sysdig SECURE EVERY SECOND.

CNAPP Unleashed: Your Key to Cloud-Native Data Protection

Sean Walsh

Sales Engineer

Our Mission

Secure and Accelerate Cloud Innovation

We Are Builders

Falco

Powered By The Open Source Solution For Cloud Threat Detection

WIRESHARK

Co-created by Sysdig Founder

aws · Microsoft Azure · Google Cloud · IBM Cloud

We Are Trusted

AIRFRANCEKLM GROUP · Alaska AIRLINES · AMERICAN EXPRESS

CISCO · COMCAST · DOLLAR GENERAL

Ford · Goldman Sachs · IBM

KAISER PERMANENTE. · worldpay from FIS · McKinsey & Company

Pfizer · VISA · SAP Concur

T··Mobile· · Calendly · YAHOO! JAPAN

We Are Leaders

7 Million Containers Analyzed Daily

65 Million Falco Downloads

700+ Valued Customers

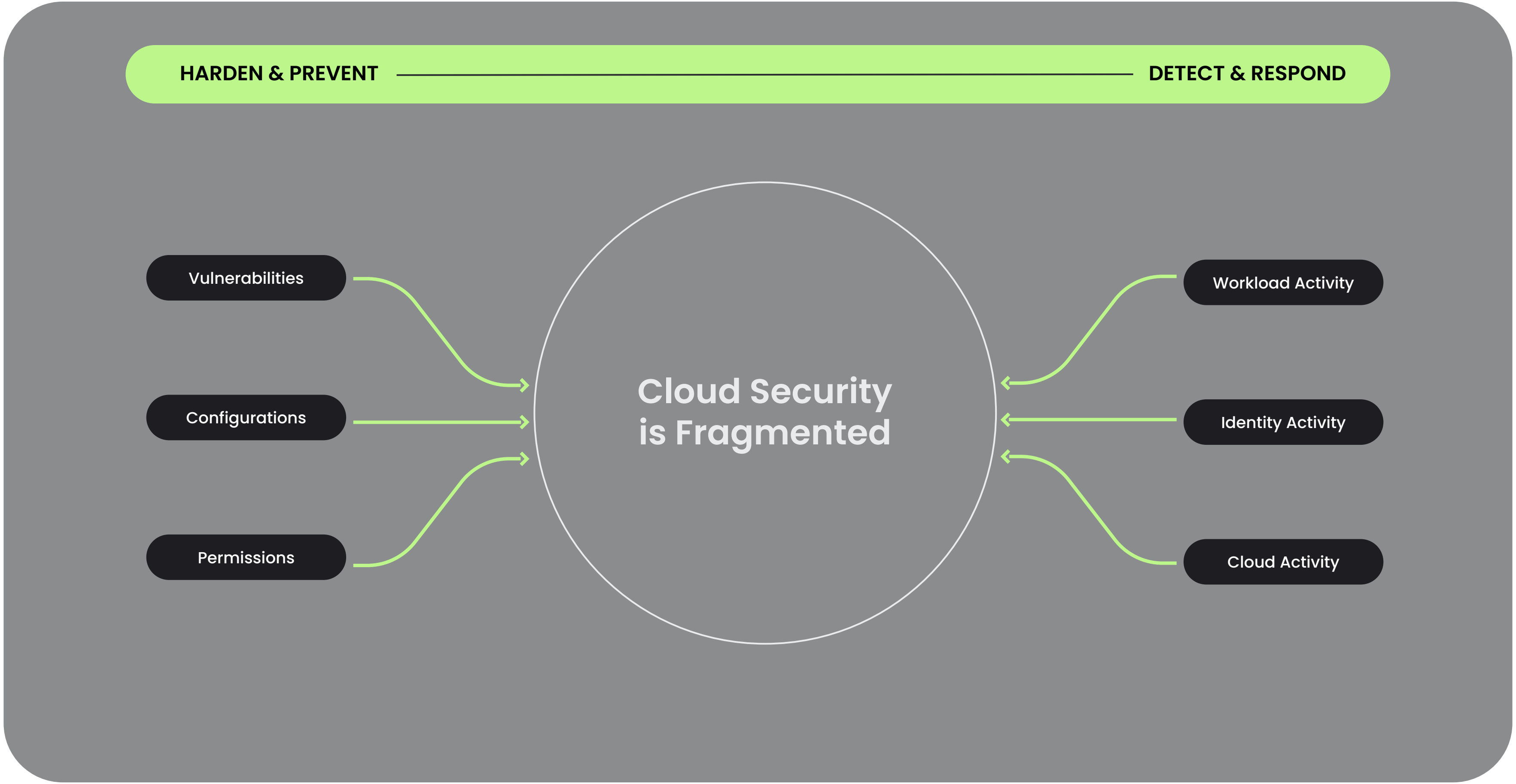
750+M In Funding

Gartner. Peer Insights.

★★★★★

The Top Rated CNAPP

LEADER IN CNAPP
(Cloud Native Application Protection Platform)



HARDEN & PREVENT

DETECT & RESPOND

Vulnerabilities

Configurations

Permissions

Cloud Security is Fragmented

Workload Activity

Identity Activity

Cloud Activity

HARDEN & PREVENT — DETECT & RESPOND

KEY RISKS BURIED IN THE NOISE

85%
Of critical and high vulnerabilities are not in use at runtime

Cloud Security is Too Slow

CLOUD ATTACKS MOVE AT WARP SPEED

<10 minutes
Time attackers need to execute an attack

Cloud Attacks are Fast & Sophisticated

Stolen Credentials

REvil

Medibank

Medical records leaked, $80M+ in damages

Critical Vulnerability

LABRAT

Gitlab

Proxyjacking for financial gain

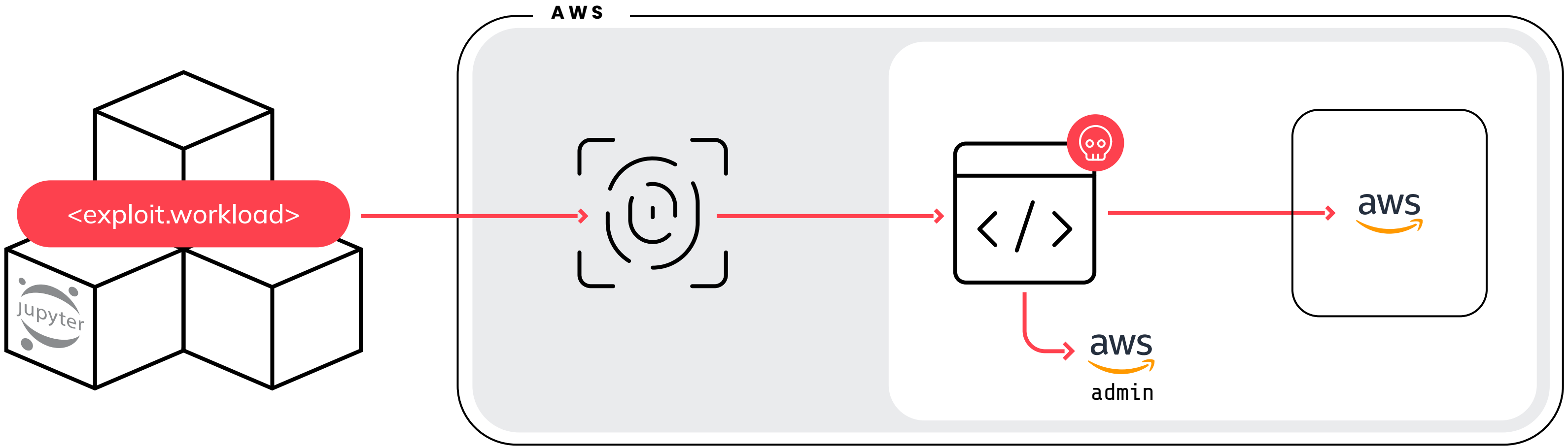
Lateral Movement

SCARLETEEL

Exfiltration of proprietary information

SCARLETEEL

Traditional Security in the Cloud is Obsolete



1

Exploit workload vuln and misconfiguration

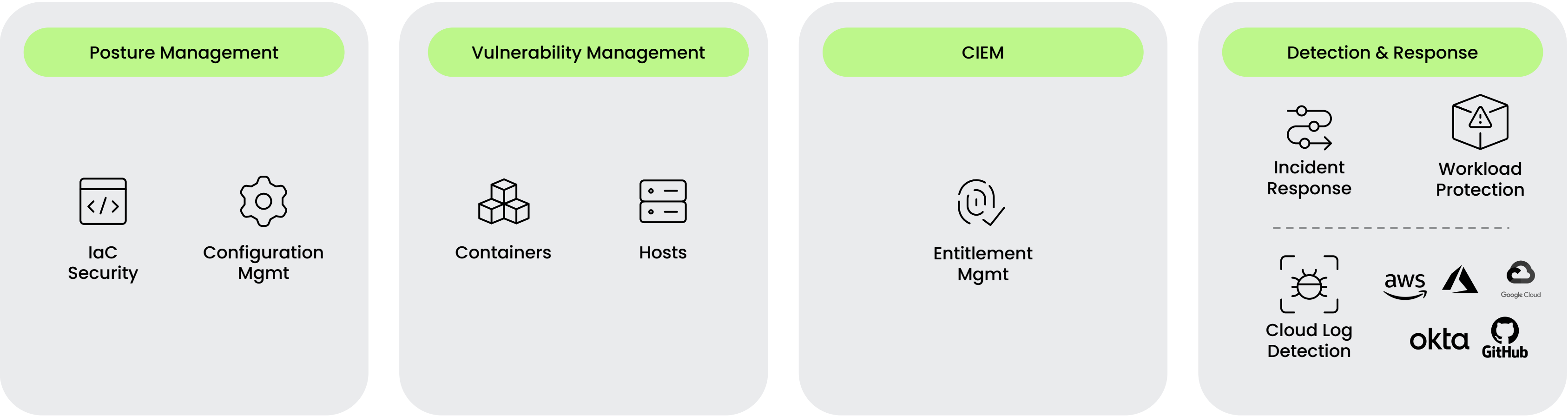
2

Deploy cryptominer as a distraction to steal AWS credentials

3

Steal proprietary data and lateral movement between AWS accounts

Unified CNAPP



Posture Management

IaC Security

Configuration Mgmt

Vulnerability Management

Containers

Hosts

CIEM

Entitlement Mgmt

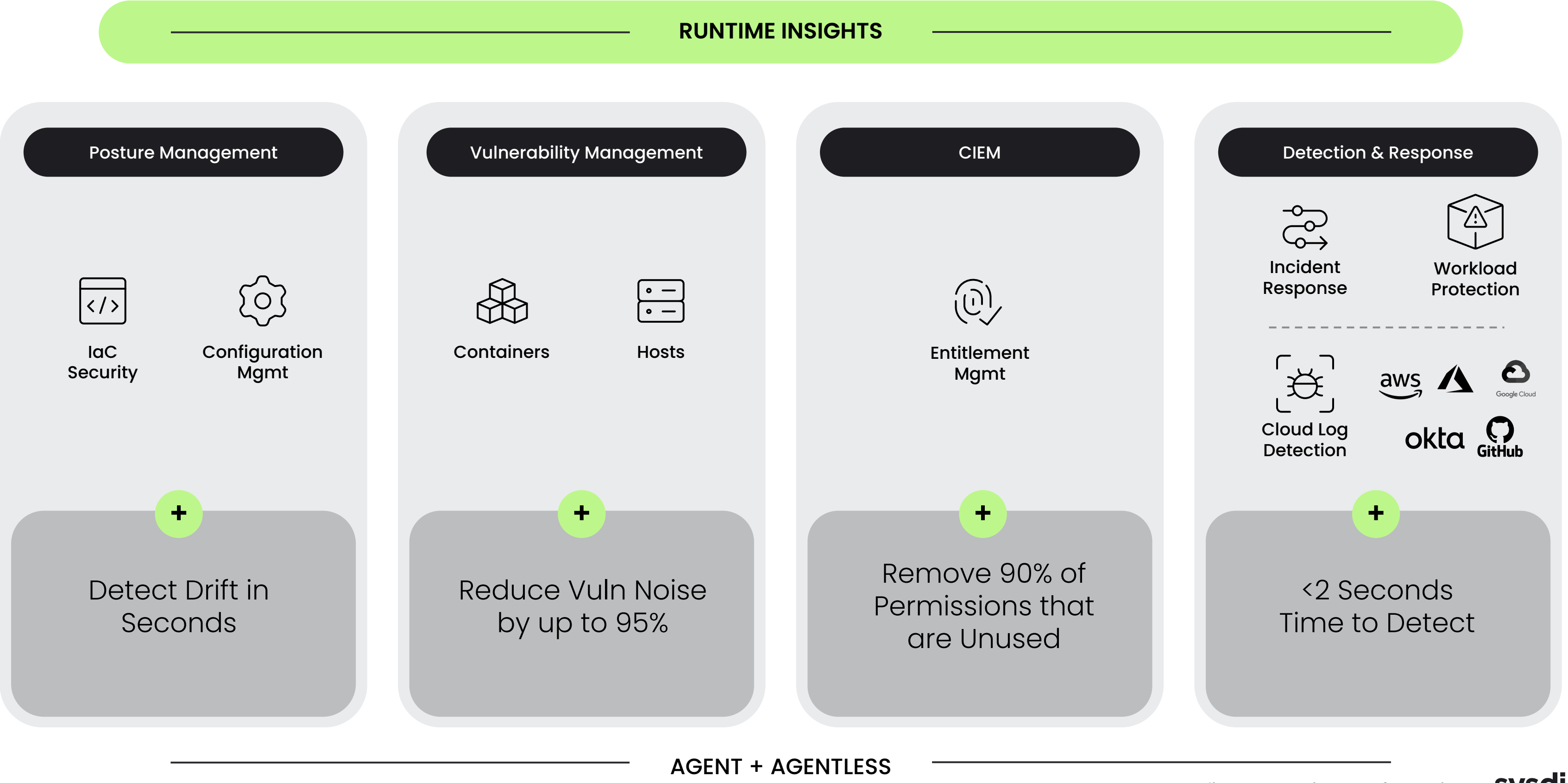
Detection & Response

Incident Response

Workload Protection

Cloud Log Detection

CNAPP Powered by Runtime Insights



RUNTIME INSIGHTS

Posture Management

IaC Security

Configuration Mgmt

+

Detect Drift in Seconds

Vulnerability Management

Containers

Hosts

+

Reduce Vuln Noise by up to 95%

CIEM

Entitlement Mgmt

+

Remove 90% of Permissions that are Unused

Detection & Response

Incident Response

Workload Protection

Cloud Log Detection

aws

Google Cloud

okta

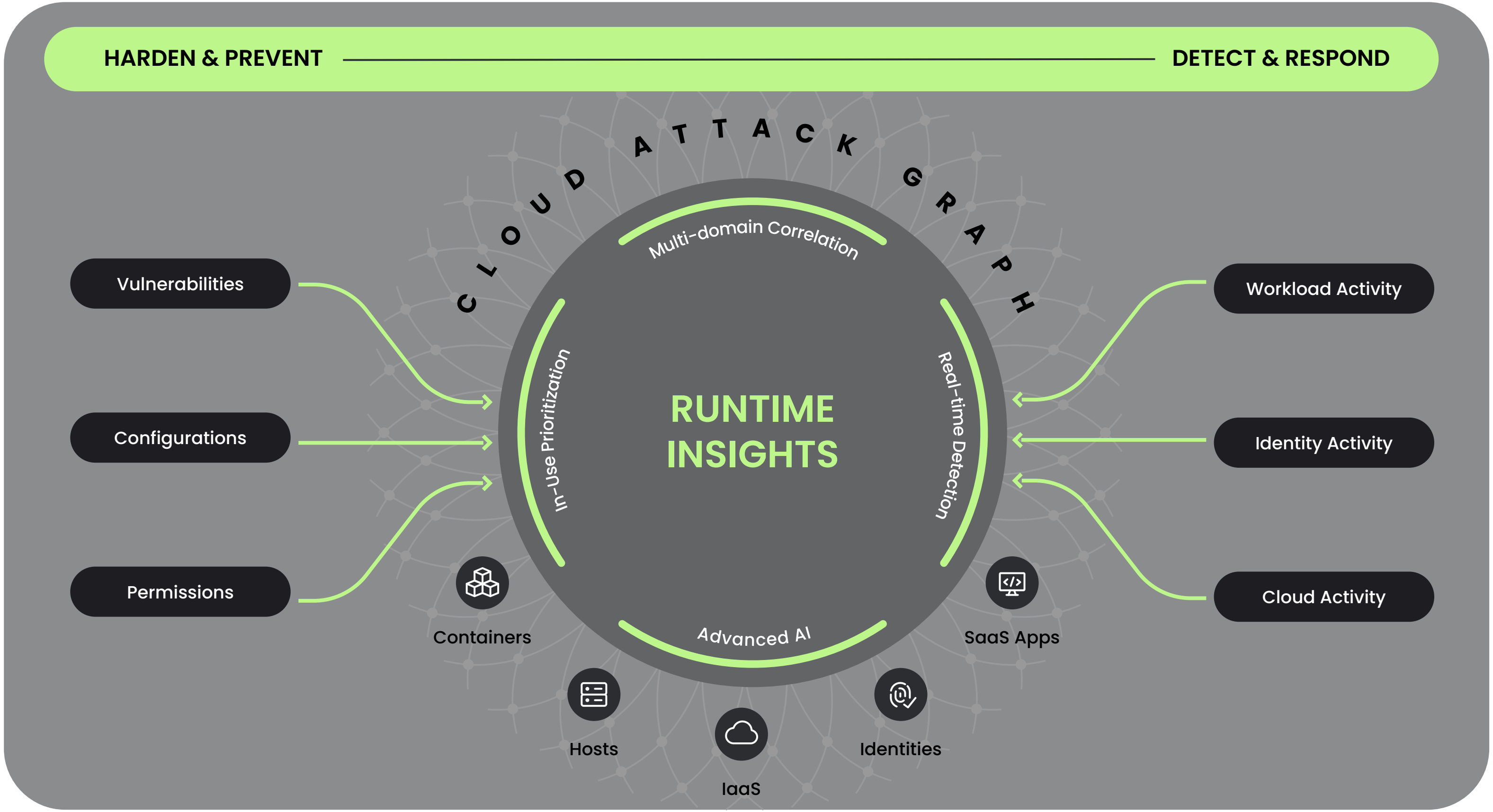
GitHub

+

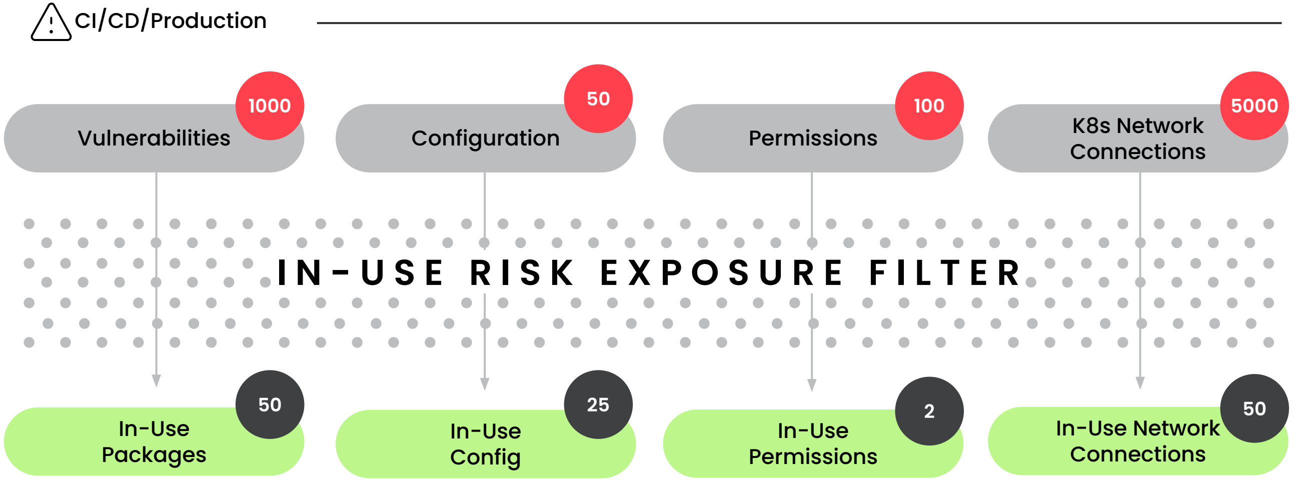
<2 Seconds Time to Detect

AGENT + AGENTLESS

CNAPP Powered by Runtime Insights

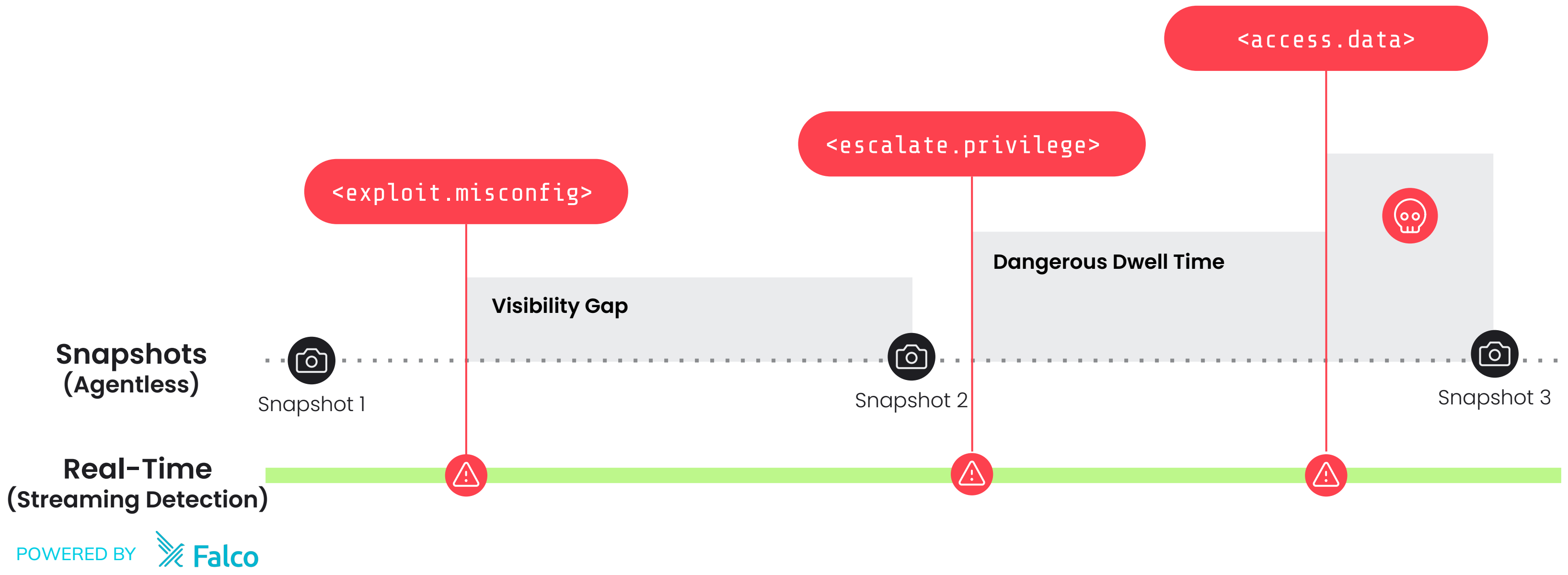


In-Use Prioritization



> “I’m saving an hour and a half per vulnerability by not having to investigate when the package is not in use.
>
> BEEKEEPER

Real-time Detection vs. Snapshots



Multi-domain Correlation

Isolated Findings Mask True Risk

Public Exposure
9% of resources are publicly exposed

Vulnerabilities
13% of resources have critical vulns within packages in-use

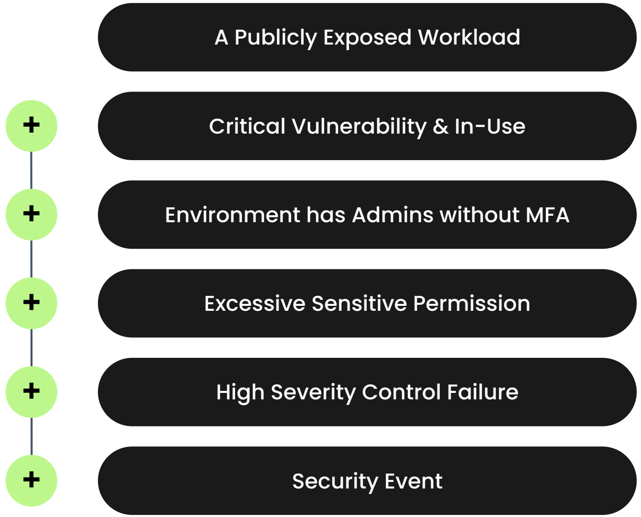
Permissions
39% of roles have excessive sensitive permissions

Insecure Identity
68% of admins don’t have MFA

Misconfigurations
33% of resources have high severity failing controls

Threats
Abnormal activity detected in 9% of the resources

⚠ Correlated findings reveal the true risk:



A Publicly Exposed Workload

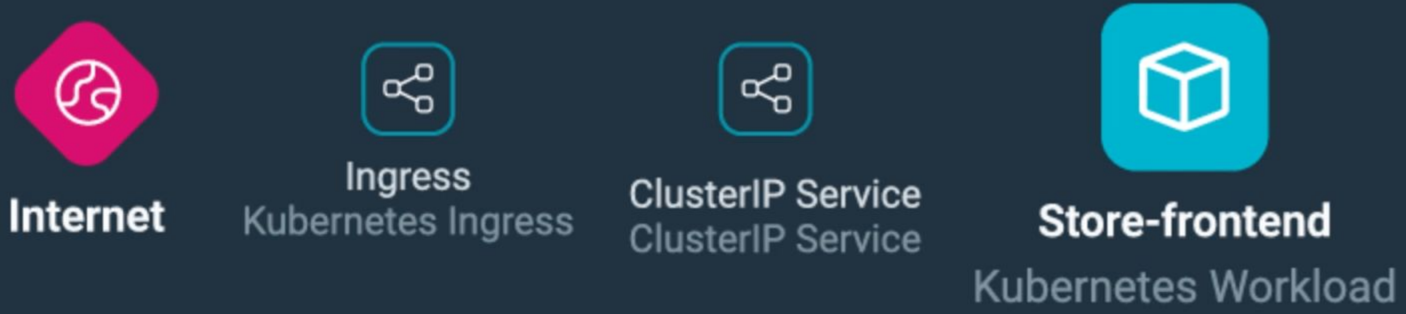
+ Critical Vulnerability & In-Use

+ Environment has Admins without MFA

+ Excessive Sensitive Permission

+ High Severity Control Failure

+ Security Event



Internet

Ingress
Kubernetes Ingress

ClusterIP Service
ClusterIP Service

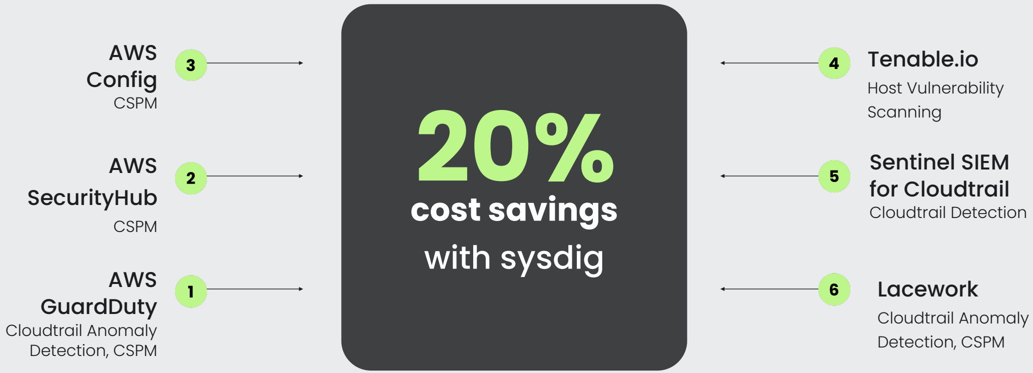
Store-frontend
Kubernetes Workload

Consolidating into a unified CNAPP

Arkose Labs

With Sysdig,
we consolidated
6 tools to 1
saving money
and time.

IT Security Manager
Leader in Bot Mitigation



AWS Config
CSPM

AWS SecurityHub
CSPM

AWS GuardDuty
Cloudtrail Anomaly Detection, CSPM

20%
cost savings
with sysdig

Tenable.io
Host Vulnerability Scanning

Sentinel SIEM for Cloudtrail
Cloudtrail Detection

Lacework
Cloudtrail Anomaly Detection, CSPM

Success Story

BigCommerce

BIGCOMMERCE

Address visibility gaps with comprehensive end-to-end platform support

Identify and prioritize misconfigurations and vulnerabilities

Quickly generate granular, actionable insights with as few clicks as possible

WITH SYSDIG

2
Second Response

80%
Noise Reduction

20%
Efficiency Increase

> I can't wait 15 minutes or several hours. With Sysdig, we can identify and address potential threats in real time..
>
> **Senior Infrastructure Security Engineer**

Real Customer Evaluation

Detection & Response Capabilities

Issue	Prisma	Lacework	SentinelOne	Wiz	sysdig
Shelled into a pod and did recon	✗	✗	✗	✗	✓
Deployed ubuntu pod	✗	✗	✗	✗	✓
Ran nmap	✓	✗	✗	✗	✓
Installed AWS CLI	✗	✗	✗	✗	✓
Stole an S3 file	✓	✗	✗	✗	✓
Spun up a ton of vulnerable EKS resources	✗	✓	✗	✓	✓
Uploaded a remote shell and ran commands	✗	✗	✗	✗	✓
Container escape	✗	✗	✗	✗	✓
Response Capabilities	Alert, defense mode kills the process	None, Alert Only	Kill Processes	None	Kill the Pod

Next: Demo

sysdig SECURE EVERY SECOND.

Next: Raffle Giveaway

Bose QuietComfort Earbuds II

Scan QR code to enter the raffle
Must be present to win

Thank you!

If you have any questions,
please contact me at sean.walsh@sysdig.com or reach out to our sales team at sales@sysdig.com