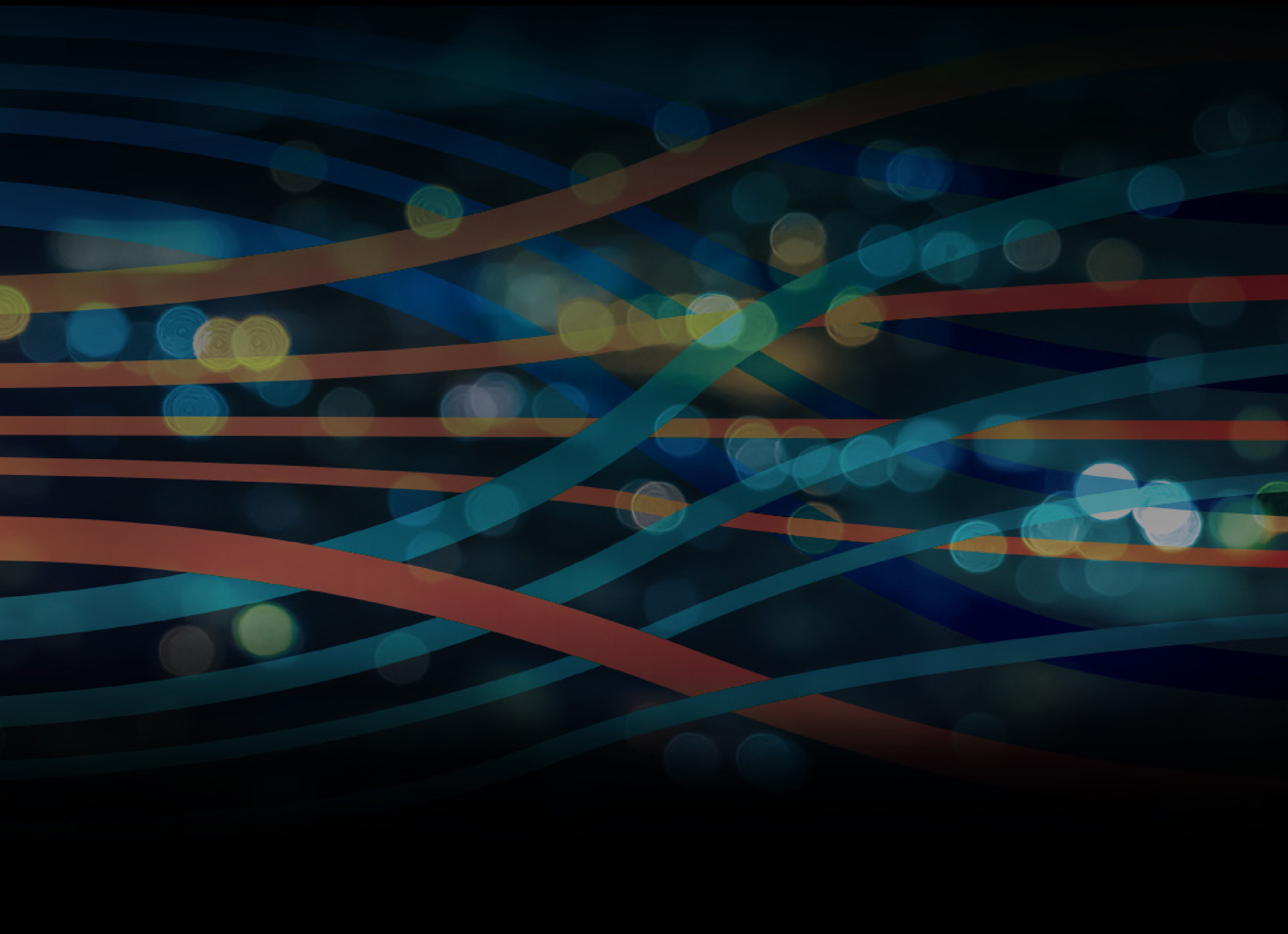
netskope

WHITE PAPER

How to Adopt a Cloud Security Risk Management Mindset



As COVID-19 took hold, remote work became the new normal, accelerating a trend that was already well underway. Today, 64% of U.S. employees complete their work outside of corporate offices[1], and few analysts expect this trend to fully reverse course once the pandemic is no longer a threat to organizations and their staffs.

But there were security issues with cloud access and applications happening long before 2020. The pandemic accelerated those challenges, and now there is risk everywhere that users access data via the cloud—meaning, almost everywhere.

Secure Access Service Edge (SASE) has emerged as a framework for how businesses and governments need to address risk factors in cloud applications, sensitive data moving to and among those applications, and users doing risky things. The constant change in those risk factors—including new applications, more data, and the types of data moving to the cloud, and a wider-than-wide range of individual users and attributes of users—drives the need for continuous risk management. Managing security isn't something teams can "set and forget"—the risk factors change, second by second, and teams need to be able to continuously adjust the policies for change.

Security teams can't tackle the cloud landscape in the same way they protect on-premises systems. And they can't force products that weren't designed for cloud security and connectivity to carry the load. Using ineffective tools and incomplete analytics challenges teams to accurately assess cloud risk posture.

Let's examine how we arrived at this current challenge—and how to solve it, today.

Jan. 2020 (before COVID-19):

89% of enterprise users were active in managed and unmanaged cloud services and applications.[2]

March 2020 projection:

55% of business workloads will have migrated to the cloud by 2022.[3]

Aug. 2021:

83% of users use personal app instances on managed devices and average **20 file uploads each month.**[4]

[1] "Remote Work @ Risk: Cloud and Threat Report," Netskope Threat Labs, Aug. 2020.
[2] "The Dark Side of the Cloud: Cloud and Threat Report," Netskope Threat Labs, Feb. 2020.
[3] Tim Maurer and Garrett Hinck, "Cloud Security: A Primer for Policymakers," Carnegie Endowment for International Peace," Aug. 31, 2020.
[4] "Cloudy with a Chance of Malice: Cloud and Threat Report," Netskope Threat Labs, Feb. 2021.

Think Outside the Box

A line-of-business manager lands on one of the many freemium or low-cost file-transfer tools available after a quick search. It's easy to use and accessible from wherever an employee happens to be working. The manager uses his corporate card and gives his employees the productivity solution they need. What he doesn't think about is whether moving to this cloud app opens a security gap that puts data at risk.

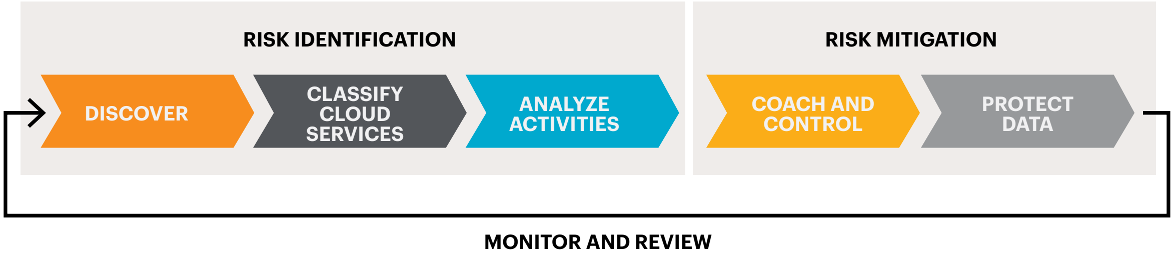
Fast-forward a few months. The security team inadvertently learns that 50,000 customer records are sitting in this file sharing tool. They have no ability to control how that data is protected, and no visibility into security events that might affect those records. The risk this creates for the company is enormous.

Data Protection Must Keep Up with the Times

How can you lock down the company's data and applications if you aren't deploying and configuring the servers, managing the databases, or even setting security policy? You can take an approach to cloud security that 1.) moves security between users and applications, regardless of where they are located, which is what a SASE architecture helps achieve, and 2.) provides continuous risk management.

MOVE TO A RISK MANAGEMENT MINDSET

There are several clear steps on the path to a risk management mindset for cloud security, represented in the diagram below.



Risk Identification

- Discover the cloud applications used by your organization.
- Classify the amount of risk associated with each app or data store, and the associated organizational risk
- Identify the users accessing each of those apps, and their activities and the associated activities that they perform.

Risk Mitigation

- Allow users to use applications by mitigating the risks to data. Coach users to better alternatives when the risk is low, and establish controls to manage risk factors when the risk is high.
- Protect especially sensitive data by refining data protection policies that oversee storage and control movement.

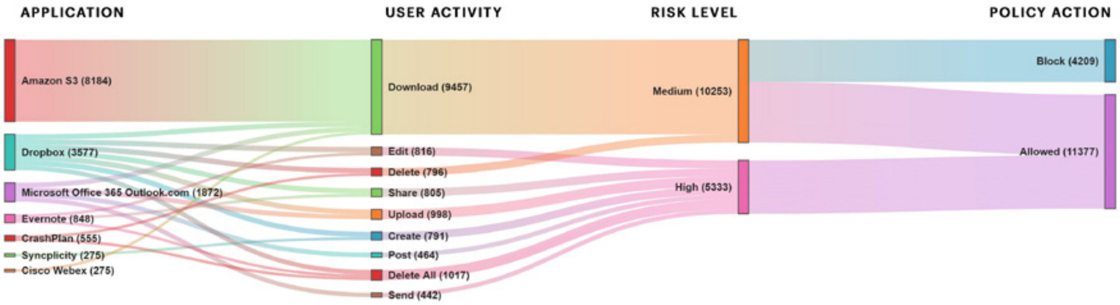
Monitor & Review

- Build a feedback loop for monitoring cloud risk on an ongoing basis, providing the right reporting to everyone from front-line security professionals to the C-suite and board.

Some of these steps may sound obvious, but the key here is that this is a process that should be continuously evaluated in a feedback loop, and that’s not simple. If you ask your security team today to list every cloud app that stores some of your organization’s data, they are unlikely to have a ready answer. It can be as tough as identifying what apps the organization uses, and gets more difficult from there. If you ask them for the risks associated with the apps, that’s even more difficult, because how do you identify and score risk factors on applications that you may (or may not) know about?

Visibility and Control for Data and Cloud Access

To build an effective security program, organizations need visibility in the applications they use, know where the data is, and where it is going. Netskope solutions are built to follow data through its entire lifecycle, wherever it goes. This approach is designed to create visibility into data storage and movement in the cloud and allow teams to take action immediately should access or movement introduce risk.



The Netskope Security Cloud combines a next-generation secure web gateway (SWG), a cloud access security broker (CASB), and award-winning data loss prevention (DLP) with security microservices such as data protection and adaptive access control. The platform discovers an organization’s usage of software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), and web apps. It can also pinpoint which users and devices are accessing each, and provide granular details about their activities.

Advanced Analytics: A Key to Risk Management

Once the Netskope Security Cloud is in place, Netskope Advanced Analytics closes the loop for continuous risk management.

That’s because the hard work is to make sure that your organization accounts for new risk vectors, and shaving off excessive access where it’s not needed. In other words, risk management requires constant adaptation to make sure that you stay within an acceptable range of risk that you can tolerate even as the applications, users and data in use are in a state of change.

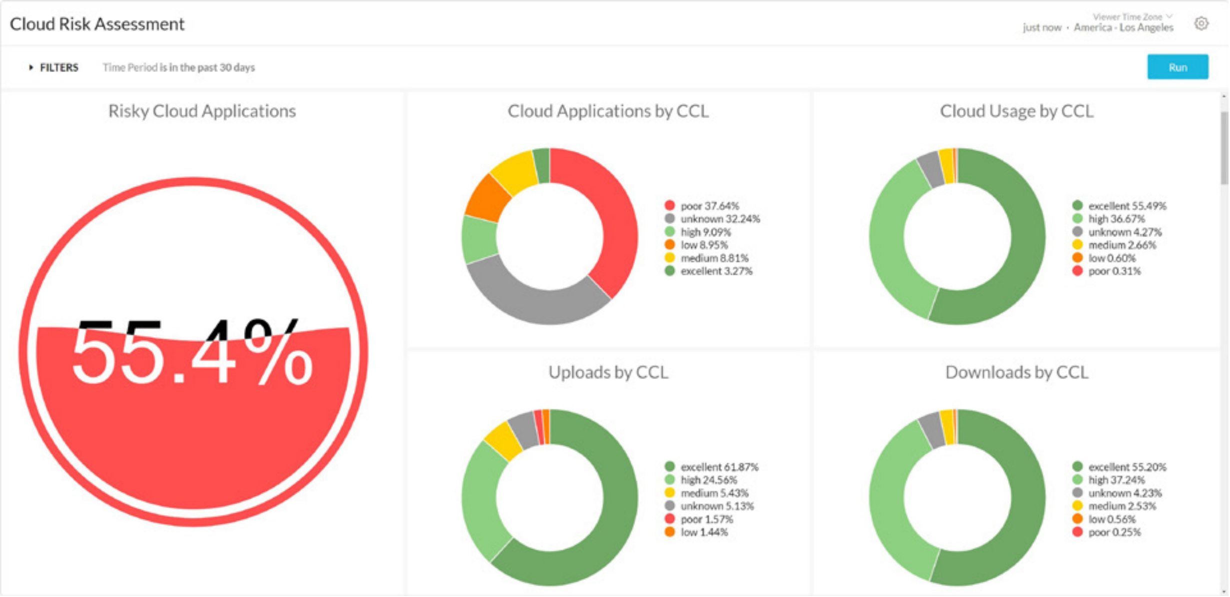
If you have 10,000 customer records spread across 10 cloud applications, is that acceptable or too risky? What if it’s 10 million records? You need analytics, because the number itself doesn’t tell the full story How can corporate information security leaders establish the company’s risk tolerance and create a security policy that accommodates the needs of the C-suite and board?

Netskope Advanced Analytics helps CIOs, CISOs, and IT teams answer those types of questions. You need to establish key performance indicators (KPIs) that describe the current status of, and trends in, security risk companywide.

You can use Advanced Analytics to establish a baseline for each metric. Then, over time, you can monitor how your risk exposure is changing—and adjust security policies appropriately.

Ultimately, Netskope Advanced Analytics supports CISOs’ through three high-level use cases:

- Prioritizing security optimization efforts
- Improving efficiency
- Monitoring the effectiveness of the security program and overall cloud security posture



Netskope's Cloud Risk Assessment allows you to monitor the Cloud Confidence Level (CCL) across your organization so you can identify the potential for risk and implement appropriate security policies for safe adoption in conformance with your business needs.

1. PRIORITIZING SECURITY OPTIMIZATION EFFORTS

From a threat perspective, your goal is to stop an attacker's ability to succeed at compromising your user or your data. But the threat landscape is enormous and growing rapidly. As with every other area of IT, risk management requires prioritization of resources across the organization's cloud exposures.

Netskope Advanced Analytics supports prioritization decisions by making assessments of the security landscape easy to understand. Dashboards, reports, and alerts deliver insights tailored to specific groups of stakeholders, in a format designed for those audiences. Thus, operations staff, the C-suite, and everyone in between can gain quick access to the information most pertinent to their role. With a wide range of data visualization options, Advanced Analytics supports at-a-glance comprehension of data trends.

NETSKOPE ADVANTAGES

- Prebuilt reporting includes dashboards tailored to operations staff, executive management, and others.
- Ability to import and export dashboards to collaborate with other security teams.
- Custom dashboards can draw on 500+ data fields.
- Alerts supplement on-demand reporting, flagging metrics that fall outside a specified range.
- Visualization options include bar graphs, pie charts, trend lines, tables, scatter plots, and more.
- Available data includes details on site, application, instance, user, activity, file, source/destination, and more.

2. IMPROVING SECURITY STAFF EFFICIENCY

Skilled security staff are one of an organization's most valuable assets. As they work to protect the organization's users and data, their time needs to be spent on analysis and strategy, not searching for relevant and appropriate data, and filtering through the alert workload to uncover root causes. Custom Netskope Advanced Analytics reports give security teams quick-read visibility into whatever information they need, to identify the signal through all of the noise.

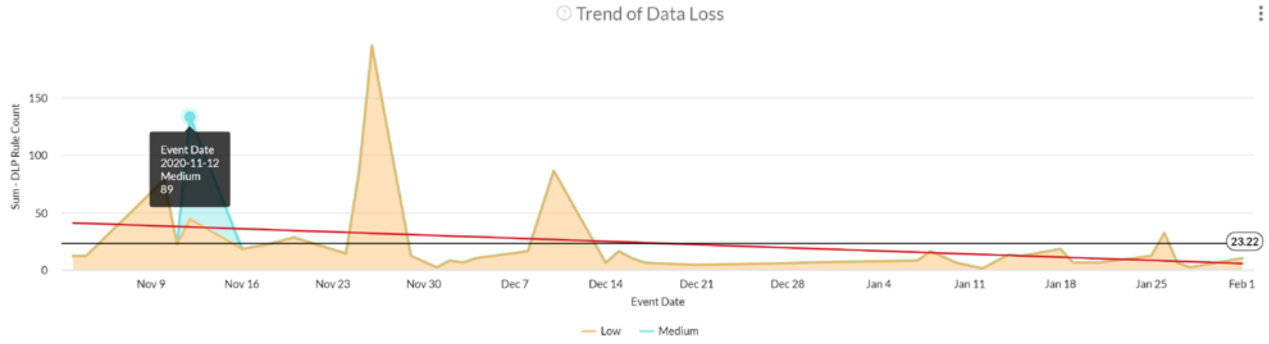
At the same time, investigating sources of risk is a critical step towards managing and controlling risk. Netskope Advanced Analytics also streamlines exploration of security trends. Interactive widgets make the drilldown process intuitive, minimizing the effort required for security teams to delve deeply into the granular information in the Netskope Security Cloud.

NETSKOPE ADVANTAGES

- Extensive library of predefined reporting for specific use cases includes CISO-focused dashboards, Cloud Risk Assessment Report, Data Protection Dashboard, GDPR Compliance Report, and many more.
- Customization enables reports to narrowly target a specific security concern, for a specific job title, which reduces time required to access relevant information.
- Simple-to-use report builder improves efficiency of custom report creation.
- Overall effect: Information is more easily accessible, with less effort, at every level of the organization.

3. MONITORING THE EFFECTIVENESS OF THE SECURITY PROGRAM AND OVERALL RISK

Ongoing protection of the company's cloud presence requires a continuously updated understanding of how well security policies and programs are working, and how they can be further improved.



Netskope Advanced Analytics summary reports provide trend data that clarifies security program efficacy. Is a given policy too permissive? Is a particular user taking increasing risks in the cloud? Stay on top of your policy changes, and explain to management that the number of security events will go up in the short term as policies tighten up, but the actions taken will reduce overall level of risk over time. Comprehensive reports with optimized data visualization make these questions easy to answer.

Security staff can monitor the effectiveness of the organization's cloud security on their dashboards, then digging into the details to uncover the underlying causes in areas of concern. Using this approach, they will learn where they need to make adjustments. They can then adjust security policies and practices throughout the organization, creating a feedback loop for continuously updating the management and mitigation of cloud risks.

NETSKOPE ADVANTAGES

- 360-degree view provides comprehensive visibility into the organization's cloud risk posture across all applications, users, and data.
- Analytics on both summary and detail data to highlight security trends in real time.

"Despite years of investment and focus on cyber risks, the costs of cyber incidents are rising. Organizations are increasing their cybersecurity spending but still often fall short."

— Tim Maurer & Garrett Hinck, Carnegie Endowment for International Peace[1]

[1] Tim Maurer and Garrett Hinck, "Cloud Security: A Primer for Policymakers," Carnegie Endowment for International Peace," Aug. 31, 2020.

CLOSE THE LOOP ON RISK MANAGEMENT

Remote work is increasingly prevalent. Cloud technologies are evolving even faster. And the threats to cloud applications and data are ballooning. Protecting your organization's users, data, and applications requires a risk management mindset and a continuous improvement process.

Fortunately, Netskope can help. The data-centric and cloud-smart Netskope Security Cloud delivers the information needed to prevent threats from reaching the assets you're charged with securing. Netskope Advanced Analytics makes that information easy and efficient to access at every level of the organization.

Using Advanced Analytics, your security team can get the information they need, spot trends, zero in on areas of concern, and address the important details. With better analytics, you build a security program to protect against the ever-changing threat landscape and effectively secure data in the cloud.

netskope

The Netskope security cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere, on any device. Only Netskope understands the cloud and takes a data-centric approach that empowers security teams with the right balance of protection and speed they need to secure their digital transformation journey.

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