FORCEPOINT
POWERED BY Raytheon

Whitepaper

Forcepoint CASB Sheds Light on the Cloud App Visibility Blind Spot

EXECUTIVE SUMMARY

Enterprise assets are more at risk than ever before. While many executives and IT leaders focus on threats to information assets inside their data centers, they may be missing the largest and most significant blind spot—their ability to see and manage their organization's risk.

Cloud apps such as Dropbox, Box, Salesforce, Office 365 and Google Apps make account creation easy for users, but IT will find it hard to take away access once users start relying on them.

In a competitive marketplace, organizations want to leverage the operational benefits and cost advantages of the Cloud, but a different approach is required if organizations are going enable the safe and productive use of cloud apps and services.

This whitepaper discusses:

- The significant blind spot in visibility and increased risks for organizations in the face of the "Shadow IT" trend, a phrase intended to encapsulate everything from the use of Bring Your Own Device (BYOD) to the creation of individual accounts on cloud apps for work-related activity such as office productivity, email, document sharing and customer relationship management.
- Why traditional controls that secure on-premise environments don't provide the required visibility into user activity and risks related to cloud app use, which means organizations can't address risks and respond to account-centric threats.

"Line-of-business leaders everywhere are bypassing IT departments to get applications from the Cloud (also known as software as a service, or SaaS) and paying for them like they would a magazine subscription. And when the service is no longer required, they can cancel that subscription with no equipment left unused in the corner."

—DARYL PLUMMER, GARTNER ANALYST

SIZING THE BLIND SPOT

Many organizations have embraced public cloud services, covering fast growing SaaS areas such as Office Suites, Digital Content Creation and Business Intelligence. Most organizations do not want to implement wholesale policies that forbid the use of personal devices and cloud apps.

Cloud apps and BYOD policies:

- Provide tangible benefits to organizations by reducing capital expenditures and elastically allocating resources for computing, processing and collaboration.
- Lower operating costs and provide organizations the ability to focus on their core business mission
- Increase user productivity

So, while organizations are aware and have sanctioned cloud apps for some functions, most drastically underestimate the number of unsanctioned, user-adopted cloud apps. In fact, one survey found that organizations underestimated cloud app usage by 90%. Unmanaged personal devices used for work-related activity add to the lack of visibility.

A significant blind spot clearly exists, as organizations lack visibility toward user activity on unmanaged devices accessing unsanctioned cloud apps.

Other scenarios that create blind spots for IT include:

- Authorized users accessing approved cloud apps from an unmanaged endpoint device
- Authorized users abusing their privileges on business-critical cloud apps such as Salesforce, NetSuite and Office 365
- Former employees still accessing cloud apps containing business-critical data
- An organization's cloud app security and configuration settings fall short of industry best practices or don't meet internal guidelines
- Real-time monitoring and control over documents shared through cloud collaboration apps such as Google Apps, OneDrive and Box
- Identifying and tracking cloud app administrators, which is critical since administrators have the ability to create and edit user permissions, change configuration settings and extract or delete entire data sets. For example, AWS administrators can change the configuration of production infrastructure without a complete audit trail of all their actions

IT may not control the endpoint or the cloud app, but are still responsible for their company's information assets. For example, while many service providers offer programming interfaces, an organization is still responsible to set security attributes for developers, control endpoint access and ensure compliance for cloud data.

Can you answer these questions about your cloud apps?

Which apps are being used and by whom?	Where is my data most at risk in the cloud?	Who are my top 10 users?
Who uses file sharing services?	What user activities are suspicious?	How many cloud apps are used worldwide?
Where is data leakage occurring in the cloud?	Where is my data in the cloud?	Who is downloading sensitive data to unmanaged devices?

What challenges do organizations face when trying to establish and maintain visibility, manage risks and protect against account-centric threats for cloud apps and services?

CHALLENGES FOR ORGANIZATIONS

Over the years, IT organizations have developed expertise and best practices for data center controls, but now face a myriad of challenges when attempting to address the visibility and control blind spot presented by cloud apps. Many traditional risk management practices lack effectiveness in cloud scenarios. Risks that can be managed inside the data center—where the app and infrastructure are accessible by IT—can't even be understood with cloud apps and services where the infrastructure is no longer under IT control.

TRADITIONAL SECURITY CONTROLS DON'T COVER CLOUD APPS

Most traditional security controls were not designed to help organizations gain visibility into cloud app usage and related risks. While the combination of existing infrastructure and the right cloud security tools can be leveraged to help organizations discover cloud apps, they cannot provide the visibility and control required for a comprehensive solution.

Perimeter devices have long been the front-line defense for organizations and continue to provide an important control point for network access. But firewalls are not able to control access to "beyond the firewall" services such as SaaS apps and public cloud computing services. And organizations can't completely rely on firewalls when hybrid applications span in-house and cloud provider environments.

Data Loss Prevention (DLP) tools are designed to stop organization data leaks due to unauthorized sharing. This control existed before cloud apps became popular, back when organizations solely focused on data leaks from portable media storage like USB keys and files externally shared by email. The Cloud makes sharing data with the wrong people easier than ever before. If an organization uses cloud file storage, a traditional DLP product will not know what data is being shared externally and who is sharing it.

Endpoint protection suffers from similar challenges as do perimeter defenses; many devices operate outside of an organization's IT perimeter. Unmanaged endpoints are vulnerable to breaches and other exploits that can steal legitimate credentials. And organizations can't enforce endpoint protection on personal devices that access unsanctioned cloud apps over public, mobile and wireless networks.

Encryption has long been considered the foundation of data security but is only effective when deployed properly, and does not protect

data from stolen credentials. Access with legitimate credentials means attackers get clear text data and the ability to export that data, depending on the user privilege level. Even Gartner warns that cloud encryption is not a silver bullet—it's often disruptive to cloud service operations and not an organization's first priority when developing a strategy for cloud data privacy and long-term security. Many data breaches have occurred even with encryption in use.

LACK OF VISIBILITY INTO WHO IS DOING WHAT

The lack of visibility into the risks and usage patterns of cloud apps is a major challenge for organizations. Cloud apps unknown to IT result in information assets that are uncontrolled and outside the governance, risk and compliance processes of an organization. Organizations require visibility into cloud app account usage, including who uses which cloud apps, their departments, locations and devices used. Critically, organizations need to know which users are administrators for each cloud app since these users have privileges that must be tracked closely.

For example, orphaned accounts create the risk of unauthorized access after an employee or external user leaves an organization. Having visibility into usage patterns as well as account inactivity ensures IT staff can delete accounts where access is no longer required or needed.

PROLIFERATION OF MANAGED AND UNMANAGED ENDPOINTS

The BYOD phenomenon has resulted in several risks to an organization:

- Restricted cloud app access to a defined set of endpoints in which access policies are based on whether the endpoint is managed or unmanaged. Managed endpoint policies can allow users to access, modify and store data on their devices. Unmanaged devices require a more restrictive policy that prevents an organization from losing control of corporate data by blocking data modifications and downloads.
- Organizations must prevent attackers from using stolen credentials to access cloud apps. It is important to note that cloud app providers do not distinguish between managed and unmanaged devices and don't provide effective endpoint control capabilities. Even if your organization uses Mobile Device Management, these solutions cannot restrict access to cloud apps from unmanaged devices.
- Managed devices are still vulnerable to insider abuse, attacks and theft. Insight into the usage patterns and device profiles across managed and unmanaged endpoints can enable proactive policy enforcement and account protections.

MALICIOUS INSIDERS

Insider threats have always presented a special challenge to organizations. It can be difficult to guard against the malicious intent of authorized users since they are more likely to use approved devices and may have knowledge of thresholds for alerts and notifications. In order to detect suspicious behavior of insiders, organizations need a comprehensive view of their normal usage patterns as they perform their assigned responsibilities. In addition, detailed activity profiles of peers in the same department forms a baseline that enables the detection of malicious actions.

Along the same lines, former employees pose a significant security risk, as they may have been disabled from the organizational directory but can still access cloud apps that contain business-critical information. Contractors and consultants present similar a security risk, as they may be able to access cloud apps for which they are not authorized.

ATTACKERS MOVING TO THE CLOUD

The critical threats for organizations include outside attacks using one of several exploits to steal account credentials to commit fraud and steal sensitive data.

The most recent Verizon Data Breach Incident Report makes clear that outside attackers are focused on the theft of cloud app credentials in their drive to steal sensitive data. In fact, Verizon reported that authentication credential theft caused the highest number of data breaches. Even more troubling, the report found the average time to discover a successful attack was days or months. The bottom line is attackers have all the time they need to extract data, given that some compromises can take one minute or less to execute.

Let's look at the anatomy of several account-centric threats to understand how an attacker can steal credentials to gain access to cloud app and services.

Spear phishing privileged users

Spear phishing is a well-established social engineering attack used by hackers to steal the legitimate credentials of a privileged user. This technique is especially powerful now that cloud accounts are globally accessible; it's even easier to commit fraud using sensitive data from the compromised accounts of individuals who perform business-critical functions for their companies.

Spear phishing attacks are increasing due to their high success rates. A combination of social engineering and technical exploit, spear phishing starts with identifying targets on social media sites like LinkedIn. The number one target in a spear phishing attack is a user's access credentials. For example, an attacker can focus on a company's SaaS administrators, carefully constructing an email that looks like it comes from the SaaS provider. SaaS administrators that have less security awareness might click on a password reset link in that email. Cloud app providers often consider such types of incidents the responsibility of the organization and not a problem with their application.

Zeus malware attacks—many variants

Recent attacks are using a variant of Zeus banking malware to target cloud application providers like Salesforce. The exploit has been used to attack users' unmanaged devices (like a home computer) that are used outside of normal business hours. Such an approach allows the attacker to bypass controls an organization may have in place and highlights the challenge of securing access to cloud apps in an environment where BYOD is pervasive. The Zeus malware steals user credentials by targeting the login form of the SaaS app. The Zeus malware is very hard to detect, making it the largest botnet on the Internet (it is estimated to infect some 3.6 million PCs in the U.S.).

The responsibility to mitigate these risks lies with an organization, even if they are not aware of the access behaviors and devices used by their employees. Most cloud service providers are not going to take responsibility for an account compromised outside their service. Since cloud app adoption goes hand in hand with BYOD and the anywhere access to cloud apps, organizations must have the visibility and control to manage risks related to cloud app credentials.

Heartbleed

Exploiting a bug in the heartbeat extension in OpenSSL, attackers can gain access to random parts of the memory heap on the systems OpenSSL is running on. Security researchers have shown that repeated use of this vulnerability yields accounts credentials, session IDs and private keys in less than an hour. The bug is especially a concern because it leaves no trace, therefore it cannot be determined if it has been used in the past. It's estimated that millions of web sites are running affected versions of the OpenSSL cryptographic software library, and many vendors embed OpenSSL in network appliances and other devices.

Using Heartbleed, attackers can gain access to the legitimate credentials of cloud app users and use them to take over accounts, leading to theft of sensitive data and fraud, even after the OpenSSL vulnerability was fixed. Many cloud providers are working to patch the use of OpenSSL but given the scale of the problem, attackers have an open window to exploit the bug.

Such vulnerabilities and attacks make it clear that the cloud visibility blind spot extends to the assignment of responsibilities for cloud app risks – what should organizations do with so many cloud apps in use? A priority should be to profile normal behavior of legitimate users across sanctioned and unsanctioned cloud apps so that anomalous and suspicious activity can be detected and acted upon immediately.

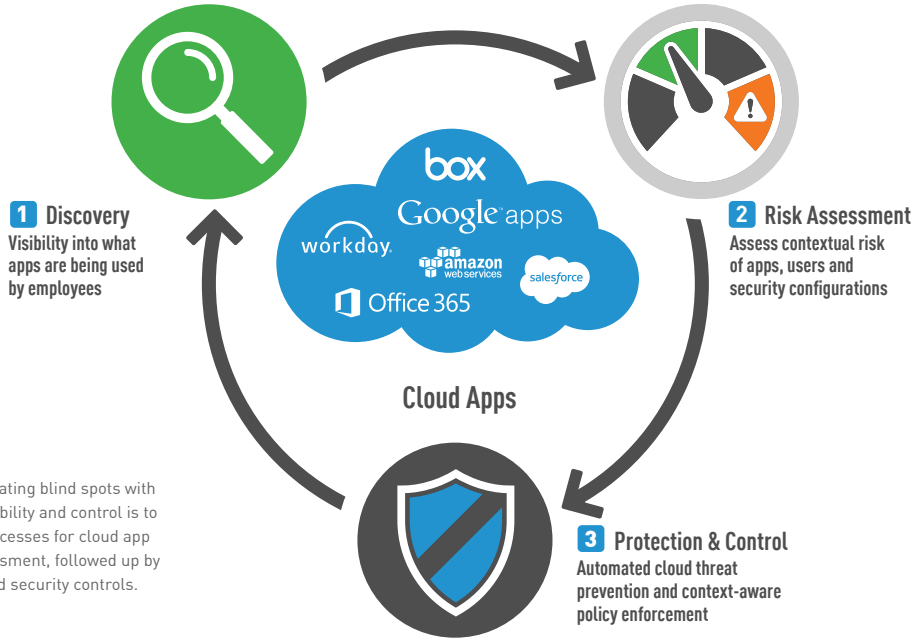
So what other criteria should organizations consider as they address the visibility and control blind spot between their organization and cloud providers?

KEY CRITERIA FOR SAFEGUARDING YOUR CLOUD APP ENVIRONMENT

Given the challenges and threats to cloud apps, what efforts should organizations prioritize in order to gain visibility and reduce the risks that cloud app adoption presents?

A concise method to address the problem consists of three critical priorities for organizations:

- Discover which cloud apps are in use. This step requires organizations to get a global view of all the cloud apps accessed by employees through active monitoring of forensic data.
- Assess the data and analytics on context-aware user activities so that more effective policies can be created to mitigate cloud app-related risks.
- Enforce controls that ensure the safe and productive use of cloud apps. This step should include advanced behavioral detection and automated policies to protect and remediate account takeover threats in real time.



The first priority in mitigating blind spots with regards to cloud app visibility and control is to establish automated processes for cloud app discovery and risk assessment, followed up by real-time monitoring and security controls.

The following criteria are essential for risk management and control of cloud apps:

1. APP DISCOVERY—OBTAIN A GLOBAL VIEW OF ALL CLOUD APPS

- Discover all cloud apps accessed by employees
- Inventory cloud apps and assess risk posture – for each app and at an organization level
- Aggregate firewall and proxy logs across the organization
- Generate a global view of cloud app usage, including metrics for traffic volume, hours of use and number of accounts
- Create a baseline view so you can see how many apps have been added over a given period of time
- Drill down into each cloud app to perform detailed risk analyses

2. RISK GOVERNANCE—ASSESS RISK CONTEXTUALLY AND SET MITIGATION POLICIES

- Identify high-risk activities for your business
- Determine who has standard and privileged access to an app
- Identify dormant (i.e., accounts not accessed for several days), orphaned (e.g., ex-employees), and external (e.g., partners) accounts to create appropriate access policies
- Benchmark current app security configurations against regulations or best practice guidelines to pinpoint security and compliance gaps
- Assess and define access policies based on the location of users and/or a cloud service provider's data centers (i.e., location-based access control)
- Assign tasks to resolve user and application issues
- Leverage a built-in organizational workflow to assign and complete risk mitigation tasks via Forcepoint CASB or through integration with 3rd-party ticketing systems

3. AUDIT & PROTECTION—AUTOMATICALLY ENFORCE POLICIES & PROTECT AGAINST CREDENTIAL MISUSE & MALICIOUS INSIDER ACTS

- Monitor and catalog who is accessing cloud apps from managed and unmanaged endpoints
- Track and monitor privileged user access and configuration changes
- Monitor cloud app usage across multiple context-aware categories including: user, location, device, action, data object and department usage
- Ensure real-time detection of anomalous and suspicious behavior
- Implement attack remediation including: strong user verification, block application actions (e.g., block downloads of shared documents) and account access
- Enforce location-based access control (aka "geo-fencing") policies
- Enforce endpoint access controls for managed and unmanaged devices, whether originating from a browser or a native mobile app
- Monitor and control uploads, downloads and sharing of sensitive data for over 100 file types
- Inspect files and content in real-time to ensure that PII, PCI, HIPAA and other sensitive information stays protected

THE FORCEPOINT CASB SOLUTION

Forcepoint CASB is the leader in cloud app visibility and control. With Forcepoint CASB, organizations can gain visibility into cloud app usage, identify high-risk activities and enforce policy and controls for cloud apps to prevent account-centric threats, meet compliance requirements and protect data.

Forcepoint CASB offers these critical capabilities via three product packages:

- Cloud Governance
- Cloud Audit & Protection
- Cloud Security Suite

GET STARTED WITH FORCEPOINT CASB

Start today with Forcepoint CASB by requesting a demonstration or free trial.

ABOUT FORCEPOINT CASB CLOUD GATEWAY

Forcepoint CASB is a cloud-based security service that provides visibility and control over sanctioned and unsanctioned cloud apps. With Forcepoint CASB, organizations can discover SaaS applications and assess related risks, enforce controls to protect cloud accounts and data and help ensure cloud activities comply with regulations and best practices.

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

[WHITEPAPER_FPCASB_SHED_LIGHT_ON_CLOUD_APP_BLINDSPOT_EN] 200053.022017