

Shadow IT In The Cloud

Rodney Beede
Seagate Technology
Copyright 2016-2017, Seagate Technology LLC

Introduction

- Rodney Beede
 - IT Cloud Security Architect & Engineer
 - Seagate Technology
- M.S. in Computer Science
 - University of Colorado at Boulder
 - “A Framework for Benevolent Computer Worms” 2012
- Recent public security work
 - “Single Sign-On Watering Hole” vuln. presentation at BSidesOK 2017
 - “Shadow IT In The Cloud” - Oklahoma Retailers InfoSec Forum, 2016
 - “Case Study: Seagate's Amazon AWS Cloud Security” – InnoTech & IWS9, 2016
 - Discovered CVE-2015-8503 XSS in Tenable SecurityCenter; 2016
 - Discovered data disclosure vuln in Google Spreadsheets; 2015
 - “Case Study: Seagate's OpenStack Swift Security” – InnoTech 2015; CSA&IAPP 2014
 - Authored chapter “Object Storage” in the OpenStack Security Guide
 - Discovered CVE-2013-3627: McAfee Agent v4.6 Denial of Service
 - AppSec USA (OWASP) - CTF winning team – 2012 & 2013
- Tech blog
 - <https://www.rodneybeede.com/>
 - The views expressed in this blog are my personal view and have not been reviewed or approved by Seagate.

Agenda

- Shadow IT - Why it exists
- Shadow IT - What to do about it?
- Two Facets of Cloud Technology
 - ◆ Hosting (IaaS, PaaS, SaaS)
 - ◆ Consumer
- Finding what you don't know
- CASB (Cloud Access Security Broker)
- Criteria for useful CASB

Shadow IT - Why it exists

“For many organizations, so-called Shadow IT grew out of pure necessity, as increasingly tech-savvy employees sought out their own solutions to specific line-of-business problems.”

- “Shadow IT: 8 Ways To Cope”, [InformationWeek.com](http://www.informationweek.com), Andrew Froehlich, 3/18/2015

“Shadow IT was born out of the need to deliver value faster to the business,”


- Quote from Ajeet Singh; “The risks and rewards of shadow IT”; <http://www.ciodive.com/>; Brown; March 30, 2016

“By its very nature, shadow IT exists to circumvent IT governance and security controls by employees believing they’re doing something beneficial for the company,” said Rick Orloff, vice president and chief security officer at Code42.”

- “The risks and rewards of shadow IT”; <http://www.ciodive.com/>; Brown; March 30, 2016

- ❖ Bring Your Own Device has allowed employees to pick personal tools they also want to reuse for business.
- ❖ Cloud computing has enabled BYOD features literally at the user’s fingertips.

Shadow IT - What to do about it?

1. Need to know what is being used and by whom
2. Understand the **real** business need
3. Does IT already have an approved alternative?
 - a. Does that approved solution lack something
4. Or should IT incorporate the tool into enterprise use?
 - a. Dropbox is one example
 - i. **Any personal @example.com accounts can be converted to enterprise**
 - ii. **For a fee of course** 
5. #3 & #4 above relate to establishing better communication & service with the business departments
 - a. What need did IT not fulfill that IT can move to meet?
 - b. Ask the user: How is your (shadow) solution protecting the company data?
 - i. **Maybe (or not) their solution is protecting the data well**

Two Facets of Cloud Technology



1. Hosting

- a. IaaS
 - i. **Servers (guest instances)**
 - ii. **Websites for your company**
 - i.e. blog.example.com
 - iii. **Public Cloud**
 - AWS
 - Azure
 - Rackspace
- b. PaaS/SaaS
 - i. **My.Salesforce.com**
 - ii. **Google App Engine**

2. Consumer

- a. Dropbox
- b. Google Drive
- c. Amazon AWS (*indirect as it hosts other services*)
 - i. **Examples: Netflix, advertising networks, etc.**
- d. iCloud

Difference - Two Facets of Cloud Technology

1. Hosting

- a. Your company runs their own virtual infrastructure
 - i. Or a third party firm is using cloud with your company name
- b. IT admins manage the virtual systems or web site configs
- c. Runs on servers in a data center somewhere
- d. Paid as business invoice

2. Consumer

- a. End-users consume the service
- b. Accessed from devices (mobile, laptop, ...)
 - i. Using your company internet
 - ii. Using personal internet at home, cafe, cellular, ...
 - iii. *Roaming users and devices*
- c. Free for personal use
- d. Per user paid license for premium features
 - i. **More storage**
 - ii. **Commercial usage allowed**

Consumer vs Enterprise Cloud Services

	Consumer	Enterprise
Audit User Activity/History		✓
Encryption	✓	✓
Customer Controlled Keys		✓
Enforce Security Controls (i.e. password complexity, 2FA, etc.)		✓

Finding what you don't know

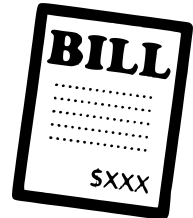


cc-by-sa/2.0 - by Colin Smith - geograph.org.uk/p/2771576

Finding - IaaS, PaaS, SaaS (Hosting)

Some department stands up their own server/site in the cloud
(without asking IT or IT Security)

1. Gate them at the DNS (branding)
 - a. You want a DNS entry for “cool-new-product.example.com” ?
 - b. Did you finish your IT Security assessment form?
 - i. **Yes? Great what is your verification number?**
 - c. What if they go out and buy www.cool-new-product-example.com
 - i. <http://dnstrails.com/>
2. Audit your existing DNS entries
 - a. *Example next slide*
3. Review perimeter firewall logs
 - a. Do any non-company IPs reverse-resolve to ...example.com ?
4. Someone's gonna pay
 - a. Help finance identify credit card or invoices to popular cloud providers
 - b. Trip-up: May have third party contractor that is billed but uses cloud



DNS Audit Report Example

dnsCloudReport_--2016-10-24_00-23-55_-0500--REPORT.csv - Excel

FILE HOME INSERT PAGE LAYOUT FORMULAS DATA REVIEW VIEW

Calibri 12 A A

Paste

Clipboard

Font

Alignment

General

Number

Conditional Formatting

Format as Table

Cell Styles

Insert

Delete

Format

Cells

Editing

A7

payment.Company.com

	A	B	C	D	E
1	Company DNS Entry	Resolved IP	Cloud Service	Cloud CIDR Range	Business Owner
2	funprogram.Company.com	1.2.3.4	Microsoft Azure	104.209.128.0/17	John Doe <john.doe@Company.com>
3	cloudsupport.Company.com	8.8.8.8	Salesforce	136.146.0.0/15	Jane Doe <jane.doe@Company.com>
4	golfing.Company.com	1.2.3.4	Amazon AWS	52.54.0.0/15	Unknown - No Record <no e-mail>
5	realbizpurpose.Companyapps.com	8.8.8.8	Amazon AWS	184.73.0.0/16	Unknown - No Record <no e-mail>
6	www.weluvthecloud.Company.com	1.2.3.4	Amazon AWS	54.68.0.0/14	John Doe <john.doe@Company.com>
7	payment.Company.com	8.8.8.8	Amazon AWS	52.70.0.0/15	Jane Doe <jane.doe@Company.com>
8	coolnewproduct.Company.com	192.168.0.1	Rackspace	72.32.0.0/16	Unknown - No Record <no e-mail>
9					

dnsCloudReport_--2016-10-24_00

READY

Finding - Consumer

■ Common places:

- Mobile devices
- Desktops (i.e. cloud sync apps)

1. Ask your users via a survey

2. Use CASB

- Cloud Access Security Broker

3. Your own perimeter firewall logs

- Fed to a CASB solution
- Identify *on-premise* usage
- Can't identify off-premise usage (like BYOD at home)
 - Unless you enforce always-on VPN perhaps

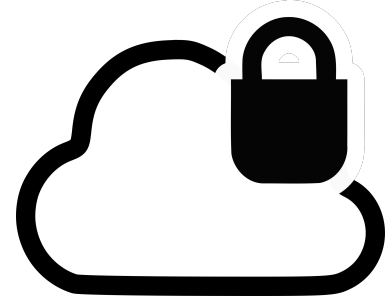
4. Detecting off-premise cloud usage is hard

- Some CASB vendors can do on or off-premise
- Can enforce monitoring or access is denied to user
- Good MDM is crucial for handling mobile devices



openclipart.org

CASB



openclipart.org

■ Usefulness

- Identify what individuals are accessing
 - Including many things they don't realize they are using
 - Identify number of users, data volume
- Provide a risk measurement of services
- Block specific services
 - Advanced solutions can allow downloads but block uploads
- Incorporate data loss prevention (DLP) policies
- Audit sanctioned enterprise cloud security settings
 - Did an IT admin change a password policy to something weaker?

■ Limitations

- May not distinguish specific application in larger provider
 - I.e. aws.amazon.com identified but used by 100's of "cloud apps" or websites
 - My DNS auditing tool helps us with that problem on the *hosting* side
- Requires deployment to all devices to be fully effective at blocking
 - Although an MDM solution makes this feasible
- Cost can be prohibitive (another per user annual license)
- Not all CASB's are good at their "risk measurement" catalog



Criteria for useful CASB

- Can it identify all the cloud apps being used on your network
 - Well known should be easy: Google Drive, OneDrive, DropBox, Box, iCloud Drive, ...
 - Lesser known but important: 4shared, mega, prezi, ...
- Does it correlate your user directory with IPs and cloud app names?
 - Also having a view of department usage can identify sensitive IP areas
- Data volume - Upload
 - Only helpful if you can filter by a useful time period
 - Ex: User uploaded 5GB but over 9 months isn't significant
 - Ex: User uploaded 1TB in 24 hours is significant
- Ability to Trust sanctioned apps
 - Shouldn't flag that Drive app as High Risk if **corporate** account used
- Ability to distinguish between personal accounts and enterprise accounts
 - Can we block uploads to personal accounts but allow enterprise account for same service?
 - Few CASB solutions can do this

Criteria for useful CASB

■ Risk Ranking Methodology

- Is the quality of the methodology worth what you pay for your CASB?
- Is it a numeric sorted score or High, Medium, Low?
- Does it cover PCI, SOX, SOC 2, HIPAA, ...
- Do they look at
 - **Password management**
 - **Encryption in-transit, at-rest**
- Does the vendor publish their scoring methodology
- Can I see documentation that the vendor reviewed a compliance audit report?
 - Or did the vendor's "research team" just read some marketing material on the cloud provider's website saying "We're PCI Regulatory Compliant!!!"
- Can they accurately tell me "these are your 10 high risk apps"
 - Can I trust that report and deliver it to my CISO/CIO and say "we must block these"
- How often does the vendor renew their review of the cloud provider?

■ Can I add unmapped/unknown cloud apps?

- If not can I purchase professional services to do it?
- Or is it just a feature request that may be added later?

Criteria for useful CASB

■ Data/Metadata Confidentiality

- How does the cloud provider protect my log data?
- Do they encrypt in-transit?
- Do they encrypt at-rest?
- Do they compile my log data on-premise into metadata before sending it to them?
- Does the vendor have SOC or other certifications for their own systems?

■ Infrastructure Requirements

- How much work is it to integrate my logs into their solution?
- Does the solution integrate into my firewall rules automatically?
 - Or do I manually block identified risks?
- Do I need to deploy additional infrastructure on-premise?
 - At every office site for optimal performance?
- If I want to keep all my metadata on-premise can I?
 - Cost?

Criteria for useful CASB

■ Mobile

- Does it require a software agent be installed on each device?
 - If not does it still enforce when device is off-premise?
- Can I force all users through a monitoring system?
 - What if the user goes off-premise?
- Can I block specific actions (upload) but allow other app actions?
- Can unmanaged devices be blocked from accessing my sanctioned cloud apps?



Criteria for useful CASB

■ DLP

- Can it block an upload/sharing in real-time (before any chance of leakage) or is it an after-the-fact revoke of unwanted sharing privileges?
 - Ex: Google doesn't provide an API for blocking only revoking (not a firewall)
 - The CASB would need to intercept the traffic
- Does it notify the user traffic was blocked and why?
 - Some solutions inject a custom message right into the app for instant notification
 - Want to avoid user confusion and help desk calls
- Can it scan my existing (before CASB install) at-rest cloud data and look for exposed IP?

■ Governance

- Can I audit security settings in my sanctioned cloud apps?
- Secure https enforced?
- Does the password policy (or SSO) meet my company policy?
- Is data at rest encryption enabled (if available)?
- Can it provide me an audit report of admin users in the cloud app?
- Are there users in the cloud app that are not in my corporate directory?

CASB Bonus Features


- Identify wasted enterprise user licenses for a cloud app
 - User's AD credential was deactivated months ago
 - Forgot to deactivate their cloud account though
 - You are overspending \$xxx dollars a month!
 - A great ROI and value-add from the security tool
 - If cloud app doesn't offer 2FA can the CASB inject that for me?
 - Can it detect abnormal login behavior and alert and/or block?
 - Any history reports of provider breaches?
 - I.e. Adobe, Dropbox, Slack, Yahoo
- 

Image care of "Bonus"; CC BY-SA 3.0 NY; August 2016



References

- <http://dnstrails.com/>
 - Useful tool for finding rouge domain names
- https://www.rodneybeede.com/AWS_Security_Architecture_work_I_ve_done.html
 - Includes a consolidated IaaS security checklist for evaluating a cloud provider
- Some images care of openclipart.org
 - [Money](#) By mfdzg 2015-07-13
 - [caution-road narrows](#) By Leomarc 2007-10-19
 - [Pay your bill icon](#) By wanglizhong 2014-11-19
 - [Detective Silhouette](#) By centroacademico 2011-10-16
 - [Secure Cloud](#) By samtuke 2015-09-15
 - [Clipboard](#) By hellocatfood 2013-06-20

