OBSIDIAN

THE CLOUD ECOSYSTEM
IMPLICATIONS FOR DIGITAL FORENSICS AND INCIDENT RESPONSE

JODY J. FORNESS, ENCE

SENIOR SECURITY RESEARCHER, OBSIDIAN SECURITY

EDUCATION

Northeastern University, B.S. Criminal Justice, Minor in Computer Science

The George Washington University, M.F.S. High-Technology Crime Investigation

EXPERIENCE

2007 → 2010 → 2014 → 2018 → 2018

THE DEPARTMENT OF THE TREASURY 1789

STROZ FRIEDBERG an Aon company

NORTHROP GRUMMAN

BAE SYSTEMS

SilverSky

KIVU

OBSIDIAN

I'm a senior security researcher at Obsidian Security. I started as a contractor for the Treasury Department doing threat intelligence, worked as a digital forensic consultant for a number of years, did some incident response. Also, I worked for a cloud security startup writing email detection logic. And then did a little bit of vulnerability research.

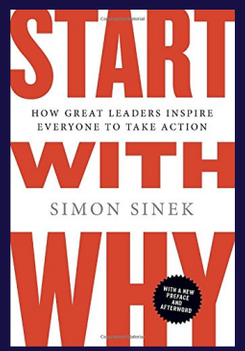
START WITH WHY

Why we do things?

Apple

WHY: In everything we do, we believe in challenging the status quo and thinking differently.

HOW: We design beautiful products.



Simon Sinek's "Start With Why"...definitely recommend the audiobook. The author reads it, and he has a British accent. Understanding the why behind what we do changes how you think about things.

WHY CLOUD?

Cloud is the technological representation of a cultural paradigm shift, a purposeful discarding of boundaries in favor of a quantum leap in how our society interacts and solves problems.

OPEN SOURCE + API-FIRST + SHARING ECONOMY = CONNECTION/COLLABORATION

(IE. FLUFFY UNICORN)

Cloud represents more than just a shift of resources from on-premise to cloud-premise, it’s a cultural paradigm shift.

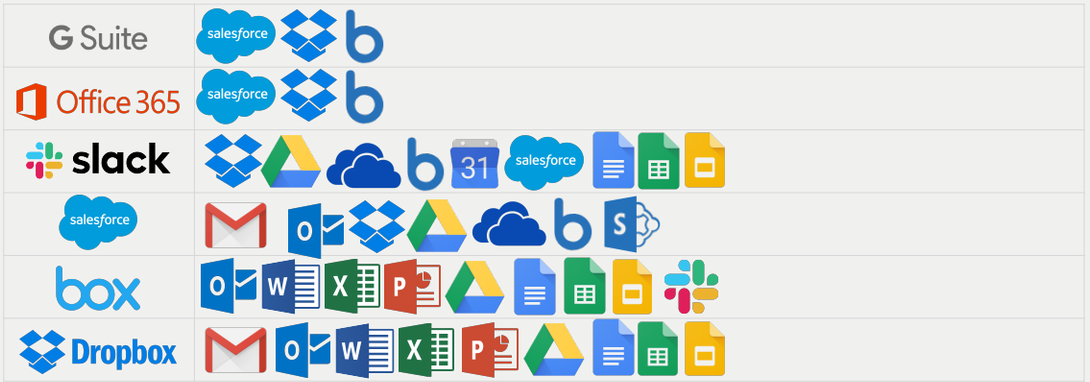
~~THEN~~ VS. NOW

Companies are picking a “cloud stack” of business services...the difference being these new technologies are designed for connection.

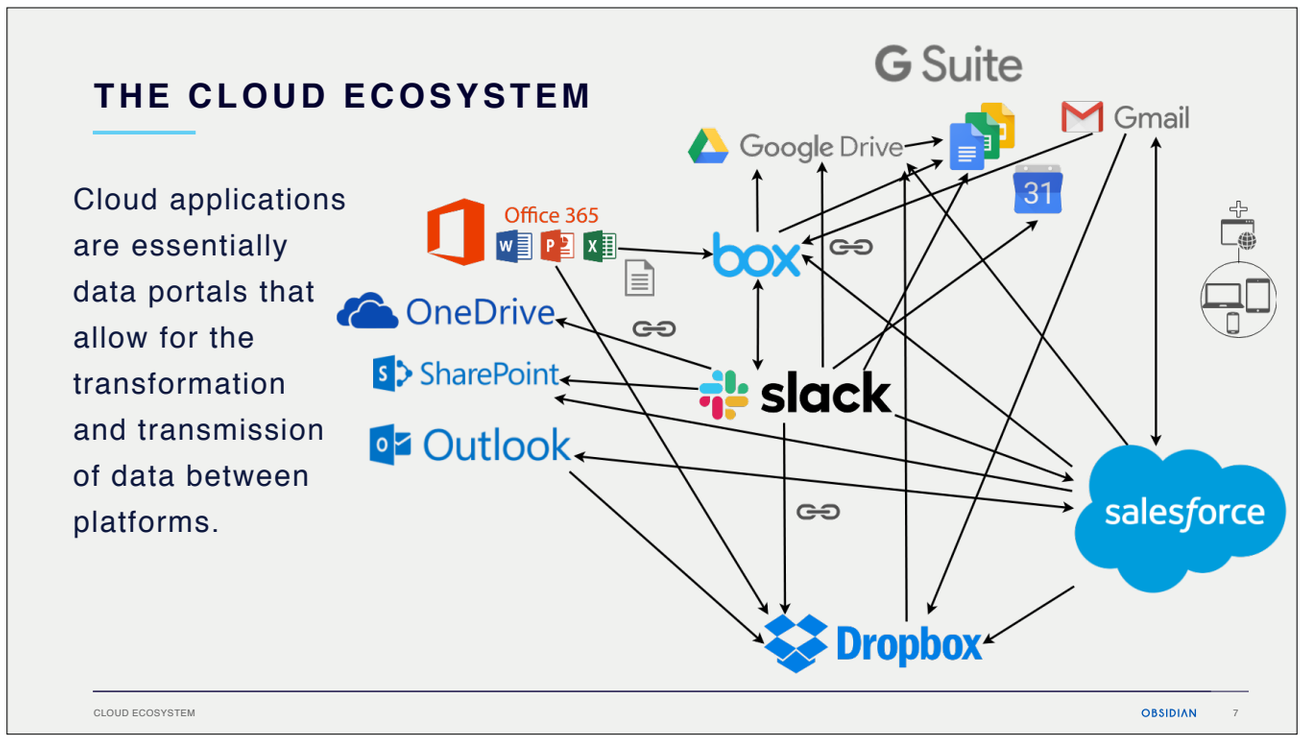
Applications used to live on individual workstations and shared internal resources. Interconnectivity was accomplished via physical networking and application plug-ins that provided additional functionality.

Thanks to Open Source + API-first + Sharing Economy, new companies are spun up quickly.

INTEGRATIONS



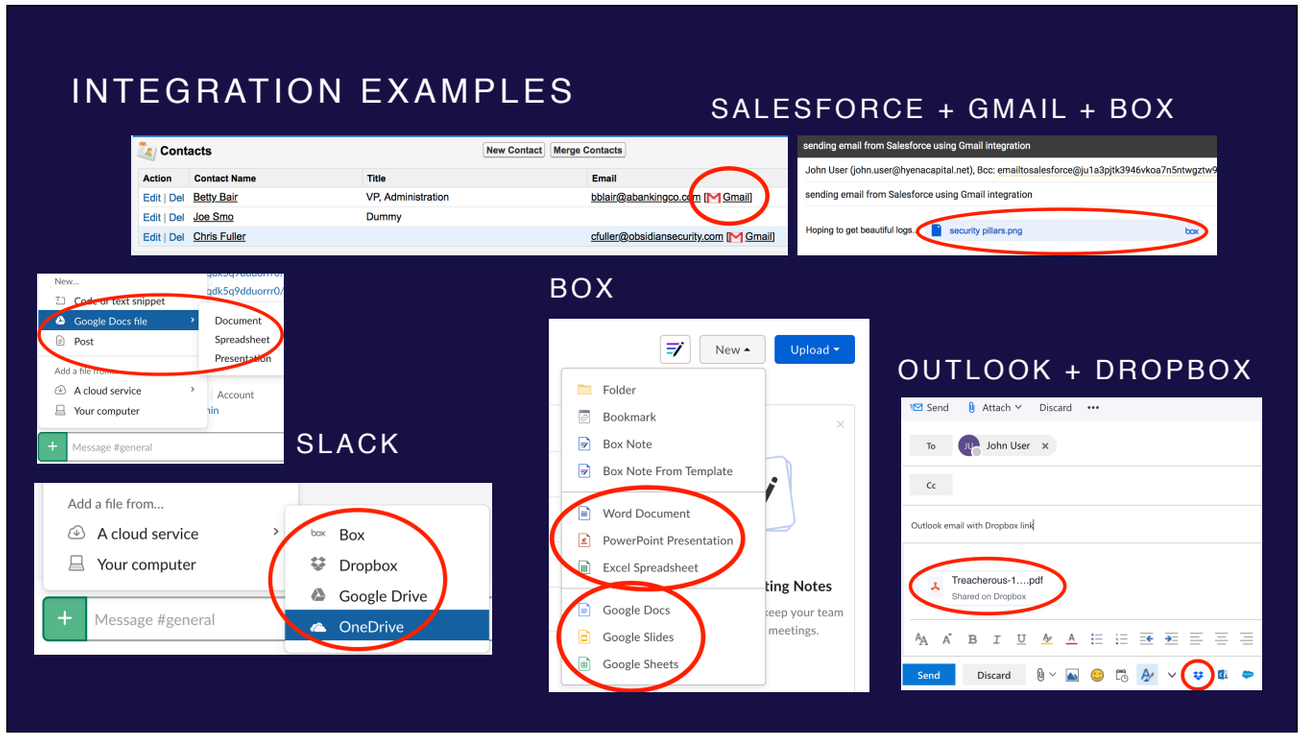
Connected via APIs. From one application, you can access the data or functionality of another application.



In Slack, it's possible to simultaneously create and share a new Google document. That document lives in Google Drive.
In Salesforce, you can draft an Outlook email, attaching files stored in Dropbox.

These cloud applications not only leverage and enhance the functionality of each other, but allow for collaboration, within and between companies, on a scale never seen before.

In the same way that team members who refuse to work together are replaced, applications that don't embrace this new collaborative mentality may die off. Companies with a "closed" suite of products don't understand that "why"…being able to collaborate and iterate quickly is becoming more important than traditional loyalty. It's a value alignment.

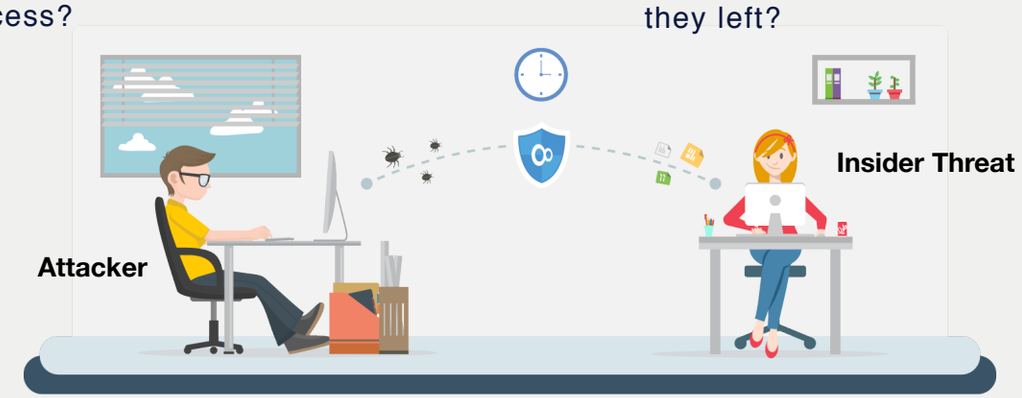


I don’t think anyone realizes how interconnected these cloud services really are.

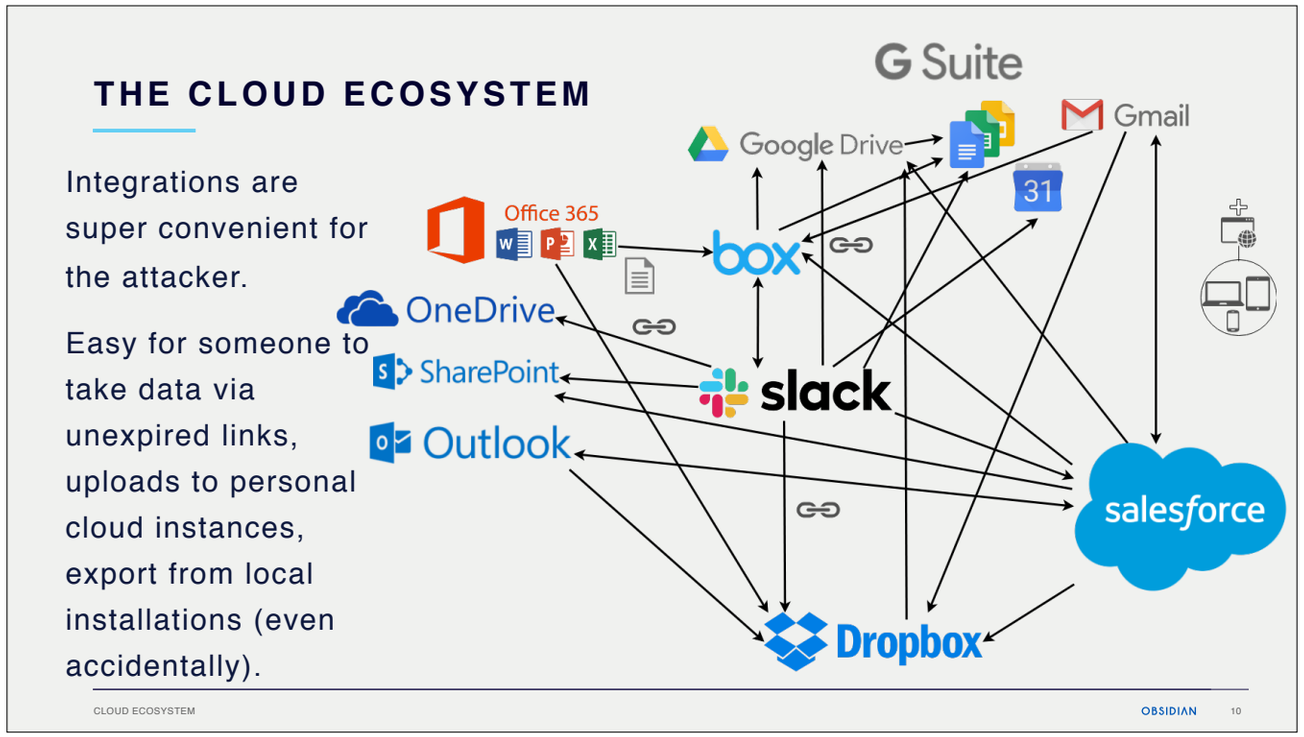
INCIDENT RESPONSE & FORENSICS

IR: What did the attacker do? What data did they access?

Forensics: Did this user take data with them when they left?



There are security implications for incident response and forensic investigations in the cloud ecosystem.

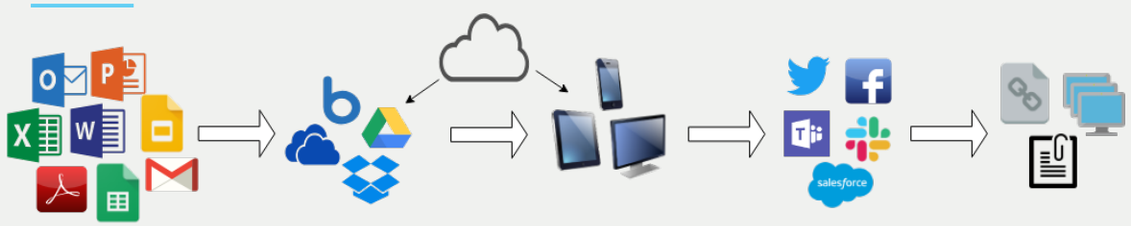


Integrations are super convenient for the user. They are convenient for the attacker too.

Now, there are a million ways a user can take data (ie. links that don't expire, uploads to personal cloud instances, integrations with personal accounts, applications on personal devices), even accidentally.

We need to understand this.

DATA FLOW



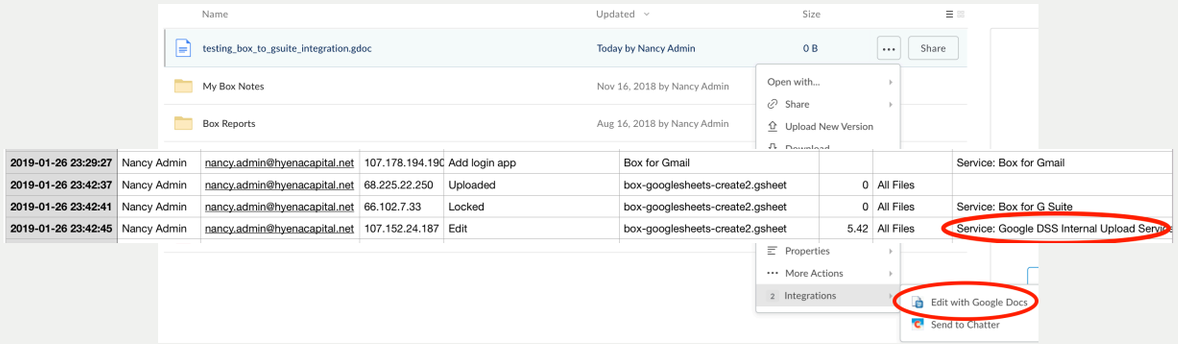
- Data flows from data creation apps to storage locations on Cloud/Desktop/Mobile to internal/external sharing platforms via links, documents and shared workspaces.
- OneDrive, Box, and Dropbox allow for data syncing between desktop applications and cloud storage.
- Both work and personal cloud accounts are possible.
- Shared workspaces are becoming more common (Box has Collaborators, Slack has Shared Channels).

The implications of the sharing economy continue to expand as employees often use personal devices for work. Because you can have both work and personal cloud accounts, it's possible to mistakenly upload to the wrong account.

If you have to remediate and delete a document that has been added…you need to know where the data actually lives.

HOW DO CROSS-PLATFORM EVENTS GET LOGGED?

BOX LOGS

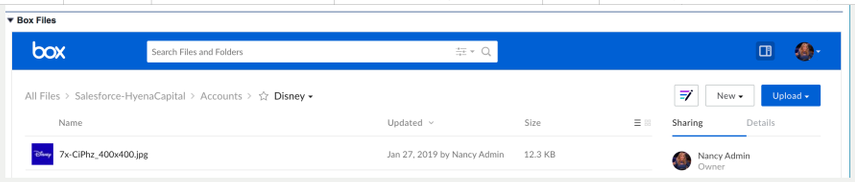


When you edit a Google document from Box, it creates a specific Box log entry referencing the Google Docs integration.

HOW DO CROSS-PLATFORM EVENTS GET LOGGED?

BOX LOGS

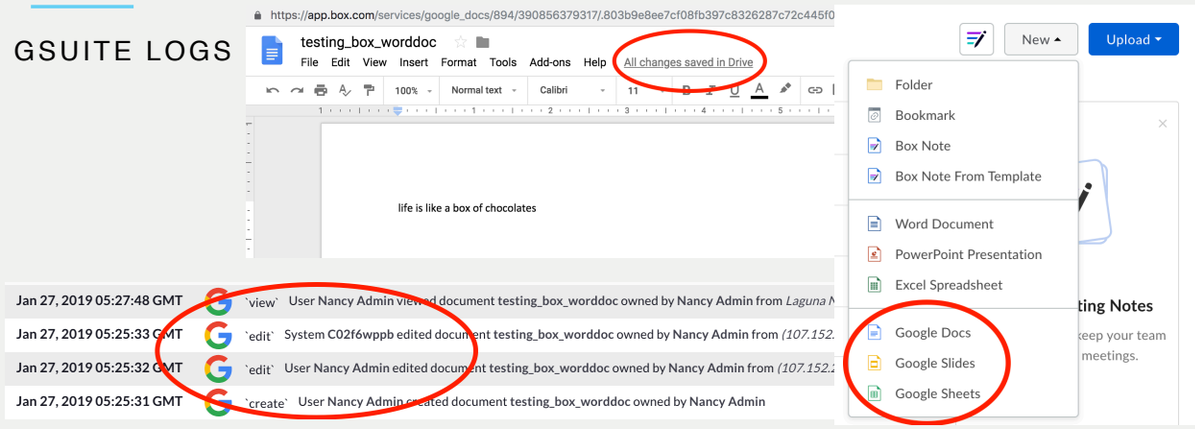
2019-01-27 02:40:05	John User	john.user@hyenacapital.net	85.222.138.8	Add login app	Box for Salesforce		Service: Box for Salesforce
2019-01-27 02:40:24	Nancy Admin	nancy.admin@hyenacapital.net	85.222.138.8	Created	Accounts	0	/Salesforce-Hy	Service: Box for Salesforce
2019-01-27 02:40:25	Nancy Admin	nancy.admin@hyenacapital.net	85.222.138.8	Created	Disney	0	/Salesforce-Hy	Service: Box for Salesforce
2019-01-27 02:40:26	Nancy Admin	nancy.admin@hyenacapital.net	85.222.138.8	Auto accepted collaboration invite	john.user@hyenacapital.net	0	Disney	As: Editor, Service: Box for Salesforce
2019-01-27 02:41:39	Nancy Admin	nancy.admin@hyenacapital.net	68.231.217.85	Uploaded	7x-CiPhz_400x400.jpg	12.28	/Salesforce-HyenaCapital/Accounts/Disney



The Box integration for Salesforce gets embedded in the “Account” object, so every time that object is created, a new Box “instance” is activated and LOGGED!

HOW DO CROSS-PLATFORM EVENTS GET LOGGED?

GSUITE LOGS



Google's activity logs are actually very detailed (every create/view/edit/delete is logged), but you must pull using the API. GSuite and Office365 offer API explorers, so you don't actually have to script anything…just make individual queries with your authentication token.

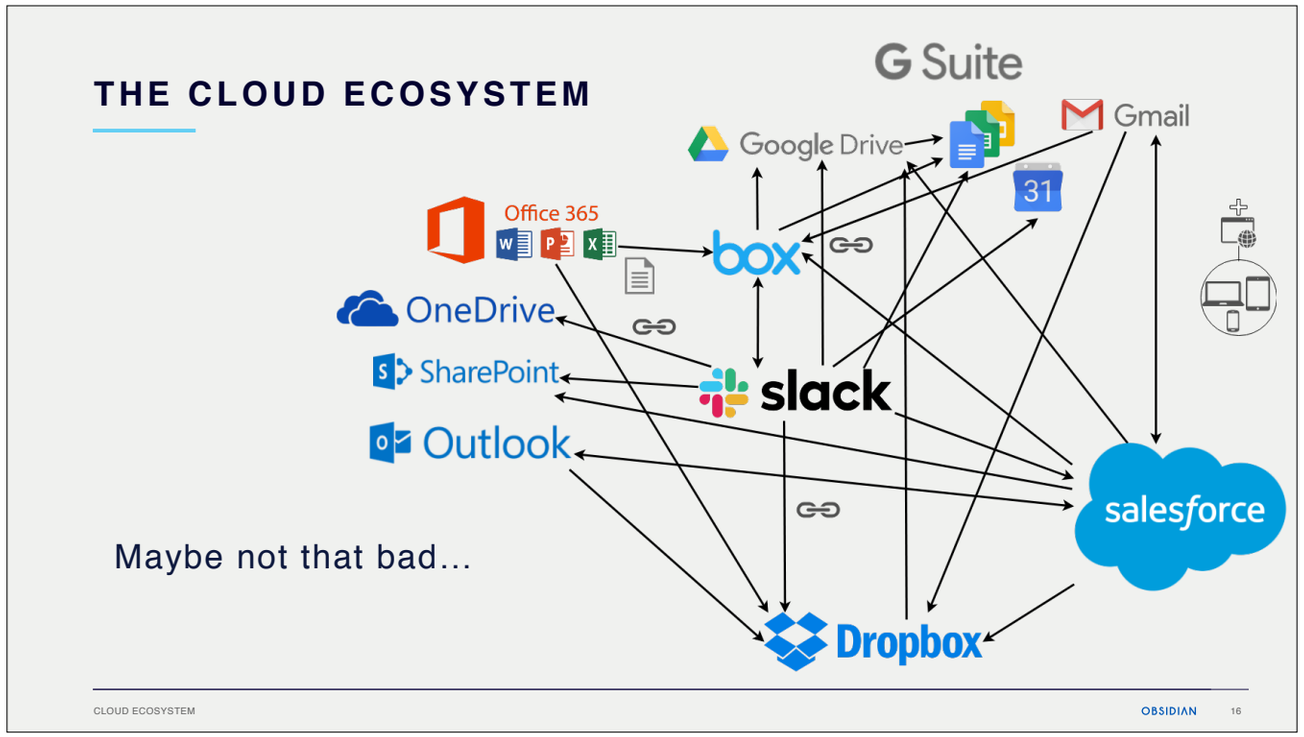
HOW DO CROSS-PLATFORM EVENTS GET METADATA-D?

METADATA

```
brew install exiftool
exiftool -ee <path to file>
mdls <path to file>
```

Type	Notes	Metadata	Extended Attributes
Microsoft Word	Created and downloaded from Box	Properties Application : Microsoft Office Word Properties Shared Doc : false Properties App Version : 15.0000 Core Properties Creator : Nancy Admin	kMDItemWhereFroms = ("https://dl.boxcloud.com/d/1/b1!HTCtnmTRAGAR2UKGyJCNY4Myh84n0xSLAPAlk_3msCIBJMP7cZsuCV-OssveEKxvceAoCiBhraqNAwPx6MZ7X_X8qJ30uN9SgOEz39GTT1LpjyNz4HQGm7eZvEa9lwhX10nyrZRdk8BMn62tl-Ozh1EozBJCKpyEqGuhL9w7kx-FagoNzKlmWNxnN8KERXavbLLf_Ij6i1MonmCAE3izOx9IeNj8e4GjV3PE5DImm7R_PggX6rpVC6mx9eFLis0B7uvT5Sa0pUptff8eJ_8D9irLtxMy-Q_YB_7GnI72K_YGfgeX1GK1xAqA1FANhO_eAw5sLm3VRBQBnC48yRlB82EEEbuLvIWASYrHx-yGxqpY7lBgsKAFEXRHSTrrfX8eWIQiURYGayUjIrSb4lVpsTFWUhulwQT0y66yFN1aBP0Ha9qWqoOLZRupgU8esSDPytmtGMjfjQEq0Nai_s6McGeEaLsPk40bFaQtzOS5erO_XbwdS_CMdpdlqGJPyf57hcplRWB1SlNSz_5A5GnMxyU5wtOw5sVVt2FOYv1UEt-BbaN9RahLosGYmg7b-NdT-R_8IyTu3Es2A0ghr1XyEo4Zn6WqNkjT1JnGCojLH8B6OBkGACYFXi_wqvViGdYGKatf5iZI_VviylCzkAk6ot5mW0ScHnZDacM_XSkryXTrSrGiyp3fWLON3gcPTUm9SxBWFO7S3Mkgvo1B1x8bHne-tz798XQ9Z14kPawrzcsEKzx_KzIsw9e9pZHumPtYohZIA6kTFZP4_1_E2RGP-L349oaSJPU820kfaiRhTdRVLCDUyLavKArAfK4zol9F_zENBNd-4XJIsJhbcG5AiQEy89gapUHoMWpllVWjvX7kaQRbQ7qwM2tFZntPUEkrNBnwnsuwG_Htw27bWEVaUJxNAFqyFOn6Cds-1V1fW4QA6xXITtR92Pmfvb6ZH_eKYTUKSiQnV0FwsR7bbvzw_R_yOtSwHl1Qn-4aFDJPMmBMcz-PyxMo_ZEdVgSJNAA1bzwCscN7zXz8zuUM1yjx7NLWwJhcfB6MopvcnhQr8dcUTVBxX6zY41ceXnew7GmoYdmsmkpW-l35_K1Q9VGM6adoI0BT4ku81wuAYWBDmH8DutG4x48l9pxbvFYm99jLxFsvZAlQiDohF3tvWfhIfR0z9LdYJ9nOX6zgbtV1sPoGqiqcROo3NHzLTGPIbywlic43gMQ8SWr8tiQrhElqXc599TlWCtsPeMuu71hSLVTrqevjqnuc8AP8f_za1-pxJkoKpgW30BvThH7UUVBKCKUOapnDDLwKABzzv-TpGc6719PpiUIJD9UUF4BEP43i3unvWi7Zc0i2tXM./download",
Google Doc	Created from Box; downloaded from Google Drive	Zip File Name : gd/snapshot Zip File Name : gd/metadata Zip File Name : gd/signature Zip File Name : gd/debuginfo	kMDItemWhereFroms = ("https://docs.google.com/document/u/0/d/1W_A6dUcVSu4ewqz_VYKAr2B0Uy7ywxNmrzTuCZ65LiI/export?format=docx", "https://drive.google.com/drive/u/0/my-drive")
PDF	Created from Box; in Google Drive, save as PDF.		kMDItemCreator = "Google" kMDItemWhereFroms = ("https://docs.google.com/presentation/u/2/d/1lUTobez6A7D5reNQ5rRY5_RO6o7PKqXgGfmFeurGXKnrlg/export/pdf?id=1lUTobez6A7D5reNQ5rRY5_RO6o7PKqXgGfmFeurGXKnrlg&pageid=p", "https://docs.google.com/presentation/d/1lUTobez6A7D5reNQ5rRY5_RO6o7PKqXgGfmFeurGXKnrlg/edit?_gfid=docs_editor_frame&fileUrl=https://api.box.com/fsip/files/390856936531&jsh=m;/_/scs/apps-static/_/js/k%3Doz.gapi.en.eUmlrZ-GjRk.O/am%3DwQ/rt%3Dj/d%3D1/rs%3DAGLTcCPbVaczsDu16R3q9EnCF7wlxlmADg/m%3D__features__&parent=https://app.box.com&pfname&rpctoken=26551390&tpat=z7XHRAkvXSbZP8ol8CD1ucS92w7ljrlJ&tpatExpirationTime=1548654820000&usegapi=1")

Embedded metadata is limited to document type, but macOS stores extended metadata attributes, which includes source.



Logging for the Cloud Ecosystem is far more robust, although still being explored and understood.

API ENDPOINTS

G SUITE	https://www.googleapis.com/gmail/v1/users/userId/settings/forwardingAddresses https://www.googleapis.com/gmail/v1/users/userId/settings/autoForwarding https://www.googleapis.com/gmail/v1/users/userId/settings/imap https://www.googleapis.com/gmail/v1/users/userId/settings/pop https://www.googleapis.com/gmail/v1/users/userId/settings/filters	https://alertcenter.googleapis.com/v1beta1/alerts https://www.googleapis.com/admin/reports/v1/activity/users/userKey https://www.googleapis.com/admin/reports/v1/activity/users/userKey ***or all***/applications/***applicationName***
OFFICE 365	https://graph.microsoft.com/beta/auditLogs/signIns https://graph.microsoft.com/beta/me/mailFolders/inbox/messagerules https://graph.microsoft.com/beta/auditLogs/directoryAudits https://graph.microsoft.com/v1.0/identityRiskEvents https://graph.microsoft.com/v1.0/anonymousIpRiskEvents https://graph.microsoft.com/v1.0/impossibleTravelRiskEvents	https://graph.microsoft.com/v1.0/leakedCredentialsRiskEvents https://graph.microsoft.com/v1.0/malwareRiskEvents https://graph.microsoft.com/v1.0/suspiciousIpRiskEvents https://graph.microsoft.com/v1.0/unfamiliarLocationRiskEvents https://graph.microsoft.com/beta/riskyUsers https://graph.microsoft.com/beta/me/messages https://manage.office.com/api/v1.0/{tenant_id}/activity/feed/{operation}
SLACK	https://api.slack.com/audit/v1/ https://api.slack.com/events-api https://slack.com/api/users.info https://slack.com/api/search.all	
SALESFORCE	https://developer.salesforce.com/docs/atlas.en-us.object_reference.meta/object_reference/sforce_api_objects_eventlogfile.htm https://developer.salesforce.com/docs/atlas.en-us.object_reference.meta/object_reference/sforce_api_objects_loginhistory.htm https://developer.salesforce.com/docs/atlas.en-us.object_reference.meta/object_reference/sforce_api_objects_verificationhistory.htm	https://developer.salesforce.com/docs/atlas.en-us.object_reference.meta/object_reference/sforce_api_objects_connectedapplication.htm https://yourInstance.salesforce.com/services/data/v20.0/sobjects/Account/
BOX	https://api.box.com/2.0/events https://api.box.com/2.0/recent_items https://api.box.com/2.0/events	
DROPBOX	https://api.dropboxapi.com/2/team/reports/get_activity https://api.dropboxapi.com/2/team_log/get_events https://api.dropboxapi.com/2/users/get_account	

The best data is available through event/audit endpoints and user/application settings.

CONCLUSION

We’re on the brink of a collaboration revolution where the technology is catching up to the shift in values. We finally realize we are not alone in solving problems.

More than ever before, the powerful desire for change is outpacing the desire for recognition and profit. Instead we’re reaching for satisfaction in knowing that our work contributed to changing the world.

The best is yet to come.

OBSIDIAN

THANK YOU

JFORNESS@OBSIDIANSECURITY.COM
NEWPORT BEACH, CA