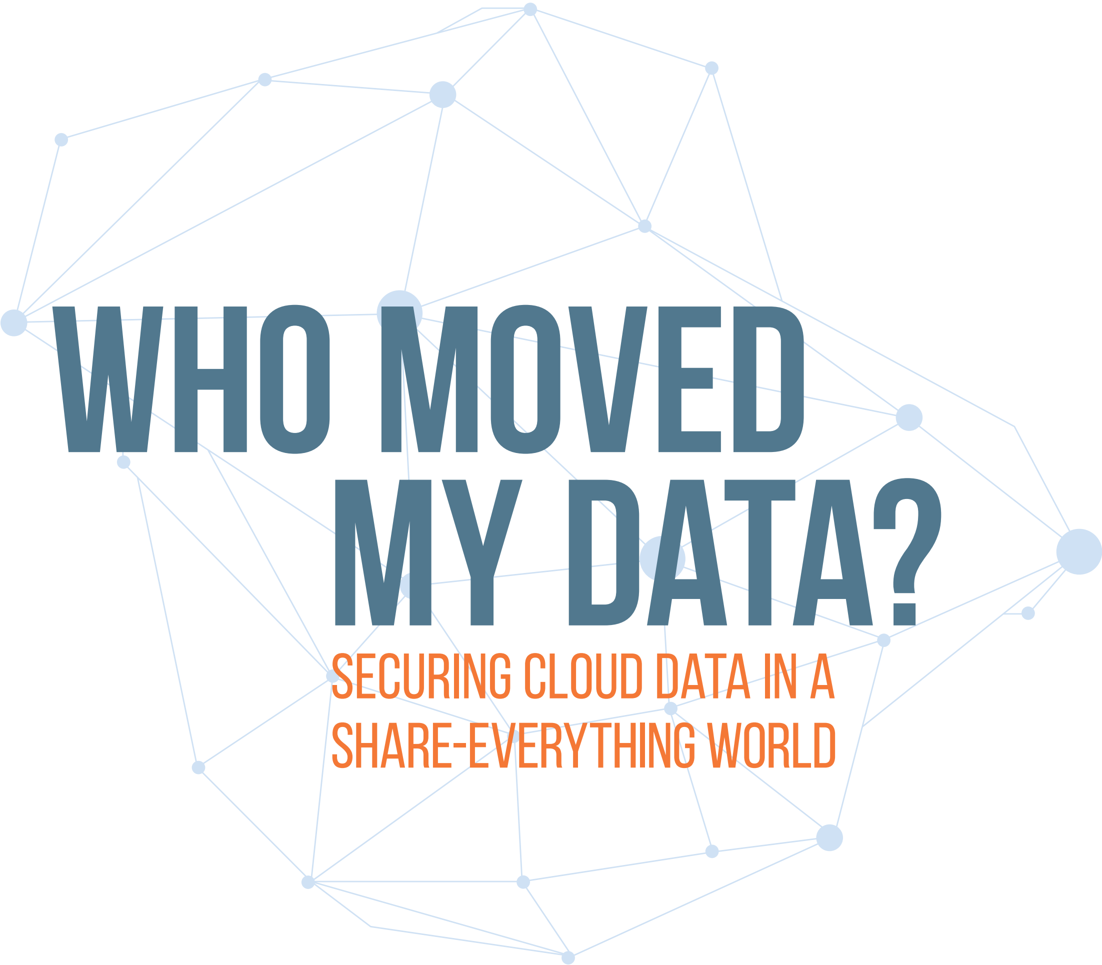
WHITE PAPER

proofpoint.



WHO MOVED MY DATA?

SECURING CLOUD DATA IN A SHARE-EVERYTHING WORLD

TABLE OF CONTENTS

INTRODUCTION

Cloud-first is the catalyst enabling organizations to digitize services and transform operations to attract the digitalized business and consumer. As part of this trend, many are embracing cloud and software-as-a-service (SaaS) apps. These flexible architecture can accelerate time to market, enable business partners, and reduce the complexity of managing IT infrastructure.

Cloud-based services used to be a giant leap of faith. Organizations questioned whether their data would be safe—and for good reason. Security controls for the cloud, such as encryption and data-loss prevention (DLP), were spotty at best. And extending enterprise security and access management tools to cloud services was difficult.

Today, the cloud has become an established part of the enterprise. Email services are most IT teams' first experience with cloud-based enterprise applications. At the same time, many other enterprise applications and services have broken through the corporate perimeter.

While the initial hesitation about cloud-based services has faded, the security challenges remain. Security teams are caught in the precarious position of either restricting these services—and hindering their organization's digital transformation—or ushering in even more risks.

Members of the Cloud Security Alliance, a nonprofit that promotes ways to bolster cloud security receive about 10 requests on average each month to approve new services. And more than 70% are planning to increase support for new cloud apps and subscriptions. Most employ formal processes for users to request new cloud services and are evaluated on their ability to support enterprise security and privacy policies.[1]

This paper explores new risks emerging from the shift to cloud-based services, the pitfalls of common approaches to cloud security, and what you can do to protect your people, data, and brand in the cloud era.

[1] Cloud Security Alliance. "The Cloud Balancing Act for IT: Between Promise and Peril." January 2016.

DIGITAL CUSTOMER EXPECTATIONS SPUR CLOUD GROWTH

A quick survey of cloud computing trends tells an interesting story about what's driving the growth across industry sectors for applications in the cloud.

Digitalization initiatives with financial service industries is being driven by savvy consumers that expect automated services and personalization. Microsoft Office 365 is proving to be the enabling layer of infrastructure to enhance productivity in key areas of front line service, including:[2]

Case Management: Claims processing and underwriting of insurance policies

Self-Services: Agent and broker portals to access documents and templates

Loan Origination: Document management and case coordination

Not too long ago healthcare organizations primarily saw cloud services as a way host healthcare information exchanges. Now, the healthcare industry is poised to triple the use of cloud services over the next several years. Cloud-based repositories such as Box coupled with direct messaging protocols are being used as the underlying infrastructure to share DICOM files, medical records and sensitive research files throughout the continuum of care.[3]

Within higher education, the early adoption of cloud services in the areas of back-end systems (HR, CRM and SIS) to reduce costs is now transforming into initiatives to attract the digitally driven student. They have high expectations of anytime, anywhere learning and access to information and productivity tools. Cloud-based productivity suites like G-Suite or Microsoft Office 365 enable all students to freely share information and avoids any incompatibility issues as all files can be shared across all devices in use.[4]

Civilian Federal and public sector agency transformation is driven by the dueling priorities of meeting compliance mandates and improving citizen engagement. No longer the last bastillions to move to the cloud, 82% of government organizations are increasing spending on cloud computing initiatives. Today, 33% of apps are run in the cloud and by 2021, 58% are predicted to run in the cloud.[5] Interestingly, self-service tools is one of the most widely deployed online apps to improve citizen service and engagement.[6]

[2] Gartner Consulting Report, Office 365 Industry Addressability Study July, 3 2017
[3] HIMSS Analytics 2016 Cloud Survey, The Cloud Evolution in Healthcare (not in copy)
[4] Technavio, Global Cloud Computing Market in Education Sector 2017-2021, August 2017
[5] Meritalk, Destination Cloud: The Federal and SLED Cloud Journey, September 19, 2016
[6] Deloitte Government Business Counsel, The Path to Customer-Centric Service, June 2015

RISK REMAINS UNDER THE COVER OF THE CLOUD

The way employees work and share data between cloud services and accounts is a growing problem. Shadow IT and unchecked cloud growth is only one facet to the complex problem of security in the cloud. Credential phishing is the No. 1 way attackers gain access to cloud repositories of PII and other sensitive data.

Just like its email counterpart, cloud-based attacks rely on the "human factor" to spread malware. They trick people into opening malicious documents, clicking malicious URLs and providing account credentials to attackers looking to steal data and profit from ransomware.

Some of the biggest risks of cloud-based infrastructure are third-party apps, abandoned services and orphaned accounts, and personal accounts used to store company data.

At the same time, attackers are pivoting to cloud, creating new levels of risk. They upload malicious documents to public-facing cloud services. They hijack synchronization tokens in so-called "man-in-the-cloud attacks." And they create malicious add-on apps.

IT teams can't just push the wait button without exposing the company to further attacks and compliance risks.

BEYOND THE REACH OF IT

Third-party business apps can streamline work. But employees rarely think about how those "shadow IT" apps, which operate without the support or knowledge of the IT department—can siphon corporate data, contact lists or hijack their device.

ABANDONED SERVICES, ORPHANED ACCOUNTS

Cloud services are great for special projects because services can be ramped-up quickly. But when the project is done, the services may not be fully decommissioned, leaving internal information in place and out of reach of IT. And when employees leave, they may still have access because no one thought to revoke their access.

PERSONAL ACCOUNTS STORING COMPANY DATA

The cloud makes everything shareable. Employees often store corporate data on their personal cloud accounts to afford them anytime, anywhere access to their work. With multiple personal and corporate accounts in the cloud, corporate and PII data are all too easily intermingled between accounts. Sensitive information can be shared with the wrong person—or even worse, with everyone.

ATTACKERS PIVOT TO THE CLOUD

Attackers bypass traditional security controls through external-facing cloud applications. It can be as easy as uploading a weaponized document to a corporate website. That's what happened in 2015, when someone uploaded what looked like a resume to the job-hunting website CareerBuilder. The "resume" was actually a malicious Word document that infected dozens of companies.[7]

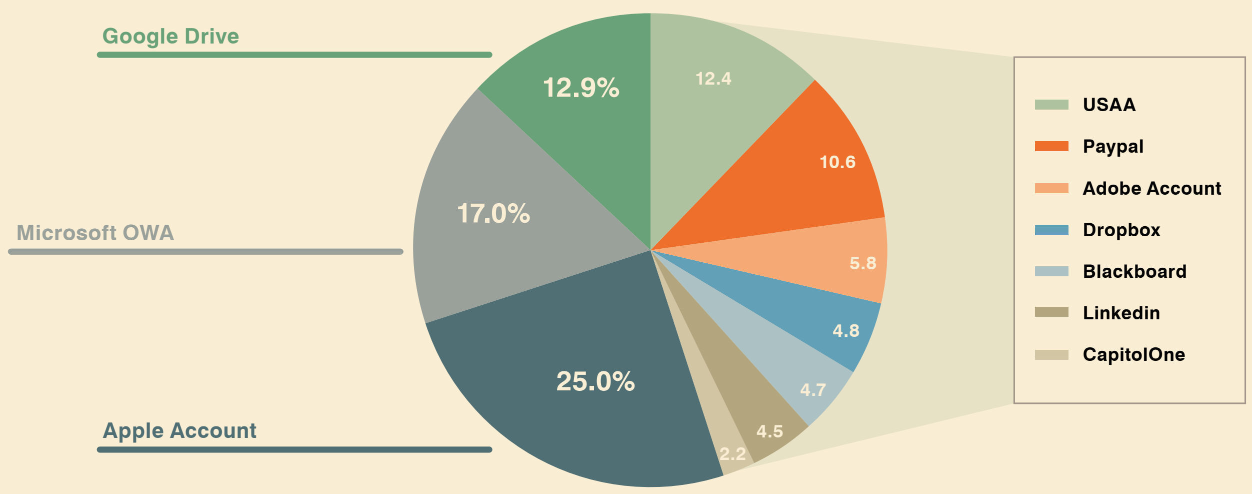
More than 90% of URL-based threats in email led employees to a credential-phishing page last year.[8] Credential phishing attacks aimed at gaining access to corporate data in Google Drive, Office 365 and Dropbox are becoming a preferred attack method. With access to your cloud based systems, spreading an infection is as easy as posting a malicious document or URL. These attacks can take the form of a trusted document such as an employee survey or resume or even a harmless-looking URL posted in Salesforce or Slack. The data you trust to your SaaS applications is becoming the next target for attackers.

[7] Infosecurity Magazine, Hackers Target Careerbuilder to Push Malware, May 6, 2017
[8] Proofpoint, Inc. Human Factor Report 2017

One in every three organizations has malware in its cloud-based repositories and don't know it.[9] And more than 60% of organizations do not scan their SaaS applications for malware.[10] Perhaps most disturbing, among the organizations that did scan for malware, more than half found malware.[11]

Last year, credential phishing lures for cloud SaaS applications accounted for more than half of all credential phishing attacks. Google Drive, Microsoft OWA and Apple made up most of these attacks. Emails sent to steal Apple credentials were the most widespread. Google Drive lures where the most clicked.[12]

Top 10 Credential Phising Lures of 2016



Proofpoint, Human Factor Report 2017

MAN IN THE CLOUD (MITC) ATTACKS

Man-in-the-cloud (MITC) attacks take advantage of file-synch services your employees use to exchange files wherever they're working. MITC attacks are as difficult to detect as a credential-phishing attack. That's because the behavior of a compromised endpoint or account looks like a user is doing everyday business.

It usually starts out as a targeted email attack. The attacker uses social engineering to trick the user into running malicious code, which gives attackers access to an employee's synchronization token used to determine who and what outside apps have access to the account. With a copy of the token, attackers can exfiltrate files, set up command-and-control (C&C) communications and upload malicious files to set off a chain of malware infections.

What makes this attack particularly disturbing is how well an attacker can hide their tracks after the initial compromise. With a copy of an employee's file synch token, they can put the original token back and virtually erase all indications that a breach occurred.

This attack is also distressing because attackers are uploading documents that look like ones employees and business partners need. Because they are accessing the files through trusted portals, collaboration or customer service ticketing systems, employees and partners assume they are safe. They skip the normal precautions they would take when downloading files from unknown sources.

[9] Ponemon Institute.Cloud Malware and Data Breaches: 2016 Study

[10 & 11] ibid

[12] Proofpoint, Inc. Human Factor Report 2017

Traditional cloud access security brokers (CASBs), the usual policy-enforcement point in cloud defenses, are not equipped detect subtle changes typical of MITC attacks.

The most effective way to mitigate these threats is by detecting and blocking attacks at the earliest possible point in the attack chain. Email systems and file-synch services are used hand-in-hand in most MITC attacks. One of the few ways advanced threats like MITC attacks can be detected is through user behavior analytics. That means correlating malicious activity at the email gateway with anomalous user actions, such as synching data to a new device or logging in from somewhere the user never has before.

THIRD-PARTY ADD-ONS

G Suite and Office 365 support large ecosystems of third-party apps. These third-party apps afford users many choices when it comes to boosting productivity, making collaboration easier, and giving users more visibility into colleagues' activities.

Most of these third-party apps are legitimate. But many are poorly constructed. They may access more data than they need to work. Or they may have loosely defined sharing features, making it too easy for users to accidently share or expose company data.

Most data breaches in the cloud happen through poor app design or user error. But for the cutting-edge attackers, counterfeit cloud apps are a great way to get unfettered access to a victims' data.

This nightmare scenario happened earlier this year. Attackers created a counterfeit version of a popular Google app and managed to get it listed in the G Suite Marketplace. Close to a million users allowed the app to connect to their Google account, potentially exposing their company's information to attackers.[13]

THE CLOUD ECOSYSTEM IS EXTENSIVE. CONSIDER THE FOLLOWING:

- Slack's App Directory includes 500 apps
- Israel's leading business software market place, DiscoverCloud hosts more than 3,000 business applications
- AngelList includes more than 12,000 SaaS start-ups
- Salesforce has 2,948 apps listed on its public AppExchange
- G Suite Marketplace has close to 1,000 business applications

Employees rarely think about the data third-party apps are accessing or where they downloaded them. Productivity, social and data sharing apps are prolific among employees and business partners. Sometimes, these apps seem completely benign but siphon data from cloud apps, contact lists or everything else in your mobile device.

COMMON CLOUD-BASED SECURITY PRACTICES

IT organizations take a number of measures to better manage their risk. Active vetting of cloud services has been the primary way IT organizations have responded to the popularity of cloud business apps.

Here are the most common tactics IT teams use to secure cloud based IT projects—and where they may fall short.

WHITELISTING CLOUD APPLICATIONS

Whitelisting may seem like a simple solution to keep employees off unsanctioned cloud apps and SaaS services. But whitelisting, like least privilege policies, has well-known pit-falls IT teams must contend with. First, the practice does not prevent employees from requesting access to cloud applications, so it's another ticketing and vetting process to support. Without timely approvals, company information eventually lands on personal devices and potentially gets exposed to the application you were trying to prevent access to in the first place. Another scenario whitelisting can't address is the known good app that infects users with an update injected with malicious code.

[13] Proofpoint. "Silver lining: Google OAuth worm leads to Proofpoint discovery and Google mitigation." July 2017

INSPECTING CLOUD TRAFFIC

Similar to network traffic monitoring, this usually includes monitoring for connections to known bad IP addresses. Other monitoring tactics may include monitoring for signs of command and control traffic and anomalous behavior.

This approach usually means having to inspect secure sockets layer (SSL) traffic, which can slow users' upload and download speeds. And beyond blocking access to known bad IPs, pinpointing malicious activity can be difficult—it looks a lot like legitimate traffic.

MICRO-SEGMENTING CLOUD WORKFLOWS

Similar to the concept of least privilege, micro segmentation limits access to cloud-based workflows. It enables you to enact security policies all the way down to the workload level.

While this can be a useful strategy to lock down user access to cloud-based business processes, it comes with a high-level of administrative overhead for security teams.

First, the team would need to transition all of their firewall definitions and access control lists (ACL) to accommodate a cloud-based environment. This is a tedious exercise that keeps security teams stuck doing continual updates of definitions and ACLs and supporting thick security clients on host systems.

Also, micro-segmentation can help stop lateral movement once malware is inside. But it won't stop it from getting there in the first place.

A BETTER WAY TO PROTECT AGAINST ADVANCED THREATS TARGETING SAAS SERVICES AND USERS

The threat landscape is always changing. But most attacks share a common trait: they target people. Credential phishing focuses on getting access to your cloud services and repositories. Cyber criminals are actively harvesting credentials so they can:

- Exfiltrate or expose valuable data for financial gain or notoriety
- Distribute malware using externally facing systems and portals—upload malicious documents and URLs to ticketing, collaboration or other types of external portals
- Take advantage of permissions/configuration mistakes to pilfer data
- Embed C&C communications in known "good" IP addresses to carry out attacks
- Spread malware infections throughout your organization and ecosystem of partners, and customers

Don't bridge the cloud security gap with traditional security processes and controls. Traditional security tools are the least effective security technologies for the cloud. Physical firewall and IDS/IPS appliances, DLP gateways, switch-and router-based ACLs, and VPN solutions are not built to secure user interactions and your cloud data.

Our researchers are drawing clear connections between email-based credential-phishing attacks and breaches that use sanctioned cloud services.

Whether you believe your security in the cloud practices are good enough (most security professionals don't), assess your defenses with the following key areas in mind.

ADVANCED THREAT AND TARGETED ATTACK PROTECTION

Malware hitting corporate cloud repositories has a variety of uses to the cyber criminal; they can siphon data, set up shop for their next campaign under a legitimate IP address, or spread a ransomware or Trojan infection.

All they need to do is keep innovating with new schemes and variants. Just like email, you can't rely on detection-based solutions. Attackers focusing on this vector are innovating, so you need a solution that applies a robust set of capabilities, including:

- Expert analysis into this emerging threat vector from an in-house threat research team
- Current threat data spanning email, social, network, SaaS and mobile apps
- Advanced detection of malicious attachments and URLs with a cloud based sandbox

Data Loss Prevention

You must think differently about protecting data stored in the cloud than in the traditional DLP set-up. You still want to classify data and apply policies to detect, block or quarantine a suspicious user transmission. And the goal is still to reduce false positives, so you can quickly get to the alerts that matter.

But you need a different approach to how you reduce false positives. Augment your efforts to fine-tune data classifications and policy by correlating the movement of your data to potential threat exposure. To make this connection and reduce the number of false positives, you need visibility into employee communications and what happens to SaaS usage as a result. With visibility into both vectors, you can better pinpoint credential theft and data exfiltration.

Risk-Based Access Control

Many solutions tout robust capabilities in risk-based authentication and access control. This usually includes detecting scenarios where an employee who has always logged in from the Toronto office is now attempting to login from, say, St. Petersburg, Russia. Or maybe it's activity within a doormat account. In this case, the attacker has already infiltrated your cloud store and could be doing damage.

While helpful, this type of detection does not connect clicks on credential phishing emails with actions that might include reducing privileges and mitigate risk. An effective solution detects this activity within email traffic and triggers the right response for access to corporate SaaS applications.

Vetting third-party cloud apps

Applications come from a vast community of developers. Some have secure development practices—others, not so much.

When considering solutions to help the team vet new cloud and mobile applications, simple risk ranking is not enough. A vendor-agnostic solution is important; you can't vet just Office 365 apps and forget the rest. The ideal solution evaluates top SaaS applications and services and gives your IT team a better understanding of how an app behaves in context so you can make informed decisions.

GET A FREE ASSESSMENT

Protect the way your people work by safeguarding SaaS applications. Get a free assessment of your Office 365, G-Suite, and Salesforce deployments today. In a few minutes, we can deploy the SaaS Protection solution to detect hundreds of risks, vulnerabilities and violation scenarios, including:

- Malware
- Phishing
- DLP violations
- Usage violations
- Third-party apps

We'll also help you identify high-risk users and files. You'll receive access to a personalized console and report after one week.

www.proofpoint.com/us/risk-assessment-saas

ABOUT PROOFPOINT SAAS PROTECTION

Proofpoint SaaS Protection secures data in your SaaS apps. We combine threat detection, data-loss prevention (DLP), third-party app control, access control, and analytics to help you protect Microsoft Office 365, Google's G Suite, and more.

www.proofpoint.com/us/products/saas-protection

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.

proofpoint.

www.proofpoint.com