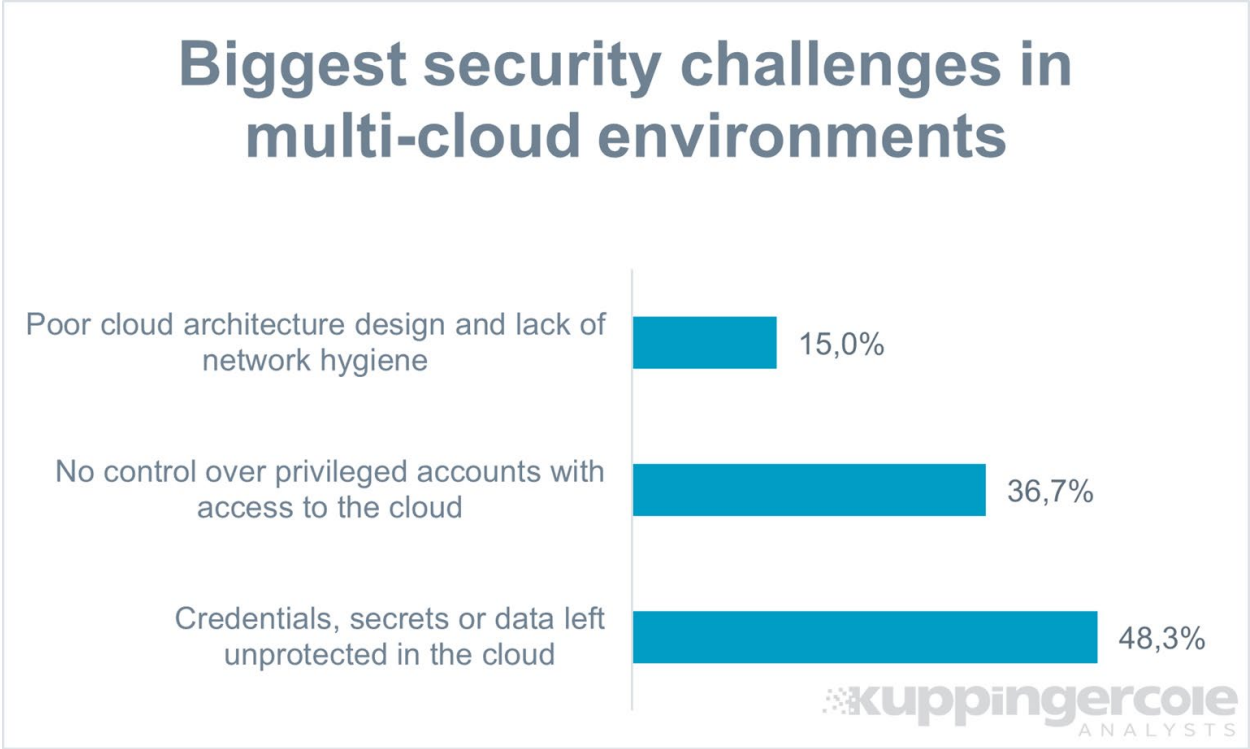
Data Breaches

More than 3.8 billion records exposed in DarkBeam data leak

3

Business Continuity

MGM Resorts reported a 36-hour outage due to the ransomware attack



Source: KuppingerCole Research

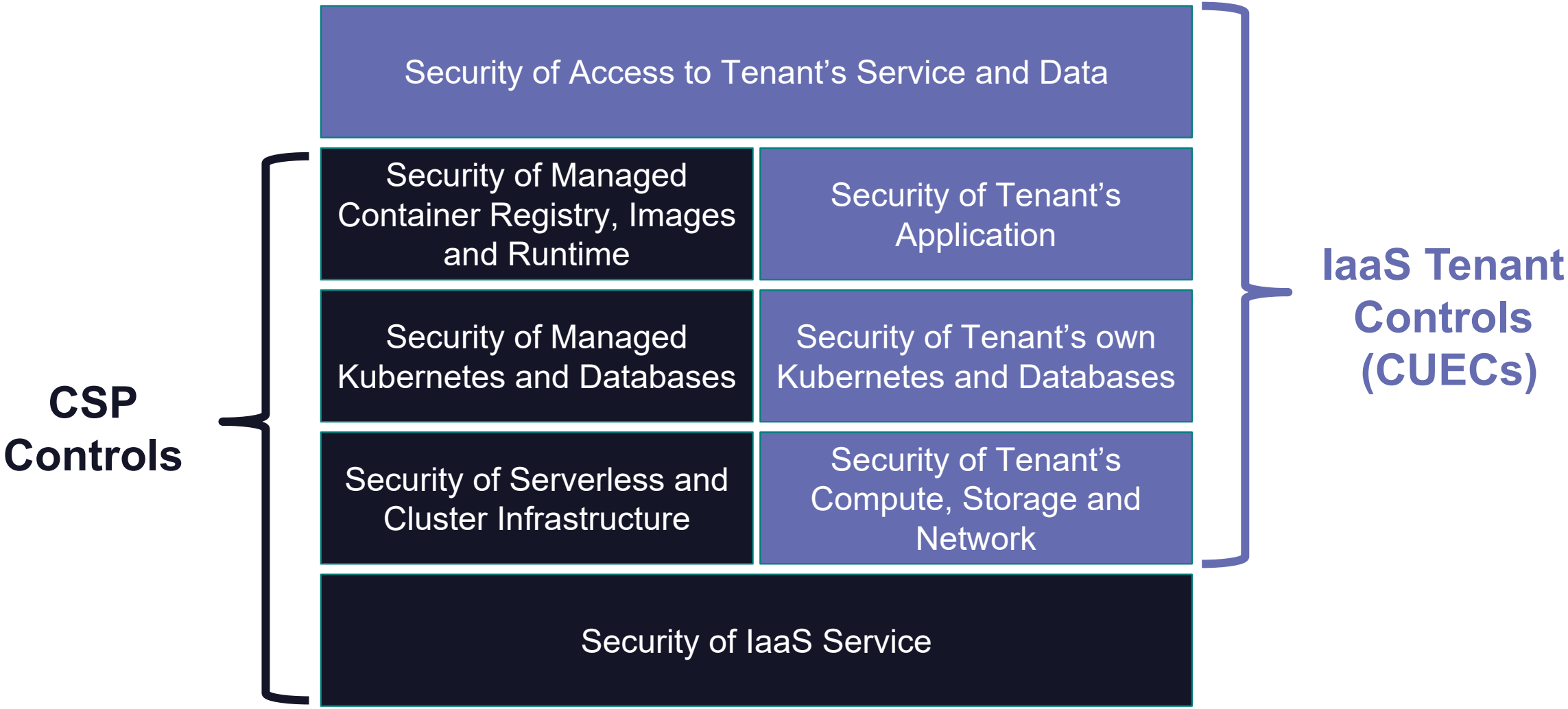
Challenges

From the multi-cloud hybrid IT service delivery

Challenge: Shared Responsibility

Can lead to confusion and poor security controls

Complementary User Entity Controls

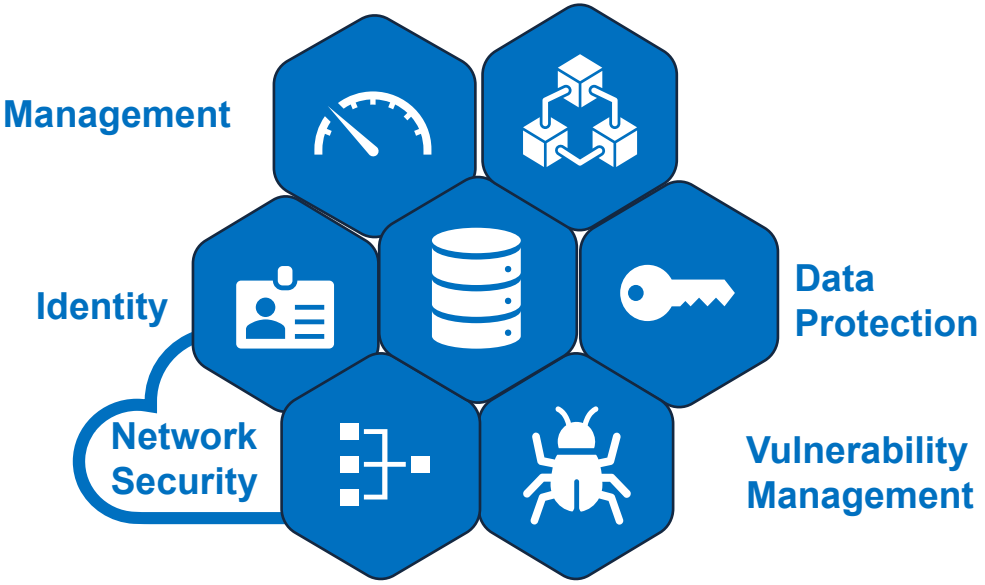


Challenge: Inconsistent Capabilities and Tools

Each cloud has own capabilities, tools, APIs and user interfaces

Ad Hoc Approach

To security and compliance



Challenge: Ephemeral Resources

Capital One Data Breach

1. **Misconfigured WAF**
   Relayed requests to a key back-end resource.

2. **Excessive privileges**
   The VM was assigned excessive privileges

3. **Used to Access S3**
   To list and read the files and buckets even when encrypted.

4. **$80M Fine**
   OCC fined and required risk management changes

10. After receiving this information, Capital One examined the GitHub file, which was timestamped April 21, 2019 (the "April 21 File"). Capital One determined that the April 21 File contained the IP address for a specific server. A firewall misconfiguration permitted commands to reach and be executed by that server, which enabled access to folders or buckets of data in Capital One's storage space at the Cloud Computing Company.

11. Capital One determined that the April 21 File contained code for three commands, as well as a list of more than 700 folders or buckets of data.

- Capital One determined that the first command, when executed, obtained security credentials for an account known as *****-WAF-Role that, in turn, enabled access to certain of Capital One's folders at the Cloud Computing Company.
- Capital One determined that the second command (the "List Buckets Command"), when executed, used the *****-WAF-Role account to list the names of folders or buckets of data in Capital One's storage space at the Cloud Computing Company.

Capital One Indictment US District Court Seattle

Cloud Acronym Soup

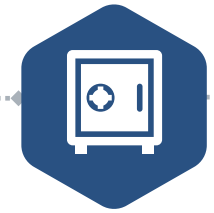
Siloed solutions cannot provide complete visibility and risk management

CIEM

- Control over cloud infrastructure elements
- Virtual Resources have entitlements
- These are invisible and can be misused
- Security and compliance

CWPP

- Protection of the DevOps cloud
- Virtual machines
- Container-based workloads
- Serverless cloud
- Proactive and runtime



CSPM

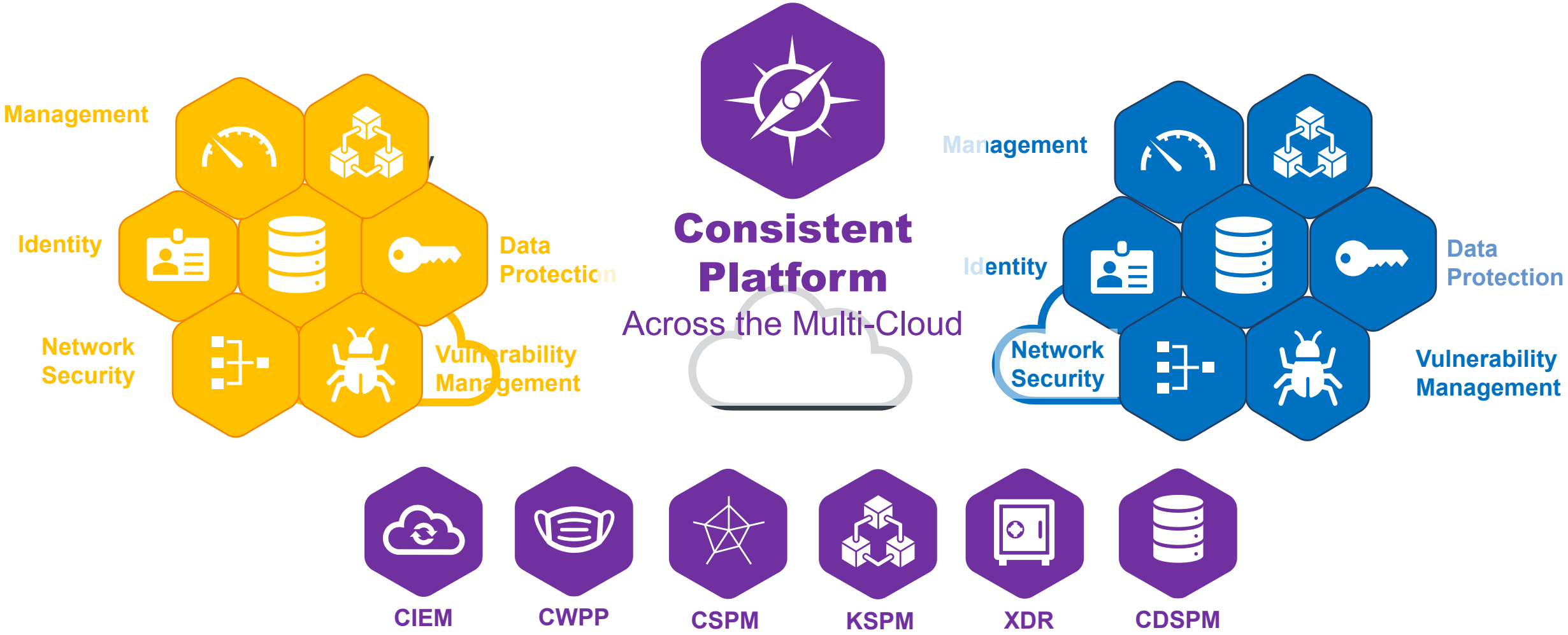
- Resource inventory
- Visibility
- Measurement
- Risk reporting
- Compliance

The Rest

- KSPM
- CDSPM
- CNSC
- CASB
- CXDR
- CASM
- Cloud SIEM/SOAR
- …

Desired Approach - Consistent Platform

For a mature approach to secure multi-cloud services



Cloud Native Application Protection Platform

What it is, how it works, key features and trends

Cloud Native Application Protection Platforms

Fundamental functionality of CNAPP solutions

01

Basic Capabilities

analyze and manage the risks of multi-cloud IaaS services' configuration and usage

02

Cloud Entitlements

discover and analyze cloud user accounts, rights, and risks

03

Cloud Storage Security

identify, report, and remediate risks of data storage services

04

Cloud Network Security

manage cloud network security controls to enforce Zero Trust principles

05

Cloud Compute Security

discover and remediate risky configurations of virtual machines and serverless

06

Cloud Container Security

Identify and remediate insecure container images, registries, and runtime deployments

07

Cloud Application Security

discover and report on cloud apps deployed, identify and remediate app-related risks

08

Cloud Posture Management

Monitor and visualize security and compliance state of cloud services

Cloud Entitlement Risks

Cloud Administrators and Cloud Infrastructure

Weak AuthN

Protect against account takeover:

- Weak authentication
- Compromised credentials
- Unused / orphan accounts

Excessive Rights

Limit scope of attack / misuse:

- Least privilege
- Separation of Duties
- Audit / Attestation

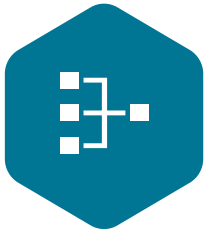
Infrastructure

Limit attack paths and technical exploits:

- Service elements
- Least privilege
- Activity monitoring

Cloud Network Risks

From virtual networks in the cloud services



Topology

Discover topology and control points:

- Range of Cloud Services
- AWS, Azure, Google, Oracle
- VMware, OpenStack, Hyper-V

Configuration

Risks related to control point configurations:

- Routing vs Policy
- Protocols vs Policy
- Zero Trust

Certificates

Risks related to the Certificate management

- Self-signed Certificates
- Weak encryption
- Certificate Root

Cloud Compute Service Risks

Virtual Servers in the cloud service

Virtual Servers

Cover Native Virtual Sever types for:

- Range of Cloud Services
- AWS, Azure, Google, Oracle
- VMware, OpenStack, Hyper-V

Entitlements

Risks related to VM entitlements:

- Excessive privileges.
- Without an owner
- Dormant / not used

OS Config

Risks related to the OS set up:

- Known CVEs
- Missing Patches
- Root enabled

Cloud Container Risks

Kubernetes within the cloud service

Registry

Kubernetes Registry:

- Discovery and visibility
- Access controls
- Lifecycle audit
- Transport security

Image

Risk related to images and their deployment:

- OS Images
- 3rd Party Packages
- Code scanning
- Container Drift

Runtime

Container runtime risks:

- Discovery and visibility
- Threat detection
- Behavior analysis
- Risk ranking

Security and Compliance Posture

Provide visibility and focus

Financial Impact

The potential financial impact of the risk

Risk Score

A configurable score for the risk

Categories

Risk described in categories (High, Medium, Low)

Laws / Regulations

With predefined policies out of the box (e.g., GDPR, HIPAA, TISAX, PCI/DSS)

Frameworks

With policies provided out of the box (e.g., ISO 27001, COBIT)

Best Practices

With policies out of the box (e.g., NIST, MITRE, CIS)

KuppingerCole Leadership Compass

Cloud Native Application Protection Platforms

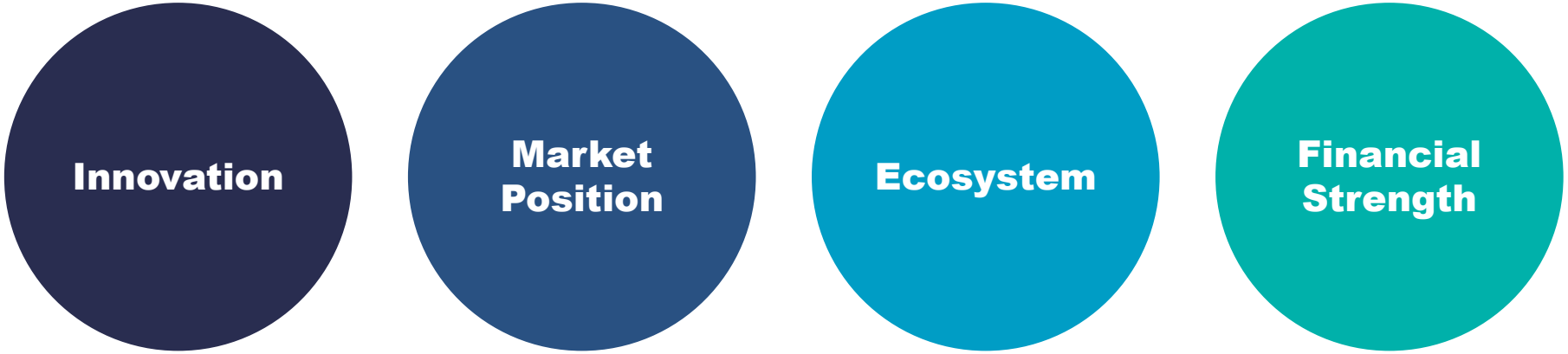
Leadership Compass Dimensions

Product-related categories that are evaluated in a Leadership Compass

Security	Function-ality	Integration	Interoper-ability	Usability
Does the product meet the security requirements of today?	Is the product feature complete?	Is it delivered as an integrated offering? Easy to deploy?	Does it work well with other services?	Is it easy for admins and analysts to use?

Leadership Compass Dimensions

Vendor-related categories evaluated in a Leadership Compass



Does the product deliver new features that customers need? Is it leading edge, or playing catch-up to others?

How many customers have deployed the product? Which industries are targeted? Which regions of the world are using it?

How many partners, ISVs, VARs, and support personnel does the vendor have, and how globally distributed are they?

Is the company profitable? Backed by venture capital? New startup or a veteran? Ready for the future?

Categories of Leadership

Analysis of combined dimensions show the strong performers

01

Product Leadership

Functionality and completeness of product vision

02

Market Leadership

Number and geographic distribution of customers, partners, and support ecosystem

03

Innovation Leadership

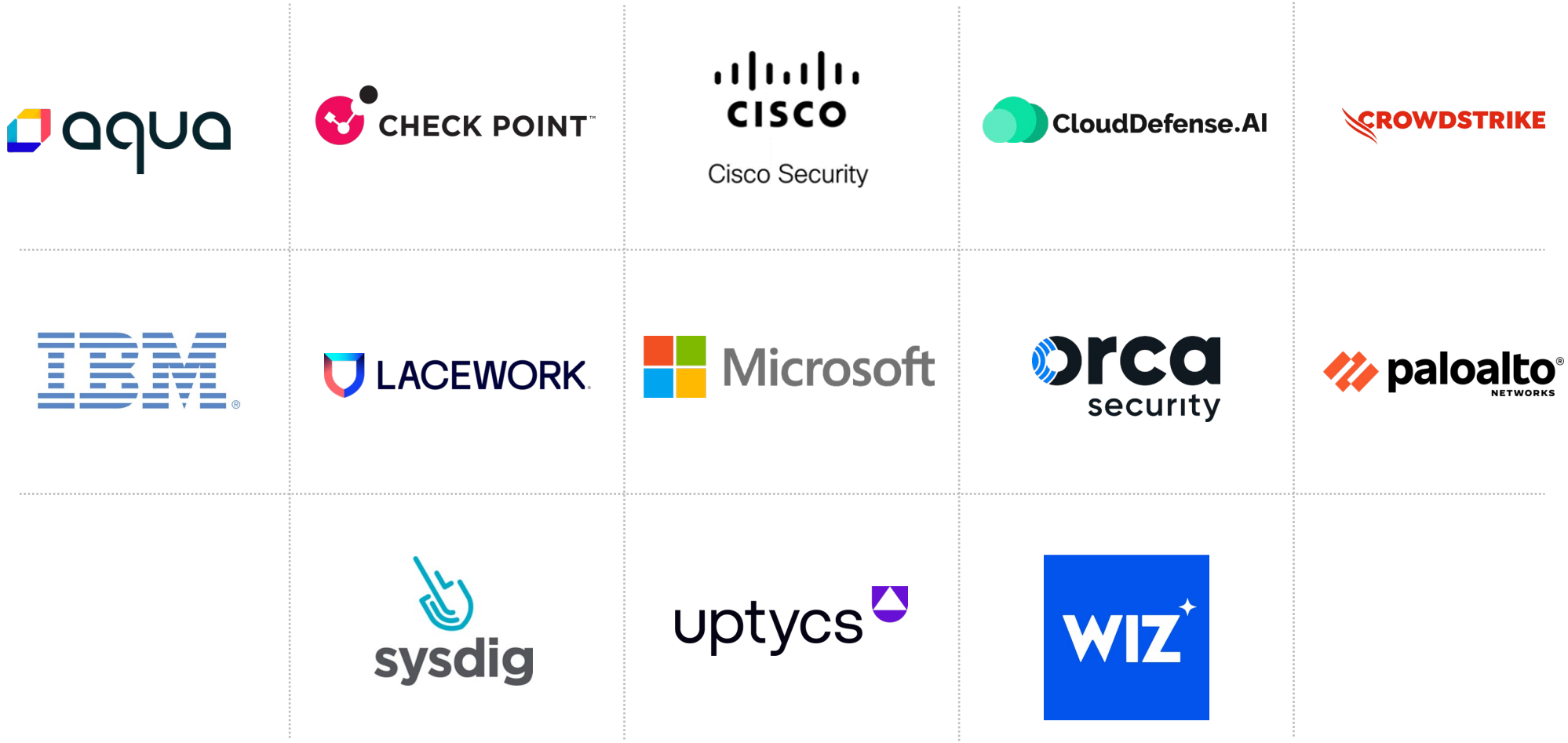
Delivering new and useful features at customer request

04

Overall Leadership

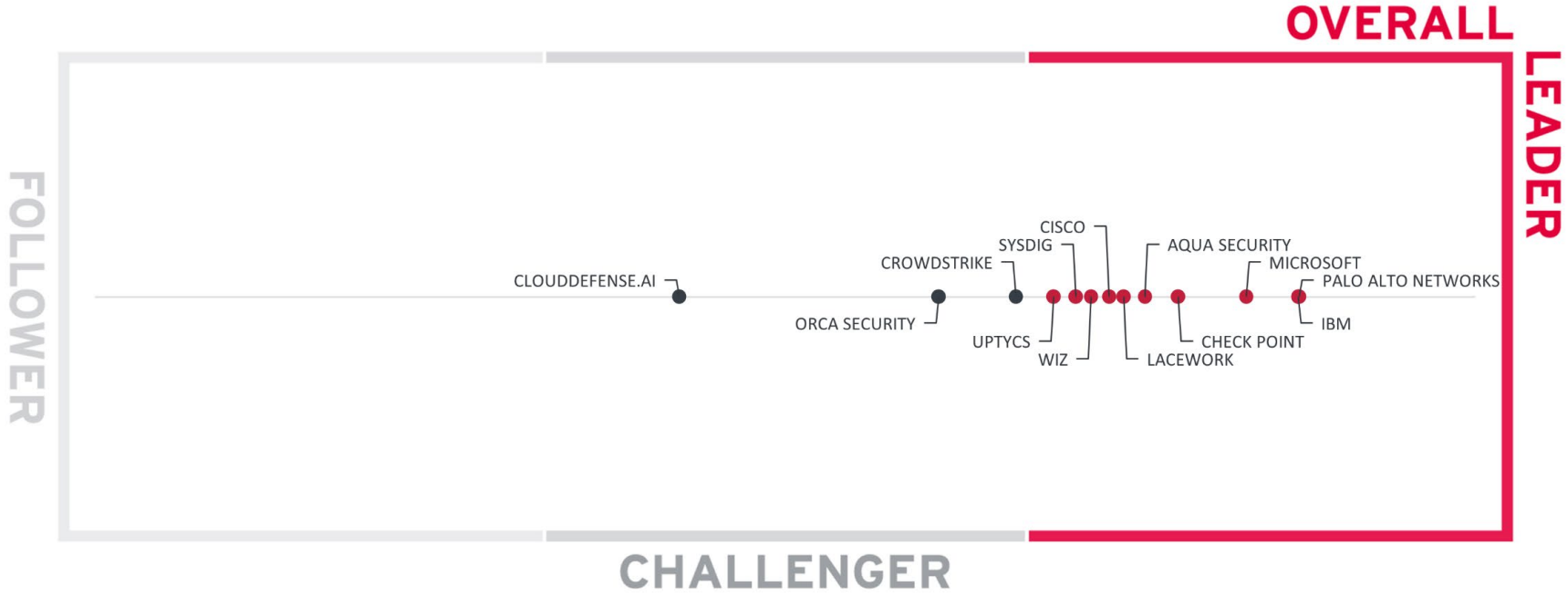
Vendors rated

Companies profiled in this Leadership Compass



Leadership Compass

Cloud Native Application Protection Platforms

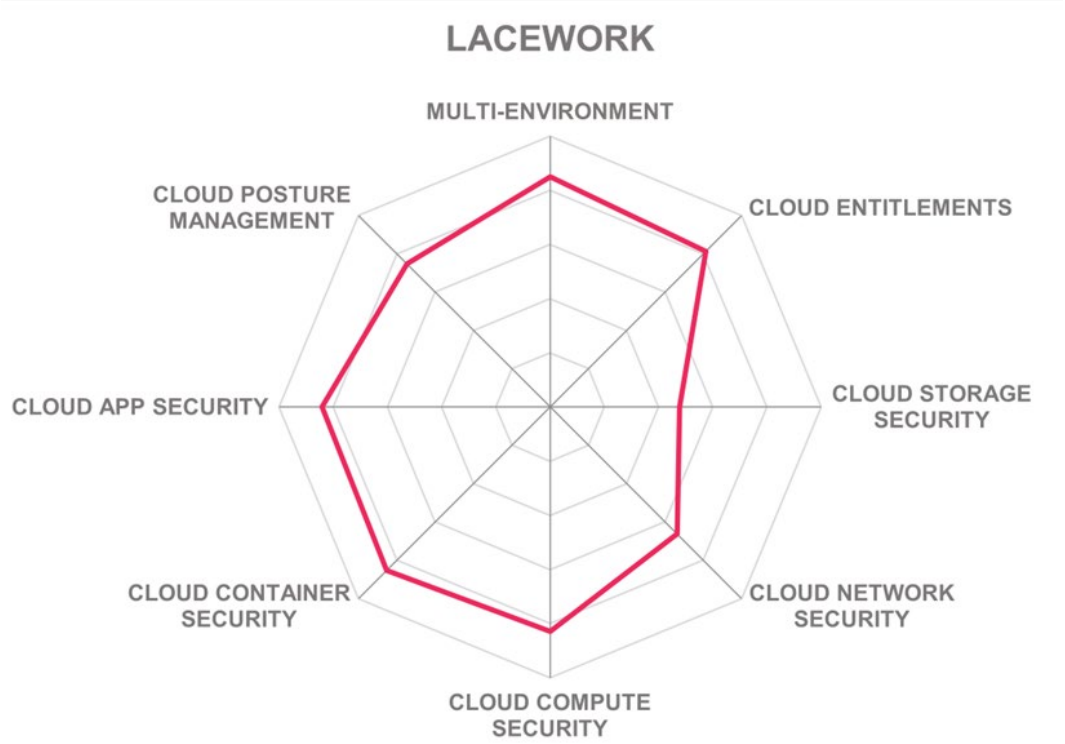


Sample vendor details

Strengths, challenges, capability scores

- Unifies code and cloud security with native software composition analysis (SCA), software bill of material (SBOM), Static Application Security Testing (SAST) and Infrastructure as Code (IaC) scanning.
- Polygraph provides rapid detection of potentially risky activities based on behavioral baseline of normal operations for cloud workloads.
- Attack path analysis capabilities assess risks based on internet path exposure, vulnerabilities, misconfigurations, exposed secrets, and privileged access.

- No risk detection for the configuration of virtual network routing control points such as firewalls.
- Does not detect missing / inoperative anti-malware on servers.
- Cannot identify risks related to poor certificate management.



Vendors to watch

Companies mentioned but not rated

POLL #2

How would you describe your organization's current stage of CNAPP adoption?

1. Fully adopted – all or most of our cloud-native apps are protected using CNAPP.
2. Partial adoption – we've started using CNAPP for some apps but not all.
3. Still evaluating – we're looking into CNAPP solutions but haven't implemented yet.
4. Not considering – we rely on other security methods and aren't currently considering CNAPP.

Summary

Dynamic infrastructure and DevOps need Dynamic Controls and Governance

Digitalization increases Cyber Risks

- Business Continuity
- Data Breaches
- Compliance failure

Cloud Security Challenges

- Shared Responsibility
- Dynamic resources
- Every cloud has its own tooling

Cloud Acronym Soup

- Siloed solutions
- Inconsistencies
- Ad hoc governance

Cloud Security Platform

- Complete and Comprehensive
- Dynamic guardrails
- Best practices and compliance

The Choice is Yours

Discover and Compare Cybersecurity Solutions for Free

Optimize your decision-making process, configure your individual requirements to find the right vendor.

Related Research

Relevant publications by KuppingerCole Analysts

Cloud Native Application Protection Platforms (CNAPP)
Leadership Compass | Read here

Analyst Chat #192: Exploring Cloud Security Posture Management (CSPM)
Podcast | Watch here

Cloud Security
Guide | Read here

Cloud Security Posture Management Tools – What They Are and Why You Need One
Blog | Read here

KuppingerCole Analysts AG
Wilhelmstr. 20 - 22
65185 Wiesbaden | GERMANY

P: +49 | 211 - 23 70 77 - 0
F: +49 | 211 - 23 70 77 – 11

info@kuppingercole.com
www.kuppingercole.com