SOLUTION BRIEF

# Fortinet Cloud Infrastructure Visibility and Control

## Executive Summary

**In the majority of instances, cloud platform security breaches are often caused by preventable misconfigurations. And as organizations continue to adopt multiple public cloud platforms, the opportunities for cloud misconfigurations continue to rise. Fortinet FortiCASB-Cloud identifies and corrects cloud misconfigurations by monitoring the activities and configuration of multiple cloud resources. It breaks down silos between and across cloud deployments to deliver consistent, real-time visibility.**

## Misconfigurations Pose Serious Cloud Security Problem

Innovations in the public cloud occur much more rapidly than in the data center. The result is an impressive proliferation of public cloud infrastructure services and interfaces offered by cloud platform providers. While new services deliver attractive benefits, they also increase management complexity. Further, they include an infinite number of configuration combinations, offering a long list of opportunities for misconfigurations. Users may also change settings at any time, introducing a misconfiguration where there was not one previously.

For the public cloud, misconfigurations are a serious problem. Data breaches caused by public cloud misconfigurations jumped 424% year over year. In all, cloud misconfigurations were responsible for the exposure of more than 2 billion records, or nearly 70% of the total number of compromised records.[1]

There are numerous examples where a cloud storage bucket was simply left open to the public whereby anyone could access it—no special hacking skills or tools required. The most famous example is perhaps that of the National Security Agency, when an Amazon S3 instance was left open and security documents could be accessed with just a web browser.[2] Many other misconfiguration examples—public and private sector—exist.

## Repercussions of Cloud Misconfigurations

In a recent survey, 92% of IT and security professionals express concerns about security risks due to misconfiguration.[5] Their concerns are not unfounded. 82% in the same survey reported security and compliance events due to cloud misconfiguration.

Misconfiguration exposes organizations to a wide variety of vulnerabilities. The following security events are tied back to misconfiguration:[6]

- Unauthorized API calls, 28%
- Critical data breaches, 27%
- System downtime events, 44%
- Unauthorized traffic to a virtual server instance, 36%
- Object storage breaches, 34%
- Unauthorized access to a database service, 34%
- Unauthorized user logins, 29%

### Key Capabilities of FortiCASB-Cloud for Monitoring the Public Cloud:

- Configuration monitoring and assessment of multiple cloud resources
- Consistent compliance reporting across multiple clouds
- Dynamic cloud heat maps and threat maps
- Streamlined incident investigation
- Fortinet Security Fabric integration

**Data breaches caused by cloud misconfigurations jumped 424% year over year.[3]**

**84% of security leaders say traditional cybersecurity tools either do not work at all in cloud environments or have limited functionality.[4]**

## Using FortiCASB-Cloud to Solve Misconfiguration

84% of enterprises have a multi-cloud strategy today.[7] This requires consistent monitoring and visibility across all cloud environments. FortiCASB-Cloud, a cloud access security broker (CASB), leverages the public cloud management API from each of the major public cloud providers to monitor activity and configuration of multiple cloud resources.

There are many ways a configuration can be mishandled, and changes can be made any time, requiring comprehensive checks and continuous monitoring to catch problems. To address these requirements, FortiCASB-Cloud performs hundreds of public cloud configuration assessments across an organization's global cloud deployments, including Amazon Web Services, Microsoft Azure, and Google Cloud Platform. FortiCASB-Cloud identifies risks associated with the unsecure provisioning and configuration of cloud resources. It also offers threat and risk management tools that help trace misconfigurations to their source.

Once IT and security staff are aware of misconfiguration problems with their public cloud provisioning and configuration, they can take appropriate actions to fix the issues. With continuous monitoring, this will occur before any damage is done.

## FortiCASB-Cloud Leads to More Proactive Compliance Risk Management

With FortiCASB-Cloud, organizations have transparent visibility and control across and between public cloud deployments. Misconfigurations are identified in real time and tracked against compliance mandates—both regulatory standards such as the Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA) and security standards such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Dynamic cloud heat maps and threat maps in FortiCASB-Cloud enable organizations to prioritize their efforts on issues with the highest risk.

FortiCASB-Cloud also provides streamlined incident response and event management investigation and the ability to automate responses. This simplifies regulatory compliance violation reporting while enhancing compliance by providing guidance around security best practices. In addition, FortiCASB-Cloud and its streamlined and automated reporting capabilities help close the gap between time to detection and time to response.

And because FortiCASB-Cloud is integrated with the Fortinet Security Fabric, it synchronizes log aggregation and correlation with FortiAnalyzer and FortiManager. In the case of FortiManager, this enables streamlined management of the FortiGate NGFWs. Integration with FortiAnalyzer pulls cloud vulnerability and risk insights into actionable dashboard reports for different personas (CIO, CISO, board of directors, security operations center [SOC] managers).

**FortiCASB-Cloud is available in both the Fortinet FortiGate Enterprise Protection Bundle and the 360 Protection Bundle subscription services.**

## Leverage FortiCASB-Cloud to Avoid Preventable Security Events

Given that misconfigured cloud services are a leading cause of security incidents, it's essential that organizations monitor and assess all public cloud configurations. FortiCASB-Cloud delivers comprehensive assessments across cloud deployments, plus it uses that data to help with compliance.

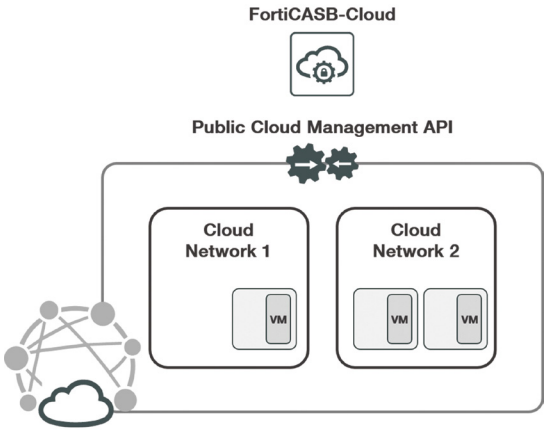


Figure 1: FortiCASB-Cloud leverages the public cloud management API to monitor multiple cloud networks.

[1] "IBM X-Force Threat Intelligence Index 2018," IBM Security, March 2018.

[2] Chris Bing, "Top secret Army, NSA data found on public internet due to misconfigured AWS server," CyberScoop, November 28, 2017.

[3] Phil Muncaster, "Breached Records Fall 25% as Cloud Misconfigurations Soar," Infosecurity, April 6, 2018.

[4] "Shining The Light On The 2018 Cloud Security Challenges And Solutions," Alert Logic, accessed March 22, 2019.

[5] "Most enterprises highly vulnerable to security events caused by cloud misconfiguration," Help Net Security, October 5, 2018.

[6] Ibid.

[7] "RightScale 2019 State of the Cloud Report from Flexera," RightScale by Flexera, February 2019.

FORTINET

www.fortinet.com



April 26, 2019 2:18 AM

377019-A-0-EN

F:\Fortinet\PDF Files\Fortinet - SB 042419\FA\FA-sb-cloud-infastructure-visibility-and-control