

# Herzlich willkommen zum Live-Webcast

## Agile Infrastruktur in der Cloud erfordert besondere Sicherheit



**Sprecher:**

**Eugen Hinz,**  
Channel Systems Engineer und Subject  
Matter Expert, Palo Alto Networks



**Moderator:**

**Martin Seiler**  
Heise Business  
Services

# Prisma Cloud

Agile Infrastruktur in der Cloud erfordert  
besondere Sicherheit



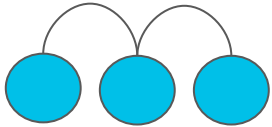
# Digital Transformation

## Development Process

Waterfall



Agile

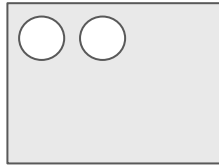


DevOps

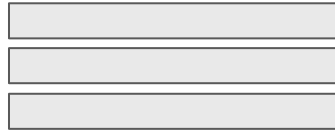


## Application Architecture

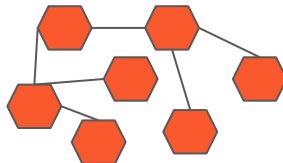
Monolithic



N-Tier

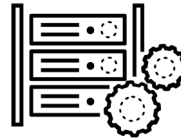


Microservices

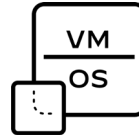


## Deployment and Packaging

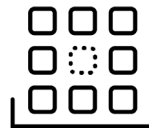
Physical Server



Virtual Servers

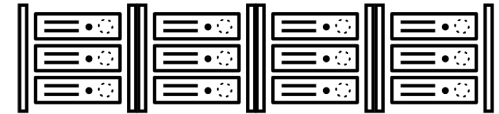


Containers



## Application Infrastructure

Datacenter



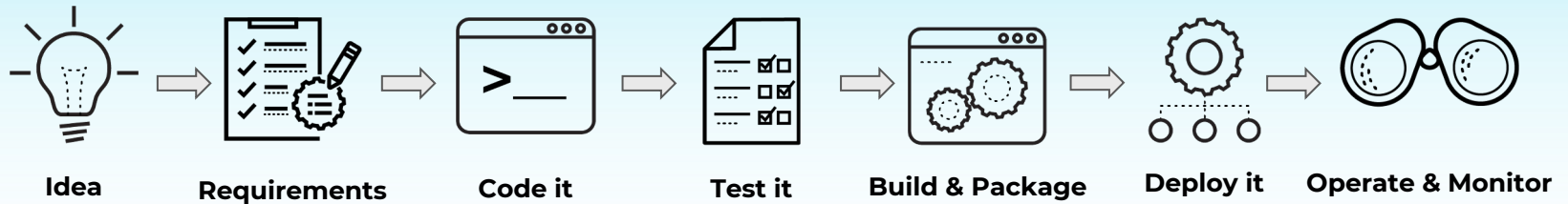
Hosted



Cloud



# Typical Software Release Process



## Initial Launch

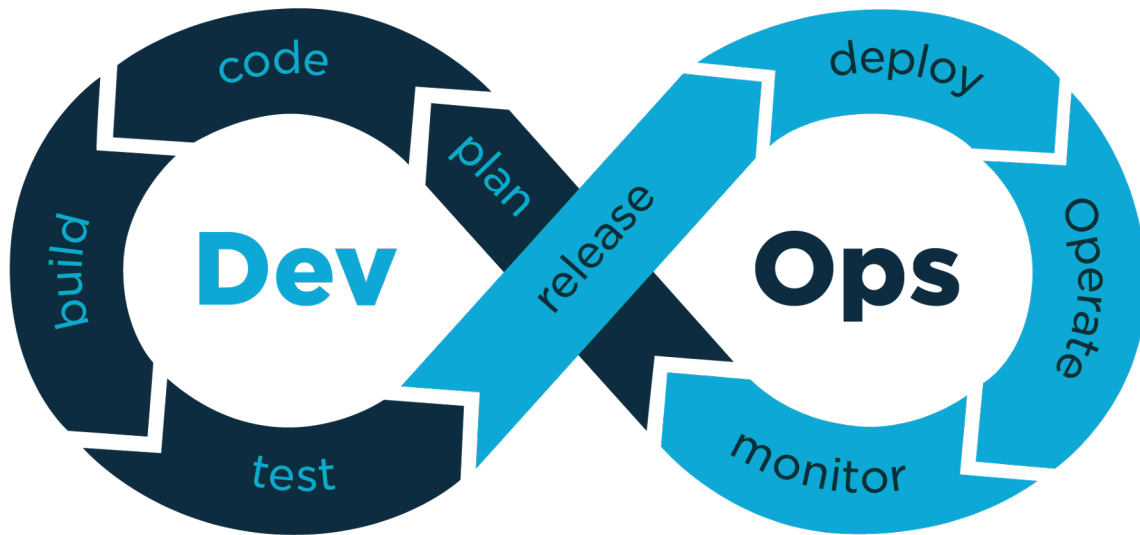


# What is DevOps?

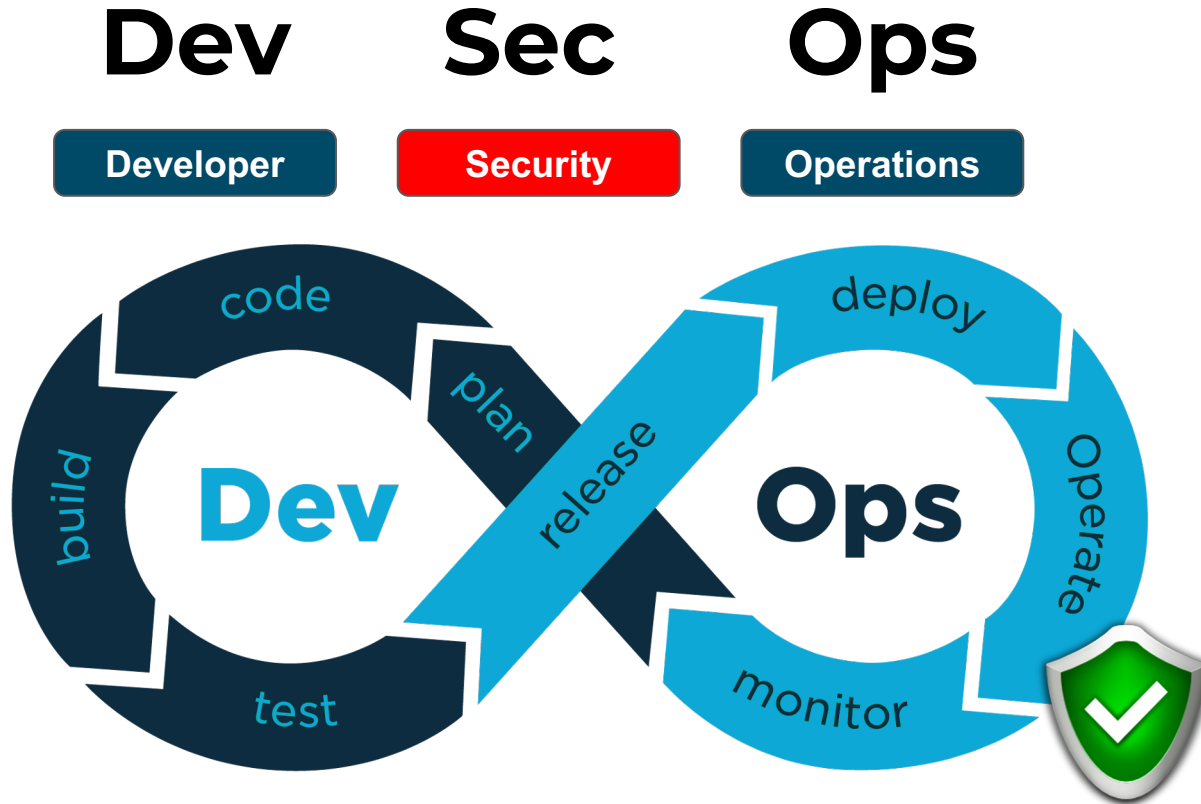
## Dev Ops



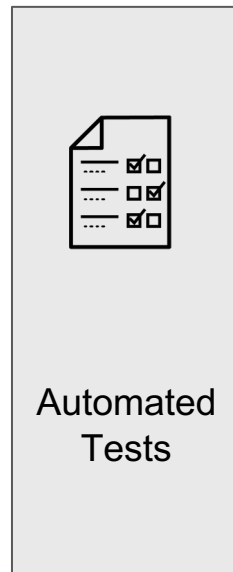
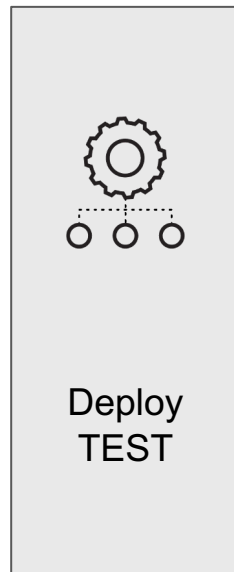
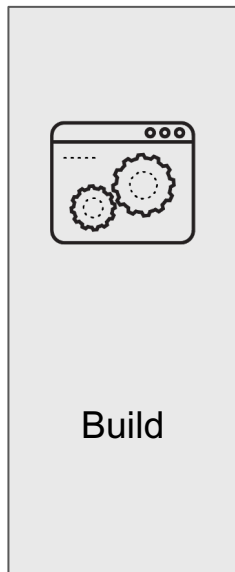
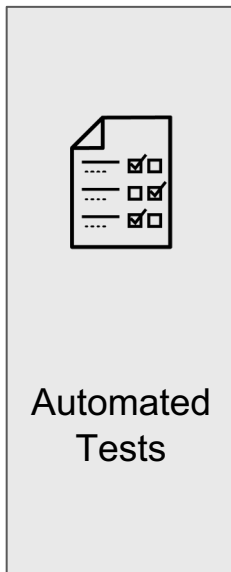
## Sec



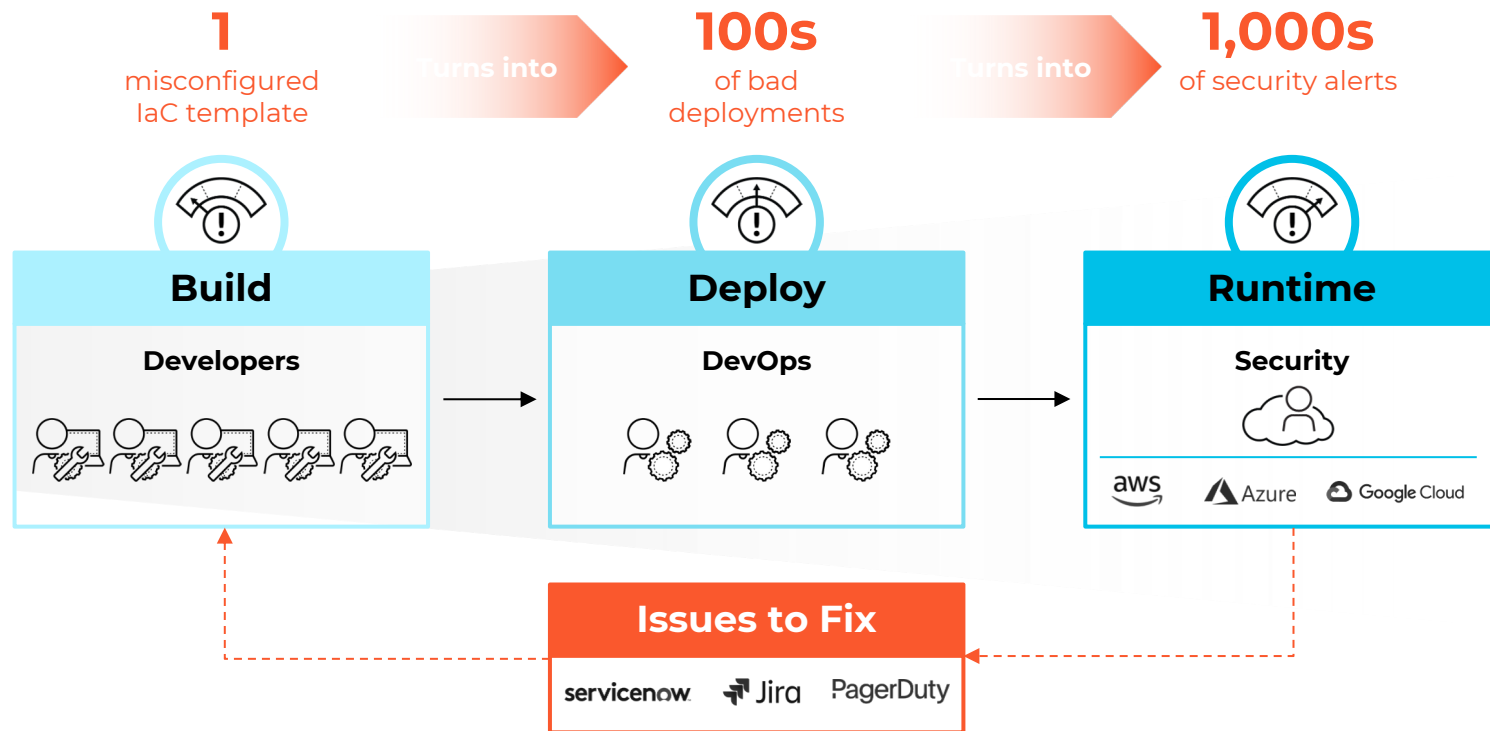
# What is DevSecOps?



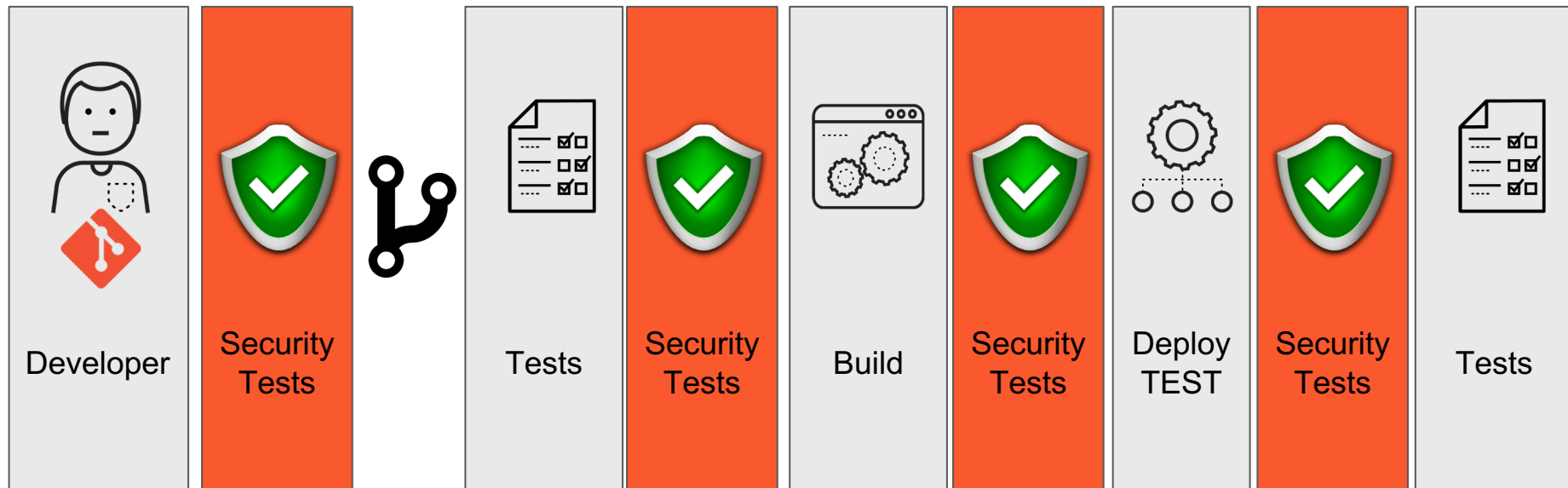
## DevOps Pipeline



# Infrastructure as Code (IaC): The Need for “Shift Left” Cloud Security



## DevSecOps Pipeline



# Prisma Cloud: Comprehensive Cloud Native Security Platform (CNSP)



## DevSecOps

Integrate and perform infrastructure and application security in the CI/CD pipeline



## Cloud Security Posture Management

Monitor posture, detect and respond to threats, maintain compliance



## Cloud Workload Protection

Secure hosts, containers, and serverless across the application cycle



## Cloud Network Security

Monitor and secure cloud networks, enforce microsegmentation



## Cloud Infrastructure Entitlement Management

Enforce permissions and secure identities across workloads and clouds

IaC Security

Visibility, Compliance & Governance

Threat Detection

Data Security

Host Security

Container Security

Serverless Security

Web Application & API Security

Identity-Based  
Microsegmentation

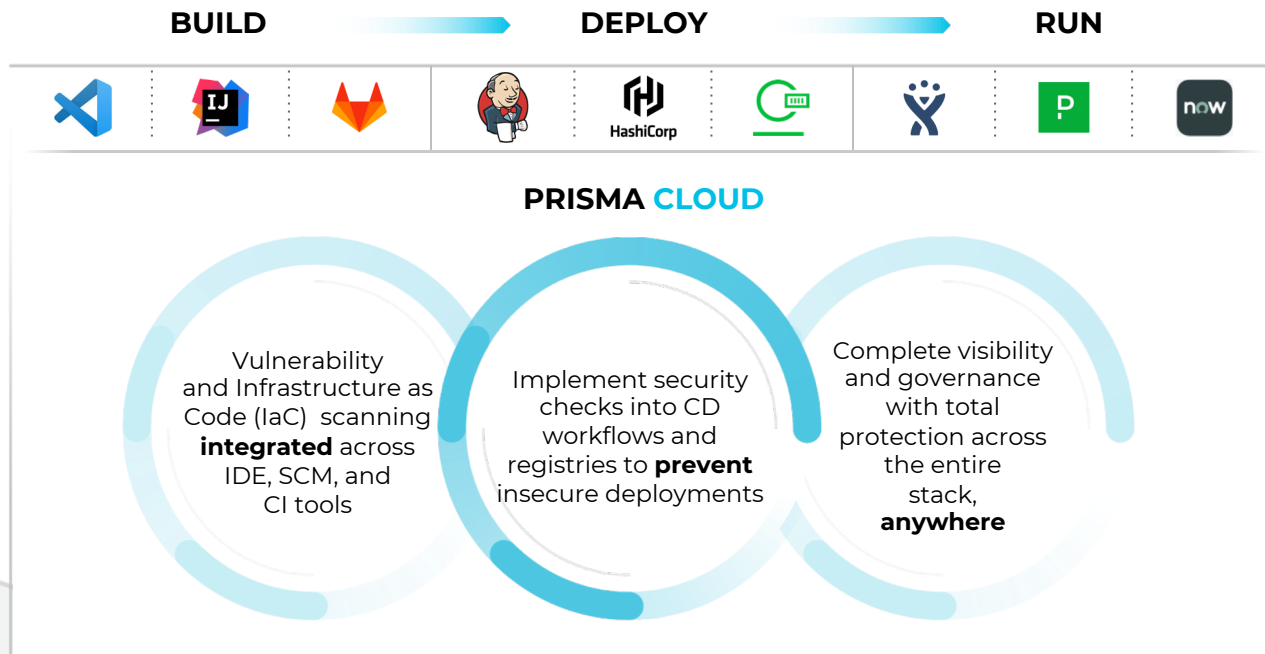
IAM Security

# Capabilities

# Shift Left Security



# Full Lifecycle Security for Cloud Native Applications



vmware

aws



Azure

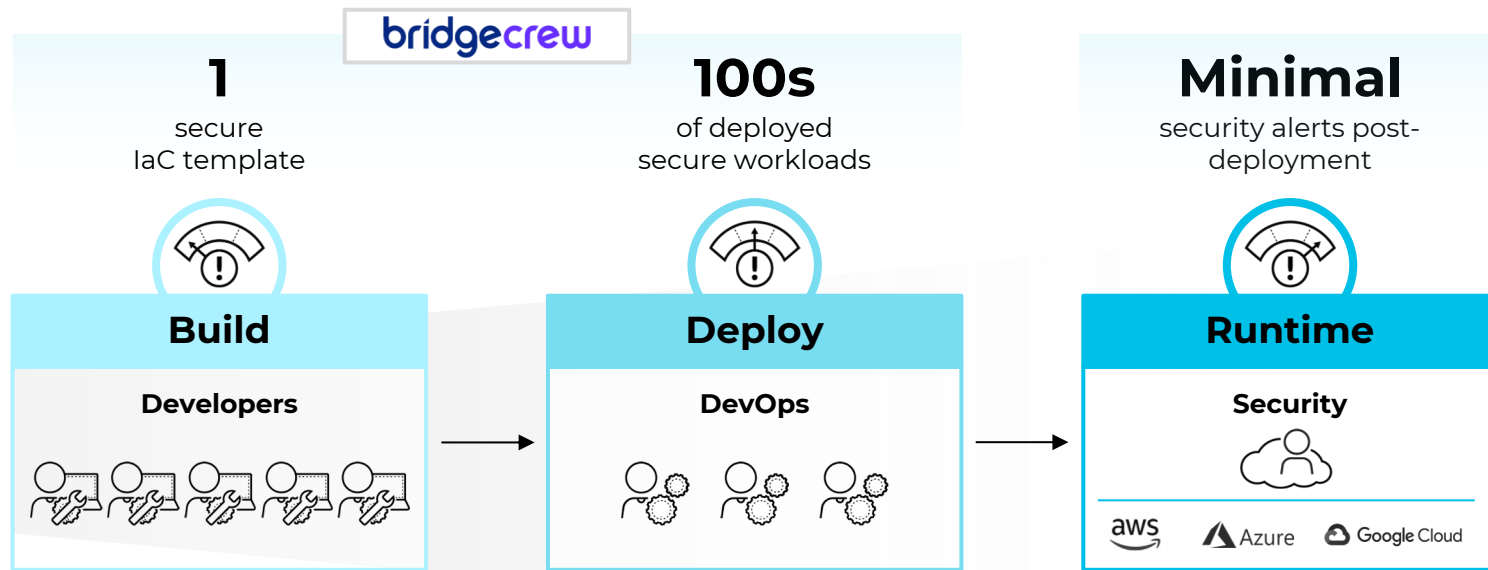
ORACLE  
Cloud Infrastructure

Alibaba Cloud

docker



# Bridgecrew Pioneered Developer-First Approach to Secure IaC



## Approach to developer-focused cloud security

- **Detect** infrastructure security issues during development process
- **Prevention** in every commit, pull request & build job using policy as code

## Focus on critical threats

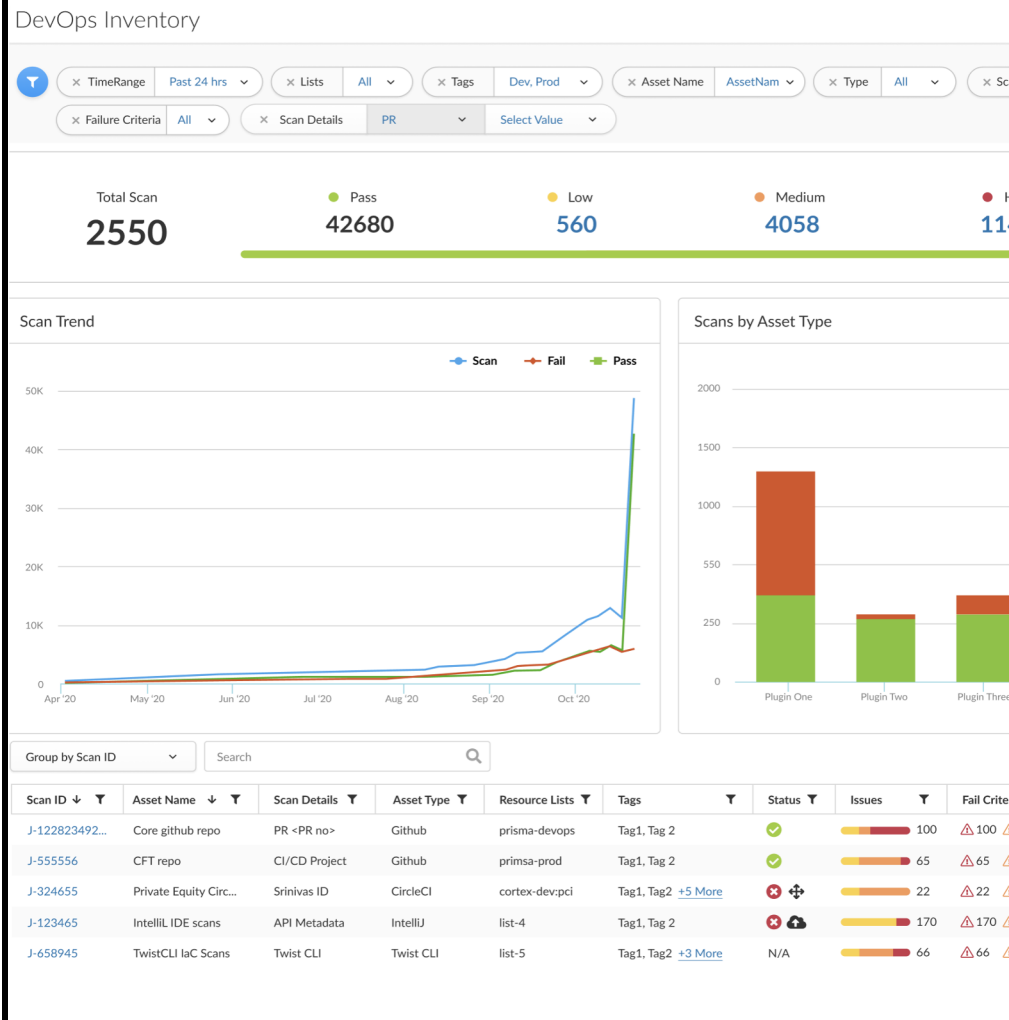
# IAC Scanning

Scanning and control over CloudFormation templates, Terraform templates, and Kubernetes deployment yaml files

Integrated with SCM, IDE, and CI tools

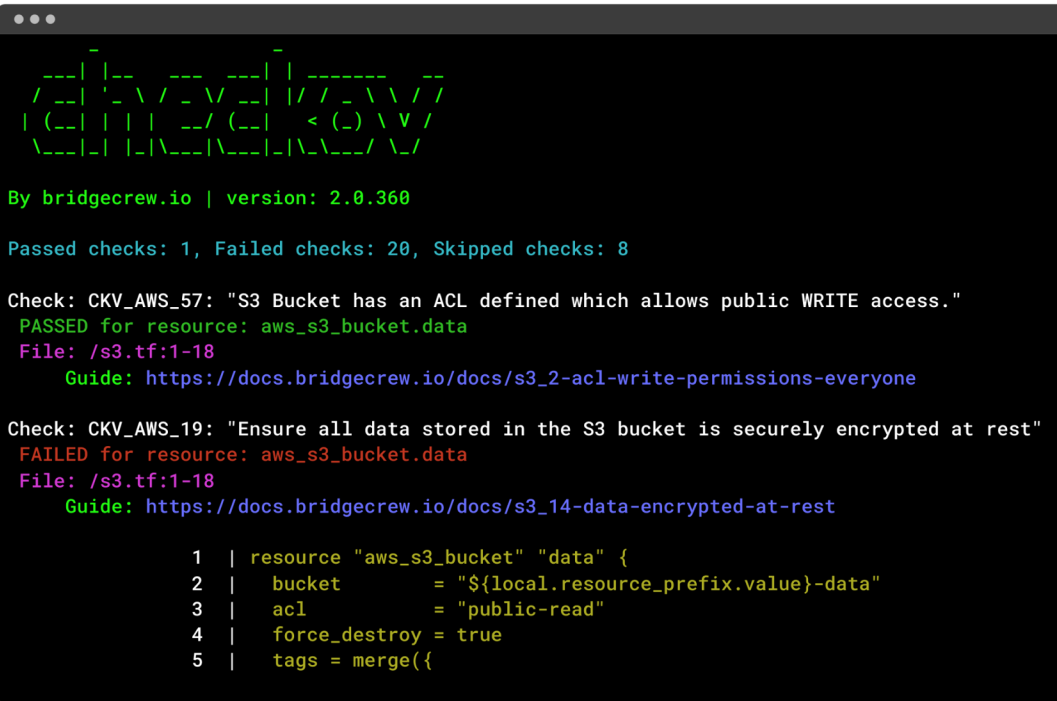
Build policies in Prisma Cloud Console  
centralize IAC governance

Integrations with SCM, IDE, and CI tools:



# Scan local files and directories from the command line

- Scan IaC files and directories for misconfigurations pre-commit with Checkov to address errors before they're integrated into shared repositories.

A terminal window with a dark background and light green text. It displays the output of a Checkov scan. At the top is a green ASCII art logo. Below it, the text 'By bridgecrew.io | version: 2.0.360' is shown in green. Then, 'Passed checks: 1, Failed checks: 20, Skipped checks: 8' is displayed in cyan. Two specific checks are detailed: CKV\_AWS\_57, which passed, and CKV\_AWS\_19, which failed. The failed check includes a red 'FAILED' status, the resource name 'aws\_s3\_bucket.data', the file path '/s3.tf:1-18', and a green link to a guide. At the bottom, a snippet of Terraform code is shown with line numbers 1 through 5.

```

  _--| |-- _-- _--| |----- _--
 / _--| ' _ \ / _ \ _--| | / _ \ \ /
 | ( _--| | | | _--| ( _--| < ( _--| \ \ /
 \ _--| | | | \ _--| \ _--| \ \ _--| \ \ /

By bridgecrew.io | version: 2.0.360

Passed checks: 1, Failed checks: 20, Skipped checks: 8

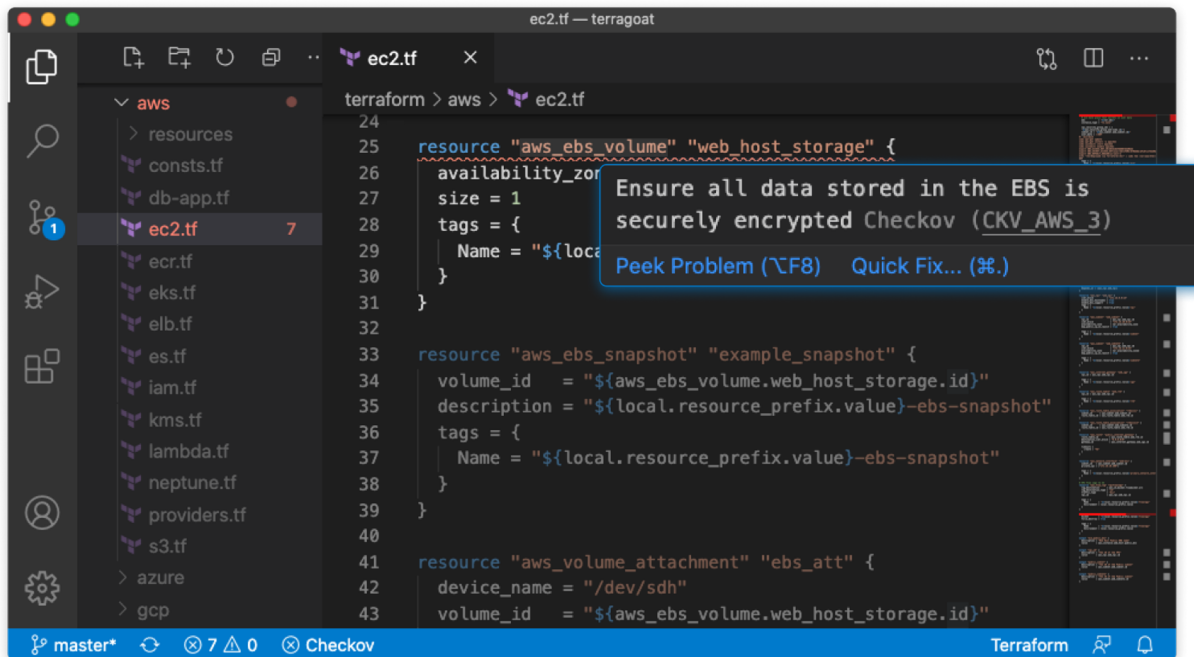
Check: CKV_AWS_57: "S3 Bucket has an ACL defined which allows public WRITE access."
PASSED for resource: aws_s3_bucket.data
File: /s3.tf:1-18
Guide: https://docs.bridgecrew.io/docs/s3_2-acl-write-permissions-everyone

Check: CKV_AWS_19: "Ensure all data stored in the S3 bucket is securely encrypted at rest"
FAILED for resource: aws_s3_bucket.data
File: /s3.tf:1-18
Guide: https://docs.bridgecrew.io/docs/s3_14-data-encrypted-at-rest

1 | resource "aws_s3_bucket" "data" {
2 |     bucket      = "${local.resource_prefix.value}-data"
3 |     acl         = "public-read"
4 |     force_destroy = true
5 |     tags = merge({
```

# IDE feedback and fixes

- Enforce guardrails as you code with Bridgecrew's IDE extensions
- Inline insights and fixes



# Git Repo Vulnerability Management

Scan Node, Java, and Python libraries on GitHub on commit or at regular time intervals

Identify Vulnerabilities and Risk Factors, integrated with Host, Container, and Serverless capabilities

Integrations with git repos:



Monitor / Vulnerabilities

Code Repositories

Code repositories

Filter code repositories by keywords and attributes

Repository

P...

Vulne...

Vulnerabili...

Risk Factors

keylowe/FoodTrucks

GitHub

2

12 6 2

8

Filter files by keywords and attributes

File Path

Type

Vulnerabilities

flask-app/requirements.txt

Python

2 6 2

8

flask-app/package.json

Node.js

1

3

keylowe/hellonode

GitHub

0

0

0

Aug 26, 2020 ...

© Critical severity

Ⓜ High severity

Ⓜ Medium severity

⚡ Attack Complexity: Low

🕒 Recent vulnerability

🔗 Attack Vector: Network

🚫 DoS

✅ Has fix

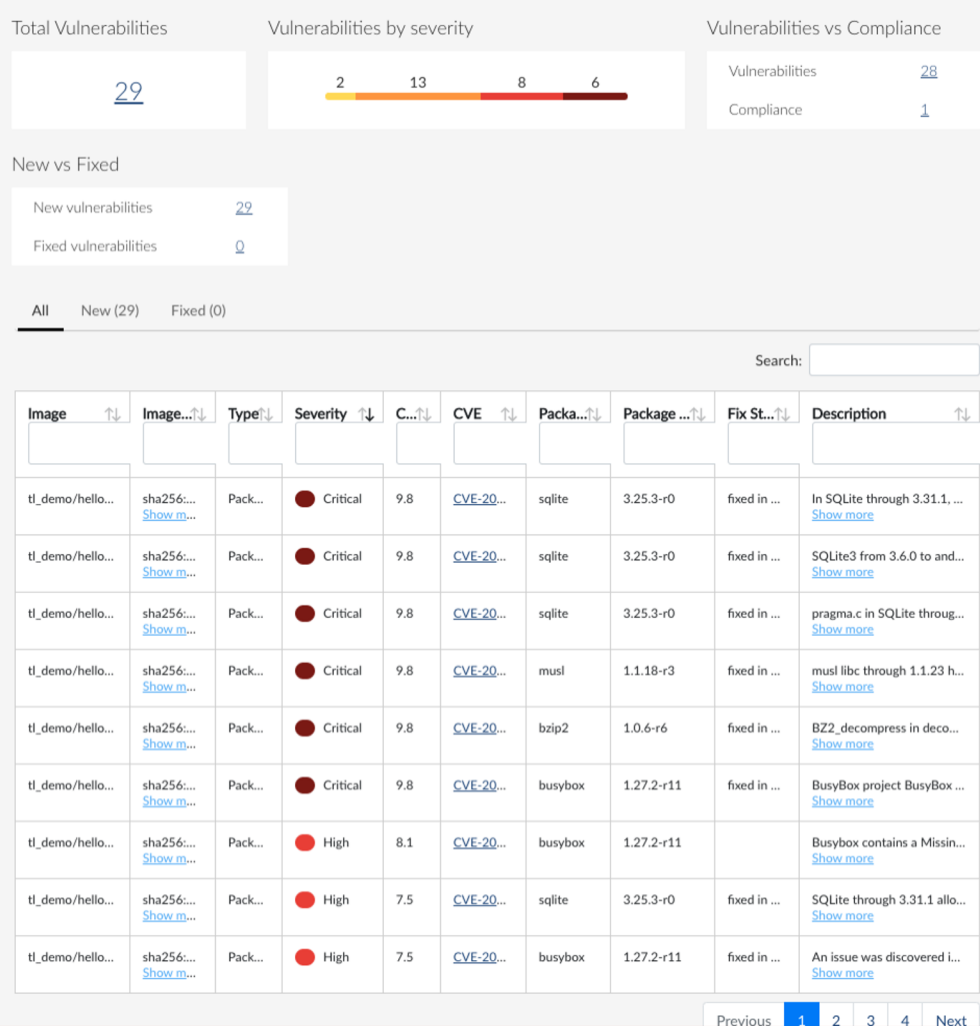
# Image and Function Scanning

Vulnerability and compliance scanning for container images and serverless zips

Support for developer desktops or CI workflows

Enforce pass / fail status, with centralized policy management, for full control over all builds

Integrations with CI tools:



# CD Security

Continuously monitor container registries and serverless repos

Set granular deployment rules to alert on or prevent vulnerability and compliance issues

Leverage powerful cloud native technologies, like Open Policy Agent integration

Integrations with notable registries:



Monitor / Vulnerabilities

Vulnerability ExplorerCode RepositoriesImagesHostsFunctionsCVE ViewerPCF Blobstore

Deployed ImagesRegistriesCI

Filter registries by keywords and attributes

Registry	Repository	Tag	Vulnerabilities	Risk Factors	Collections
	library/httpd	latest	31 1	6	
registry.infra.svc.clust...	alpine	latest	0	0	
registry.infra.svc.clust...	clockworksoul/zork1	latest	15 9 2	8	
registry.infra.svc.clust...	infra/my_jenkins	latest	69 8 19 7	10	
registry.infra.svc.clust...	infra/portal_httpd	latest	31 1		
registry.infra.svc.clust...	servethehome/moner...	latest	107 8		
registry.infra.svc.clust...	tl_demo/attacker-client	1	0		
registry.infra.svc.clust...	tl_demo/attacker-client	latest	0		
registry.infra.svc.clust...	tl_demo/hellonode	latest	6 6 5	7	
registry.infra.svc.clust...	tl_demo/hellonode	1	6 6 5	7	
registry.infra.svc.clust...	tl_demo/hellopython	1	2 13 7 6	8	
registry.infra.svc.clust...	tl_demo/hellopython	latest	2 13 7 6	8	
registry.infra.svc.clust...	tl_demo/struts2_demo	1	55 9 16 8	10	
registry.infra.svc.clust...	tl_demo/struts2_demo	2.3.37	55 7 8 1	10	
registry.infra.svc.clust...	tl_demo/struts2_demo	2.3.12	55 9 16 8	10	
registry.infra.svc.clust...	tl_demo/struts2_demo	latest	55 7 7	9	

High severity

Medium severity

Attack Complexity: Low

Recent vulnerability

Attack Vector: Network

DoS

Has fix



RUN

# Runtime Visibility

Prioritize risk and compliance with Top 10 lists, including Vendor Fix information, Risk Trees, Risk Profiles, and more

Integrate with common alerting, issue tracking, and remediation platforms

Integrations with Third-Party tools:



Monitor / Vulnerabilities

CVE-2020-10188 details

Description

utility.c in telnetd in netkit telnet through 0.17 allows remote attackers to execute arbitrary code via short writes or urgent data, because of a buffer overflow involving the netclear and nextitem functions.

Vendor fixed in 2:1.9.4-2+deb9u1

status

More CVE-2020-10188

info

Impacted packages

inetutils:2:1.9.4-2

Images (2)

Hosts (0)

Functions (0)

Search for image

1 container at high environmental risk

2 images 2.6% of all images

vulnerables/we... (image info, 1 container, 1 container at high risk)

dwaa (1 container)

app-embedded-cnaf... (image info, no containers)

Max risk profile

Images risk score 92

Environmental Risk Factors

3

No mandatory security profile applied

Reachable from the internet

Container is running as root

Listening ports

Running as privileged container

CVE Risk Factors

6

Attack Vector: Network

Attack Complexity: Low

Recent vulnerability

DoS

Critical severity

Remote execution

Legend: Image Namespace Container Host Function

Close

CVE-2018-100088 92 6 3 php-pear:1:1.10.1...

paloalto NETWORKS

# Visibility, Compliance and Governance

# Compliance Management

Continuous compliance posture monitoring  
and 1-click reporting

Comprehensive coverage (CIS, GDPR, HIPAA,  
ISO-27001, NIST-800, PCI-DSS, SOC 2, etc.)  
and support for custom reporting

Easily investigate and auto-remediate  
compliance violations



# Network Resource Query Language (RQL)

Gain security and operational insights about your deployments in public cloud environments.

Perform configuration checks on resources and query network events across different cloud platforms.

Turn queries into custom cloud agnostic policies and define remediation steps and compliance implications.

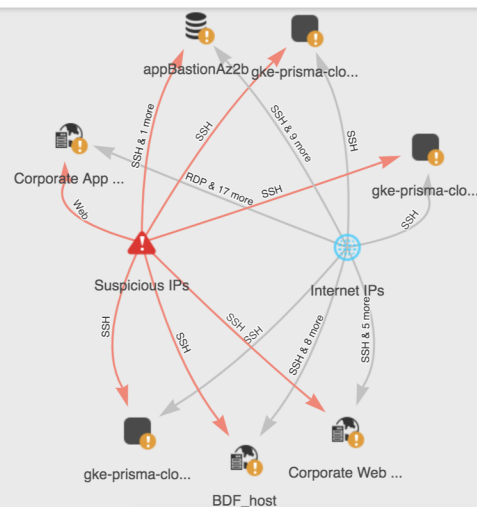
## Investigate

hosts w/ known vulnerabilities

✓ network where source.publicnetwork IN ( 'Internet IPs', 'Suspicious IPs' ) AND bytes > 0 AND dest.resource IN ( resource where hostfinding.type IN ( 'Vulnerability' ) ) |

AND

limit search records to

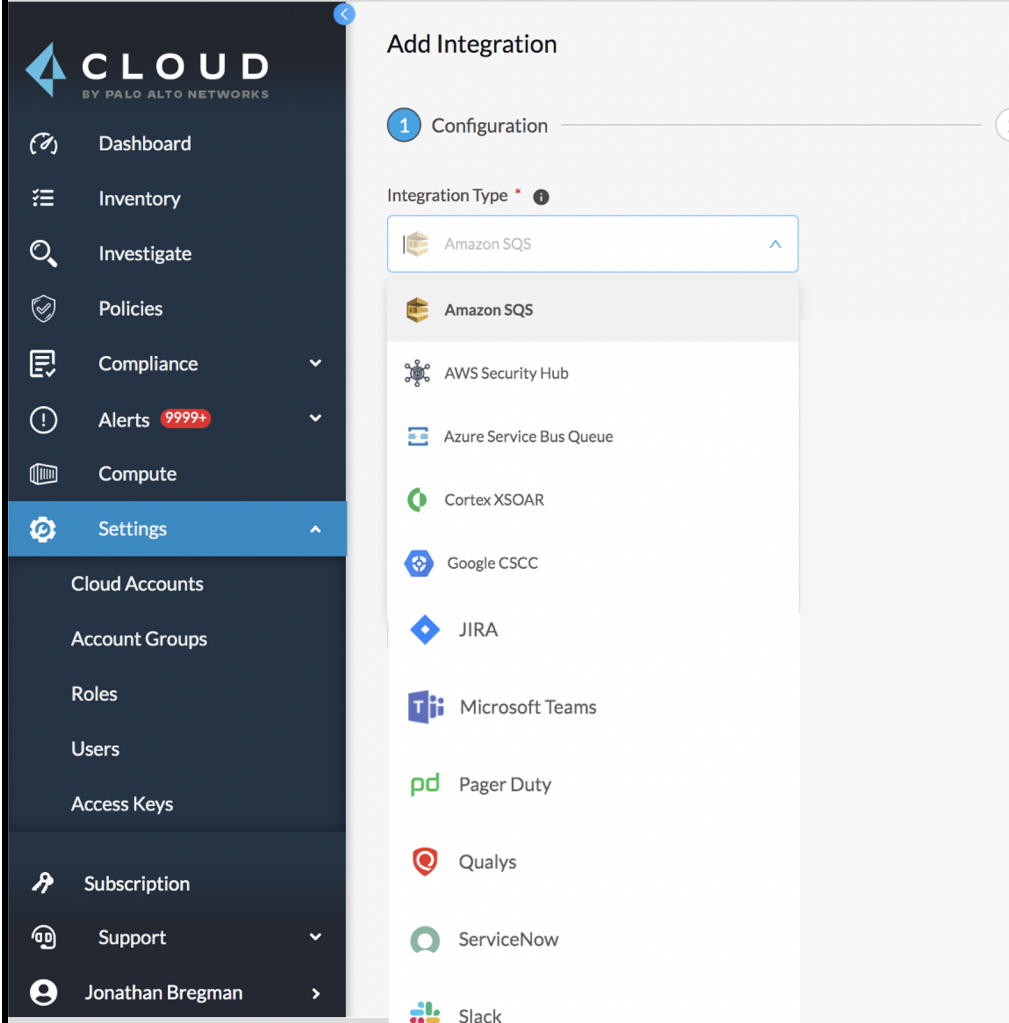


# Automated Remediation

Automatically resolve policy violations, such as misconfigured security groups within the Prisma Cloud console

Send alert notification to 14 third-party tools including email, Lambda, Security Hub, PagerDuty, ServiceNow or Slack

Integrate with SOAR tools including Cortex XSOAR for multi-step remediation playbooks




# Workload Protection

# Vulnerability Management

Industry leading precision across hosts, images, containers, and serverless functions

Automated prioritization of vulnerabilities based on your unique environment

Prevent running vulnerable software across your environment

 **postgres:10.6**

OS distributionDebian GNU/Linux 9 (stretch)

OS releasestretch

Digestsha256:1bd46192a12a1012d52f41186c83dc343b4b2d07ad9836fb37a08cdf22041537

VulnerabilitiesComplianceRuntimeLayersProcess infoPackage infoEnvironmentTrust groupsLab

25 Layers, Image Size: 229.6 MB

Filter layers by keywords and attributes

Details	Size	Vulnerabilities
ADD file:5a6d066ba71fb0a4789971... Feb 5, 2019 7:30:19 PM	55.3 MB	37 6 13 7
CMD ["bash"] Feb 5, 2019 7:30:19 PM	0 B	0
RUN set -ex; if ! command -v gpg > /d... Feb 6, 2019 12:14:57 AM	10.2 MB	6 5 29 1

Component	Version	Vulnerability	Severity
libidn	1.33-1	<a href="#">CVE-2017-14062</a>	critical
nettle	3.3-1	<a href="#">CVE-2021-3580</a>	high
openldap	2.4.44+dfsg-5+deb9u2	<a href="#">CVE-2021-27212</a>	high

```
RUN set -ex; if ! command -v
install -y --no-install-recon
/var/lib/apt/lists/*; fi
RUN set -eux; groupadd -r pos
--home-dir=/var/lib/postgres
/var/lib/postgresql; chown -R
ENV GOSU VERSION=1.11
RUN set -x && apt-get update
certificates wget && rm -rf /
/usr/local/bin/gosu
"https://github.com/tianon/g
print-architecture)" && wget
"https://github.com/tianon/g
print-architecture).asc" && e
keyserver ha.pool.sks-keyser
B42F6819007F00F88E364FD4036A
/usr/local/bin/gosu.asc /usr/
/dev/null && gpgconf --kill a
/usr/local/bin/gosu.asc && ch
apt-get purge -y --auto-remov
RUN set -eux; if [ -f /etc/dp
'/usr/share/locale' /etc/dpke
'\usr\share\locale\d' /et
```

# VM Image Scanning

Scan your images that are in your CSP accounts, including private Images or selected public/community images your application teams use

Integrate twistcli to scan for VM image vulnerabilities or compliance issues on developer desktop or in your CI/CD pipelines

LOUD

Defend / Vulnerabilities

?

+

+

Add new setting

Version

Amazon Machine Images (AMI)

▼

Console Address

127.0.0.1

⊗ ▼

Region

N. Virginia

▼

VM images

\* Specify a VM image ⓘ

Tags

\* Specify a tag

Excluded VM images

Add a VM image to exclude

Credential

▼

Use AWS STS

Off

Number of scanners

1

Cap

5

Cancel

Add

PRISMA CLOUD

Monitor / Vulnerabilities

?

+

+

Vulnerability Explorer

Images

Hosts

Functions

CVE Viewer

PCF Blobstore

Running Hosts

VM Images

Filter VM Images

Collections

Image Name	Distribution	Release	Region	AWS Tags	Vulnerabilities	Risk Factors	Collections
ubuntu-1604-vm-circlci-classic-fixap-157...	Ubuntu 16.04.5 LTS	xenial	us-east-1		112 315 12	1	
bitnami-ghabricator-2018.47-0-linux-debia...	Debian GNU/Linux 9 (stretch)	stretch	us-east-1		292 153 162 37	15	



# Web Application and API Security

Auto-discover unprotected web apps and APIs

OWASP Top 10 security, API Protection, File Upload Protection, Location-based Access Control and more; all integrated with our Cloud Workload Protection capabilities

Fully-configurable protection for each application

Ability to inspect and protect east-west API traffic within cloud-native clusters

## Edit dvwdemo

App definition **App firewall** DoS protection Access control Bot protection Custom rules Advanced settings

1 Ban is applied by client IP

### Firewall settings

Protection	Mode	Exceptions
SQL Injection	Disable Alert Prevent Ban	
Cross-Site Scripting (XSS)	Disable Alert Prevent Ban	
OS Command Injection	Disable Alert Prevent Ban	
Code Injection	Disable Alert Prevent Ban	
Local File Inclusion	Disable Alert Prevent Ban	
Attack Tools & Vulnerability Scanners	Disable Alert Prevent Ban	
Shellshock	Disable Alert Prevent Ban	
Malformed HTTP Request	Disable Alert Prevent Ban	
Prisma Cloud Advanced Threat Protection	Disable Alert Prevent Ban	
Detect Information Leakage	Disable Alert Prevent Ban	
Cross Site Request Forgery Protection	On	
Clickjacking Prevention	On	
Remove Server Fingerprints	On	

# Access Control

Central monitoring of docker, sshd, and sudo events

Secrets management integrated with all popular providers

Real-time stream processing of Kubernetes AuditSink and security with Open Policy Agent (OPA)

## Kubernetes audit details

Time	Apr 21, 2021 12:58:46 PM				
Message	Pod created without security context				
Verb	create				
Resources	Pods				
Request URI	/api/v1/namespaces/struts-demo/pods				
Authorization Info	["authorization.k8s.io/decision": "allow", "authorization.k8s.io/reason": "RBAC: allowed by ClusterRoleBinding \"/>tr> <tr><td>Account</td><td>["username": "system:serviceaccount:kube-system:replicaset-controller", "uid": "fcdc2ed8-3ef7-4665-923e-a869e1689da2", "groups": ["system:serviceaccounts", "system:serviceaccounts:kube-system", "system:authenticated"]]</td></tr> <tr><td>Source IPs</td><td>["10.128.1.29"]</td></tr>	Account	["username": "system:serviceaccount:kube-system:replicaset-controller", "uid": "fcdc2ed8-3ef7-4665-923e-a869e1689da2", "groups": ["system:serviceaccounts", "system:serviceaccounts:kube-system", "system:authenticated"]]	Source IPs	["10.128.1.29"]
Account	["username": "system:serviceaccount:kube-system:replicaset-controller", "uid": "fcdc2ed8-3ef7-4665-923e-a869e1689da2", "groups": ["system:serviceaccounts", "system:serviceaccounts:kube-system", "system:authenticated"]]				
Source IPs	["10.128.1.29"]				

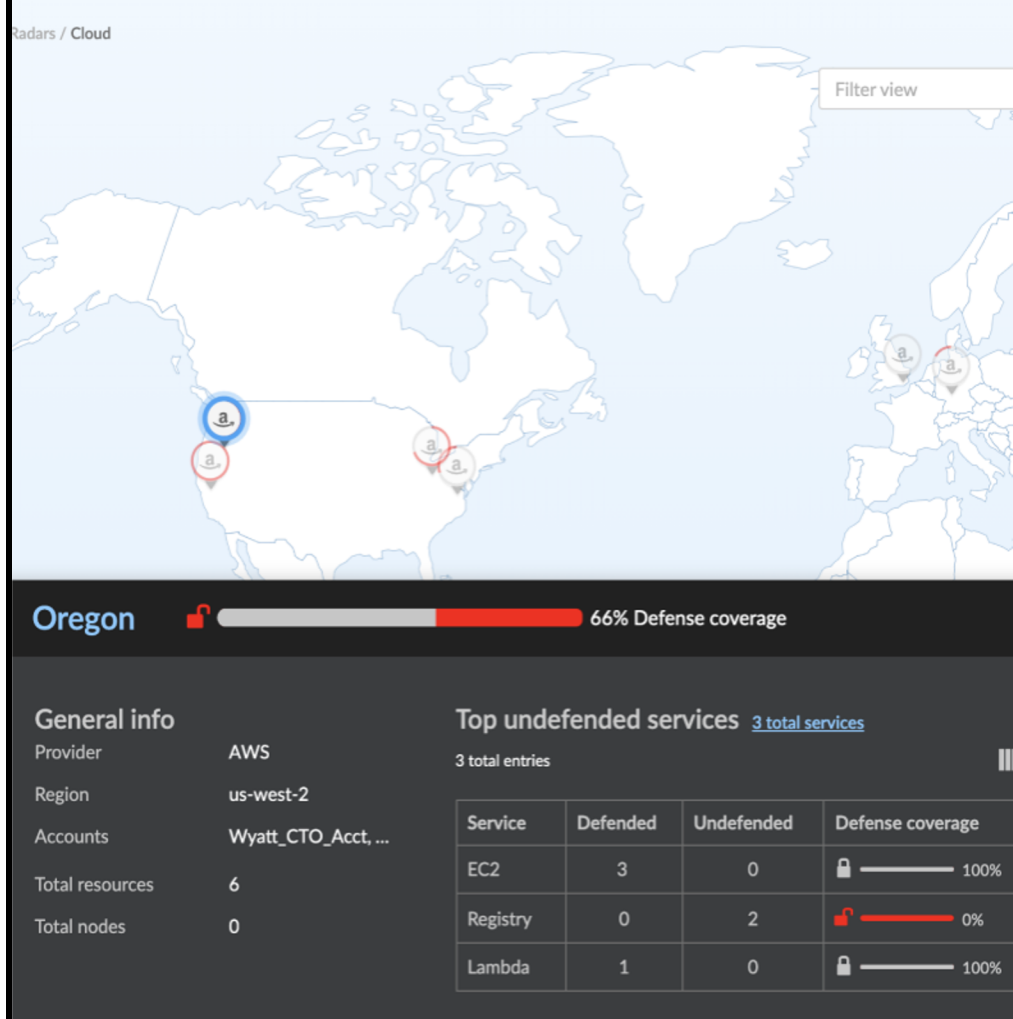
Event blob	<pre>{   "annotations": {     "authorization.k8s.io/decision": "allow",     "authorization.k8s.io/reason": "RBAC: allowed by ClusterRoleBinding \"/&gt;tr&gt;</pre>
------------	---

Close

# Auto-Discovery and Defense

Discover virtual machines/instances in your cloud accounts and automatically protect.

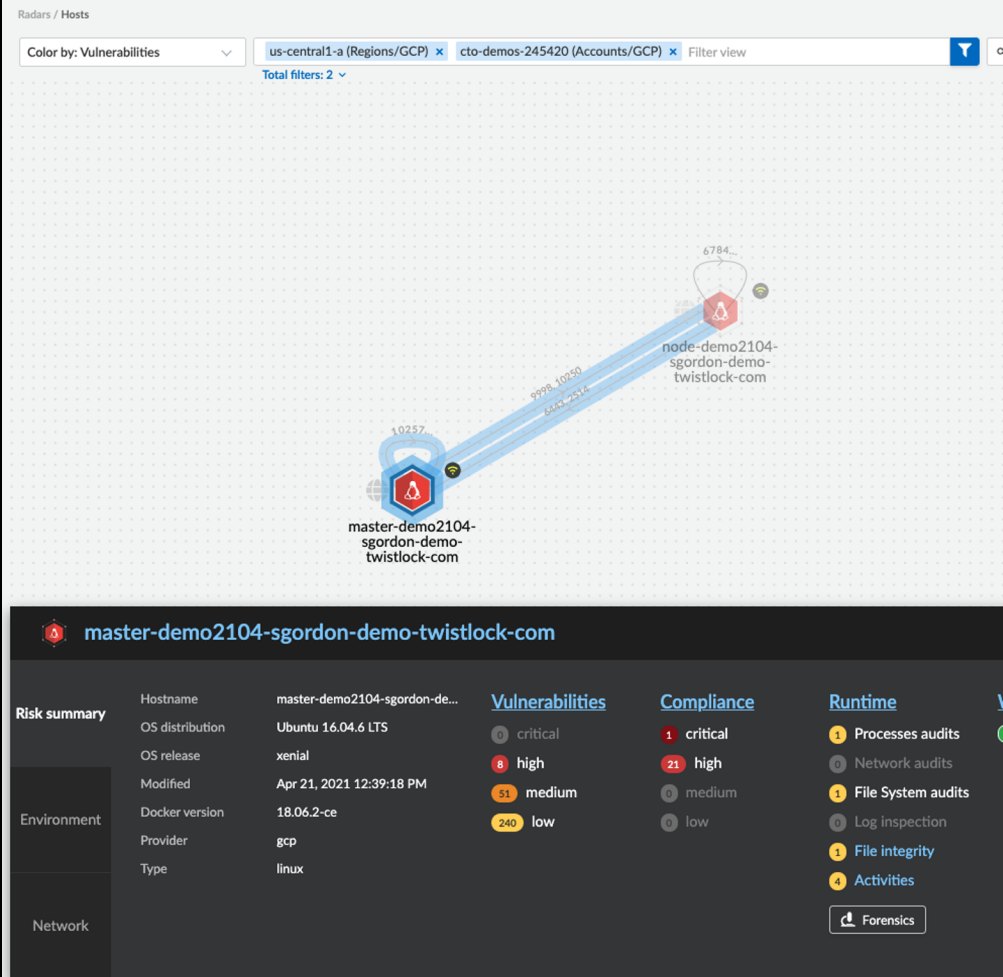
Gain visibility into all your assets enable granular controls to deploy agents which enable full security across virtual machines in AWS, Google Cloud, and Azure VMs



# Network Visibility

Real-time mapping of host network traffic flows

See vulnerability, compliance, and runtime status with a single-click from Radar



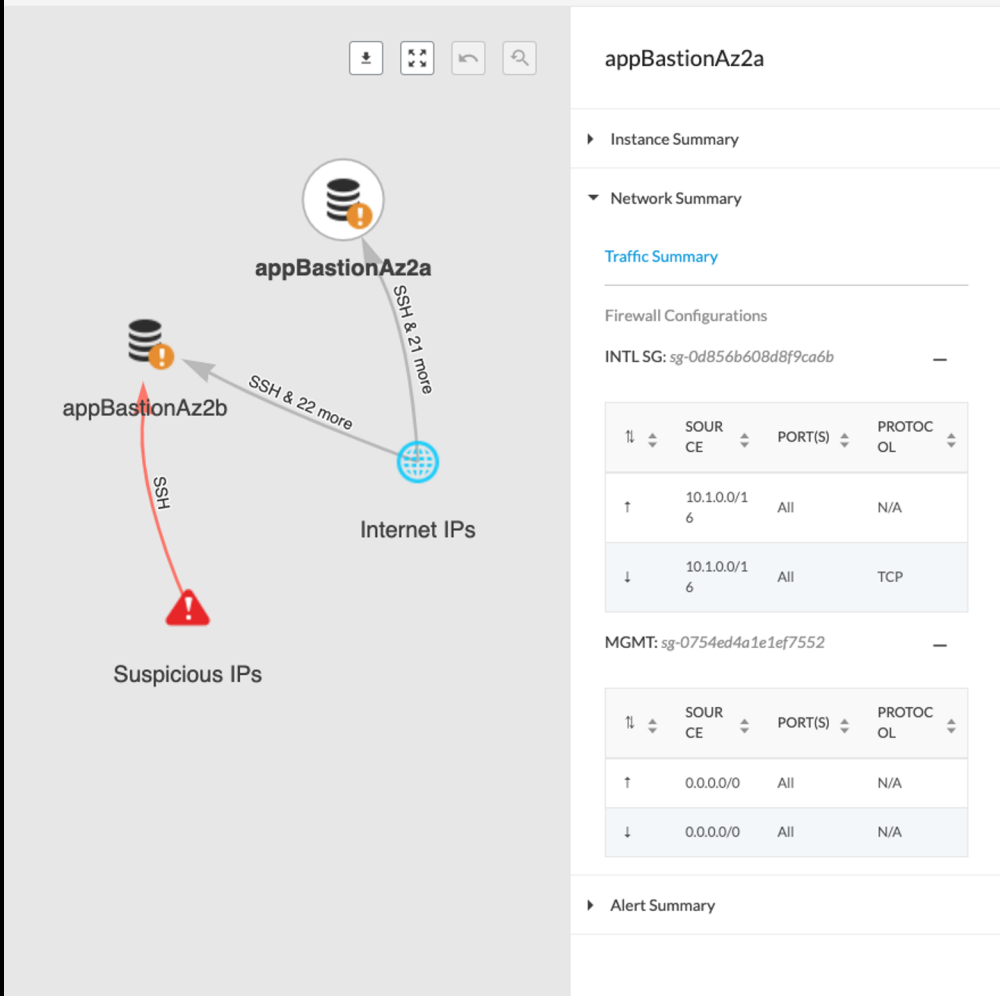
# Threat Detection

# Network Anomaly Detection

Over 500B+ flow logs ingested weekly to pinpoint unusual network activities

Classify and view detailed information on suspicious IPs and investigate affected resources with powerful visualizations

Detect port scan or port sweep activities that probe a server or host for open ports




















# Network Data Exfiltration Activity Detection

Use unsupervised ML to learn normal traffic pattern of each VM

Identify combination of anomalous egress activity & traffic to known TOR exit nodes

Detect data exfiltration

Policy Name ↕	Policy Type ↕
Anomalous compute provisioning activity	 Anomaly
Cryptominer activity (Internal)	 Anomaly
Loader activity (External)	 Anomaly
Cryptominer activity (External)	 Anomaly
Wiper activity (External)	 Anomaly
Webshell activity (External)	 Anomaly
Port scan activity (External)	 Anomaly
Linux Malware activity (Internal)	 Anomaly
Dropper activity (Internal)	 Anomaly
Exploit Kit activity (Internal)	 Anomaly
Backdoor activity (External)	 Anomaly
Worm activity (External)	 Anomaly
InfoStealer activity (Internal)	 Anomaly
Backdoor activity (Internal)	 Anomaly
DDoS activity (Internal)	 Anomaly
Dropper activity (External)	 Anomaly
Hacking Tool activity (External)	 Anomaly

# True Internet Exposure

Multi-dimensional approach to identifying overly exposed resources and provides end-to-end network path visibility from ANY source to ANY destination

Correlates multiple data points, including routing table configurations, to determine true network reachability

Vastly reduces alert fatigue by delivering high fidelity alerts and help customers to take meaningful action

## Investigate

config from network-analyzer where source.publicnetwork = INTERNET AND dest.instance.id = ANY and dest.protocol = TCP and dest.port

Show additional filters

My Recent Searches

My Saved Searches

All Saved Searches

Search Results

10 results View as

Table

Graph

Source	Destination		
Public Network	Resource Name	Account	VPC
internet	EC2-x	my-accloud-1	my-vpc-1
internet	EC2-y	my-accloud-1	my-vpc-1
internet	EC2-c	my-accloud-1	my-vpc-1
internet	EC2-b	my-accloud-1	my-vpc-1
internet	EC2-a	my-accloud-1	my-vpc-1

Network Path Analysis

Overview

Network Logs

Destination

Source

i-Of4aeb

eni-02e4

sg-0bd2

acl-0747

rtb-0575

igw-08d

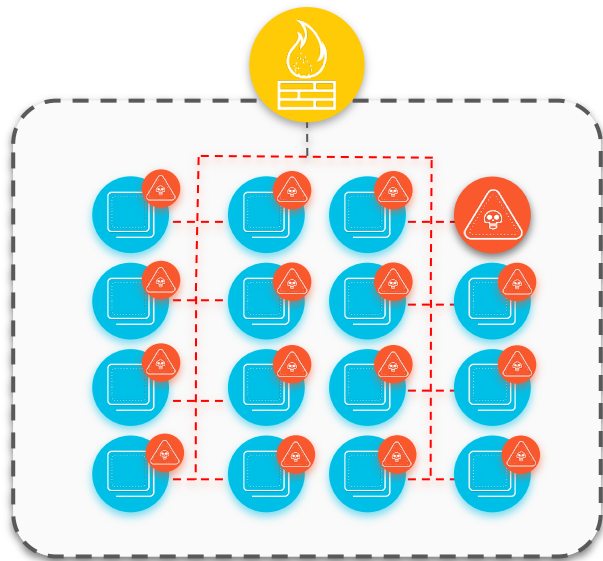
internet



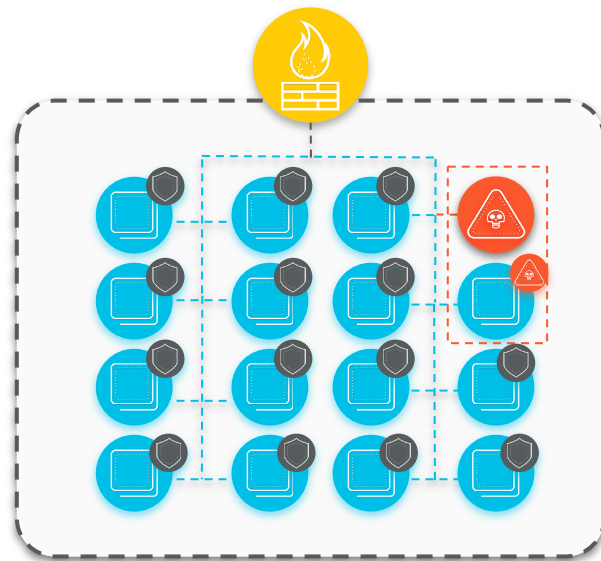
# Identity-Based Micro Segmentation

Micro Segmentation for hosts and containers in any cloud

# What happens *when* a breach occurs?

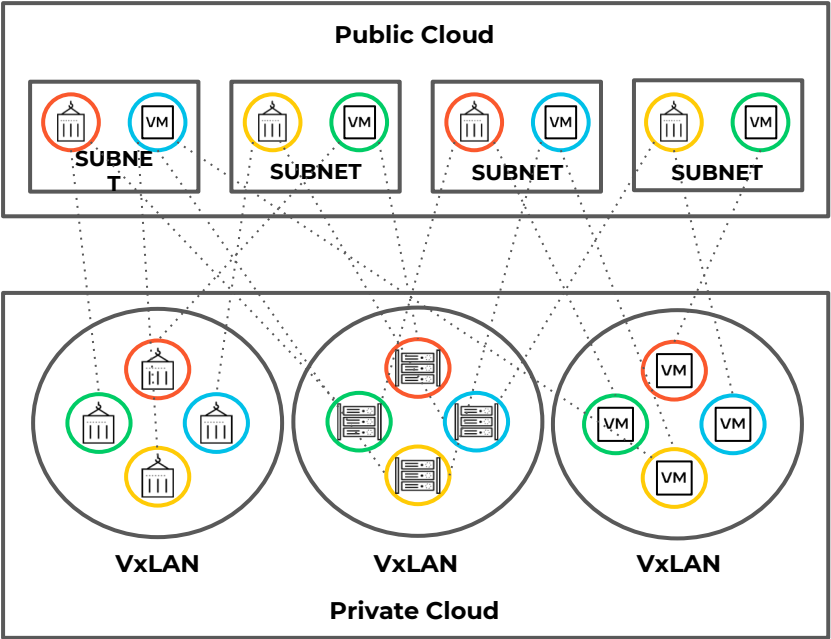


Without Identity-Based  
Microsegmentation



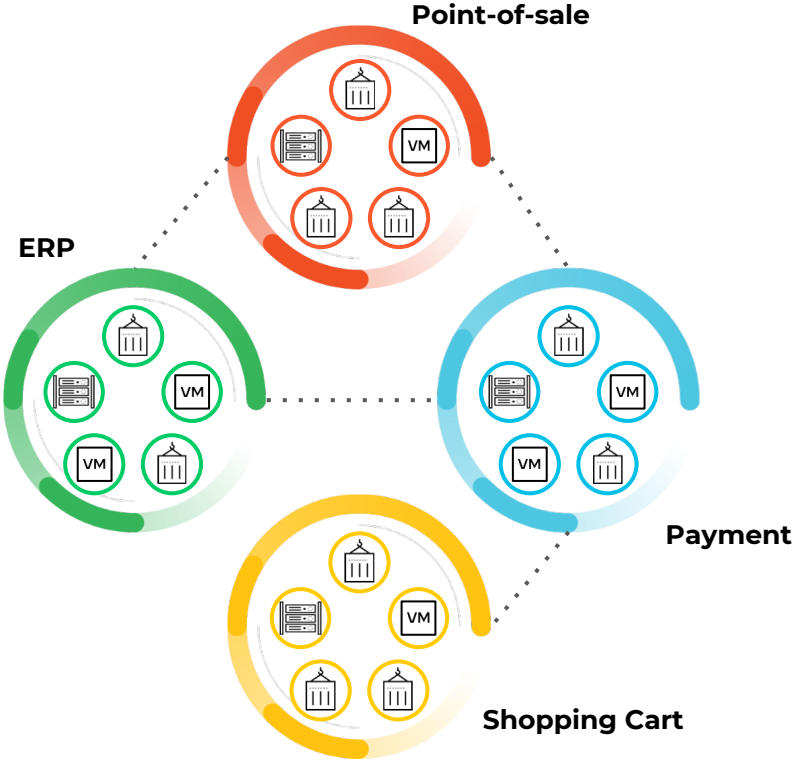
Identity-Based  
Microsegmentation

# Network Segmentation is Insufficient



Applications: ■ Point-of-sale ■ Payment app ■ Shopping Cart ■ ERP App

**What the network delivers**



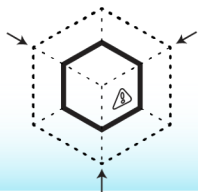
**What security needs**

# How Customers Use Identity-Based Micro Segmentation



## Application Flow Visibility

See how applications communicate



## Zero Trust Segmentation

Segment critical applications for protection and compliance



## Automate NetSec Workflows

Protect new applications without hindering developer workflows



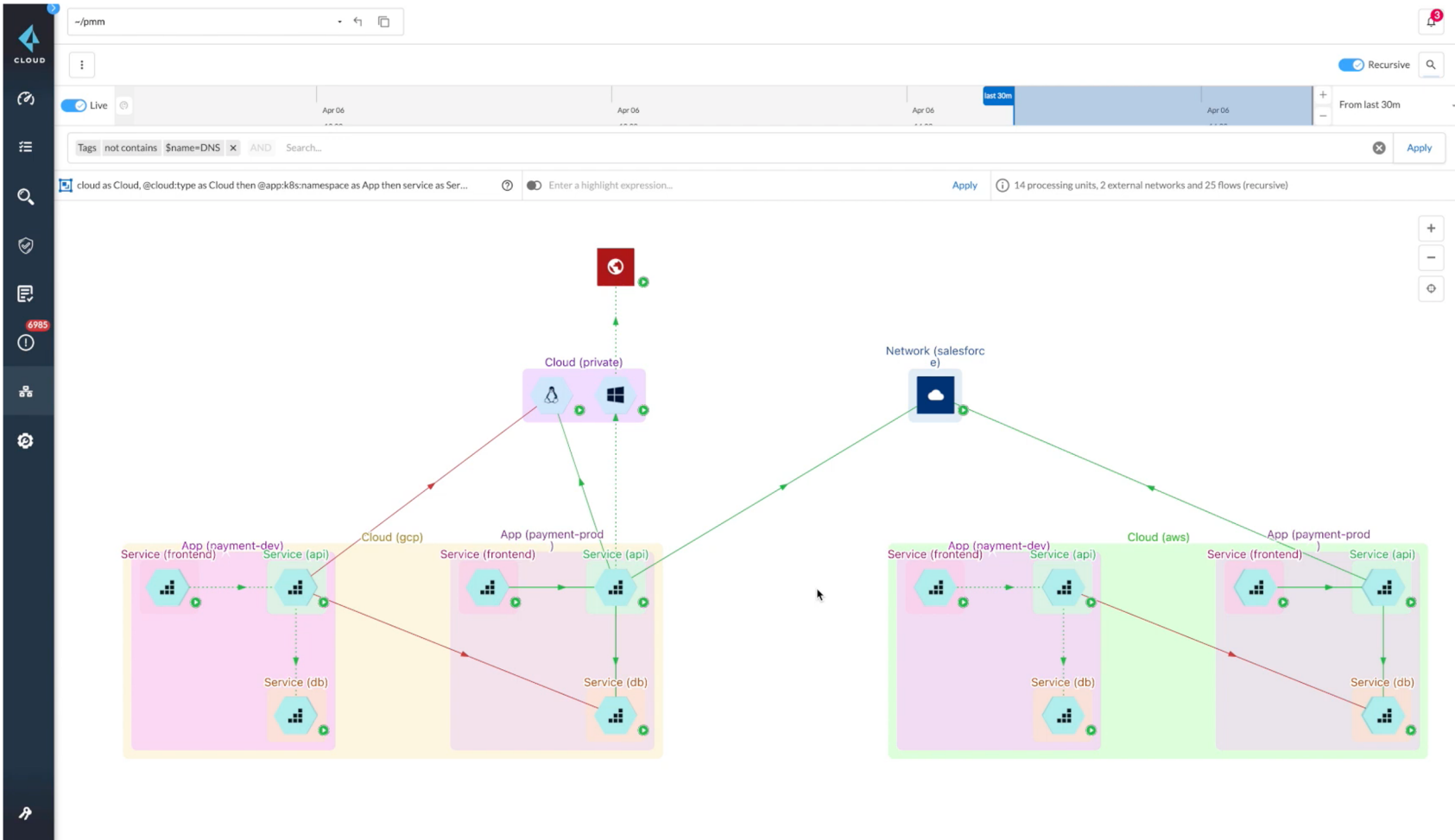
## Secure Hosts and Containers

Unify host and container network security with a single platform



## Secure Hybrid and Multi-Cloud

Protect cloud migrations, new clouds, and multi-cloud with consolidated network security



# Thank you

