




What Every CISO Should Know About Cloud Security

**Find out how CISOs and security
leaders navigate the growing
challenges of cloud security**





This eBook contains a collection of best practices from customers who have implemented Netskope to enable the cloud within their company, while maintaining security and control.

Understand your cloud usage and risk exposure



Christopher DeHart

Director of Public Cloud Services and Cloud Governance
Hospital Corporation of America

Industry: Healthcare

Visibility and control will continue to be key concerns for business as they move to the cloud. Our security teams lacked visibility into our cloud usage, the apps being accessed, the data in use, and the potential risky activities performed with protected health information (PHI) data. We're always looking at ways data can leave HCA and the tools to help us identify and stop it from taking place. Netskope enables visibility, when we can see the data and risk, we're obligated to take action. We're increasingly seeing healthcare companies as the target of cyber attacks in the news. HCA does not underestimate the cloud as a threat vector and plans on staying ahead of cloud malware and ransomware attacks with Netskope.

Netskope enables contextual visibility, when we can see the data and risk, we're obligated to take action. For the data important to your organization, how much risk are you willing to live with?

Understand your cloud usage and risk exposure

Christopher DeHart

Director of Public Cloud Services and Cloud Governance

Hospital Corporation of America

Industry: Healthcare

Determine if you have gaps in your security approach

First, determine if your organization has the security measures to respond to threats like malware and ransomware using the cloud to hide. Then pick the right tools for the job. Security is an evolving concept. Understand what you do have, if it's capable of addressing cloud threats and if you need to cover the gap with additional security measures.

Contextual visibility into cloud usage is key

Understand how cloud apps are being used within your organization. Contextual visibility into activities taking place like app, users, activity, and the device being used is critical. I would guess that more than 50% of users are going direct to cloud while mobile and or remote. This can be risky depending on what users are accessing and doing with the data. Our CIO was alarmed at how much data was leaving the organization discovered by Netskope for cloud storage.

Ensure uniform security policies across SaaS, PaaS and IaaS through a single pane of glass



Luckily we found Netskope and are able to write a single policy that works across all of our apps. It's been a game-changer for the team.

Craig Guinasso

Chief Information Security Officer

Genomic Health, Inc.

Industry: Life Sciences

Whether it's for big data analysis or simply finding a collaboration app for our researchers, at Genomic Health we look to the cloud, and this changes the way we talk to our business counterparts and how they see IT. Being in the healthcare industry means we have to comply with regulations. Stopping PHI and personally identifiable information (PII) from making its way to user-led cloud apps is necessary. We started down the path of looking at all the individual app controls across the many cloud services in use within our environment for protecting sensitive data and quickly realized that there was no way our team could learn and manage so many different systems. With Netskope we're able to write a single policy that works across our entire cloud environment.

Ensure uniform security policies across SaaS, PaaS and IaaS through a single pane of glass

Craig Guinasso

Chief Information Security Officer

Genomic Health, Inc.

Industry: Life Sciences

You need a single control point and multi-cloud protection

Many enterprises have security silos. IT and security teams are juggling multiple security functions for each cloud application which can leave gaps in a security program and blind spots. If your enterprise is running a multi-cloud environment, using Amazon Web Services, Microsoft Azure, Google Cloud Platform, make sure you take appropriate security measures, keep security best practices at the forefront and take steps to ensure visibility across your cloud environments. With Netskope, we ensure consistent visibility, security and policy controls across our entire cloud environment.

Cloud security is a journey... not a destination

Like many organizations, Genomic Health's decision to move to the cloud went way beyond cost savings and was driven by the needs of the business. While not everyone's journey to the cloud follows the same path, there are often similarities when it comes to cloud security. Today, Netskope helps us find out what users are doing, and put controls around those activities. No one knows what tomorrow looks like, but I'm sure Netskope will already have it figured it out.

IDaaS and CASB are an integral part of your cyber risk management



Jerry Sto. Tomas

Chief Information Security Officer

Apria Healthcare

Industry: Healthcare

Identity as a Service (IDaaS), cloud access security broker (CASB) and third-party risk management are the fundamentals of a cloud security foundation. However, you can't have a cloud strategy without considering mobility. At Apria our mobility solution is a combination of Mobile Device Management (MDM) to secure and manage iOS devices, IDaaS to manage identities and Netskope to secure and manage access and improve visibility.

Most companies overlook mobility as part of their overall cloud strategy while more users are now accessing apps from their mobile devices. You need to consider mobility. You can't have a cloud strategy without considering mobility and Netskope can help you secure it.

IDaaS and CASB are an integral part of your cyber risk management

Jerry Sto. Tomas

Chief Information Security Officer

Apria Healthcare

Industry: Healthcare

Develop a cloud strategy and determine your third party cloud providers

First, consider your security architecture and their interdependency. Because of the proliferation of cloud apps in our environment the most common challenge has been managing multiple identities and having visibility across our environment. Multiple identities with multiple access controls comes with a complex environment that is difficult to manage. Apria has more than 300 locations with mobile drivers and remote employees working from different locations and types of devices. With Netskope we create the granular access control policies for any use case imaginable and are able to prioritize the enforcement of compliance against our third party cloud providers.

Device visibility is key

When we first rolled out Netskope we learned that thousands of cloud applications were being accessed by our users. It's also critical to understand the who, what, where, context by device. With Netskope, we have full visibility of cloud applications and user behavior which includes data inspection and loss prevention, regardless of device.



Netskope is the leader in cloud security. Using patented technology, Netskope's cloud-scale security platform provides context-aware governance of all cloud usage in the enterprise in real-time, whether accessed from the corporate network, remote, or from a mobile device. This means that security professionals can understand risky activities, protect sensitive data, stop online threats, and respond to incidents in a way that fits how people work today. With granular security policies, the most advanced cloud DLP, and unmatched breadth of workflows, Netskope is trusted by the largest companies in the world. Netskope — security evolved.

To learn more, visit www.netskope.com.
