PingSafe

PingSafe the only cloud security platform
powered by attacker’s intelligence

Team

Our team is dedicated to revolutionize Cloud Security

- Top **5 White Hat Hackers** in bug bounty programs of Meta Uber Twitter LinkedIn salesforce
- Forbes **'Asia 30 under 30'**, 2017 - Enterprise Tech.
- Top ranked Security Researcher. Participated in Bug bounty programs of more than **400+ global companies**.

Anand Prakash

Founder, CEO

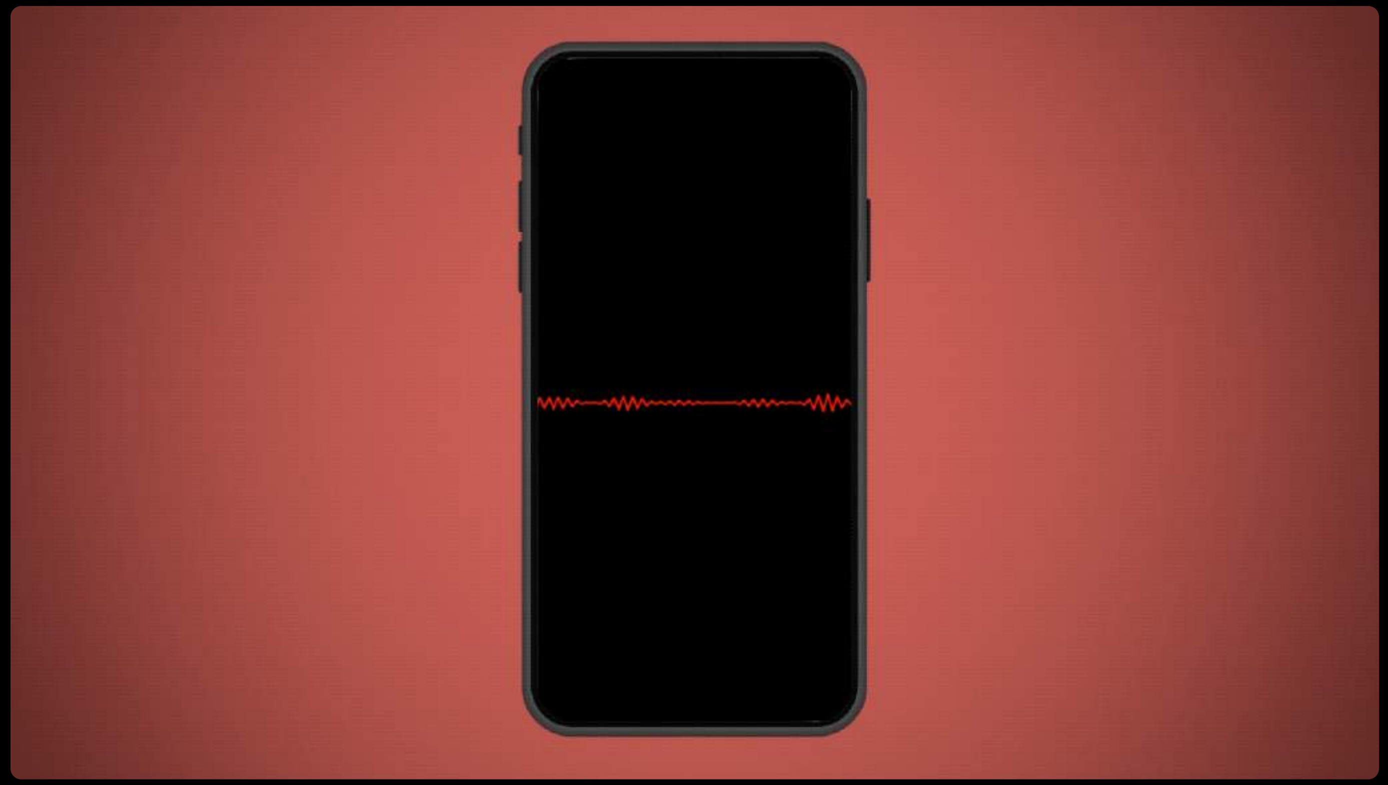
- An **IIT Dhanbad** alumnus and part of the early team at PhonePe
- Experience of building **modern cloud-native platforms** at a massive scale.
- Headed multiple platforms to build a smooth payment experience for users and merchants, which ranged from street vendors to MNCs.

Nishant Mittal

Founder, CPTO

News

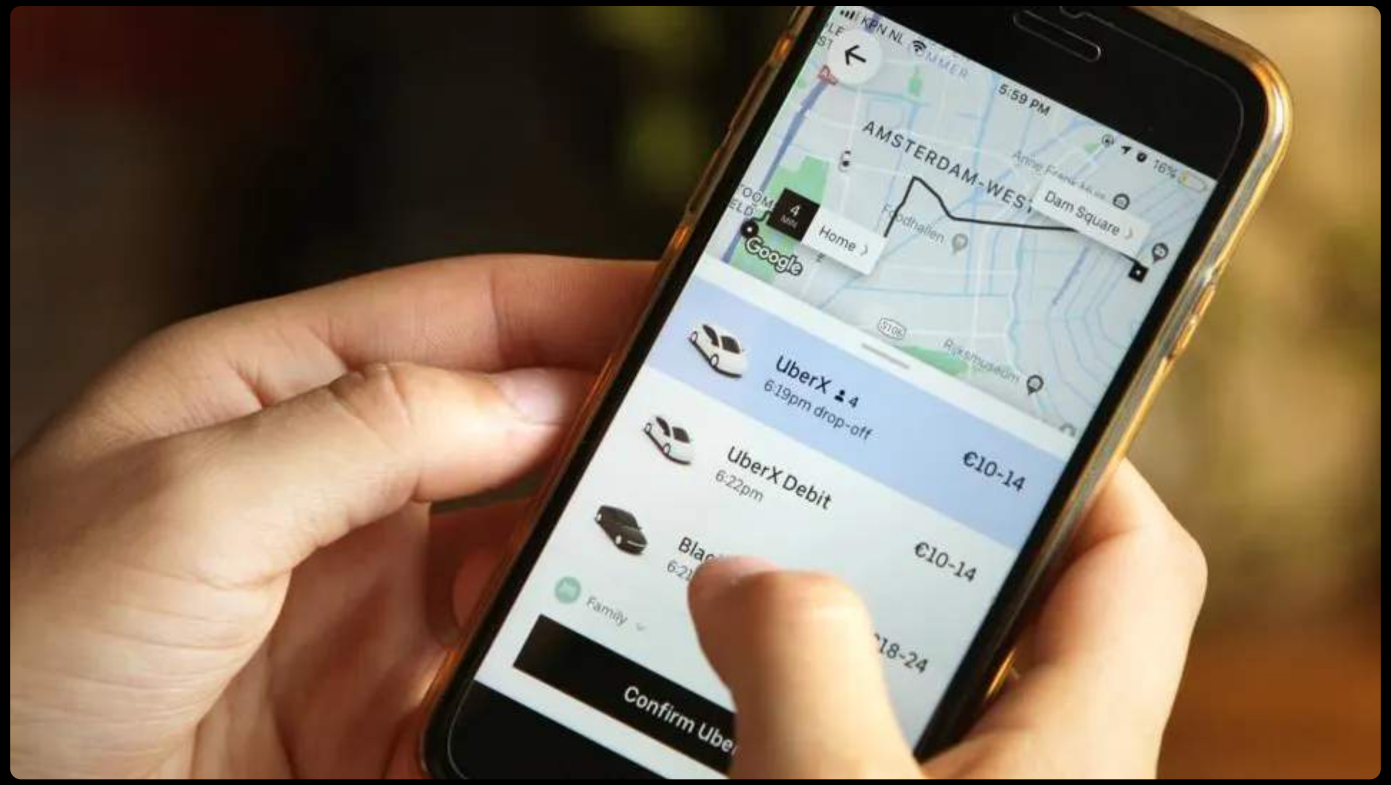
In the News



TechCrunch

A bug in a popular iPhone app exposed thousands of call recordings

Read Article →



Forbes

Uber Confirms Account Takeover Vulnerability Found By Forbes 30 Under 30 Honoree

Read Article →

GIZMODO

Researcher Found Another Twitter Vulnerability That Allowed Tweeting From Any Account

Read Article →

Problem

Gaps in current offerings:

Increasing cloud security challenges

- Complex infrastructure
- Sophisticated external threats

+

Defensive approach to security by current players

- Lack of context
- Lack of proof of exploitability

= A need for **more modern holistic approach** to put an end to these challenges

Solution

Modernize Cloud Security. Outsmart Attackers.

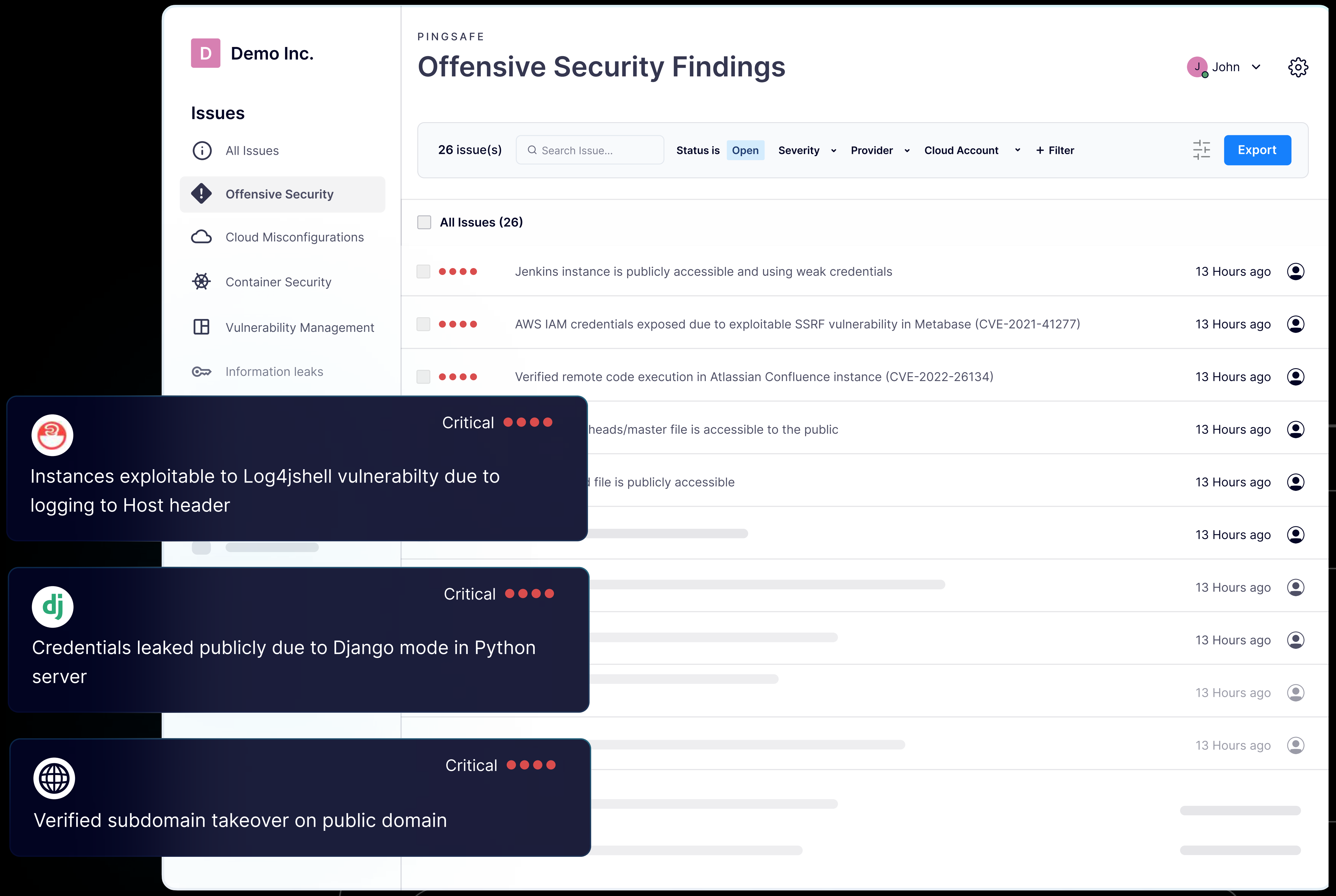
Choose **unparalleled protection** for your multi-cloud infrastructure, from **development to deployment.**

Multi-Cloud Environment Support:

aws   Google Cloud   DigitalOcean

Azure   Oracle Cloud   Alibaba Cloud

#1 CNAPP Platform on



D Demo Inc.

Issues

- All Issues
- Offensive Security
- Cloud Misconfigurations
- Container Security
- Vulnerability Management
- Information leaks

PINGSAFE

Offensive Security Findings

John

26 issue(s)   Search Issue...   Status is Open   Severity   Provider   Cloud Account   + Filter   Export

□ All Issues (26)

□ ●●●●	Jenkins instance is publicly accessible and using weak credentials	13 Hours ago
□ ●●●●	AWS IAM credentials exposed due to exploitable SSRF vulnerability in Metabase (CVE-2021-41277)	13 Hours ago
□ ●●●●	Verified remote code execution in Atlassian Confluence instance (CVE-2022-26134)	13 Hours ago
	heads/master file is accessible to the public	13 Hours ago
	file is publicly accessible	13 Hours ago
		13 Hours ago
		13 Hours ago
		13 Hours ago
		13 Hours ago
		13 Hours ago

Critical ●●●●

Instances exploitable to Log4jshell vulnerabilty due to logging to Host header

Critical ●●●●

Credentials leaked publicly due to Django mode in Python server

Critical ●●●●

Verified subdomain takeover on public domain

Solution

Impact of PingSafe

$400-500k
Average annualized Savings*

>85%
Reduced False Positives

1500
Monthly Developer Hours Saved**

89%
MTTR Reduction**

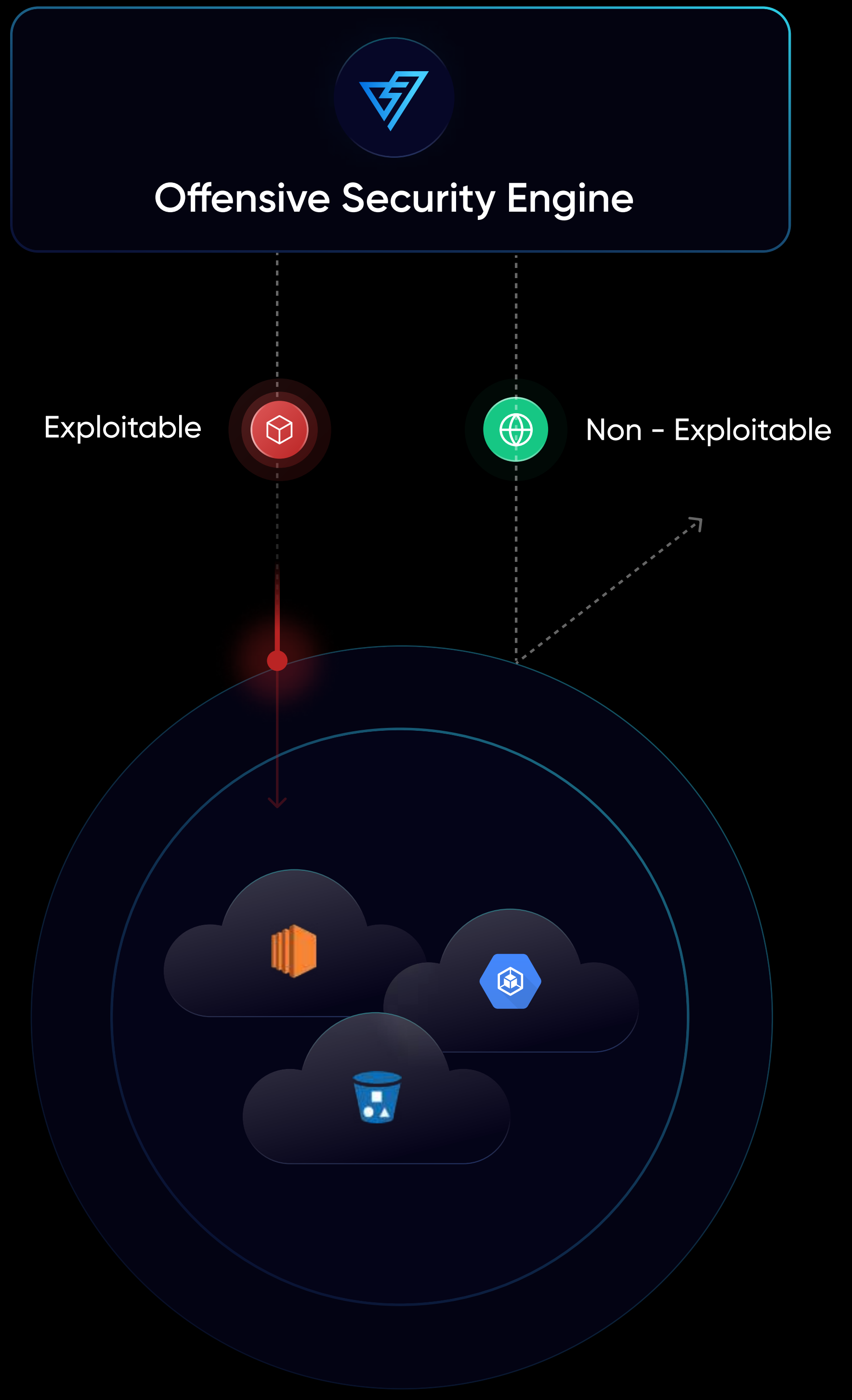
97%
MTTD Reduction**

* Includes tool consolidation, bug bounty cost reduction and reduced security team size

** For a 15-member security team based on average time saved

Solution

How Does PingSafe work?



Fast and Agentless Onboarding

Instant and seamless onboarding across AWS, GCP, Azure, OCI and DigitalOcean with auto detection of incrementally added accounts.

Discovering Cloud & Beyond

Monitor all cloud resources - VMs , databases, container workloads, & serverless resources, etc. along with events occuring outside the cloud.

Context Establishment

PingSafe understands complex relationships between the cloud assets and external events.

Attack Paths

The platform identifies all potential attack paths by triaging resources which are exposed to external threats.

Proof of Exploitability

PingSafe automatically simulates attacks on the discovered attack paths to eliminate false positives and highlight truly exploitable vulnerabilities.

Real-Time Alerts & Auto-Remediation

Automate alerting workflows across JIRA, Slack, PagerDuty, Sumo Logic, Splunk, OpsGenie & email along with real time auto remediation of misconfigurations

Use Cases

PingSafe's Offensive Security Engine lets you focus on the actual exploitable threats

Cloud Misconfiguration	✓ 1500+ Policies	✓ Custom Policies	✓ Context Awareness	AWS GCP Azure DigitalOcean Oracle Cloud (Beta)
Container & Kubernetes Security	✓ Misconfigurations	✓ RBAC Visualization	✓ Custom Policies	EKS GKE AKS Self Managed (Beta)
Compliance Monitoring	PCI & CIS. NIST ISO 27001 AICPA SOC 2 CSA CCM			+ many more
IaC Scanning	✓ 700+ Policies ✓ VCS Integration	✓ Custom Policies ✓ CI/CD Integration	✓ Context Awareness	Terraform CloudFormation Helm

Secret Scanning

- ✓ 900+ Secrets
- ✓ Secret Validation
- ✓ Private Repo Scanning
- ✓ Developer Repo Scanning
- ✓ Open Secret Scanning
- ✓ CI/CD Integration
- ✓ VCS Integration

Pre-commit Hook · Github · Gitlab · Bitbucket

Cloud Detection & Response

- ✓ Real time detection
- ✓ In-built Policies
- ✓ Custom Policies

AWS CloudTrail · GCP Audit Logs · Azure Activity Logs

Offensive Security Engine

- ✓ Simulation of exploitable vulnerability
- ✓ Proof of concept generation

Cloud Vulnerability Management

- ✓ Container Vulnerability
- ✓ Snapshot Scanning
- ✓ PingSafe Exclave Beta

AWS · GCP · Azure

Integratons

PingSafe has integrations into security ecosystem to enable repeatable process creation for teams

Cloud Providers

- AWS Cloud
- Google Cloud Platform
- Azure
- DigitalOcean
- Beta Oracle Cloud
- Alibaba Cloud

Container Registry

- ECR (AWS)
- GCR (GCP)
- Azure Registry
- SonaType Nexus
- Docker Hub
- JFrog Artifactory
- Harbor

Container Orchestrators

- ECS
- EKS
- GKE
- AKS
- Beta Self Managed

Version Control

- Github
- Github Enterprise
- Gitlab
- Gitlab Server
- Bitbucket Cloud

CI/CD & Git Hooks

- Pre-commit Hook
- Github Action
- Gitlab Pipeline
- Bitbucket Pipeline
- PingSafe CLI

Alerting

- Email
- Jira
- Slack
- QRadar
- OpsGenie
- PagerDuty
- Webhook
- AWS SQS

Traction

Clients across multiple geographies and verticals

Walmart
Flipkart
skyflow
belvilla
stripe
recko
PhonePe

halodoc
Razorpay
Osmo
WADHWANI AI
zepto
epic!

GeoGebra
Groww
bidgely
envoy
policybazaar.com
dash

zamp
OYO
TATA 1mg
TYNKER
slice
ixigo

Investors

Backed by the best

SEQUOIA SURGE

General Stanley A. McChrystal

United States Army

Rahul Chari

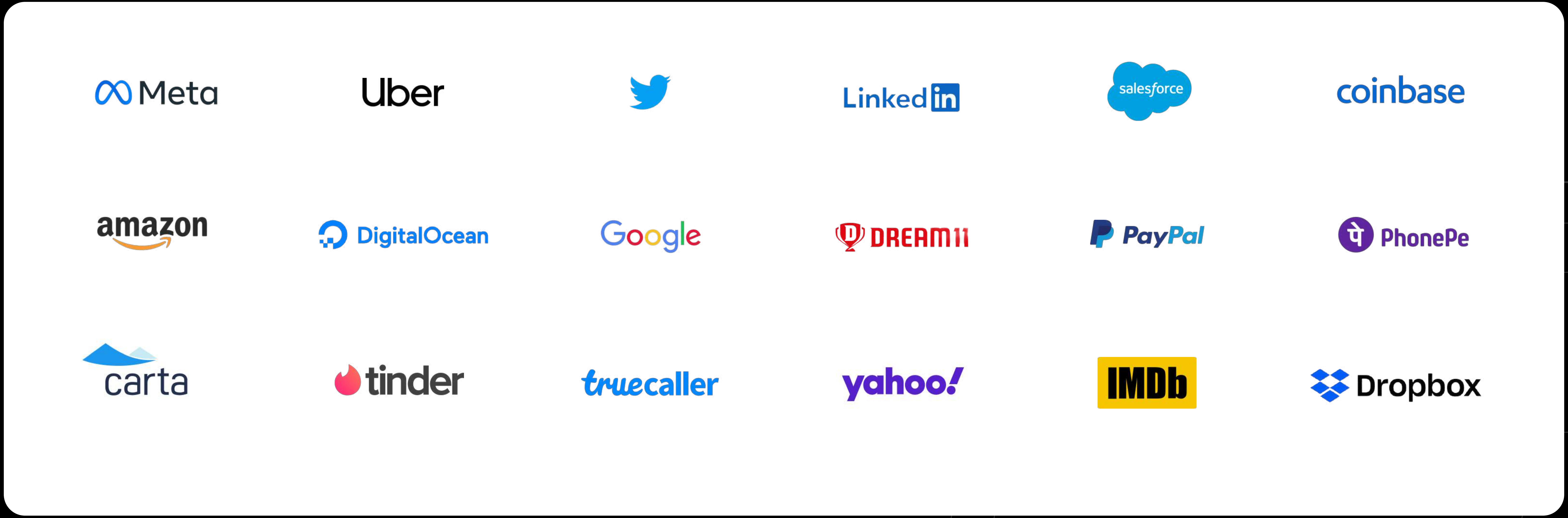
Founder & CTO, PhonePe

Neeraj Arora

Ex-CBO

Traction

PingSafe's team has secured leading enterprise companies across the globe



Client Testimonial

Clients perceive PingSafe as a long term security partner

envoy

"PingSafe is an excellent solution for dynamic and real-time monitoring of all the multi-cloud workloads. The flexibility of configuration and the ease of maintenance is a big plus."

skyflow

"PingSafe's CNAPP platform is significantly less noisy and its alerts are more actionable as compared to alternatives. With its exceptional customer support and differentiators like secret scanning capabilities, PingSafe is poised to be an integral part of our security landscape for the coming future."

stripe recko

"PingSafe has solved a big problem for us by organising everything around cloud monitoring and data leak protection in a single product. Our security team loves the fact that it lets them focus on what's important."

Market Validation

PingSafe is the Leading CNAPP platform according to G2

G2
Best ROI
SPRING
2023
G2
Leader
SPRING
2023
G2
Easiest To Use
WINTER
2023

Marketplace

We are available on

aws marketplace

Google Cloud Marketplace

Microsoft Azure
MARKETPLACE

Compliance

Your business is safe with us

ISO/IEC 27001

Information Security Management

SOC 2 TYPE II

Certified

PingSafe

www.pingsafe.com