Making Everything Easier!™

Netskope 2nd Edition

Cloud Security

FOR DUMMIES®

A Wiley Brand

Learn to:

- Evaluate the risk of enterprise cloud services
- Monitor your organization's cloud usage
- Create a cloud security policy
- Protect against cloud threats

Brought to you by

netskope

Lebin Cheng
Ravi Ithal
Krishna Narayanaswamy
Steve Malmskog

About Netskope

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.

Serving a broad customer base including leading healthcare, financial services, high technology, and retail enterprises, Netskope has been named to *CIO Magazine's* top 10 cloud security startups and featured in such business media as CBS News, *The Wall Street Journal*, and *Forbes*. Netskope is headquartered in Los Altos, California.

Cloud Security

FOR DUMMIES®

A Wiley Brand

Netskope 2nd Edition

by Lebin Cheng, Ravi Ithal, Krishna Narayanaswamy, and Steve Malmskog

FOR DUMMIES®

A Wiley Brand

Cloud Security For Dummies®, Netskope 2nd Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-39599-7 (pbk); ISBN 978-1-119-39603-1 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Writer: Rebecca Senninger
Development Editor: Elizabeth Kuball
Copy Editor: Elizabeth Kuball
Acquisitions Editor: Amy Fandrei
Editorial Manager: Rev Mengle
Business Development Representative: Karen Hattan
Production Editor: Magesh Elangovan

Introduction

Employees expect to work efficiently and flexibly wherever they are — at the office, at home, or on the road — using the most convenient way possible — whether that's with a desktop computer, laptop, tablet, or smartphone.

Increasingly that means people are getting their jobs done using cloud services. It also means that sensitive company data is being uploaded, downloaded, and shared on a daily basis.

And many times, the services being used to do that work aren't being used safely. That's where *Cloud Security For Dummies,* Netskope 2nd Edition, comes in.

About This Book

You may be intimidated by the idea of doing business in the cloud. But chances are, even if you don't know it, you probably are. Today, people buy and deploy cloud services often without IT's permission or involvement. This is called "shadow IT." The question it brings up is: How do you keep your information secure when it's out of your control? This book helps you get started on your journey! Here you find the information you need to confidently adopt the cloud:

- Discover the cloud services that employees are already using in your enterprise.
- Understand how employees are using these services.
- Assess each service's risk level.
- Adopt a cloud policy tailored to fit the way you do business.
- Protect sensitive data in the cloud and stop and remediate cloud threats.
- Monitor ongoing cloud app usage and enforce policy compliance.

By applying the principles outlined in this book, you can make a successful transition from using traditional on-premises infrastructure and applications to cloud-based ones.

Icons Used in This Book

Throughout this book, you find special icons to call attention to important information. Here's what you can expect:

The Tip icon marks tips and shortcuts that you can take to make a specific task easier.

The Remember icon marks the information that's especially important to know.

The Technical Stuff icon marks information of a highly technical nature that you can safely skip over without harm.

The Warning icon tells you to watch out! It marks important information that may save you headaches.

Beyond the Book

If you find yourself wanting more information after reading this book, go to `www.netskope.com`, where you can get more information about Netskope's products. You can find webinars, reports on the state of the cloud, best-practices videos, and much more!

Chapter 1

Assessing the Current State of Cloud Security

In This Chapter

- Taking a look at the cloud adoption trends in business
- Assessing the use of sanctioned and unsanctioned cloud services
- Employing a cloud access security broker (CASB)
- Using services securely on mobile devices and ecosystems
- Identifying threats and malware in the cloud

The number of cloud services being used in the enterprise is growing daily. This should come as no surprise: Cloud services are easy for users to buy and require minimal effort to get up and running. Not only is cloud adoption high, but users find that they can get their jobs done more quickly and flexibly in the cloud. Furthermore, cloud services often lend themselves well to mobile access, so growth in mobile devices has only served to increase cloud usage.

Social media services (such as Twitter and LinkedIn) and file-sharing services (such as Google Drive, Box, and Dropbox) are among the most visible. But companies are also adopting the cloud across their lines of business, including for human resources (HR), finance, customer relationship management (CRM), and marketing.

In this chapter, you find out why you should integrate the cloud into your daily business, the platforms you can use, and how to address any security concerns as you make the transition from a business that runs on traditional software to one that runs on cloud services.

Cloud is no longer a question — it's the way business is done.

Understanding the Growth of Cloud

When you think about cloud growth in business, you probably think it's mostly people accessing file-sharing services like Box and Dropbox or productivity tools like Evernote. However, enterprise cloud adoption goes beyond these consumer-friendly services. Entire functional groups — including marketing, human resources, finance, and research and development — are doing business in the cloud.

Reasons for cloud adoption

Put simply, the cloud allows employees to get their jobs done more quickly, easily, and flexibly than traditional computing tools. Here are some reasons any organization — including yours — should consider embracing the cloud:

- **Business agility:** People want to be productive now; they don't want to wait until the next software rollout happens. Many cloud services have more frequent release schedules than traditional software, which allows your company to take advantage of the latest features.
- **Device choice:** The cloud gives people the flexibility to work on whatever device they want — a desktop, laptop, tablet, or smartphone — whenever and wherever they want. Turn to the upcoming section, "Accessing the Cloud Securely from a Mobile Device," for more information.
- **Collaboration:** The cloud allows colleagues and business partners to share and access data in a seamless, frictionless way.
- **Minimal expense:** Deploying, maintaining, and updating on-premises software (along with the infrastructure to run it) can be expensive. You can reduce the expense of doing business, as well as more closely match expense with value, by using cloud services.

Because the reasons for cloud adoption are so compelling, your employees are most likely already using cloud services without your knowledge (see "The Rise of 'Shadow IT,'" later in this chapter), which can put your business at risk of data

compromise or noncompliance. Officially adopting cloud services allows you to set norms and establish policies to keep your sensitive corporate data secure and maintain compliance with regulatory policies.

Types of cloud services

When you're ready to start doing business in the cloud, you can choose one or more of the following. All three are being adopted at a rapid clip, but SaaS is the most fragmented of the types, with thousands of choices across dozens of business categories.

- **Infrastructure as a service (IaaS):** This is the most basic model of cloud service. With this model, you outsource equipment for your day-to-day business operations, including storage, hardware, servers, and networking components. The service provider owns, houses, runs, and maintains the equipment. An IaaS gives you the most flexibility for your applications, but it requires operations expertise and development resources.
- **Platform as a service (PaaS):** With PaaS, you build your applications on top of a platform with a well-defined software development kit (SDK). The application is deployed on the PaaS vendor's data centers. With PaaS, you have fewer items to set up and don't need as many development resources as IaaS, but you're still responsible for development and monitoring.
- **Software as a service (SaaS):** With SaaS, you use apps over a network — typically, the Internet — that the vendor makes available for your use. SaaS gets you up and running quickly because it works right out of the box and you don't typically need additional development resources. On the downside, you're completely dependent on the vendor for additional features.

No matter which model you choose (and you may end up with more than one), your corporate data is stored in the cloud, so you run the risk of unauthorized users accessing your data. If you use the cloud, consider establishing fine-grained cloud data loss prevention (DLP) policies to help you manage what gets stored in the cloud, how it gets stored, and what stays on-premises.

The Rise of "Shadow IT"

Systems and applications that are deployed and maintained by people or departments outside of IT's knowledge are known as *shadow IT*. If you assess cloud services in your organization, you'll likely find that employees use both *sanctioned* and *unsanctioned* services:

- **Sanctioned cloud services:** Services that the company provides for employee use and of which IT is aware. IT usually has full administrative control over these cloud services and maintains them on behalf of the business.

  

  Even though IT may manage sanctioned services, the department still may lack specific knowledge about how users are accessing them and what activities those users are performing, including uploading, downloading, sharing, or editing corporate data.

- **Unsanctioned cloud services:** Services that the company doesn't know about and may not approve of. Very often, if IT doesn't provide the necessary tools to accomplish a needed business function or disallows the use of such tools, employees go outside of IT and procure their own cloud services. Employees can easily find, pay for, download, and administer these services without IT's knowledge or assistance.

  On the one hand, the use of unsanctioned services is a good thing because it gives employees a way to work efficiently. On the other hand, these unsanctioned cloud services create risk for the business. Keeping services — and the data within them — secure is impossible when IT doesn't know about them. IT can't properly enforce security or compliance in unsanctioned services. Without important security features, such as strong user authentication and audit logging, these services, and the data within them, are vulnerable to inadvertent or intentional data exposure.

  Finally, IT has no idea how employees are using unsanctioned services. Are they uploading sensitive data to high-risk services, sharing data outside of the company, or downloading to a personal device?

Safely enabling the cloud means you not only manage all the sanctioned services but also find the unsanctioned cloud services in use. You can then begin securing services and data, including implementing strong authentication, monitoring administrator and user activities, preventing data loss or exposure, and protecting against threats such as malware and ransomware. IT can consistently manage and secure all the cloud services running in the organization and enforce security and compliance controls.

Cloud Access Security Brokers

IT departments have limited visibility when it comes to cloud services — especially with "shadow IT." They have no efficient way to track service usage or control sensitive data after it's uploaded. To bridge this gap in security, you can deploy a cloud access security broker (CASB).

The advantage of a CASB is that it enables an organization to use the cloud without compromising security or compliance. By combining security functions within a single enforcement point across all cloud services, CASBs drastically reduce the complexity of securing data in the cloud.

Some key capabilities CASBs enable include:

- **Discover and assign a risk score to all cloud services.** They discover and assign a risk score to each identified service. This allows you to decide whether services are acceptable for business use.
- **Provide adaptive access controls.** They enable you to control user access based on a number of conditions such as group or organizational units within your enterprise directory, device attributes, or other factors such as network or geo-location.
- **Monitor and set up alerts for admin and user activities.** They help you understand admin and user activity and its context, such as whether users are sharing sensitive data outside of the company, downloading to an unauthorized device, or escalating privileges within a service. They may also alert you to anomalous activities or activities that could lead to data exposure (see Figure 1-1).

- **Secure sensitive data and prevent its loss.** They enable you to enforce policies that secure sensitive data at rest in or en route to or from cloud services, as well as prevent its loss.
- **Coach users.** They enable you to coach users about risky cloud services and guide them to less risky alternatives, as well as provide feedback to users about noncompliant activities.
- **Monitor for threats and malware.** They monitor for the presence of malware at rest in or en route to or from cloud services, or detect anomalies that could indicate malware activity within cloud services.

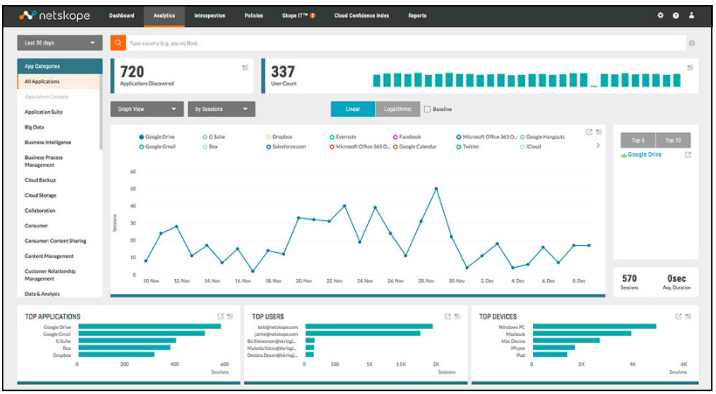

Figure 1-1: You have an easy way of monitoring cloud service usage.

If your employees use their personal devices to access company information in the cloud, there's no need to discontinue the practice. A CASB can keep your business data secure while still giving your employees the flexibility to get their jobs done.

Accessing the Cloud Securely from a Mobile Device

It's hard to find a business user today who doesn't use one or more mobile devices to get work done. Users want to be agnostic in how they access cloud services, and they often do so from multiple types of devices over the course of a single day.

You probably already give employees a variety of choices for how they can access cloud services. These choices are a good thing, but they can also increase the risk to your sensitive business data. More than a third of all cloud data policy violations occur on mobile devices.

Employees may not even be aware of your organization's mobile and cloud policies. After adopting cloud services and enabling mobile access to them, you need to make sure users understand what the policies are, how to follow them, and the consequences of noncompliance.

Cloud Ecosystems

Many popular cloud service vendors encourage ecosystems, or third-party services that integrate with them to share data and enable solutions that one service by itself may not be able to achieve. Anchor tenant services typically do this by providing application programming interfaces (APIs) to their ecosystem partners. By using APIs, those partners can share data back and forth with the anchor tenant service.

For example, the enterprise file-sharing and collaboration service, Box, has an ecosystem of more than a thousand cloud service partners that access and share content with Box to facilitate extended use cases such as electronic signature workflows, business intelligence reporting, and project management.

It's important to note that, while an anchor tenant service like Box may have security features built in, its ecosystem partners may not be as enterprise-ready. Because those services may access the data you have in Box, you need to have similar visibility and control across not just the anchor tenant service, but the ecosystem as well.

Threats and Malware in the Cloud

As users adopt cloud services, those services increasingly attract the attention of hackers seeking new ways to deliver malware, steal valuable data, disrupt business, and do harm

to systems. Cloud services have valuable features such as sync and share that make collaboration easy, but those same capabilities also make it easy for malware to propagate in the cloud, creating a dangerous fan-out effect.

Ransomware, a particularly damaging form of malware that automatically encrypts an enterprise's files until a ransom is paid, can not only spread itself quickly through cloud services, but can also spread the effect of its program — the encrypted files themselves — across synchronized folders, thereby encrypting shared files on the computers of all users sharing them.

Traditional threat protection and anti-malware solutions don't address cloud services effectively. There are several reasons for this, including the fact that many cloud services are unsanctioned and IT is often unaware of them and, therefore, doesn't scan those systems for malware. Another reason is that, even when IT is aware of cloud services, they still may not inspect the encrypted inbound cloud traffic because doing so can negatively impact network performance. Instead, they allow the encrypted session to bypass perimeter tools that inspect for malware, accepting the risk and hoping that their endpoint systems will detect the malware once it's delivered. Malware developers know this, and often use popular cloud services to either deliver malware or communicate with it once it has infected endpoints in order to perform network reconnaissance or exfiltrate valuable data.

Chapter 2

Finding and Evaluating Cloud Services in Your Enterprise

In This Chapter

- Finding the cloud services in your enterprise
- Evaluating the risk of those services
- Deciding whether to block services

Cloud services help your people get their jobs done more efficiently. But they're hardly risk-free. How can you ensure a service adheres to your organization's policies? Offers the right level of data encryption? Has a disaster recovery plan in place? In short, how do you know if a service is enterprise-ready?

The average organization has around 1,000 cloud services in use. Of these, eight or nine out of ten are *not* enterprise-ready, meaning they fail to meet enterprise standards for security, auditability, and business continuity. In this chapter, you learn the process you go through to discover cloud services in your environment, evaluate their enterprise-readiness, and assess whether you should block their use or if there's a more granular alternative.

Discovering Cloud Services: Perception versus Reality

You're ready to adopt a cloud service policy. The first step, of course, is finding all the services currently in use in

your company. You may think that most services fit right in with company policy, but the reality is that most services that people use — even ones sanctioned by IT — are not enterprise-ready.

To get a complete picture, look for services accessed from desktops and laptops within the office, as well as from remote laptops and mobile devices, regardless of whether users are accessing those services from a browser, desktop app, mobile app, or sync client.

Table 2-1 shows the number of cloud services that people typically use in the enterprise by category, along with the percentage that are not enterprise-ready in terms of security, auditability, and business continuity.

In addition to the consumer and prosumer services that you expect to find in use — such as Twitter, Dropbox, and Evernote — line-of-business services are actually the most prevalent. The marketing category has the most, followed by collaboration, productivity, finance/accounting, and human resources (HR).

Table 2-1 Cloud Services per Category, including Percent Not Enterprise Ready

Category	*Number per Enterprise*	*Percent That Aren't Enterprise Ready*
Marketing	105	98%
Collaboration	73	91%
Productivity	61	98%
Finance/accounting	63	96%
HR	77	97%
CRM/SFA	30	93%
Social	32	90%
Software development	40	96%
IT/Application management	23	98%
Cloud storage	29	76%

Report findings are based on tens of billions of cloud app events seen across millions of users and represent usage trends from October 1 through December 31, 2016.

Later in this chapter, you can find out how to evaluate the risk these services pose, whether you should block them from being used, and what your alternatives are.

Don't underestimate the number of unsanctioned cloud services being used in your company. Many companies underestimate that number by about 90 percent.

Evaluating the Risk of Cloud Services

Companies that embrace the cloud must first understand, manage, and minimize the inherent risks in each cloud model.

You can evaluate the enterprise readiness of a cloud service based on objective criteria in the following functional areas:

- Certifications and standards
- Data protection
- Access control
- Auditability
- Disaster recovery and business continuity
- Legal and privacy
- Vulnerabilities and exploits

Evaluate cloud services based on these objective measures, but remember that while a service's enterprise readiness is important, the bigger risk can come from how people are *using* that service.

Inherent risk

When your sensitive business data resides outside of your company, you take on a level of *inherent risk*. You're storing data and — depending on the functionality from the public cloud — losing your capability to have physical access to the servers hosting your information. As a result, confidential, regulated, or other sensitive data may be at risk because of the inherent capabilities of the cloud services in which they reside. For example, if the service doesn't separate one

tenant's data from another's or doesn't provide adequate access controls as part of its offering, your data is beholden to those deficiencies. As a buyer, implementer, or approver of such services, you need to ensure that the inherent security capabilities you require are available in the cloud services your organization is using. It is important to ensure that, whenever your data is out of your control and stored in the cloud, the services you choose have the security measures in place to protect your data and comply with your policies.

Your cloud services should follow these practices in order to limit your inherent risk:

- **Certifications and standards:** Your services and the data centers in which they're hosted should be in compliance with regulations and industry guidance that matter to your business. The "Common cloud security certifications" sidebar explains the key certifications you should consider.
- **Data protection:** Services that house your corporate data should enable you to protect that data according to your requirements. This may include
  - Classifying your data and enforcing access and data protection policies based on classification levels
  - Protecting your confidential and regulated data with strong encryption and your corporate-managed keys (find out more about encryption in Chapter 4)
  - Separating your cloud service instance from those of other clients to ensure zero chance of data exposure or one client's corrupted data affecting that of another client

Related to data protection is data ownership. Be aware that some services do not specify that the customer owns the data in their terms and conditions. For any services that contain your business-critical data, only choose ones that specify that *you* own your own data. Also, look for terms that specify the process for retrieving your data should you discontinue the service.

- **Access control:** Your services should offer access controls and policy enforcement commensurate with your on-premises controls. These include features such as

multifactor authentication, single sign-on support, and granular access controls.

- **Disaster recovery and business continuity:** Your services should provide very clear details about disaster recovery plans and processes. Those details should reflect your business requirements for uptime and data access depending on criticality of the data. Know where your backup offsite location is, what the provider's disaster recovery plan is, and how your data will be backed up and failed over.
- **Encryption:** Your services that store sensitive or regulated data should offer encryption of data at rest and give you choices for how to manage those encryption keys per your policies. (Find out more about encryption in Chapter 4.) Moreover, they should ensure that your data is managed separately from other tenants in the same cloud.
- **Audits and alerts:** Your services that deal with critical business processes, contain sensitive data, or have access to your enterprise systems should offer robust administrator, user, and data access logging and alerting features (see Figure 2-1). This helps you detect noncompliant behavior as it's happening, as well as perform forensic audit trails after a suspected event occurs.

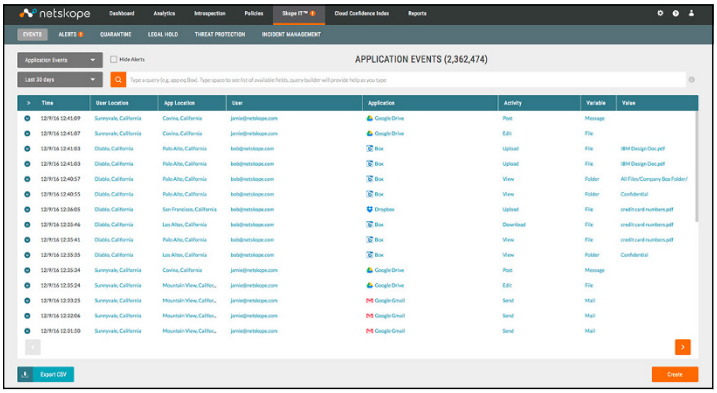

Figure 2-1: Robust activity-level audit trails.

- **File sharing:** Your services that enable file sharing should support file capacities that meet your large-file requirements. This will ensure that people will use the corporate cloud services available to them and will be less likely to seek out a potentially lower-quality service — and one that you have no visibility into — to support their file sharing requirements.

Common cloud security certifications

When it comes to certifications regarding cloud services, you should be familiar with a few key certifications:

- **SOC-1, SOC-2, and/or SOC-3:** With these certifications, you get a baseline for a service's physical and logical access, data security, and business continuity procedures. Make note of whether the certification is Type I or II; the former reports on the existence of control procedures, while the latter verifies those procedures in practice.
- **SAS-70/SSAE-16:** This certification details how a service reports on compliance controls, and how its system matches control objectives.
- **ISO27001:** This certification defines a top-down approach for information security management. It includes a six-part process, including policy definition, scope, risk assessment, risk management, control objectives, and statement of applicability.
- **The latest HIPAA regulation:** This regulation ensures privacy of personal health data, if applicable.
- **The latest PCI-DSS security standard:** This security standard ensures privacy of personal credit card information, if applicable.
- **Privacy Shield certified:** This new certification (which is a replacement for Safe Harbor), serves as assurance that cloud services outside of the European Union comply with EU privacy standards laid out in the General Data Protection Regulation (GDPR), including disclosing to users how their personal information will be used.
- **TRUSTe certified:** This certification indicates that the cloud service has undergone a privacy assessment and audit for data privacy and regulatory requirement adherence.

Contextual risk

Before you even begin inspecting content and enforcing policies to protect data, you need the relevant context of the activity.

Your CASB should allow you to see the following details:

- Which users and user groups are using specific cloud services
- What services they're using
- Whether the services are sanctioned, unsanctioned, or personal instances
- What devices and browsers they're on
- What classification of device they're using (managed or unmanaged)
- Where both users and services are located
- Activity details (upload, download, share, edit, approve, create, delete, and so on)
- Which users are sharing, what they're sharing and with whom, and whether recipients are outside the company

In the next section, you find out why these details are important. Not all activities are harmless!

Cloud service activities: Not all are created equal

It's not enough to know what services are running in your organization; you also need to understand what activities people are doing within them.

Your cloud vendor should give you granular-level detail to all activities, and provide you with real-time alerts when a user activity violates policy. (See the earlier section on inherent risk for more on alert functionality.)

Downloading, uploading, sharing, or simply viewing data are all activities that can be benign for one employee, but not so benign for another:

- A professional in the human resources department who is working at the headquarters office may have a legitimate reason to download salary information from a cloud-based HR service to perform analysis. However, a similar professional working in a satellite office probably has no business downloading the same salary information.
- An authorized employee in the finance department may need to edit field-level data within a cloud-based financial management solution. However, a different, unauthorized employee in the same finance department may need only to view documents, but not actually edit any of them.
- A business development professional may have a legitimate reason to share a presentation with a partner from a file-sharing service. However, it may not be wise to allow professionals from investor relations to share spreadsheets outside of the company from the same service during the company's quiet period.

These are all situations you'll want to know about right away to prevent potential data exposure or noncompliant activity.

Here are activities you need to make sure are secure:

- **Activities that can get you into trouble:** Cloud activities that create the most policy violations on average include upload, create, share, edit, and download.
- **Activities on mobile devices:** Half of all cloud activities occur on mobile devices, with more than half of send, approve, and download activities occurring on mobile. It's important to consider risks that are unique to mobile devices when you're setting policies in your cloud services.

With contextual information in hand — such as who the users or groups are, what cloud service or service category they're in, what device they're on, and what activity they're performing — you can be precise in identifying potential risky scenarios so you can protect your organization and its data in a targeted way. This helps you increase the accuracy of sensitive data detection and protection.

Cracking Down: To Block or Not to Block?

As you find unknown cloud services, you may be inclined to simply block them if they pose a risk. After all, up until now the only choices you've had have been *allow* and *block.*

Blocking policies don't work as well these days because people can usually get around your "no." They may seek an exception, go off-network and connect directly to a cloud service, or use a mobile app. Because many of the cloud services in question are actually used for legitimate business purposes that make the company more productive and competitive, exceptions need to be made. In fact, the majority of cloud activity happens in services for which IT has made exceptions. This phenomenon is called *exception sprawl.*

But with cloud services you *can* take a more nuanced approach to deciding whether to block or not. Instead of taking a simple binary approach and blocking the cloud, you could say "yes" to many of the services people want to use. Then, like a surgeon, you could slice out certain activities to make the usage of those services acceptable to your company from a security and compliance standpoint.

This approach would put you in the position of partnering with and enabling the business rather than saying "no" in a wholesale way. And for the cloud services that the company is slow to adopt because of security and compliance concerns, this approach lets you adopt them more quickly.

Taking a scalpel instead of a sledgehammer to the problem paves the way to cloud confidence.

The tool you use to manage your cloud services should let you create sophisticated, precise policies quickly and enforce those policies in real time.

In Chapter 4, you find out why enforcing policies on activities and data, rather than blocking cloud services outright, is often the right choice for businesses today.

Chapter 3

Putting Cloud Security into Practice

In This Chapter

- Cloud security architectural choices
- Understanding how the cloud services in your environment are being used
- Logging cloud activities
- Finding cloud usage anomalies

Cloud services are an increasing part of doing work today, with thousands of services being used across virtually every business function. But many times, the cloud is not being used safely or in accordance with company policy – if there is a policy.

As you make decisions and institute policies to make cloud services secure and compliant, you're becoming cloud confident.

In this chapter, you take the steps you need to be cloud confident. (In the next chapter, you learn how to create a policy for employees to follow.)

Cloud Security Architecture

Before exploring the steps to cloud confidence, it's important to note that CASBs can vary widely based on how they are architected. Many CASBs were built to solve a particular use case such as discovering shadow IT or enforcing policy in a single cloud service. You should evaluate your CASB based

not just on current use cases, but future ones, too, and that's where architecture matters. Some key things to look for include

- **An all-mode architecture, or the ability to deploy your CASB in a host of inline and out-of-band ways to fit your current and future use cases:** Deployment considerations should include the ability to see and enforce policy not just on sanctioned but also unsanctioned services.
- **Visibility of all cloud traffic, including to both sanctioned and unsanctioned services, usage coming from remote and mobile users, and traffic not just from users' browsers, but also their native apps, mobile apps, and sync clients.**
- **Rich context, or the ability to see and enforce policy on a set of granular parameters that include user, recipient, group, device, device classification, location, cloud service, service category, or service instance, user activity, content, and more.**
- **Cloud scalability, or the ability to grow to as many users, deployment options, cloud services, or security offerings, independent of hardware or network limitations.**
- **Deep integrations with the rest of your technology infrastructure, such as data loss prevention (DLP), security information and event management, mobile device management, and threat protection.**

Discovering Cloud Services

The first step is to always know exactly which cloud services people are using in your organization. Your CASB should give you a snapshot of all the enterprise-sanctioned cloud services as well as discover any unknown ones in use.

After those services are discovered, IT should evaluate each against a set of objective criteria:

- Score services on enterprise-readiness, as measured by security, auditability, and business continuity.
- Evaluate those services' risk based on your organization's usage of them.

- Make risk-based decisions about whether to standardize on, and migrate users to, certain services.

Evaluating cloud service use

After you know what cloud services everyone in your company is using, you should be able to drill down into the information surrounding those services and understand how people are using them.

This step actually involves understanding contextual cloud usage:

- **Drill down into user identity.** This includes
  - An individual or group defined in your enterprise directory
  - Where people are when they access the cloud
  - What devices and browsers they are using
  - If the cloud transaction involves sharing or sending, the identity of not just the sender, but also the recipient
  - The risk of the user based on risky cloud services they're accessing, visits to malicious websites, and whether they've had other accounts breached
- **Understand the cloud service.** This includes
  - The service, category, and in some cases, the *service instance* (different accounts created within a service) that are being accessed, and by whom
  - The service location (where the service and its data are being hosted at any given time)
  - Vulnerabilities and threats associated with the service
- **Ascertain cloud activities.** This includes
  - What discrete activities users are doing (for example, log in, upload, download, edit, share, and approve)
  - Administrative activities (such as the escalation of privileges or creation of a new instance, such as in IaaS)

- **See content details.** This includes
  - What content type and file or object name they are dealing with
  - Whether the content is deemed sensitive given your organization's data loss prevention (DLP) profiles
  - Whether content has public, externally shared, or internally shared links exposing it to unauthorized users
- **Discover sensitive content.** You're looking for the content existing at rest within a cloud service, including any that violate a DLP profile. Figure 3-1 shows you the exposure of your sensitive data in your sanctioned cloud services.

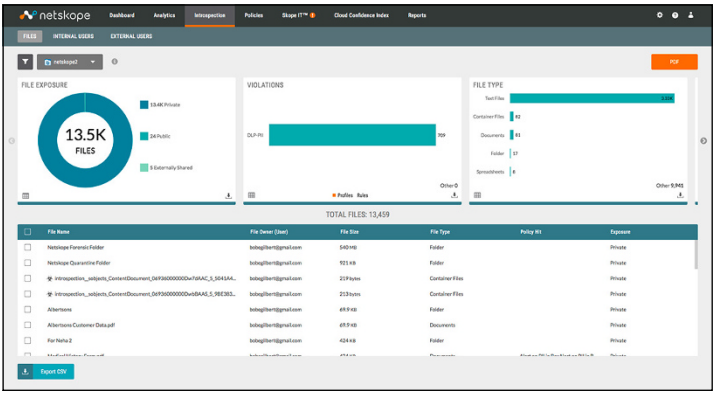

Figure 3-1: Understand exposure of sensitive content in cloud services.

You also get one consistent view across service behaviors and can use that view to enforce one simple policy uniformly across all relevant services instead of having to set policies service by service. For instance, *share* and *send file, download* and *export,* and *edit* and *change* can each mean the same thing across different cloud services.

With a cloud policy in place, you don't have to analyze service after service. All user activities should be normalized across each category of services so you don't have to understand each service and map its activities to understand what's going on.

Auditing Activities

The capability to audit not just cloud access but actual activities in sanctioned and unsanctioned services, as well as perform incident management, are critical to performing accurate forensic analysis and responding to security events such as unauthorized data exfiltration.

To audit activities, you need to understand user activity and its context. For example, who's downloading from a cloud-based HR service, who's modifying instances within IaaS, and who's sharing content outside the company from any file sharing service?

A CASB should let you query your security data and answer any business or security question, understanding the *who, what, when, where,* and *with whom* of any user's or administrator's activity within a cloud service, users' activity overall, or activity compared to a baseline. Furthermore, it should enable you to respond to security violations with robust incident management workflows. You should be able to

- Perform granular, multi-variate queries to answer these questions.
- Do forensic analysis after a security incident or breach.
- Respond to incidents by viewing details and event history, assigning reviewers, adjusting severity, and changing status, as well as integrating with your enterprise incident management system.
- Be alerted to granular behavioral anomalies in any sanctioned or unsanctioned cloud service; see Figure 3-2 for a report on anomalies.
- Set watch lists that alert you to any activity.

You must be able to analyze any activity against policy, pivoting around any of the parameters. You must also be able to use analytics to detect anomalies to identify risky behavior and potential data loss or breach.

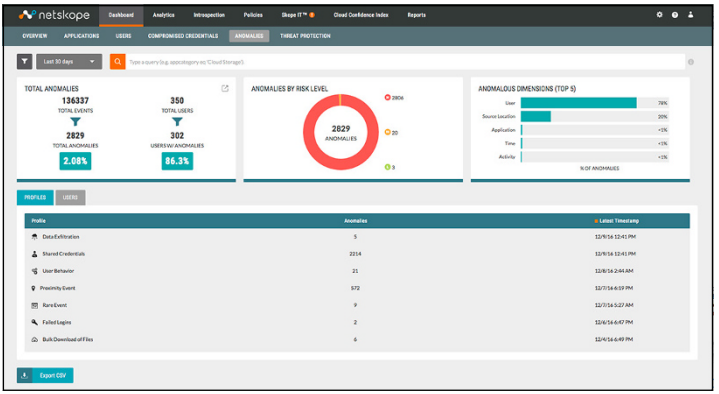

Figure 3-2: Find all the anomalies that indicate compromised credentials, out-of-compliance behavior, or even the presence of malware.

Depending on your business operations and regulations, compliance-oriented questions will rise to the top. IT should be able to answer specific questions. Here are a few examples:

- Who from my overseas call center is accessing my CRM system, and what specifically is he or she doing?
- Who from my Investor Relations group is sharing content from our file-sharing service during the company's "quiet period"?
- Has any non-HR manager downloaded salary data from any cloud service in the past three months?
- Is there any excessive downloading or sharing that could signal a data breach or theft?

When you set a policy once, you can set it to be carried out across all the cloud services you want it to. So, when you set a granular policy such as "Let people in my call center use CRM, but don't let them download customer contacts onto an unmanaged device if they're outside my country," or set policies about what services you will and won't allow based on their risk score, you know that those policies will be enforced immediately before an undesired act occurs, and you can do it at network speed across the entire business.

Beyond viewing cloud service access and activity, at a certain point, you should also have the capability to do *continuous compliance* — ongoing and uninterrupted visibility of all activities that could impact compliance with your organization's policies. IT should be able to turn any analytics query into a watch list or report, where any defined event or any deviation from a baseline will trigger an action.

For example, you can set up watch lists to uncover suspicious behavior, prove a breach occurred, and clearly demonstrate malicious or even criminal activity. You can create a granular cloud activity audit trail following a suspected event, such as the theft of sensitive content upon employee departure. For example, an employee logged into Microsoft SharePoint or OneDrive using corporate credentials, downloaded sensitive content, logged into a totally different service such as Dropbox or Google Drive using personal credentials, uploaded that same content, and then shared it with a new employer. IT should be able to construct a forensic audit trail showing every cloud service action for that user leading up to and immediately following the incident.

Detecting Anomalies

You also need to be able to detect anomalies in sanctioned and unsanctioned cloud services. For example, find out when an employee is exfiltrating data from a sanctioned service to an unsanctioned service, excessively downloading, sharing, or uploading data in services, or logging into services from multiple locations. These usage anomalies can indicate compromised credentials, out-of-compliance behaviors, and even the presence of malware.

If a cloud service doesn't support multifactor authentication, several anomalous attempted logins may be an indicator that someone is trying to hijack a user's account. Your CASB should offer protection by alerting you to the attempted access, preventing further access to the cloud service, and reporting on any attempted accesses for security and compliance purposes.

Protecting against Threats and Malware

Even if you have an anti-malware solution in place, your CASB needs to detect and respond to threats and malware in the cloud. The popularity of cloud services makes them attractive targets for hackers. Also, cloud-based threats can fly under your radar. This happens for two reasons:

- You haven't sanctioned the service and don't know it's in use.
- You have sanctioned it but aren't monitoring it for malware.

Many organizations do not inspect encrypted cloud traffic inbound, making it a rich opportunity for hackers who want to deliver malware without detection. Because the cloud makes collaboration easy, hackers can take advantage of features like sync and share to propagate threats in the cloud, creating a dangerous fan-out effect.

Your CASB should detect malware both in content at rest in sanctioned cloud services, as well as en route to or from any service. It should take immediate action to quarantine that malware for further inspection and replace it with a benign, "tombstone" file. When the malicious file is replaced with the "tombstone," your cloud service will sync and share the harmless file so it's remediated everywhere it has traveled.

But the remediation shouldn't stop there! Your CASB should integrate with the rest of your security infrastructure. For example, it should send the malware sample (or other indicators of compromise) to your enterprise sandbox, as well as your endpoint detection and response system so that those solutions can take action as well. In fact, the communication should be two-way, so your CASB is learning from threats seen on the endpoint and network as well.

Beyond anti-malware, your CASB should integrate threat intelligence from third parties to alert you to things like cloud services with unremediated vulnerabilities, users with compromised account credentials, and user visits to malicious websites, all of which carry risk to your organization if combined with an active threat.

Behind the Netskope scenes

So, how exactly does Netskope gain visibility and enforce policy dynamically on your enterprise's cloud transactions and traffic? It enables and has production deployments on non-mutually exclusive inline and out-of-band deployment options. Each of these methods has a different level of coverage, visibility, and enforcement, from the most basic to the most advanced, and in real time, so it's important to choose the right one(s) to facilitate your use cases.

Out-of-band options are

- **Log-based discovery:** You can upload logs from your perimeter networking equipment such as your web gateway or next-generation firewall to Netskope offline. Log analysis provides you information about what services you have, and the Netskope Active Platform categorizes them, gives you a view of their enterprise-readiness, and gives you a risk view based on a combination of those services' enterprise-readiness. Though useful, it's only a small fraction of what you'd be able to see and doesn't include the real-time policy enforcement that you'd get with the other implementations.
- **Sanctioned cloud service introspection via APIs:** Netskope uses secure APIs published by your sanctioned services to control behaviors and content residing in those services. Introspection gives you a deep view within specific services that you administer. It enables you to e-discover and inventory both content and users of that content. It then lets you take action on that content, including reassigning ownership, setting sharing permissions, quarantining files, and applying encryption of data at rest.

The inline options are

- **Agentless:** Netskope steers your users' on-premises cloud traffic to the closest one of Netskope's global network of SOC-3, Type 1– and 2–certified data centers, which sit between your network and the cloud services they're accessing. This is transparent and provides a "touchless" way to get cloud traffic from a user's PC or mobile device to the Netskope cloud for analysis and policy enforcement. Because it sits at your network's egress point, it's limited to on-premises cloud traffic.
- **Thin agent or mobile profile:** Netskope steers your users' remote cloud traffic to the Netskope cloud via a thin agent or, if a mobile device, a mobile

(continued)

(continued)

profile. The thin agent gives you the same visibility, analytics, and enforcement as in the agentless option, but it also covers any device that's outside of the four walls of your organization.

- **Reverse proxy:** Netskope redirects your users' traffic to a modified URL of your sanctioned cloud services. The reverse proxy method gives you a "touchless" way to get cloud service visibility and control; however, it is limited only to browser traffic and services that you administer.

Chapter 4

Creating a Cloud Security Policy

In This Chapter

- Operating in a shared-responsibility environment
- Creating data loss prevention (DLP) policies
- Protecting sensitive data with encryption
- Enforcing your policies
- Educating your users on your cloud policy
- Preventing activities that put the company at risk

When your goal is to reduce the risk of sensitive company information getting into or being shared from cloud services, you need to create a cloud policy and then have an effective way of enforcing it without compromising user productivity.

In this chapter, you find out how to create and enforce a cloud security policy.

The better you define your cloud policy, the better everyone will understand how to use the cloud while reducing risk to your organization.

Shared Responsibility in the Cloud

With *shared responsibility,* both cloud vendors and enterprises are responsible for cloud security:

- **Cloud vendors selling to enterprises must build services that are inherently enterprise ready.** Cloud service vendors and their ecosystem partners should obtain key third-party certifications and build in enterprise security settings and privacy features to meet their responsibility.
- **Enterprises must ensure that their users perform safe activities within the cloud.** Unsafe activities include theft of confidential documents, inadvertent exposure to and disclosure of sensitive data, and compromise of authentication credentials. For this, you will need to maintain visibility and granular activity- and data-level controls across sanctioned and unsanctioned services.

As an organization consuming cloud services, hold your vendors to their part of the shared-responsibility model and assume responsibility for your end, which is ensuring safe usage.

Incorporating Data Loss Prevention Policies

Look to your CASB to incorporate data loss prevention (DLP) profiles into your policies. You should be able to enforce DLP policies in context, including user, cloud service or category, activity, and so on. Some DLP profiles you may want to consider include

- **PII:** Personally identifiable information
- **PHI:** Protected health information
- **PCI:** Payment Card Industry information
- **Specific keywords, keyword dictionaries, fingerprints, or content exact matches:** Keywords you specify,

combinations of keywords, or other matched content such as sensitive forms, diagrams, or content that can be considered intellectual property, trade secrets, or proprietary information

- **Source code**

You should also be able to create custom profiles. The content-matching profiles can be applied to any user, user group, cloud service, cloud service instance or category, location, device, device classification, activity, and more, as shown in Figure 4-1.

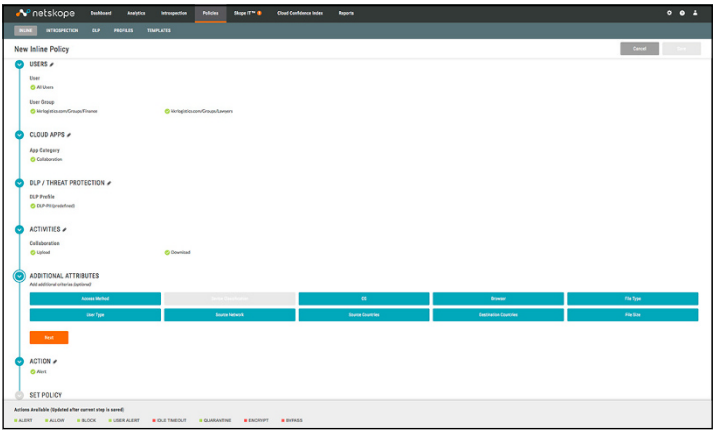

Figure 4-1: Enforce policy in context.

Be sure to pick a CASB that supports all the DLP profiles you need, whether they're predefined or custom ones that you build.

For example, if you're a healthcare company and you want to detect PHI violations, you can create a DLP profile using a predefined dictionary that contains hundreds of PHI-related classifiers (patient's name, Social Security number, medical procedures, drugs, and so on). You should also be able to create your own profile using regular expressions, form fingerprinting, exact match, custom keyword dictionaries, and more.

You can generate reports based on DLP violations. For example, you can find out which users are most often violating PCI rules, or the top services and devices being used to violate PHI rules in the organization. You can also send these

reports to other employees to curb policy-violating activities. Figure 4-2 shows a compliance report in the Netskope interface. You can also download it as a PDF or schedule its delivery to other users.

Here are some tips on creating DLP profiles in your enterprise:

- Create relevant DLP profiles for your cloud services, including PII, PHI, PCI, and more.
- Base your DLP profiles on industry-standard data identifiers and rules and incorporate rich context (services, users, time, location, and user activities) into your DLP policies.

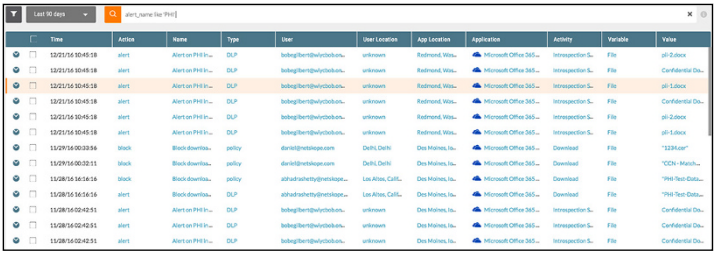

Figure 4-2: A PHI violations report.

- Discover content at rest already resident within your cloud services, and take action such as change ownership, quarantine content, or encrypt content.
- Set DLP policies that take effect not just in one service, but across an entire category if you need them to. Figure 4-3 shows how you can set up a DLP policy.
- Ensure that your DLP policies can be enforced in real-time before a data breach or exposure occurs.

For example, if your company has an internal policy that prevents employees from including a credit card number in email, anyone who tries to do so will automatically receive a coaching message. Such a message can also be sent if the user tries to send the credit card number via a file-sharing service.

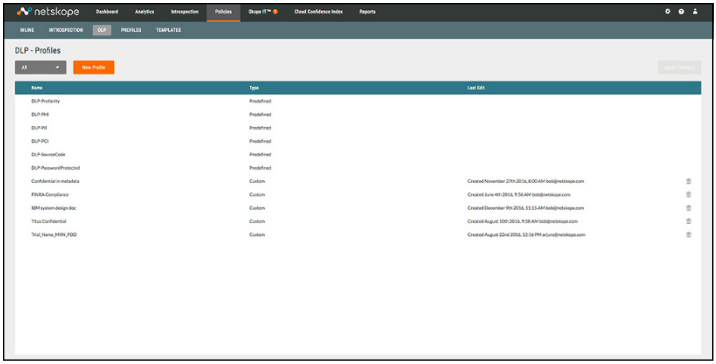

Figure 4-3: Set up your DLP profiles.

As another example, if your policy only allows upload of confidential documents to Microsoft OneDrive, you can detect and block anyone who tries to upload documents to another service, or even to the non corporate-sanctioned instance of OneDrive, and redirect the user to the correct OneDrive instance.

Truly preventing data loss means making users part of your compliance process. See the upcoming section "Coaching End-Users and Giving Them a Say" for more about coaching end-users on company policies. DLP ensures that your business is not interrupted or delayed.

Including Data Encryption Policies

Every policy should outline how enterprise data is encrypted:

- Where does your data reside and how is it being secured in the cloud?
- How are keys managed? In the cloud or on-premises? Are they managed according to your corporate policies? Are they held in a hardware security module (HSM)? Who controls the keys?
- How will the cloud vendor handle a data breach or exposure?

These questions should be answered in your policy. Figure 4-4 shows how data travels between cloud services and devices, between users via cloud sharing, and app-to-app in cloud ecosystems.

Data at rest in a cloud service

Data at rest refers to data that is physically stored in the cloud service provider's data center. Sensitive data should be protected while at rest within cloud services. And, depending on the level of sensitivity or confidentiality, encryption standards matter. Some encryption standards you're likely to encounter include AES, RSA, and DES, and each comes with a set of tradeoffs, usually along the dimensions of usability and level of protection.

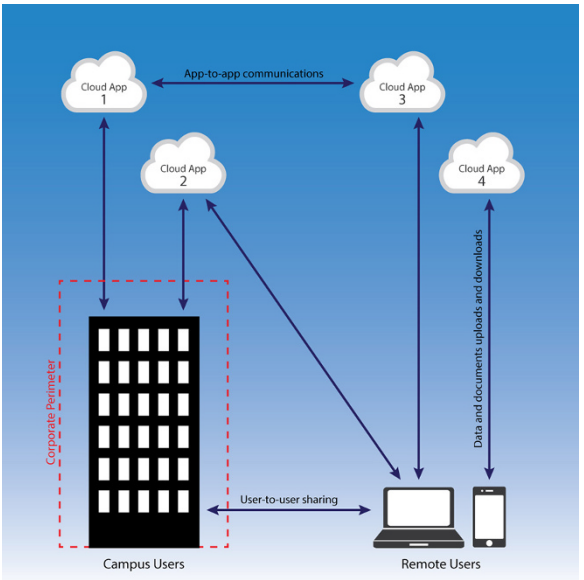

Figure 4-4: The complexity of the cloud.

For highly sensitive or confidential data, consider strong encryption such as AES-256.

When sensitive data is discovered at rest, it should be classified and inventoried. From there, you can take action such as quarantining it for legal review.

Key management is one of the most important considerations when encrypting content:

- After data is encrypted, the party that holds the keys (that can be you) has complete access to the data.
- Manage your keys with great care. If you lose the keys, your data is unusable.
- You can specify that keys be managed on-premises (versus in the cloud) and in purpose-built modules called hardware security modules (HSMs) certified under the Federal Information Processing Standard (FIPS) Publication 140-2 standard.
- Look for Key Management Interoperability Protocol (KMIP) support in a CASB, to ensure maximum compatibility with key managers in the market.

Related to encryption and key management is separation of data in the cloud. A best practice for cloud vendors dealing with business-critical data or processes is the separation of tenant data in the cloud. This is important because when multiple customers' data are commingled in the same cloud tenant, they run the risk of being exposed to each other. Plus, if one customer in the tenant experiences a technology failure or data corruption, all of the others can be impacted as well.

Data traveling to the cloud

As users are uploading, creating, sharing, editing, and downloading data, that data is at risk. Beyond encrypting data at rest, it's important that the data is secure when it's moving to and from the cloud.

Data needs to be encrypted as it moves to and from the cloud. And be sure that only authorized users have the capability to gain access to the data.

When sensitive content is discovered being uploaded into a cloud service where it's not supposed to be, the CASB should quarantine that content for review by a security, risk, or legal professional.

Data leakage

Even though in many ways cloud services can be as secure as on-premises applications, they can also make it easy for data to be exposed or leaked. Traditional security measures tend not to cover mobile devices, where cloud services can be accessed anywhere and at any time from any device. There's a bigger risk of an intentional or inadvertent data leak. The cloud also makes it far easier than traditional computing to share data with unauthorized users and people outside of the company.

For these reasons, using the cloud means that data is often out of your control. Yet you need to protect the data you can least afford to lose: your intellectual property (IP), nonpublic financials, strategic plans, customer lists, personally identifiable information belonging to customers or employees, and other sensitive data residing in your cloud services.

A good CASB provides robust and thorough DLP capabilities covering both structured and unstructured data, all major file types and with support for keyword search, pattern matching, data classification, validation, proximity, regular expressions, fingerprinting, exact match, international support, and more.

More than one-third of all data leakage policy violations (violating a DLP profile such as PHI, PCI, or other confidential information) occur on mobile devices.

The consequences of a data breach can be huge:

- Your company could end up spending millions of dollars to remediate systems, notify customers, pay fines, and settle legal actions following a significant data breach.
- Loss of reputation following a significant data breach can have a long-lasting negative impact on company value.

Enforcing Policies

A cloud security policy is only as good as you can enforce it. Here's how:

- **Enforce activity- and data-level policies rather than blocking the cloud.** You allow people to still use their favorite services, and only block certain activities. The last section in this chapter, "Blocking Risky Activities, Not Services," goes into greater depth.
- **Enforce policies on data whether being uploaded to, downloaded from, or residing in cloud services.**
  - Inspecting content as it's being uploaded to and downloaded from the cloud
  - Inspecting content that resides in your services, regardless of when it was uploaded or created

  Introspection is useful when you need to retrieve, encrypt, or quarantine sensitive content that resides in cloud services. It also covers data that is inserted into your cloud service by other ecosystem services.

- **Enforce policies whether you manage the cloud service or not.**
- **Enforce policies in real time and in context.** This includes user, cloud service, cloud service category or instance, device, activity, and content.
- **Coach users on policy violations.** You can direct users to the right action (like a link to sign up for a sanctioned service), or give them the opportunity to report a false positive or bypass the policy with a short business justification.

Controlling cloud services

Controlling cloud services is a big part of enforcing a cloud policy. You can set and enforce granular policies that take effect across whatever services you specify (one service, one service instance, or a category of services) in a few clicks.

In your CASB, you should be able to specify a variety of actions as an outcome of policy noncompliance. You can block, alert, bypass, encrypt, coach users, or begin a workflow to remediate, record, or report on an out-of-compliance event or activity.

Defining actions

There are number of actions you can take when you find company-sensitive information, as shown in Figure 4-5. You can set up a policy that

- Sends an alert when content matches your DLP profile
- Blocks cloud transactions (upload, download, share, and so on)
- Encrypts the content as it's being uploaded or created
- Quarantines the content for review by a designated IT or legal professional

For example, if you want to set sophisticated, precise policies, here's the start to a policy:

- Enable the use of collaboration services, but prevent or closely monitor sharing of data with people outside of the company.

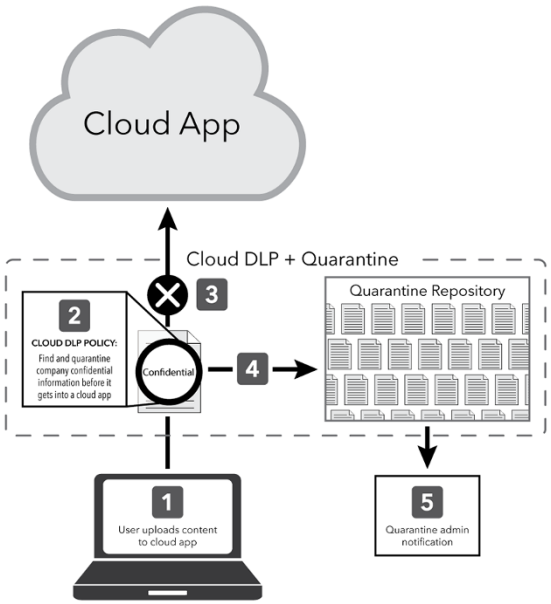

Figure 4-5: You can set up several different actions based on information.

- Disallow file uploads to file-sharing services that contain highly sensitive data or intellectual property that, if ever leaked, stolen, or modified, could cause serious damage to the company.
- Allow people in the HR and finance groups worldwide to access HR or finance/accounting services, but block anyone outside the headquarters country from downloading salary information.
- Allow users in sales to share any public collateral while preventing them from downloading content deemed confidential from a file-sharing service.
- Block any user located outside your country from downloading contacts from any customer relationship management (CRM) service.
- Encrypt sensitive content in context as it's being uploaded or when it's resident within services.
- Alert IT if any user in investor relations shares content from a finance/accounting service with someone outside of the company.
- Enforce granular, specific policies on any of the visibility parameters or DLP profiles.
- Set policies once and have them enforced in real time in any service, at the service, service instance, or service category level.
- Enforce policies if there is sensitive data involved, whether or not you manage the service.
- Enforce policies in real time, before an undesired event or behavior happens.
- Allow data uploads only to services that have a risk score of "medium" or above, and block uploads to the rest.
- Coach users on policy violations to educate them about risky behaviors and to create transparency.

You have to enact a cloud policy that people can get behind. It also needs to be transparent to users and not get in the way of their experience. Otherwise, they'll simply use unsanctioned services to get around your policy.

Coaching End-Users and Giving Them a Say

People know how their cloud services work. And when they don't work the way users expect because you've blocked the service or an activity, they get frustrated.

When you need to enforce policies, it's always a good idea to coach users. Here's why:

- You can change the way employees use cloud services.
- You create transparency about policy and rationale.
- You give users some control and a say in the policy that affects them.
- You can change in what circumstances people use a service with a fine-grained policy.

Coaching can mean simply letting users know that you've blocked them from an activity because it's against company policy, such as the alert shown in Figure 4-6.

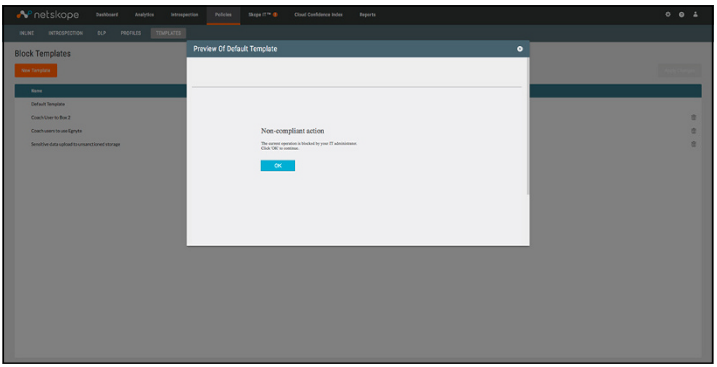

Figure 4-6: An alert telling the user he's blocked from that activity.

But even more useful is to give employees alternatives:

- **Block them from uploading content to an unsanctioned service.** You can then redirect them to a sanctioned service to upload the content.

When an activity is blocked, a custom coaching page takes the end-user through a step-by-step process to mitigate risks.

- **Allow the activity anyway.** You can configure the system to let the user continue and enter a short business justification so you can report it for compliance at a later date.
- **Let users indicate that the activity is a false positive, and let them continue.** You gather useful user feedback, making your detection and policy enforcement stronger.

When an activity is blocked, the user is routed to a coaching page giving these alternatives.

Blocking Risky Activities, Not Services

Cloud policy enforcement doesn't need to be an all-or-nothing proposition. There's no need to block services entirely when you can simply block risky activities.

Some examples of blocking activities rather than blocking services outright include the following:

- Downloading salary data if the user is outside of HR
- Sharing documents outside the company during a quiet period
- Uploading sensitive content to certain services
- Viewing but not downloading information

When you take a more nuanced approach — blocking risky activities rather than apps — employees will be more willing to adhere to your policy.

Chapter 5

Ten Must-Haves to Ensure Secure Usage of Cloud Services

In This Chapter

- Discovering, segmenting, and securing your cloud services
- Creating policies to audit cloud activities, detect anomalies, and protect data
- Coaching end-users to ensure compliance

Embarking on cloud security can seem like a daunting task, even for the most experienced IT professionals. Here are ten must-haves you need to ensure that you're successful with your transition to the cloud:

- **Discover cloud services.** Discover the services in your environment and assess their risk — both inherent and in the context of how they're used. Understand their category and identify the sanctioned ones.
- **Secure and control access.** Secure access to your sanctioned cloud services with single sign-on (SSO). Consider multi-factor authentication for business-critical services or ones containing sensitive data. Also, enforce adaptive access controls based on context, such as user group or device type or classification.
- **Audit activities.** Understand user and administrator activities and their context. Who's downloading from HR services? Who's sharing content outside of the company, and with whom? Who's escalating privileges in IaaS?

- **Understand content.** Understand and classify sensitive content residing in, or traveling to or from, your cloud services. Monitor and alert on sensitive or data moving into the cloud or leaking from the cloud.
- **Detect anomalies.** Monitor cloud services for anomalous activities that could signal compromised credentials, security threats, noncompliant behavior, data theft or exposure, and even malware.
- **Enforce granular policies.** Define granular policies that are enforceable in real time, across both sanctioned and unsanctioned services, regardless of whether users are on-network or remote, and whether accessing from a browser, sync client, or mobile app.
- **Protect data in context.** Have a data protection strategy. For highly sensitive content that can't be in the cloud at all, define policies that prevent it from being uploaded to any cloud service. For the next tier of content that can reside in the cloud, apply the appropriate level of security policy. This may include encrypting sensitive or regulated data en route to the cloud and/or limiting sharing options once it's there.
- **Detect and respond to cloud threats.** Detect cloud threats such as malware and ransomware propagating in cloud services. Respond by remediating malware and alerting the rest of the security infrastructure so it can take action such as isolating endpoints and terminating malicious processes.
- **Ensure compliance.** Ensure regulatory compliance with continuous cloud monitoring, maintenance and review of cloud audit trails, threat remediation, and comprehensive reporting.
- **Coach users.** Coach users both through conversations and in an automated way. Let them know when they've done something that's out of compliance (ideally in real time, as the action is occurring), whether you block them, let them report a false positive, or allow them to enter a business justification.

Netskope is the Leader in Cloud Security

We help organizations understand online activities, protect data, stop threats, and respond to incidents.

Netskope — security evolved.

netskope

Take your company into the cloud securely

The cloud enables business users to work more productively and flexibly, whether on a computer, tablet, or smartphone. But doing business in the cloud comes with security concerns. How do you ensure compliant cloud usage and protection of your sensitive corporate data? This book answers all your questions so you can conduct business securely in the cloud.

- ***Find and assess your cloud risk* — *find all of the cloud services in your organization and see how risky they are***
- ***Understand your cloud usage* — *drill into who's using cloud services, what they're sharing and downloading, and more***
- ***Develop a cloud policy* — *develop a cloud policy that people can get behind, while still getting their work done***
- ***Protect against cloud threats* — *find and remediate malware in cloud services***

Open the book and find:

- **How to assess cloud service risk**
- **How to protect sensitive data in the cloud**
- **How to stop and remediate cloud threats**
- **The steps to create an effective cloud policy**
- **The ten must-haves for cloud security**

Go to Dummies.com®
for videos, step-by-step examples, how-to articles or to shop!

Lebin Cheng is Netskope's vice president of application engineering. **Ravi Ithal** is Netskope's chief architect. **Krishna Narayanaswamy** is Netskope's chief scientist. **Steve Malmskog** is Netskope's chief network architect.

FOR DUMMIES®
A Wiley Brand

ISBN 978-1-119-39599-7
Not for resale

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.