netskope

WHITEPAPER

Optimized Security for Multi-Cloud IaaS Environments

INTRODUCTION

Public cloud—both Infrastructure as a Service (IaaS) and Platform as a Service (PaaS)—are being adopted rapidly and widely by organizations in order to benefit from the scalability and efficiency offered. But extending an organization's workloads outside its perimeter, and moving its data into cloud services, creates a new wave of security challenges. These challenges cannot be addressed with the traditional perimeter-based security tools of yesterday. And this is forcing organizations to seek out new solutions for securing public cloud or look to the public cloud providers themselves for help.

Most organizations do not have in-house expertise in securing public cloud environments, instead they are deploying the Netskope platform to secure their growing off-premises workloads. At the same time, with Netskope, an organization can gain visibility and control of the business-led (shadow IT) services used by its employees, and manage the use of the web generally. This is the power of Netskope, a unified cloud-native security platform to secure, manage and analyze the use of cloud and web for any user on any device, at any location.

SHARED RESPONSIBILITY MODEL

Popular public cloud services such as Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP) all operate and publish a shared responsibility model [1]. A shared responsibility model is specifically about security, and as its name suggests—understanding where the responsibility for security lies. Generally, the cloud provider is responsible for the infrastructure of the service (security ***of*** the cloud) and the customer is responsible for the configuration and data within the service (security ***in*** the cloud). Regardless of which public cloud service an organization uses, the 'security of the cloud' is undoubtedly robust. It is very much in the business interests of Microsoft, Amazon and Google to prevent any security incident that could damage the reputation of their brand and services. Accordingly these public cloud services prioritize the people skills, budgets and resources to ensure their environments are secured to standards beyond most enterprises' reach. In fact, Gartner's confidence in the cloud providers' security had them recently predict that "Through 2023, at least 99% of cloud security failures will be the customer's fault"[2].

> **THROUGH 2023, 99% OF CLOUD SECURITY FAILURES WILL BE THE CUSTOMER'S FAULT**
>
> Gartner Magic Quadrant for Cloud Access Security Brokers, October 2018

THE MISCONFIGURATION PROBLEM

In a recent Cloud Security Report produced by Cybersecurity Insiders[3], survey respondents identified one of the biggest threats to cloud security as misconfiguration by an organization's own administrators. This probably shouldn't come as a surprise, given that humans are notorious for being the weakest link in any cybersecurity chain. Within public cloud environments administrators may not have sufficient security expertise to correctly interpret corporate security policies and will struggle to map those policies to configuration options. Administrators may also underestimate, or not understand, the risks associated with the use of public cloud. Ultimately administrators will carry out tasks within the public cloud without thinking about the risks, and how their intentions or actions may have unintended results.

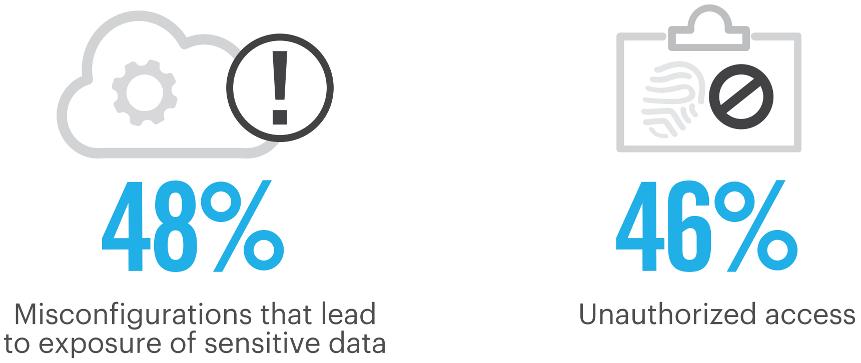


Figure 1. | What do you see as the biggest security threats in public clouds?
Infographic from Cybersecurity Insiders Cloud Security Report 2019 [3]

Examples of misconfigurations leading to a security breach are not hard to find, as much IT press coverage has been given to public cloud storage resources—such as Amazon S3 buckets—being configured improperly and exposing sensitive data to the Internet. Amazon S3 buckets are, however, just the tip of the iceberg; misconfiguration of Virtual Machines, Identity and Access Management (IAM) Policies, Virtual Networks, Logging, or any other public cloud resources could potentially be disastrous.

The ease with which public cloud services can be provisioned, and the sheer volume of resources within those environments—multiplied by the hundreds of configuration parameters and control options—leaves most organizations facing a significant security operations and audit headache.

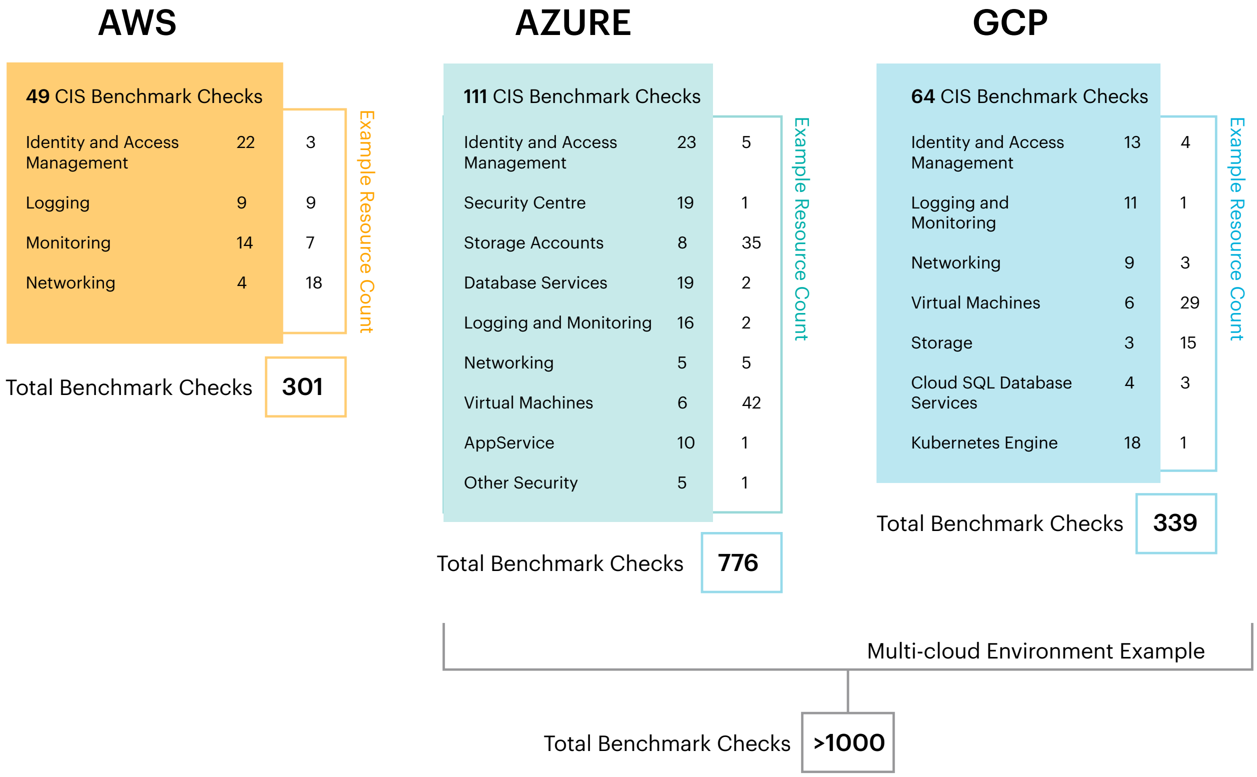
AUDITING AGAINST KNOWN BENCHMARKS

It is a fact that adoption and use of public clouds within organizations is outpacing the security expertise needed to securely configure these environments. As such, several organizations—including some of the public cloud vendors themselves—have published secure baseline configurations. An example of one such resource is the Center for Internet Security (CIS) Benchmark available for AWS, Azure and GCP. Although it's not an exhaustive list of all possible security configurations and architectures, these benchmarks each contain hundreds of pages of recommended configurations. The expectation that IT security personnel will manually and continuously measure every public cloud resource configuration against its benchmark recommendations is understandably unrealistic. It is, therefore, necessary to seek automation of these assessments in order to effectively scale and maintain compliance for your public cloud environment(s).

MULTI-CLOUD MULTIPLIES THE PROBLEM

An organization may be using multiple public cloud providers for a number of reasons. Different teams may have tactically adopted a cloud service without awareness of similar services already in use by another part of the business. In other cases, different cloud providers may be selected because they provide better specific functions or capabilities than another. For example, Google Cloud Platform may provide a better analytics platform than Azure etc. Whatever the reason might be, organizations are regularly finding themselves using multiple cloud providers. The distribution of workloads and associated mitigation of risk, means a multi-cloud approach is increasingly recognized as a good strategy for organizations that want to maximize the benefits of the cloud and also easily adapt to changing business needs. But what's best for the business compounds the risk of misconfiguration by multiplying those configuration parameters, control options, and compliance checks.

Let's take an example of an organization using Amazon Web Services and Microsoft Azure. A large organization might have hundreds of AWS accounts, containing thousands of IaaS resources such as EC2 machines, S3 buckets, VPC and IAM policies. Furthermore, this environment is typically not static—project-based DevOps work can see resources being created and dismantled on a regular and ongoing basis. Now, multiply the scale of this environment because somewhere else in the organization Azure is deployed with additional Virtual Machines, Blob storage accounts, and Database services. This is a challenging infrastructure environment for security teams to monitor and secure—especially when most IT security teams are already stretched for resources and lacking appropriate cloud-specific expertise and training.



AWS

49 CIS Benchmark Checks		Example Resource Count
Identity and Access Management	22	3
Logging	9	9
Monitoring	14	7
Networking	4	18
Total Benchmark Checks	301	

AZURE

111 CIS Benchmark Checks		Example Resource Count
Identity and Access Management	23	5
Security Centre	19	1
Storage Accounts	8	35
Database Services	19	2
Logging and Monitoring	16	2
Networking	5	5
Virtual Machines	6	42
AppService	10	1
Other Security	5	1
Total Benchmark Checks	776	

GCP

64 CIS Benchmark Checks		Example Resource Count
Identity and Access Management	13	4
Logging and Monitoring	11	1
Networking	9	3
Virtual Machines	6	29
Storage	3	15
Cloud SQL Database Services	4	3
Kubernetes Engine	18	1
Total Benchmark Checks	339	

Multi-cloud Environment Example

Total Benchmark Checks >1000

Figure 2: | CIS Benchmark checks within a multi-cloud environment

THE DATA PROTECTION PROBLEM

Misconfiguration can lead to sensitive data being exposed to the internet—most commonly this is due to a storage bucket being (mis)configured as “public”. There are numerous high-profile and news worthy examples of this happening. However, in other scenarios, the storage buckets are correctly configured as public—because it is the intention to share some data externally—but the organization is not monitoring exactly what data is in the bucket. This is not a problem that auditing configuration against benchmarks can solve because there is no misconfiguration. Instead, it is necessary to continuously monitor the data stored within the public cloud environment, or inspect the data being uploaded to the environment.

While addressing data protection, an organization should also consider the risk created by employees accessing (and uploading data to) public cloud environments not owned by the company. Typical security perimeter controls such as a web filter or firewall might allow access to ‘aws.amazon.com’ or ‘azure.microsoft.com’ but there is nothing to control what credentials are used to sign-in and, therefore, what account is being accessed.

WHY CHOOSE AN INDEPENDENT SECURITY SOLUTION FOR PUBLIC CLOUD?

Currently, each of the major public cloud providers provide varying degrees of built-in security assessment and control features (i.e. their native capabilities for security in the cloud). The inconsistency of security controls between providers, and the lack of any capability mapping across providers, creates a security challenge. This challenge is most apparent when considering a migration to a new provider, or when moving workloads between providers in a multi-cloud setup.

47% OF ENTERPRISES STATE THAT A MULTI-CLOUD MODEL IS THEIR PRIMARY CLOUD DEPLOYMENT STRATEGY

Cybersecurity Insiders Cloud Security Report, March 2019

Whether it’s the AWS Security Hub, the Azure Security Centre, or the Google Cloud Security Command Center, organizations will find differing features and capabilities that will help secure their respective environments. In some cases, these capabilities might not require any additional licenses which makes them attractive, but are they the right security solution for an organization?

Some organizations will not feel comfortable relying on the cloud provider to deliver the security for their own service. This is a classic ‘fox guarding the henhouse’ dilemma and may also jeopardize a robust defense-in-depth security strategy. These are good reasons for selecting an independent best-of-breed security solution to provide the governance of public cloud environments.

A 2019 survey by Cybersecurity Insiders[3] suggests that the future is undoubtedly multi-cloud, with 47% of respondents following a multi-cloud deployment strategy. When an organization utilizes more than one cloud provider, then the benefit of an independent security assessment and data protection platform becomes easier to understand. Multiple cloud platforms mean a broader attack surface with increased vulnerabilities; and therefore maintaining a consistent uniform security policy across multiple clouds becomes critically important. Only an independent cloud security platform can provide an aggregated view of resources and services, unified assessment of configurations, and consistent data protection policies across a multi-cloud environment.

Regardless of multi-cloud coverage it will certainly be the case that an industry-leading cloud security platform will be able to provide more advanced controls for data and threat protection than the public cloud providers themselves. This is typical across most areas of cybersecurity and the very reason that organizations select best-of-breed solutions.

More advanced controls for securing public cloud typically include:

- A wider range of security assessment benchmarks, such as PCI-DSS, NIST, etc.
- An explanation of the remedial steps for security assessment failures. In some cases, it may be possible to automatically adjust configurations based on audit results to resolve misconfigurations.
- A deeper level of threat detection, including next-gen anti-virus which can leverage artificial intelligence and machine learning techniques to detect malware rather than signatures; and zero-day protection through the sandbox analysis of suspicious files.
- Advanced insider threat detection using user and entity behavior analytics (UEBA)
- Enterprise-class Data Loss Prevention (DLP) capabilities, supporting identifiers such as RegEx, Fingerprinting, Exact Data Matching, and optical character recognition (OCR) analysis.

WHY CHOOSE NETSKOPE?

Many of Netskope's customers are leveraging a multi-cloud approach and have chosen Netskope to address the unique security challenges this brings. The Netskope platform provides a unified and extensible cloud platform for visibility, control, and protection of an organization's multi-cloud environment. Netskope provides enterprises with the necessary insight and control of risk within their existing public clouds, and future-proofs cloud security for the organization's further adoption of cloud.

Netskope delivers the advanced security controls for public clouds mentioned previously and, more importantly, extends data protection into real-time. Real-time policies allow the granular control of end user activities within public clouds—both sanctioned and unsanctioned.

The Netskope platform can extend cloud security further—beyond the public cloud and into all Security-as-a-Service (SaaS) and Web services. If unifying threat protection, data protection, and their associated analytics and incident management across multiple IaaS environments simplifies and strengthens security, then extending this unification across Web and SaaS will totally transform and optimize an organization's security operations. Ultimately policies become based on the organization's data, protecting it wherever it goes—Microsoft Office 365, Box, Salesforce, G Suite, AWS, GCP, Facebook, or any other cloud service or website visited by an end-user.

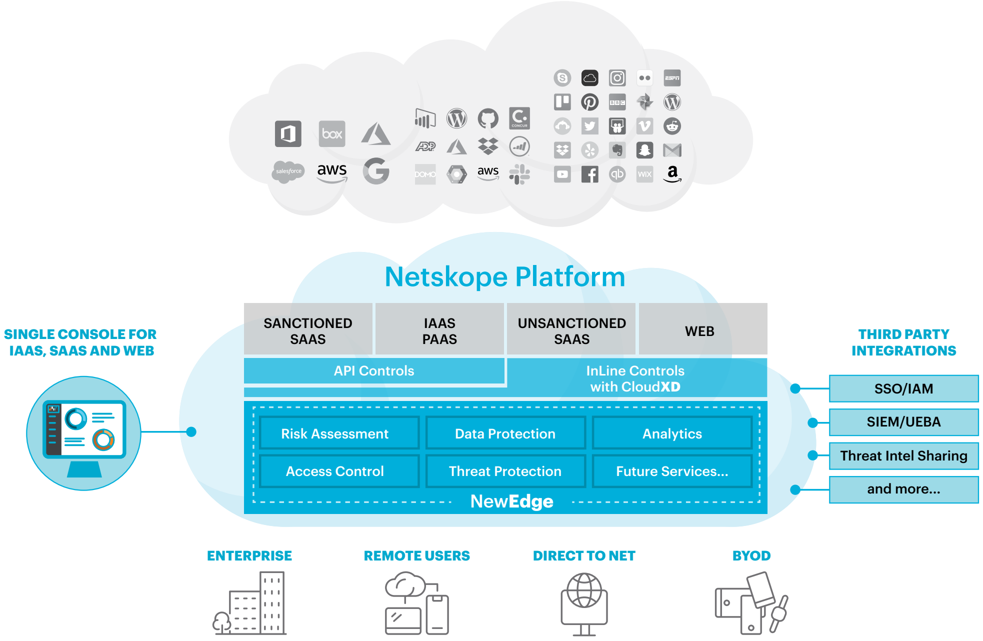


Figure 3 | Netskope platform architecture

Security teams can effectively leverage the Netskope platform to secure their use of cloud and web services without needing to be experts in every cloud service adopted by the organization. At the same time, an organization can also gain visibility and control of the business-led (shadow IT) services used by its employees. This is the power of Netskope, a unified cloud-native security platform to secure, manage, and analyze the use of cloud and web for any user on any device, at any location.

REFERENCES

[1] Shared responsibility model

https://aws.amazon.com/compliance/shared-responsibility-model/

https://azure.microsoft.com/en-us/blog/microsoft-incident-response-and-shared-responsibility-for-cloud-computing/

https://cloud.google.com/security/overview/

[2] Gartner Magic Quadrant for Cloud Access Security Brokers 2018

https://www.netskope.com/lp/gartner-magic-quadrant-for-casb

[3] Cybersecurity Insiders Cloud Security Report, March 2019

https://resources.netskope.com/cloud-security-collateral-2/2019-cloud-security-report

netskope

Netskope is the leader in cloud security. We help the world's largest organizations take advantage of cloud and web without sacrificing security. Our patented Cloud XD technology targets and controls activities across any cloud service or website and customers get 360-degree data and threat protection that works everywhere. We call this smart cloud security.

To learn more visit, https://www.netskope.com.