Security Intelligence:
THE NEW FRONTIER FOR PROTECTING CORPORATE DATA IN THE CLOUD
Introduction

Data Theft from Cloud Systems of Record

6-Step Process to Protect Data from Insider Threats and Compromised Accounts

Data Exfiltrated via Cloud Services

4-Step Process to Prevent Data Exfiltration

Important Considerations for Improving Cloud Security
INTRODUCTION

The recent spate of damaging data breaches has brought cyber security into the spotlight. The issue is now so pressing that the President of the United States was compelled to issue an executive order on April 1, 2015 declaring a national emergency to deal with the threat of cyber security. Echoing this sentiment globally, Inga Beale, CEO of Britain’s largest insurer, Lloyd’s of London, said “Cyber risk poses the most serious threat to businesses and national economies, and it’s an issue that’s not going to go away.”

This recognition is an important step in developing a stratagem to address this issue, which has far reaching implications for both individual consumers, businesses, and the economy as a whole. Traditionally, cyber security efforts were focused on protecting the company’s perimeter and keeping cyber criminals out of their networks. However, with breaches becoming a weekly, if not daily, occurrence, more and more security professionals have to work with the assumption that malicious hackers have already broken into their corporate networks. The big question is no longer how do we keep cyber criminals out of a corporation’s network but rather how do we protect the corporate data and limit the damage when a breach occurs?

Just as enterprises get a handle on monitoring & protecting their networks against cyber crime, their plans are being challenged by the explosion of cloud service usage, extending their risk surface area from within their corporate network into third-party environments. Skyhigh’s most recent Cloud Adoption and Risk report indicates that the average company uses 923 cloud services today. Highly valuable data in ERP, CRM, CMDB, and Collaboration systems has been migrating to the cloud, and cloud services are becoming the de facto systems of record for customer data, financial data, employee information, and other corporate intellectual property. Given the rate of adoption over the last five years, one can expect that the majority of companies’ systems of record will soon live in the cloud.
Many companies have overlooked these challenges, and as a result, the cloud has created a cyber-security blind spot, which can be broken down into two distinct risk vectors: 1) Data stolen from cloud-based systems of record (e.g. Salesforce, Box, ServiceNow, Success Factors, etc.) and 2) Data exfiltrated from the enterprise via cloud services.

**The Growing Challenge of Cloud**

1. Data Stolen from Cloud-based Systems of Record
   - B2B Connections with High-Risk Partners
   - Compromised Accounts
   - Insider Threats

2. Data Exfiltration via Shadow IT
   - Data Exfiltration via Shadow IT

In this paper we will provide examples of breaches occurring in each of these areas and offer guidance on how to protect your company from data loss across these two vectors.
DATA THEFT FROM CLOUD SYSTEMS OF RECORD

Many companies now house their most valuable data in IT-sanctioned cloud services such as Salesforce, Box, ServiceNow, 0365, SuccessFactors, Workday, Jive, and Google Drive. This can include customer information, employee information, financial data, IT infrastructure data, and intellectual property. In addition to compliance requirements, this also creates an imperative to protect the data within these systems. While companies spend billions of dollars guarding access to on-premises systems of record, they often overlook protecting their cloud-based systems of record, perhaps because they expect the services themselves have a higher level of security. However, the security of the services themselves cannot protect the organization from insider threats, compromised accounts, or high-risk third-party applications downloading data from these systems of record.

Here are a few examples to help illustrate how insider threats and compromised accounts can be used to steal valuable data from an organization.

**Salesforce:** An account manager at a professional services company planned to leave his current company and join a competitor. Prior to leaving, he mined Salesforce for all the customer and prospect data in his territory. To do so, he logged into Salesforce and ran reports for all contacts, leads, opportunities, and customers in the West region, downloaded the reports, and then saved them to a USB.

**ServiceNow:** An IT contractor had been provided access to an organization’s configuration management database ServiceNow. Unfortunately this contractor’s credentials were compromised and exposed in the Darknet. These credentials were used to login and gather intelligence of sensitive network and system configuration details that elevated the enterprise’s cyber-risk.

**Office 365:** An executive at a high-tech company was collaborating on a folder with multiple design documents with a partner organization. One of the partner’s employees moved to a competitor and continued to have access to sensitive files including financial projections, product roadmaps, and other intellectual property.
These examples serve to show that the use of even the most secure services can present risk to a company if there is an insider threat or compromised account. Organizations across verticals such as Construction, Defense, Federal Government, Financial Services, Healthcare, High Tech, Manufacturing, Media, Oil & Gas, Professional Services, Retail, State and Local Government, Transportation, and Utilities are utilizing Skyhigh to protect their organizations from insider threats and compromised accounts using a six-step process.

**SIX-STEP PROCESS TO PROTECT DATA FROM INSIDER THREATS AND COMPROMISED ACCOUNTS**

**STEP 1: AUDIT THE SECURITY SETTINGS OF YOUR SANCTIONED CLOUD SERVICES**
Many cloud services have advanced security features such as two-factor authentication that may or may not be enabled. Using Skyhigh, organizations can audit the security settings of their mission critical cloud services and modify settings where needed based on best practices in the industry.

**STEP 2: MONITOR ALL CLOUD ACTIVITY IN SANCTIONED CLOUD SERVICES**
Identifying malicious behavior begins with monitoring activity. Using Skyhigh, organizations gain deep visibility into all user, admin, and third-party application activities with drill downs into the actions and objects. Skyhigh also provides a live log of all activity for forensics and investigations.

**STEP 3: IDENTIFY ANOMALIES INDICATIVE OF INSIDER THREAT OR COMPROMISED ACCOUNTS**
With hundreds or thousands of users, it can be difficult to discern activities within cloud-based systems of record that indicate a security incident. Using Skyhigh, organizations leverage behavioral analysis to identify and prevent data loss from compromised accounts and insider threats, driven by anomalies that take into account the context of the user (e.g. role, privilege level, reputation), application, data, action, device, and location.

**STEP 4: ANALYZE OUTSIDE COLLABORATORS WITH ACCESS TO SANCTIONED SERVICES.**
The average company is connected to 1,555 business partners via cloud services. Using Skyhigh, organizations identify all outside partners collaborating with their company via the cloud and leverage risk ratings for each partner to identify potential areas of risk.
**STEP 5: ANALYZE THIRD-PARTY APPS WITH ACCESS TO YOUR SANCTIONED CLOUD SERVICES.**

Security is only as strong as the weakest link, and in many cases third-party apps with access to your mission-critical cloud services are the weakest link. For example, Salesforce has enterprise-grade security, but a mobile CRM application used by a rep that connects to Salesforce using the rep’s Salesforce credentials may not, as is the case with the hundreds of Force.com and third-party apps that have access to data in Salesforce. Using Skyhigh, organizations identify all third-party applications connected to cloud services, assess the risk of these applications, and monitor all data moving to the application.

**STEP 6: ENSURE THAT SENSITIVE DATA IS NOT STORED IN THE CLOUD IN VIOLATION OF COMPLIANCE POLICIES**

Many companies are subject to compliance requirements such as PCI DSS, HIPAA, HITECH, GLBA, SOX, CIPA, FISMA, and FERPA which dictate that sensitive personal or financial data must be protected. Using Skyhigh, companies conduct sensitive data analysis to identify all sensitive data (such as PII, HIPAA or corporate IP) stored in the cloud, where the data is located, who is accessing it, and whether it constitutes a compliance or DLP policy violation.

**DATA EXFILTRATED VIA CLOUD SERVICES**

Due to the large number of unmonitored cloud services in use, the cloud has become the exfiltration vector of choice for remote cyber criminals. Once they have infiltrated corporate systems to steal data, they need a way to get it out. What they realize is that the proliferation and widespread adoption of cloud services within the enterprise has created a proverbial haystack, inside which they can hide their needles – that is, the stolen data they wish to export from the enterprise to their possession.

Here are a few examples, some startlingly clever, to help illustrate the variety of methods used by attackers to exfiltrate data via the cloud.
Twitter: Attackers infected a bank employee’s corporate laptop with malware that collected sensitive data from the local machine. In order to exfiltrate the data, the malware initiated a Twitter session and then exfiltrated the customer data 140 characters at a time over a sequence of 86,000 tweets.

Youtube: Attackers compromised a large manufacturing company’s internal systems and gained access to valuable information. In order to exfiltrate the stolen IP, the attackers created VAR segments, leveraged stenography to insert the stolen data into mpg4 files, and then uploaded them onto YouTube. The videos would play within YouTube, but once downloaded the VAR segments could be unpacked, providing the attackers with the stolen data.

Evernote: Attackers hacked a public-facing administrative website for a healthcare provider and obtained admin credentials. Once they had infiltrated the on-premises systems, attackers queried the customer records database and downloaded all its personally identifiable information (PII) PII including SSNs, names, addresses, etc. The attackers then exfiltrated all this sensitive data by uploading the data to a personal Evernote account.

These examples serve to show that the way in which a service is used, not just its security capabilities or lack thereof, can create significant risk for organizations. Organizations across verticals are utilizing Skyhigh to safeguard against cloud-based data exfiltration using the following four-step methodology.

FOUR-STEP PROCESS TO PREVENT DATA EXFILTRATION

STEP 1: GAIN VISIBILITY INTO ALL CLOUD USAGE
The first step in preventing data exfiltration is to identify and understand all the potential cloud paths out of the organization. Using Skyhigh, organizations uncover all cloud services in use including SaaS, IaaS, and PaaS, and understand usage with detailed statistics including service access count, upload and download volume, and user count.
Skyhigh helps organizations triage their risk management by providing detailed risk ratings for each service based on over 50 attributes developed in conjunction with the Cloud Security Alliance.

**STEP 2: GAIN VISIBILITY INTO ALL OUTBOUND TRAFFIC FROM THE ENTERPRISE**

In addition to cloud services, attackers may attempt to upload stolen data to other destinations such as an FTP site or a website. Using Skyhigh, organizations can identify and analyze all unmatched uploads. Trusted destinations in the Internet (such as sanctioned cloud services) and untrusted domains (like many dropzones and unsanctioned file sharing services) are conduits of data leaving the enterprise. Skyhigh helps organizations gain visibility into outbound traffic to these destinations using multiple protocols.

**STEP 3: ANALYZE THE EFFECTIVENESS OF CLOUD ACCESS POLICIES AND REMEDIATE ANY “PROXY LEAKAGE”**

Many organizations believe they are blocking traffic to all or some cloud services, but in reality they are only partially blocking access. This “proxy leakage” is the result of either inconsistent policies across a patchwork of firewalls and proxies, or mismanagement of exceptions which are often intended for individual employees or individual services but, in reality, are granted to entire business units or categories of services. Using Skyhigh, organizations can analyze allow/deny statistics, identify policy enforcement inconsistencies, and eliminate them using Skyhigh’s closed-loop remediation leveraging their firewalls and proxies.

**STEP 4: ANALYZE USAGE TO IDENTIFY ANOMALIES AND MANAGE SECURITY INCIDENTS**

With the vast number of services used in an organization, identifying malicious data exfiltration can feel like looking for a needle in the haystack. However, using Skyhigh, organizations leverage machine-learning algorithms to identify anomalous activity indicating a data exfiltration event. The network effect of Skyhigh’s more than 17 million users strengthens the accuracy of anomaly detection, thereby reducing false positives and the time required to investigate them.
IMPORTANT CONSIDERATIONS FOR IMPROVING CLOUD SECURITY

Using the steps above, over 400 companies have eliminated significant blind spots in their cyber security operations. There are three key factors you should consider before selecting a cloud cyber security solution:

CLOUD CYBER SECURITY REQUIRES A HOLISTIC APPROACH
As evidenced above, cyber security threats are not isolated to shadow cloud services or sanctioned cloud services. Companies must enable security capabilities across both types of cloud services in order to fully protect the organization from sensitive data loss, so ensure that your cloud security platform has deep capabilities for both shadow IT and sanctioned IT services.

ALL ANOMALY DETECTION IS NOT CREATED EQUAL
More is not always better, but in the case of big data it certainly is. Larger data sets lead to more robust data models and thus more accurate anomaly detection. Anomaly detection algorithms, if not carefully tuned, can also generate a large number of false positives and create more work for an already overworked SOC. Companies should favor anomaly detection products that benefit from network effects generated through work with a large number of organizations and take into account the context of the user (e.g. role, privilege level, reputation), application, data, action, device, and location.

ENABLE ACTION NOT FEAR
Providing information is one thing, but enabling action is quite another. The volume of data related to cloud usage can be overwhelming for companies that have gained visibility for the first time. Look for solutions that go beyond presenting data and enable policy-driven remediation (e.g. block, quarantine, encrypt, force two-factor authentication) and leverage existing firewalls, proxies, SIEMs, and DLP systems where applicable.

To gain visibility and control over the cloud contact Skyhigh Networks today.