PINGSAFE

Technology Solutions Overview

Build Your Business on Secure Clouds

Digital Transformation is bringing exciting opportunities to your company but also exposing it to new security risks. There are new vulnerabilities, new regulations, new tools appearing all the time. PingSafe can guide your company through all of it.

Why Cloud Security?

Data breaches can occur for a number of reasons, including accidentally, but targeted attacks occur because of exploiting system vulnerabilities; o software can also create a hole that allows an attacker to sneak malware onto a computer and steal data. For example, a privilege escalation flaw uncovered could allow attackers to steal sensitive data, inject malicious code, and bring down production apps and services.

Moreover, researchers have pointed out how Docker containers are becoming a prime target for cryptojackers at a time when fraudulent Cryptocurrency mining is a lucrative business. Similarly, ransomware variants have also been reported by some companies where victims have been locked out, files and drives often encrypted, and in some cases, backups, too in order to extort a payment from the user.

There have also been reports of a Software company exposing millions of data records upon failing to secure its cloud instances because of a Leaky AWS S3 bucket at the center of a data breach. Thus all these examples very well emphasize the need for a cloud security service that helps prevent data breaches.

PingSafe Cloud Security

Digital Transformation brings new opportunities to your company but also exposing it to new security risks as well. New vulnerabilities, new regulations, and new tools appear all the time. PingSafe can guide your company through all of it.

PingSafe assists companies in detecting data leakages occurring due to Cloud Security misconfigurations. This integrated platform has been built by analyzing the root causes of thousands of data breaches. It detects security risks and helps prevent data breaches because of the public cloud (Azure, AWS, GCP, and Alibaba). This eradicates

the need to deploy and maintain multiple tools such as cloud vulnerability management, workload protection, and security posture management solutions.

Features

- End-To-End Security Governance and Cloud Compliance.
- Analysis and Management of Inventory & Assets.
- In-depth scans rather than just configuration checks.
- Generation of valid alerts and zero false positives.
- Vulnerability Identification and Patch Deployment.
- Cloud Credentials Leakage Monitoring.

Technology Solution Platforms

AWS Security

AWS Security

PingSafe allows organizations to gain visibility into security and compliance posture, eliminate AWS misconfiguration with drift detection and context-aware guardrails, and enable security automation with CI/CD integration and pre-deployment policy compliance checks.

- PingSafe AI carries out in-depth scans rather than just configuring checks like other CSPM solutions in the market.
- It scans containers, dockers, configurations, servers deployed across the company's network in AWS to figure out any data leaks happening because of misconfigurations.
- Scans public Github repositories for data leakage of your AWS cloud credentials and your source code.
- Covers public cloud governance and the latest compliances such as PCI DSS, HIPAA, and CIS etc.
- Gives complete visibility into your environment from a hacker's/ bug bounty perspective.
- Using PingSafe reduces vulnerabilities that white hat hackers discover in bug bounties related to infrastructure.

Services Covered in AWS

- Security groups (removal of false positives)
- Data storage
- Public assets
- Subdomains
- IP address
- ELBs
- Databases
- Containers
- Dockers
- Grafana
- Kibana
- RabbitMQ

Increase Visibility
Gain Visualization of AWS compliance with PingSafe's powerful diagramming and reporting tools

Misconfiguration Elimination
Facilitate comprehensive drift detection for critical resources

Security Integration
Develop AWS security and compliance into the development lifecycle with PingSafe's API and IaC Checks

Shared Responsibility- Security and Compliance
Cloud Security and compliance is a joint responsibility between the organization and AWS, the CSP (Cloud Service Provider). AWS is responsible for protecting the infrastructure running all the services offered in the cloud, including the hardware, software, networking, and facilities that run the cloud services. The organization is responsible for any data, applications, operating systems, and resource configurations that run on CSP's infrastructure.

Signup for a Free Trial

Technology Solution Platforms

GCP Security

GCP Security

PingSafe allows organizations to gain visibility into security and compliance posture, assure continuous compliance, and enable security automation with CI/CD integration and pre-deployment policy compliance checks.

- PingSafe's Google Cloud Platform (GCP) security provides excellent disaster recovery plans.
- It monitors logs of cloud activity.
- PingSafe uses Identity Access Management (IAM) tools.
- It also helps organizations gain high visibility into their security and compliance posture of the cloud environment.
- PingSafe assures continuous compliance and enables security automation with CI/CD integration and pre-deployment policy compliance checks.

Services covered in GCP

- Security groups (removal of false positives)
- Data storage
- Public assets
- Subdomains
- IP address
- ELBs
- Databases
- Containers
- Dockers,
- Grafana
- Kibana
- RabbitMQ

Increase Visibility
Gain Visualization of Google Cloud compliance with PingSafe's powerful diagramming and reporting tools

Misconfiguration Elimination
Facilitate comprehensive drift detection for critical resources

Security Integration
Develop Google Cloud security and compliance into the development lifecycle with PingSafe's API and IaC Checks

Shared Responsibility- Security and Compliance
Cloud Security and compliance is a joint responsibility between the organization and Google Cloud, the CSP (Cloud Service Provider). Google Cloud is responsible for protecting the infrastructure that runs all of the services offered in their cloud. The organization is responsible for any data, applications, operating systems, and network or firewall configurations that run on the CSP's infrastructure.

Signup for a Free Trial

Technology Solution Platforms

AZURE Security

AZURE Security

PingSafe allows organizations to gain visibility into security and compliance posture, eliminate Azure misconfigurations with drift detection, and enable security automation with CI/CD integration and pre-deployment policy compliance checks.

- PingSafe protects data, apps, and infrastructure quickly with built-in security services in Azure that include unique security intelligence to help identify rapidly emerging threats early so that you can respond instantly.
- PingSafe implements an in-depth defense strategy across identity, data, hosts, and networks.
- With PingSafe, organizations gain visibility into security and compliance posture, eliminate Azure misconfigurations with drift detection.
- PingSafe also enables security automation with CI/CD integration and pre-deployment policy compliance checks.

Services Covered in Azure

- Security groups (removal of false positives)
- Data storage
- Public assets
- Subdomains
- IP address
- ELBs
- Databases
- Containers
- Dockers
- Grafana
- Kibana
- RabbitMQ

Increase Visibility
Gain Visualization of Azure compliance with PingSafe's powerful diagramming and reporting tools

Misconfiguration Elimination
Facilitate comprehensive drift detection for critical resources

Security Integration
Build Azure security and compliance into your software development lifecycle with PingSafe's API and IaC checks

Shared Responsibilities- Security and Compliance
Security in the cloud is the joint responsibility between the organization and the CSP (Cloud Service Provider) Microsoft Azure. Azure is responsible for the protection of the infrastructure that runs all of the services offered in their cloud. The organization is responsible for any data, applications, operating systems, and network or firewall configurations that run on the CSP's infrastructure.

Signup for a Free Trial