

SUPPORTED BY



WELCOME TO

Cloud Early Warning Systems

From CSPM to CNAPP

Mike Small

Senior Analyst | KuppingerCole

Andre Rall

Director of Cloud Security | Uptycs



Agenda

Why cloud services need dynamic rather than static controls.

Mike Small KuppingerCole

02

Benefits of using a single platform, data model, and user interface.

Andre Rall Uptycs

03

Q&A



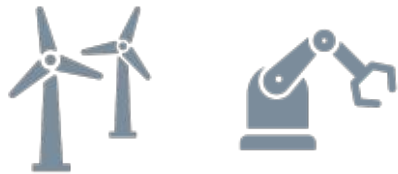
Digital Transformation

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

Fined \$80M for hack that exposed 100 Million accounts

2

Data Breaches

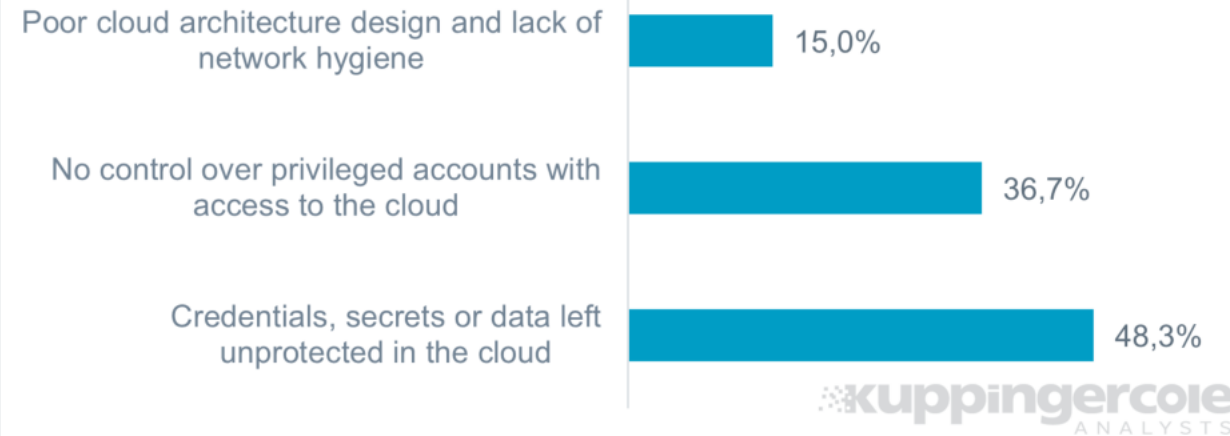
Fined £20m by UK (ICO) for a data breach affecting 400,000 customers.

3

Business Continuity

REvil set the price of a universal decryptor at \$70 million

Biggest security challenges in multi-cloud environments



Source: KuppingerCole Research

Challenge Infrastructure as Code

Capital One Data Breach 2019

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

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

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

- 16 ■ Capital One determined that the first command, when executed,
17 obtained security credentials for an account known as *****-WAF-Role
18 that, in turn, enabled access to certain of Capital One’s folders at the
19 Cloud Computing Company.
- 20 ■ Capital One determined that the second command (the “List Buckets
21 Command”), when executed, used the *****-WAF-Role account to list
22 the names of folders or buckets of data in Capital One’s storage space at
23 the Cloud Computing Company.

Capital One Indictment US District Court Seattle

Challenges

From the multi-cloud hybrid IT service delivery

Challenge: Shared Responsibility

Can lead to confusion and poor security controls



Access

To your services and your data.



Application

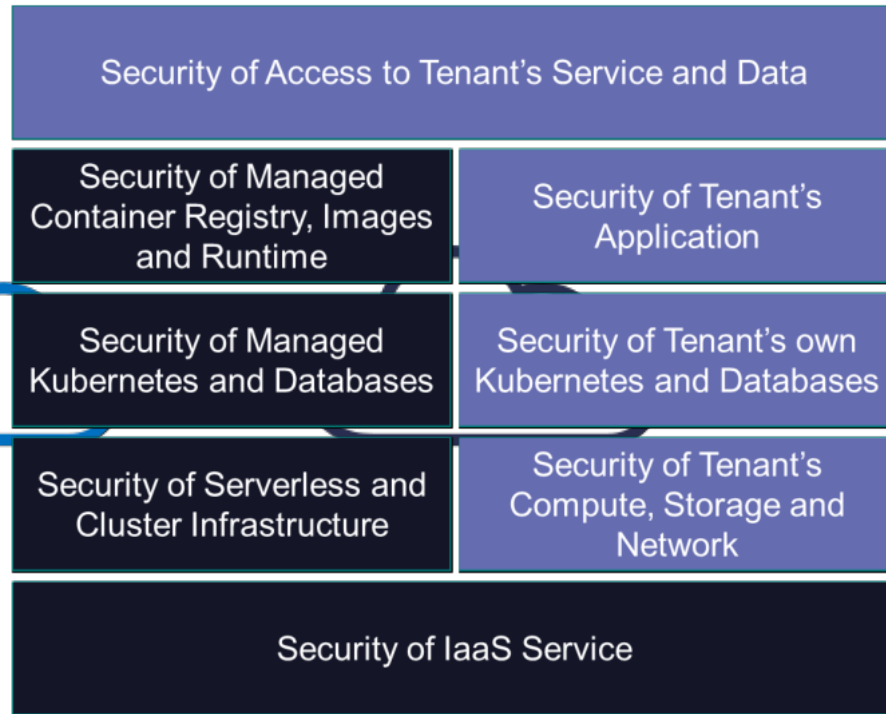
Your applications, code, configuration and deployment.



Virtual Services

Your Compute, Storage and Networks.

IaaS Tenant Responsible



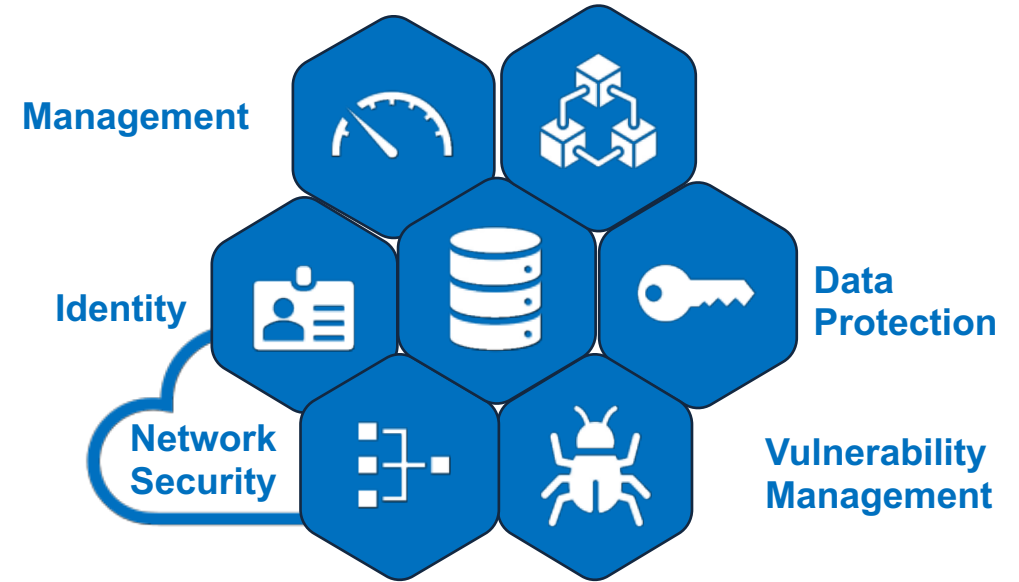
CSP Responsible

Challenge: Inconsistent Capabilities and Tools

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



Ad Hoc Approach
To security and compliance



Cloud Acronym Soup

Siloed solutions don't meet the challenge



CIEM

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

CWPP

- Protection of the DevOps cloud
- Container based workloads
- Serverless cloud
- Visibility and Control
- Over VMs, Containers and Serverless



XDR

- Threat Detection
- Block and remediate
- Incident Response
- Security Hygiene
- Vulnerability Management.

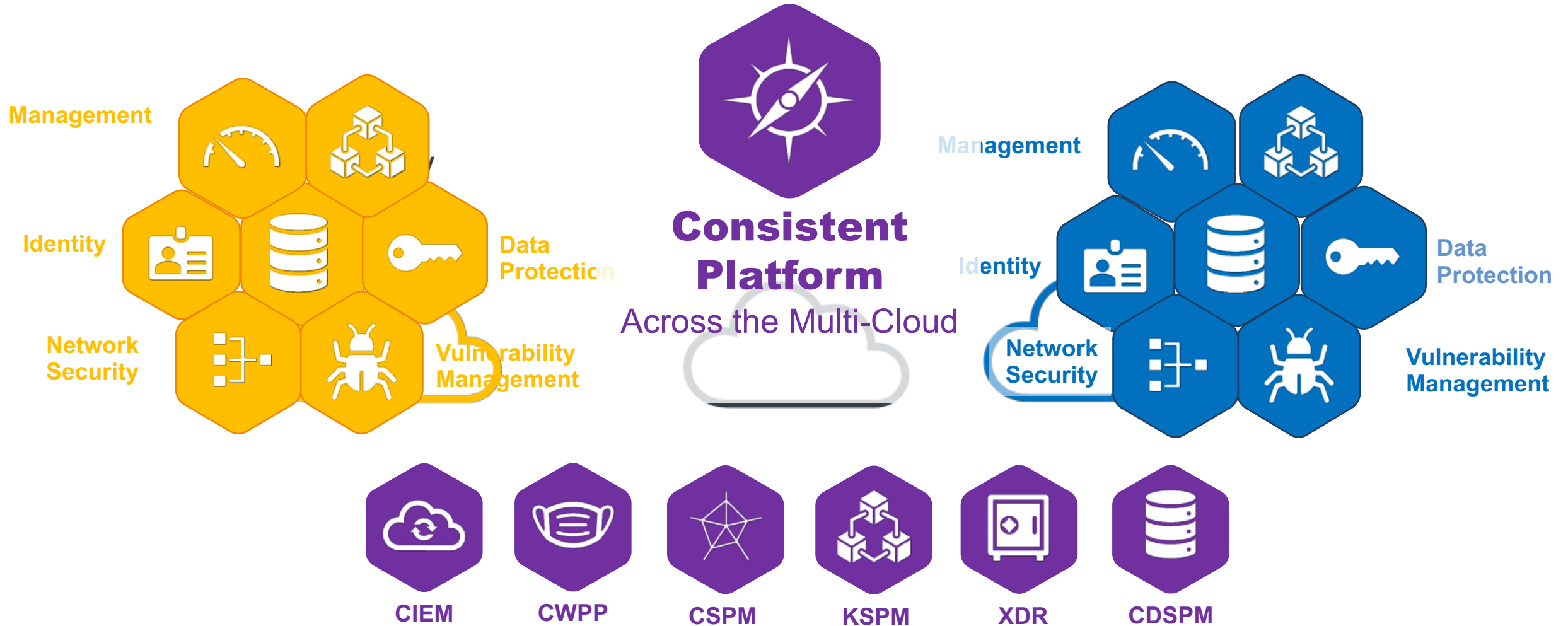
CSPM

- Inventory
- Visibility
- Measurement
- Risk reporting
- Compliance



Desired Approach - Consistent Platform

For a mature approach to secure multi-cloud services



Cloud Security Platform

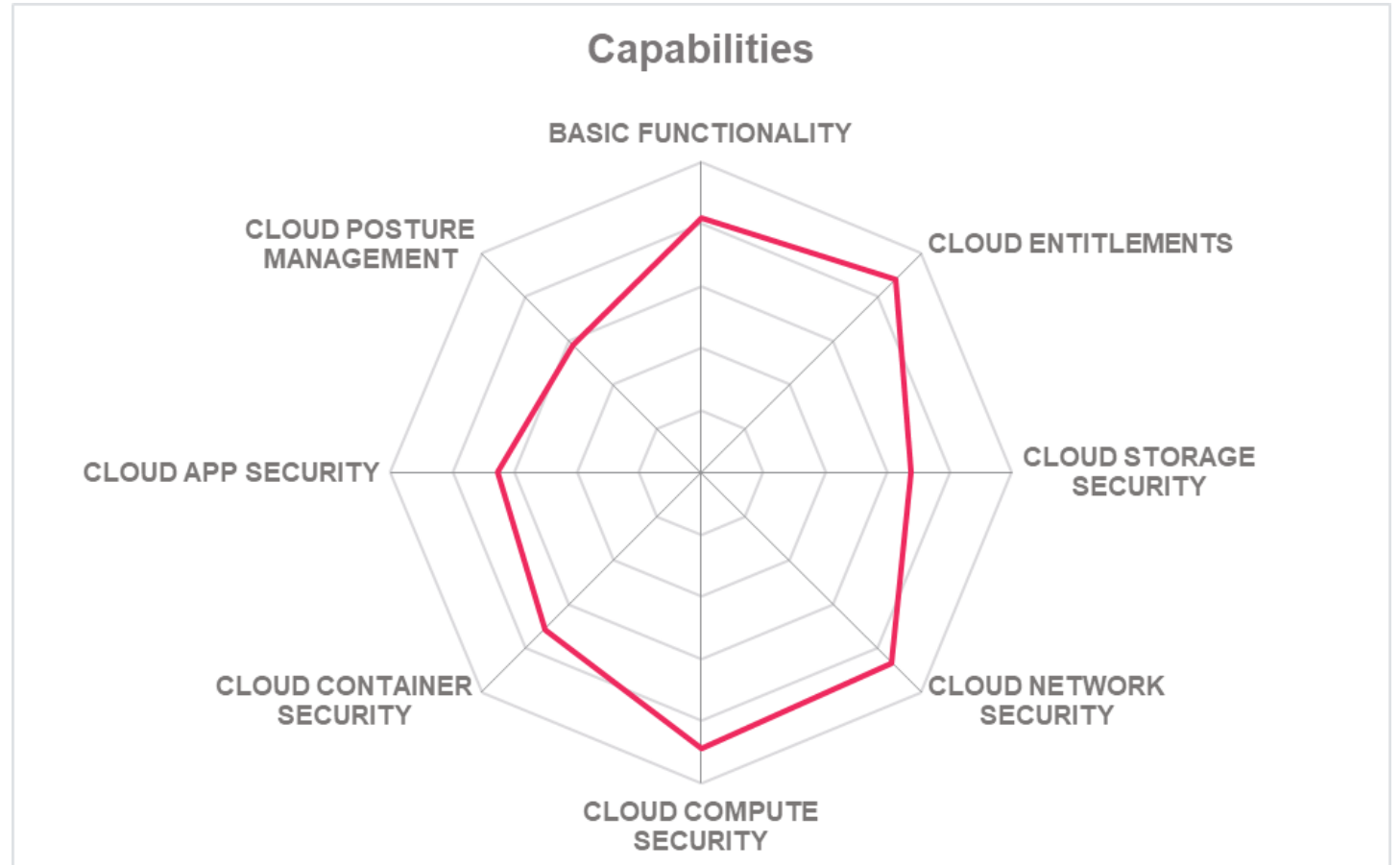
What are the capabilities to look for?

Cloud Security Platform

What a Cloud Security Platform should offer

Eight Major Areas:

- Basic functionality
- Cloud Entitlements
- Cloud Storage Security
- Cloud Network Security
- Cloud Compute Security
- Cloud Container Security
- Cloud App Security
- Cloud Posture Management



Basic Capabilities

For Cloud Security Posture Management

Inventory

Of what needs to be governed:

- Services
- Service elements
- In use and owned

Visibility

Of security and compliance of cloud assets:

- Against Policy
- Against best practices
- Against regulations

Control

Policy based controls for cloud assets:

- Enforce
- Remediate
- Report

Cloud Entitlement Risks

Cloud Administrators and Cloud Infrastructure



Weak AuthN

Protect against account takeover:

- Weak authentication
- Compromised credentials
- Unused / orphan accounts.

Excessive Privilege

Limit scope of attack / misuse:

- Least privilege
- Separation of Duties
- Audit / Attestation

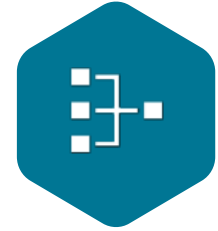
Infrastructure

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 Security

Virtual Servers in the cloud service



Virtual Servers

Cover Native Virtual Server 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

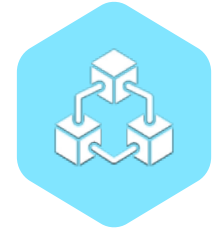
OS Config

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

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

Best Practices

Best practices with policies out of the box. (e.g., NIST, MITRE, CIS)

From CSPM to CNAPP

Security and Compliance for the multi-cloud

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
- Support best practices and compliance





Agenda

Why cloud services need dynamic rather than static controls.

Mike Small KuppingerCole

02

Benefits of using a single platform, data model, and user interface.

Andre Rall Uptycs

03

Q&A

Uptycs Unified CNAPP and XDR

Shift up security

Andre Rall
Director of Cloud Security

uptycs 

By the numbers...Cloud Adoption

94% of enterprises use cloud services.

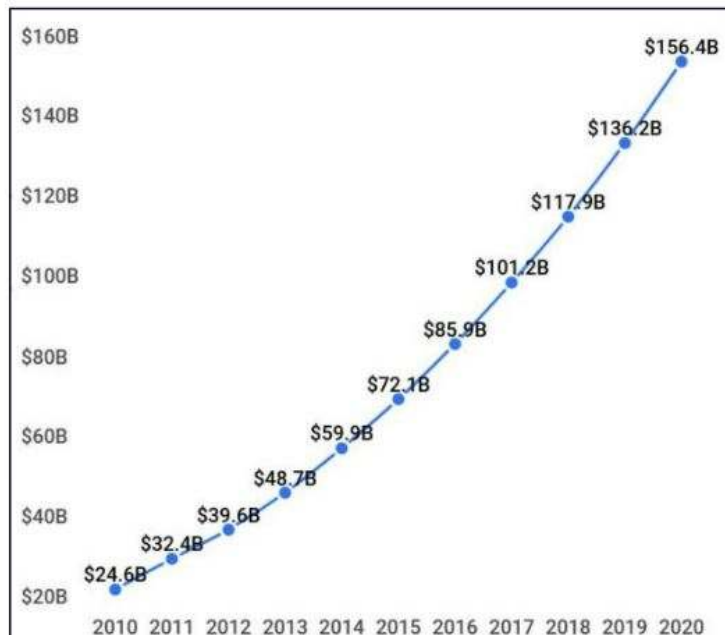
67% of enterprise infrastructure is now cloud-based.

\$90 billion - U.S. cloud spending reached by the end 2022 (27.8% growth compared to 2021).

61% of businesses migrationed their workload to the cloud in 2020 alone.

Estimated 175 zettabytes of stored data on the cloud by 2025 (a 61% increase from today).

\$947.3 billion by 2026! Global cloud market expecting CAGR of 16.3% through 2026



Global Cloud Computing & Hosting Market Size Over Time

By the numbers...Cloud Attacks

45%

of global respondents said they have experienced a data breach at some point.

19%

of respondents said they know where all of their data is stored.

32%

of respondents reported having to issue a breach notification to a government agency, customers, partners or employees.

Threat actors are now cloud security experts

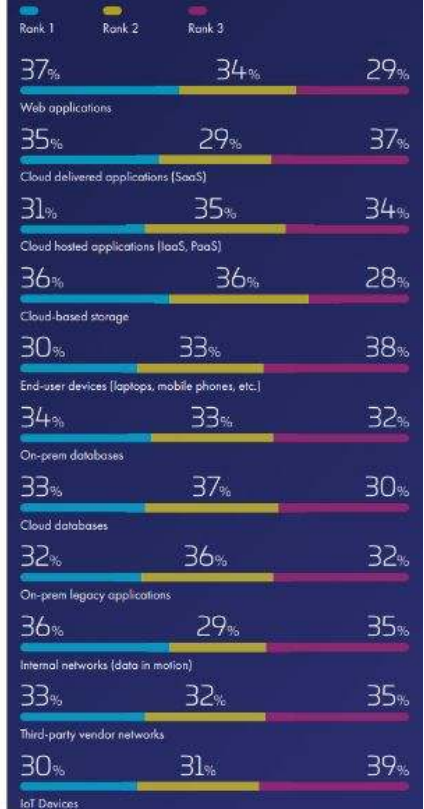


Source: 2022 Thales Cloud Security Report, conducted by 451 Research, part of S&P Global Market Intelligence

Primary Perceived Targets for Cyberattacks

IN GENERAL, HOW DO YOU RANK THE FOLLOWING AS TARGETS FOR CYBERATTACKS?

RANK 3 IN ORDER OF PRIORITY



Assume breach!

CYBERSCOOP

Topics ▾ Special Reports Events Podcasts Videos Insights

CYBERCRIME

Cybercrime groups offer six-figure salaries, bonuses, paid time off to attract talent on dark web

Despite the obvious risks, tech jobs with hacking groups can be alluring for those who need the money or want to do the work.

BY AJ VICENS • JANUARY 30, 2023

DARKREADING

The Edge

DR Tech

Sections ↻

Events ↻

Cloud | ⌚ 8 MIN READ | 📖 PRODUCTS & RELEASES

Cloud Security Market Worth \$62.9B by 2028

August 04, 2023

DARKReading

The Edge

DR Tech

Sections ↻

Events ↻

Cloud | ⌚ 4 MIN READ | 📖 COMMENTARY

How the Cloud Is Shifting CISO Priorities

The greatly expanding attack surface created by the cloud needs to be protected.



Shai Morag
CEO, Ermetic

February 03, 2023

THE NEW STACK

PODCASTS EBOOKS EVENTS NEWSLETTER

ARCHITECTURE ENGINEERING OPERATIONS

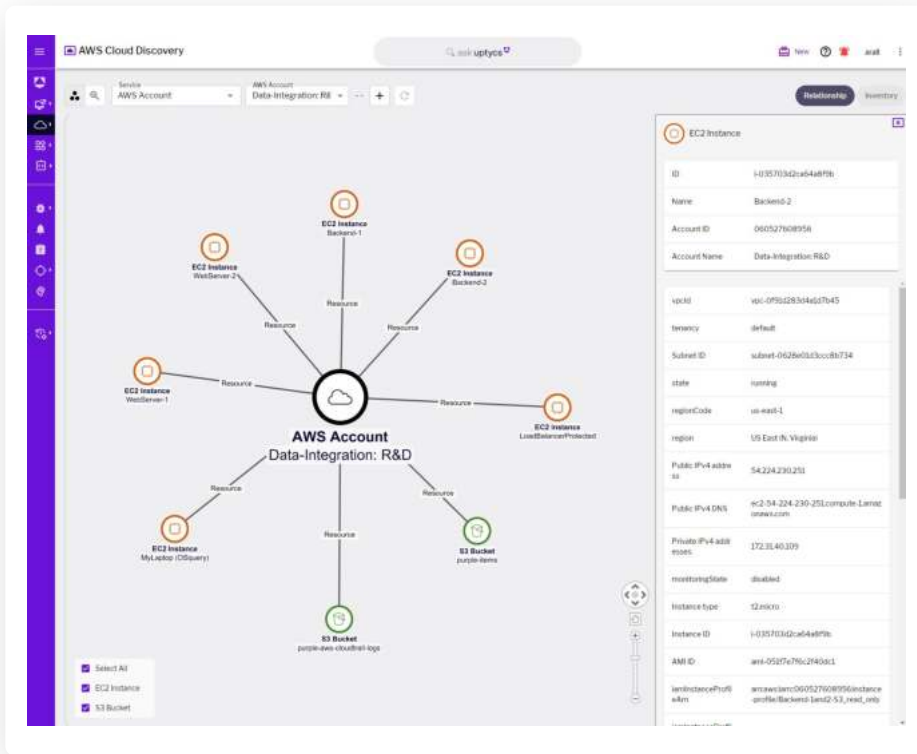
CULTURE / SECURITY / SOFTWARE DEVELOPMENT

Watch Out, Attackers Have Their Heads in Your Cloud!

Security teams need an adversary-focused approach — understanding hackers, their mindset, tools and techniques — that automates security controls

Feb 2nd, 2023 12:29pm by David Pizias

What outcomes does a CSPM deliver?



- Asset discovery & configurations
- Securing your posture
- Compliance in the cloud

Risk assessment

= CSPM

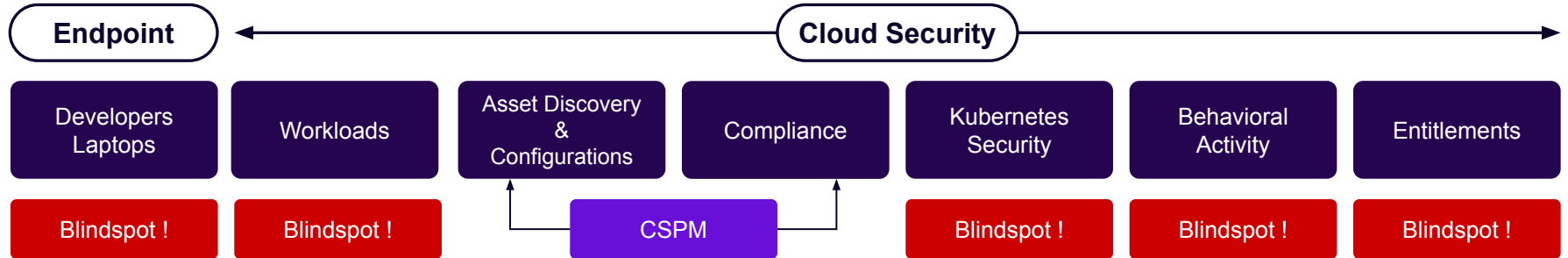
Why CSPM is not enough: Holistic view

› Threat actors don't think in silos

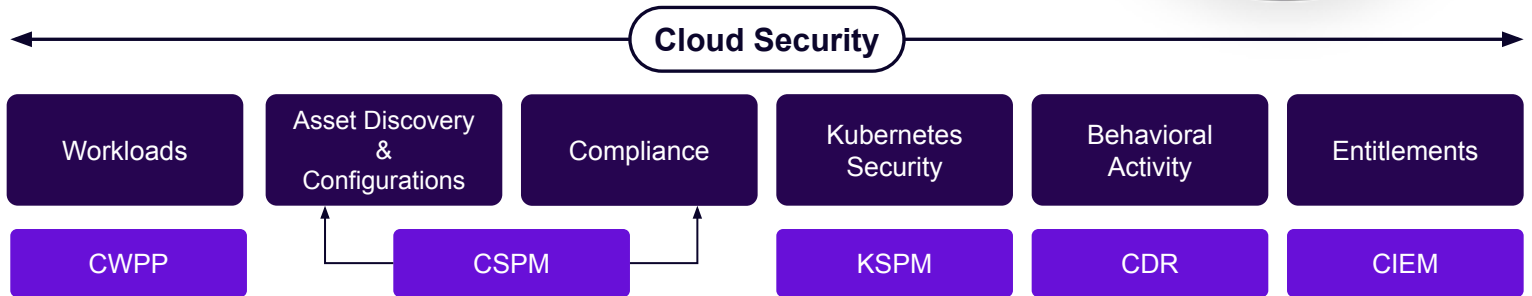
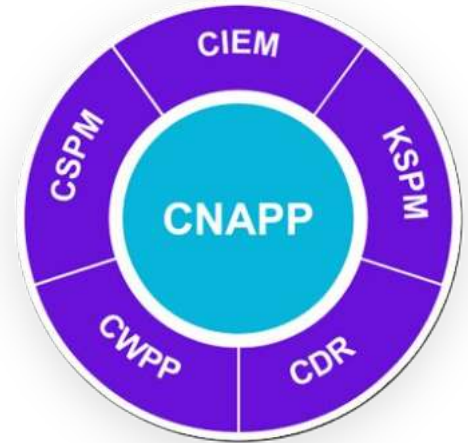
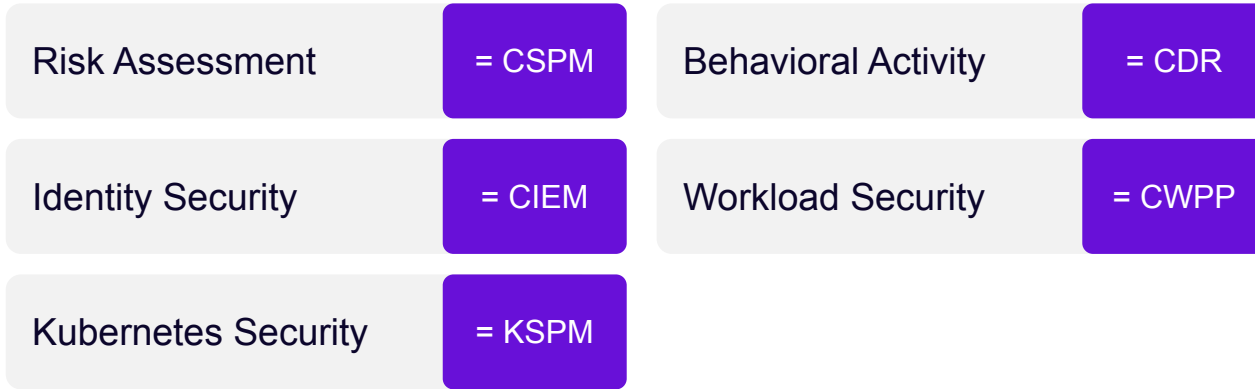
› Interconnected cloud services

› Threat landscape has expanded

› Cloud Native Protection Platform (CNAPP) is becoming a standard

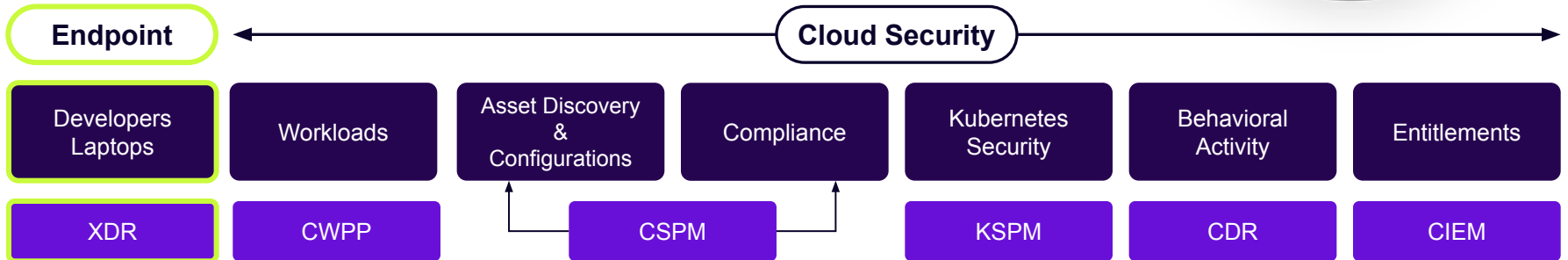
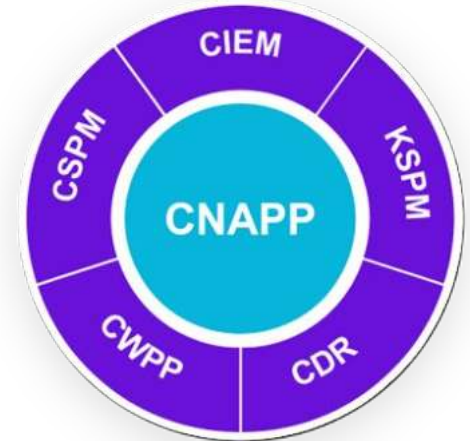


What is a CNAPP?

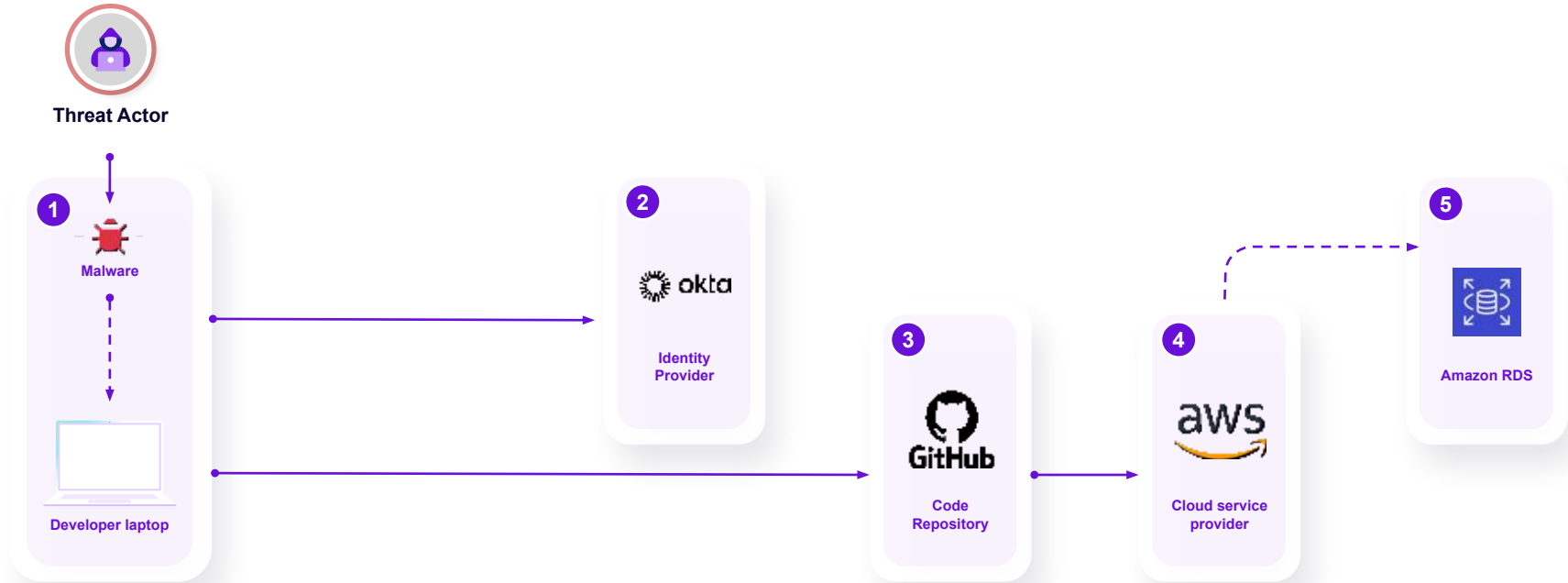


CNAPP also needs to include developer workspaces

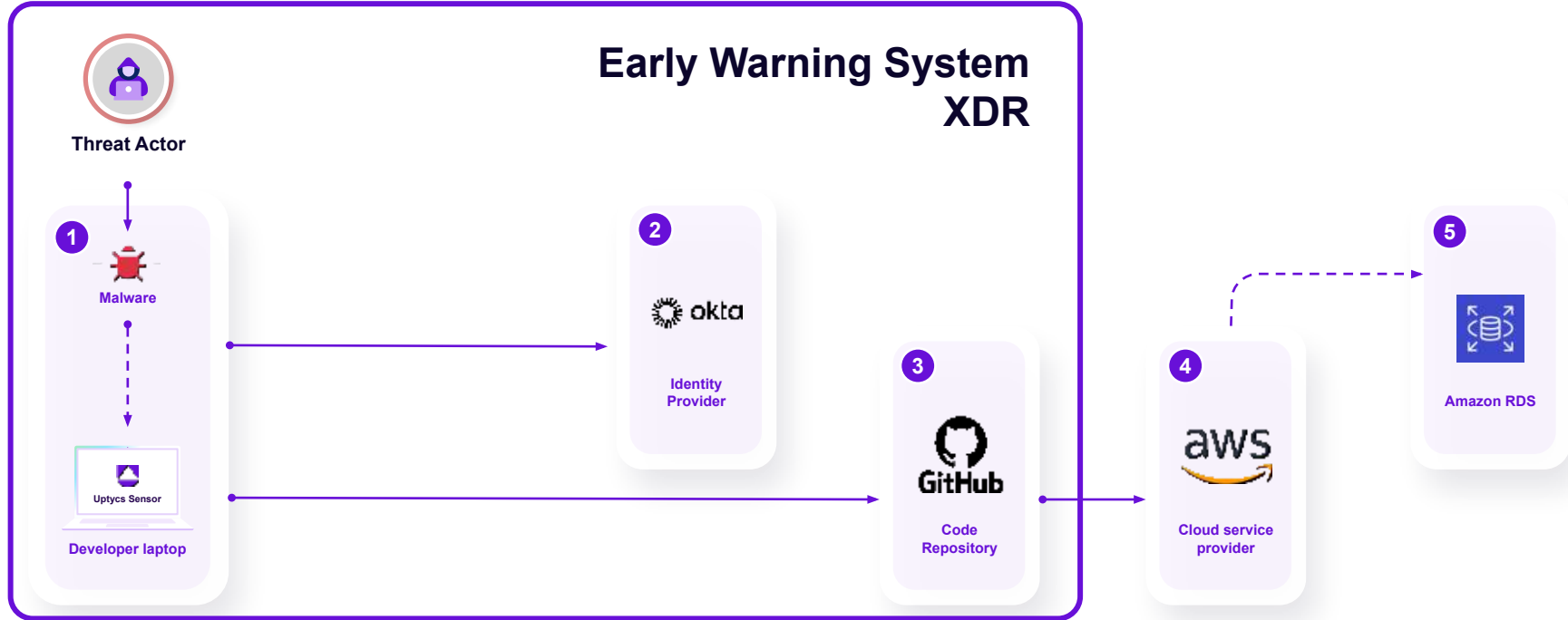
Risk Assessment	= CSPM	Behavioral Activity	= CDR
Identity Security	= CIEM	Workload Security	= CWPP
Kubernetes Security	= KSPM	Dev. Workspace Sec.	= XDR



Major breaches often start with the developer's laptop



Protect the developer environment that connects to your cloud



Example Warning: Impossible Travel

The screenshot shows the Uptycs Unified Detection Dashboard. The page title is "Unified Detection Dashboard" and the URL is "protectum.uptycs.io/ui/customdashboards/37e4d788-704e-4cd7-9d40-77704e53a39c". The dashboard displays a "Suspicious git event - Anomalous location" with 2 rows of data. A red arrow points to the "Country" column, highlighting the transition from "IN" to "US" within a short time period, which is an impossible travel warning.

Detectedtime	Username	Organization	Repo	Ippaddress	Country	Session time	Hashedtoken	Isr
2023-04-20 13:01:15.0	wolverine-1974	cloud-exile	cloud-exile/aws-dev-jenkins	[REDACTED]	IN	2023-04-20 13:01:15.0	b68hPUhbGkznwLvd1tZ0J	fal
2023-04-20 13:31:48.0	wolverine-1974	cloud-exile	cloud-exile/aws-dev-jenkins	[REDACTED]	US	2023-04-20 13:31:48.0	b68hPUhbGkznwLvd1tZ0J	fal

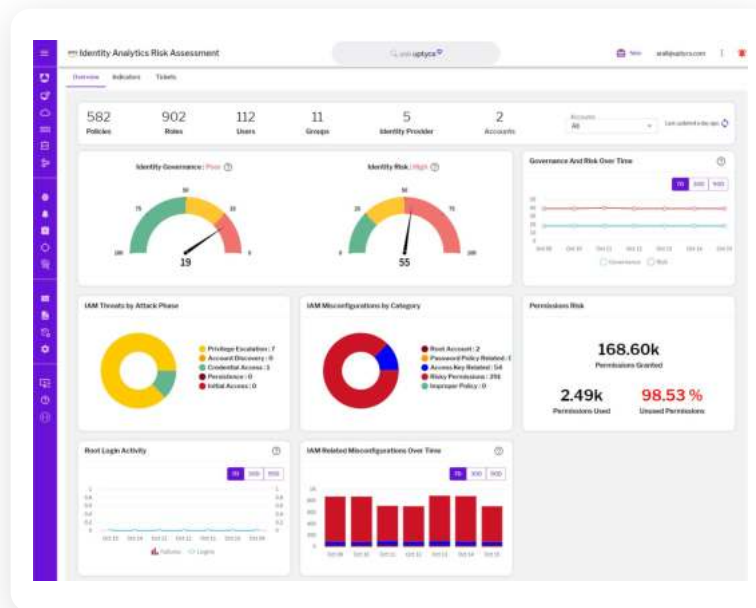
Early warning system: CIEM (Identity Security)

Example Warning 1:

User has full administrator privileges

Example Warning 2:

Unused entitlements



CSPM

CIEM

KSPM

CWPP

CDR

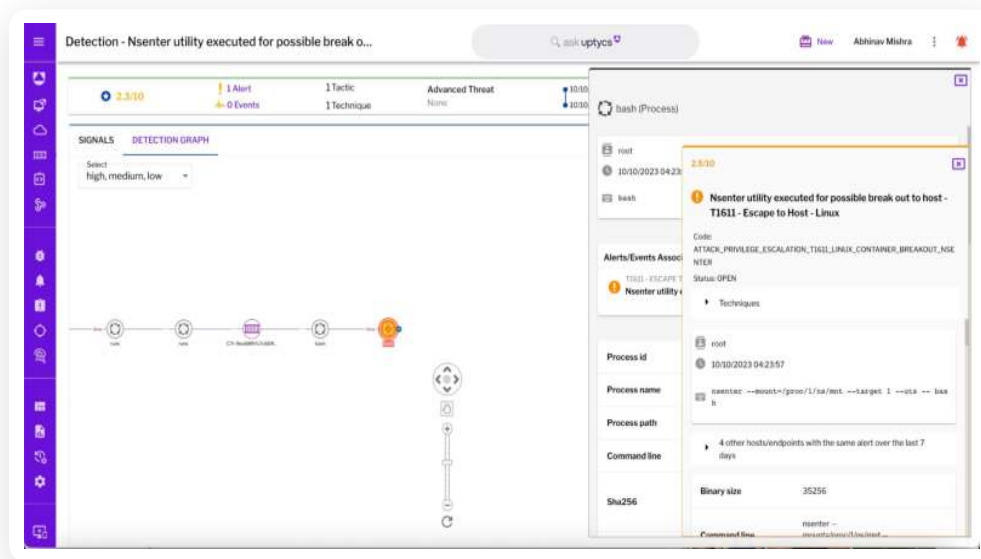
Early warning system: **KSPM** (Kubernetes Security)

Example Warning 1:

Container escape to the host system

Example Warning 2:

Default service account lateral movement



CSPM

CIEM

KSPM

CWPP

CDR

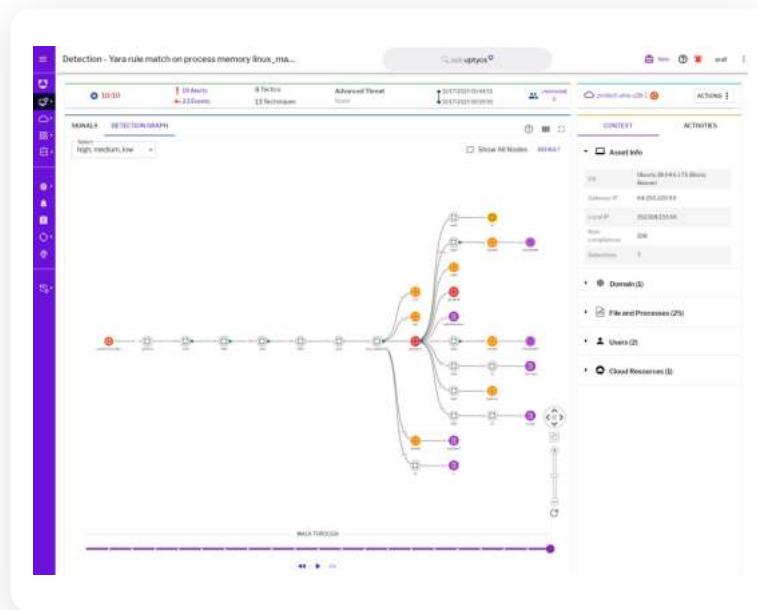
Early warning system: CWPP (Workload Security)

Example Warning 1:

Reverse shell detected

Example Warning 2:

SSH keys allow for lateral movement



CSPM

CIEM

KSPM

CWPP

CDR

Early warning system: CDR (Behavioral Activity)

Example Warning 1:

Privilege escalation via IAM policy reversion

Example Warning 2:

New action for a user

Detection - Privilege escalation - AWS Identity and Access Management (IAM) policy version reverted (5 Signals)

Who: [root@us-east-1.amazonaws.com](#) (IAM User)

When: 10/16/2022 20:09:01

What: Changes consistent with privilege escalation have been detected in your account. Specifically, you have identified an AWS Identity and Access Management (IAM) policy (1 policy) to which you have added permissions that Administrator permissions for your account and applied to policy version to this user. Privilege escalation is when an entity gains elevated access to your resources and/or environment that they normally would not have access to.

Where: [Arlington, Virginia \(United States\)](#)

Metadata

- Access Key: [AKIAI4478117611](#)
- IP Address: [44.206.255.110](#)
- User Agent: [Botocore/1.26.6 Python/3.7.13 Linux/5.4.0-103-amd64-Ubuntu](#)

It has been used in your account in the trailing 30 days.

It has been used in your account in the trailing 30 days.

Enable the access key for this IAM user by using the following in the AWS console:

- AWS Identity and Access Management (IAM)
- Users
- Search for root@us-east-1.amazonaws.com
- Security credentials
- Search for Access Key
- For access key ID: AKIAI4478117611, select Make inactive

CSPM

CIEM

KSPM

CWPP

CDR

Summarize it all



Threat actors are **cloud security experts**

- The cloud has become their playground



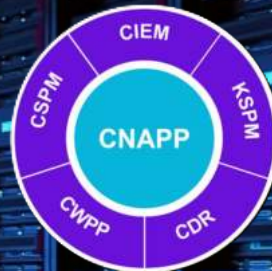
CSPM by itself opens you to blind spots



Need to focus on multiple attack surfaces, including developer laptops



Keeping yourself secure requires a platform (CNAPP) that gives you complete coverage



Appendix

Uptycs is the first unified CNAPP and XDR platform

Reduce Risk
Via...



Ask Uptycs



Cyber Asset
Inventory &
Insights



Governance,
Compliance &
Audit Evidence



Extended Detection
& Response
(XDR)



Cloud-Native
Application
Protection Platform
(CNAPP)

Detection
Cloud



Identity Fabric



Detection
Network



Lambda
Analytics



Flight Recorder



Threat
Correlation



Data Lake



Structured & Normalized Telemetry

Attack
Surfaces

Cloud Providers



Cloud Workloads
Container Runtime



Kubernetes



Endpoints
Host OS



SaaS and Identity



The three key platform capabilities...

1. Discover



What's out there?
Inventory and Insight

2. Audit



Identify what's wrong and fix it
Hygiene and Security Posture
Management

3. Secure



Respond to suspicious behavior
Detect, Respond, Block and/or
Remediate



**Some popular use cases
to get started with Uptycs**

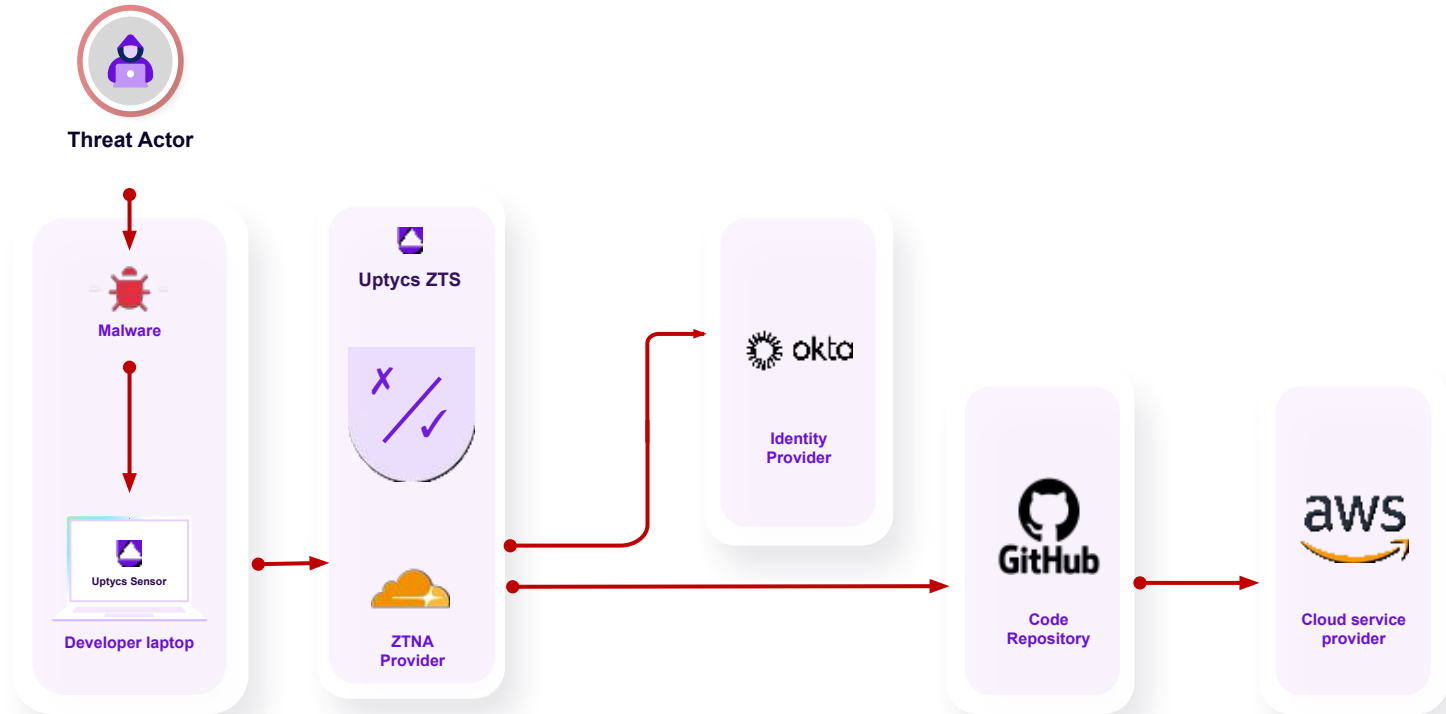
Some popular use cases...

- › Laptop to cloud early warning system
- › Mastering threat operations
- › Linux security at scale
- › K8s and container security at scale
- › Team augmentation with managed detection and response (MDR)

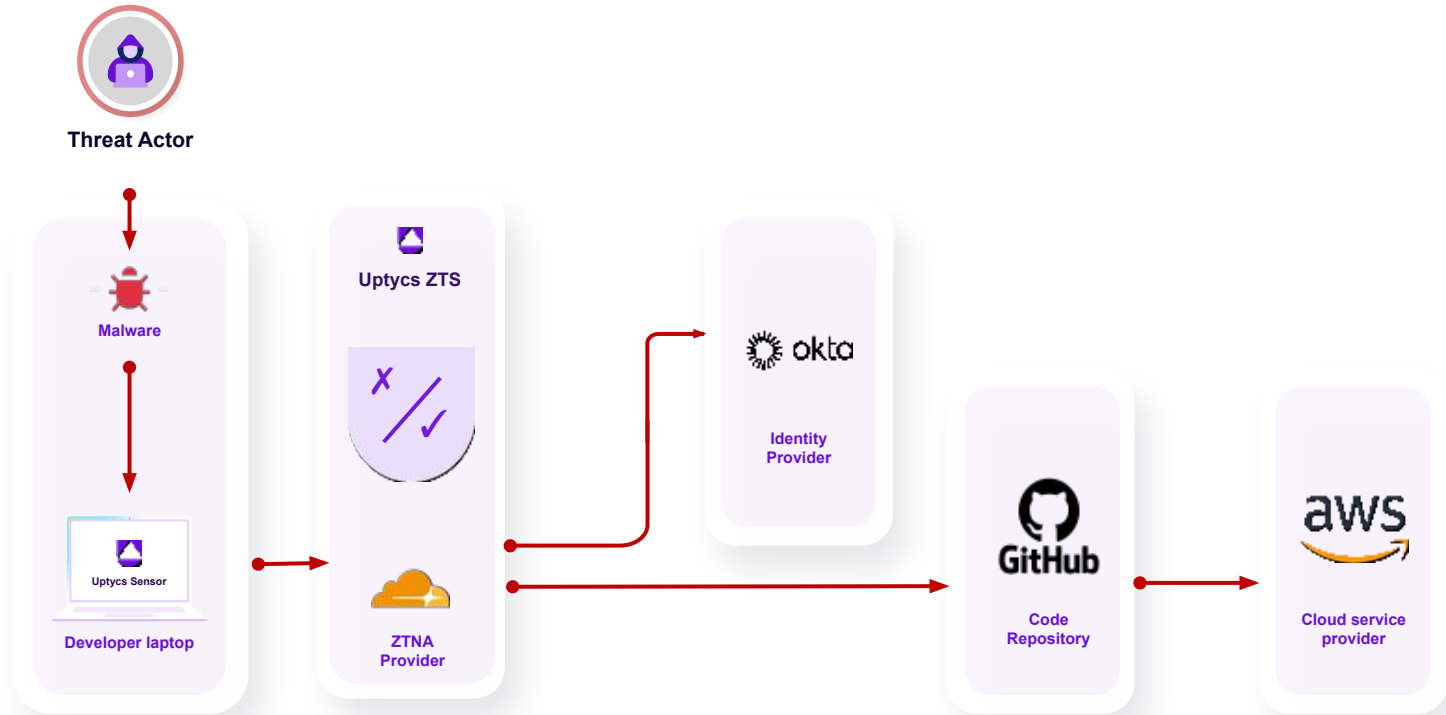


**Create a cloud security
early warning system**

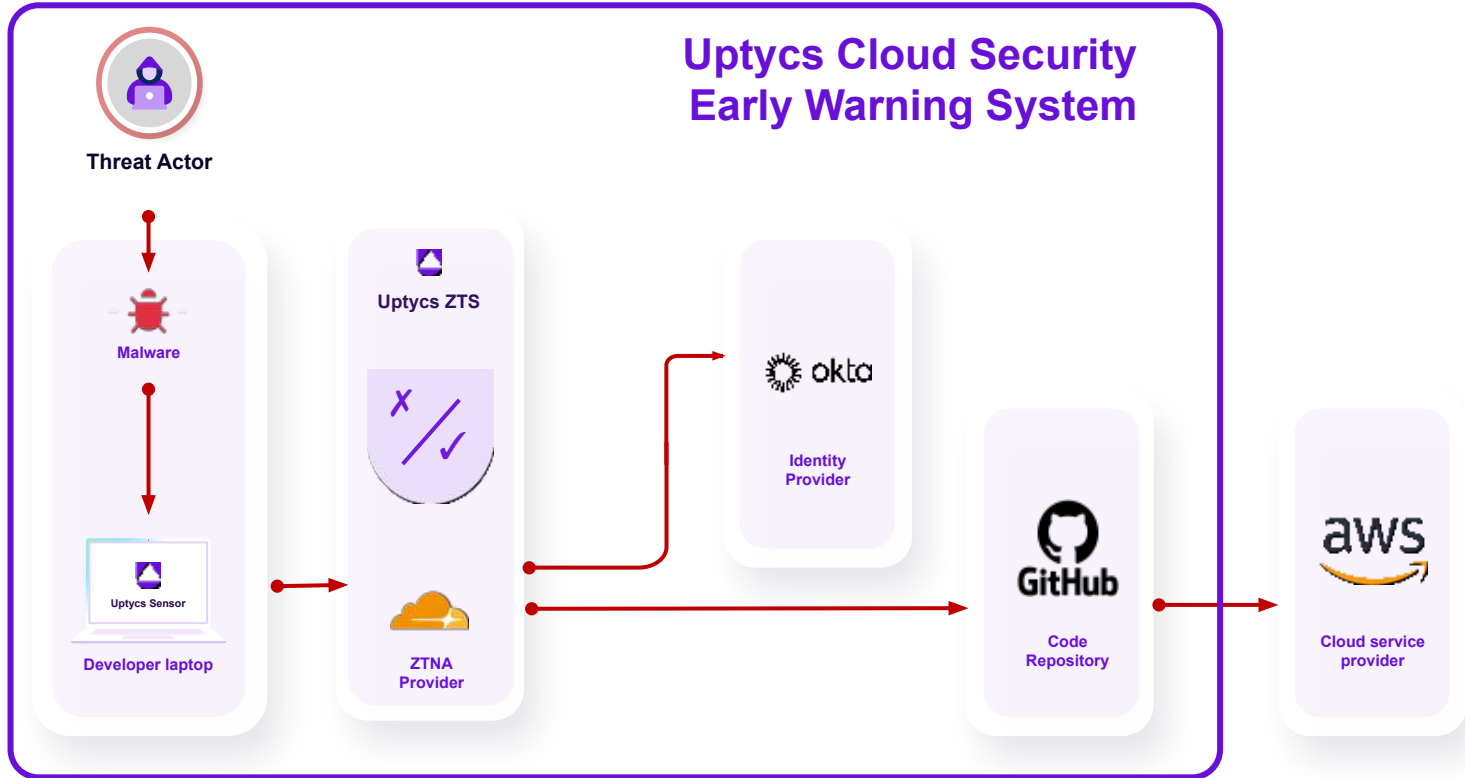
Major breaches often start with the developer's laptop



Uptycs unifying golden thread — from laptop to cloud



Gives defenders a cloud security early warning system



Uptycs Detection Cloud

 Structured and Normalized Telemetry



Developer Laptop



Identity Provider



Code Repository



Cloud Service Provider



Master your threat operations



Extensible with Powerful Threat Exposure Management

Extensible

SaaS



Identity



API First

servicenow



PagerDuty



Threat Exposure Mgmt.

- › Behavioral and anomaly detection
- › Attack path analysis
- › YARA rules
- › Correlate discrete events
- › Lateral movement detection
- › 1700+ rules mapped to ATT&CK
- › Threat intel feed
- › Secrets scanning
- › VirusTotal integration
- › Protection, blocking, and remediation
- › User-driven security

Reduce dwell time with real-time security graph and attack path analysis and monitoring

aws AWS Resource Details

Search

AWS Overview / Resource / i-020b33e36a22ed855

Security Graph Attack Path

cspm-1
Scanned by: Sensor
t2.micro
US East (N. Virginia)
Uptime 8 D 23 Hr 29 Min
frictionfree revert

Internet

Internet Gateway

Network ACL

Security Group

EC2 Instance

EC2 Instances +6

S3 Buckets +37

Possible Lateral Movement

Network

Access to resources

Critical resource

Internet exposure

EC2 Details Network Security Groups Role Volumes Security Findings Tags Activity Zero Trust Score

Master your threat operations

Fastest Speed-to-know



Search across your live infrastructure or investigate historical states going back up to 13 months

Customize for DevSecOps efficiency



Tag and group assets, tailor threat analysis via detection as code, and create custom dashboards

Don't Just Detect. Defend.



Kill or pause a process, disable users, quarantine a host, run mediation scripts, and more



Malware Detection and Forensic Investigations

“I would not want to do security anywhere without this level of visibility.”

Uptycs XDR for SEI

- › 13k+ productivity endpoints across Windows, macOS, and Linux
- › Faster time to resolution of incidents
- › Replaces a traditional forensic investigation tool with much more efficient data gathering and analysis

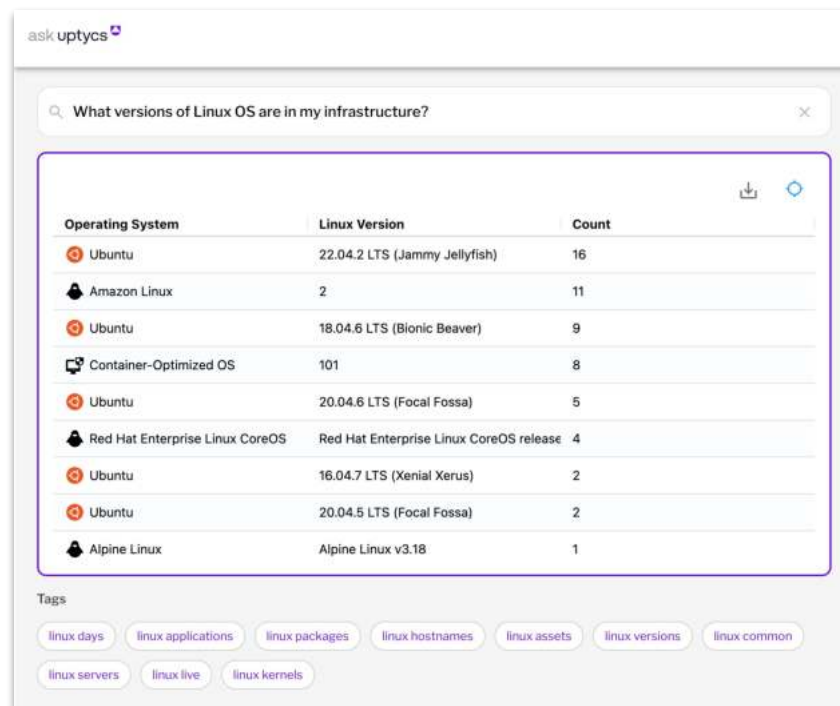




Linux security at scale

Linux security at scale

- ▶ Blazing fast response times with osquery-based agent with eBPF
- ▶ Support for rare Linux distros, IBM AIX, Linux on Z, Amazon Linux, and HPC environments
- ▶ Powerful detections framework for tracing processes and forming event alerts



The screenshot shows the 'askuptycs' interface with a search query: 'What versions of Linux OS are in my infrastructure?'. Below the search bar is a table with the following data:

Operating System	Linux Version	Count
Ubuntu	22.04.2 LTS (Jammy Jellyfish)	16
Amazon Linux	2	11
Ubuntu	18.04.6 LTS (Bionic Beaver)	9
Container-Optimized OS	101	8
Ubuntu	20.04.6 LTS (Focal Fossa)	5
Red Hat Enterprise Linux CoreOS	Red Hat Enterprise Linux CoreOS release	4
Ubuntu	16.04.7 LTS (Xenial Xerus)	2
Ubuntu	20.04.5 LTS (Focal Fossa)	2
Alpine Linux	Alpine Linux v3.18	1

Below the table, there is a 'Tags' section with several buttons: linux days, linux applications, linux packages, linux hostnames, linux assets, linux versions, linux common, linux servers, linux live, and linux kernels.



Uptycs meets the needs of cybersecurity, compliance, and platform teams

“Great compliance configuration, FIM, and XDR—and a data recorder for threat hunting.”

Uptycs for Comcast

- › Hybrid deployment: 60k Linux endpoints, 20k Windows endpoints including workstations and 40k hosts in the cloud
- › PCI compliance and CIS benchmark audits
- › FIM and configuration monitoring
- › Threat hunting and incident investigation
- › Integrations with Splunk and ServiceNow



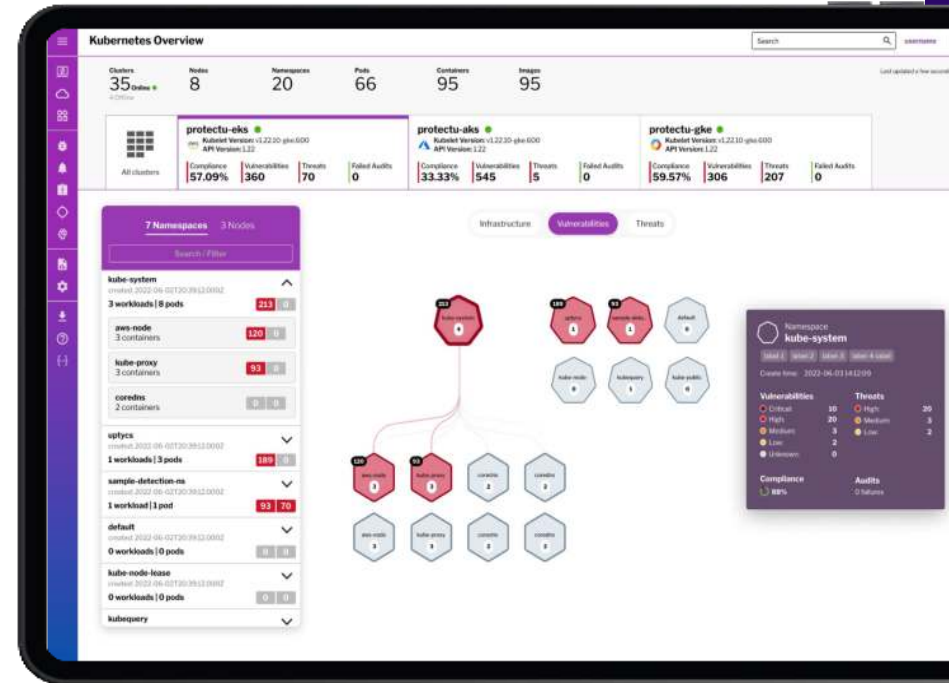


K8s and container security at scale

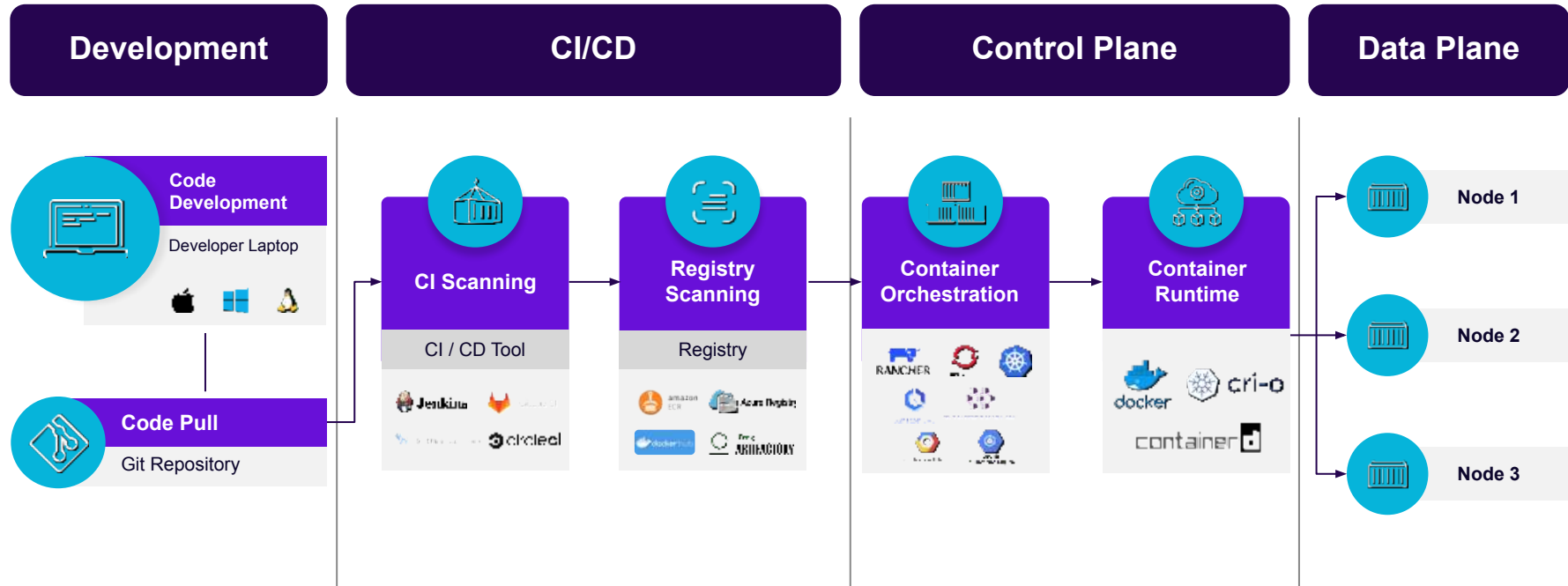
Kubernetes and container security at scale

Real-time correlation of data plane risks with K8s control plane misconfigurations

- › Single pane of glass
- › Compliance reporting / evidence
- › KPI-based vuln. management
- › Real-time threat detections



Securing your innovation pipeline with shift left controls



Real-Time Threat Detection and Correlation

Correlate runtime data plane threat info with misconfigurations in your K8s control plane

Examples

External request to
command execution
in pod - T1610
Execution Kubernetes
















Privileged pods being
created in Kubernetes
cluster - T1610
Execution Kubernetes

The screenshot displays a security dashboard interface. At the top, the title is "Detection - Kubectrl trying to access kubernetes secrets - T1552 Credential Access for Linux /usr/bin/kubectrl". The dashboard shows 12 Alerts, 0 Events, 1 Tactic, and 1 Technique. The main area is divided into "SIGNALS" and "DETECTION GRAPH". Under "SIGNALS", there are two entries for "T1552 CREDENTIAL ACCESS FOR LINUX_CLONE" with a severity of -5. Each entry is titled "Kubectrl trying to access kubernetes secrets" and has 6 associated signals. The right sidebar shows "CONTEXT" and "ACTIVITIES" for the selected signal, including "Asset Info" (OS: Amazon Linux 2, IP: 34.237.0.234), "File and Processes (1)" (path: /usr/bin/kubectrl), and "Users (1)" (username: root).



Managed Detection and Response

Uptycs Managed Services Coverage

	Managed Onboarding	Managed Monitoring	Managed Protect
Prepare			
Identify			
Contain / Intel Development			
Eradicate			
Recovery			



Crossbeam lowers risk and costs with CNAPP, XDR & MDR

“Uptycs is a single solution where we can correlate data across endpoints, containers, and cloud.”



Uptycs for Crossbeam

- › Uptycs responds to alerts so Crossbeam’s SecOps team can focus on strategic tasks
- › Single UI and data model provides visibility across endpoints, containers, and cloud
- › Meet SOC 2 and ISO 27001 security controls for FIM, malware detection, and more
- › Easy to answer questions about risk, such as Log4j exposure